RSA® Authentication Manager 8.2

Service Pack 1 Patch 8 Readme

February 2018
Prerequisite Release:
RSA Authentication Manager 8.2 Service Pack 1

Contents

Before Installing This Patch

Note: All RSA Authentication Manager 8.2 SP1 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 8.2 SP1 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 8.2 SP1 before installing this patch. See the *RSA Authentication Manager 8.2 SP1 Setup and Configuration Guide* for instructions.

Installing a Patch

The RSA Authentication Manager 8.2 SP1 Patch 8 ZIP file (**am-update-8.2.1.8.0.zip**) contains the following file:

- **am-update-8.2.1.8.0.iso**. The RSA Authentication Manager 8.2 SP1 Patch 8 ISO file 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 8.2 SP1 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 8.2 SP1 Patch 8

RSA Authentication Manager 8.2 SP1 is a prerequisite release for this patch. Version 8.2 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 8.2.
4. Install Service Pack 1
5. Install this patch.

New Features and Enhancements in SP1 Patch 7

Web Tier Qualification for RHEL 7.4

RSA has qualified the Authentication Manager 8.2 SP1 Patch 7 web tier for compatibility with Red Hat Enterprise Linux version 7.4.

New Features and Enhancements in SP1 Patch 3

Change the Auto-Registration Queue Size

To address issue AM-31274, SP1 Patch 3 allows you to configure the number of agents that can be queued for auto-registration. Consider using this feature to increase the queue size if you need to auto-register a large number of agents (more than 1000) simultaneously.

To set auto-registration queue size for the first time:

1. Log on to the primary appliance using an SSH client.
2. Change directories:
   ```
   cd /opt/rsa/am/utils
   ```
3. Type the following, then press ENTER:
   ```
   ./rsautil store -a add_config
   auth_manager.agent_protocol.auto_reg_queue_size <x> GLOBAL INTEGER
   ```
   where *<x>* is the queue size limit you want to set.
4. Restart all Authentication Manager services on the primary server and replicas:
   ```
   cd /opt/rsa/am/server
   ./rsaserv restart all
   ```

To update auto-registration queue size:

1. Log on to the primary appliance using an SSH client.
2. Change directories:
   ```
   cd /opt/rsa/am/utils
   ```
3. Type the following, then press ENTER:

```
./rsautil store -a update_config
auth_manager.agent_protocol.auto_reg_queue_size <x> GLOBAL INTEGER
```
where <*x*> is the updated auto-registration queue size you want to set.

4. Restart all Authentication Manager services on the primary server and replicas:
```
cd /opt/rsa/am/server
./rsaserv restart all
```

New Features and Enhancements in SP1 Patch 1

Hide Menu Items from Administrators

To address issue AM-31082, SP1 Patch 1 allows you to hide menu items in the Security Console from administrators (except Super Admins). The menu items can be entire submenus or specific items in a menu. You can enable verbose tracing to see which items have been hidden by this command. Hiding menu items in the Security Console does not prevent administrators from accessing the function through other means, such as the Admin SDK.

To hide menu items from Administrators:

1. Log on to the primary appliance using an SSH client.
2. Change directories:
```
cd /opt/rsa/am/utils
```
3. Type the following, then press ENTER to hide menu items from administrators:
```
./rsautil store -a add_config
auth_manager.security_console.permissions.hidden_menu_items
<item1>,<item2>,<item3> GLOBAL STRING
```
where <*item1*>,<*item2*>,<*item3*> is a comma-separated list of the items you want to hide. For example:
```
./rsautil store -a add_config
auth_manager.security_console.permissions.hidden_menu_items
IssueSoftwareTokenBatch GLOBAL STRING
```
hides the “Distribute Software Tokens in Bulk” menu option from administrators.
4. Restart all Authentication Manager services on the primary server and replicas:
```
cd /opt/rsa/am/server
./rsaserv restart all
```

To restore hidden menus:

1. Log on to the primary appliance using an SSH client.
2. Change directories:
```
cd /opt/rsa/am/utils
```
3. Type the following, then press ENTER to restore hidden menus:
```
./rsautil store -a update_config
auth_manager.security_console.permissions.hidden_menu_items "" GLOBAL
```
4. Restart all Authentication Manager services on the primary server and replicas:
```
cd /opt/rsa/am/server
./rsaserv restart all
```

Generate Text-Based Report of Current Configuration Settings

To address issue AM-31059, SP1 Patch 1 allows you to generate a CSV or XML report that lists all current configuration and policy settings for Authentication Manager. You can analyze this report using third-party tools to monitor changes to the Authentication Manager configuration over time.

To generate the configuration settings report:

1. Log on to the primary appliance using an SSH client.
2. Change directories:
   `cd /opt/rsa/am/utils`
3. Type the following, then press ENTER to generate the report:
   `./rsautil export-config -o <OutputFile>`
   where `<OutputFile>` is the file name for the report.

   The report uses CSV format by default. Add the `-x` option to generate the report in XML format.

   Note: The file name must be unique. This command cannot overwrite an existing output file.

Known Issues

If the scheduled time is changed for a log archive job after Patch 7 (or later) is installed, the log archive job do not run on replica instances.
Tracking Number: AM-31718
Problem: After installing Patch 7 (or later), scheduled log archive jobs do not run on replica instances if the scheduled time for the job is changed in the Security Console.
Workaround: After changing the scheduled time for the log archive job, restart services on the replica instance.

After running to completion, the archive audit log batch job shows batch job status as only 50% complete on replica instances.
Tracking Number: AM-31717
Problem: The status of the archive audit log batch job shows 50% completion on replica instances after the job has finished running.
Workaround: None.

When batch jobs are run on both primary and replica instances, duplicate batch job entries appear on the replica instance.
Tracking Number: AM-31716
Problem: Duplicate batch job entries appear on replica instances after running batch jobs on both primary and replica instances.
Workaround: None.

Authentication Manager does not boot if 8.2 SP1 Patch 4 or later is installed and rolled back, then a patch update lower than Patch 4 is installed.
Tracking Number: AM-31714
Problem: After installing and rolling back Authentication Manager 8.2 SP1 Patch 4 or later, then rolling back that patch and applying a patch update lower than Patch 4, Authentication Manager no longer boots.
Workaround: Contact RSA Customer Support for assistance.

Patches 2, 3, and 4 do not install successfully on Dell PowerEdge R230 and R630 hardware appliances. Patch 1, if installed, cannot be rolled back.
Tracking Number: AM-31472

Problem: Attempting to upgrade from Authentication Manager 8.2 SP1 to Patch 2, 3, or 4 on Dell PowerEdge R230 or R630 hardware appliances causes the error "Unable to retrieve current platform specification. Platform mismatch detected." Upgrading to Patch 1 works as expected, but the update cannot be rolled back once installed.
Workaround: Only apply RSA Authentication Manager 8.2 SP1 Patch 5 or later to Dell PowerEdge R230 and R630 hardware appliances. Do not apply earlier patches, or you may need to restore the original system image. Patch 5 contains all of the updates provided in earlier patches.

After exporting and importing users and tokens, imported users who have fixed passcodes are prompted to set new PINs for on-demand authentication (ODA).

Tracking Number: AM-31304
Problem: AM-29134 addresses an issue where users with fixed passcodes were prompted to set new PINs after being exported and imported, but the issue still occurs for ODA users.
Workaround: None.

After installing SP1 Patch 3 and updating logging settings to record Operations Console events in the syslog, the events do not appear as expected.

Tracking Number: AM-30940
Problem: SP1 Patch 3 addresses an issue where Operations Console events were not properly recorded in the syslog. After installing SP1 Patch 3 or later, an additional workaround is required to fully resolve the issue.
Workaround: *****After installing SP1 Patch 3 or later and configuring logging to send Operations Console events to the syslog, do the following to restart the RSA admin service:

1. Log on to the appliance using an SSH client.
2. Type the following, then press ENTER:
   `/opt/rsa/am/server/rsaserv restart admin nodep`

After promoting a replica instance to primary, attempting to promote the former primary instance back to primary status fails.

Tracking Number: AM-30394, AM-30564
Problem: Promoting a replica instance to primary succeeds, but subsequent attempts to promote the former primary instance back to primary status fail, triggering the message "Promotion was unsuccessful. Unable to extract logs from original primary."
Workaround:

1. Log on to the appliance using an SSH client.
2. Change directories:
   `cd /opt/rsa/am/utils`
3. Type the following, then press ENTER to update TLS 1.2 Mode properties:
   `/rsautil store -a enable_min_protocol_tlsv1_2 <setting> restart`
   The command creates a required property in the file. It is recommended you assign <*setting*> as false. If you want to enforce strict TLS 1.2 Mode, assign it as true. Older Windows clients will not work with strict TLS 1.2 mode.

Local backup fails after planned promotion of a replica instance.

Tracking Number: AM-30364
Problem: After promoting a replica instance to primary, attempting to make a local backup from the new primary fails, triggering the message "An error occurred while backing up the system: Failed to backup the system files."
Workaround:

1. Log on to the appliance using an SSH client.
2. Change directories:
   `cd /opt/rsa/am/utils`

3. Type the following, then press ENTER to update TLS 1.2 Mode properties:
   `/rsautil store -a enable_min_protocol_tlsv1_2 <setting> restart`
   The command creates a required property in the file. It is recommended you assign <*setting*> as false. If you want to enforce strict TLS 1.2 Mode, assign it as true. Older Windows clients will not work with strict TLS 1.2 mode.

Do not promote a version 8.1 SP1 replica instance if there is a version 8.2 primary instance
Tracking Number: AM-29322
Problem: After the primary instance has been upgraded to version 8.2, promoting a version 8.1 SP1 replica instance for disaster recovery creates a second primary instance.
Workaround: If the upgrade to version 8.2 does not succeed, you must restore from a backup file, a VMware snapshot, or a Hyper-V checkpoint. Always apply version 8.2 to the primary instance before upgrading the replica instances in your RSA Authentication Manager 8.1 SP1 deployment.

Defects Fixed in This Patch

8.2 SP1 Patch 8

SP1 Patch 8 contains fixes for the following issues:

AM-31765 – Problems related to parsing and printing packet data existed in the tcpdump Linux command line tool.

AM-31699 – 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.

8.2 SP1 Patch 7

SP1 Patch 7 contains fixes for the following issues:

AM-31736 – It was possible to import iOS CTKIP software tokens to Android devices, and vice versa.

AM-31607 – The version of Oracle WebLogic used by Authentication Manager and the web tier was 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 8.2 SP1 Setup and Configuration Guide* for instructions.

AM-31600 – 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-31593 – The file **AMBulkAdmin.jar** was deleted from /opt/rsa/am/utils/lib when Authentication Manager 8.2 SP1 patch update 4, 5, or 6 was installed.

AM-31585 – A serious security issue existed in the RSA Authentication Manager Security Console.

AM-31570 – Attempting to access the Self-Service Console Help from the Self-Service Console resulted in a 404 error.

AM-31411 – In some cases, attempting to view associated users for a RADIUS profile failed, triggering an error message.

AM-31243 – 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-31236 – Special characters in reports caused problems when the reports were exported in CSV format and viewed using Microsoft Excel.

AM-30859 – Archived logs were not stored under the **/opt/rsa/am/Log_archive** path as specified in the Security Console.

AM-30530 – 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.

8.2 SP1 Patch 6

SP1 Patch 6 contains fixes for the following issues:

AM-31596 – A problem with the RSA Authentication Manager 8.2 SP1 Spanish Language Pack caused a display issue in the Security Console. To resolve this issue, download and install the updated language pack from RSA Link.

AM-31550 – In some cases, a message indicating that a trusted realm relationship must be repaired appeared after successful migration of an Authentication Manager 8.2 deployment for which no trusted realms were configured.

AM-31539 – After installing Patch 5, importing users sometimes caused a DataNotFound error, and some users with replacement tokens were not imported as expected.

AM-31484 – X-Frame-Options, X-Content-Type, and X-XSS-Protection header options for some parts of the Self-Service Console were either missing or incorrect.

AM-31462 – In some cases, Authentication Manager 8.2 P5 replica instances stopped responding to authentication requests due to a timeout issue.

AM-31449 – A problem with the RSA Authentication Manager 8.2 SP1 German Language Pack caused a display issue in the Security Console. To resolve this issue, download and install the updated language pack from RSA Link.

AM-31427 – Input fields on the Dashboard page of the Security Console were vulnerable to Cross-Site Scripting (XSS) attacks.

AM-31403 – Administrators lacked an option to manually transfer the dump file from a primary instance to a replica instance to facilitate replica synchronization in environments where network latency and packet transmission problems interfered with the automated transfer process. Contact RSA Customer Support if you need to perform a manual dump file transfer.

AM-31285 – HTTP Strict-Transport-Security headers were not included in responses sent between the web tier and the curl command-line interface tool.

AM-31281 – 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-29022 – 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.

8.2 SP1 Patch 5

SP1 Patch 5 contains fixes for the following issues:

AM-31472 – Patches 2, 3, and 4 cannot be installed on Dell PowerEdge R230 and R630 hardware appliances. Patch 1, if installed, cannot be rolled back. Patch 5 can be installed and rolled back on both appliances as expected.

AM-31458 – In some deployments, the **rsautil** file became corrupted, which prevented the replication service on the primary instance from starting.

AM-31421 –The time zone region drop-down menu on the Date and Time Settings page of the Operations Console incorrectly listed the offset for the Europe/Moscow time zone as UTC+4 rather than the correct offset, UTC+3.

AM-31408 – The Authentication Manager 8.2 Extension Code text box, which allows for the extension of evaluation licenses, was not visible or usable in Patch 2, Patch 3, or Patch 4.

AM-31381 – Authentication Manager did not properly migrate replacement tokens when exporting and importing users with tokens from one deployment to another.

AM-31355 – In some deployments, after a backup to a Windows shared folder was interrupted due to network or port problems, all subsequent backup attempts also failed, displaying the message "Another task in progress. Please wait for it to finish."

AM-31326 – In some deployments, when registering authentication agents that use TCP connections, such as web agents and the RSA SecurID Access identity router, the key negotiation service sometimes used an incorrect certificate from the keystore.

AM-31240 – The Identity Source Mapping page of the Security Console was vulnerable to a Cross-Site Scripting (XSS) attack.

AM-31227 – The Linux kernel used by Authentication Manager was vulnerable to a denial of service attack as described in CVE-2017-8890.

AM-30952 – For users with replacement tokens in some deployments, if an error occurred while unassigning old tokens and updating the replacement token status during authentication, the replacement tokens for those users were left in a corrupt state where they could not be assigned or unassigned, their status did not appear in the Help Desk Admin Portal, and new replacement tokens could not be assigned.

AM-30944 – In certain deployments, the Security Console job Copy CLU Audit Logs stopped working and triggered an "exception while decrypting" error.

AM-29809 – Application Trust Certificates were displayed in the Trusted Realm Name drop-down menu on the Add New Trusted User page of the Security Console. As part of the fix for this issue in Patch 5 and later versions, you can add a trusted user only when a trusted realm exists.

AM-29413 – Authentication Manager 8.1 and later versions did not support password integration with RSA Authentication Agent for Microsoft Windows if certain special characters (such as å, ä, ö, Å, Ä, or Ö) were present in the password.

8.2 SP1 Patch 4

SP1 Patch 4 contains fixes for the following issues:

AM-31303 – The version of Oracle WebLogic used by Authentication Manager and the web tier was 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 8.2 SP1 Setup and Configuration Guide* for instructions.

AM-31302 – The version of Java used by Authentication Manager and the web tier was 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 8.2 SP1 Setup and Configuration Guide* for instructions.

AM-31300 – Users with “Auth Mgr User Admin” or “Auth Mgr Token Admin” administrative roles could not send SMS test messages for on-demand authentication.
AM-31291 – Authentication Manager did not include the date field in the mail header for on-demand authentication emails.

AM-31290 – The User Dashboard did not load properly if a user had a period-separated name with three or more parts, where the first part of the name was capitalized (for example, Ext.name.name).

AM-31280 – When updating user profile information using the web tier or the Self-Service Console, users could provide email addresses with invalid domains, which bypassed built-in email validation and prevented administrators from editing the affected user profiles until the invalid domains were corrected.

AM-31272 – The version of SUSE Enterprise Linux used by Authentication Manager was vulnerable to several security exploits.

AM-31053 – A null pointer exception occurred when running the Administration API command “SendTestSMSMessageCommand”.

AM-30860/AM-31007 – On Internet Explorer 11, when attempting to export users with tokens and filtering the users by group membership, Super Admins could not select and move groups from the Available Groups list to the Selected Groups list.

AM-30357 – The country code for Montenegro (+382) did not appear in the **Default country code** drop-down menu on the **SMS Configuration** tab when configuring on-demand tokencode delivery in the Security Console.

AM-26911 – If the activity log contained a large amount of data (approximately 28 million rows in test cases), the **Recent Authentication Activity** section of the User Dashboard in the Security Console did not load and display activity data.

8.2 SP1 Patch 3

SP1 Patch 3 contains fixes for the following issues:

AM-31274 – Super Admins lacked the ability to configure queue size for automatic agent registration. The new configuration value `auth_manager.agent_protocol.auto_reg_queue_size` allows you to adjust the queue size limit. For instructions, see New Features and Enhancements in SP1 Patch 3.

AM-31149 – After assigning emergency access to a new token for one user in the Security Console, the unassigned tokens list for all other users became empty.

AM-31130 – In certain cases, a timeout error occurred while attempting to download troubleshooting logs from the Operations Console for Authentication Manager instances running on slow or overtaxed servers.

AM-31020 – The message “system is unusable” appeared in the syslog each time an authorized administrator made a successful configuration change in the Security Console.

AM-30940 – Operations Console login events were not recorded in the syslog. After installing SP1 Patch 3 (or later), additional steps are required to fully resolve this issue. For instructions, see Known Issue AM-30940.

AM-30530 – In certain cases, after configuring a secondary network interface for an Authentication Manager instance, the IP address of the secondary interface appeared as the primary IP address in the Security Console.

AM-29134 – After exporting and importing users and tokens, imported users who had fixed passcodes were prompted to set new PINs. See Known Issue AM-31304 for more information related to this fix.

8.2 SP1 Patch 2

SP1 Patch 2 contains fixes for the following issues:

AM-31185 – The Self-Service Console allowed users unlimited attempts to change their PIN or password.

AM-31131 – A null pointer exception sometimes occurred when a Citrix agent performed risk-based authentication with offline password recovery and update service requests.

AM-31097 – Authentication Manager and the web tier used a version of Oracle WebLogic that was vulnerable to CVE-2017-3531. 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 8.2 SP1 Setup and Configuration Guide* for instructions.

AM-30949 – In certain deployments, the Security Console stopped responding and authentication problems occurred due to an out-of-memory error.

AM-30698 – The Self-Service Console was not fully localized into Norwegian.

AM-30403 – The UTC dates and times for Operations Console events were incorrect compared to the local log times and UTC timestamps for other types of events in the rsa_logrep.ims_log_audit_rt table.

AM-30168 – License Type descriptions in the Security Console have been updated to reflect current license types.

AM-29574 – Security Console, Operations Console, and Self-Service Console pages did not include X-XSS-Protection headers, which are used by some web browsers to make cross-site scripting attacks more difficult to exploit.

AM-28890 – The Remote Syslog did not log real-time timestamps for OC_OS_PASSWORD_CHANGE events.

AM-27112 – When viewing users with assigned tokens in the Security Console, administrators were not able to sort users by username in the **Assigned To** field.

8.2 SP1 Patch 1

SP1 Patch 1 contains fixes for the following issues:

AM-31091 – Third-party security tests identified issues related to ICMP redirection, environment variables, and file permissions and associations.

AM-31086 – The Users Enabled for On-Demand Authentication report did not run successfully if the userid field for any of the records included in the report was null.

AM-31082 – Super Admins lacked the ability to hide specific Security Console menu items, such as the "Distribute Software Token in Bulk" option in the Manage RSA SecurID Tokens section, from lower-level administrators. The new configuration value `auth_manager.security_console.permissions.hidden_menu_items`

allows you to hide menu items from administrators (except Super Admins). For instructions, see New Features and Enhancements in SP1 Patch 1.

AM-31079 – The RSA Authentication Manager appliance operating system did not start successfully if the NTP server was unreachable.

AM-31077 – Distributing Soft Tokens from the Security Console in the "Distribute Software Token in Bulk" interface without specifying any search criteria redistributed all Soft Tokens in a security domain and required all Soft Tokens to be updated for authentication use. You must now check **Select All Tokens** to perform this task.

AM-31076 – Hostname information was not recorded in the header section of log messages sent from multiple Authentication Manager servers to a remote syslog server.

AM-31072 – Replacing a fob-style token with a fob-style soft token did not retain the PIN if the PIN included an alphabetic character.

AM-31070 – Attempting to grant or revoke user group access to one or more restricted agents selected from the results of a search triggered the error "System internal error. Please contact your system administrator."

AM-31059 – Super Admins lacked the ability to generate a text file detailing current configuration and policy data for Authentication Manager. The new command-line utility export-policy-config allows you to export all configuration and policy settings in CSV or XML format. For instructions, see New Features and Enhancements in SP1 Patch 1.

AM-31057 – In certain deployments, virtual appliance CPU load exceeded 100% and authentication attempts were unsuccessful due to a problem with socket handling for UDP requests.

AM-31048 – In certain deployments, the Security Console stopped responding due to an out-of-memory error.

AM-31047 – If the hardware clock on the appliance was not updated by the NTP server and indicated a significantly different time from the operating system clock, all authentication attempts were unsuccessful and triggered the error "Passcode reuse or previous token code detected."

AM-31046 – Deployments with large numbers of trusted groups (approximately 2000 in test cases) caused a spike in CPU load and degraded performance during authentication and related administrative activities.

AM-31045 – Software token requests made through the Self-Service Console incorrectly required administrators to grant approval for distribution of the token.

AM-31044 – In deployments without Risk-Based Authentication or On-Demand Authentication licenses, users who were not enabled for RBA sometimes triggered the error "RBA/ODA feature is not licensed. Principal cannot be enabled for RBA/ODA null" when logging into a custom portal.

AM-31043 – If a primary Active Directory (AD) stopped responding and Authentication Manager connected to a failover AD, but the failover AD also stopped responding and subsequently recovered, Authentication Manager was unable to reconnect to the failover AD.

AM-31042 – If a user without any assigned tokens requested a hardware token through the Self Service Console and the request was approved, but not distributed, by an administrator who was subsequently removed from the identity source database, other administrators could not distribute the token, and encountered the following error: "There was a problem processing the request, unexpected error during command com.rsa@ucm.request.AdditionalTokenRequestCheckCommand execution".

AM-30948 – In certain deployments with a large number of users (around 100,000 or more), generating a report of all users in the deployment required significantly more time than expected.

AM-30939 – An error occurred when downloading troubleshooting files from the Operations Console in cases where the System Log Report file size was too large.

AM-30913 – CK-KIP provisioning failed when attempting to use a software token profile that did not specify the device type. You can now use the same profile to provision software tokens for different device types by clearing the DeviceSerialNumber value from the profile before saving and distributing assigned tokens.

AM-30899 – The Linux-based operating system on the RSA Authentication Manager appliance was susceptible to a number of security vulnerabilities, including several related to the tcpdump service.

AM-30727 – When distributing software tokens using Dynamic Seed Provisioning in Authentication Manager 8.2, the **URL without Activation Code** delivery method option was not displayed in the Security Console.

AM-30721 – The **Profile Name** field on the Add Software Token Profile page of the Security Console was vulnerable to Cross-Site Scripting attacks.

AM-30590 – The Token Management Snap-In, installed on an Active Directory server, did not connect to Authentication Manager when the minimum protocol TLS1.2 was enabled on the Authentication Manager server.

AM-30255 – Authentication Manager and the web tier did not enforce HTTP Strict Transport Security headers.

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.

February 2018

Trademarks

Intellectual Property Notice

Open Source License