RSA® Authentication Manager 8.4

Patch 4 Readme

June 2019

Prerequisite Release:
RSA Authentication Manager 8.4

Contents

What's New in Patch 4

RSA Authentication Manager 8.4 Patch 4 introduces new features that make it easier than ever for you to adopt modern multifactor authentication from RSA with minimal infrastructure updates to your deployment:

- Use the Security Console Home page to quickly configure a seamless connection to the cloud.

- Authenticate with a Push notification to your mobile device; No agent updates required.

- Manage Cloud Authentication Service users in the Authentication Manager User Dashboard.

For more information on these important new features, see New Features and Enhancements in Patch 4.

Before Installing This Patch

Note: All RSA Authentication Manager 8.4 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 8.4.

Before installing this patch, review the following guidelines:

- You must upgrade RSA Authentication Manager to version 8.4 before installing this patch. See the *RSA Authentication Manager 8.4 Setup and Configuration Guide* for instructions.

- You must have at least 4 GB of free disk space to apply the patch.

- You must apply this patch to the primary and all replica instances in your RSA Authentication Manager 8.4 deployment. Make sure you apply the patch to the primary instance before applying the patch to the replica instances.

- Before using the new feature in Patch 4 that connects 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 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.

- 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 4. See the web-tier server *Readme* for information on the updates to the web-tier server.

Installing This Patch

The RSA Authentication Manager 8.4 Patch 4 ZIP file (**am-update-8.4.0.4.0.zip**) contains the RSA Authentication Manager 8.4 Patch 4 ISO file, **am-update-8.4.0.4.0.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 8.4 to locate patches.

If you have already specified a location, see

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.

     o 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**

     o (Optional) In the **Windows Username** field, enter a username. If your Windows share configuration requires it, enter the domain and username.

     o (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 4.

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 4.

- 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.

- Reinstall the web tier. An updated web-tier server (available *here*) is available with Patch 4. See the web-tier server *Readme* for information on the updates to the web-tier server.

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 8.4

RSA Authentication Manager 8.4 is a prerequisite release for this patch.

Version 8.4 does not support direct migration from earlier versions. To use existing data from earlier versions of RSA Authentication Manager, see "Upgrading RSA Authentication Manager" on RSA Link at https://community.rsa.com/docs/DOC-100620.

New Features and Enhancements in Patch 4

RSA Authentication Manager 8.4 Patch 4 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 4 introduces the following new features.

Easily Connect RSA Authentication Manager 8.4 Patch 4 to the Cloud Authentication Service and Deploy Modern MFA

Patch 4 allows you to more easily connect RSA Authentication Manager to the Cloud Authentication Service and quickly roll out modern MFA to your users. You use a Security Console wizard to configure the connection and invite users to authenticate to the Cloud.

To start using this feature, see *Connect RSA Authentication Manager to the Cloud Authentication Service* on RSA Link.

Authenticate with a Push Notification to Your Mobile Device; No Agent Updates Required

Users can access resources protected by existing RSA authentication agents, including existing agents that use UDP or TCP protocols, by entering their existing RSA SecurID PIN and tapping Approve on a registered device. You do not need to replace or update your existing agents or RSA Ready products, and users do not need to memorize a new PIN.

As in previous integrations, RSA Authentication Manager accepts tokencodes generated by the RSA SecurID Authenticate app. Users install the Authenticate app on a supported device to generate tokencodes. Authentication Manager does not support PINs for Authenticate Tokencode.

REST protocol authentication agents can continue to authenticate to the cloud with any form of multifactor authentication that is supported by the Cloud Authentication Service, such as Approve authentication, biometric methods such as fingerprint verification, hardware devices such as RSA SecurID Token and FIDO Token, and context-based authentication using factors such as the user's location and network.

Manage Cloud Authentication Service Users in the RSA Authentication Manager User Dashboard

The new integration also allows your Help Desk Admins to manage Authenticate app users in the RSA Authentication Manager User Dashboard:

- Manage Authenticate app users:
    - Enable or disable a user in the Cloud Authentication Service
    - Synchronize a user in the Cloud Authentication Service
    - Delete or undelete a user from the Cloud Authentication Service
- Unlock a user's SMS Tokencode, Voice Tokencode and Authenticate Tokencode
- Change a user's SMS Tokencode or Voice Tokencode phone number
- Delete a user's registered device or browser

The earlier approaches that connected Authentication Manager to an identity router do not support this feature.

New Features and Enhancements in Patch 3

RSA Authentication Manager 8.4 Patch 3 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 3 introduces a new optional field for an AMBA command.

Force a Password Change When Adding a User in AMBA

The **AU** command in AMBA adds a new user and optionally adds the user to an existing group. If a security domain and identity source are not provided, then the user is added in the RSA Authentication Manager internal database and the default security domain (SystemDomain).

Action	**AU**
Required Fields	LastName, DefLogin
Optional Fields	FirstName, Email, CertDN, ChangePwdFlag, DefShell, GrpName, GrpDefLogin, GrpDefShell, UserPwd, IdentitySource, SecurityDomain, EnableFlag, ForceGroupSearch, AttributeName, AttributeValue, AttributeName1, AttributeValue1, AttributeName2, AttributeValue2, AttributeName3, AttributeValue3, AttributeName4, AttributeValue4

To address AM-33260, Patch 3 adds the new, optional **ChangePwdFlag** field that allows you to force a password change while using the **AU** action to add a user. The CSV input file can include the **ChangePwdFlag** field with a value of true or false. The default value is false.

For example, the CSV file could contain the following data:

```
action,deflogin,lastname,UserPwd,ChangePwdFlag,EnableFlag
au,User1,User1,Password$,true,true
au,User2,User2,Password!,true,true
```

After you run the following AMBA command, each user is prompted to change their password during their first successful login:

```
./rsautil AMBulkAdmin  -a SuperAdminUserID -P SuperAdminPassword --
verbose -m 0 -i au.csv
```

New Features and Enhancements in Patch 2

RSA Authentication Manager 8.4 Patch 2 includes all new features and enhancements introduced in version 8.4 Patch 1 and all version 8.3 patches. In addition, Patch 2 includes the following item.

Disable the Offline Authentication Port

To address issue AM-32336, version 8.4 Patch 2 allows you to disable the offline authentication port. If your RSA Authentication Manager deployment does not use offline authentication, which allows users to authenticate when they are not connected to the network, then you might want to prevent security scans from finding that the default offline authentication port 5580/TCP is enabled and listening.

Authentication Manager does not allow you to disable this port if offline authentication is enabled for any security domains in your deployment. For more information, see "Offline Authentication Policy" on RSA Link at https://community.rsa.com/docs/DOC-77354.

Procedure

1. In the Security Console, click **Setup > System Settings**.

2. Under **Authentication Settings**, click **Agents**.

3. Under **Communication Ports**, click the **Disable Offline Authentication Port** checkbox.

4. Click **Save**.

New Features and Enhancements in Patch 1

RSA Authentication Manager 8.4 Patch 1 includes all new features and enhancements introduced in version 8.3 patches. In addition, Patch 1 includes the following items.

Support for Microsoft Active Directory 2019

RSA now officially supports Microsoft Active Directory 2019 as an identity source.

VMware Virtual Appliance Qualified on the VMware ESXi 6.7 Server

RSA has qualified the RSA Authentication Manager 8.4 Patch 1 VMware virtual appliance for compatibility with the VMware ESXi 6.7 server.

Web Tier Qualification for Red Hat Enterprise Linux 7.6 Server (64-Bit) and Windows Server 2019

RSA has qualified the RSA Authentication Manager 8.4 Patch 1 web tier for compatibility with Red Hat Enterprise Linux 7.6 Server (64-bit) and Windows Server 2019.

Known Issues

User Dashboard displays an Enable button for users who are disabled in Active Directory
Tracking Number: AM-33201
Problem: After you apply Patch 4 and configure a connection to the Cloud Authentication Service, the Authentication Manager User Dashboard can display Cloud Authentication Service users. If a user is disabled in Active Directory, the Cloud Authentication User Profile continues to display the **Enable** button, even though the user status is correctly displayed as disabled.
Workaround: The user can be enabled in Active Directory.

User Dashboard displays details for one Cloud Authentication Service user if two users have the same email ID in two different Active Directory identity sources
Tracking Number: AM-33204
Problem: After you apply Patch 4 and configure a connection to the Cloud Authentication Service, the Authentication Manager User Dashboard can display Cloud Authentication Service users. If two users have the same email ID in two different Active Directory identity sources, the RSA Authentication Manager User Profile can display details for both users, but the Cloud Authentication User Profile can only synchronize and provide for one user.
Workaround: Before inviting users to authenticate to the Cloud Authentication Service, clean up your identity sources so that each email ID belongs to only one user.

If the SMTP Mail Service is not available, error messages are not displayed until every user invitation to authenticate to the Cloud Authentication Service has timed out
Tracking Number: AM-33467
Problem: After you apply Patch 4, when you invite users to authenticate to the Cloud Authentication Service, success, warning, and error messages are not displayed until the system has processed every invitation. If the SMTP Mail Service is not available, error messages are not displayed until each invitation has taken one minute to time out. For example, ten invitations can take almost ten minutes to time out, but ten successful invitations result in a success message within a few seconds.
Workaround: When you configure the SMTP Mail Service, make sure to test the connection. If a large number of invitations are sent, you do not need to wait for a response. Instead, you can view the success, warning, and error messages in the system and audit logs.

Security Console message says that users were notified by e-mail but the e-mail (SMTP) server did not send any notifications
Tracking Number: AM-33526
Problem: After an administrator approves token provisioning requests, users are notified by e-mail. The Security Console can display a message that users were sent e-mail notifications, but the System Activity Monitor reports that the e-mail (SMTP) server did not notify the users.
Workaround: Before sending e-mail notifications to users, configure an e-mail (SMTP) server. For instructions, see "*Configure the SMTP Mail Service*" on RSA Link.

Cloud Authentication Service User Event Monitor Does Not Display the Latest User Status
Tracking Number: AM-33789
Problem: After you apply Patch 4 and configure a connection to the Cloud Authentication Service, the Authentication Manager User Dashboard displays a Cloud Authentication Service User Event Monitor. You can view a user's cloud authentication activity and event monitor messages in real time, but the most recent user status messages from an identity source are not displayed.
Workaround: The Cloud Authentication Service does not automatically update information from identity sources. Click **Refresh** to obtain the most recent information from the identity source.

Canceling the Cloud Authentication Service Configuration page returns you to the Settings page
Tracking Number: AM-33798
Problem: After you apply Patch 4 and configure a connection to the Cloud Authentication Service, you can select **Edit Connection Settings** on the Security Console Home page. On the Cloud Authentication Service Configuration page, if you click **Cancel**, you are returned to the System Settings tab on the Settings page.
Workaround: Clicking **Cancel** in Authentication Manager always returns you to the area in which you are making updates. To return to the Security Console Home page, click **Home**.

Web Tiers page does not indicate that a reinstall is required after you apply Patch 4
Tracking Number: AM-34010
Problem: Patch 4 includes third-party software updates that require you to reinstall the web tier. After applying Patch 4, the Web Tiers page in the Operations Console displays the **Update** button for each web tier, instead of "Reinstall Required."
Workaround: After you reinstall the web tier, the correct status is reported in the Operations Console.

You must upgrade all replica instances to Patch 4 before you connect to the Cloud Authentication Service
Tracking Number: AM-34011
Problem: Multifactor authentication methods can fail if you connect to the Cloud Authentication Service before you upgrade all existing replica instances to Patch 4. If you connect to the Cloud before upgrading the replica instances to Patch 4, those replica instances cannot be used for Cloud authentication methods.
Workaround: Delete any replica instances that were upgraded after connecting to the Cloud. Then add new replica instances and upgrade them to Patch 4.

An error message is not displayed if the invitation to authenticate to the Cloud Authentication Service fails for more than 500 users
Tracking Number: AM-34114
Problem: After you apply Patch 4, if more than 500 users are invited to authenticate to the Cloud Authentication Service and the invitation fails for all users, the Security Console displays the misleading statement "The number of users found exceeds the search results limit of 500. Change your search criteria to narrow your search." The correct messages display if the invitation succeeds for some or all of the users.
Workaround: You can view the success, warning, and error messages in the Administration Activity Monitor.

Defects Fixed in This Patch

Version 8.4 Patch 4

RSA Authentication Manager 8.4 Patch 4 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 4 contains fixes for the following issues:

AM-30943. On the License Status page, "Reached limit" is displayed instead of "Approaching limit" when the maximum number of replica instances have been added.

AM-33243. In the report output, the Administrative Scope column now shows the scope present for each administrative role.

AM-33479. Backup errors result if it takes too much time to back up to a Windows shared folder. To resolve this issue, you can increase the timeout period for backing up to a remote system. Run the following command line utility (CLU) to add a database variable with the default value of 60 seconds:

```
./rsautil store -o admin -a add_config
auth_manager.remote.backup.copy.timeout.sec 60 GLOBAL 501
```

Update the timeout period, for example, to 120 seconds, by running the following command:

```
./rsautil store -o admin -a update_config
auth_manager.remote.backup.copy.timeout.sec 120 GLOBAL 501
```

AM-33747. Fixed an issue in which the RSA Authentication Manager Bulk Administration utility was unable to parse the **SoftTokenProfile** header.

AM-33788. An error was generated when a non-administrator ran the "Authentication Activity Report Filtered By Security Domain" with an "Unspecified" security domain.

AM-33846. RSA Authentication Manager does not save the user password when password integration is implemented with RSA Authentication Agent for Citrix StoreFront, when logging into StoreFront with Risk Based Authentication.

AM-33988. Previously, RSA Authentication Manager users who no longer had an assigned authenticator were unable to use the RSA SecurID Authenticate app until an administrator enabled them using a command line utility. This issue has been fixed.

Version 8.4 Patch 3

RSA Authentication Manager 8.4 Patch 3 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 3 contains fixes for the following issues:

AM-33733. Applying patches to RSA Authentication Manager 8.4 sometimes fails because of pending changes to Oracle WebLogic files.

AM-33265. Resolved an issue in which hidden basic user attributes and identity attributes were erased when an administrator updated a user record.

AM-33260. An administrator can force a password change while using the AU command to add a user in AMBA. For more information, see above on page 9.

AM-33207. Updated some components used by Authentication Manager that were susceptible to security vulnerabilities.

AM-33205. Updated the operating system on the appliance to address security vulnerabilities in SUSE Linux components.

AM-32722. Corrected an issue in which the URL for logging on to the Self-Service Console could be modified.

AM-32500. The User ID for logging on to the Self-Service Console was saved in the browser's cache.

AM-32478. Filtering the Authentication Activity Report by security domain resulted in unexpected events if a non-administrator ran the report.

AM-32340. When the virtual host certificate was restored from a backup to a new primary instance, the certificate password was not restored.

AM-26302. A scroll bar allows you to see more than three Assigned SecurID Tokens in the User Dashboard.

AM-25077. In the Self-Service Console, tokens were being displayed in a random order that changed every time a user accessed the home page.

Version 8.4 Patch 2

RSA Authentication Manager 8.4 Patch 2 includes all fixes in version 8.4 Patch 1 and version 8.3 Patch 6. In addition, Patch 2 contains fixes for the following issues:

AM-33242, AM-33071. After upgrading to RSA Authentication Manager 8.4, certificates that are at least 2048 bits are required. If the Authentication Manager is configured with LDAPS and the https plugin to deliver ODA code, and the connection to the LDAP and SMS provider servers is configured with SSL key exchange algorithms DH (Diffie-Hellman) and DHE, the connection fails. To work around the issue, you can run the following command line utility (CLU) to turn on the pre-configured cipher list for SSL connections:

```
./rsautil store -a add_config ims.tls.cipher_list.use_via_trust true
GLOBAL BOOLEAN
```

AM-32916. Updated the warning message that displays if you add an RSA Authentication Manager license file that is not compatible with the current license.

AM-32862. RSA Authentication Manager created duplicate users in trusted realms because the user name was case-sensitive.

AM-32721. Updated the operating system on the appliance to address security vulnerabilities in SUSE Linux components.

AM-32661. Fixed the GetSiteStatusCommand feature of the Authentication Manager SDK so that it can retrieve replication status when retrieving instance information. The command returns 0, 1, or 2:

> 0 - Unknown: cannot get the status from the system.
>
> 1 - Normal: HEALTHY, ATTACHING or SYNCHRONIZING
>
> 2 - Unhealthy: FAILED, UNHEALTHY, OUT_OF_SYNC or OFFLINE

The Operations Console provides the details for each status.

AM-32336. Added a **Disable Offline Authentication Port** checkbox in the Security Console, under **Setup > System Settings > Agents**. If you are not using offline authentication, you can select this checkbox to prevent security scans from finding that the default offline authentication port 5580/TCP is enabled and listening. For instructions, see Disable the Offline Authentication Port.

AM-31664. 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.

AM-30842. Added a command line utility (CLU), change-admin-password, that allows an administrator to change the Security Console password:

```
./rsautil change-admin-password -u | -- username <username> -p | --
oldpassword <password> -n | --newpassword <password> -c | --
newpasswordAgain <password>
```

Version 8.4 Patch 1

RSA Authentication Manager 8.4 Patch 1 includes all fixes in version 8.3 Patch 6. Patch 1 contains fixes for the following issues:

AM-32701. The AMBA REPT action now shows the **SoftTokenProfile** field.

AM-32688. In some cases, offline authentication did not work consistently for users with multiple tokens.

AM-32687. The Security Console displayed a misleading success message after unsuccessful attempts to delete a user from the parent group of a nested subgroup.

AM-32686. In some cases, a timing issue during RADIUS server startup prevented planned promotion of a replica instance to primary instance.

AM-32684. After promoting a replica instance, synchronization problems occurred if either the primary or replica instance included mixed-case characters in its hostname.

AM-32676. The version of Oracle WebLogic used by Authentication Manager and the web tier was 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 8.4 Setup and Configuration Guide* for instructions.

AM-32675. A "Requested READ on security domain unauthorized" error occurred if an administrator for a security sub-domain attempted to run a Token Expiration Report for users with expired tokens within the sub-domain.

AM-32674. A formatting problem prevented web browsers from recognizing the X-Content-Type-Options header on Authentication Manager console pages.

AM-32673. Most console pages and some responses now include Content-Security-Policy headers.

AM-32671. Some components used by Authentication Manager were susceptible to security vulnerabilities.

AM-32670. The domain password was stored in cleartext. Any authenticated Operations Console administrator could obtain the Windows Share Password that was used to configure a Windows Share as an update source.

AM-32669. Password hashing for the operating system now allows SHA-512.

AM-32668. 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-32663. The RSA Authentication Manager configuration and policy settings report now includes archive table data. This allows administrators to monitor configuration changes over time.

AM-32662. Authentication Manager did not support uploading patches greater than 2GB in size through a web browser.

AM-32660. 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-32659. AMBA 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.

AM-32658. When revisiting the **Administration > Archive Audit Logs > Schedule Log Archival page** in 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-32657. Authentication Manager now supports sending critical system event notifications when scheduled log archive jobs fail.

AM-32655. Added a timestamp to the Trace log in verbose mode when a response is sent over the network.

AM-32654. 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-32653. AMBA now includes a CPADC (Clear Principal Attribute Data Clear) command to clear existing custom attribute data for custom attributes that are assigned to a principal (user).

AM-32652. For the AMBA **Add Agent Host** (AAH) command, a Super Admin can use the new **AgentNewHostName** parameter to update the agent hostname.

AM-32642. The List All User Alias report would not run when there were too many user aliases and migrated user aliases that contained commas.

AM-32641. After server restarts, users who had registered a device for Risk-Based Authentication were incorrectly prompted to re-register their device.

AM-32640. It was possible to save an rsaadmin password in the Operations Console which contained a backslash character (\), but the administrator could not use that password to log in. The Operations Console now rejects passwords containing backslash.

AM-32638. 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-32609. Added the agent IP address to the Trace log for troubleshooting.

AM-32563. Fixed a connection issue between Authentication Manager and the Cloud Authentication Service. A firewall rule was causing UDP and TCP port changes to affect each other.

AM-32562. Security vulnerabilities were resolved by updating operating system components, including updates to the SUSE Linux kernel.

AM-32532. AMBA now provides an **ETL** (Extend Software Token Lifetime) command that extends the lifetime of software tokens. The TokSerial field is required for tokens that require a new expiration date.

AM-32506. AMBA can set the Authentication Type as Tokencode using a software token profile while deploying a token.

AM-32491. The **rsautil** command did not export XML in the correct format.

AM-32478. When the Authentication Activity report was filtered by Security Domain, it also displayed administrative authentication activity that was not part of any Security Domain.

AM-32445. The SUSE Linux kernel and other operating system components used by Authentication Manager were susceptible to several security vulnerabilities.

AM-32362. Troubleshooting logs were too large to easily send to RSA Customer Support. To make the files smaller, the Operations Console now excludes archive logs when administrators download troubleshooting logs.

AM-31907. The **imsTrace.log** did not rotate when the maximum file size was reached.

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.

Trademarks

RSA, the RSA Logo, SecurID, and EMC are either registered trademarks or trademarks of Dell Inc throughout the world. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Intellectual Property Notice

This software contains the intellectual property of Dell Inc or is licensed to Dell Inc 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 Dell Inc.

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.