RSA® Authentication Manager 8.6

Patch 4 Readme

Before Installing This Patch

Note: All RSA Authentication Manager 8.6 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 8.6.

Before installing this patch, review the following guidelines:

- You must upgrade RSA Authentication Manager to version 8.6 before installing this patch. For more information, see Upgrading RSA Authentication Manager on RSA Link.
- You must have at least 4 GB of free disk space to apply the patch.
- You must apply this patch to the primary instance before applying the patch to the replica instances in your deployment.
- If you have a replicated environment, all replica instances must be running and replicating successfully before you apply the patch to the primary or replica instances.
- SSH clients and SCP clients can no longer connect to the appliance with weaker algorithms, for example, MD5 and 96-bit MAC algorithms. It may be necessary to upgrade your SSH and SCP clients to more recent versions that can handle more restrictive SSH algorithms.
- An updated web-tier server (available here) is also available with Patch 1. See the web-tier server Readme for information on these updates.

  Note: RSA recommends backing up your deployment before applying Patch 4. This cumulative patch updates the Oracle WebLogic Server to version 12.2.1.4. RSA first included this update in Patch 1. Rolling back Patch 4 does not revert the WebLogic upgrade.

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

Installing This Patch

The RSA Authentication Manager 8.6 Patch 4 ZIP file (**am-update-8.6.0.4.0.zip**) contains the RSA Authentication Manager 8.6 Patch 4 ISO file, **am-update-8.6.0.4.0.iso**, that is used to apply the patch to Authentication Manager.

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

- NFS share
- Shared folder on Windows

- DVD/CD
- ISO image on your local machine.

The overall steps to install this patch are as follows:

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

Specify a Product Update Location

To specify a product update location, perform the following procedure. This will allow RSA Authentication Manager 8.6 to locate patches.

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

Before You Begin

If you intend to scan for updates on an RSA-supplied DVD or CD, do the following:

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

Procedure

1. In the Operations Console, click **Maintenance** > **Update & Rollback**.
2. On the **Update & Rollback** page, the default update source is your local browser. To change that setting, click **Configure Update Source**.
3. On the Configure Update Sources page, specify a location for updates.

- To apply a specific update from your local machine, select **Use your web browser to upload an update**. You do not need to scan for updates.
- If you want to scan for updates on an NFS share, select **Use NFS as the update source**. Enter the full path, including the IP address or hostname where updates are stored. For example: **192.168.1.2:/updates**
- If you want to scan for updates on a Windows shared folder, select **Use Windows Share** as the update source.
    - In the **Windows Share Path** field, enter the full path, including the IP address or hostname where updates are stored. For example: **\\192.168.1.2\updates**
    - (Optional) In the **Windows Username** field, enter a username.
    - (Optional) In the **Windows Password** field, enter a password only if it is required by your Windows share configuration.
- If you want to scan for updates on a DVD or CD, select **Use DVD/CD as the update source**.

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

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

5. Click **Save**.

Next Steps

Do one of the following:

- If you configured your local web browser as the method to apply an update, see Apply Product Update below
- If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, scan for product updates.

Scan for Product Updates

If you configured an update location, you can scan to locate and review a list of available product updates.

Procedure

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

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

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

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

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

Next Steps

Apply the patch to the RSA Authentication Manager deployment.

Apply Product Update

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

Before You Begin

- RSA recommends backing up your deployment before applying Patch 4. This cumulative patch updates the Oracle WebLogic Server to version 12.2.1.4. RSA first included this update in Patch 1. Rolling back Patch 4 does not revert the WebLogic upgrade.

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

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

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

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

  If an external firewall blocks this port, the browser displays an inaccessible or blank web page, but the update can successfully complete.
- In a replicated deployment, all replica instances must be running and replicating successfully before you apply the update to the primary or replica instances. To verify the replication status, log on to the primary instance Operations Console, and then click **Deployment Configuration > Instances > Status Report**.

  After upgrading the primary instance, the replication status displays "Internal Replication Error" or another error message until all replica instances have been upgraded or patched.

Procedure

1. In the Operations Console, click Maintenance > Update & Rollback.
2. RSA recommends that you apply the most recent update. Do one of the following, depending on your configuration:

- To apply an update through your local web browser, do the following:
  a. Click **Upload & Apply Update**. Because browser uploads require additional processing, the Upload & Apply window may open slowly.
  b. Under **Update Location**, click **Choose File** to navigate to the location of the update. You cannot type the update location in the **Update Path** field.
  c. Click **Upload**.
- If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, do the following:
  a. Click **Scan for Updates**. **Available Updates** displays all of the updates that can be applied.
  b. Next to the update to apply, click **Apply Update**.

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

   As the update process begins, the following occurs:

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

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

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

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

   The Operations Console opens to the Log On page.

   Applying the patch results in the following:

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

Next Steps

- You can download a detailed log file containing the information that was displayed on the **Advanced Status View** tab. The file is named **update-**version-timestamp**.log**, where version is the update version number and timestamp is the time that the update completed. For instructions, see the Operations Console Help topic "Download Troubleshooting Files."
- After you have upgraded the primary instance and all of the replica instances, verify that replication and RADIUS replication is functioning correctly on the primary instance and each replica instance.
- Patch 4 includes an updated web-tier server (available here). See the web-tier server Readme for information on these updates.

Rolling Back This Patch

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

Patch 4 updates Oracle WebLogic Server to version 12.2.1.4. RSA first included this update in Patch 1. Rolling back Patch 4 does not revert the WebLogic upgrade.

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

Before You Begin

- If you are rolling back all version 8.6 patches, download any copies of the List all Authentication Agent Records report and the List all Installed Agents report that you ran after applying Patch 1 or later. After removing version 8.6 patches, the new **Agent Language** column prevents version 8.6 from opening the upgraded reports.
- (VMware only) Patch 1 or later adds support for the VMXNET 3 and E1000E virtual network adapters for the VMware virtual appliance. If you changed the default network adapter, you must do the following:

1. Manually add the E1000 virtual network adapter or connect the E1000 adapter if it is disconnected.
2. Delete the VMXNET 3 or E1000E virtual network adapter.
3. Reboot the virtual appliance.

Procedure

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

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

- **Version**. The version of the update. To see the current version of the Authentication Manager instance, refer to the top of the Update & Rollback page.
- **Updated on**. When 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.

Next Steps

After you roll back Patch 4 on the primary and replica instances, you must reinstall the previous version of the web tier:

- Patch 1 includes an updated web tier version (available here).
- The version 8.6 web tier is included in the RSA Authentication Manager 8.6 Extras download kit (available here).

For instructions, see "Reinstall the Web Tier section of the RSA Authentication Manager 8.6 Setup and Configuration Guide.

If you restore the version 8.6 web tier, the web tier status remains as "Online, reinstall required." This message

displays because the reinstalled web tier has an earlier version of WebLogic than the Authentication Manager instances. Functionality is not affected.

New Features and Enhancements in Patch 3

Patch 3 for version 8.6 includes all new features and enhancements introduced up to 8.6 Patch 2. In addition, version 8.6 Patch 3 introduces the following new feature:

Web Tier Qualification for Red Hat Enterprise Linux 8.4 Server (64-Bit)

This RSA Authentication Manager 8.6 Patch 3 web tier version supports the web tier on Red Hat Enterprise Linux 8.4 Server (64-bit).

Web Tier Qualification for Oracle Linux 7 Server (64-Bit)

This RSA Authentication Manager 8.6 Patch 3 web tier version supports the web tier on Oracle Linux 7 Server (64-bit).

New Features and Enhancements in Patch 2

Patch 2 for version 8.6 includes all new features and enhancements introduced in version 8.6 Patch 1. In addition, version 8.6 Patch 2 introduces the following new feature.

Automatic Removal of Log4J-2

RSA Authentication Manager 8.6 Patch 2 and the updated web-tier server automatically remove Log4J 2.x libraries.

Log4j-2 is an open-source Java-based logging utility used in enterprise and cloud applications. Security vulnerabilities were recently discovered, but RSA Authentication Manager and the web-tier server are not affected.

Authentication Manager and the web-tier server utilize a SecurID internally maintained and supported version of a log4j 1.2.x library separate and distinct from the Apache branch. This is a SecurID internal, special-purpose implementation and has no known, exploitable vulnerabilities.

For more information on log4j-2 issues, see RSA Customer Advisory: Apache Vulnerability | Log4j2 (CVE-2021-44228).

New Features and Enhancements in Patch 1

RSA Authentication Manager 8.6 includes all new features and enhancements introduced in the cumulative Patch 3 for version 8.5.

Patch 1 for version 8.6 includes the new features and enhancements introduced in version 8.5 Patch 4 and Patch 5. See New Features and Enhancements from Version 8.5 Patch 4 and Patch 5 on page 12

In addition, version 8.6 Patch 1 introduces the following new features.

Removed the Ability to Request a Cloud Authentication Service Account Through the Security Console

To address **AM-43736** Patch 1 removes the ability to request a Cloud Authentication Service account through

the Security Console. The Security Console no longer displays the **Request an account** link on the Home page or the **Request Account** checkbox on the Cloud Authentication Service Configuration page. You can continue to use your existing Cloud Authentication Service accounts.

If you need a new Cloud Authentication Service account, call SecurID Sales at 1 800 995 5095.

Send On-Demand Tokencodes with Both SMS and E-mail

To address **AM-43654** Patch 1 allows you to send on-demand tokencodes with both SMS text messages and e-mail, instead of allowing only one method per user. You configure this feature by running a command line utility (CLU) and adding e-mail delivery to the SMS configuration option for on-demand tokencodes.

After you select the **Add Delivery by E-mail** checkbox on the SMS Configuration tab, when you use the Security Console to select the delivery method for a user, you can choose SMS to send both a text message and an e-mail. You can locate users with the **Authentication** > **On-Demand Authentication** > **Enable Users** menu or in the User Dashboard.

Users who request on-demand tokencodes in the Self-Service Console can select from the methods you configure (SMS text message or e-mail). After you select the **Add Delivery by E-mail** checkbox, users who select SMS receive an SMS text message and an e-mail.

Enable On-demand Authentication by Both SMS and E-mail

A command line utility (CLU) adds the **Add Delivery by E-mail** checkbox on the SMS Configuration tab.

Before you begin

- Obtain the **rsaadmin** operating system password.
- You must be an Operations Console Administrator.

Procedure

1. Log on to the appliance using an SSH client.
2. When prompted, enter the operating system User ID, **rsaadmin**, and the operating system account password.
3. Change directories:

   ```
   cd /opt/rsa/am/utils
   ```

4. Run the following command line utility (CLU):

   ```
   ./rsautil store -a update_config auth_manager.sms.smtp.feature.enabled true GLOBAL
   BOOLEAN
   ```

5. When prompted, enter your Operations Console administrator user ID and password.
6. Flush the cache:
   1. In the Operations Console, click **Maintenance** > **Flush Cache**.
   2. If prompted, enter your Super Admin User ID and password, and click **OK**.
   3. Select **Flush all cache objects** and click **Flush**.

Add E-mail to the SMS Delivery Option

On the primary instance, you can select the **Add Delivery by E-mail** checkbox on the SMS Configuration tab.

You can remove the e-mail option from SMS by clearing the checkbox.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Click **On-Demand Tokencode Delivery**.
3. On the SMS Configuration tab, select the **Add Delivery by E-mail** checkbox to deliver tokencodes by both SMS and e-mail.
4. Click **Save**.

After you finish

E-mail delivery requires a configured e-mail (SMTP) server and a user e-mail address if the user selects Mobile Number (SMS) as the preferred option for on-demand authentication.

Make sure that you have configured the following:

- An e-mail (SMTP) server on the primary instance and each replica instance. See the Help topic Configure the SMTP Mail Service.
- User e-mail addresses. See the Help topic Configure E-Mail for On-Demand Tokencode Delivery.

Define Custom Attributes to Send Transaction-Specific Data During On-Demand Authentication

To address **AM-43643** Patch 1 lets you define custom attributes to send users transaction-specific data during on-demand authentication. This feature only supports REST-based authentication to RSA Authentication Manager.

After you define custom attributes for the clients that you developed with the SecurID Authentication API, you can provide these custom attributes in the on-demand tokencode message users receive.

For example, your users could receive a custom message that replaces the following variables with values:

```
To confirm that you want to <BUY or SELL> <number> shares of <stock symbol>, please enter the tokencode:
```

Users would enter a tokencode to confirm the transaction.

Provide Custom Attributes During On-Demand Authentication

You can develop clients that use custom attributes to provide transaction-specific information during on-demand authentication.

Before you begin

Use the SecurID Authentication API to define custom attributes for your REST-based, multifactor authentication clients. Your clients can use the existing SessionAttribute parameter to provide attributes during the Initialize interface.

During authentication, the initialization payload should contain the session attributes name and corresponding value. See the following example:

```
{

"authnAttemptTimeout": 180,

"clientId": "rest-007",
```

```
"subjectName": "adUsr",
"lang": "us_EN",
"sessionAttributes": [
{
"dataType": "STRING", "name": "DemoAttribute1", "value": "Demo Attribute1_value" }
,
{ "dataType": "STRING", "name": "DemoAttribute2", "value": "Demo Attribute2_value" }
],
"subjectCredentials": [],
"context":
{ "messageId": "test" }
}
```

For more information, see the SecurID Authentication API Developer's Guide.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Click **On-Demand Tokencode Delivery**.
3. On the **Tokencode Settings** tab, specify the on-demand tokencode message text that users receive and the message lifetime.

   Use the following syntax for your custom attributes:

   ```
   $S.<Custom Session Attribute name>
   ```

   Note: Do not remove $OTT from the message template. This variable is replaced with the tokencode in the actual message.
4. Click **Save**.

VMXNET 3 and E1000E Virtual Network Adapters Supported for the VMware Virtual Appliance

To address **AM-43265**. Redistributing a software token caused offline authentication to stop working for the MFA Agent for Microsoft Windows. This issue has been fixed.

AM-43263. Resolved an issue in which the **log4j.properties** file was not available after applying a patch.

AM-43195, Patch 1 adds support for the VMXNET 3 and E1000E virtual network adapters for the VMware virtual appliance. VMware describes these adapters. See Choosing a network adapter for your virtual machine (1001805).

To change the default E1000 virtual network adapter, do the following:

1. Apply Patch 1 on each Authentication Manager instance that uses the VMware virtual appliance.
2. Use the VMware vSphere Client to add the VMXNET 3 or E1000E virtual network adapter.

You can either disconnect the existing adapter to stop using it or delete the existing adapter to remove it from the virtual appliance.

3. Reboot the virtual appliance

If you roll back Patch 1, you must first manually add the E1000 virtual network adapter or connect the E1000 adapter if it is disconnected. Delete the VMXNET 3 or E1000E virtual network adapter. See Rolling Back This Patch on page 5 on page Rolling Back This Patch on page 5.

AMBA Supports Unlocking Specified Users

To address **AM-44483**, Patch adds the **ULSU** (Unlock Specified Users) command to use the default login or account name to unlock users. You can specify a single user or provide a list of users in a CSV file.

Action -> **ULSU**

Required Fields -> DefLogin

Optional Fields -> IdentitySource

Unlike the similar **ULU** (Unlock Users) command, you must already know which users need to be unlocked. You can search for locked users in the Security Console.

The **ULSU** command always searches the System Domain and all subdomains for the users that you specified. You can specify an optional identity source or search the internal database.

For example, a sample CSV file, called **ulsu.csv**, can contain the following data:

```
Action,DefLogin

ULSU,ulsuuser1

ULSU,ulsuuser2

ULSU,ulsuuser3

ULSU,ulsuuser4

ULSU,ulsuuser5

ULSU,ulsuuser6

ULSU,ulsuuser7

ULSU,ulsuuser8

ULSU,ulsuuser9

ULSU,ulsuuser10
```

Run the following command to unlock all specified users in the System Domain and all subdomains. Because an identity source is not specified, the command searches the internal database:

```
./rsautil AMBulkAdmin -a <oc admin> -P <oc admin password> -g -i ulsu.csv -o ulsu.log --
verbose
```

New Features and Enhancements from Version 8.5 Patch 4 and Patch 5

RSA Authentication Manager 8.6 Patch 1 adds the following new features and enhancements from version 8.5 Patch 4 and Patch 5.

AMBA Supports the Finding and Unlocking Up to 500 Users

To address **AM-41727**, Patch 1 adds the **ULU** (Unlock Users) command that allows AMBA to find and unlock up to a maximum of 500 locked users at the same time in the RSA Authentication Manager internal database and LDAP identity sources. To unlock more users, run the command again.

Action -> ULU

Required Fields -> None

Optional Fields -> IdentitySource, SecurityDomain, SubDomain, GrpName

The **ULU** command would be especially useful if some unforeseen event caused failed authentications and locked accounts. For example, if the RSA Authentication Manager primary instance had the incorrect time and this caused authentication failures. You can unlock multiple users in the Security Console, but more steps are required: You must use the **Identity > Users > Manage Existing** menu, do an advanced search to find "Locked Out Users," and then select and unlock up to 500 accounts at the same time.

The optional fields for the **ULU** command restrict the search as needed. For example, you can provide a SecurityDomain to search for locked out users in a specific security domain.

For example, a sample CSV file, called **ulu.csv**, can contain the following data:

```
Action,SecurityDomain

ULU,eu-realm
```

Run the following command to unlock up to 500 locked users in the eu-realm security domain and its subdomains:

```
./rsautil AMBulkAdmin -a <oc admin> -P <oc admin password> -g -i ulu.csv -o ulu.log --verbose
```

Hide or Show Agent Information in the User Dashboard

To address **AM-42856** and **AM-36889**, Patch 1 adds the ability hide or show agents in the User Dashboard. By default, the User Dashboard shows the agents that are associated with an individual user. When users are associated with hundreds of agents, you can choose to hide the agent information to avoid performance issues.

Procedure

1. Log on to the appliance operating system.
2. Change directories to `/opt/rsa/am/utils`.
3. You can hide or show agents:

   To hide agent information in the User Dashboard, run the following command line utility (CLU):

   ```
   ./rsautil store -a add_config auth_manager.dashboard.hide.agent true GLOBAL BOOLEAN
   ```

   To show the agent information, run the following command:

```
./rsautil store -a update_config auth_manager.dashboard.hide.agent false GLOBAL BOOLEAN
```

4. Change directories to `/opt/rsa/am/server`.
5. Run the following to restart all services:

   ```
   ./rsaserv restart all
   ```

Web Tier Qualification for Red Hat Enterprise Linux 8.3 Server (64-Bit)

As of RSA Authentication Manager 8.5 Patch 4, the web tier is supported on Red Hat Enterprise Linux 8.3 Server (64-bit).

Defects Fixed in Patch 4

RSA Authentication Manager 8.6 Patch 4 includes all fixes introduced in all versions 8.6 and 8.5 patches and security updates. In addition, Patch 4 also contains fixes for the following issues.

AM-47103: Fixed an issue wherein the RADIUS authentication with European characters had failed.

Note: If Clients use RADIUS authentication to enable UTF-8 encoding, then authentication will fail if the request has double byte Unicode variable. This issue has been fixed in 8.7 P1.

AM-46616: Fixed an issue wherein the RADIUS authentication on Primary and Replica instances had failed for clients who had special and non-Ascii characters in their shared secret.

AM-46736: Fixed an issue wherein the RADIUS authentication had failed when the RADIUS client associated agent was in a different sub security domain.

AM-46737: RADIUS authentication is successful when the "Username" attribute is assigned to a profile.

AM-46738: ODA functions accurately (for both SMS and Email) with Clickatell and Prove API (public facing) SMS configurations.

AM-46761: Updated SUSE Linux components used by RSA Authentication Manager.

AM-46855: Updated the Oracle WebLogic components used by RSA Authentication Manager to prevent potential security vulnerabilities. Java is rolled back to avoid a conflict with the AM 8.7 upgrade from P4 .

AM-47121: Fixed an issue to cleanup logs that are accumulated in the **appserver/wls/cfgtoollogs/opatch** directory in webtier and Authentication Manager.

Defects Fixed in Patch 3

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

AM-38662: Fixed an issue in which failover AD now takes less time to stabilize authentications when primary AD is down. Time latency between failover AD connection to successful authentication is approximately 2 minutes.

AM-43644: Fixed an issue for listing all active user’s session in Security Console Page after successful authentication.

AM-44951: Removed the Swagger UI in Authentication Manager and Web tier.

AM-45174: Patch 3 allows you to enable On-demand Authentication for multiple users both Internal Database/External Identity Source even for admin user who does not have superadmin role. See Send On-Demand Tokencodes with Both SMS and E-mail on page 8

AM-45475: Users can now perform successful RADIUS authentication after upgrading from Authentication Manager version 8.6 with custom console certificate.

AM-45941: Fixed an issue in which running CLU "rsautil manage-ssl-cert --regen-internal-ca" for second time does not give error, also radius authentication works fine.

AM-45965: Updated the Oracle WebLogic components used by RSA Authentication Manager to prevent potential security vulnerabilities.

AM-45966: Updated SUSE Linux components used by RSA Authentication Manager.

Defects Fixed in Patch 2

RSA Authentication Manager 8.6 Patch 2 includes all fixes introduced in all versions 8.6 and 8.5 patches and security updates. In addition, Patch 2 includes fixes for the following issues.

AM-45075. Updated the Oracle WebLogic components used by RSA Authentication Manager to prevent potential security vulnerabilities.

AM-45263. Updated the application server log4j-2 files to version 2.17 and then removed them. See Automatic Removal of Log4J-2 on page 7

AM-45076. Update OS components and kernel to address potential security vulnerabilities.

AM-45070. Unable to install RSA Authentication Manager 8.6 and 8.6 P01 web tier on Oracle Linux platforms. Fix has been given to support installation on Oracle Linux platforms from 8.6 Patch 2

AM-45055. Running CLU "rsautil manage-ssl-cert --regen-internal-ca" has not provided administrator with information about the required changes and need for restarting the AM services, this has been fixed.

AM-44454. Incorrect country code representation for Republic of Colombia has been corrected.

AM-44236. Backup failed to an extremely large NFS or windows share. This has been fixed.

AM-43763. Running CLU "rsautil manage-ssl-cert --regen-internal-ca" failed since upgrade to Authentication Manager 8.6. This has been fixed.

AM-43413. User reported insufficient authorization on accessing a URL. As fix removed the dashboard.

AM-42484. The CLU manage-readonly-dbusers do not need database restart for actions delete, update, and create.

Defects Fixed in Patch 1

RSA Authentication Manager 8.6 Patch 1 includes all fixes introduced in RSA Authentication Manager 8.5 Patch 4, Patch 5, and earlier patches. In addition, Patch 1 contains fixes for the following issues.

AM-44483. The ULSU (Unlock Specified Users) command uses the default login or account name to unlock users. You can specify a single user or provide a list of users in a CSV file. See VMXNET 3 and E1000E Virtual Network Adapters Supported for the VMware Virtual Appliance on page 10.

4. Apply Patch 1 on each Authentication Manager instance that uses the VMware virtual appliance.
5. Use the VMware vSphere Client to add the VMXNET 3 or E1000E virtual network adapter. You can either disconnect the existing adapter to stop using it or delete the existing adapter to remove it from the virtual appliance.
6. Reboot the virtual appliance.

If you roll back Patch 1, you must first manually add the E1000 virtual network adapter or connect the E1000 adapter if it is disconnected. Delete the VMXNET 3 or E1000E virtual network adapter. See Rolling Back This Patch on page 5 and AMBA Supports Unlocking Specified Users.

AM-44154. Fixed a certificate error that prevented Authentication Manager from creating a new connection to the Cloud Authentication Service. This issue only affected deployments that were upgraded from RSA Authentication Manager 8.5 Patch 5 to RSA Authentication Manager 8.6.

AM-44111. Updated the Oracle WebLogic and Java components used by RSA Authentication Manager to prevent potential security vulnerabilities. Updated Oracle WebLogic Server to version 12.2.1.4.

AM-44014. Updated SUSE Linux components used by RSA Authentication Manager to prevent potential security vulnerabilities.

AM-43982. Updated content security policy headers used by RSA Authentication Manager.

AM-43785, AM-43637. Fixed an issue in which authentication was unsuccessful due to an invalid character in a RADIUS attribute.

AM-43736. Removed the ability to request a Cloud Authentication Service account through the Security Console. If you need a new Cloud Authentication Service account, call SecurID Sales at 1 800 995 5095. You can continue to use your existing accounts. See Removed the Ability to Request a Cloud Authentication Service Account Through the Security Console on page 7.

AM-43654. Patch 1 allows you to send on-demand tokencodes with both SMS text messages and e-mail, instead of using only one method per user. See Send On-Demand Tokencodes with Both SMS and E-mail on page 8.

AM-43643. Patch 1 allows you to define custom attributes to send users transaction-specific data during on-demand authentication. See Define Custom Attributes to Send Transaction-Specific Data During On-Demand Authentication on page 9

AM-43607. Users with names that contain an apostrophe can now display in the Registered Devices or Browsers panel and the Cloud Authentication Service User Event Monitor panel in the User Dashboard.

AM-43265. Redistributing a software token caused offline authentication to stop working for the MFA Agent for Microsoft Windows. This issue has been fixed.

AM-43263. Resolved an issue in which the **log4j.properties** file was not available after applying a patch.

AM-43195. Patch 1 allows you to change the default E1000 virtual network adapter for the VMware virtual appliance. See VMXNET 3 and E1000E Virtual Network Adapters Supported for the VMware Virtual Appliance on page 10.

AM-42191. Users can now authenticate with PIN+Approve or PIN+Biometrics to disable online emergency tokencode authentication if the authenticator becomes available.

AM-42156. Users successfully authenticating with fixed online Emergency Token to access resources protected by Authentication Manager were locked by the Cloud Authentication Service. This issue has been resolved.

AM-41274. Added the language used by authentication agents to the telemetry data sent by Authentication Manager. A new **Agent Language** column is available for the List all Authentication Agent Records report and the List all Installed Agents report.

AM-40607. The Operations Console user interface now states that you need to upload an ISO file to apply an update.

Known Issues

1. Version 8.6 Cannot Access Agent Reports that Ran in a Patch

Tracking Number: **AM-44016**

Problem: Patch 1 or later adds a new **Agent Language** column to the List all Authentication Agent Records report and the List all Installed Agents report. After rolling back Patch 1 or later, version 8.6 is unable to access these reports.

Workaround: Before rolling back to version 8.6 without any patches, download any recent copies of these reports. To run these reports again, you must recreate the reports or apply Patch 1 or later.

2. RADIUS Clients Unable to Authenticate with the NAS IP Address

Tracking Number: **AM-43999**

Problem: RADIUS clients are unable to authenticate with the NAS IP address. The Windows Network Policy Server (NPS) reports that Authentication Manager did not process the authentication requests.

Workaround: Do the following:

1. Use the **rsaadmin** account to log on to the appliance operating system.
2. Change directories to `/opt/rsa/am/utils`.
3. Run the following command line utility (CLU) to change a configuration value from 'Packet-Src-IP-Address' to 'NAS-IP-Address':

   ```
   ./rsautil store -o <admin> -a update_config auth_manager.radius.rest_
   service.clientid.attribute.name 'NAS-IP-Address' GLOBAL 503
   ```

4. Change directories to `/opt/rsa/am/server`.
5. Run the following to restart all services:

   ```
   ./rsaserv restart all
   ```

3. When the AM 8.6 P3 was upgraded to 8.6 P4, Java was rolled back to an older version.

Tracking Number:**AM-47529**

Problem:When the AM 8.6 P4 is applied to an AM 8.4 P3 system, Java is not updated to the latest version, unlike the AM 8.6 P4 Web-tier. Although it could result in a web-tier warning ("Reinstall required"), the warning can be ignored.

Note: Reverting the AM 8.6 P4 to an older version will not resolve the issue.

Workaround:The issue is resolved in AM 8.7.

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.

© 1994-2022 RSA Security LLC or its affiliates. All rights reserved. RSA Conference logo, RSA, and other trademarks are trademarks of RSA Security LLC or its affiliates. For a list of RSA trademarks, https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

August 2022

Intellectual Property Notice

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

Open Source License

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