RSA® Authentication Manager 8.5

Patch 2 Readme

January 2021

Prerequisite Release:
RSA Authentication Manager 8.5

Contents

Before Installing This Patch

Note: All RSA Authentication Manager 8.5 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 8.5.

Before installing this patch, review the following guidelines:

- You must upgrade RSA Authentication Manager to version 8.5 before installing this patch. For more information, see Upgrading RSA Authentication Manager on RSA Link at https://community.rsa.com/docs/DOC-100620.
- 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.

Updated Web-Tier Server

Patch 2 includes an updated web-tier server (available here). See the web-tier server Readme for information on the updates to the web-tier server.

The Patch 2 web tier version includes the same updated Oracle WebLogic and Java software components as the Patch 1 Security Update 1 web-tier server.

If you have already applied the Patch 1 Security Update 1 web tier server, applying Patch 2 automatically updates the web-tier server to Patch 2. You do not need to update the web-tier server again.

Installing This Patch

The RSA Authentication Manager 8.5 Patch 2 ZIP file (**am-update-8.5.0.2.0.zip**) contains the RSA Authentication Manager 8.5 Patch 2 ISO file, **am-update-8.5.0.2.0.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
- Scan for Product Updates
- Apply Product Update

Specify a Product Update Location

To specify a product update location, perform the following procedure. This will allow RSA Authentication Manager 8.5 to locate patches.

If you have already specified a location, see Scan for Product Updates on page 3.

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 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 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 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 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

- 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 **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 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 2 includes an updated web-tier server (available here). See the web-tier server Readme for information on the updates to the web-tier server.

  If you have already applied the Patch 1 Security Update 1 web tier server, applying Patch 2 automatically updates the web-tier server to Patch 2. You do not need to update the web-tier server again.

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.

New Features and Enhancements in Patch 2

Patch 2 includes all new features and enhancements introduced in all version 8.5 and version 8.4 patches. In addition, Patch 2 introduces the following new features.

Using High Availability with RSA SecurID Authentication or Authenticate Tokencode when the Cloud Authentication Service is Not Available

When RSA Authentication Manager is connected to the Cloud Authentication Service, users can still authenticate when the Cloud Authentication Service is slow or not available. To address **AM-39183**, Patch 2 allows all users to be prompted for local authentication with Authenticate Tokencode or RSA SecurID authentication regardless of whether the authentication agent is configured in Authentication Manager mode or Cloud Authentication Service mode.

The following table shows two possible deployment options.

Scenario	Authentication Methods	High Availability
Direct connection to RSA Authentication Manager 8.5 with the UDP protocol or the REST protocol. Authentication Manager is connected to the Cloud Authentication Service	RSA Authentication Manager always validates RSA SecurID authentication, and always sends other authentication methods to the Cloud Authentication Service, for example, Authenticate Tokencode, Approve, and Device Biometrics.	When the Cloud Authentication Service is not available, Authentication Manager prompts users for local authentication with Authenticate Tokencode or RSA SecurID authentication.
Direct connection to the Cloud Authentication Service with the REST protocol is updated to use RSA Authentication Manager 8.5 as a secure proxy server. Authentication Manager is connected to the Cloud Authentication Service.	Authentication Manager sends all authentication requests which are to be proxied to the Cloud Authentication Service, for example, Approve, Device Biometrics, Authenticate Tokencode, RSA SecurID hardware and software tokens, Emergency Tokencode, SMS Tokencode, and Voice Tokencode.	When the Cloud Authentication Service is not available, Authentication Manager prompts users for local authentication with Authenticate Tokencode or RSA SecurID authentication.

For configuration instructions, see your *authentication agent documentation*.

Replica Instance Administrative Tasks

To address **AM-40623**, Patch 2 adds the ability to perform the following administrative tasks on replica instances:

- Clear a PIN
- Assign a Temporary Fixed Tokencode for Online Emergency Access
- Assign a Set of One-Time Tokencodes for Online Emergency Access
- Provide an Offline Emergency Access Tokencode
- View Real-Time Authentication Log Entries Generated on the Replica Instance

The primary instance is the only system in the deployment that allows you to perform all administrative tasks, but with Patch 2, administrators can clear PINs and provide emergency access to users on the primary instance or any replica instance.

This feature provides high availability and avoids downtime for administrative functions, when the primary instance is temporarily offline or replication is not available. For example, the primary instance might be offline for 15 minutes while a patch is applied or for a longer period during a major upgrade, but administrators can continue to assist users.

When the primary instance or replication is not available, there is no communication between the primary instance and the replica instances and there is no communication between replica instances. An administrator can use a replica instance to assist users, but the changes made by the administrator are only available to authentication agents using the respective server. For example, if an administrator generates an emergency access tokencode on Replica-2, only agents connected to Replica-2 would be able to authenticate using that emergency access token.

After replication is restored, the primary instance collects logs for the administrative tasks that were performed locally on the replica instances. All runtime authentication log entries are collected on the primary instance and replicated throughout the deployment. The most recent PIN changes and emergency access code changes are retained.

Note: Administrative permissions are required to perform these tasks on a primary or replica instance. By default, the pre-defined administrative roles Auth Mgr Privileged Help Desk, Auth Mgr Token Administrator, Auth Mgr User Admin, and Super Admin include the correct permissions.

Clear a PIN

You can use a primary instance or a replica instance to clear the current PIN for a user's token and set the token into New PIN mode.

When the primary instance is temporarily offline or replication is not available, the PIN changes and the associated runtime authentication log entries are only available on the replica instance. After replication is restored, the primary instance collects the runtime authentication log entries from the replica instance. The most recent PIN changes are retained.

Suppose that the primary instance went offline while being upgraded. The following scenarios are some examples of what could occur:

- A user's PIN is cleared on a replica instance, and a new PIN is created. When the primary instance is available again, replication occurs and the new PIN can be used on the primary instance or any replica instance.

- New PINs were separately created on more than one replica instance. When the primary instance is available again, the user can authenticate with the most recent PIN.
- Changes that occurred before the primary instance went offline are replaced by later changes that occurred on a replica instance.

You can clear an RSA SecurID PIN in the User Dashboard or by selecting an assigned RSA SecurID Token. See *User Dashboard* or *Clear an RSA SecurID PIN*.

Assign a Temporary Fixed Tokencode for Online Emergency Access

You can use a primary or replica instance to generate a temporary fixed tokencode. The temporary fixed tokencode gives a user temporary emergency access to resources protected by RSA Authentication Manager. This tokencode can be used when a user's RSA SecurID Token or RSA SecurID Authenticate app is temporarily unavailable and the user has network connectivity to RSA Authentication Manager.

When the primary instance is temporarily offline or replication is not available, you can use a replica instance to generate a temporary fixed tokencode. The temporary fixed tokencode can be used for online authentication to resources protected by the replica instance. After replication is restored, the most recent temporary fixed tokencode can be used for authentication to any Authentication Manager instance.

For example, suppose that the primary instance went temporarily offline while being upgraded. In this situation, there is no replication and there is no communication between replica instances. Two administrators on two replica instances each generate a temporary fixed tokencode as a replacement for a user's lost token. When the primary instance is available again, the temporary fixed tokencode that was created last can be used to authenticate to any Authentication Manager instance in the deployment.

You can assign a temporary fixed tokencode for online emergency access in the User Dashboard or by selecting an assigned RSA SecurID Token. See *Assign a Temporary Fixed Tokencode for Online Emergency Access*.

Assign a Set of One-Time Tokencodes for Online Emergency Access

You can use a primary or replica instance to generate a set of one-time tokencodes. These tokencodes can provide online emergency access for a user whose RSA SecurID Token or RSA SecurID Authenticate app is temporarily unavailable. Each one-time tokencode can be used once in place of the user's missing token. The set of tokencodes allows a user to authenticate multiple times without contacting an administrator each time.

When the primary instance is temporarily offline or replication is not available, you can use a replica instance to generate a set of one-time tokencodes. The set of tokencodes can be used for online authentication to resources protected by the replica instance. After replication is restored, all active emergency access tokencodes are accepted throughout deployment. Any tokencodes that were used by a user or cleared by an administrator are no longer available for authentication.

Suppose that the primary instance went offline while being upgraded. The following scenarios are some examples of what could occur:

- An administrator uses a replica instance to generate a set of one-time tokencodes. When the primary instance is available again, replication occurs and the set of one-time tokencodes can be used on the primary instance and any replica instance.
- Two administrators on two replica instances each generate a set of one-time tokencodes for the same user. When the primary instance is available again, all of the tokencodes that have not been used yet are accepted on the primary instance and any replica instance.

You can generate a set of one-time tokencodes for online emergency access in the User Dashboard or by selecting an assigned RSA SecurID Token. See *Assign a Set of One-Time Tokencode for Online Emergency Access*.

Provide an Offline Emergency Access Tokencode

You can use a primary or replica instance to generate an offline emergency access tokencode. A user needs offline emergency access when the user's Windows device cannot contact the Authentication Manager server through the network and the user's RSA SecurID Token is unavailable, or the user forgot his or her PIN.

When the primary instance is temporarily offline or replication is not available, you can use a replica instance to generate an offline emergency access tokencode.After replication is restored, the most recent offline emergency access tokencode is retained.

Suppose that the primary instance went offline while being upgraded. The following scenarios are some examples of what could occur:

- An administrator uses a replica instance to generate an offline emergency access tokencode. When the primary instance is available again, replication occurs and the offline emergency access tokencode can be used on the primary instance and any replica instance.
- Two administrators on two replica instances each generate an offline emergency access tokencode. When the primary instance is available again, if neither tokencode was used, the last offline emergency access tokencode that was generated is accepted on the primary instance or any replica instance.

You can provide an offline emergency access tokencode for an assigned token. See *Provide an Offline Emergency Access Tokencode.*

View Real-Time Authentication Log Entries Generated on the Replica Instance

When the primary instance or replication is not available, you can view recent runtime authentication log entries on the replica instance. Only entries for the replica instance are displayed.

When replication is restored, the log entries are replicated, and become available for viewing on the primary or any replica instance.

You can view system activity, such as log entries, in real-time by selecting an Activity Monitor in the Security Console. See *View Messages in the Activity Monitor*.

Removed Support for Requesting a Cloud Authentication Service Account Through the Security Console

RSA no longer supports requesting a Cloud Authentication Service account through the Security Console. If you try to request an account, your patch level determines the error message that you receive.

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.

Web Tier Qualification for Red Hat Enterprise Linux 7.9 Server (64-Bit)

As of RSA Authentication Manager 8.5 Patch 2, the web tier is supported on Red Hat Enterprise Linux 7.9 Server (64-bit).

New Features and Enhancements in Earlier Cumulative Patches

Each RSA Authentication Manager cumulative patch includes all new features and enhancements introduced in earlier patches.

What is New in Patch 1 Security Update 1

Patch 1 Security Update 1 includes all new features and enhancements introduced in Patch 1. In addition, Security Update 1 updates RSA Authentication Manager components to prevent potential security vulnerabilities.

Updated RSA Authentication Manager Components

To address **AM-39894**, Patch 1 Security Update 1 provides new versions of the Oracle WebLogic and Java components used by RSA Authentication Manager 8.5. These updates prevent the potential security vulnerabilities that were announced by Oracle as part of the *Oracle Critical Patch Update Advisory (CPU) for October 2020*:

- Oracle WebLogic

  CVE-2019-17267, CVE-2020-14841, CVE-2020-14825, CVE-2020-14859, CVE-2020-14820, CVE-2020-14757

- Oracle Java

  CVE-2020-14792, CVE-2020-14781, CVE-2020-14782, CVE-2020-14797, CVE-2020-14779

The update also resolves issue in components and features that are not used by Authentication Manager, such as the WebLogic Console (CVE-2020-14883, CVE-2020-14882, CVE-2020-11022 and CVE-2020-14750).

New Features and Enhancements in Patch 1

RSA Authentication Manager 8.5 includes all new features and enhancements introduced in the cumulative Patch 13 for version 8.4. Patch 1 for version 8.5 includes the following new feature introduced in Patch 14 for version 8.4:

Administrative Roles Have Separate Permissions to Unlock an Account or Enable and Disable Accounts

To address **AM-39487**, Patch 1 changes the permissions that you can select when you add or edit an administrative role. On the General Permissions tab, the **Unlock Accounts** checkbox and the **Enable/Disable Accounts** checkbox replace the combined **Enable/Disable/Unlock Accounts** checkbox. When you add or edit a predefined or custom administrative role, you can give the role permission to unlock accounts and you can give the role permission to enable and disable accounts.

When you apply Patch 1, both new permissions are enabled for any predefined or custom administrative roles that have the **Enable/Disable/Unlock Accounts** checkbox selected.

If you remove Patch 1, the **Enable/Disable/Unlock Accounts** checkbox is selected for administrative roles that have the **Unlock Accounts** checkbox enabled. If only the **Enable/Disable Account** checkbox is selected, then the **Enable/Disable/Unlock Accounts** checkbox is not selected.

When you restore Patch 1 from a backup created with an earlier version of Authentication Manager, the **Enable/Disable Accounts** checkbox is not selected. The **Unlock Accounts** checkbox is selected if the **Enable/Disable/Unlock Accounts** checkbox is selected in the backup file. For each administrative role that requires permission to enable and disable accounts, select the **Enable/Disable Accounts** checkbox.

Defects Fixed in This Patch

Version 8.5 Patch 2

RSA Authentication Manager 8.5 Patch 2 includes all fixes introduced in all version 8.5 and version 8.4 patches and security updates. In addition, Patch 2 includes fixes for the following issues:

AM-40623. The primary instance is the only system in the deployment that allows you to perform all administrative tasks, but Patch 2 allows administrators to clear PINs and provide emergency access to users on any primary or replica instance. For more information, see Replica Instance Administrative Tasks on page 8.

AM-40088. Resolved an HTTP 503 “Service Unavailable” error in the Security Console.

AM-39981. Fixed a minor labeling issue on the patch ISO file.

AM-39894. Provided new versions of the Oracle WebLogic and Java components used by RSA Authentication Manager 8.5. These new versions are also provided in Patch 1 Security Update 1.

AM-39620. Alphanumeric PINs are no longer case-sensitive for PIN+Approve authentication. Mixed case alphanumeric PINs are supported.

AM-39183. All users can be prompted for local authentication with Authenticate Tokencode or RSA SecurID authentication when the Cloud Authentication Service is slow or not available, regardless of whether the authentication agent is configured in Authentication Manager mode or Cloud Authentication Service mode. For more information, see High Availability with RSA SecurID Authentication or Authenticate Tokencode when the Cloud Authentication Service is Not Available on page 7.

AM-37192. Fixed an issue that prevented the RSA Authentication Manager SDK from doing iterative searches with more than one SSL client authenticated session.

Version 8.5 Patch 1 Security Update 1

RSA Authentication Manager 8.5 Patch 1 Security Update 1 includes all fixes introduced in all version 8.5 and version 8.4 patches. In addition, Security Update 1 addresses **AM-39894**. See Updated RSA Authentication Manager Components on page 11.

Version 8.5 Patch 1

RSA Authentication Manager 8.5 Patch 1 includes all fixes introduced in RSA Authentication Manager 8.4 Patch 14 and earlier patches. In addition, Patch 1 contains fixes for the following issues:

AM-39706. Updated the version of Oracle WebLogic used by Authentication Manager to prevent potential security vulnerabilities.

AM-39690. Fixed an issue that caused backups to freeze while backing up RSA RADIUS. This situation sometimes occurred after Back Up Now in the Operations Console was used to perform dozens of continuous manual backups at intervals of an hour or less.

AM-39675. Fixed the MinTokenLife option for the AMBA **Replace Token Automatic** (REPTA) command.

AM-39530. Added information about the Dell PowerEdge R240 to the *RSA SecurID Hardware Component Updates* page on RSA Link.

AM-39514. Corrected a field that was not localized into Japanese in the Self-Service Console.

AM-39513. Fixed an issue in which on-demand authentication was not enabled for a customer who was imported into a new deployment.

AM-39512. Fixed the "Administrators of a Security Domain" report to display the correct administrative scope.

AM-39489. Fixed an issue that caused email notifications to be sent based upon the last saved workflow policy, instead of the workflow policy for the user domain

AM-39488. When Authentication Manager is configured to not require a PIN for any tokens, Authenticate Tokencode users are no longer prompted to create a PIN.

AM-39486. Fixed an issue that caused a memory leak while backing up data

AM-39484. Updated the system log to provide more information on which Active Directory connection is being used. The system log now reports when the Directory URL (primary AD connection) fails and when the primary connection is restored

AM-39469. Can now delete CT-KIP activation codes for deleted users.

AM-39468. Resolved an issue with regenerating the root CA for trusted realms.

AM-39466. Resolved a certificate issue that blocked access to the Identity Router Setup Console.

AM-38418. The patch installer restores the PAM configuration to the auto-generated, default state. This could eliminate unsupported changes to this configuration which might cause problems in the RSA Authentication Manager.

AM-32381, AM-32382, AM-32383, AM-32384. Reject some cross-site scripting attempts as invalid.

Known Issues

Server Certificates and Software Token Files Include Additional Content at the End of the File

Tracking Number: AM-40515
Problem: When a server certificate or a software token distribution file is downloaded from the Security Console, extra HTML and JavaScript is included at the end of the file.
Workaround: To obtain the correct server certificate, use one of the following procedures:

- Use SSH to log on to the appliance operating system and retrieve a copy of the file:

  `/opt/rsa/am/config/src/resources/certs/server.cer`

- Use the Security Console to download the **server.cer** file and manually remove the extra content. Use a text editor to remove the HTML beginning with <meta http-equiv="X-UA-Compatible" and continuing through to the end of the file.

The **Software_Tokens.zip** file can be safely distributed.

A future update will resolve this issue.

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.

January 2021

Revised: November 2021

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.