RSA® Authentication Manager 8.4

Patch 2 Readme

March 2019

Prerequisite Release:
RSA Authentication Manager 8.4

Contents

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 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.
- If you have a replicated environment, all replica instances must be running and replicating successfully before you apply the patch to the primary or replica instances. On the primary instance, the replication status displays “Internal Replication Error” or another error message until all replica instances have been upgraded or patched.
- You must have at least 4 GB of free disk space to apply the patch.
- You must upgrade RSA Authentication Manager to version 8.4 before installing this patch. See the *RSA Authentication Manager 8.4 Setup and Configuration Guide* for instructions.
- 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.

Installing a Patch

The RSA Authentication Manager 8.4 Patch 2 ZIP file (**am-update-8.4.0.2.0.zip**) contains the RSA Authentication Manager 8.4 Patch 2 ISO file, **am-update-8.4.0.2.0.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

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 Scan for Product Updates on page 3.

Before You Begin

To scan for updates on an RSA-supplied DVD or CD, do the following:

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

Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. On the Update & Rollback page, the default update source is your local browser. To change that setting, click **Configure Update Source**.
3. On the Configure Update Sources page, specify a location for updates.
    - To apply a specific update, select **Use your web browser to upload an update**. You do not need to scan for updates.
    - To scan for updates on an NFS share, select **Use NFS as the update source**. Enter the full path, including the IP address or hostname where updates are stored. For example: **192.168.1.2:/updates**
    - To scan for updates on a Windows shared folder, select **Use Windows Share** as the update source.
        - In the **Windows Share Path** field, enter the full path, including the IP address or hostname where updates are stored. For example: **\\192.168.1.2\updates**
        - (Optional) In the **Windows Username** field, enter a username. If your Windows share configuration requires it, enter the domain and username.

    - (Optional) In the **Windows Password** field, enter a password only if it is required by your Windows share configuration.
  - To scan for updates on a DVD or CD, select **Use DVD/CD as the update source**.
4. To test the NFS or Windows share directory settings, click **Test Connection**.

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

Next Steps

Do one of the following:

- If you configured your local web browser as the method to apply an update, see Apply Product Update on page 4.
- If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, see Scan for Product Updates on page 3.

Scan for Product Updates

If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, you can scan to locate and review a list of available product updates. If you want to apply an update through your local web browser, then you do not need to scan for updates.

Procedure

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

   The system displays the progress of the scan on the **Basic Status View** tab. You can view more detailed information on the **Advanced Status View** tab.
3. Click **Done** to return to the Update & Rollback page.
4. In the **Applied Updates** section, click **Download Detailed History Log** for a complete update history.

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

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

Next Steps

Apply the patch to the RSA Authentication Manager deployment.

Apply Product Update

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

Before You Begin

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

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

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

  If an external firewall blocks this port, the browser displays an inaccessible or blank web page, but the update can successfully complete.
- Specify a Product Update Location, as described on page 2.
- If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, Scan for Product Updates, as described on page 3.
- In a replicated deployment, all replica instances must be running and replicating successfully before you apply the update to the primary or replica instances. To verify the replication status, log on to the primary instance Operations Console, and then click **Deployment Configuration > Instances > Status Report**.

  After upgrading the primary instance, the replication status displays “Internal Replication Error” or another error message until all replica instances have been upgraded or patched.
- Download and unzip the patch from RSA Link to a location that the primary or replica instance can access.

Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. RSA recommends that you apply the most recent update. Do one of the following, depending on your configuration:
   - To apply an update through your local web browser, do the following:
     a. Click **Upload & Apply Update**.
     b. Under **Update Location**, click **Browse** to navigate to the location of the update. You cannot type the update location in the **Update Path** field.
     c. Click **Upload**.
   - If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, do the following:
     a. Click **Scan for Updates**. **Available Updates** displays all of the updates that can be applied.
     b. Next to the update to apply, click **Apply Update**.

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

   As the update process begins, the following occurs:

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

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

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

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

   The Operations Console opens to the Log On page.

   Applying the patch results in the following:

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

Next Steps

- You can download a detailed log file containing the information that was displayed on the **Advanced Status View** tab. The file is named **update-*version-timestamp*.log**, where *version* is the update version number and *timestamp* is the time that the update completed. For instructions, see the Operations Console Help topic "Download Troubleshooting Files."
- After you have upgraded the primary instance and all of the replica instances, verify that replication and RADIUS replication is functioning correctly on the primary instance and each replica instance.

Rolling Back This Patch

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

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

Procedure

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

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

   - **Version**. The version of the update. To see the current version of the Authentication Manager instance, refer to the top of the Update & Rollback page.
   - **Updated on**. When the update was applied. If a log file is available, you can click **Download log** to save and read information about the update process.
   - **Updated by**. The user who applied the update.
   - **Action**. Displays the **Roll Back Update** button or the message "Cannot be rolled back."

2. To roll back the last update that was applied, click **Roll Back Update**. Only a reversible update can be rolled back.
3. Enter the password for the User ID **rsaadmin**, and then click **Rollback**.

   As the patch rollback process begins, the following occurs:

   - In the **Confirm Rollback Update** window, the **Basic Status View** tab shows the progress of the rollback preparation process. More detailed information appears on the **Advanced Status View** tab.
   - When the update preparation is complete, the **Confirm Rollback Update** window closes, and a new browser window opens in which to complete the rollback process.
   - In the new browser window, the Update Installer rolls back the update. The **Basic Status View** tab shows the progress of the update as it is rolled back. More detailed information appears on the **Advanced Status View** tab.

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

   The Operations Console opens to the Log On page.

Rolling back the patch results in the following:

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

Upgrading to RSA Authentication Manager 8.4

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 2

RSA Authentication Manager 8.4 Patch 2 includes all of the new features and enhancements introduced in version 8.4 Patch 1 and all of the 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 of the 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.

Defects Fixed in This Patch

Version 8.4 Patch 2

RSA Authentication Manager 8.4 Patch 2 includes all of the 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 of the 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 the 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.

March 2019

Trademarks

Intellectual Property Notice

Open Source License

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