RSA® Authentication Manager 8.4

Patch 13 Readme

June 2020

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 upgrade RSA Authentication Manager to version 8.4 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 and all replica instances in your RSA Authentication Manager 8.4 deployment. Make sure you apply the patch to the primary instance before applying the patch to the replica instances.
- Before using the Security Console wizard to connect Authentication Manager directly to the Cloud Authentication Service, you must upgrade your primary instance and all replica instances.
- If you have a replicated environment, all replica instances must be running and replicating successfully before you apply the patch to the primary or replica instances. On the primary instance, the replication status displays "Internal Replication Error" or another error message until all replica instances have been upgraded or patched.
- SSH clients and SCP clients can no longer connect to the appliance with weaker algorithms, for example, MD5 and 96-bit MAC algorithms. It may be necessary to upgrade your SSH and SCP clients to more recent versions that can handle more restrictive SSH algorithms.
- An updated web-tier server (available *here*) is also available with Patch 13. See the web-tier server *Readme* for information on the updates to the web-tier server.

Installing This Patch

The RSA Authentication Manager 8.4 Patch 13 ZIP file (**am-update-8.4.0.13.0.zip**) contains the RSA Authentication Manager 8.4 Patch 13 ISO file, **am-update-8.4.0.13.0.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.
        - (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 3.
- 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**. 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.
- An updated web-tier server (available *here*) is also available with Patch 13. See the web-tier server *Readme* for information on the updates to the web-tier server.

Rolling Back This Patch

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

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

Procedure

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

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

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

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

   As the patch rollback process begins, the following occurs:

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

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

   The Operations Console opens to the Log On page.

New Features and Enhancements in Patch 13

Patch 13 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 13 introduces the following new features.

Web Tier Qualification for Red Hat Enterprise Linux 7.7 Server (64-Bit)

RSA has qualified the RSA Authentication Manager 8.4 Patch 13 web tier for compatibility with Red Hat Enterprise Linux 7.7 Server (64-bit).

AMBA Supports Removing a Logon Alias from a Group

To address AM-37518, Patch 13 updates the **CAU** (Change or Add User) command with a new RemoveGrpDefLogin option to remove a logon alias from a group.

A logon alias allows users to log on with a user group ID. For example, users can have a User ID based on their first initial and last name, such as, “kmiller,” as well as an administrative User ID with a specific name, for example “root.” If a logon alias is established, Authentication Manager verifies the authentication using the user’s passcode, regardless of the User ID that the user entered to log on to the operating system.

Instead of removing a logon alias from a group, you can use AMBA to remove a user from a group with the **DUG** (Delete User from Group) command, but this command does not apply to external identity sources. For example, Authentication Manager cannot remove an Active Directory user from an Active Directory group. Instead, you can use the RemoveGrpDefLogin option for the **CAU** command to remove a logon alias from any group.

More Flexibility When Regenerating the Access ID and Access Key for REST Protocol Authentication Agents

After you use the RSA SecurID Authentication API to regenerate agent credentials, either in the Security Console or on a command line, you must provide REST protocol authentication agents with the new Access ID and Access Key. To address AM-37087, Patch 13 makes this process easier and more flexible:

- REST Protocol authentication agents can use the previous Access ID and Access Key for 60 days or a timeframe that you specify. This allows authentication to continue until the agents receive the new credentials. If necessary, you can extend the timeframe.
- You can restore the previous Access ID and Access Key. This provides a way to undo the process, for example, if the credentials were regenerated by mistake.
- You can list the current and previous credentials.
- System audit logs indicate when authentication agents use the previous credentials.

If you feel as though the Access ID and Access Key have been compromised, regenerate credentials two times before providing the new credentials to your agents.

Regenerate and Restore REST Protocol Authentication Agent Credentials

A new command line utility, manage-rest-access-credential, provides the ability to manage REST protocol authentication agent credentials. You can regenerate the Access ID and Access Key, restore the previous Access ID and Access Key, and list both the current and previous Access ID and Access Key.

After you regenerate credentials, you can use the previous credentials for authentication. If you restore the previous credentials, the credentials that you replaced can be used for authentication for 60 days or the timeframe that you specify.

Before You Begin

Obtain the **rsaadmin** operating system password.

Procedure

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

   ```
   cd /opt/rsa/am/utils
   ```
4. To regenerate the Access ID and Access Key, enter:

   ```
   ./rsautil manage-rest-access-credential -a generate
   ```

   To list the current and previous Access ID and Access Key, enter:

   ```
   ./rsautil manage-rest-access-credential -a list
   ```

   To restore the previous Access ID and Access Key, enter:

   ```
   ./rsautil manage-rest-access-credential -a restore
   ```
5. Restart the services on the primary instance. If there are replica instances, restart the services after replication is complete.
   a. Change directories:

      ```
      cd /opt/rsa/am/server
      ```
   b. Run the following:

      ```
      ./rsaserv restart all
      ```

Change the Timeframe for Using REST Protocol Authentication Agent Credentials

After you use the RSA SecurID Authentication API to regenerate agent credentials, REST Protocol authentication agents can use the previous Access ID and Access Key for up to 60 days or a timeframe that you specify. This allows authentication to continue until the agents receive the new credentials. If necessary, you can extend the timeframe.

Note: If you believe the Access ID and Access Key have been compromised, instead of changing the timeframe, regenerate credentials two times before providing the new credentials to your agents.

Before You Begin

Obtain the **rsaadmin** operating system password.

Procedure

1. Log on to the appliance using an SSH client.
2. When prompted for the user name and password, enter the operating system User ID, **rsaadmin**, and the operating system account password.

3. Change directories:

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

4. To change the number of days that REST protocol authentication agents can use the previous agent credentials, enter:

   ```
   ./rsautil store -o admin -a update_config
   auth_manager.rest_service.old_access_retain_days Number GLOBAL 503
   ```

   Where *Number* is the number of days, for example, 90.

5. Restart the services on the primary instance. If there are replica instances, restart the services after replication is complete.

   a. Change directories:

      ```
      cd /opt/rsa/am/server
      ```

   b. Run the following:

      ```
      ./rsaserv restart all
      ```

New Features and Enhancements in Earlier Cumulative Patches

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

New Features and Enhancements in Patch 12

Patch 12 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 12 introduces the following new feature.

Require the Security Console and the Self-Service Console to Provide the Same Response for Valid and Invalid Usernames

To address AM-37367, Patch 12 allows you to require the Security Console and the Self-Service Console to display the same response for both valid and invalid usernames, instead of returning different responses.

This feature helps to prevent an attacker from learning which usernames are valid. These usernames can be used for brute force attacks on user passwords, to attempt to reset passwords, to lock user accounts with invalid logon attempts, to deny users access to their accounts, or for social engineering.

After you complete the procedure below, the Self-Service Console prompts every user to select from a drop-down list of authentication methods that are configured in the RSA Authentication Manager deployment. These methods can include password, passcode, or on-demand authentication.

Before You Begin

Obtain the **rsaadmin** operating system password.

Procedure

1. Log on to the appliance using an SSH client.
2. When prompted for the user name and password, enter the operating system User ID, **rsaadmin**, and the operating system account password.

3. Change directories:

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

4. To add the parameter that allows the Security Console and the Self-Service Console to give the same response for both valid and invalid usernames, enter:

   ```
   ./rsautil store -o admin -a add_config
   ims.authentication.service.all.methodchoice false GLOBAL 500
   ```

5. To require the Security Console and Self-Service Console to give the same response for both valid and invalid usernames, enter:

   ```
   ./rsautil store -o admin -a update_config
   ims.authentication.service.all.methodchoice true GLOBAL 500
   ```

6. Restart the services on the primary instance. If there are replica instances, restart the services after replication is complete.

   a. Change directories:

      ```
      cd /opt/rsa/am/server
      ```

   b. Run the following:

      ```
      ./rsaserv restart all
      ```

New Features and Enhancements in Patch 11

RSA Authentication Manager 8.4 Patch 11 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 11 introduces the following new features.

AMBA Lists Security Domains for Tokens and Users

To address AM-37169, Patch 11 updates AMBA to add security domains to the results file for the **LTIF** (List Token Information by Field) command and the **LUIF** (List User Information by Field) command.

The **LTIF** command lists the security domain for each token, and the **LUIF** command lists the security domain for each user. Both commands allow you to search for records based upon security domain. You can use this output for reporting and administrative purposes.

AMBA Supports the Bulk Administration of RADIUS Clients in the RSA Authentication Manager Internal Database

To address AM-32526, Patch 11 adds a new **ARC** (Add RADIUS Client) command that allows AMBA to add RADIUS clients in the RSA Authentication Manager Internal database. These RADIUS clients use IPv4 addresses. To add an IPv6 RADIUS client, you must use the Security Console, which allows you to add both IPv4 and IPv6 RADIUS clients. The ARC command supports the Add *Operation*.

Action	**ARC**
Required Fields	ClntName, ClientIPAddress, RadiusClientModel, *Operation*, SharedSecret
Optional Fields	AnyRadiusClient, ClientIPAddressType, CreateAssociatedAgent, GrpName

You must add a RADIUS client to the deployment for each RADIUS device that is configured to use RSA SecurID as its authentication method, for example, a RADIUS-enabled device at the network perimeter, such as a VPN firewall server. The RADIUS client sends authentication requests to the RSA RADIUS server, which then forwards the request to RSA Authentication Manager.

You can configure RADIUS clients with or without an assigned authentication agent. The difference between the two methods is in the level of access control and logging you want to have.

- RADIUS client with an agent. Adding an agent to a RADIUS client allows Authentication Manager to determine which RADIUS client is used for authentication and to save this information in log files.
- RADIUS client without an agent. Without an assigned RADIUS client agent, Authentication Manager cannot track which RADIUS client sends authentication requests and you cannot assign a profile to the client.

You can use the same AMBA command for all of the following examples:

```
./rsautil AMBulkAdmin -a admin -P Password$ --verbose -m 0 -i arc.csv
```

Where *Password$* is the password for the Super Admin.

Add a RADIUS Client Example

To add a RADIUS client named `WIN-9K35LDRF4P2.example.com` to the group `rad` in the Authentication Manager internal database, you can create a sample CSV file, called **arc.csv**, that contains the following data:

```
Action,ClntName,AnyRadiusClient,ClientIPAddressType,ClientIPAddress,RadiusCli
entModel,SharedSecret,CreateAssociatedAgent,GrpName,Operation
ARC, WIN-9K35LDRF4P2.example.com,N,0, 192.0.2.255,Cisco PIX
Firewall,1111,Y,rad,ADD
```

Add the Any RADIUS Client

You add an ANY RADIUS client if you do not want to track which RADIUS client sends authentication requests, for example, because you want to quickly add many RADIUS clients. Authentication requests using the shared secret specified for the ANY client are processed regardless of the originating client's IP address. An IP address is not added for the ANY client.

To add an ANY RADIUS client to the group radius in the RSA Authentication Manager internal database you can create a sample CSV file, called **arc.csv**, that contains the following data:

```
Action,ClntName,AnyRadiusClient,ClientIPAddressType,ClientIPAddress,RadiusCli
entModel,SharedSecret,CreateAssociatedAgent,GrpName,Operation
ARC,<ANY>,Y,0,,Aventail,2222,N,radius,ADD
```

Add RADIUS Clients in Bulk

You can add multiple RADIUS clients by adding more data to the CSV file.

To add five RADIUS clients, each with a restricted agent that is assigned to the group radius in the Authentication Manager internal database, you can create a sample CSV file, called **arc.csv**, that contains the following data:

```
Action,ClntName,AnyRadiusClient,ClientIPAddressType,ClientIPAddress,RadiusCli
entModel,SharedSecret,CreateAssociatedAgent,GrpName,Operation
ARC,new.example.com,N,0,192.0.2.91,Cisco ASA Firewall,5555333,Y,radius,ADD
ARC,new.example.com,N,0,192.0.2.92,IP3 Networks,4333,Y,radius,ADD
ARC,new.example.com,N,0,192.0.2.93,Extreme Networks,65333,Y,radius,ADD
ARC,new.example.com,N,0,192.0.2.94,Cisco PIX Firewall,5555,Y,radius,ADD
ARC,new.example.com,N,0,192.0.2.95,Cisco ASA Firewall,3333,Y,radius,ADD
```

New Features and Enhancements in Patch 10

RSA Authentication Manager 8.4 Patch 10 is a maintenance patch that includes software fixes. Patch 10 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches.

New Features and Enhancements in Patch 9

RSA Authentication Manager 8.4 Patch 9 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 9 introduces the following new features.

Support for PIN with Device Biometrics Authentication

Patch 9 allows users to authenticate with Device Biometrics. Users must first set up biometrics on their Apple Touch ID or Face ID, Android fingerprint, or Windows Hello devices. RSA SecurID Access does not force users to do this.

Users can authenticate by entering their existing RSA SecurID PIN and either tapping Approve (added in Patch 4) or using Device Biometrics on a registered device. The method used is determined by the access policy that is configured in the Cloud Authentication Service.

Users who can authenticate with either Approve or Device Biometrics are initially prompted for the first method listed in the assurance level for the protected resource or agent that is being accessed. After successfully authenticating, users are prompted for the method that they used for their last authentication. Users can choose to authenticate with a different method, if the new method is configured on the user's device and allowed by the access policy. Authentication Manager does not support assurance levels that combine two forms of authentication, such as RSA SecurID Token and Approve, so users must choose to authenticate with one supported and configured method.

This feature is available after you use the Security Console wizard to connect RSA Authentication Manager to the Cloud Authentication Service, unless you have already done so. You do not need to update or replace your existing agents or RSA Ready products that use UDP or TCP protocols.

For more information, see *Connect RSA Authentication Manager to the Cloud Authentication Service* on RSA Link.

Resolves an Issue Using Specified Software in TCP Mode

Patch 9 resolves an issue that prevents users from authenticating to deployments running RSA Authentication Manager 8.4 Patch 8 from the following agents if they are configured to use the special, non-default TCP mode:

- RSA Authentication API for C version 8.5.*x* or 8.6.*x*
- RSA Authentication Agent for Web for IIS version 8.*x*
- RSA Authentication Agent for Web for Apache Web Server version 8.*x*

If you are using one of the specified agents in TCP mode, apply Patch 9.

Only these agents are impacted and only when configured to use TCP mode authentication. These agents (and all other RSA SecurID agents) are NOT impacted when using the normal UDP or REST mode authentication. Agents based on the RSA Authentication API for Java version 8.5.*x* or 8.6.*x* are NOT impacted, even if they are configured to use the TCP mode.

The RSA SecurID Access Cloud Authentication service and identity router are not impacted.

New Features and Enhancements in Patch 8

RSA Authentication Manager 8.4 Patch 8 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 8 introduces the following new feature.

Encrypt the RSA SecurID Hardware Appliance 350 Hard Drive

To address AM-34613, Patch 8 qualifies the PowerVault self-encrypting hard drive feature on the RSA SecurID Hardware Appliance 350. Enabling this feature encrypts the RAID 1 logical drive, which consists of a dual physical hard drive that uses mirroring. This feature is not included on other RSA SecurID Hardware Appliance models.

Note: You must back up or record your passphrase. RSA cannot recover it, and you cannot reverse encryption without resetting your hard drive.

Before You Begin

You must know the following:

- After enabling encryption, you should wait for at least 8 to 12 hours before using the hard drive. When the hard drive is fully encrypted, there is little or no impact on performance.
- The encrypt operation is performed as the **root** user.
- Encryption does not protect data that is copied off the hard drive.
- If you enable encryption, you must back up or record your passphrase, so that you can access it when you need it. RSA does not provide a utility for recovering the passphrase used to encrypt your hard drive.
- Removing encryption resets your hard drive and permanently clears your data. Make sure to back up your hard drive before you remove encryption.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. Switch to the **root** user.
3. Run the following command:

   ```
   encryptSedVd.py
   ```

   A message states whether the drive is encrypted.
4. To encrypt the drive, do the following:
   a. At the Enable disk encryption **y/n?** prompt, type **y** and press ENTER.
   b. If you are prompted to enter a security key, you must enter a passphrase, and press ENTER.

      The passphrase must be between 8 and 32 characters long, and contain lowercase letters, uppercase letters, numbers, and special characters. For example, nFreDaW$792

      Avoid characters that can be problematic on command lines, such as dashes, dollar signs, backslashes, blank spaces, single and double quotation marks, and non-ASCII characters.
   c. Re-enter the passphrase two more times to validate it, and press ENTER each time.
   d. You can enter an optional ID string to identify the security key, or press ENTER for no ID string.

The ID string is optional because the RSA SecurID Hardware Appliance 350 only has one logical drive and only one security key.

The optional ID string for the security key must be fewer than 256 characters. Avoid characters that can be problematic on command lines, such as dashes, dollar signs, backslashes, blank spaces, single and double quotation marks, and non-ASCII characters.

e. When you are prompted, backup or record your passphrase, and enter **y** to verify that you did so.

Note: Make sure to save your passphrase. RSA cannot recover it for you, and removing encryption will permanently erase your data.

A success message displays.

New Features and Enhancements in Patch 7

RSA Authentication Manager 8.4 Patch 7 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 7 introduces the following new feature.

Prioritize Approve Authentication for On-Demand Authentication Users

After you use the Security Console wizard to connect Authentication Manager to the Cloud Authentication Service, on-demand authentication (ODA) users can have the same PIN for both ODA and Approve authentication. When these ODA users enter their PINs, they are issued one-time tokencodes because ODA has priority over Approve authentication.

To address AM-35277, Patch 7 allows you to prioritize Approve authentication for these ODA users.

Before You Begin

Obtain the **rsaadmin** operating system password.

Procedure

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

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

4. To add the parameter that lets you specify whether ODA or Approve authentication has priority, enter:

   ```
   ./rsautil store -o admin -a add_config
   auth_manager.cas.authentication.runtime.precedence.enabled false GLOBAL
   500
   ```

5. To prioritize Approve authentication for ODA users, enter:

   ```
   ./rsautil store -o admin -a add_config
   auth_manager.cas.authentication.runtime.precedence.enabled true GLOBAL 500
   ```

6. Restart the services on the primary instance. If there are replica instances, restart the services after replication is complete.

   a. Change directories:

   ```
   cd /opt/rsa/am/server
   ```

   b. Run the following:

   ```
   ./rsaserv restart all
   ```

New Features and Enhancements in Patch 6

RSA Authentication Manager 8.4 Patch 6 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches. In addition, Patch 6 introduces the following new features.

AMBA Supports the Bulk Administration of Trusted Realm User Groups in the RSA Authentication Manager Internal Database

To address AM-34362, Patch 6 adds new commands that allow AMBA to add, update, and delete trusted realm user groups, authentication agent associations, and user group members, in the local RSA Authentication Manager Internal database. This allows you to move user groups and their associations from an external trusted realm into the local realm, for example, if you are moving data from one Authentication Manager deployment to another.

Add Remote Group

The **ARG** (Add Remote Group) command adds user groups from a trusted realm into the RSA Authentication Manager internal database.

Action	**ARG**
Required Fields	GrpName
Optional Fields	SecurityDomain

If Security Domain is not provided, then the remote group is added in the default security domain (System Domain) created during RSA Authentication Manager installation.

A trusted user group restricts access to an agent that is enabled for trusted realm authentication. When you create a trusted user group and enable associated agents, only members of the trusted user group can access that authentication agent.

By adding a trusted user group, only users who have a business need to access the resources protected by the agent can authenticate. For example, by creating a trusted user group for human resource workers, you can limit access to personnel records to those in the group.

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

```
Action,GrpName
arg, tgroup1
arg, tgroup2
arg, tgroup3
```

After you run the following AMBA command, the three user groups listed above are added to the RSA Authentication Manager internal database:

```
./rsautil AMBulkAdmin -a admin -P Password$ --verbose -m 0 -i arg.csv
```

Delete Remote Group

The **DRG** (Delete Remote Group) command removes a remote user group from the RSA Authentication Manager internal database.

Action	**DRG**
Required Fields	GrpName
Optional Fields	SecurityDomain

If Security Domain is not provided, then the remote group is added in the default security domain (System Domain) created during Authentication Manager installation.

Delete a trusted user group to revoke a user group's access privileges on a trusted realm.

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

```
Action,GrpName
drg, tgroup1
drg, tgroup2
drg, tgroup3
```

After you run the following AMBA command, the three user groups listed above are removed from the RSA Authentication Manager internal database:

```
./rsautil AMBulkAdmin -a admin -P Password$ --verbose -m 0 -i drg.csv
```

Add User to Remote Group

The **AURG** (Add User to Remote Group) command links a trusted user to a trusted user group in the RSA Authentication Manager internal database.

Action	**AURG**
Required Fields	GrpName, DefLogin
Optional Fields	SecurityDomain

If Security Domain is not provided, then the remote group is added in the default security domain (System Domain) created during RSA Authentication Manager installation.

A trusted user group restricts access to an agent that is enabled for trusted realm authentication. When you create a trusted user group, only members of the trusted user group can access the agent that is enabled for trusted realm authentication.

You can add new trusted users to an existing trusted user group.

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

```
Action, GrpName, DefLogin, SecurityDomain
aurg,tgroup1,tuser1
aurg,tgroup1,tuser2
aurg,tgroup2,tuser3
```

After you run the following AMBA command, the three trusted users listed above are added to trusted user groups in the RSA Authentication Manager internal database:

```
./rsautil AMBulkAdmin -a admin -P Password$ --verbose -m 0 -i aurg.csv
```

Delete User from Remote Group

The **DURG** (Delete User from Remote Group) command removes a trusted user from a trusted user group in the RSA Authentication Manager internal database.

Action	**DURG**
Required Fields	GrpName, DefLogin
Optional Fields	SecurityDomain

If Security Domain is not provided, then the remote group is added in the default security domain (System Domain) created during Authentication Manager installation.

You can remove existing trusted users from an existing trusted user group.

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

```
Action, GrpName, DefLogin, SecurityDomain
durg,tgroup1,tuser1
```

After you run the following AMBA command, the trusted users listed above are removed from the trusted user group in the RSA Authentication Manager internal database:

```
./rsautil AMBulkAdmin -a admin -P Password$ --verbose -m 0 -i durg.csv
```

Add Client to Remote Group

The ARGC (Add Remote Group Client) command links an authentication agent to a trusted group in the RSA Authentication Manager internal database.

Action	**ARGC**
Required Fields	GrpName, ClntName
Optional Fields	SecurityDomain

If Security Domain is not provided, then the remote group is added in the default security domain (System Domain) created during Authentication Manager installation.

A trusted user group restricts access to an authentication agent that is enabled for trusted realm authentication. When you create a trusted user group, only members of the trusted user group can access the agent that is enabled for trusted realm authentication.

You can select which authentication agents that you want a trusted user group to have permission to access.

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

```
Action,GrpName,ClntName,SecurityDomain
argc,tgroup1,primary-PR-84.corp.emc.com
```

After you run the following AMBA command, the authentication agent listed above is added to the trusted user group in the RSA Authentication Manager internal database:

```
./rsautil AMBulkAdmin -a admin -P Password$ --verbose -m 0 -i argc.csv
```

Delete Client from Remote Group

The **DRGC** (Delete Remote Group Client) command removes an authentication agent from a trusted user group in the RSA Authentication Manager internal database.

Action	**DRGC**
Required Fields	GrpName, ClntName
Optional Fields	SecurityDomain

If Security Domain is not provided, then the remote group is added in the default security domain (System Domain) created during Authentication Manager installation.

A trusted user group restricts access to an agent that is enabled for trusted realm authentication. When you create a trusted user group, only members of the trusted user group can access the agent that is enabled for trusted realm authentication.

You can unselect which authentication agents that you want a trusted user group to not have permission to access.

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

```
Action,GrpName,ClntName,SecurityDomain
drgc,tgroup1,primary-PR-84.corp.emc.com
```

After you run the following AMBA command, the authentication agent listed above is removed from the trusted user group in the RSA Authentication Manager internal database:

```
./rsautil AMBulkAdmin -a admin -P Password$ --verbose -m 0 -i drgc.csv
```

Require AMBA to Only Extend Software Token Lifetimes with Tokens from the Same Security Domain

The **ETL** (Extend Software Token Lifetime) command extends the lifetime of a distributed software token that has expired or is expiring soon. By extending software token lifetimes, you can avoid replacing expired software tokens on user devices, such as mobile phones, tablets, and PCs. Software token provisioning only needs to occur one time on each user device, and RSA Authentication Manager assumes full administrative control over whether an extended token is available for authentication.

The **ETL** command requires the serial number for each software token that is being extended. RSA Authentication Manager selects an unassigned software token that has the longest lifetime, assigns its expiration date to the original software token, and then deletes the token that provided its expiration date.

Action	**ETL**
Required Fields	TokSerial
Optional Fields	UseSameSecurityDomain

To address AM-33399, Patch 6 adds an optional **UseSameSecurityDomain** field that requires AMBA to only select unassigned software tokens that share the same security domain as the tokens that are being extended.

New Features and Enhancements in Patch 5

RSA Authentication Manager 8.4 Patch 5 is a maintenance patch that includes software fixes. Patch 5 includes all new features and enhancements introduced in all version 8.4 and version 8.3 patches.

New Features and Enhancements in Patch 4

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

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

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

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

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

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

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

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

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

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

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

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

New Features and Enhancements in Patch 3

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

Force a Password Change When Adding a User in AMBA

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

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

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

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

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

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

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

New Features and Enhancements in Patch 2

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

Disable the Offline Authentication Port

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

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

Procedure

1. In the Security Console, click **Setup > System Settings**.
2. Under **Authentication Settings**, click **Agents**.
3. Under **Communication Ports**, click the **Disable Offline Authentication Port** checkbox.
4. Click **Save**.

New Features and Enhancements in Patch 1

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

Support for Microsoft Active Directory 2019

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

VMware Virtual Appliance Qualified on the VMware ESXi 6.7 Server

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

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

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

Defects Fixed in This Patch

Version 8.4 Patch 13

RSA Authentication Manager 8.4 Patch 13 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 13 contains fixes for the following issues:

AM-37692, AM-37879. Updated the RSA Authentication Manager topic on RSA Link to specify that ClamAV requires an additional antivirus definition file, **bytecode.cvd**. See *Run Clam Antivirus Software*.

AM-37518. The **CAU** (Change or Add User) command includes a new RemoveGrpDefLogin option to remove a logon alias from a group. For more information, see AMBA Supports Removing a Logon Alias from a Group on page 7.

AM-37087. When the agent credentials are regenerated for REST protocol authentication agents, the previous credentials can be used for up to 60-days or a timeframe that you specify. For more information, see More Flexibility When Regenerating the Access ID and Access Key for REST Protocol Authentication Agents on page 7.

AM-36334. Fixed an issue with log rotation.

AM-36747. Updated Authentication Manager WebLogic components to prevent potential security vulnerabilities.

Version 8.4 Patch 12

RSA Authentication Manager 8.4 Patch 12 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 12 contains fixes for the following issues:

AM-37562. Updated the `auth_manager.dashboard.hide.grpagent` option so that an administrator who is not a Super Admin, such as a Help Desk Administrator, can see the User Dashboard without information about user groups and authentication agents. In addition, restarting all services is now required if you change the value of the `auth_manager.dashboard.hide.grpagent` option.

If a user who is associated with a huge number of user groups and authentication agents cannot be displayed in the User Dashboard, you can do the following:

1. Change directories to `/opt/rsa/am/utils.`
2. Run the following command line utility (CLU) to add a configuration value:

   ```
   ./rsautil store -a add_config auth_manager.dashboard.hide.grpagent
   false GLOBAL BOOLEAN
   ```

   Setting the value to `false` means that the User Dashboard does not hide user groups and authentication agents.

3. Run the following CLU to stop displaying user groups and authentication agents in the User Dashboard:

   ```
   ./rsautil store -a update_config auth_manager.dashboard.hide.grpagent
   true GLOBAL BOOLEAN
   ```

   Setting the value to `true` means that the User Dashboard hides user groups and authentication agents.

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

   ```
   ./rsaserv restart all
   ```

AM-37489. Updated the version of Oracle WebLogic used by the RSA Authentication Manager.

AM-37488. Updated Authentication Manager components to prevent potential security vulnerabilities.

AM-37367. Added a parameter that allows you to require the Security Console and the Self-Service Console to provide the same response for valid and invalid usernames. This helps to prevent an attacker from obtaining information about usernames and helps to prevent brute force attacks. For instructions, see Require the Security Console and the Self-Service Console to Provide the Same Response for Valid and Invalid Usernames on page 9.

AM-37274. Corrected a misleading message in the **imsTrace.log**.

AM-37043. Resolved errors running the “Administrators of a Security Domain" report for deployments with large numbers of subdomains.

AM-36935, AM-36934. Updated the Security Console page to prevent a potential Cross-Site Scripting (XSS) attack. The attacker would need control of an administrator’s browser.

AM-35755, AM-37483. Resolved an issue that sometimes prevented successful authentication with a temporary fixed tokencode on a replica instance.

Version 8.4 Patch 11

RSA Authentication Manager 8.4 Patch 11 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 11 contains fixes for the following issues:

AM-37172. Updated Authentication Manager components to prevent potential security vulnerabilities.

AM-37169. Patch 11 updates AMBA to allow the **LTIF** (List Token Information by Field) command and the **LUIF** (List User Information by Field) command to list security domains in the results file. You can use this output for reporting and administrative purposes. For more information, see AMBA Lists Security Domains for Tokens and Users on page 10.

AM-37080. Applied updates to the Linux operating system used by Authentication Manager.

AM-36785. Added the primary or replica instance hostname to critical system event notifications for identity source connection problems.

AM-36673. After using the Security Console wizard to connect Authentication Manager and the Cloud Authentication Service, you can remove the connection by doing both of these steps:

1. In the Security Console, click **Setup** > **System Settings**, and then click **Cloud Authentication Service Configuration**. Clear the **Enable Cloud Authentication** checkbox.
2. Run the following command, and restart all services:

```
./rsautil store -o <OC_admin> -a update_config
auth_manager.cas.authentication.enabled false GLOBAL 500
```

AM-36558. For PINPad-style software tokens, a syntax error was sometimes displayed instead of a failed authentication error message.

AM-36432. After importing users who are not enabled for on-demand authentication (ODA) into a deployment, existing ODA users were disabled for ODA, but they appeared to be enabled. This issue has been resolved, and these existing ODA users can be enabled again.

AM-36320. Updated RSA RADIUS to prevent the wrong type of response from being sent.

AM-36007. Duplicate user IDs stopped the users with aliases report.

AM-35996. Fixed the log rotation settings.

AM-32526. Patch 11 adds a new **ARC** (Add RADIUS Client) command that allows AMBA to add IPv4 RADIUS clients in the RSA Authentication Manager Internal database. For more information, see AMBA Supports the Bulk Administration of RADIUS Clients in the RSA Authentication Manager Internal Database on page 10.

Version 8.4 Patch 10

RSA Authentication Manager 8.4 Patch 10 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 10 contains fixes for the following issues:

AM-36578. Removed the ssh-dss HostKeyAlgorithm. Use any other HostKeyAlgorithm while connecting to Authentication Manager through SSH.

AM-36577. Updated Authentication Manager components to prevent potential security vulnerabilities.

AM-36576. Non-SSL external identity sources do not support forcing user password changes. When internal Authentication Manager users are exported to an external identity source, the force password change flag is now always marked as false.

AM-36575. An updated web-tier server (available *here*) is also available with Patch 10. See the web-tier server *Readme* for information on the updates to the web-tier server.

AM-35999. After restoring a backup file to a new primary server that contains a partial version of the original hostname, Authentication Manager did not redirect to the correct URL

AM-35756. An error message displays when an administrator attempts to assign an expired token to a user.

AM-35591. The Security Console prevents JavaScript from running on the security domain and identity source pages related to the Default Security Domain Mapping page.

AM-35459. The Security Console prevents JavaScript from running on the user and report pages that display the Custom User Attributes field.

AM-34545. When archived log files are deleted, the signature files are now also deleted.

AM-31913. The Administration Activity Monitor and the System Activity Monitor can display data from up to 1000 security domains or subdomains.

Version 8.4 Patch 9

RSA Authentication Manager 8.4 Patch 9 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 9 contains fixes for the following issues:

AM-36208. Updated Authentication Manager components to prevent potential security vulnerabilities.

AM-36140. Added the area code for Kosovo.

AM-35763. Risk-based authentication in RSA Web Agent-protected-sites was affected by successful authentication to the RSA Self-Service Console.

AM-35594. Updated the documentation, including the Help topics “Sample Reports” and “RSA Authentication Agents” to provide more details about agent reporting for REST protocol authentication agents.

AM-35438. Remote syslog records did not include the "HOSTNAME" field.

AM-34670. Fixed an issue on the Authentication Manager appliance that prevented the SDK from doing iterative searches over an SSLClientAuthentication connection.

AM-32343. Addressed a bypass vulnerability.

Version 8.4 Patch 8

RSA Authentication Manager 8.4 Patch 8 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 8 contains fixes for the following issues:

AM-35884. Updated Authentication Manager components to prevent potential security vulnerabilities.

AM-35390. Re-indexing resolved an issue in which the hardware appliance took longer than an hour to restart.

AM-35388. Users who were not required to change their RSA SecurID PIN when replacement software tokens were assigned were unable to authenticate with their original hardware tokens.

AM-35076. AMBA couldn’t successfully run commands, such as the **AUG** command, when the internal database name was changed in the Operations Console.

AM-34613. The PowerVault self-encrypting hard drive feature is qualified on the RSA SecurID Hardware Appliance 350. Enabling this feature encrypts the RAID 1 logical drive. This feature is not included on other RSA SecurID Hardware Appliance models. For instructions, see Encrypt the RSA SecurID Hardware Appliance 350 Hard Drive on page 13.

Version 8.4 Patch 7

RSA Authentication Manager 8.4 Patch 7 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 7 contains fixes for the following issues:

AM-35277. Added a parameter that allows you to specify whether on-demand authentication (ODA) or Approve authentication has priority for users who have the same PIN for both authentication methods. For instructions, see Prioritize Approve Authentication for On-Demand Authentication Users on page 14.

AM-35274. The RSA Authentication Manager's strict transport security settings will now also apply to any other web services that are defined in your organization in subdomains of the domain used by the RSA Authentication Manager. This may mean that any web services in subdomains using only HTTP could become inaccessible.

AM-35266. RSA Authentication Manager now recognizes an extended set of top-level domains (including many of those recognized by the IANA organization).

AM-35258. Resolved an issue in which a failed Authenticate Tokencode authentication was logged one time in Authentication Manager and two times in the Cloud Authentication Service.

AM-35250. Updated an internal component to prevent cross-site scripting attacks. Risk-based authentication (RBA) users must re-register their devices/browsers.

AM-35117. Fixed an issue in which REST agents ignored domain name mapping options,

AM-35049. Authentication requests from the RSA Authentication Agent 2.0 for Active Directory Federation Services (AD FS) no longer take up to 20 seconds to verify.

AM-34523. Resolved a flaw which allowed an XML External Entity (XXE) injection vulnerability.

AM-31739. Misleading passcode format errors were displayed in the Authentication Monitor for users who did not use Authenticate Tokencode.

AM-29006. Updated the documentation to explain when security questions are displayed in the Self-Service Console.

Version 8.4 Patch 6

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

AM-34809. Updated Authentication Manager components to prevent potential security vulnerabilities.

AM-34769. The Security Console no longer allows you to create duplicate trusted user groups by entering the same name with a different case. For example, you cannot create both Test1 and TEST1.

AM-34647. Resolved an intermittent issue in which multifactor authentication failed on a replica instance.

AM-34514. System performance was initially slow after the database was restored.

AM-34362. Patch 6 adds new commands that allow AMBA to add, update, and delete trusted realm user groups, authentication agent associations, and user group members, in the local RSA Authentication Manager Internal database. For more information, see AMBA Supports the Bulk Administration of Trusted Realm User Groups in the RSA Authentication Manager Internal Database on page 15.

AM-33810. Corrected errors seen in the French language version of Authentication Manager.

AM-33399. The AMBA **ETL** (Extend Software Token Lifetime) command now includes an optional **UseSameSecurityDomain** field that requires AMBA to only select unassigned software tokens that share the same security domain as the tokens that are being extended. For more information, see Require AMBA to Only Extend Software Token Lifetimes with Tokens from the Same Security Domain on page 18.

AM-33070. Corrected issues with the way that the text was displayed on the RADIUS client PIN reset page.

AM-32917. Updated the documentation to explain that interrupting Quick Setup or replica attachment on Amazon Web Services prevents you from accessing your Authentication Manager instance through the Quick Setup URL.

AM-28464. Added a note to the *Setup and Configuration Guide* mentioning that the web tier requires the System Management BIOS (SMBIOS).

AM-25506. Corrected a spelling error on the command line installation of the web tier.

Version 8.4 Patch 5

RSA Authentication Manager 8.4 Patch 5 includes all fixes introduced in all version 8.4 and version 8.3 patches. In addition, Patch 5 contains fixes for the following issues:

AM-34448. Updated Authentication Manager components to prevent potential security vulnerabilities.

AM-34391. The AMBA **AU** command can now read the **AttributeValue1** header.

AM-34185. Fixed an issue in which replication stopped working after an Authentication Manager patch was applied to a replica instance.

AM-33987. Updated the commons-fileupload component to the latest version used by Authentication Manager.

AM-33847, AM-33464. The User Dashboard was unable to display information about a user who was associated with a huge number of user groups and authentication agents. To display user information, a command line utility (CLU) was provided. For instructions, see AM-37562.

AM-33773. When you are adding a user to a user group, the User Dashboard displays the internal database and not the last identity source that was viewed.

AM-33259. Updated the Configure Update Source window to remove references to the Windows domain. If you configure a Windows Share as an update source, a Windows username, without a domain, is required.

AM-31261. The Self-Service Console hides the “Request a new token” link if a user has the maximum allowed number of assigned authenticators.

AM-30882. Restarting Authentication Manager took longer than an hour if there were millions of authentication activity log records.

Version 8.4 Patch 4

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

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

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

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

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

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

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

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

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

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

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

Version 8.4 Patch 3

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

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

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

AM-33260. An administrator can force a password change while using the AU command to add a user in AMBA. For more information, see above on page 20.

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

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

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

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

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

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

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

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

Version 8.4 Patch 2

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

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

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

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

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

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

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

0 - Unknown: cannot get the status from the system.

1 - Normal: HEALTHY, ATTACHING or SYNCHRONIZING

2 - Unhealthy: FAILED, UNHEALTHY, OUT_OF_SYNC or OFFLINE

The Operations Console provides the details for each status.

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

AM-31664. SSH clients and SCP clients can no longer connect to the appliance with weaker algorithms, for example, MD5 and 96-bit MAC algorithms. It may be necessary to upgrade your SSH and SCP clients to more recent versions that can handle more restrictive SSH algorithms.

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

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

Version 8.4 Patch 1

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

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

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

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

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

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

AM-32676. The version of Oracle WebLogic used by Authentication Manager and the web tier was potentially vulnerable to security exploits. If your deployment includes a web tier, you must reinstall the web tier with the latest version for this fix to work. See “Reinstall the Web Tier” in the *RSA Authentication Manager 8.4 Setup and Configuration Guide* for instructions.

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

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

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

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

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

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

AM-32668. Input validation for SearchGroupCommand and SearchGroupIterativeCommand incorrectly required a Group GUID value for searches that could be completed successfully if Group GUID was set as null.

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

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

AM-32660. When editing an offline authentication policy in the Security Console, Minimum Passcode Length for offline authentication remained visible and editable when **Enable Offline Authentication** was disabled.

AM-32659. AMBA includes a **SoftTokenProfile** attribute and a **Set Software Token Profile** (SSTP) command for software token distribution with CT-KIP and SDTID files. AMBA does not support CTF.

AM-32658. When revisiting the **Administration > Archive Audit Logs > Schedule Log Archival page** in the Security Console after selecting **Purge online log data stored for more than number of days specified below, Days Kept Online** was incorrectly displayed under the Log Archival Export Directory section.

AM-32657. Authentication Manager now supports sending critical system event notifications when scheduled log archive jobs fail.

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

AM-32654. AMBA did not allow an administrator to assign a nickname to a token that had been unassigned from a user and reassigned to a different user.

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

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

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

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

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

AM-32638. The online emergency access token count on the **Authentication > SecurID Tokens > Statistics** page of the Security Console incorrectly included tokens for which online emergency access had expired.

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

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

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

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

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

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

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

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

Known Issues

An error message is not displayed if the invitation to authenticate to the Cloud Authentication Service fails for more than 500 users

Tracking Number: AM-34114
Problem: After you apply Patch 4 or later, if more than 500 users are invited to authenticate to the Cloud Authentication Service and the invitation fails for all users, the Security Console displays the misleading statement "The number of users found exceeds the search results limit of 500. Change your search criteria to narrow your search." The correct messages display if the invitation succeeds for some or all of the users.
Workaround: You can view the success, warning, and error messages in the Administration Activity Monitor.

You must upgrade all replica instances to Patch 4 or later before you connect to the Cloud Authentication Service

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

Web Tiers page does not indicate that a reinstall is required after you apply Patch 4 or later

Tracking Number: AM-34010
Problem: Patch 4 or later includes third-party software updates that require you to reinstall the web tier. After applying Patch 4 or later, the Web Tiers page in the Operations Console displays the **Update** button for each web tier, instead of "Reinstall Required."
Workaround: After you reinstall the web tier, the correct status is reported in the Operations Console.

Canceling the Cloud Authentication Service Configuration page returns you to the Settings page

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

Cloud Authentication Service User Event Monitor Does Not Display the Latest User Status

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

Security Console message says that users were notified by e-mail but the e-mail (SMTP) server did not send any notifications

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

If the SMTP Mail Service is not available, error messages are not displayed until every user invitation to authenticate to the Cloud Authentication Service has timed out

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

User Dashboard displays details for one Cloud Authentication Service user if two users have the same email ID in two different Active Directory identity sources

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

User Dashboard displays an Enable button for users who are disabled in Active Directory

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

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.

June 2020

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.