# RSA® Authentication Manager 8.2

# Patch 4 Readme

**January 2017**
**Prerequisite Release:**
**RSA Authentication Manager 8.2**

## Contents



## Before Installing This Patch

**Note**: RSA Authentication Manager 8.2 patches include fixes from Authentication Manager 8.1 SP1 Patch 15. All Authentication Manager 8.2 patch releases are cumulative.

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 8.2 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 a VMware virtual appliance or a hardware appliance to version 8.2 before installing this patch. See the *RSA Authentication Manager 8.2 Setup and Configuration Guide* for instructions.

# Installing a Patch

The RSA Authentication Manager 8.2 Patch 4 ZIP file (**am-update-8.2.0.4.0.zip**) contains the following file:

- **am-update-8.2.0.4.0.iso**. The RSA Authentication Manager 8.2 Patch 4 ISO file 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 8.2 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**.

**Note**: If the update file is smaller than 2 GB, you can upload it through your local browser. If the size of the patch file exceeds 2 GB, however, you must change the update source settings and configure a new 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

- 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 version 8.2 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.

### 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 8.2 Patch 4

RSA Authentication Manager 8.2 is a prerequisite release for this patch. Version 8.2 does not support direct migration from earlier versions. To use existing data from Authentication Manager 6.1, 7.1, or 8.0, do the following:

1. Deploy Authentication Manager 8.1 Service Pack 1. (8.1.1)
2. Migrate existing data from Authentication Manager 6.1, 7.1, or 8.0.
3. Update Authentication Manager 8.1.1 to version 8.2.
4. Install this patch.

# New Features and Enhancements in Patch 4

## Support for Active Directory 2016

RSA Authentication Manager now officially supports Active Directory 2016 as an identity source.

# New Features and Enhancements in Patch 2

## Export On-Demand Authentication User Data

To address issue AM-30278, Patch 2 allows you to export On-Demand Authentication (ODA) user data from your Authentication Manager deployment. You specify whether or not to export ODA data on the Export Tokens and Users page of the Security Console. If you export ODA data from your deployment, users configured for ODA authentication will be able to continue using ODA features when you import the data to another deployment.

The user attribute configured for default ODA delivery (for example, **email** or **mobile**) is transferred between deployments according to fixed, direct attribute mapping. For example, if the source deployment has multiple email attributes such as **email** and **email2**, and **email** is set as the default ODA delivery method, the values for the **email** attribute will be exported. When importing the data, the values will be imported to the **email** attribute in the destination deployment. Values for **email2** will not be exported or imported.

**Note:** To avoid ODA problems for imported users, ensure that the user attribute setting for default ODA delivery method is the same in the source and destination deployments.

# New Features and Enhancements in Patch 1

## Change Character Length for On-Demand Authentication Tokencodes

To address issue AM-30290, Patch 1 allows you to choose either six digits or eight digits as the character length for the On-Demand Authentication (ODA) tokencodes generated by RSA Authentication Manager.

**To set the ODA character length:**

1. Log on to the appliance using an SSH client.

2. Change directories:
   `cd /opt/rsa/am/utils`
3. Type the following, then press ENTER to set the character length:
   `./rsautil store -a add_config auth_manager.oda.token_code_length <X> global 503`
   where <*X*> is either 6 or 8, depending on the character length you want to set.
4. Restart all Authentication Manager services on the primary server and replicas:
   `cd /opt/rsa/am/server`
   `./rsaserv restart all`

**To change the ODA character length after setting it for the first time:**

1. Log on to the appliance using an SSH client.
2. Change directories:
   `cd /opt/rsa/am/utils`
3. Type the following, then press ENTER to set the character length:
   `./rsautil store -a update_config auth_manager.oda.token_code_length <X> global 503`
   where <*X*> is either 6 or 8, depending on the character length you want to set.
4. Restart all Authentication Manager services on the primary server and replicas:
   `cd /opt/rsa/am/server`
   `./rsaserv restart all`

## Allow the Use of Nonstandard Email Domains

To address issue AM-30262, Patch 1 allows the use of the .local domain. Apache component updates included in RSA Authentication Manager 8.2 prevent the use of other nonstandard domains, unless you edit the **ims.properties** file.

**To use nonstandard email domains:**

1. Log on to the appliance with the User ID **rsaadmin** and the current operating system password:
   - On a hardware appliance, log onto the appliance using the SSH client.
   - On a virtual appliance, log on to the appliance using an SSH client, the VMware vSphere client, the Hyper-V System Center Virtual Machine Manager Console, or the Hyper-V Manager.
2. Change directories:
   `cd /opt/rsa/am/utils/resources`
3. In a text editor, such as the vi editor, open the **ims.properties** file.
4. Add the nonstandard domain to the validDomainList entry:
   `validDomainList=.`*`nonstandard`*`;.local;`
   Where *nonstandard* is the name of the nonstandard domain. For example, you could enter **validDomainList=.sms;.local;**
   You can add more than one nonstandard domain. Separate each name with a semicolon.
5. Save your changes. For example, in the vi editor, type **:wq!**.
6. Change directories:

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

7. Restart Authentication Manager services:

   ```
   ./rsaserv restart all
   ```

   The nonstandard domains are listed in **/opt/rsa/am/utils/resources/ims.properties**.

8. The **ims.properties** file is not replicated. If you promote a replica instance, you must repeat this procedure, unless you prepare for promotion by repeating these steps on each Authentication Manager instance in your deployment.

## Known Issues

**After installing Patch 4, additional steps are required to fully resolve OpenSSL denial-of-service vulnerabilities.**

**Tracking Number**: AM-30476

**Problem:** Patch 4 addresses an issue where deployments with read-only database users created using the `./rsautil manage-readonly-dbusers` command were susceptible to OpenSSL vulnerabilities described in CVE-2016-6306 and similar attacks. After installing Patch 4, additional steps are required to fully resolve the issue.

**Workaround:**

If your deployment includes read-only database users, do the following after installing Patch 4:

1. Log on to the appliance using an SSH client.
2. Enter the following command:
   ```
   sudo su-
   ```
3. Change directories:
   ```
   cd /opt/rsa/am/utils/bin/appliance
   ```
4. Type the following, then press ENTER:
   ```
   ./configureFirewall.sh close postgres inet,tcp,7050
   ```
5. Enter the following command, where <*x.x.x.x*> is the IP address through which read-only database users remotely connect to the database:
   ```
   ./configureFirewall.sh open-4ip postgres inet,tcp,7050, <x.x.x.x>
   ```
6. Repeat step 5 for each IP address that requires database access.

**After promoting a replica instance to primary, attempting to promote the former primary instance back to primary status fails.**

**Tracking Number**: AM-30394, AM-30564

**Problem:** Promoting a replica instance to primary succeeds, but subsequent attempts to promote the former primary instance back to primary status fail, triggering the message "Promotion was unsuccessful. Unable to extract logs from original primary."

**Workaround:**

1. Log on to the appliance using an SSH client.
2. Change directories:
   ```
   cd /opt/rsa/am/utils
   ```
3. Type the following, then press ENTER to update TLS 1.2 Mode properties:
   ```
   /rsautil store -a enable_min_protocol_tlsv1_2 <setting> restart
   ```
   Where <*setting*> is true if you want to enforce strict TLS 1.2 Mode, or false if you do not.

**Generating System Log Report fails when downloading troubleshooting logs from Operations Console.**

**Tracking Number**: AM-30375

**Problem:** When downloading troubleshooting files from the Operations Console, the Generating System Log Report task fails in cases where the System Log Report file size is too large. The rest of the troubleshooting files generate successfully, but system log data is not included.
**Workaround:** Clear the System Log Report checkbox to omit system log data from the report, or reduce the number of reporting days when downloading troubleshooting files. You can generate the System Log Report separately from the Reporting tab in the Security Console.

### Operations Console shows intermittent replication failure on the primary instance.

**Tracking Number**: AM-30373
**Problem:** In Authentication Manager 8.2, the Operations Console displays intermittent reports that replication has failed on the primary instance. Actual replication of data between instances works properly, but the replication status error interferes with all Authentication Manager functions that rely on a system health check.
**Workaround:** Modify objects (such as users or tokens) using the Security Console, or perform authentication to trigger replication and reset the replication status indicator.

### Local backup fails after planned promotion of a replica instance.

**Tracking Number**: AM-30364
**Problem:** After promoting a replica instance to primary, attempting to make a local backup from the new primary fails, triggering the message "An error occurred while backing up the system: Failed to backup the system files."
**Workaround:**

1. Log on to the appliance using an SSH client.
2. Change directories:
   `cd /opt/rsa/am/utils`
3. Type the following, then press ENTER to update TLS 1.2 Mode properties:
   `/rsautil store -a enable_min_protocol_tlsv1_2 <setting> restart`
   Where <*setting*> is true if you want to enforce strict TLS 1.2 Mode, or false if you do not.

### Need instructions on how to hide a link to an English language video in the Self-Service Console

**Tracking Number:** AM-30224
**Problem:** The Security Console Help is missing the instructions on how to hide the link to the English Language video in the Self-Service Console. These instructions were provided in the *RSA Authentication Manager 8.1 Service Pack 1 Patch 5 Release Notes*.
**Workaround:** The Self Service Console displays a link to an English language video for users about self service. For non-English users, you can hide this link.
Do the following:

1. Log on to the appliance using an SSH client.
2. Change directories:
   `cd /opt/rsa/am/utils`
3. Run one of the following commands:
   - To hide the video link, type the following, and then press ENTER:
     `./rsautil store -a add_config ucm.selfservice.console.novideo true <FQDN> 503`
   - To show the video link, type the following, and then press ENTER:
     `./rsautil store -a update_config ucm.selfservice.console.novideo false <FQDN> 503`
4. When prompted, enter your Operations Console administrator User ID, and press ENTER.
5. When prompted, enter your Operations Console administrator password, and press ENTER.
6. Restart all Authentication Manager services on the primary instance and the replica instances:
   ```
   cd /opt/rsa/am/server
   ./rsaserv restart all
   ```

### Hardened RSA Authentication Manager 8.1 SP1 machine without a Network Time Protocol (NTP) server not restarting after an upgrade

**Tracking Number:** AM-30172
**Problem:** If an RSA Authentication Manager 8.1 SP1 machine that was hardened with the ADG Security Control file does not have access to an NTP server, it will not restart after a successful upgrade to RSA Authentication Manager 8.2.
**Workaround:** Before upgrading a hardened machine to version 8.2, select an NTP server as a time source. In version 8.1 SP1, go to **Administration > Date & Time**, and follow the instructions in the Operations Console Help topic "Update System Date and Time Settings."

### Web-Tier Installer License Agreement screen includes clickable links that do not open external websites

**Tracking Number:** AM-30162
**Problem:** The Web-Tier Installer includes a License Agreement screen that allows you to click the links for external websites. The links redirect you to the top of the license agreement.
**Workaround:** To visit the external websites, copy each link from the License Agreement screen, and paste it into a browser.

### Restored certificates cannot be activated after restoring a backup to a new deployment

**Tracking Number:** AM-30103
**Problem:** After you restore a backup to a new deployment, the restored certificates cannot be activated. The restored certificates were issued with the hostname of the original Authentication Manager instance.
**Workaround:** Either create new certificates or continue to use the certificates that were present on the Authentication Manager instance before the backup was restored. For instructions, see Chapter 7, "Administering RSA Authentication Manager" in the *RSA Authentication Manager 8.2 Administrator's Guide*.

### Restoring a backup to a new deployment requires an additional procedure for the web tier

**Tracking Number:** AM-30099
**Problem:** If you restore an RSA Authentication Manager backup to a new deployment, the web tier cannot be reinstalled. Generating the web-tier deployment package results in a web-tier host certificate failure.
**Workaround:** Before you generate the web-tier deployment package, you must disable and re-enable the virtual host. To disable the virtual host, in the Operations Console, click **Deployment Configuration > Virtual Host & Load Balancing**, clear the **Configure a virtual host and load balancers** check box, and click **Save**. To enable the virtual host, follow the instructions in the Operations Console Help topic "Configure a Load Balancer and Virtual Host." You can then generate the web-tier deployment package. For instructions, see the Operations Console Help topic "Add a Web-Tier Deployment Record."

### Authentication Manager does not track which IPv6 RADIUS Clients are sending authentication requests

**Tracking Number:** AM-29509
**Problem:** If the <ANY> client is not selected, Authentication Manager should track which IPv6 RADIUS clients are sending authentication requests. Instead, authentication requests using the shared secret specified for the <ANY> client are processed regardless of the originating client's IPv6 address.
**Workaround:** This feature works for IPv4 RADIUS clients. This issue is being resolved in a future RSA Authentication Manager 8.2 patch.

### Cannot create IPv4 addresses for IPv6 RADIUS clients after removing IPv6 network settings

**Tracking Number:** AM-29485
**Problem:** If you disable IPv6 network settings in the Operations Console, you cannot update existing IPv6 RADIUS clients to use IPv4 addresses.

**Workaround:** Re-enable IPv6 network settings, update the IPv6 RADIUS clients to use IPv4 addresses, and then disable the IPv6 network settings again. Delete any IPv6 RADIUS clients that are no longer needed.

### Do not promote a version 8.1 SP1 replica instance if there is a version 8.2 primary instance

**Tracking Number:** AM-29322
**Problem:** After the primary instance has been upgraded to version 8.2, promoting a version 8.1 SP1 replica instance for disaster recovery creates a second primary instance.
**Workaround:** If the upgrade to version 8.2 does not succeed, you must restore from a backup file, a VMware snapshot, or a Hyper-V checkpoint. Always apply version 8.2 to the primary instance before upgrading the replica instances in your RSA Authentication Manager 8.1 SP1 deployment.

### VMware virtual appliance does not include a DVD/CD drive

**Tracking Number:** AM-28663
**Problem:** The VMware virtual appliance does not include a DVD/CD drive for applying updates.
**Workaround:** Use the VMware vSphere Client to shut down the virtual machine and add a DVD/CD drive. For more information, see the Operations Console Help topic "VMware DVD/CD or ISO Image Mounting Guidelines."
In addition, you can apply RSA Authentication Manager updates through your local browser, or you can scan for stored updates in an NFS share or a Windows shared folder.

### The first Quick Setup task on a Hyper-V virtual appliance displays a later start time than the second task

**Tracking Number:** AM-28393
**Problem:** If you select a Network Time Protocol (NTP) server for RSA Authentication Manager that the Hyper-V host machine does not use, the first Quick Setup task might display a later start time than the second Quick Setup task.
**Workaround:** This time display issue does not affect deployment or RSA SecurID authentication.

## Defects Fixed in This Patch

## 8.2 P4

Patch 4 contains fixes for the following issues:

**AM-30716 –** The **Self Service Console URL** field on the E-mail Notifications for User Account Changes page of the Security Console did not allow URLs with the `.local` domain.

**AM-30640 –** Performance issues including crashing, authentication errors, and depletion of network ports and other system resources occurred on the RSA Authentication Manager appliance after performing simultaneous RADIUS authentication attempts for an extended period of time.

**AM-30634 –** In deployments without Risk-Based Authentication or On-Demand Authentication licenses, users who were not enabled for RBA sometimes triggered the error "RBA/ODA feature is not licensed. Principal cannot be enabled for RBA/ODA null" when logging into a custom portal.

**AM-30582 –** Attempting to grant or revoke user group access to one or more restricted agents selected from the results of a search triggered the error "System internal error. Please contact your system administrator."

**AM-30574 –** Software token requests made through the Self-Service Console incorrectly required administrators to grant approval for distribution of the token.

**AM-30567 –** The RSA Authentication Manager appliance operating system did not start successfully if the NTP server was unreachable.

**AM-30555 -** The Operations Console was vulnerable to a reflected cross-site scripting attack using the Ping tool on the Network Tools page.

**AM-30552 –** If the hardware clock on the appliance was not updated by the NTP server and indicated a significantly different time from the operating system clock, all authentication attempts were unsuccessful and triggered the error "Passcode reuse or previous token code detected."

**AM-30476 –** RSA Authentication Manager deployments with read-only database users created using the `./rsautil manage-readonly-dbusers` command were susceptible to OpenSSL vulnerabilities described in CVE-2016-6306 and other similar attacks. After installing Patch 4, additional steps are required to fully resolve this issue. For instructions, see Known Issue AM-30476.

**AM-30358 –** In certain circumstances, the optional, non-default SSH console interface to the RSA Authentication Manager appliance may have been vulnerable to a denial-of-service attack.

**AM-30353 –** The RSA Authentication Manager appliance kernel did not properly determine the rate of challenge ACK segments.

**AM-30263 –** Penetration tests indicated that the **Administration > Trusted Realms** page of the Security Console may have been susceptible to an XML External Entity (XXE) attack.

**AM-30246 –** In certain deployments, the Security Console stopped responding due to an out-of-memory error.

## 8.2 P3

Patch 3 contains fixes for the following issues:

**AM-30523 –** Replication failed after replacing default console certificates with custom SHA256 certificates on primary and replica instances.

**AM-30489 –** The appliance operating system included several disabled default users in the etc/passwd and shadow file.

**AM-30484 –** A typo on the **Trusted Realms > Trusted User Groups** page incorrectly labeled the **Grant Access to More Accessible Agents** option as **Grant Access to More User Groups**.

**AM-30460 –** The user dashboard displayed the extendable flag for the non-extendable SID700 and SID800 tokens.

**AM-30386 –** New licenses obtained after downloading (but before installing) Authentication Manager 8.2 were rejected by Authentication Manager 8.1.

**AM-30350 –** Distributing tokens through the MMC snap-in using CTKIP failed.

**AM-30266 –** Third-party components of the Authentication Manager appliance were susceptible to security vulnerabilities CVE-2016-3706 and CVE-2016-4429.

**AM-30153 –** Extension data for some users in All Users reports was formatted incorrectly in CSV file output.

**AM-29897 –** Export Token Only failed to properly export pending replacement tokens. After importing the tokens to a new instance, PINs could not be set for tokens that were marked as replacements prior to the export.

**AM-26794 –** Token serial numbers were not masked in the local operating system syslog for AUTHMGR_CTKIP_AUTHCODE_CREATE, UPDATE, and DELETE activities when the **Mask Token Serial Number** field was configured on the **Setup > System Settings > Basic Settings > Logging** page of the Security Console.

## 8.2 P2

Patch 2 contains fixes for the following issues:

**AM-30367 –** If an identity source used a non-default port that was not included in the Directory URL during identity source configuration, using the Security Console to view group membership for users in that identity source triggered an error.

**AM-30365 –** When using the Security Console to view group membership for a user, an error occurred if one or more groups that existed in Active Directory were excluded from the Authentication Manager internal database by the Group Search Filter.

**AM-30326 –** An error occurred when an assigned token was unassigned in the Security Console, then subsequently reassigned as a replacement token.

**AM-30278 -** Authentication Manager did not support exporting ODA user data from one deployment to another. Using a new checkbox on the Export Tokens and Users page of the Security Console, you can now specify whether or not to include ODA attributes when exporting user data. For more information, see New Features and Enhancements in Patch 2.

**AM-30265 –** In deployments with large numbers of auto-registered agents (more than 30,000), the primary server became unresponsive, causing authentication and replication failure.

**AM-29400 –** Authentication Manager reported unnecessary warning messages to the system activity log when performing certain Active Directory group searches.

## 8.2 P1

Patch 1 contains fixes for the following issues:

**AM-30337 –** After updating to version 8.2, CT-KIP token activation codes generated by the Authentication Manager SDK failed when using the Authentication Manager Prime Self-Service Portal. The complete fix for this issue requires that you install an update provided by your RSA Professional Services engineer in addition to Authentication Manager Patch 1.

**AM-30331 –** In deployments modified to run customized reports (by using commands such as ./rsautil store -o OCadmin -a add_config auth_manager.reports.principal.registered_group_only true GLOBAL 500), updating to Authentication Manager 8.2 failed, causing the Authentication Manager server to become unusable and require a full factory reset.

**AM-30313 –** Installing or updating to Authentication Manager 8.2 on an appliance running on Dell PowerEdge R710 hardware caused PCI firmware errors and a 30 to 40 minute delay when restarting the appliance.

**AM-30307 –** In deployments configured with zero approval steps for token provisioning, after requesting a token using the Self-Service Console, users received an error when attempting to access the token enablement link in the automated email sent by Authentication Manager.

**AM-30296** – Users could not download offline days when authenticating through RSA Authentication Agent for Microsoft Windows using one-time emergency access codes. Authentication succeeded, but

offline days were not downloaded to the client, and an unexpected exception was reported in the Activity Monitor.

**AM-30294** – If web tier services did not start within 30 seconds (for example, when hosted on slow or overloaded hardware), then the web tier sometimes appeared to be disconnected after startup.

**AM-30293** – In some cases, after updating Authentication Manager, the Operations Console displayed the status “Online, Reinstall Required” for web tiers hosted on Linux servers.

**AM-30292** – After many successful backups (between approximately 100 and 250 in test scenarios), subsequent backups failed, reporting the message “OutOfMemoryError: getNewTla” in the Authentication Manager logs.

**AM-30291** – In some cases, if the primary identity source directory became unavailable for any reason, Authentication Manager did not connect to a properly configured failover directory.

**AM-30290** – Authentication Manager required all On-Demand Authentication tokencodes to be eight digits in length. Using a command-line utility, you can now configure Authentication Manager to generate either six-digit or eight-digit codes. For instructions, see New Features and Enhancements in Patch 1.

**AM-30285** – For Active Directory configurations with multiple domains, where a universal group exists in one domain, Restricted Agent Authentication did not succeed for members of the universal group whose user accounts belonged to a different domain. Affected users received the message “Principal does not belong to any groups activated on restricted agent”.

**AM-30283** – Help desk users with token edit privileges in one domain were able to move tokens out of other domains without possessing the corresponding edit privileges for those domains.

**AM-30282** – Authentication event records were not recorded in the Real Time Authentication Monitor for login attempts by users who were initially assigned tokens, but whose tokens were subsequently unassigned.

**AM-30280** – The dates and times describing the reporting period for Activity Reports were listed in reverse order.

**AM-30279** – Except for Super Admins, other types of administrators were not able to resend emails to distribute software tokens, even when assigned the correct administrative roles and permissions. When attempting to resend token distribution emails, affected administrators received the message “Unexpected error during command com.rsa.ucm.request.ResendLastMailCommand execution.”

**AM-30276** – Token serial number was missing from the description field for Login with Temporary Fixed Tokencode events in the Authentication Activity Monitor.

**AM-30275** – On-Demand Authentication (ODA) token requests made through the Self Service Console failed when the number of assigned tokens approached (but did not exceed) the ODA license limit, triggering the error message "License violation, on-demand authentication is not licensed.”

**AM-30274** – Attempting to assign tokens to unregistered users using the context menu on the **Identity > Users > Manage Existing** page of the Security Console resulted in an error when using the search filter “Search for users across all identity sources” if multiple users had similar names and belonged to more than one identity source.

**AM-30273** – Custom user attribute values were not displayed in the Users with Tokens report if the identity source for the report was unspecified.

**AM-30262** – After updating to Authentication Manager 8.2, administrators were unable to add or edit internal database users that had email addresses ending in top-level domains with more than three characters (such as .local). See New Features and Enhancements in Patch 1 for more information.

**AM-30258** – An administrator with permissions for one or more specific security domains received an error message when attempting to view group membership for users belonging to different user groups with different security domains.

**AM-30253 –** Attempting to add notes containing “new line” characters to users in the Security Console Dashboard failed, triggering the message “Unable to process request. Try again.”

**AM-30238** – Authentication Manager was vulnerable to specific timestamp-based NTP client attacks.

**AM-30237** – Authentication Manager was vulnerable to specific man-in-the-middle padding oracle attacks against OpenSSL components. See CVE-2016-2107 for more information.

**AM-30219 –** The Authentication Manager SNMP agent debug trace log output included unnecessary detailed network packet content information when the Authentication Manager log level was set to verbose.

**AM-30217 –** The Operations Console did not accept fully-qualified domain names where the first segment of the domain name did not include an alphabetic character or dash (-).

**AM-30213** – If an administrator uploaded a custom logo as part of web tier customization, the custom logon banner on the web tier displayed an RSA logo instead of the custom logo.

**AM-30148** – Users in an Active Directory OU with a DN containing a backslash (\) could not log into restricted agents. Authentication failed, triggering the message “AGENT_ACCESS_CHECK_FAILED_NO_ASSOCIATED_GROUP” in the RSA Authentication Monitor.

**AM-30131 –** Attempting to view group membership for an Active Directory user on the Users page of the Security Console failed if an identity source group search filter was configured in the Operations Console.

**AM-30123** – The Security Console lacked sufficient validation for GUID values, which caused Reflected Cross-Site Scripting vulnerabilities. Authentication Manager no longer accepts invalid GUIDs such as "<script>alert(gotcha)</script>" or other forms. GUIDs must use no more than 40 alphanumeric characters, plus dot (.), dash (-), blank space ( ), and underscore (_).

**AM-29877 –** The SNMP event “BROKEN_RADIUS_REPLICATION=Primary RADIUS server reported a problem with replication” was not properly recorded in the management information base file for Authentication Manager (**AM.mib**). Some RADIUS-related SNMP events now have new, valid object IDs.

## Support and Service

You can access community and support information on RSA Link at **https://community.rsa.com**. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at **www.rsaready.com** provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.



### Trademarks



### 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.