RSA® Authentication Manager 8.1 Patch 4 Readme

September 2014
Prerequisite Release:
RSA Authentication Manager 8.1

Contents

Before Installing This Patch

Note: RSA Authentication Manager 8.1 patches include fixes from Authentication Manager 8.0 Patch 5, Patch 6, and Patch 7. All Authentication Manager 8.1 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 8.1 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 when you apply the patch to the primary or replica instances. All instances must be able to communicate while the patch is applied.
- You must have at least 4 GB of free disk space to apply the patch.
- From the 8.0 virtual appliance, you must upgrade to 8.1 before installing this patch. See the *RSA Authentication Manager 8.1 Setup and Configuration Guide* for instructions.

Installing a Patch

The RSA Authentication Manager 8.1 Patch 4 ZIP file (**am-update-8.1.0.4.0.zip**) contains the following files:

- **am-update-8.1.0.4.0.iso**. The RSA Authentication Manager 8.1 Patch 4 ISO file that is used to apply the patch to Authentication Manager.
- **RSA Authentication Manager 7.1 Migration Export Utility**. The folder that contains the necessary files for installing the updated Migration Export Utility on version 7.1. If you plan to perform a migration from version 7.1, or are testing the version 7.1 migration process, use this version of the utility with Patch 4. See RSA Authentication Manager 7.1 Migration Export Utility on page 7 for details.

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
- Scan for Product Updates
- Apply Product Update

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 8.1 to locate patches.

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

Before You Begin

Download and unzip the patch from RSA SecurCare Online to a location that the primary or replica instance can access.

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 is open for https traffic.
- 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, after upgrading the primary instance, wait for the replication status to return to normal for all replica instances before upgrading the replica instances. To verify the replication status, log on to the primary instance Operations Console, and click **Deployment Configuration > Instances > Status Report**.

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: The first time the update is applied, 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

- If the deployment includes a web tier, you must update the web tier when you update the version of Authentication Manager. Authentication Manager provides an **Update** button in the Operations Console for each web tier that is out-of-date. For more information, see "Update the Web Tier" in Appendix A of the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.
- 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 8.1 Patch 4

RSA Authentication Manager 8.1 is a prerequisite release for this patch. Therefore, you must deploy version 8.1, then apply Patch 4, and then you can migrate data from an earlier version. This section provides information to guide you in that migration process.

From RSA Authentication Manager 6.1

If you are migrating from RSA Authentication Manager 6.1, refer to the following documents:

- *RSA Authentication Manager 6.1 to 8.1 Migration Preparation Guide* – This document is available, along with the **RSA Authentication Manager 6.1 Migration Assessment Utility**, on RSA SecurCare Online, at the following location: **https://knowledge.rsasecurity.com/scolcms/set.aspx?id=9620**
- *RSA Authentication Manager 6.1 to 8.1 Migration Guide*

From RSA Authentication Manager 7.1

If you are migrating from RSA Authentication Manager 7.1, refer to one of the following documents, as appropriate for your configuration:

- *RSA Authentication Manager 7.1 to 8.1 Migration Guide: Upgrading RSA SecurID Appliance 3.0 on Existing Hardware*.
- *RSA Authentication Manager 7.1 to 8.1 Migration Guide: Migrating to a New Hardware Appliance or Virtual Appliance*.

RSA Authentication Manager 7.1 Migration Export Utility

To migrate from RSA Authentication Manager 7.1, or to test the migration process, do the following:

1. Install the RSA Authentication Manager 7.1 Migration Export Utility, which is packaged with this patch.
2. Use the utility to generate a migration package for your pre-production testing environment.

If you have already installed another version of the RSA Authentication Manager 7.1 Migration Export Utility on version 7.1 for testing purposes, you must do the following:

1. Uninstall the previous version of the utility.
2. Install the utility that is packaged with this patch.
3. Generate a new migration package for your version 8.1 pre-production testing environment.

To install the utility, access the required files in the **RSA Authentication Manager 7.1 Migration Export Utility** folder that appears when you extract the patch ZIP file. For instructions on installing or uninstalling the utility, see one of the following documents, as appropriate for your configuration:

- *RSA Authentication Manager 7.1 to 8.1 Migration Guide: Upgrading RSA SecurID Appliance 3.0 on Existing Hardware*
- *RSA Authentication Manager 7.1 to 8.1 Migration Guide: Migrating to a New Hardware Appliance or Virtual Appliance*

From RSA Authentication Manager 8.0

If you are upgrading from RSA Authentication Manager 8.0, refer to Appendix A, "Upgrading RSA Authentication Manager 8.0 to 8.1," in the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

Known Issues

AM-28295 – Excess traffic between LDAP and Authentication Manager can cause performance issues in configurations where a Base Domain Identity Source is mapped in the Operations Console, and Organizational Units under that Base Domain are mapped to sub-security domains. As a workaround for this issue, RSA recommends configuring a separate Identity Source in Operations Console for each individual Organizational Unit. See AM-28156 for related information.

AM-28350 – On Red Hat® Enterprise Linux®, the Authentication Manager 8.1 web tier fails to start unless /bin/bash is set as the default shell for the user account that installs and runs the web tier. As a workaround for this issue, RSA recommends configuring /bin/bash as the default shell for any user account that will install or run the web tier.

Defects Fixed in This Patch

8.1 P4

Patch 4 contains fixes for the following issues:

AM-27819 – If a user entered an incorrect value for **Current PIN**, or left the field blank when attempting to change his or her On-Demand Authentication PIN in the Self-Service Console, the user was redirected to the My Account page, and a nonspecific failure message appeared. A message describing the specific error now appears on the Change Your PIN page if the user leaves the field blank, or on the My Account page if the user enters an incorrect value.

AM-27820 – Password changes via the "Forgot your password" link on the Self-Service Console landing page succeeded, even when the user entered mismatched values in the **Create New Password** and **Confirm New Password** fields. Password changes now fail as expected in such cases.

AM-27848 – Authentication Manager's real-time activity monitor did not log authentication requests from machines that were configured with incorrect IP addresses, or were not defined as agent hosts. The real-time activity monitor now logs such requests.

AM-28040 – The Token Expiration report retrieved all of a user's groups from an identity source, instead of only groups that were managed by Authentication Manager. Reports containing thousands of users who belonged to thousands of groups took multiple hours to complete, or did not complete at all. The Token Expiration report now retrieves only groups that are managed by Authentication Manager, and completes properly. If an administrator specifies a group name when running the report, however, the report retrieves all users in that group, regardless of whether the group is managed by Authentication Manager.

AM-28265 – In environments where LDAP's Virtual List View feature was disabled, or in Active Directory environments where the number of user groups exceeded 10,000, Security Console user group searches failed, triggering an error message. Security Console user group searches no longer rely on paginated lists or the Virtual List View feature, and now succeed in such cases.

AM-28266 – The List All User report retrieved all of a user's groups from an identity source, instead of only the groups that were managed by Authentication Manager. Reports containing thousands of users who belonged to thousands of groups took multiple hours to complete. The List All User report now retrieves only groups that are managed by Authentication Manager. Administrators who require backwards compatibility, however, can configure the report to retrieve all groups by running the following command-line utility:

```
./rsautil store -o <OCadmin> -a add_config
auth_manager.reports.principal.all_group true GLOBAL 500
```

AM-28325 – The write cache was disabled by default on the Intel A130 appliance, which caused poor Authentication Manager performance on the device. The Authentication Manager startup script now enables the write cache automatically when the server starts, which improves performance.

AM-28399 – If an identity source used the external enable flag in its identity source mapping, List All User reports run against that identity source failed. List All User reports now succeed in such cases.

AM-28431 – Authentication Manager was susceptible to the security vulnerability outlined in CVE-2014-0224. This security vulnerability has been resolved.

8.1 P3

Patch 3 contains fixes for the following issues:

AM-10837 – Although system account settings prevented root login, the Secure Shell daemon configuration did not prevent SSH root login. The SSHD configuration now explicitly prohibits root login via SSH.

AM-27100 – When migrating from Authentication Manager 6.1, the **Prevent auto registration from unassigning IP address** setting is enabled for agents by default, which can cause authentication problems if the agents acquire new IP addresses post-migration. The Scan Results page now displays a warning message during migration, to remind users to change the default configuration using the Custom migration option, if necessary.

AM-27367 – The default connection timeout period for the IPv4/IPv6 agent was set to 60 seconds, which caused delays in authentication return-trip time when an authentication server could not be reached. The default timeout period has been reduced to 10 seconds to eliminate such delays. Customers who configured a custom value for the timeout period before installing Patch 3 will need to reapply their custom setting after installing the patch.

AM-28055 – If a user clicked **Cancel** at any point when prompted for authentication credentials, and then tried to authenticate normally, an error message appeared, and authentication failed. Authentication now succeeds in such cases, and the error message no longer appears.

AM-28088 – The **Return List Attributes** and **Check List Attributes** fields on the Edit RADIUS Profile page of the Security Console did not display the code string for the line feed control (\n) properly. The code string now appears correctly.

AM-28107 – Administrators monitoring the Self-Service approval queue received email notifications when users applied for new tokens, even if email notifications were disabled in the **E-mail Notification Settings** section of the Self-Service workflow policy. Email notifications are now properly disabled in such cases.

AM-28240 – Authentication Manager was susceptible to the security vulnerability outlined in CVE-2014-0114. This security vulnerability has been resolved.

AM-28242 – Backups created from Authentication Manager environments with one primary instance and at least one replica instance, where an alternative IP address was configured for a RADIUS agent on a replica server, could not be restored successfully on a new primary instance. Restoring such backups now succeeds.

AM-28274 – In Patch 1, the fix for AM-27997 introduced a regression that prevented users from typing multi-byte encoded characters as answers to security questions. Patch 3 removes this fix and the regression it caused. As a result, answers to security questions are no longer masked during RBA authentication.

AM-28405 – RSA Authentication Manager 8.1 web tiers now support Microsoft Windows Server 2012 R2.

8.1 P2

Patch 2 contains fixes for the following issues:

AM-26825 – In environments where the BASEDN value for an identity source was a root context, such as "DC=RSA, DC=COM", various user and administrator actions generated warnings containing Java stack traces in the system activity monitor. The method by which the system handles warning messages has been modified so that the unnecessary warnings are no longer captured in the logs.

AM-26880 – Appliance startup occasionally failed on the OS level while trying to sync time, if all configured Network Time Protocol servers were unreachable. Startup no longer depends on successful NTP time sync. If the time sync does not succeed after 60 seconds, the operation times out and system time is used as the current time. A console warning is triggered in this case. If Critical System Event notifications are configured, a Critical System Event Notification is also triggered.

AM-27767 – Frequent web-tier update checks caused sharp spikes in CPU utilization on the web-tier server. The time interval between web-tier update checks has been increased to 15 minutes, which reduces overall web-tier server CPU utilization.

AM-27789 – An Authentication Manager service would shut down unexpectedly, and attempt to restart, if the Java Virtual Machine on which it was running became temporarily unresponsive. The timeout period before Authentication Manager services restart in the event of an unresponsive JVM has been increased, which gives the JVM more time to recover, and resolves this issue in most cases.

AM-27799 – RADIUS authentications generated defunct processes on Authentication Manager servers. A shared library used by RADIUS has been modified so that Authentication Manager no longer generates defunct processes.

AM-27832 – User options for On-Demand Authentication were inconsistent. **EMAIL** and **SMS** options appeared interchangeably with **Mail Address** and **Mobile Number**. Additionally, if users selected the **EMAIL** delivery method, the value field for **Mobile Number** was still visible. User options for On-Demand Authentication have been modified to display consistent information.

AM-27905 – If a user was enabled or disabled from the User Dashboard under **User Profile**, the Administration Activity report showed an "update principal" activity, but not the specific action. Enabling and disabling users from the User Dashboard is now clearly reported in Administration Activity logs.

AM-27918 – The web-tier application server was generating excessive log files that caused delays in the uninstallation process, and negatively impacted performance. Generation of the log files responsible for this issue has been disabled so that it no longer affects uninstallation or performance.

AM-27925 – The icon image for the Blackberry 10, which would normally appear along with the device name on various menus and information pages in the Security Console and the Self-Service console, was missing. The missing icon image has been added, and now appears in all appropriate menus and information pages.

AM-27936 – Critical System Event Notifications were triggered, advising that "a backup had not been created successfully in the last 7 days," even when a successful backup had occurred during that time. The mechanism that generates Critical System Event Notifications has been modified so that notifications regarding backups are sent only when appropriate.

AM-27975 – Authentication failed in environments with overlapping user IDs and aliases, which prevented successful migration from Authentication Manager 6.1. Authentication now fails only if neither user ID nor alias resolves successfully, or if neither has access.

AM-28015 – It was possible to authenticate using an expired token if the token's expiration date was extended by directly updating the Authentication Manager database. It is no longer possible to authenticate with an expired token.

AM-28028 – On the SecurID Tokens page, sortable columns such as **Serial Number** and **Token Type** could not be sorted, while unsortable columns such as **Assigned To** and **SecurID PIN** appeared sortable. The sort function now sorts the appropriate columns, and is disabled for unsortable columns.

AM-28050 –If a user had more than 50 authentication activities over multiple days, the User Dashboard did not properly reflect the most recent user authentication activities. The User Dashboard activity log now correctly displays the 50 most recent user authentication activities from the last 6 days.

AM-28060 – "Users Enabled for On-Demand Authentication" report displayed a maximum of 500 results, even when more than 500 users were enabled for On-Demand Authentication. All ODA-enabled users are now displayed in the report.

AM-28149 – If a user had both a current token and a replacement token, and both were disabled in Authentication Manager 6.1, the replacement token became enabled after migration to an Authentication Manager 8.1 environment. Disabled tokens now remain disabled after migration to Authentication Manager 8.1.

AM-28152 – It was possible to register a user to an incorrect identity source if two identity sources had the same user base domain name but different group domain names, which caused authentication through restricted agents to fail. Users are now registered to the correct identity source in these cases.

AM-28156 – In environments where a large user population was divided into multiple Active Directory organizational units, which were mapped to corresponding security domains in Authentication Manager, user searches returned incomplete subsets of the expected search results. A complete set of results is now returned in these cases, up to the maximum console limit of 500. See AM-28295 for related information.

AM-28201 – When an EAP authentication was handled by a replica server, it created an EAP32 session on the replica that could not be successfully deleted by the primary replication service. This caused replication to fail, and generated an "Internal Replication Error" in the Replication Status Report. Replication is now successful in these cases.

AM-28205 - A reflected cross-site scripting issue existed in two operations console pages. This security vulnerability has been resolved.

AM-28251 – RADIUS installation included unnecessary files which were considered insecure by certain customer guidelines. The unnecessary files have been removed from the RADIUS installation.

8.1 P1

Patch 1 contains fixes for the following issues:

AM-27293 – Users in an external group linked to a restricted agent can now authenticate to the restricted agent, even if the name of the group ends with an asterisk (*).

AM-27630 – Migrated users with aliases were unable to authenticate. Authentication now succeeds for migrated users with aliases.

AM-27660 – Characters that were previously restricted in migrations from AM 6.1 are now permitted for AM 6.1 migrations. User names, groups, alias names, and other data containing these characters can now be migrated from Authentication Manager 6.1 to AM 8.1 Patch 1 and above.

AM-27943 – During automatic token replacement, some token entries were missing from internal database tables. As a result, those tokens could not be unassigned. The code now handles this case so that such tokens can be unassigned successfully.

AM-27947 – With **User Account Enabled State** set to **Directory and Internal Database**, a user from an external identity source was disabled in Authentication Manager even when enabled from a disabled state in the external directory, and not disabled in Authentication Manager. Such a user is now enabled when enabled in both the external identity source and the internal Authentication Manager database.

AM-27960 – When a password policy required no periodic password changes (**Periodic Expiration** was not set), the **Max Lifetime** column displayed "0 seconds," which was misleading. To clarify, when **Periodic Expiration** is not set (no periodic password changes required), **Max Lifetime** now displays "None" instead of "0 seconds."

AM-27961 – (Virtual appliance only) Certain vmware-tools operations generate "appLoader-*.log" files under **/tmp/vmware-root-***. The script **vmware-apploader-cleanup** has been created and added to **/etc/cron.daily** so that appLoader files are deleted every 24 hours.

AM-27966 – User token report showed an incorrect last token authentication date. The report now correctly shows the date the token was last used for authentication ("Last Used to Authenticate").

AM-27967 – In the Operations Console, connecting to an external identity source failed if the target URL included upper- instead of all lower-case letters (for example, "LDAPS://*domainname.com*" instead of "ldaps://*domainname.com*"). The connection no longer fails when the URL includes both upper-and lower-case letters.

AM-27973 – The RSA Authentication Manager 7.1 Migration Export Utility failed to create a migration package on Authentication Manager 7.1 when the system had a large Oracle Systems Change Number (SCN) value. The Authentication Manager 7.1 Migration Export Utility has been changed in Patch 1 so that it successfully creates a migration package on systems with large SCNs.

AM-27991 – Token-related reports gave incorrect data when two date-related filters were specified. The affected reports now provide the correct data when two such filters are specified.

AM-27992 – When the global option **Show only attributes with values** was selected, the View user pages showed all identity attributes, with or without values. The option has been improved so that when it is selected, the View user pages now show only the identity attributes with values.

AM-27995 – The **RSA-AM.mib** file was being generated with syntax errors, which prevented its use by third-party applications. The **RSA-AM.mib** file is now generated correctly.

AM-27996 – Due to a time-out configuration, a trusted realm could not be established over a wide area network (WAN). The time-out setting was corrected to resolve the connection problem.

AM-27999 – When running the report "Agents not updated by auto-registration more than a given number of days," and if an invalid value is entered for **Days agent record was not updated by auto-registration service**, the resulting error message was unclear. The error message now clearly specifies both the incorrect value and the maximum value allowed, which is 365.

AM-28000 – The internal Authentication Manager password policy was overriding the LDAP password policy so that LDAP users were locked out of the Security Console and the Self-Service Console. The internal password policy now affects only internal users, and the LDAP password policy affects only LDAP users.

AM-28001 – The activity log was not correctly logging when an administrator changed passwords due to the applied password policy. The activity log now specifies the reason for changing passwords.

AM-28002 – An administrator belonging to LDAP was failing login because the password had expired due to the LDAP password policy. The activity log, however, provided no reason for the failure. The activity log now provides a clear reason for the login failure.

AM-28004 – In user search, administrators were unable to search for users within their scope by custom attribute, but able to do so in advanced search. Administrators now require **View** permission for **User Authentication Attributes** in order to search for users within their scope by custom attribute, either in user search or advanced search.

AM-28010 – The UNIX **service** command to check Authentication Manager status was actually stopping AM services. The same command now checks AM status without stopping AM services.

AM-28011 – If the customer license does not include the RBA/ODA feature, external LDAP users could not activate hardware tokens using the Self-Service Console; the operation failed with an RBA/ODA license error. External users for such customers can now successfully activate tokens using the Self-Service Console.

AM-28019 – Replication failed when an agent with auto-registration enabled was registered on both primary and replica instances at the same time. The following error message appeared:

```
RSA1.local.hrw.org,,,,Unhandled exception during main loop. Shutting
down this service thread.
com.rsa.replication.UnexpectedApply2PException: unable to apply replica
changes
      at com.rsa.replication.ApplyR2P.executeChanges(ApplyR2P.java:337)
      at com.rsa.replication.ApplyR2P.commitBatches(ApplyR2P.java:250)
      at com.rsa.replication.ApplyThread$1.doWork
```

Replication no longer fails when an agent with auto-registration enabled is registered simultaneously on primary and replica instances.

AM-28118 – Patch 1 resolves an issue in which RSA Authentication Manager 8.x software could be affected by (CVE-2014-0160) in the event a customer had enabled one or more read-only database users via the "manage-readonly-dbusers" command line utility (CLU).

Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.emc.com/support/rsa/index.htm**
RSA Ready Partner Solution Gallery	**https://gallery.emc.com/community/marketplace/rsa**

Trademarks

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.