RSA® Authentication Manager 8.0 Patch 7 Readme

January 2014

Prerequisite Release:
RSA Authentication Manager 8.0

Contents

Before Installing This Patch 1
Installing a Patch 2
After Installing This Patch 5
Migrating Data From RSA Authentication Manager 7.1 7
Rolling Back This Patch 7
Known Issues 8
Defects Fixed in This Patch 9
Support and Service 14

Before Installing This Patch

Note: RSA Authentication Manager 8.0 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 8.0 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.

Note: If you are running RSA Authentication Manager 8.0 or RSA Authentication Manager 8.0 P 01, you must perform additional tasks described in *After Installing This Patch* on page 5. To view the current software version, log on to the Security Console and click **Software Version Information**. Check if the value in the version field is **8.0** or **8.0 P 01**.

Installing a Patch

The RSA Authentication Manager 8.0 Patch 7 ZIP file (**am-update-8.0.0.7.0.zip**) contains the following:

- **am-update-8.0.0.7.0.iso**. The RSA Authentication Manager 8.0 Patch 7 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 you are testing the version 7.1 migration process, install this version of the utility after applying the patch. For more information, see *After Installing This Patch* on page 5.

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 to allow RSA Authentication Manager 8.0 to locate patches.

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

Before You Begin

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

To scan for updates on a DVD or CD, 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.”

To specify or edit a product update location:

1. In the Operations Console, click **Maintenance** > **Update & Rollback**.
2. On the **Update & Rollback** page, your local browser is configured as the method for applying an update. 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 setting 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**.
    - 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.

To scan for product updates:

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

   The **Available Updates** section displays a list of updates, with the following information for each update:

   - **Version**. The version of the update. To see the current Authentication Manager version, see the top of the Update and Rollback page.
   - **Reversible**. Indicates whether you can roll back (undo) the update.

- **Automatic Appliance Reboot**. Indicates whether Authentication Manager automatically restarts the Appliance to apply the update. If the Appliance restarts, you must perform another scan to see a current list of updates.

- **Automatic Operations Console Reboot**. Indicates whether Authentication Manager automatically restarts the Operations Console to apply the update. If the Operations Console restarts, you must perform another scan to see a current list of updates.
- **Action**. States whether the update is available to apply. Lists the minimum system requirement for the update.

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.

   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

- *Specify a Product Update Location*
- If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, *Scan for Product Updates*.

To apply the patch:

1. In the Operations Console, click **Maintenance** > **Update & Rollback**.
2. RSA recommends applying 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. Click **Browse** to navigate to the location of the update. You cannot type the update location in the **Update Pat**h field.
     c. Click **Upload**.
     d. Verify the update details, and click **Apply**.

- 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**.
    c. Click **Confirm** to apply the update.

3. In the **Password** field, enter the password for the operating system user **rsaadmin**, and click **Log On**.
4. The basic status messages appear while the update is applied. You can view more detailed information on the **Advanced Status View** tab.

After the patch is applied, the following occurs:

- Authentication Manager moves the update from the **Available Updates** section to the **Applied Updates** section.
- The Operations Console or Appliance automatically restarts. When the restart is complete, click **Done**.
- When you return to the **Update & Rollback** page, the update is listed in the **Applied Updates** section. To save the high-level update history, click **Download Detailed History Log**.
- The software version information is updated with the patch number. To view the software version information, log on to the Security Console, and click **Software Version Information**.

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.
- 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 Installing This Patch

Depending on the software version that you are running before Patch 2, you might need to perform additional, patch-specific tasks. Before installing the patch, verify the version that is currently running on your server. To view the software version information, log on to the Security Console, and click **Software Version Information**.

- If the current version is AM 8.0, apply post-installation tasks for Patch 1 and Patch 2.
- If the current version is AM 8.0 P1, apply post-installation tasks for Patch 2.

Post-Installation for Patch 1

Patch 1 prevents the logging of the Operating System password and the Simple Network Management Protocol (SNMP) passwords in the Syslog. To further secure these passwords, do the following:

- Change the Operating System account password and the passwords that are associated with your SNMP configuration. For instructions, see the Operations Console Help topics "Change the Operating System Account Password" and "Configure SNMP."
- Remove the Operating System account password and the SNMP passwords from existing log entries. For instructions, see the knowledgebase article with the Solution ID a61380 on RSA SecurCare Online.

Patch 1 resolves an issue regarding the display options. If you changed the default Security Console display options in version 8.0 or in a version 7.1 deployment that was migrated before applying Patch 1, review the display options for token lists in the Security Console. This patch includes the following improvements:

- More display options available for token lists. For instructions on configuring these additional options, see the Security Console Help topic "Set Console Display Options."
- Consistent terminology between the column names that display in the Security Console and the values that can be set to display token lists.

Note: These improvements do not change which display options were set to show or hide in the Security Console for token lists.

If you migrated data from RSA Authentication Manager version 7.1 before applying Patch 1, and you had imported a migration package from the local machine, a copy of the encrypted migration package was automatically created in the following location on the virtual appliance: /opt/rsa/am/utils/packages. RSA recommends that you delete the migration package from this location.

If you migrated data from RSA Authentication Manager 7.1 before applying Patch 1, and the migrated data included HTTP plug-in settings that use a Short Message Service (SMS) HTTP proxy for on-demand tokencode delivery, you must reconfigure the proxy password. For instructions, see the Security Console Help topic "Configure the HTTP Plug-In for On-Demand Tokencode Delivery."

Next Steps

RSA recommends that you back up the version 8.0 deployment. For instructions, see the Operations Console Help topic "Create a Backup Using Back Up Now."

Post-Installation for Patch 2

Patch 2 prevents Authentication Manager from logging the administrative account password that is used to create a connection between Authentication Manage and applications developed with the RSA Authentication Manager 8.0 Software Development Kit (SDK).

If you used the SDK to develop an application that communicates with Authentication Manager, and you configured the log level for Trace logs as **Verbose**, RSA recommends that you create a new password for the administrative account that is responsible for this connection. For instructions, see the Security Console Help topic “Change a User's Password.”

Next Steps

After changing the password in the Security Console, you must communicate the new password to the administrators who use the custom application.

RSA recommends that you back up the version 8.0 deployment. For instructions, see the Operations Console Help topic “Create a Backup Using Back Up Now.”

Migrating Data From RSA Authentication Manager 7.1

If you plan to migrate from RSA Authentication Manager 7.1, or if you are currently testing 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 8.0 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 the *RSA Authentication Manager 7.1 to 8.0 Migration Guide*.

Rolling Back This Patch

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

Note: If your software version was 8.0 before installing this patch, and you need to roll back the patch, you must reinstall the web tier after you roll back. If you were running software version 8.0 P 01 or greater before installing this patch, there is no need to reinstall the web tier after rolling back this patch.

To roll back this patch:

1. In the Operations Console, click **Maintenance** > **Update & Rollback**.
2. 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.”
3. To roll back the last update that was applied, click **Roll Back Update**. Only a reversible update can be rolled back.
4. Click **Confirm** to roll back the update.
5. In the **Password** field, enter the password for the operating system user **rsaadmin**, and click **Log On**.

    The Progress Monitor shows the basic status view of the rollback. You can view more detailed information on the **Advanced Status View** tab. When the rollback completes, the Operations Console restarts.
6. When the restart is complete, click **Done**.

Next Steps

Verify the software version information. To view the software version information, log on to the Security Console, and click **Software Version Information**.

Known Issues

AM-26636, AM-24612 Clicking certain **Help on this page** links in the Security Console or the Operations Console displays a blank page in the Help window. If this occurs, try accessing the topic through the Help table of contents by clicking **Help** > **All Help Topics**.

Defects Fixed in This Patch

8.0 P7

Patch 7 contains fixes for the following issues:

AM-27342 If the customer license does not include the RBA/ODA feature, external LDAP users could not activate 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-27680 User token report showed incorrect last token authentication date. The report now correctly shows the date the token was last used for authentication ("Last used to Authenticate").

AM-27816 Due to a timeout configuration, unable to establish a trusted realm over a wide area network (WAN). The timeout setting was corrected to resolve the connection problem.

8.0 P6

Patch 6 contains fixes for the following issues:

AM-27071 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-27115 The UNIX **service** command to check AM status was actually stopping AM services. The same command now checks AM status without stopping AM services.

AM-27301 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 why the login failed.

AM-27302 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-27303 Internal password policy was overriding LDAP password policy so that LDAP users were locked out of the Security Console and Self Service Console. Internal password policy now affects internal users only, and the LDAP password policy affects LDAP users only.

AM-27436 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 now when it is selected, the View user pages show only the identity attributes with values.

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

AM-27712 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.

8.0 P5

Patch 5 contains fixes for the following issues:

AM-27247 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-27254 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-27260 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-27444 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-27538 Replication services failed to start after shutting down due to an HTTP: ERROR 500 exception, as follows:

```
Caused by:
com.rsa.authmgr.internal.replication.TransportClientUnexpectedStatusExc
eption: Expected the HTTP response code 200 or 202, but got: 500
Message: java.net.SocketTimeoutException: Read timed out
```

Replication services now restart after such an unexpected exception, and they keep attempting to restart until the temporary network issue is resolved.

8.0 P4

Patch 4 contains fixes for the following issues:

AM-26224 Migration failed during the migration package scan phase without generating any logs. 6.1 migration has been improved to accommodate for slow network connections.

AM-26907 The User Dashboard displayed only 50 recent authentication events for a user, when a larger number of authentication records for that user were collected from the last six days. Refreshing the dashboard did not work. The dashboard now refreshes correctly to show the next 50 events, and so on, until all retrieved authentication records are displayed.

AM-27178 The **Last Modified** field of the user record displayed "<system>" and not the actual administrator who performed the administrative task. This field now displays the administrator who performed the task if the administrator has sufficient permissions to perform the operation.

AM-27205 The pathname for the location of the migration package generated by the migration utility does not allow special characters. The message that appears when a customer enters a pathname with special characters has been reworded.

AM-27256 Super admins were blocked from receiving critical notifications when authentication threads were deadlocked. Authentication Manager now maintains a separate list of super admins so that they receive critical notifications even if authentication threads are deadlocked.

8.0 P3

Patch 3 contains fixes for the following issues:

AM-27000 If you imported some version of Android, iPhone, or Windows phone software token definition file in 7.1, after migrating to 8.0, the **Add Software Token Profile** page did not include “Compressed Token Format CTF” as a **Delivery Method** option. The option now appears as a **Delivery Method** option.

AM-27042 If system backup failed due to insufficient disk space, the error message was unclear. The error message now specifies the minimum amount of disk space required for a successful backup.

AM-27059 After migrating from 7.1 SP4, security questions for migrated users were not displaying in the Security Console. The security questions for migrated users are now displayed.

8.0 P2

Patch 2 contains fixes for the following issues:

AM-26900 If the license batch job was migrated from version 7.1, the job was unable to run in version 8.0 and resulted in an error in the system log. The RSA Authentication Manager 7.1 Migration Export Utility no longer exports the 7.1 license batch job.

If you plan to perform a migration or you are currently testing the migration process, install the Migration Export Utility that is packaged with this patch to apply this fix. If you already have a previous version of the utility installed, you must uninstall the utility and install the utility that is packaged with the patch ZIP file. For instructions, see the *RSA Authentication Manager 7.1 to 8.0 Migration Guide*.

AM-26924 If you created a custom application with the RSA Authentication Manager 8.0 Software Development Kit (SDK), and you chose to record trace logs with a verbose logging level, the administrative account password that is used by the custom application to connect to Authentication Manager was in clear text in the trace log file.

AM-26939 A migrated version 7.1 report that was based on the 7.1 template **Event Token Expiration by Event** report caused an error when attempting to manage any existing report in version 8.0. Event-based tokens are not supported in version 8.0. The RSA Authentication Manager 7.1 Migration Export Utility no longer exports any version 7.1 report that was created with this unsupported template.

If you plan to perform a migration or you are currently testing the migration process, install the Migration Export Utility that is packaged with this patch to apply this fix. If you already have a previous version of the utility installed, you must uninstall the utility and install the utility that is packaged with the patch ZIP file. For instructions, see the *RSA Authentication Manager 7.1 to 8.0 Migration Guide*.

AM-26993 Replica instance promotion was unsuccessful when the original primary instance included alias IP addresses.

8.0 P1

Patch 1 contains fixes for the following issues:

AM-9405 If you disabled the option to protect the IP address of auto-registered agents during version 6.1 migration, auto-registered agents were still protected after migration.

AM-24142 on the **SecurID Tokens** page in the Security Console, the columns **Pending Replacement By Token** and **Will Replace Token** did not display and were not available as display options for token lists in the Security Console. You can now configure these options to display in the Security Console. The following changes also apply:

- The display options and column names now use consistent terminology.
- There is a new default order to the display options.
- Certain display options are now hidden or shown by default in the Security Console.

AM-24672 When a user set an on-demand authentication PIN through the Self-Service Console, the SNMP GET counters did not update.

AM-24776 On the **SecurID Tokens** page in the Security Console, RSA improved the sorting of assigned and unassigned tokens.

AM-25985 The SNMP GET counters did not increase when calculating the following events:

- Self-Service Console and on-demand authentication requests
- Token assignments
- PIN events
- Self-service enrollment
- Offline authentication policies

AM-26224 A version 6.1 import may have been unsuccessful when importing a database dump file that was smaller than 2 GB.

AM-26514 If you migrated data from version 7.1 before applying the patch, and you had imported a migration package from the local machine, a copy of the encrypted migration package was automatically created in the following location on the virtual appliance: **/opt/rsa/am/utils/packages**. This directory temporarily stores the migration package for import purposes only. The import process now deletes this migration package after data is migrated into version 8.0.

AM-26616 After migrating from RSA Authentication Manager 6.1, migrated RADIUS clients were not associated with a RADIUS agent.

AM-26651 If you never managed a user group from an external identity source in RSA Authentication Manager 8.0, you could not configure restricted access times for the user group.

AM-26662 A warning message did not display when a user enabled for risk-based authentication attempted to use on-demand authentication as an identity confirmation method but did not have the necessary attributes mapped for on-demand authentication. A message now appears that describes the issue and advises users to contact an administrator to set up on-demand authentication.

AM-26669 If more than 500 administrators ran concurrent searches for tokens when a large number of tokens were deployed, the Security Console might display an internal server error.

AM-26689 In a deployment with multiple replica instances, any attempt to synchronize the replica instances was unsuccessful when the operation was performed within 15 minutes of completing any of the following tasks:

- Reverting the primary instance to a snapshot
- Restoring the primary instance with a backup
- Promoting a replica instance to a primary instance

AM-26692 RSA updated the RSA Authentication Manager 8.0 to prevent storing the Short Message Service (SMS) HTTP plug-in proxy password in clear text in configuration file.

AM-26707 When viewing silent collection details for an enabled risk-based authentication user, the Security Console did not display the correct number of days remaining in the silent collection period.

AM-26715 When migrating from RSA Authentication Manager 6.1, user groups in external identity sources that were activated on agents, and had access time restrictions, did not retain these settings after migration. The settings for restricted access times and access to restricted agents are now migrated to 8.0.

AM-26723 The Security Console periodically displayed a blank page when administrators attempted to view trusted users from the context menu of the **Trusted Realms** page.

AM-26727 In the Operations Console, downloaded troubleshooting files related to product information provided misleading information about the software version.

AM-26742 If you rolled back a product update, the web tier failed to update and, as a result, was unavailable.

AM-26750 Jython scripts did not automatically use package-scanning functionality.

AM-26759 If an SSL-VPN was associated with the replica instance, and a user was auto-enabled for risk-based authentication, the Security Console did not show that the user was enabled for risk-based authentication when viewing risk-based authentication settings through the **Users** page.

AM-26760 After more than 24,000 authentications, an out-of-memory error did not allow an administrator to log on to the Security Console, or a user to log on to the Self-Service Console.

AM-26769 The virtual appliance logged when network time protocol (NTP) packets were sent and received. The virtual appliance no longer logs these events.

AM-26798 If you changed the browser language preferences to an invalid language or locale, the Security Console did not load.

AM-26805 Editing the RADIUS server agent host in the Security Console changed the Protect IP Address setting from **Yes** to **No**. The **Protect IP Address** setting is no longer modified when you edit the agent host associated with the RADIUS server.

AM-26807 When you configured the **TokenDTO.setPIN** API with an empty string parameter, Authentication Manager cleared the PIN instead of returning an error. Authentication Manager now returns an error in this case.

AM-26810 The filter in the Real-Time Authentication Activity Monitor is no longer case-sensitive in the **User ID** or the **Authentication Agent** fields.

AM-26813 When you updated a lockout policy with the **UpdateLockoutPolicyCommand** API, Authentication Manager did not validate the provided value for the maximum number of failed authentication attempts. Authentication Manager now validates accepted values when the lockout policy is updated with the **UpdateLockoutPolicyCommand** API. If values are set beyond the accepted range, Authentication Manager returns the expected error codes.

AM-26815 When you configured an external identity source and used a semicolon as a separator for the Distinguished Name (DN), the Operations Console reported that the **User Base DN** and **User Group Base DN** did not exist.

AM-26838 RSA updated the RSA Authentication Manager 8.0 embedded database **PostgreSQL** to mitigate known vulnerability (CVE-2013-1899).

AM-26858 Internal files that are used to replicate data from the primary instance to a replica instance may have consumed disk space and slowed performance.

AM-26872, **AM-26885** RSA updated the Syslog to prevent logging of the Operating System password and the Simple Network Management Protocol (SNMP) passwords.

AM-26873 If you disabled **LDAP Password** as a non-native authentication method in version 7.1, and you combined **LDAP_Password** with another authentication method by using the operators AND (+) or OR (/), you could not log on to the version 8.0 Security Console after performing a migration. For instructions on configuring these options, see the Security Console Help topic “Configure Security Console Authentication Methods.”

AM-26892 After importing security questions in the Security Console, the following occurred:

- Users originally enabled for risk-based authentication were disabled for risk-based authentication.
- Users originally disabled for risked based authentication were automatically disabled for on-demand authentication.
- Users originally enabled for risk-based authentication were automatically enabled for on-demand authentication.

AM-26902 Corrects a potential Java issue (CVE-2013-1537) announced by Oracle in April of 2013. This patch updates the RSA Authentication Manager's JRockit Java Runtime Environment (JRE) to the version provided with the **Oracle Java SE Critical Patch Update Advisory** for April 2013. The update is cumulative, including all previously released fixes for this JRE.

AM-26923 A backup operation was unsuccessful when backing up a database that contained 500,000 users with assigned tokens.

AM-26931 If you disabled **LDAP Password** as a non-native authentication method for the Security Console, and you use the operators AND (+) or OR (/) to combine **LDAP_Password** with another authentication method for the Self-Service Console, you could not log on to the Self-Service Console.

Support and Service

RSA SecurCare Online: *https://knowledge.rsasecurity.com*

Customer Support Information: *www.emc.com/support/rsa/index.htm*

RSA Secured Partner Solutions Directory:
https://gallery.emc.com/community/marketplace/rsa?view=overview

Copyright © 2014 EMC Corporation. All Rights Reserved. Published in the USA.

Trademarks

RSA, the RSA Logo, SecurID, and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to *www.emc.com/legal/emc-corporation-trademarks.htm#rsa*.