RSA Authentication Manager 7.1 SP4 Patch 10

December 2011
Prerequisite Release:
RSA Authentication Manager 7.1 SP4
Appliance Version 3.0.4.9 or Later

Table of Contents

Important: Before updating the Appliance with Patch 10 (Appliance version 3.0.4.20), verify that the following preconditions have been met:

1. RSA© Authentication Manager 7.1 SP4 Appliance Version 3.0.4.9 or later is installed.
2. Authentication Manager is authenticating and replicating properly. Do not install Patch 10 on a system that is currently broken.

   Note: For detailed instructions on updating the Appliance, see "Updating the Appliance" in the *RSA SecurID Appliance 3.0 Owner's Guide.*

The following Appliance versions are now being used for Appliance SP4 patches:

- 3.0.4.9: SP4 Factory Reset Image. This updates the restore image that is stored on the appliance's recovery partition. If the appliance is factory reset after installing this update, any future quicksetup will result in SP4 without patches. In order to preserve your system data, your Appliance must be running SecurID Appliance 3.0 SP4 before you install this factory reset patch. The process of installing Factory Reset Service Pack 4 on a pre-SP4 Appliance causes you to lose any existing system data on your Appliance.

  For more information, see the *RSA SecurID Appliance 3.0 Factory Reset Service Pack 4 Release Notes* on RSA SecurCare Online at https://knowledge.rsasecurity.com/scolcms/sets.aspx?product=appliance.

- 3.0.4.10: Appliance running Authentication Manager 7.1 SP4 without patches. If an appliance is factory reset after 3.0.4.9 was applied, the system will be identified as version 3.0.4.10. This is also the current shipping version for our appliance.

Note: All patches after SP4 Patch 3 will require that the system is updated to 3.0.4.9 or later. These newer patch versions are tracked by adding 3.0.4.10 to the patch number. For example, SP4 patch 8 will be identified as version 3.0.4.18 after being installed.

Previous Updates

RSA Authentication Manager 7.1 now logs all critical operations that are performed in the RSA Operations Console or through a Command Line Utility (CLU) on a primary instance.

The following Operations Console actions are logged:

- Backups (create)
- Appliance Backup/Schedule Backup (create, schedule modified)
- Restore Appliance Backup (restore)
- Replication (add, remove, attach, promote, clean demoted primary)
- Identity Sources (add, delete, update)
- Radius (promote, edit dictionary, edit configuration, delete, start, stop, trusted root certificate management, server certificate replacement)
- Appliance SSH (enable, disable)

Actions are logged for the following CLUs:

- Manage Backups (create and restore)
- Manage Secrets (change, export, import, recover)
- Store (delete_report, config, ldap_user_expiration, fixlogs, add_config, clearanswers, admin_roles, config_all, delete_report_jobs)
- Archive UCM Requests (export, import)
- Manage Replication (delete)
- Restore Administrator (restore)
- Manage SSL Certificates (import,config-server, update-server-certs)
- Manage Operations Console Administrators (create, delete, update, list)

You can use the RSA Security Console to view these logs by generating the System Activity Report, Administrator Activity Report and Authentication Activity Report. These logs provide a record of system events that can aid in security auditing or monitoring unauthorized activity.

RSA recommends that, when possible, you should make sure the Operations Console is running when you run CLUs. If the Console is not running, some logging events will not be available in reports generated by the Security Console.

Dynamically Generated Seeds for Software Tokens. During software token import, software token seeds are automatically replaced with dynamically generated seeds. The seed numbers are random rather than sequential.

Choosing Authentication Methods in the RSA Security Console. If you configure a choice between authentication methods for the RSA Security Console or the RSA Self-Service Console, users must now choose to log on with a password or a passcode, even if no tokens are assigned to their accounts. After the first logon, the authentication method used to access the Security Console or the Self-Service Console is saved in the user's browser and is the user's default on the next logon attempt.

PIN Management. The RSA Security Console now clearly states which settings will trigger new PIN mode for non-compliant users.

Password Dictionary. An editable password dictionary starter file is available in Patch 6. If you want to use the Authentication Manager 7.1 password dictionary starter file, download the dictionary.txt file from the Resources directory of the patch. For instructions, see the RSA Security Console Help topic "Add a Password Dictionary."

Master Password. The documentation for changing the master password has been improved and clarified. The updated documentation is in the *RSA Authentication Manager 7.1 Administrator's Guide*.

Token Serial Number Masking. The RSA Security Console provides a setting that allows you to configure masking for token serial numbers that appear in log messages.

^Top

Before Updating the Appliance with this Patch

Before you install Patch 10, check the following:

Important: If you have a replicated environment, all replica instances must be running when you apply the Patch to the primary or replica instances. All machines in your deployment must be able to communicate while the Patch is being applied.

- To monitor your patch installation, you will need to enable SSH in the Operations Console. To enable SSH, in the Operations Console, click Administration > Networking > Configure SSH and Operating System Connectivity, and select Enable SSH.
- If you use a localized Security Console, contact RSA Professional Services.
- If you are using cross-realm authentication with RSA Authentication Manager version 6.1 or 5.2 , you must configure a restricted port range to be used for cross-realm authentication with a firewall. Make sure the ports in the range are not blocked by the firewall.

  For example, if you want to specify a restricted port range with a minimum port number of 10000 and a maximum port number of 10011, enter the following commands from RSA_AM_HOME/utils:

  ```
  ./rsautil store -a add_config auth_manager.cross_realm.min_port 10000 Global 501
  ./rsautil store -a add_config auth_manager.cross_realm.max_port 10011 Global 501
  ```

  These commands allow the server to use the port range 10000 through 10011 for cross-realm authentication.

  Important: If you are specifying a port range for the first time, you must restart the RSA services on the Appliance after specifying the port numbers and before applying this Patch.

^Top

Configure the Appliance to Scan for Updates

You must configure the Appliance to scan for updates on a Network File System (NFS) or a USB drive. The Appliance is configured to scan a DVD by default. Installing SP4 Patch 10 from a USB drive or a DVD requires physical access to the Appliance. Installing from an NFS requires a stable network connection to avoid corrupting the Appliance during the update procedure.

To configure the Appliance for updates:

1. In the Operations Console, click Maintenance > Manage Updates > Configure Updates.
2. Specify the locations of the updates. The RSA SecurID Appliance always searches for updates on the Appliance DVD drive. You can also configure the Appliance to search for updates on the Appliance hard drive, a USB drive or an NFS. If you downloaded an ISO image, do not burn the ISO image to a DVD. Only use a DVD that has come directly from RSA. You must copy the ISO image to the Appliance hard drive, a USB drive, or NFS, and configure the Appliance to search for updates on the Appliance hard drive, USB drive, or NFS.

   Do one of the following:

   - If you want the Appliance to search for updates on a USB drive that you have connected to the Appliance, select Configure USB as a source of update. (The Appliance automatically mounts the USB drive.) Enter the directory on the USB drive where the ISO image is stored, for example, /updates.
   - If you want the Appliance to search for updates on an NFS, select Configure NFS as a source of update. Enter an IP address or hostname, and then enter the full path to the directory where the ISO image is stored, for example, /home/nfs/securid_appliance/updates.

   The Appliance does not scan subdirectories within a directory. Make sure that you store am-appliance-3.0.4.20.iso in your specified location.

3. Click Save.

Alternative Method: Download and Copy SP4 Patch 10 to the Appliance Hard Drive

If your Appliance is not physically accessible, the most reliable method for installing SP4 Patch 10 is to download the ISO file to the Appliance hard drive, ensure the MD5 checksum value of the downloaded ISO file matches the published value of the MD5 checksum, and install using the ISO file on the Appliance hard drive.

Download and Copy SP4 Patch 10 to Your Local Windows Machine.

Download SP4 Patch 10 from SecurCare Online, and verify the MD5 checksum of the `am-appliance-3.0.4.20.iso`. Copy `am-appliance-3.0.4.20.iso` to your Appliance hard drive.

To copy SP4 Patch 10 to your Appliance hard drive from a Windows machine:

1. Open an SSH connection to your Appliance.
2. Log on as emcsrv using the operating system password.
3. Switch users to root. Type:

   ```
   sudo su -
   ```

   Press ENTER.
4. Create a new directory called updates. Type:

   ```
   mkdir /updates
   ```

   Press ENTER.
5. Set read and write permissions for the new directory. Type:

   ```
   chmod 777 /updates
   ```

   Press ENTER.
6. Copy the ISO file from your Windows machine to the `/updates` directory on your Appliance using a third-party utility such as WinSCP.

Configure the Appliance to Search the Hard Disk for Updates

Use the following workaround to configure the Appliance to search the hard drive for updates.

To configure the Appliance to search the hard drive for updates:

1. In the Operations Console, click Maintenance > Manage Updates > Configure Updates.
2. Select Configure USB as a source of update. Enter the directory on the Appliance hard drive where you have copied the ISO image, for example, /updates.
   The Appliance does not scan subdirectories within a directory. Make sure that you store the ISO image in your specified location.
3. Click Save.

^Top

Appliance Update Instructions

Note: Install this patch on the primary instance first, before installing it on the replica instances.

Important: Before you install on a primary or replica instance, make sure replication is working by checking in the Operations Console. Before installing on the replica, check on the primary instance Security Console that the patch level updated to Patch 10.

To update the Appliance with Patch 10 (Appliance version 3.0.4.20):

1. Back up the database. For instructions, see "System Maintenance and Disaster Recovery" in the *RSA SecurID Appliance 3.0 Owner's Guide*.

If the backup fails, do not proceed. Contact RSA Customer Support.

2. Log on to the Operations Console.
3. Enable SSH. Click Administration > Networking > Configure SSH and Operating System Connectivity, and select Enable SSH.
4. Configure updates. Select Maintenance > Manage Update > Configure Updates.
5. Scan for updates. Select Maintenance > Manage Update > Scan For Updates.
6. Apply updates. Select Maintenance > Manage Update > Apply Updates.

   For a detailed description of updating the Appliance, see "Updating the Appliance" in the *RSA SecurID Appliance 3.0 Owner's Guide*.

During the patch installation, the Operations Console restarts. After the installation completes, you can log on to the Console.

Use the following procedure to monitor the patch installation and to ensure that it completes. These instructions also display in the Operations Console.

To determine if the installation has completed:

1. Log on to the Appliance operating system using SSH. Use the User ID emcsrv and the operating system password that you created during Appliance Quick Setup.

2. Change user to rsaadmin. Type:

   ```
   sudo su - rsaadmin
   ```

   Enter the operating system password when prompted.

3. From a command shell, change to the ApplyUpdateStatus directory. Type:

   ```
   cd /usr/local/RSASecurity/RSAAuthenticationManager/ApplianceUpdateLogs
   /ApplyUpdateStatus
   ```

4. Type:

   ```
   tail -f am---3.0.4.20---timestamp_ippi.log
   ```

   Press Enter.

   The installation is complete when the following line is displayed:

   *****update.sh: Finished Applying Update at *timestamp*

^Top

Appliance Update Rollback Instructions

Important: Only roll back an update if RSA Customer Support instructs you to do so. Rolling back an update removes the selected update (and its specified version) from your system and may make it unstable.

Note: Uninstall this patch on your replica instances before uninstalling it on the primary instance.

To roll back Patch 10 (Appliance version 3.0.4.20):

1. Log on to the Operations Console and roll back the Appliance to the previous Patch, as described below:
2. Enable SSH. Click Administration > Networking > Configure SSH and Operating System Connectivity, and select Enable SSH.
3. Select: Maintenance > Manage Rollback > Execute Rollback
4. Under Version 3.0.4.20 select Roll Back This Update.

   For a more detailed description of updating the Appliance, see the *RSA SecurID Appliance 3.0 Owner's Guide* (Chapter 11, Section: Rolling Back an Update)

To determine if the rollback has completed, execute the following commands to tail the most recent log file from the console:

1. Log on to the Appliance operating system using SSH. Use the User ID `emcsrv` and the operating system password that you created during Quick Setup of the Appliance.
2. Change users to rsaadmin. Type:

   ```
   sudo su - rsaadmin
   ```

   and enter the operating system password when required.

3. From a command shell, change to the `PerformRollbackStatus` directory. Type:

   ```
   cd /usr/local/RSASecurity/RSAAuthenticationManager/ApplianceUpdateLogs
   /PerformRollbackStatus
   ```

4. Type:

   ```
   ls -lt
   ```

   Press Enter.

5. Type:

   `tail -f am---`*`version rolling back to`*`---`*`timestamp`*`.log`

   Press Enter.

   The rollback is complete when the following line is displayed:

   ***** rollback.sh: Finished Rolling Back Update at *timestamp* *****

^Top

Masking Token Serial Numbers Displayed in Log Messages

This patch allows you to mask token serial numbers in log data. This capability ensures that any log data sent in the clear over a non-secured network, or is saved to a local file, adheres to RSA Authentication Manager Best Practices. You configure how many token serial number digits to display in the log message.

The patch applies to log data that is saved to a local file or is sent over the network using the following methods:

- Syslog for UNIX
- Syslog for Windows
- SNMP to an external file store
- Network Monitoring system (NMS)
- Security Information and Event Management (SIEM) solution

This document also describes how to configure RSA Authentication Manager to send log messages to a Syslog and a local file. For instructions on setting up SNMP with Authentication Manager and for detailed information about the types of logs you can use, see the *RSA Authentication Manager 7.1 Administrator's Guide*.

`Note`: After you enable SSH, Secure File Transfer Protocol (SFTP) and Open SSL will allow Authentication Manager to securely send log messages to other applications, such as Envision. For instructions on enabling SSH, see the *RSA SecurID Appliance 3.0 Owner's Guide*.

When you mask the token serial number, the masked digits display as x's. The masked digits are always at the beginning of the serial number, while the exposed digits are always at the end.

For example, if you mask the first 4 digits, the number displays as follows:

```
xxxx48697056
```

`Note`: Any object with a name that has exactly 12 numeric digits, such as trusted realm name, trusted realm active group name, or agent name for auto registration, will also be masked when you mask the token serial number. This does not affect object names that have fewer than or greater than 12 digits. The Authentication Activity Monitor and the Authentication Activity report are

not affected.

Procedure

To set the number of digits that you want to display in log messages, perform these steps:

Note: If you configured this setting prior to Patch 10, your change will be retained when you install Patch 10. In addition, you can now view and update the Token Serial Number Masking setting in the RSA Security Console. If you previously configured a value outside the acceptable range (0..12), you will be required to change the value the next time you change the Authentication Manager Basic Settings in the Security Console.

1. Log on to the Security Console.
2. Navigate to the Authentication Manager Basic Settings configuration page:
   Setup > Component Configuration > Authentication Manager > Basic Settings
3. On this page, find the section titled Token Serial Number Masking for Logs.
4. Enter the number of token serial number digits to display in log messages in the text box labeled Number of digits of the token serial number to display.
5. Click the Save button.

Configure Syslog for RSA Authentication Manager in an Appliance Environment

This section describes how to configure RSA Authentication Manager to send log messages to a local Syslog server in an Appliance environment.

Before You Begin

The default port is 514/UDP for sending and receiving log messages.

Procedure

To configure Syslog in an Appliance environment, perform these steps on the primary and replica instances:

1. Configure Authentication Manager to send log messages to a local or remote Syslog server.
   Using a text editor, open the RSA_AM_HOME/utils/resources/ims.properties file for editing.
2. Replace the values shown in italics. The Syslog server name can be a local or remote host name or IP address.

   ```
   ims.logging.audit.admin.syslog_host = host_name
   ims.logging.audit.admin.syslog_layout = %d, %X{clientIP}, %c, %p, %m%n
   ims.logging.audit.admin.syslog_facility = 8
   ims.logging.audit.admin.use_os_logger = false
   ims.logging.audit.runtime.syslog_host = host_name
   ims.logging.audit.runtime.syslog_layout = %d, %X{clientIP},%c, %p, %m%n
   ims.logging.audit.runtime.syslog_facility = 8
   ims.logging.audit.runtime.use_os_logger = false
   ims.logging.system.syslog_host = host_name
   ims.logging.system.syslog_layout = %d, %X{clientIP},%c, %p, %m%n
   ims.logging.system.syslog_facility = 8
   ims.logging.system.use_os_logger = false
   ```

   Where:
   host_name is the Syslog server name.

3. Change *false* to true to enable logging.
4. Save the file.
5. Open a new command prompt, and type (as root):

   ```
   touch /var/adm/rsa.log
   ```

   Note: Make sure that the owner of the rsa.log file is also the owner of RSA Authentication Manager.

To configure the Syslog server to write log messages to a file from RSA Authentication Manager:

1. At the Syslog server host, open the /etc/syslog.conf file for editing.

2. At the bottom of the file, add the following text:

   ```
   # RSA Authentication Manager 7.1 log
   user.* /var/log/rsa.log
   ```

3. Save the file.

To configure the syslog daemon to receive logs from user processes:

1. Open the /etc/sysconfig/syslog file for editing.
2. Locate SYSLOGD_OPTION and add the "-r" option, as follows:

   ```
   SYSLOGD_OPTIONS="-m 0 -r"
   ```

3. Save the file.
4. Restart the Syslog daemon using the following command:

   ```
   /etc/init.d/syslog restart
   ```

To configure the logging levels:

1. Log on to the RSA Security Console on the primary instance.
2. Click Setup > Instances.
3. Select the name of the instance for which you want to configure event logging.
4. From the Context menu, click Logging.
5. Specify the logging levels. For information on each log level, see the Security Console Help topic "Configure Logging."
6. To ensure that all log messages are written to the system log, make sure the option Send system messages to OS system log is checked.
7. Click Save.

Configure Authentication Manager to Send Log Messages to a Local File

This section describes how to configure Authentication Manager to send log messages to a local file.

Before You Begin

Local log files are kept in the following locations:

- Admin: RSA_AM_HOME/server/logs/imsAdminAudit.log
- Authentication: RSA_AM_HOME/server/logs/imsRuntimeAudit.log
- System: RSA_AM_HOME/server/logs/imsSystem.log

These locations cannot be changed.

Use the store CLU to perform this configuration. The general usage for store is as follows:

To make the change for all of the instances (primary and replicas):

```
./rsautil store -a config_all name value
```

Where:
name is the entry to be changed
value is the value to be set

To make the change for only one instance (primary for example):

```
./rsautil store -a config name value instance_name
```

To obtain the exact *instance_name*, log on to the Security Console and click Setup > Instances.

Procedures

To configure all instances in your deployment to send log messages to a local file:

1. Log on to the primary instance.
2. Enter one of the following commands from RSA_AM_HOME/utils:

   For the admin log:

   ```
   ./rsautil store -a config_all ims.logging.audit.admin.datastore database,file
   ```

   For the runtime log:

   ```
   ./rsautil store -a config_all ims.logging.audit.runtime.datastore database,file
   ```

   For the system log:

   ```
   ./rsautil store -a config_all ims.logging.system.datastore database,file
   ```

3. When prompted, enter the master password, and press ENTER.

To configure one instance to send log messages to a local file:

1. Log on to the primary instance.
2. Enter one of the following commands from RSA_AM_HOME/utils:

   For the admin log:

   ```
   ./rsautil store -a config ims.logging.audit.admin.datastore database,file instance_name
   ```

   Where *instance_name* is the name of the primary instance or replica instance.

   For the runtime log:

   ```
   ./rsautil store -a config ims.logging.audit.runtime.datastore database,file instance_name
   ```

   Where *instance_name* is the name of the primary instance or replica instance.

   For the system log:

   ```
   ./rsautil store -a config ims.logging.system.datastore database,file instance_name
   ```

   Where *instance_name* is the name of the primary instance or replica instance.

3. When prompted, enter the master password, and press ENTER.

Set the Maximum Number of Local Log Files

You can use the store utility to determine how many local log files are saved. After the maximum is reached, the oldest file(s) are automatically deleted. You change the maximum backup file index to set this limit. The default is 100 files.

Procedure

To set the maximum number of local log files:

1. Log on to the primary instance.
2. Do the following:
   a. For the admin log, enter the following command :
      ```
      ./rsautil store -a config ims.logging.audit.admin.file.max_backup_index n instance_name
      ```

      Where *n* is the maximum number of local log files and *instance_name* is the name of the primary instance or replica instance.

      For example:

      ```
      ./rsautil store -a config ims.logging.audit.admin.file.max_backup_index 50 instance1
      ```

   b. For the runtime log enter the following command:
      ```
      ./rsautil store -a config ims.logging.audit.runtime.file.max_backup_index n instance_name
      ```

      Where *n* is the maximum number of local log files and *instance_name* is the name of the primary instance or replica

instance.

For example:

```
./rsautil store -a config ims.logging.audit.runtime.file.max_backup_index 50 instance1
```

c. For the system log, enter the following command:

```
./rsautil store -a config ims.logging.system.file.max_backup_index n instance_name
```

Where *n* is the maximum number of local log files and *instance_name* is the name of the primary instance or replica instance.

If you want to change the setting for all of the instances, use the config_all option instead of config and omit the *instance_name*.

For example, to change the setting for System Log:

```
./rsautil store -a config_all ims.logging.system.file.max_backup_index 5
```

Set the Maximum Size of Each Local Log file

The default size of a local log file is 10 MB.To change the maximum file size:

1. Log on to the primary instance.
2. Do the following:
   a. For the runtime log, enter the following command:

```
./rsautil store -a config ims.logging.audit.runtime.file.rotation_size n instance_name
```

Where *n* is the maximum size in MB of the local log files and *instance_name* is the instance name.

For example:

```
./rsautil store -a config ims.logging.audit.runtime.file.rotation_size 5 instance1
```

   b. For the administrative log, enter the following command:

```
./rsautil store -a config ims.logging.audit.admin.file.rotation_size n instance_name
```

Where *n* is the maximum size in MB of the local log files and *instance_name* is the instance name.

For example:

```
./rsautil store -a config ims.logging.audit.admin.file.rotation_size 5 instance1
```

   c. For the system log, enter the following command:

```
./rsautil store -a config ims.logging.system.file.rotation_size n instance_name
```

Where *n* is the maximum size in MB of the local log files and *instance_name* is the instance name.

For example:

```
./rsautil store -a config ims.logging.system.file.rotation_size 5 instance1
```

If you want to change the setting for all of the instances, use the config_all option instead of config and omit the *instance_name*. For example, to change the setting for System Log:

```
./rsautil store -a config_all ims.logging.system.file.rotation_size 5
```

^Top

Known Issues

AM-19941 The replica instance is attached to the primary instance and is replicating, but you cannot log on to the Security Console or use any Operations Console functions that require Security Console credentials. When this happens, a message similar to the following appears in the RSA Authentication Manager server log:

"Exception Unable to create archive log policy entry offline file path: ..."

This problem occurs because the primary instance has a default archive log folder that is also set on the replica instance during installation or startup. If the primary instance uses an archive log folder other than the default, the replica instance prevents you from logging on to the Security Console.

To work around this problem, if you specify a non-default folder on the primary instance for the archive log, you must manually create the same non-default folder on the Replica either before or after you install or start up the replica instance. If you create this folder after installation or start up, you must restart RSA Authentication Manager services before the change will take effect.

AM-21487 and AM-21984: These two issues are fixed in this patch, but you must apply the patch to all primary and replica instances and then detach and reattach all replica instance to implement the fix. If you do not want to disrupt your authentication service, contact RSA Customer Support for a fix you can apply to a running system.

AM-21969 When you run the rsautil store command to configure masking for token serial numbers, you must allow some time for the command to take effect. If you want masking to be active immediately, restart the Authentication Manager server.

AM-21975 After you configure masking for token serial numbers, any object with a name that has exactly 12 numeric digits, such as trusted realm name, trusted realm active group name, and agent name for auto registration, will also be masked when you mask the token serial number. This does not affect object names that have fewer than or greater than 12 digits. The Authentication Activity Monitor and all reports are not affected by masking.

AM-22106 On the SecurID Token Policy page, the following information does not display beside the Maximum Lifetime settings, "Changing this setting will cause the system to prompt users for a new PIN, if their current PIN's lifetime exceeds the new maximum lifetime." Before you change the Maximum Lifetime setting, be aware of this information.

AM-22962 Since SP4 Patch 9, in the RSA Security Console, search filters do not work when you perform an advanced user search.

^Top

Defects Fixed In This Patch

7.1 SP4 P10

AM-21996 Self-service enrollment approval for active directory users failed if you used .NET with the Authentication Manager Software Development Kit (SDK).

AM-21997 When a user answered security questions to enroll in self-service, the user displayed as unenrolled in the SDK.

AM-22433 Two new command API's were added to support RSA Professional Services Kerberos integration.

For more information, see the *RSA Authentication Manager 7.1.4.10 Software Development Kit (SDK))*.

AM-22471 If you had multiple patch versions available in the patch installer, the following message displayed when you selected to update to the highest numbered version:

"It is recommended that you update from the lowest version to the highest one. Do you want to continue?"

AM-22532 In the RSA Security Console, the "Agents with Un-assigned IP Address" report failed to run if the "auto-registration date" field was empty. The report now handles empty values properly.

AM-22629 In the RSA Security Console on the "Assigned SecurID Tokens" page, when a user had a phone number with an incorrect country code or format, the phone number did not display.

AM-22741 In an environment with cross-realm trust between an Authentication Manager 7.1 realm and one or more Authentication Manager 6.1 realms, user authentications timed out if AM 6.1 users authenticated to AM 7.1. This occurred if a user's realm was not reachable.

AM-22764 There was no way to track, list or delete read-only database users. For security purposes, two new scripts were added for listing and deleting read-only database users created for reporting.

1. list_readonly_users.sql : This script lists all the existing read-only database users. You can run this script with the manage-

database CLU using the following command:

./rsautil manage-database -a exec-sql -f diagnostics/list_readonly_users.sql

2. drop_readonly_user.sql : This script will delete a given user. You can run this script with the manage-database CLU using the following command:

   ./rsautil manage-database -U com.rsa.db.root -a exec-sql -f diagnostics/drop_readonly_user.sql -A *username*"

For more information on managing read-only database users, see the *RSA Authentication Manager 7.1.4.10 Software Development Kit (SDK)*.

AM-22800 The SDK API LoginCommand supports case sensitive PIN's. If you used the SDK API LoginCommand to handle passcode authentication, user authentication requests failed if they entered their PIN's with the incorrect case.

7.1 SP4 P9

AM-21984 In the RSA Operations Console, if users authenticated through an EAP32 client, and if a user's authentication requests were sent to the replica instance but then the user was deleted from the primary instance, replication broke and the replication status displayed "needs action".

Note: To complete this fix you must apply the patch to all primary and replica instances and then detach and reattach all replica instances. If you do not want to disrupt your authentication service, contact RSA Customer Support for a fix that you can apply to a running system.

AM-22376 If you promoted a replica instance and reattached the demoted primary instance, some jobs scheduled on the primary instance before demotion continued to run on that instance.

AM-22452 In the RSA Security Console, for some Active Directory configurations, the following error displayed when you searched for user groups mapped to the top level of Active Directory:

"System Internal Error"

AM-22519 Administrators scoped to a security subdomain could not run activity reports.

AM-22577 During a patch installation, if replication was down between the primary instance and a replica instance, the installation failed, but the patch_install log did not display which replica instance could not be reached. The patch_install log now displays the replica instance that it failed to connect to when the installation fails.

AM-22578 During a patch installation, if database services were down, the patch installation failed and an error message was logged, but did not say that database services needed to be running. Now, the following message is logged when primary services are down during a patch installation:

"Install, com.installshield.rsa.ippi.install.actions.wizard.CollectPrimaryInstanceName, err, Collecting replication information failed. Please verify that database services are running. Io exception: The Network Adapter could not establish the connection."

AM-22582 Users with a Bhutan country code (+975) in their phone numbers displayed the wrong country code when you enabled them for on-demand authentication.

AM-22583 In the RSA Security Console, when you enabled users with the Mongolia country code (+976) for on-demand authentication, the following error displayed when you tested the user's country code and phone number:

"Cannot determine the country code. Please select a country code from the list and then enter a valid phone number."

AM-22584 In the RSA Security Console, after you set up on-demand authentication for a user and sent a test text message to the user's cell phone, the test message would not be sent if the phone number included the country code.

AM-22628 If you navigated to a page in the RSA Security Console that lists some domain objects, the system occasionally becomes unresponsive and displays the following error:

"503--service unavailable."

7.1 SP4 P8

AM-13166 In the RSA Security Console, if you mapped an identity source attribute with a dash (-) in its name to an identity source, then the definition failed and the following error displayed:

“Invalid input data. Validation failed for Identity Source Mappings. Identity Source Mappings is not valid.”

AM-22067 If a user had membership in two groups and used the same logon alias for both groups, had access to a restricted agent, and authenticated to the restricted agent using their logon alias, then authentication failed.

AM-22117 In the RSA Security Console, if you assigned RADIUS attributes with values mapped from an external identity source to a user, the same attributes were sometimes removed from other users who had them assigned previously.

AM-22201 If one user used a logon alias to access a restricted group agent, and another user's userid matched the logon alias, when the first user authenticated with their logon alias on the restricted group agent the authentication failed and the following error displayed in the system activity report:

"Principal does not belong to any groups activated on restricted agent"

AM-22226 The patch installer failed to identify a promoted replica instance as a primary instance.

AM-22234 If you added a country code and phone number to a user without a space between them and tried to enable the user to receive on-demand tokencodes, then Authentication Manager 7.1 failed to read the country code. Authentication Manager can now parse country codes from phone numbers
without including a space between them. If an incorrect or unlisted country code precedes a phone number, then the following message will display when you try to enable the user for on-demand tokencodes:

"Cannot determine the country code.
Please select a country code from the list and then enter a valid phone number."

AM-22437 On the RSA Security Console, a column title on the Offline Authentication Policies page was incorrect.

AM-22454 Offline authentication data failed to upload when there were users with duplicate userid's in different identity sources.

AM-22482 If a user authenticated offline to a disconnected agent, but the user was deleted from the internal database, then the offline authentication data failed to upload when connection to the agent was restored.

AM-22492 If there were corrupted dates in the Offline Authentication Data, then the offline authentication data failed to upload when connection to the agent was restored.

AM-22501 When you ran the patch installer, the following image would sometimes display:

"The InstallShield Wizard has successfully installed RSA Patch Installer. Choose Finish to exit the wizard.
The automated sql scripts failed to complete successfully. Exit code: 49" (or Exit code: 11)

This error no longer displays.

AM-22503 The patch install log displayed errors with no impact.

AM-22516 When resynchronizing the primary and replica instances, if replication failed, then the following error displayed in the replication error report:

“ORA-02291: integrity constraint (RSA_REP.FK_AM_HOST_ID_AGENT) violated – parent key not found”

AM-22520 The patch installer allowed you to apply a patch to the wrong version of RSA Authentication Manager. You must have RSA Authentication Manager 7.1 SP4 installed before installing any patches.

7.1 SP4 P7

AM-17414 WebLogic case sensitive URL-pattern matching property is not set. RSA has addressed this issue.

AM-20186 In the RSA Security Console, the "Software Token Deployed on Device" report failed to complete. In the system activity log, the following error displayed:

"Execute batch job Failure
Administrator "admin attempted to execute batch job "":""

UNEXPECTED_EXCEPTION"

AM-22069 In the RSA Security Console, if you configured the Clickatell plug-in with a proxy server and you had not sent an on-demand tokencode in over an hour, the server failed the next time it sent an on-demand tokencode to a phone. The following message appeared in the system log:

"ERROR TRANSMIT_TXT_MSG_SMS.message Failure"

AM-22169 When you restored a backup from a system with SP4 Patch 4 or lower to a replica instance with SP4 Patch 5 or SP4 Patch 6, and then promoted the replica instance, the following message displayed at the top of the Authentication Manager Settings page in the RSA Security Console:

“Cannot load data for Token Serial Number Masking from the database.”

AM-22200 If two users with the same logon name, one using samaccountname as their logon name and the other using a UPN name as their logon name, authenticate using the same agent, and the "Send Domain and User Name to RSA Authentication Manager" checkbox is selected, then the samaccountname user's authentication will fail since the agent will send the default domain name. In this case, NTLM names can now be mapped so the domain name is dropped when the agent sends it. In the RSA Security Console, the administrator needs to define a domain name mapping where the NTLM name maps to the UPN name RSAOMIT.

To configure domain name mapping:

1. In the RSA Security Console, click > Component Configurations > Authentication Manager > Basic Settings.
2. In the NTLM Name field, enter an NTLM domain name.
3. In the UPN Name field, enter a UPN name that you want to map to.
4. Click Add.
5. Click Save.

AM-22255 When resynchronizing the primary and replica instances, if replication failed, then the following error displayed in the replication error report:

“ORA-01460: unimplemented or unreasonable conversion requested”

AM-22259 In the RSA Security Console, bulk provisioning requests were not approved if any of the requests failed, but approval e-mails still went out for processed user provisioning requests. Multiple approval e-mails were sent when you reapproved the provisioning requests.

AM-22264 A system configured to deliver SMS on-demand tokencodes using the HTTP plugin worked properly if the server returned the HTTP response 200 "OK", but failed to recognize response 202 "Accept". If the system did not recognize 202 "Accept" as a successful HTTP response, then the following message displayed on the On-Demand Tokencode Delivery page in the RSA Security Console:

“An error occurred while sending the test message. Please check your configuration and try again."

“An error occurred while sending the test message. Please check your configuration and try again."

AM-22440 Some authentication activity log errors could not be investigated because of insufficient logging information. Logging information was expanded to include the specific agent host or user id when an error occurs while importing offline authentication data.

7.1 SP4 P6

AM-22115 In the RSA Security Console, the RADIUS server took a long time to display on a replica instance when the primary instance was down.

AM-22238 A user whose account is stored in Active Directory logged on to the RSA Self Service Console, and the following message displayed:

“There was a problem processing your request. Please contact your system administrator!”

The message occurred because one of the user's core attributes, such as “initials,” contained a space in an empty field.

AM-22254 If the nodemanager.properties file was not properly updated during SP4 installation, it appeared to use a weak cipher suite at port 5556 during a security scan.

AM-22301 If the same User ID was stored in two Active Directory identity sources and each identity source had the same User BaseDN and Group Base DN, but the User ID was mapped to two different attributes, then incorrect user profile information displayed when the user logged on to the RSA Self-Service Console.

AM-22303 In the RSA Security Console, if an Active Directory user made a provisioning request, and the text case of the user's User ID was updated before the request was approved, the following message displayed when you approved the provisioning request:

"User IDs must be unique within an identity source."

AM-22332 If you restored a backup taken before you applied SP4 Patch 2 to a system with SP4 Patch 2 through Patch 5 installed, the system failed when you imported software tokens using CT-KIP, and the following message displayed:

"Token import failed. Verify the activation code or contact your administrator."

7.1 SP4 P5

AM-19929 In the RSA Security Console, if you ran the "List all users with assigned RADIUS profile" report, the report displayed the security domain from each user's RADIUS profile instead of listing each user's security domain.

AM-20233 In the RSA Security Console, you were able to view and edit the PrincipalRuntimeCache. The PrincipalRuntimeCache is used internally and should not display.

AM-20711 In the RSA Security Console, if you edited the "account information" section for a user from a read-only external identity source, and the user's record contained trailing spaces in fields in the "User Basics" section, a message displayed indicating that the LDAP identity source was read-only.

AM-20914 If you created a custom identity attribute that was optional and listed one predefined value, then the default option "-unspecified-" was not available when you edited users.

AM-21604 When you downloaded a completed report in .csv format and opened it with Microsoft Excel, unknown characters displayed in place of quotation marks.

AM-21912 Administrators with permission to manage users and user identity attributes were not able to view or edit identity attribute values if their administrative scope was limited to a subdomain.

AM-22052 In the RSA Operations Console, version verification results did not display when installing an Appliance patch.

AM-22057 If the country code for Nigeria was configured as the default country code for on-demand tokencodes delivered by SMS, the country code for Nigeria did not automatically display when enabling users for on-demand tokencodes.

AM-22102 The monitoring mechanism used to restart Oracle's propagation process caused Oracle jobs to back up and never complete.

AM-22125 If the RSA Security Console was configured to automatically delete replaced software tokens, replication failed after both of the following events occurred:

- A software replacement token with attributes was used to authenticate through a replica instance while the primary instance was temporarily offline.
- The same software token with attributes was then used to authenticate through the primary instance while a replica instance was temporarily offline.

AM-22133 If you cancelled a patch installation, the software version information updated even though the patch was not successfully installed.

AM-22189 In the RSA Operations Console, you were able to install a patch on the Appliance if the running software version was not the correct version.

7.1 SP4 P4

AM-18173 In the RSA Security Console, when you ran the "Users with Tokens" report, the output files displayed duplicate rows of user data.

AM-18768 Administrators assigned the permission "May import and manage smart card details including PIN unlocking key" were not able to view the PIN unlocking key (PUK) without the super administrator role. Now, all administrator roles with the "May import and manage smart card details including PIN unlocking key" permission can view and edit SID-800 Smart Card details, including the PUK.

AM-19855 If you migrated from RSA Authentication Manager 6.1 to RSA Authentication Manager 7.1, RADIUS user profiles were assigned to a subdomain and the migration failed.

AM-21218 When you set your Offline Authentication Policy to download offline authentication data, and you configured a realm to use PINless tokens, offline data failed to download.

AM-21443 If an administrator's account was removed from an LDAP identity source after the administrator approved or rejected a user's provisioning request, the user who made the request received a "System Internal Error" when attempting to log on to the Self-Service Console. Any administrator who tried to view the details of this request also received a "System Internal Error." This problem no longer occurs.

AM-21487 Replication failed between an RSA Authentication Manager replica instance and an RSA Authentication Manager primary instance if a user who was provisioned with a software token was later issued a replacement software token and the first authentication with that new token occurred on the replica instance. If the administrator had selected "Automatically delete replaced tokens", then the actions to replace and delete the token during authentication caused replication to fail. This scenario no longer causes replication to fail.

Note: To complete this fix you must apply the patch to all primary and replica instances and then detach and reattach all replica instances. If you do not want to disrupt your authentication service, contact RSA Customer Support for a fix you can apply to a running system.

AM-21836 When administrators scoped to security subdomains selected "Search for users across all identity sources", the Security Console failed to display users.

AM-21916 When you replaced a hardware token containing a numeric PIN with a software token, the PIN did not migrate and the software token was in New PIN mode.

AM-21945 If you used a Sun Java Directory Server as an external identity source and configured its schema with any user defined attribute, the following error displayed in the System Activity Monitor when you searched for a user in this identity source:

"There was a problem processing your request. A system error has occurred"

This error no longer displays.

AM-21970 The Taiwan Country Code was missing from the Self-Service Console's SMS country list. It is now included in the list.

7.1 SP4 P3

AM-21598 If you added a new RADIUS user attribute to a user's authentication settings, it overwrote previously assigned RADIUS user attributes of the same type. Now, when you reconfigure a user attribute definition as multivalued in the internal database, you can create and edit multiple instances of the same RADIUS user attribute with different values. If you add multiple values for a RADIUS user attribute that has not been redefined as multivalue, the following error message will display:

"There was a problem processing your request. Multiple values were specified for an attribute which is not defined as multi-valued."

AM-21956 Previously, when you edited the RSA_AM_HOME/utils/resources/ims.properties file, a trailing space at the end of a value, this prevented some CLU's, such as rsautil store, from running. Trailing spaces no longer cause CLU's to fail.

7.1 SP4 P2

AM-18755 If a Self-Service Console user clicks Get an On-Demand Tokencode to request an on-demand tokencode, cancels the request, and clicks Get an On-Demand Tokencode again, the user will not be redirected to the Security Console logon page.

AM-20566 When you enter an invalid custom attribute for a user on the Edit User page of the Security Console, the following

error message displays:

"Invalid input data. The following characters are not allowed < > % &"

AM-20640 After you promote a replica instance, update the CT-KIP Token Key Generation URL in the Security Console to reflect the new primary instance, and distribute software tokens to users, the following error message no longer displays when users import software tokens from the web:

"Token import failed. Verify the activation code or contact your administrator"

AM-21088 Authentication Manager backups stored on a remote Network File Server (NFS) no longer create hidden files when you exceed the maximum number of backups configured in the Operations Console. Now, you must remove the configuration for the NFS portion, remove the scheduled job, and execute a single backup. Once complete, you can create the NFS directory path and enable the scheduled job.

AM-21266 When a user successfully changes his or her password on the Security Console, the Authentication Activity Monitor and System Log Report no longer fail to log a successful authentication event.

AM-21378 When you disable a user account that uses Active Directory in read/write mode as its identity source, and Directory is the user's enabled state, the following error message no longer displays:

"A directory-naming exception error occurred. Possible causes include an invalid character entry, incorrect identity source mapping, or invalid attribute definition mapping. Check the system log for more details"

AM-21566 When you import a wildcard SSL certificate for an SMS provider using the SP4 HTTP plug-in for on-demand tokencode delivery, the following error message no longer displays:

"SSL connection not verified with peer. Please check that the certificate you imported is valid for the configured SMS provider."

AM-21625 Administrators without proper permissions can no longer overwrite user RADIUS profile assignments. Administrators with view-only permission can see user RADIUS profile assignments but not change them. Administrators without view permission cannot see them.

7.1 SP4 P1

AM-16413 The Security Console no longer displays the error: "Error 503--Service Unavailable" when you log in or perform other Security Console functions.

AM-16578 You are no longer forced to change your password in the normal Self-Service Console or Security Console login process after trying and failing to reset your password on the Self-Service Console.

AM-16792 Once you have entered all required information in the Mail Server (SMTP) tab of the Instance Configuration page in the Security Console, you can now click the Test Connection button and have the test run successfully without having to click the Save button first.

AM-17325 A warning pop-up message has been added to the Security Console flow for issuing new software tokens for some users to help prevent you from accidentally re-issuing software tokens for existing users, thus invalidating their current tokens.

AM-17715 When creating a backup via the Operations Console, and the backup filename has ORA- or SP2- as part of it, the error message 'com.rsa.tools.common.OracleException' is no longer displayed.

AM-17808 Excessive database log messages are no longer written to the Windows Application Event log or, on Linux and Solaris, to the following location: RSA_AM_HOME/db/admin/<instance_name>/adump/

AM-17993 If your RSA Authentication Agent uses a hostname that does not contain a period (.) character, you can now get updated dayfiles on that system with a refresh operation by providing proof of a previous authentication on that system.

AM-18229 If you lose your token, you can now authenticate successfully from the EAP client using emergency access tokencodes.

AM-18307 The following procedure allows you to change the number of characters in an online emergency access tokencode.

The following example illustrates how to change the number of characters. The valid tokencode length is from 4 through 8.

1. Open a command window, and change directories to RSA_AM_HOME/utils.
2. Type:

```
./rsautil store -a add_configauth_manager.emergency_access.tokencode_size
<number of characters> Global 501
```

3. Press ENTER.
4. When prompted, enter the master password and press ENTER.

Note: To modify the number of characters again for the online emergency access tokencode, type:

```
./rsautil store -a config auth_manager.emergency_access.tokencode_size
<number of characters> Global 501
```

AM-18701 When you run the CLU "import-bulk-request" to request tokens, the console output now displays the location of the file containing the PINs and passwords.

AM-19453 Replication no longer fails when you update the AM_TOKEN_OTT database table.

AM-19532 The option to configure On Demand Token Authentication for a user has been removed from the Security Console interface as the option is not supported.

AM-19539 You can now send SMS messages successfully using Clickatell because RSA Authentication Manager can now handle malformed responses from Clickatell.

AM-19637 When the number of users associated with a RADIUS profile is greater than the number of users that can be shown on the RADIUS Profile Associated Users page in the Security Console, the "Next" and "2" links on that page now work properly and display the next page of users.

AM-20131 The "Workstation Unlock With RSA SecurID PIN" feature in RSA Authentication Agents 7.0.x now works correctly, allowing the user to unlock the workstation using only the PIN, within the pre-configured timeframe.

AM-20427 The default legacy cross-realm authentication no longer requires that an agent exist on both the local and remote realms, as it did after SP3 HF4.

AM-20714 When a token is not in next tokencode mode,and a one-time tokencode is issued, the one-time tokencode flag is no longer set (prompting the user for another tokencode) when the user's attempted login fails three times.

AM-20800 Configuring RADIUS on RSA SecurID Appliances and Linux platform installations will now complete successfully in cases where the original failure was due to a large,unparsable DNS message.

AM-20849 The conflict handler for table AM_HOST now logs all errors so that you know whenever a conflict cannot be resolved in this table.

AM-20934 When configuring a RADIUS replica, you no longer see the erroneous message 'Unable to contact Primary RADIUS Server'.

AM-21086 Kill scripts are now executed properly to stop the RSA Services on the Appliance during a system shutdown or reboot.

^Top

Support and Service

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

Customer Support Information: www.rsa.com/support

RSA Secured Partner Solutions Directory: www.rsasecured.com

^Top

Trademarks

^Top