RSA Authentication Manager 7.1 SP4 Patch 4

June 2011
Prerequisite Release and Build Number:
RSA Authentication Manager 7.1 SP4
Appliance Version 3.0.4.9 or 3.0.4.10

Table of Contents

Important: Before updating the Appliance with Patch 4 (Appliance version 3.0.4.14), verify that the following preconditions have been met:

1. RSA Authentication Manager 7.1 SP4 Appliance Version 3.0.4.9 or 3.0.4.10 is installed.
2. Authentication Manager is authenticating and replicating properly. Do not install Patch 4 on a system that is currently broken.
3. Verify the SHA1SUM of am-appliance-3.0.4.14.iso is

   2b9795367125e28a0abc919ac920022f5f09bea9

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

What's New in this Patch Release

The prerequisite version for Appliance SP4 Patch 4 [3.0.4.14] is version 3.0.4.9 or 3.0.4.10.

The following version numbers are now being used for Appliance SP4 patches:

- 3.0.4.9: SP4 Factory Reset Image. This does not include any of the previous patches, nor does it remove any previously applied patches. There are 4 different update versions based upon the 4 models of the appliance: r200, r210, 2950 and r710.
- 3.0.4.10:
  - SP4 Full Kit that is shipped with new appliances. This does not include any SP4 patches.
  - Appliance that was factory reset after applying the Factory Reset Image [3.0.4.9]. This does not include

any SP4 patches.

- 3.0.4.14: SP4 Patch 4. The prerequisite version for SP4 Patch 4 [3.0.4.14] is version 3.0.4.9 or 3.0.4.10.

The Factory Reset Service Pack 4 [3.0.4.9] updates your factory reset partition with all of the updates that are delivered in the RSA SecurID Appliance 3.0 Service Pack 3 (SP3) and RSA SecurID Appliance 3.0 Service Pack 4 (SP4). 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.

^Top

Before Updating the Appliance with this Patch

- 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.
- 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 4 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-3.0.4.14.iso** in your specified location.

3. Click **Save**.

Alternative Method: Download and Copy SP4 Patch 4 to the Appliance Hard Drive

If your Appliance is not physically accessible, the most reliable method for installing SP4 Patch 4 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 4 to Your Local Windows Machine.

Download SP4 Patch 4 from SecurCare Online, and verify the MD5 checksum of the **am-appliance-3.0.4.14.iso**. Copy **am-appliance-3.0.4.14.iso** to your Appliance hard drive.

To copy SP4 Patch 4 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.

To update the Appliance with Patch 4 (Appliance version 3.0.4.14):

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 and update the Appliance
3. Configure updates. Select **Maintenance** > **Manage Update** > **Configure Updates**.
4. Scan for updates. Select **Maintenance > Manage Update** > **Scan For Updates**.
5. 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*.

To determine if the installation 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 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:

   ```
   ls -lt
   ```

   Press Enter.

5. Type:

   ```
   tail -f am---3.0.4.14---timestamp.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 4 (Appliance version 3.0.4.14):

1. Log on to the Operations Console and roll back the Appliance to the previous Patch, as described below:
2. Select: **Maintenance** > **Manage Rollback** > **Execute Rollback**
3. Under Version 3.0.4.14 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 hotfix 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 hotfix 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:

1. Log on to the primary instance.
2. Do one of the following:
    - The first time you set the number of digits to display, enter this command from **RSA_AM_HOME/utils**:

      ```
      ./rsautil store -a add_config auth_manager.token_serial_number.digits_shown n Global 501
      ```

      where *n* is the number of digits you want to display.

    - After the first time you have run the command, enter this command to change the setting:

      ```
      ./rsautil store -a config auth_manager.token_serial_number.digits_shown n Global 501
      ```

      where *n* is the number of digits you want to display.

3. When prompted, enter the master password, and press ENTER.
4. If you want the changes to take effect immediately, you can restart RSA Authentication Manager. Otherwise, a restart is not necessary.

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.

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-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-22052 The Appliance Operations Console function: "Scan for Updates" allows you to select an invalid patch version for update. However, the patch is not installed and no rollback is necessary.

During an appliance update, if the "tail -f am---3.0.4.14---timestamp.log" command that monitors the installation displays the following error message:

"The appliance encountered an error during the update or rollback process"

then check the end of the "/var/log/am-update" file for the following line:

"---preUpdate: version 3.00.04.14 is not allowed to update version 3.00.##.##"

If you find the previous line, then the Appliance is not at the correct prerequisite version. Check this readme for the valid prerequisite version, apply that version, and then apply 3.0.4.14.

^Top

Defects Fixed In This Patch

7.1 SP4 P4

AM-18173 In the Security Console, when you ran the "Users with Tokens" report, the output files displayed duplicate rows of user data. Now, there are no duplicated rows in the "Users with Tokens" report output files.

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. Now, migrating RSA Authentication Manager 6.1 to RSA Authentication Manager 7.1 sends RADIUS user profiles to the parent domain.

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. Now, offline authentication data downloads correctly when a realm is configured to use PINless tokens.

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. Now, if administrators scoped to security subdomains select "Search for users across all identity sources", they can view users across all identity sources.

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. Now, when you replace a hardware token containing a numeric PIN with a software token, the PIN migrates to the new software token, and the software token will not be 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 occured"

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

Getting 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