RSA® SecurID Appliance 3.0 SP4 Patch 29 Readme

September 2013

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

Important: In order to streamline the patching process, RSA has aligned the Authentication Manager software and the Appliance versions. Beginning with Patch 25, the Appliance version now follows the same format as the Authentication Manager software version: **am-7.1 SP4 P*xx***, where *xx* is the current patch number. Once P25 is installed, the displayed Appliance version in the Operations Console will no longer be **3.0.4.9** or later, but **am-7.1 SP4 P25** or later.

Updated Installation Instructions

If your current Appliance version is less than **AM 7.1 SP4 P25**, install the patch according to instructions in the section *Command Line Installation* on page 6. Otherwise, follow instructions in the section *Configure the Appliance to Scan for Updates* on page 9.

To determine the appropriate installation procedure:

1. Log on to the Security Console of the Appliance to be updated.
2. Go to **Software Version**.
3. Look for the name of the instance to update, and check in the corresponding **Patches** column for the version. If the version is less than **AM 7.1 SP4 P25**, install the patch from the command line according to the procedure in *Command Line Installation* on page 6.

Contents

Prerequisite Information

Review the following information before updating the Appliance with Patch 29.

Preconditions

Verify that the following preconditions are met:

1. RSA SecurID Appliance version 3.0.4.9 or later is installed.
2. You have at least 4GB of free disk space to install the patch.
3. Authentication Manager authenticates and replicates properly. Do not install Patch 29 on a system that is currently broken.

Appliance Versions for SP4 Patches

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 recovery partition of the Appliance. 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.

Functionality Added Since AM 7.1 SP4 Patch 5

System Logging. 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. 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
- Simple Network Management Protocol (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 more information, see the following sections:

- *Configure Syslog for RSA Authentication Manager in an Appliance Environment*, page 13
- *Configure Authentication Manager to Send Log Messages to a Local File*, page 14

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.

To set the number of digits to display in log messages:

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. Locate the section titled **Token Serial Number Masking for Logs**.
4. In the text box labeled **Number of digits of the token serial number to display**, specify the number of token serial number digits to display in log messages.
5. Click **Save**.

   Note: If you configured this setting prior to Patch 29, your change will be retained when you install Patch 29. 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 must change the value the next time you change the Authentication Manager **Basic Settings** in the Security Console.

Before Updating the Appliance With This Patch

Before you install Patch 29, 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 must enable SSH in the Operations Console, as follows:
  1. Click **Administration > Networking > Configure Connectivity using SSH**.
  2. Select **Enable SSH**.
- If you use a localized Security Console, contact RSA Professional Services.
- If you use cross-realm authentication with RSA Authentication Manager 6.1 or 5.2, you must configure a restricted port range to be used for cross-realm authentication with a firewall. Make sure that the ports in the range are not blocked by the firewall.

  For example, to specify 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: The first time you specify a port range, you must restart the RSA services on the Appliance after specifying the port numbers and before applying this patch.

Command Line Installation

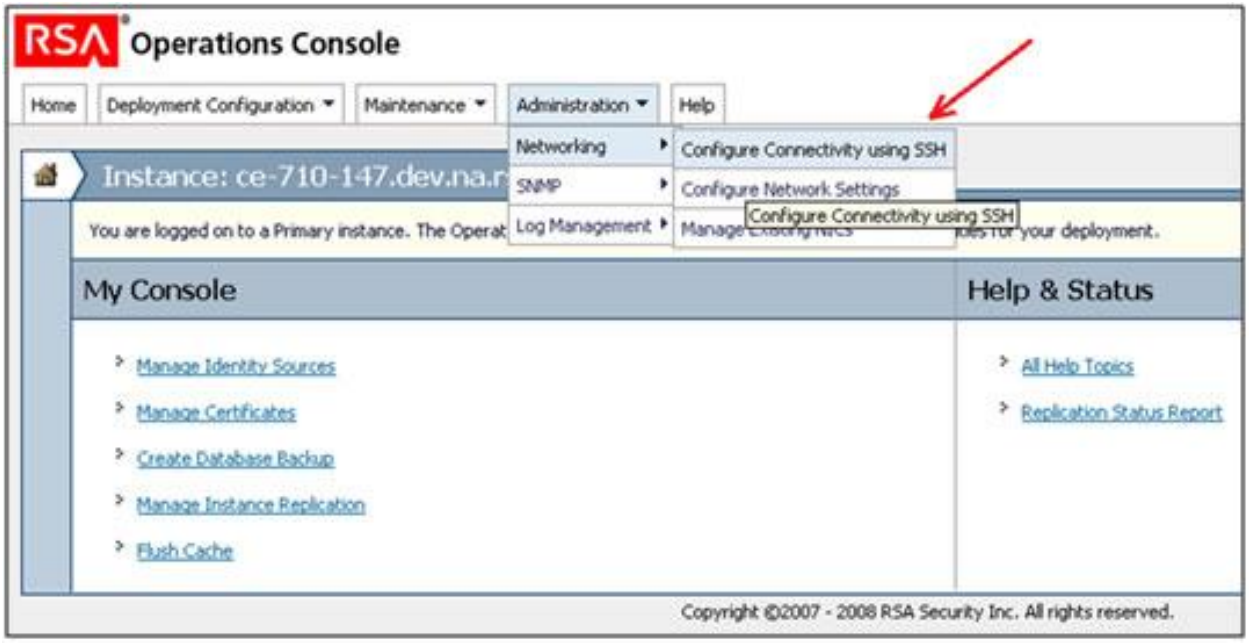
If the current version of your appliance is less than **AM 7.1 SP4 P25** (see *To determine the appropriate installation procedure* on page 1), use the following procedure to install the patch from the command line.

Important:

- If the system has replica(s), make sure replication is working.
- If your system has a primary and replica(s), start installing with the primary, and then continue with each replica.

To install the appliance patch:

1. In the Operations Console, open the **Configure SSH and Operating System Connectivity** page.



2. Under **SSH Settings**, make sure **Enable SSH** is selected.

3. Click **Save** to save the changes.

4. Open an SFTP session in binary mode, and upload the patch ZIP file to a temporary location (such as **/tmp**):

   ```
   file: am-7.1-sp4-p<patch number>-appliance.zip
   user: emcsrv
   password: <EMCSRV_PASSWORD>
   ```

5. Open an SSH session and log in as **emcsrv**.
6. Switch users to **rsaadmin**:

   ```
   sudo su – rsaadmin
   password: <EMCSRV_PASSWORD>
   ```

   The current directory should be **/home/rsaadmin**.

7. Create a subdirectory called **patch#** (where # corresponds to the patch number, for example, patch29):

   ```
   mkdir patch#
   ```

8. Navigate to **/home/rsaadmin/patch#**:

   ```
   cd patch#
   ```

9. Extract the patch ZIP file:

   ```
   unzip <temporary_location>/am-7.1-sp4-p<patch number>-appliance.zip
   ```

10. Run the patch installer:

    ```
    ./setupLinux.bin -silent -V
    RSA_APPLIANCE_LOG=/usr/local/RSASecurity/RSAAuthenticationManager/logs/
    install_patch#.log
    ```

    Where: # corresponds to the patch number.

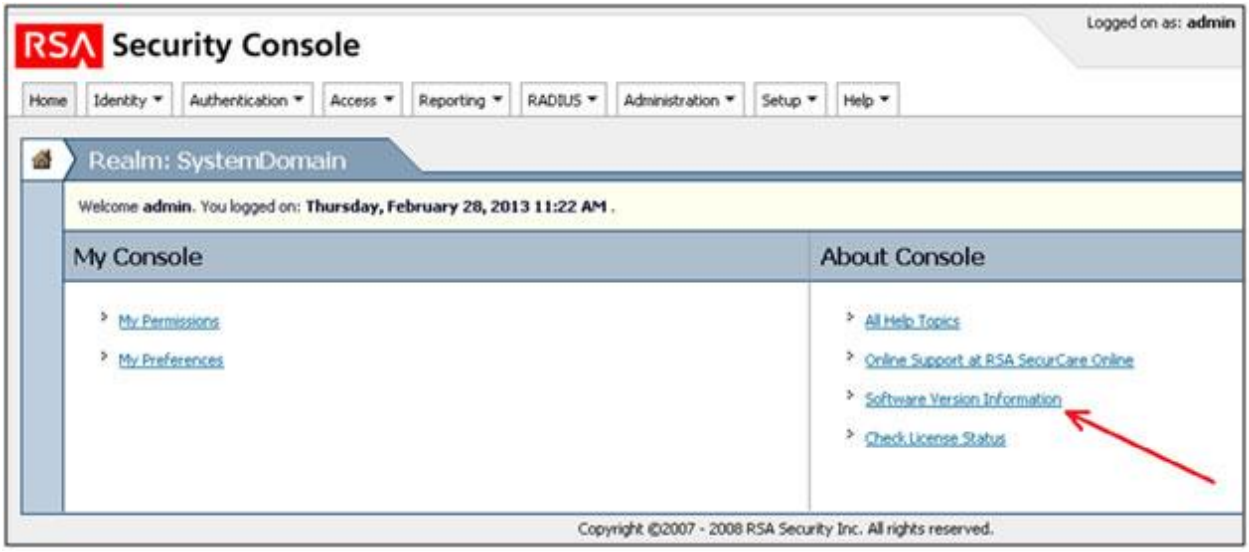
11. Open another SSH session, monitor progress in the patch log, and wait until the command prompt appears:

    ```
    $
    ```

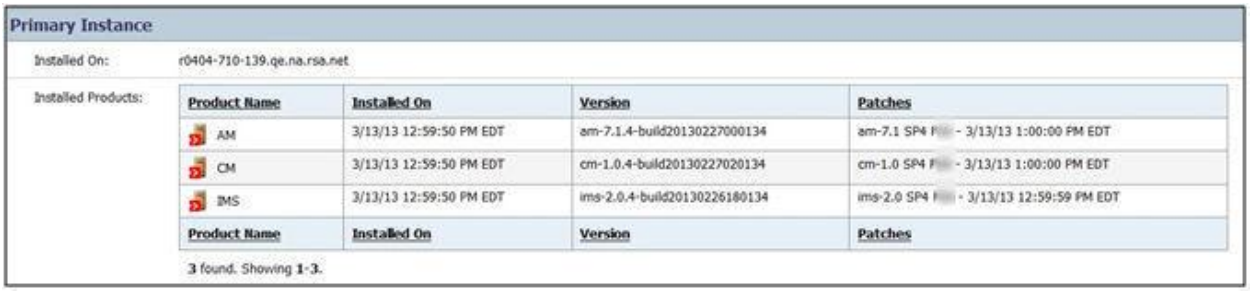
12. When finished, make sure there are no errors in the patch install log file, which is located in **/usr/local/RSASecurity/RSAAuthenticationManager/logs**.
13. If there are no errors in the log file, navigate to **/usr/local/RSASecurity/RSAAuthenticationManager/server**, and start the rest of AM services:

    ```
    ./rsaam start all
    ```

14. Log in to the Security Console on the primary and each replica, and check **Software Version Information**.



15. For the primary/replica on which the patch installer just ran, the number of the installed patch should now appear, as in the following example:



16. To check the number of the installed patch on the Operations Console, go to **Maintenance** > **Manage Rollback** > **Execute Rollback**.

17. If the system has replica(s), log in to the Operations Console and make sure replication is working.
18. Navigate to **/home/rsaadmin** and delete the patch installer:

    ```
    rm -rf patch#
    ```

    Where: # corresponds to the patch number.
19. At the prompt, exit as **rsaadmin**:

    ```
    $ exit
    ```
20. Delete the ZIP file:

    ```
    rm <temporary_location>/am-7.1-sp4-p<patch number>-appliance.zip
    ```
21. At the prompt, exit as **emcsrv**:

    ```
    $ exit
    ```
22. Repeat all steps for each replica.

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 the patch 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 a ZIP file, do not burn the ZIP file to a DVD. Only use a DVD that has come directly from RSA. You must copy the ZIP file 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:

   - To enable 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 ZIP file is stored, for example, **/updates**.
   - To enable 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 ZIP file is stored, for example, **/home/nfs/securid_appliance/updates**.

   Note: The Appliance does not scan subdirectories within a directory, so make sure the ZIP file is stored in the specified location.
3. Click **Save**.

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

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

Download and Copy the Patch to Your Local Windows Machine

Download the patch from SecurCare Online, and verify the MD5 checksum of the ZIP file. Copy the ZIP file to your appliance hard drive.

To copy the patch 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**:

   ```
   sudo su -
   ```

4. Create a new directory called **updates**:

   ```
   mkdir /updates
   ```

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

   ```
   chmod 777 /updates
   ```

6. Copy the ZIP file from your Windows machine to the **/updates** directory on the 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**.
3. Enter the directory on the Appliance hard drive where you have copied the ZIP file, for example, **/updates**.

   
   Note: The Appliance does not scan subdirectories within a directory, so make sure the ZIP file is stored in the specified location.

4. Click **Save**.

Appliance Update Instructions

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

Note: When scanning for updates (**Scan For Updates** page), all ZIP files in the configured update sources are analyzed and validated. Only valid AM patch kits pass the validation. Only patches with a version higher than the current Appliance version will be listed as available updates on the **Apply Updates** page (the next page).

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 29.

To update the Appliance with Patch 29:

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

   Note: When taking a backup of the Appliance, the name of the backup file follows the already established pattern of **am-<*CAP_VERSION*>-<*IDENTITY*>-backup-<*TIMESTAMP*>.tgz**. To identify the newest backup, look for the file with the latest timestamp.

   If the backup fails, do not proceed. Contact RSA Customer Support.
2. Log on to the Operations Console.
3. Configure updates. For more information, see the *Configure the Appliance to Scan for Updates* section of this document.
4. Scan for updates. Select **Maintenance > Manage Update > Scan For Updates**.
5. Apply updates. **Select Maintenance > Manage Update > Apply Updates**.

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. Switch users to **rsaadmin**:

   ```
   sudo su - rsaadmin
   ```

   When prompted, enter the operating system password.
3. From a command shell, change to the **ApplyUpdateStatus** directory:

   ```
   cd /usr/local/RSASecurity/RSAAuthenticationManager/ApplianceUpdateLogs/
   ApplyUpdateStatus
   ```
4. From the console, tail the most recent log file:

   ```
   tail -f am---7.1_sp4_p29---timestamp_ippi.log
   ```

The installation is complete when the following line appears:

```
*** install.sh: Finished Applying Update: am-7.1 SP4 P29 (<build
version>) <timestamp> ***
```

Appliance Update Rollback Instructions

Important: Do not roll back an update unless RSA Customer Support instructs you to do so. Rolling back an update removes the selected update (and its specified version) and might make your system unstable.

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

To roll back the Appliance from Patch 29 to the previous patch:

1. Log on to the Operations Console.
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 7.1 SP4 P29**, select **Roll Back This Update**.

To determine if the rollback 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 Quick Setup of the Appliance.
2. Switch users to **rsaadmin**:

   ```
   sudo su - rsaadmin
   ```

   When prompted, enter the operating system password.
3. From a command shell, change to the **PerformRollbackStatus** directory:

   ```
   cd /usr/local/RSASecurity/RSAAuthenticationManager/ApplianceUpdateLogs/
   PerformRollbackStatus
   ```
4. From the console, tail the most recent log file:

   ```
   tail -f am---7.1_sp4_p29---timestamp_ippi.log
   ```

   The rollback is complete when the following line appears:

   ```
   *** uninstall.sh: Finished rolling back update: am-7.1 SP4 P29 (<build
   version>) <timestamp> ***
   ```

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. Perform the procedures on the primary and replica instances.

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

To configure Authentication Manager to send log messages to a local or remote Syslog server:

1. 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.

   ```
   ms.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. To enable logging, change **false** to **true**.
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 to configure event logging.
4. From the **Context** menu, click **Logging**.
5. Specify the logging levels. For information on each log level, see the "Configure Logging" topic in Security Console Help.
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. Local log files are stored 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**


Note: These locations cannot be changed.

Use the store Command Line Utility (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
  ```

  where:
  value is the value to be set
  instance_name is the name of the primary instance or the replica instance

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

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**.

   Note: In each of the following command lines, *instance_name* is the name of the primary instance or the replica instance.

   - For the admin log:

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

   - For the runtime log:

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

   - For the system log:

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

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.

To set the maximum number of local log files:

1. Log on to the primary instance.

2. Enter one of the following commands from **RSA_AM_HOME/utils**.

Note: In each of the following command lines, *n* is the maximum number of local log files and *instance_name* is the name of the primary instance or replica instance.

- For the admin log:

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

For example:

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

- For the runtime log:

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

For example:

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

- For the system log:

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

For example:

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

- To change the setting for all instances, use the **config_all** option instead of **config**, and omit the *instance_name*.

For example, to set the maximum number of system log files for all instances to 50:

```
./rsautil store -a config_all
ims.logging.system.file.max_backup_index 50
```

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. Enter one of the following commands from **RSA_AM_HOME/utils**.

Note: In each of the following command lines, *n* is the maximum size in MB of the local log files and *instance_name* is the instance name.

- For the runtime log:

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

For example:

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

- For the administrative log:

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

  For example:

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

- For the system log:

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

  For example:

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

- To change the setting for all instances, use the **config_all** option instead of **config**, and omit the *instance_name*.

  For example, to set the maximum size of the system log files for all instances to 5 MB:

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

Known Issues

The following are known issues:

AM-18877 The **import-bulk-request** command only accepts requests from Active Directory and SunONE users registered in the Authentication Manager database. If a user is not registered, the generation of the request may fail with an Oracle error, for example: "ORA-12899: value too large for column."

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-20316 For the Linux 32-bit and 64-bit platforms, stop all RSA services before rebooting the server. Replication may be adversely affected if the RSA services are not stopped before the server is rebooted.

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 instances 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-21604 When you downloaded a completed report in .csv format and opened it with Microsoft Excel, unknown characters displayed in place of quotation marks. To display the quotation marks correctly in Excel, you can use Microsoft Office Excel to import data into the worksheet. For more information, see http://office.microsoft.com/en-us/excel-help/text-import-wizard-HP010102244.aspx

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-22671 If you installed P20, P21, P22, or P23, the fix for AM-22671 might have caused an issue. In P24, however, AM-22671 has been reworked to resolve that issue. Therefore, please install P24 or greater.

AM-23369 The **import-bulk-request** command creates requests for group membership in groups in an identity source other than the identity source where the user is located. In this situation, the RSA Security Console's list of Provisioning Requests will refer to the identity source of the target group and not the identity source of the user.

AM-26772 Some application security scanners may report a potential vulnerability when, during a test attack, they append SQL statements to a pToken value. The AM server then returns an HTTP status of "200 OK", which the scanner mistakenly interprets to mean that the appended SQL was executed. In reality, however, the SQL was ignored – AM removes the invalid, unused SQL data and responds with a web page and a successful response code at completion. Since the SQL data is not executed, there is no vulnerability in this case.

Defects Fixed in This Patch

7.1 SP4 P29

Patch 29 contains fixes for the following issues:

AM-27020 When logging off from the Security Console or Self-Service Console without closing the browser, a subsequent attempt to access the Security or Self-Service Console after going to other sites in the same session, resulted in an "Invalid Request" error. In this case, an issue with the browser cache in the Console has been resolved and the error no longer occurs.

AM-27052 On Windows 2003 64-bit platforms, reattaching a demoted primary no longer reports a failure at the last stage when restarting services.

AM-27166 When a software token was unassigned from a user, software token attribute values were deleted from token attribute value table. Due to this, no attributes were displayed for that token when viewed. Software tokens attributes are no longer deleted when unassigning a token.

AM-27168 Cannot install a patch using a USB device. After installing P29, you can use a USB device to install later patches.

7.1 SP4 P28

Patch 28 contains fixes for the following issues:

AM-24253 When using the Self-Service Console to request a new software token, the user was required to enter an initial PIN, even when the token policy was set to "Require system-generated PIN."
In Patch 28, when the token policy is set to "Require system-generated PIN", user-generated PINs are eliminated for self-service requests for new tokens. Instead, the Self-Service Console displays the system-generated PIN when users request new tokens, request replacement tokens, or enroll for self-service.

AM-26856 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-27049 Hidden files in the NFS share were cleaned up for manual backups, but not for scheduled backups. Hidden files are now properly cleaned up for both manual and scheduled backups.

AM-27087 When users enabled for On-Demand token codes are missing certain values (such as phone number or email address), the On-Demand tokencode service report failed with "Error" status and no records displayed. The report now successfully completes even when those user values are missing.

AM-27088 Attaching a demoted primary as a replica failed with the error "ORA-08181: specified number is not a valid system change number". This issue occurred when the system change number (SCN) was large and has been fixed by allowing larger SCN numbers.

AM-27192 Beginning with patch 25, the Security Console function to clean unresolvable users stopped working. An error message displayed and the cleanup was unsuccessful. This problem was fixed and the cleanup succeeds.

AM-27198 When a scheduled NFS backup ran, it was reported as an error in the Security Console, even though the backup file had been transferred successfully to the NFS Server. This issue was fixed previously for manual backups (AM-24889) and is now fixed for scheduled backups. A scheduled backup that runs successfully now no longer reports an error.

7.1 SP4 P27

Patch 27 contains fixes for the following issues:

AM-26819 The Patch installer now verifies replication at the beginning of the installation so that any issues can be reported and fixed before installation fails.

AM-27043 SDK sample code no longer fails when using "securid" authentication method.

7.1 SP4 P26

Patch 26 contains fixes for the following issues:

AM-25683 On Windows 2008, RSA RADIUS now works when Network Security policy "Send NTLVv2 only. Refuse LM & NTLM" is enabled.

AM-26780 If you used the RSA Authentication Manager 7.1 Software Development Kit (SDK) to develop a custom application that connects with Authentication Manager, and if trace logging was set to **Verbose**, the administrative account password used by the custom application appeared in the trace log file as clear text. Patch 26, however, prevents Authentication Manager from logging that administrative account password, independent of the specified logging level.

RSA recommends that after applying Patch 26, you create a new password for the administrative account that an SDK-developed custom application uses to connect with Authentication Manager. After changing the password in the Security Console, you must communicate the new password to the administrators who use the custom application. For instructions on changing a user password, see the Security Console Help topic "Change a User's Password."

AM-26946 Authentication Manager (AM) now supports the Active Directory (AD) group type "BUILTIN". Therefore, AD users mapped to this group no longer cause warnings to appear in the System Activity Monitor when running an AM user report.

AM-27005 Can now increase SGA size, using **rsautil** to tune **db_sga_target** and **db_sga_max**, to greater than 2050MB, as long as **db_sga_target** is less than or equal to **db_sga_max**, and the system has sufficient memory to allocate to the increased SGA.

AM-27012 In the Security Console, when the "Users with days since last login using specific token" report fails, system activity logs now provide more information about the data causing problems (such as user ID and identity source ID) so that the data can be corrected.

AM-27036 Corrects an issue in P25 that caused authentications to fail if verbose tracing was enabled.

7.1 SP4 P25

Patch 25 contains fixes for the following issues:

AM-24529 Reworked fix to resolve an issue caused by the fix for AM-24529 in P20.

AM-25879 A check for missing arguments has been added when executing the manage-database in manage-database command line utility (CLU).

AM-26701 Replication no longer breaks when an update is being done on the same record on primary and replica at the same time.

AM-26772 Possible "Blind SQL-Injection" vulnerability has been addressed.

AM-26785 Users in an external group linked to a restricted agent can now authenticate to the restricted agent, even if the name of the group ends with an asterisk (*).

AM-26883 Uninstalling the patch now finishes without giving any errors on Linux.

AM-26906 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-26922 Patch uninstall now uses a predetermined name and location for uninstall log.

7.1 SP4 P24

Patch 24 contains fixes for the following issues:

AM-12879 In the Operations Console, on the Configure Secondary NIC page, iHelp that appears when you hover over the Type field has been corrected.

AM-22671 If the Authentication Method field is set to "none" in the Self-Service Troubleshooting Policy, then enable token using "Enable Token" link on the Self-Service Console process failed. This issue is fixed and token can be enabled through the Self-Service Console.

Note: The fix for this issue, included in P20, caused an issue that has been corrected in P24.

AM-23516 User's "Last Login" date now updates in sync with token's "Last used to Authenticate" date on all replicas.

AM-24183 Authentication Manager now correctly handles HTTP error code 500 from SMS provider.

AM-25191 When network cable is unplugged from primary instance, promoting a replica in disaster recovery mode does not fail.

AM-25367 Activity log for offline authentication now displays user ID instead of "SYSTEM" when user no longer exists on the server. Other fields such Last Name/First Name, however still display as "SYSTEM".

AM-25864 In Security Console, user icon now changes to admin icon after the admin role is assigned.

AM-26431 In some Linux systems, AM services did not restart appropriately after system reboot, due to corruption on the start-up script. The start-up script has been fixed.

AM-26613 Hint text for On-Demand Tokencode Message now provides the correct value for the maximum length of the final message, which is 140 bytes instead of 160 characters.

AM-26672 In certain circumstances, executing the RSAUTIL command to generate the replica info report produced a LocaL_log_apply_timeout value of TIMEOUT. This issue has been corrected so that command no longer returns that value.

AM-26712 Backups created on NFS Windows server were creating hidden files. This issue has been fixed so that no hidden files are created.

AM-26773 When invalid URL is entered, Security Console help now returns error status code instead of "200 OK" status code.

AM-26836 Deleting an agent associated with a RADIUS client and then publishing the RADIUS no longer breaks replication for all replicas.

7.1 SP4 P23

Patch 23 contains fixes for the following issues:

AM-19975 In the RSA Security Console, granting access to particular user groups produced a confusing error. The error message was rewritten to explain the problem and recommend corrective action.

AM-27198 Scheduled appliance backup no longer reports an error when the backup file transfers successfully to the NFS server.

AM-23263 The RSA Security Console now prevents the creation of a RADIUS Client with an invalid IP address.

AM-25688 In Authentication Manager 7.1 SP4, executing the "tune-system" command with invalid credentials now returns the appropriate error message.

AM-25868 In Authentication Manager 7.1 SP4, filtering by UserID in the Real Time Authentication Activity Monitor is no longer case-sensitive.

AM-25869 When migrating users from Authentication Manager 6.1 to Authentication Manager 7.1, users who belong to an internal group before the migration are now members of the internal group after the migration. If a migrated user belongs to External Identity Source, only unregistered users will be members of the internal group after the migration.

AM-26130 In Authentication Manager 7.1 SP4, the Log Archive Job was not purging log records corresponding to activity on Operations Console. The log records are now purged appropriately.

7.1 SP4 P22

Patch 22 contains fixes for the following issues:

AM-21670 When configuring an External Identity source and using a semicolon as a separator for the Domain Name (DN), the RSA Operations Console reported that User Base DN and User Group Base DN did not exist. Configuring an External Identity Source and using a semicolon as separator for DN no longer produces this error.

AM-22390 In the RSA Security Console, advanced search to manage existing users did not display disabled users. Disabled users in an external identity are now displayed as expected. Note that this fix supersedes the fix previously documented in P14.

AM-22523 Unable to import software token into a Mac desktop when using a generic 128 device type. A software token can now be distributed successfully to a Mac desktop using CT-KIP and a generic 128 device type.

AM-24854 Authentication Manager 7.1 SP4 did not validate maximum failed attempt value while updating a lockout policy using UpdateLockoutPolicyCommand API. Authentication Manager 7.1 SP4 now validates maximum and minimum accepted values when update is done using UpdateLockoutPolicyCommand API. If values are set beyond accepted range, expected error codes are returned.

AM-25468 In Authentication Manager, after a replica promotion and demoted primary re-attach, scheduled report jobs disappeared. Auth Manager has been fixed so that all scheduled report jobs are properly switched to the replica promoted to primary.

AM-25963 Multiple values for user's alias data did not migrate from Authentication Manager 6.1 to Authentication Manager 7.1. Those values now migrate successfully.

AM-25967 When using TokenDTO.setPIN API to pass an empty string, Authentication Manager was erroneously clearing the PIN instead of returning an error. Authentication Manager now returns an error in this case.

AM-26082 In the RSA Security Console, when the agent host associated with the RADIUS Server is edited, the "Protect IP address" setting was changed from "Yes" to "No". The "Protect IP Address" setting is no longer modified as the result of editing the agent host associated with the RADIUS server.

AM-26219 An incorrect warning message that appeared in logs and in progress pages while attaching a demoted primary or replica instance no longer appears.

7.1 SP4 P21

Patch 21 contains fixes for the following issues:

AM-18003 RADIUS clients and profiles are not accessible on RADIUS replicas when the primary is shut down. When this situation occurred the following error message displayed:

"Unable to connect to RADIUS server within the given timeout."

Now, one of the following error message displays:

- If a user logs in to the Security Console for the first time, the following displays:

  "You need to accurately configure a RADIUS server before you can view or edit any RADIUS Clients or Profiles. Could not connect to RADIUS server. The RADIUS server may be down or the wrong connection information has been given."

- If a user has already logged in and connection to the primary instance breaks, the following displays:

  "You need to accurately configure a RADIUS server before you can view or edit any RADIUS Clients or Profiles. Could not connect to RADIUS server. The RADIUS server may be down or the wrong connection information has been given."

AM-22541 If you re imported a trust package after reinstalling on one of the primary instances, then the package did not update the stored root certificates in the system and SSL errors occurred in the logs. This issue has been fixed and the stored root certificate is updated when you re-import a trust package.

AM-23140 In the RSA Security Console, a defect existed where security questions displayed as an available authentication method for users to login to the RSA Self-Service Console. This issue has been fixed, and security questions no longer displays as an authentication method.

AM-23141 In the RSA Security Console, on-demand authentication was listed as an available authentication method for users to login to the RSA Self-Service Console. This issue has been fixed, and on-demand authentication no longer displays as an available authentication method.

AM-23502 In Authentication Manager, emergency access tokencodes were not reset after being reassigned to a user. This caused failed authentications when the user authenticated with an unused emergency access tokencode. This issue has been fixed, and emergency access tokencodes are cleared every time a software token is unassigned.

AM-24293 After replica instance promotion, the new primary Operations Console has the option **Restore from backup**. This option should not exist in a promoted replica instance. This issue is fixed, and the option is no longer available.

AM-25286 The RSA SDK command EnableOnDemandForPrincipalsCommand showed incorrect behavior while re-enabling users with SDK code. This issue has been fixed and the server now returns the correct values.

AM-25433 Authentication Manager 6.1 users with multi-byte characters in the default shell experienced authentication failures after they were migrated to Authentication Manager 7.1. This issue has been fixed, and migrated users can authenticate successfully.

AM-25672 In the RSA Security Console, after restoring a pre-SP4 database, the software version displayed incorrect version data. This issue is fixed and the software version displays the correct Authentication Manager version.

AM-25679 In the RSA Operations Console, an issue existed where you could delete multiple replica instances at once. This functionality is not supported in Authentication Manager. This issue is fixed and you can no longer delete multiple replica instances at once.

AM-25798 Corrects a potential Java issue announced by Oracle in October of 2012. 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 October 2012. The update is cumulative, including all previously released fixes for this JRE.

AM-25812 There have been time zone changes in the past year. This fix updates authentication manager to reflect these changes. This fix does not update your operating system.

AM-25819 In the Authentication Activity report, the Authentication Method ihelp displayed unwanted html characters. This issue has been fixed and no unwanted html displays in the report.

AM-25825 The manage-database CLU failed to send notification e-mails to administrators when certain configurable parameters had been reached for database files. This issue is fixed and administrators will receive notification e-mails.

AM-25848 Some CLUs could not run successfully because the **From E-Mail Address** field in the E-Mail (SMTP) page was empty. This issue is fixed and the **From E-Mail Address** field is now mandatory.

7.1 SP4 P20

Patch 20 contains fixes for the following issues:

AM-16477 If, after changing SSL certificates on the primary RADIUS server, the appropriate process is not applied on the replica server, the communication with the primary RADIUS server failed during configuration of the replica RADIUS server and an unclear error message was displayed. This issue is fixed to provide an appropriate error message.

AM-16765 The SearchPrincipalsCommand throws UnexpectedDataStoreException when filter and setAttributeMask are set. This issue is fixed by correcting underlying query.

AM-22671 If the Authentication Method field is set to "none" in the Self-Service Troubleshooting Policy, then enable token using "Enable Token" link on the Self-Service Console process failed. This issue is fixed and token can be enabled through the Self-Service Console.

Note: In P20, the fix for AM-22671 caused an issue that is resolved by the reworked fix for AM-22671 provided in P24. See *Known Issues* on page 17 for details.

AM-22953 On restoring a backup taken before you applied the SP4 Patch 6 from a promoted primary to a primary system with the SP4 Patch 6 through Patch 19 installed, the restore failed with following error message:

"Unable to apply IMS SP4 bootstraps :consolidated-ims-bootstrap-sp4.sql"

This issue is fixed, and restore backup works without any error.

AM-23014 If the SMS message delivery through HTTP failed due to SocketTimeoutException, the system event log displayed InvalidArgumentException. This issue is fixed to display the correct error in the system event log.

AM-23644 In the Token Expiration report, if the Token Enabled filter is used, User ID, First Name or Last Name filters did not provide correct result. This issue is fixed to apply all the filters independently.

AM-24094 In the RSA Security Console, the Users with Tokens report may contain some duplicate and missing entries. This issue is fixed to display all the entries with no duplication.

AM-24529 If the deployment has multiple replica instances, deleting one of the replica instances can result in the following error in the alert log of another replica:

Replication Error Unhandled apply error 22922 occurred in RSA_REP.IMS_INSTANCE_NODE_ADDRESSES (or RSA_REP.IMS_INSTANCE_NODE).

The deletion issue has been fixed to prevent the replication error condition in the future when a replica is deleted. The fix does not address replica systems already in this state. If the system already has this error, contact RSA Customer Support.

Note: In P20, the fix for AM-24529 caused an issue that is resolved by the reworked fix for AM-24529 provided in P25.

AM-24826 During startup of an RSA RADIUS server on a windows system that is part of a windows domain, the RSA RADIUS server performs queries to domain controllers for user information. This issue is fixed to limit the query.

AM-24934 The remote backup of an appliance shows the following error in the Operations Console log file:

"Error deleting NFS backup hidden files"

This issue is fixed and no error is displayed in the log file.

AM-25357 The troubleshooting section on the Self-Service Console page of the Authentication Manager contained several typographical errors. This issue is fixed by correcting all the spellings.

AM-25454 In the Security Console, the Force Replication to All process in RADIUS caused stuck thread error java.net.SocketTimeoutException. This issue is fixed to release the threads.

AM-25561 The phone numbers for users from Albania with Country Code +355 was not accepted for the on-demand tokencodes, because the Country Code +355 was not listed in the available country codes. This issue is fixed to allow +355 country code in the phone numbers.

AM 25563: Authentication Manager could not find a user's group membership if there were nested groups in the group membership lookup. This issue is fixed to handle nested groups in the group membership lookup.

AM-25564 The Active Directory identity source may become unresponsive if the RSA Authentication Manager uses restricted agent groups with many users. This issue is fixed by optimizing the queries for groups.

7.1 SP4 P19

Patch 19 contains fixes for the following issues:

AM-11559 If you select "Validate identity attribute definition mappings against directory schema" option, adding an external identity source as a Global Catalog fails with the following error:

"The physical attribute's schema name samAccountName does not exist in the directory or the attribute syntax is not supported."

This issue is fixed by skipping the schema validation for the attribute samAccountName while adding an external identity source as a Global Catalog.

AM-13017 If multiple external identity sources whose users are authenticated through a Global Catalog are linked to the realm, then an unreachable identity source cannot be unlinked from the realm. This issue is fixed to unlink the identity source even if it is not reachable.

AM-13725 If you have an external identity source whose users are authenticated through a Global Catalog, removing the Global Catalog was not possible. This issue is fixed by making the external identity source users to authenticate against the external identity source that they belong, when the Global Catalog is removed.

AM-14755 The default token image, which is displayed while requesting a new token, did not correspond to the requested token type. This issue is fixed to add default images for different types of tokens.

AM-16095 If a user record in a read-only external identity source had more than 255 characters in the Comment field, the edit user operation failed during validation. This issue no longer occurs because Authentication Manager does not validate the Comment field for this operation in read-only external identity sources.

AM-18383 In the RSA Self-service console, a desktop image was displayed for BlackBerry 3.5 when requesting a new token. This issue is fixed to display corresponding image.

AM-18788 In the RSA Self-service console, an old KEYFOB image was displayed for SID700 token, when requesting a new token. This issue is fixed to display updated SID700 image.

AM-20082 The Boolean field Authentication Method in the Authentication Activity report did not work for multiple authentication methods. This issue is fixed to support multiple authentication methods separated by "OR", "or" and "/" Boolean operators, where "OR" and "or" must have a single white space before and after.

AM-20497 In the RSA Security Console, enabling or disabling users did not work from the drop-down list on the Manage Existing page, if the users belong to an external identity source. This issue is fixed to update disabled status of those users, who are managed in the external identity source.

AM-21399 In the RSA Self-service console, a desktop image was displayed for Desktop MAC 4.0 when requesting a new token. This issue is fixed to display corresponding image.

AM-21874 The User ID filter in the Authentication Activity report was case-sensitive and the report did not contain all the authentication messages. This issue is fixed and the report is no longer case-sensitive.

AM-23567 The offset value was not updated when a hardware token is out of sync by one window interval. This issue is fixed to update the offset value even for one window interval.

AM-23836 When users authenticate through RADIUS in Next Tokencode or New PIN Mode, the Client IP column in Authentication Activity Monitor displays wrong IP address. The client IP column is fixed to display the IP corresponding to the hostname.

AM-23855 If there are multiple realms and if the date format is different from the default format, the Scheduled Report Job cannot be created in the RSA Security Console. You see the following error message:

"Job Starts" must be a date.

This validation problem is fixed by using the local date format for the validation.

AM-23862 When users authenticate through RADIUS, the Client IP column in Authentication Activity Monitor displays the wrong IP address. The client IP column is fixed to display the IP corresponding to the hostname.

AM-23870 Software Tokens issued in SDTID format used birth date based on the current local date instead of UTC date. This issue is fixed to get the birth data from the server.

AM-24253 In the Self-service console, users were allowed to create a PIN while requesting a new software token, even if the token policy allows system generated PINs only. This issue is fixed to hide the Create PIN dialog if the policy is enforcing system generated PIN only.

AM-24254 If an existing CT-KIP activation code is used, distribution of software token as CT-KIP fails with the following error message:

"Unable to distribute a software token as CT-KIP"

The error message is updated as follows:

"The CT-KIP authcode already exists."

AM-24366 If the time between the primary and replica servers are different by a small amount, attaching replica may fail with the following error:

"The system time at current instance is different from the primary instance. Please change it"

The error message is corrected to display the following:

"The system UTC time at current instance is different from Primary instance. Please sync system time with Primary instance and try again."

AM-24453 If a token request is archived and then restored before user has enabled their token, clicking the Token Enablement link displays the following error:

"There was a problem processing your request. The information you entered is incorrect. Please try again, or contact your administrator."

This error is fixed and the user is able to login after entering the right enablement code.

AM-24616 In the RSA Operations Console help, a session cookie was not SSL secure and it was used for all types of connections. This was fixed by making the cookie SSL secure, so that it can be used for encrypted connections only.

AM-24645 User's alias data was not migrated from Authentication Manager 6.1 to Authentication Manager 7.1. This issue is fixed to migrate the alias data.

AM- 24895 In the RSA Security Console, if you click Reporting> Report Output > Completed Reports, the Submitted column displays the time when the scheduled report job was created and not the time when it was actually run. The Completed Reports page is enhanced to add a new column Completed On to display the time when the scheduled job was run. The name of the column **Submitted to** is also modified to **Submitted On**.

AM-25027 In the RSA Security Console, when a software token is distributed through CT-KIP, the Software Token Settings Displayed Value did not retain its value if it is set to Tokencode (PIN entered followed by tokencode during authentication). This issue is fixed to retain Displayed Value setting.

AM-25184 Cross-realm authentication from RSA Authentication Manager 6.1 to RSA Authentication Manager 7.1 was not successful. This issue is fixed.

AM-25193 In the RSA Security Console, Administrative Audit log did not include failure messages from token resynchronizations. This issue is fixed by adding failure messages to the administrative audit log, if the resynchronization of a token fails.

AM-25231 Cross-realm authentications from RSA Authentication Manager 6.1 to RSA Authentication Manager 7.1 always displayed N/A for Client IP column in the Authentication Monitor. This issue is fixed to display the IP address of the client, if it is available.

7.1 SP4 P18

Patch 18 contains fixes for the following issues:

AM-11663 The EmbeddedLDAPAccess.log file was growing rapidly in size. This issue is fixed by rotating the EmbeddedLDAPAccess.log file and retaining only one old log file containing logs from current and previous date to reduce the size of the overall logs.

AM-13967 If a CN, associated to the user in the Active Directory, contained leading or trailing spaces, the edit user operation for that user failed with the following error message:

"There was a problem processing your request. Operation failed because data was updated concurrently by another user. Reload data and try again."

This issue is fixed to support CN with leading or trailing spaces.

AM-18075 Before killing the RSA AM server processes, the RSA kill rsaauthmgr scripts for Linux did not remove the locks properly. This issue is fixed to kill the processes correctly, so that the scripts are called during reboot and shutdown of the machine

AM-18397 The Software Version Information page displayed the last restart time of the instance instead of the patch installation time in the Installed On column. This was fixed to display the patch installation date and time in the Installed On column.

AM-18698 In the Self-Service Console, the Request a new account link was displayed on the homepage after the troubleshooting process, even if the provisioning license was not available. This issue is fixed to check provisioning license before displaying the Request a new account link.

AM-18877 The import-bulk-request CLU fails for an unregistered user belonging to an Active Directory Identity Source. One of the following error messages was displayed in the log file:

```
Error : failed to find principal
```

```
Error : ORA-12899: value too large for column
"RSA_REP"."UCM_REQUEST"."CREATED_BY"
```

The error message is corrected to read as follows:

```
Error : Principal must be registered for token request.
```

AM-20986 The list for selecting the attribute name from the User Attribute to Provide SMS Destination drop-down list under the SMS Configuration tab does not include User Identity Attributes of type Integer. This issue is fixed by modifying the iHelp description. The following modified iHelp description clearly indicates the attribute type:

Select a user attribute of type string that provides the telephone number to which the tokencode will be sent. The telephone number should be in the format: +Country code City or Area code Telephone number.

AM-21683 In the Security Console, the "Test Connection" functionality for testing email configuration from the replica server sent email from the primary server. This issue is fixed to send test email from the replica server.

AM-22548 The Offline Authentication (OA) download failure due to passcode length requirements was not reported in the Authentication Manager logs. This issue is fixed to report the following message in the Authentication Manager logs.

"Passcode does not meet minimum length requirement for OA download"

AM-23355 The LogoutCommand execution displayed "unknown" as the client IP in the Authentication Monitor. The LogoutCommand is fixed to display the correct client IP address in the Authentication Monitor.

AM-23382 If the principal did not belong to any of the groups that were allowed to authenticate through a restricted agent, the authentication request resulted in the following misleading error message:

"Unable to resolve user by login ID and/or alias, or authenticator not assigned to user"

This issue is fixed to provide the following correct error message:

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

AM-23638 In the Security Console, if the User Authentication Requirement field for a SecurID Token is set to "Do not require PIN (only tokencode)", the following value for the field Displayed Value was displayed in the next page:

"Tokencode (PIN entered followed by tokencode during authentication)"

This issue is fixed to display the value for the field Displayed Value as "Tokencode (Tokencode Only)".

AM-23757 When a user accessed the Self-Service Console, the internal server name was returned in the HTTP header. This issue is resolved by encoding the RelayState parameter of the HTTP header.

AM-23879 If you execute manage-trust CLU to create an application trust with a name of an existing user, unique constrain violation error was displayed. The error message is updated to the following message:

"The CLU command cannot proceed because application trust already exists".

AM-23918 The On-Demand tokencode service report did not filter users by the identity source that is selected in the User Identity Source filter. The report is fixed to apply the filter correctly.

AM-24023 If you edit the fields of Self-Service Troubleshooting Policy, the following error message is displayed in the rsa-console.log file:

"Cannot find bean: "SelfServicePolicy_pManager" in any Scope"

This issue is fixed to update Self-Service Troubleshooting Policy correctly.

AM-24044 Certain administrative passwords and other information were not properly propagated from the primary to replicas. This problem was fixed to update the replica instance **systemfields.properties** file correctly.

AM-24047 In some situations, uninstalling patches P14, P15 or P16 on Windows systems would result in the original radAdmin.dll file being placed in a directory "null" under the RSA_AM_HOME directory rather than the correct location under Program File\Common Files. This could prevent the RADIUS service from starting after the uninstall.

AM-24252 When a user accessed the Security Console or the Operations Console, the following popup warning message was sometimes displayed:

"Missing or invalid license for PopCalendarXP!"

The warning is fixed and the popup message is no longer displayed.

AM-24256 When a Helpdesk Admin, who also has permission to manage on-demand tokencodes, logs in after the server is re-started, the Enable On-demand Tokencode checkbox does not appear for the first time in the SecurID Tokens page. This issue is fixed to show the page correctly based on the permissions.

AM-24473 If the size of the replicaAttach.dmp file was more than 2GB, the manual attachment process for the replica failed. This issue is fixed to support the files that are larger than 2GB in size.

AM-24735 After installing P16 or P17 cross-realm authentication from AM 6.x servers to AM 7.x servers stops working. The issue has been fixed to allow AM 6.x to AM 7.x cross-realm authentication.

7.1 SP4 P17

Patch 17 contains fixes for the following issues:

AM-9979 On the logon page of the Self-Service Console, the title was displayed as Security Console. The logon page is fixed to display the title as RSA Secure Logon and the correct logo.

AM-14205 When you download the System Log Report in .csv format, some of the replication messages were not sorted by time. The report is fixed to sort all the messages by time.

AM-22164 In the RSA Operations Console, the backup operation on the replica instance failed and displayed an incorrect error message after SP4 was installed. This issue is no longer occurs because the link to the backup operation was removed from the Operations Console home page.

AM-22229 If the On-Demand Tokencodes configuration was changed on the primary instance, the changes were not reflected on the replica instance. This issue is fixed to update the configuration changes on the replica instance.

AM-22400 For the users whose last name was entered as Null, the RSA Security Console displayed their first name and last name as Not Provided. This issue is fixed to display the correct first and last name.

AM-22525 If an identity attribute name contained an apostrophe (’), the attribute value was not displayed correctly in the Self-Service Console. The issue is fixed to display the correct attribute values.

AM-22613 If a user logged on to the RSA Self-service Console through a proxy server or a Web SSL VPN, images associated with tokens assigned to the user were not displayed on the home page. This issue is fixed to display token images correctly.

AM-23381 In the RSA Security Console, importing a password dictionary with additional carriage returns at the end of the file caused an error message to be displayed. This issue is fixed to import the password dictionary correctly.

AM-23523 If a user entered the wrong tokencode during an on-demand authentication, RSA RADIUS did not respond properly. The RADIUS response is fixed by sending an Access-Denied response rather than an Access-Challenge response, when a wrong on-demand tokencode is entered.

AM-23990 Since Authentication Manager 7.1 SP4 patch 14, the AddPrincipalsCommand API fails while using the SOAPCommandTargetBasicAuth. The AddPrincipalsCommand API is now fixed to send the correct message.

AM-24145 The Authentication Manager patch installation failed if the default Token Administration role was missing from the server. The installation issue is fixed to complete the patch installation.

AM-24177 When you run “Administrators of a Security Domain” report and try to download it in the csv format or view it in the browser, the following error was displayed on the status:

“Either another administrator deleted one or more of the selected objects, or you attempted to delete objects from more than one identity source at the same time”.

This issue is fixed to run and download the report correctly.

7.1 SP4 P16

Patch 16 contains fixes for the following issues:

AM-10559 In the Security Console, a failed token import job was not reported in the Administrator Activity or the System Log. This problem is fixed to report the failure in the log files.

AM-11456 When an activity log record used a future date, the Activity Monitor in the Security Console stopped displaying the current records until the future time. Now the activity monitor works properly in this case.

AM-11602 In the Security Console, the expiration date of the tokens did not reflect the server time zone. The time display is fixed to display server time zone correctly.

AM-11686 In the Security Console, after an identity source cleanup batch job runs, the 'submitted on' time changed to the 'completed on' time. The time display is fixed to show the submitted and completed times correctly.

AM-12013 On Windows systems, the ORACLE_HOME value was not set correctly after running the rsaenv.bat file. The issue was fixed to update the ORACLE_HOME value during patch installation.

AM-17967 In the RSA Security Console, authentication failure due to an expired LDAP password was not reported in the runtime activity log. This is fixed to show a password expiration message in the activity log.

AM-20929 CLU help for manage-ssl-certificate was updated to indicate that copy and paste of command lines may result in a failure.

AM-23128 When a nonadministrative user tried to log on to the Security Console with valid credentials, the following error message was displayed.

"Sorry, your request cannot be processed at this time. Return to home and try again"

The user could not return to the logon screen from the message page. This issue was fixed by asking the user to log off, which redirects the user to the login screen.

AM-23548 When the same User ID is present in more than one realm, the Windows Agent cannot recharge offline days after changing the Windows password. It was fixed to recharge offline days for the user that belongs to the realm associated with the agent.

AM-23576 In the Security Console, saving emergency access tokencodes from the Identity->Users->Manage Existing page removed the Next Tokencode mode flag, even if there was no change on the page. The page was fixed to retain the value of the Next Tokencode mode after the save operation.

AM-23711 The 'All users' report for an internal group did not list users from any external identity source. The issue is fixed to include users from the external identity sources.

AM-23716 When non-supported Active Directory groups are excluded from the search result, a warning message was logged. Warning message is no longer added to the log.

AM-23759 The authentication of users in large groups from external identity sources, which are associated with restricted agents, sometimes caused authentication to fail due to a timeout. The problem was resolved by improving LDAP queries.

AM-23796 In the RSA Security Console, the hint text for the port number on the Authentication Manager Settings page is updated to indicate correct port range values from 1025 to 49151.

AM-23814 In the RSA Self Service Console, cacheable SSL pages were found. This security vulnerability was addressed by removing the pages from the browser cache.

AM-23836 When users authenticate through RADIUS in Next Tokencode or New PIN Mode, the Client IP column in Authentication Activity Monitor displays wrong IP address. The Client IP column is fixed to display the IP address corresponding to the hostname in the Agent column.

AM-23839 In the RSA Security Console registering a RADIUS client, which is already registered by selecting RADIUS Clients-> Manage Existing menu, displayed DuplicateDataException in the traces. Duplicate data error was fixed by adding a check for duplicate registration.

AM-23862 When users authenticate through RADIUS, the Client IP column in Authentication Activity Monitor displays the wrong IP address. The Client IP column is fixed to display the IP address corresponding to the hostname in the Agent column.

AM-23866 In the RSA Security Console, an exception in listing RADIUS clients caused "503–service unavailable" error. Service unavailable error was fixed.

AM-23876 In the RSA Self Service Console, accessing URL to confirm an image file existence, caused "503–service unavailable" error. Service unavailable error was fixed.

AM-23885 The RADIUS ExtOutputDeniedFinal prompt keyword in the securid.ini file is corrected.

7.1 SP4 P15

Patch 15 contains fixes for the following issues:

AM-18476 In the RSA Operations Console, on the replica instance, the following incorrect error message displayed when you entered an incorrect administrator password during RSA RADIUS configuration:

"There was a problem processing your request. - Invalid primary RADIUS server's replication secret was provided."

The error message has been changed to the following:

"There was a problem processing your request. - Either an invalid administrator password or an incorrect primary RADIUS server replication secret was provided."

AM-19536 In the Self-Service Console, if you created a new account for a user who is in an external identity source and has an apostrophe (') in the e-mail address, the following error was displayed:

"There was a problem processing your request. Incorrect Data. Kindly check your information"

This was fixed to allow apostrophe (') in the e-mail address.

AM-21324 The manage-replication command line utility displayed an error if you did not use a filename with an absolute file path. You can now use relative paths with the manage-replication command line utility.

AM-22535 Spelling mistake in the error message for license mismatch is corrected to show the following:

com.rsa.license.CustomerLicenseMismatchException: Customer Account Id does not match database entry.

AM-22598 In the RSA Security Console, when you unlock a user account using the context menu on the search window, the user account becomes locked again after a single failed authentication attempt. If you unlock user account from the Edit User page, the user account becomes locked based on the lockout policy.

AM-23028 Starting in SP4 Patch 5, an error occurred when you ran the rsautil manage-secrets command line utility in the **radiusoc/utils** directory.

AM-23359 In RSA Security Console, while redistributing software token, if you change the device type and click Update, the values entered for the fields Disabled, SecurID Pin Set and Force SecurID Pin Change are lost. This was fixed to preserve the values.

AM-23545 If you used the SDK class SearchPrincipalIterativeCommand to search for users stored in an external identity source and assigned to a security subdomain, you received different results depending on the search limit you set.

AM-23659 In the RSA Security Console, the following message displayed in an unexpected page after you successfully assigned an administrative role to a user:

"Sorry, your request cannot be processed at this time. Return to home and try again."

AM-23670 If you used the rsautil manage-database –a create-readonly-user command line utility to create a read-only user in a database, and the password you created for that user contained some special characters, the following error displayed:

"Error: com.rsa.tools.common.ScriptExecutionException: Error when executing the sql script with sqlplus, Done"

AM-23708 In RSA Security Console, some SMTP servers were not responding if you reuse the same SMTP connection for large number of consecutive messages. This was fixed by setting a limit to the number of messages sent over the same connection.

7.1 SP4 P14

Patch 14 contains fixes for the following issues:

AM-12681 Addresses cross frame scripting vulnerability (CVE-2012-2280).

AM-16474 In the RSA Operations Console on the replica instance, the following message displayed when the RSA RADIUS Server Operations Console service was down and you tried to configure the RADIUS server:

"Unable to contact the Primary RADIUS Server."

This message was incorrect. The message was corrected to read as follows:

"The RSA RADIUS Server Operations Console service is down."

AM-17430 The manage-database command line utility "create-readonly-user" failed when the read only user password contained an exclamation point (!). This character is not allowed in database passwords.

AM-21692 Tokencodes failed frequently during authentication, which caused the following error message to display in the authentication activity monitor:

"Passcode reuse or previous token code detected"

AM-22390 In the RSA Security Console, disabled users in an external identity source did not display when you performed an advanced search for disabled users.

AM-22599 If a configured SNMP server hostname could not be resolved and you restarted Authentication Manager services, the Security Console displayed a blank page.

AM-22761 The manage-ssl-certificate command line utility contained incorrect help text.

AM-23361 The patch installer did not check for available free space before it installed the patch. This has been fixed.

AM-23395 If you ran a Token Expiration Report and used the Token Serial Number filter, the output file was incorrect.

AM-23437 In the RSA Security Console, you could not delete a security domain because of leftover attributes from unassigned software tokens from users in the security domain.

AM-23446 Updates the cipher suites to disable weak SSL ciphers for an internal connection to a RADIUS port.

AM-23450 When you attempted to assign a token to a user in an external identity source that had the special character "&" in its base DN, the following error displayed:

"INVALID_DATA is thrown, on SunOne, PRINCIPAL_NOT_FOUND_LDAP"

AM-23452 Addresses the open redirection vulnerability on the RSA Security Console (CVE-2012-2279).

AM-23484, AM-23445 Addresses cross-site scripting vulnerabilities on the RSA Self-Service and Security Consoles (CVE-2012-2278).

AM-23509 On the software token distribution page of the RSA Security Console, the default radio buttons were not pre-selected for administrators assigned the "token administrators" administrator role.

AM-23560 On the provisioning page of the RSA Security Console, a system error displayed when you searched with the filters "userid" or "lastname", and the filter "does not contain".

7.1 SP4 P13

Patch 13 contains fixes for the following issues:

AM-20895 An additional Copy CLU job was created during every time you re-attached a replica instance.

AM-21906 On the Provisioning page in the RSA Security Console, you could not search for pending SecurID enrollment requests using User ID or User Lastname as search criteria.

AM-22969 The PIN re-use policy was not enforced when you used the RSA Software Development Kit (SDK).

AM-23126 In the RSA Security Console, the advanced user search does not work when searching for an identity attribute that is mapped to the internal database.

AM-23232 In the RSA Security Console, self-service provisioning requests did not include the user's first name, unless you had configured the option to edit first names.

AM-23326 The RSA Security Console did not allow connections with the TLS 1.0 protocol on some systems.

AM-23363 When some versions of RSA Authentication Agent for Windows with no node secret set attempted to connect, the host name and IP address of the violating agent were not logged.

AM-23378 In the RSA Security Console, if you downloaded a completed authentication activity report in .csv format and opened it with Microsoft Excel, and the data contains ",", the data in that row will be shifted and does not match column headers.

AM-23434 In SP4 Patch 12, if you installed Authentication Manager in a Windows 2008 R2 64-bit environment, RADIUS services did not restart automatically when you promoted or attached a replica instance.

AM-23453 In the RSA Security Console, a session cookie did not have a secure flag. This was fixed by making the cookie secure.

AM-23475 Authentication Manager patches installed on Windows 2008 SP1, which is an unsupported platform.

AM-23481 The RSA Operations Console allowed a connection via the SSL version 2 protocol if you installed the Authentication Manager SP4 full kit for Red Hat 5 64-bit, Windows Server 2008 64-bit, or appliance with an SP4 factory image.

7.1 SP4 P12

Patch 12 contains fixes for the following issues:

AM-22396 Some UNIX environments had an issue with the **configUtil.sh** tool that caused the script to fail. An error in **configUtil.sh** can cause the RADIUS configuration in the RSA Operations Console to fail.

AM-22937 If a user authenticated with a fixed passcode, Authentication Manager did not return a token serial number to the authentication agent.

AM-23058 The **import-bulk-request** command could not create group membership requests for users in external identity sources to groups located in the internal database. Now, the **import-bulk-request** command can create bulk requests for group membership, but only if all of the user's target groups are in the internal database.

AM-23095 In the RSA Security Console, if you issued a software token to a user, changed the token's device type to "Desktop 4.0" on the **Edit Token** page, and clicked **Update**, the user authentication requirement changed from "Require PIN during authentication" to "Do not require PIN (only tokencode)".

AM-23129 If your authentication method was set as (RSA_Password+SecurID_Native)/(LDAP_Password+SecurID_Native), and you tried to log on to the RSA Security Console and entered the incorrect passcode, the incorrect passcode stayed on the page. Now, the Security Console clears the incorrect passcode and you must enter your passcode again.

AM-23228 The User and User Group Activity report was not limited to the scope of the administrator running the report.

AM-23236 During patch installation, when you used the command line utility to bypass the post-installation scripts execution, the scripts were not copied on the server.

AM-23261 If you installed patch 11 or later and there was already a folder named **RSA_AM_HOME/utils/jvm_backup** in Authentication Manager, then patch installation failed.

AM-23270 Authentication Manager could not log post-installation script execution output. Now, Authentication Manager creates a new file, **RSA_AM_HOME/logs/post-scripts.log**, during patch installation. The file collects all script execution output, including names of executed scripts and output from the database.

AM-23295 In the RSA Security Console, after you installed patch 11, the following error displayed when you tried to access the tokens statistics page:

"The server encountered an unexpected condition which prevented it from fulfilling the request."

Now, the token statistics page displays correctly.

AM-23397 If you installed Patch 11 in a Windows 2008 R2 64-bit environment, starting and stopping RADIUS services, RADIUS promotions, and planned and unplanned promotion, failed.

7.1 SP4 P11

Patch 11 contains fixes for the following issues:

AM-22463 In the RSA Security Console, the report "List all Users with assigned RADIUS profile" failed if it encountered a problem with an Active Directory user.

AM-22521 If you configured groups from more than one identity source to authenticate to the same restricted agent, and one of the identity sources was offline, then authentication failed for users in the other identity source.

AM-22642 In Authentication Manager, some operations failed when they exceeded the maximum message size. The maximum message size was increased.

AM-22736 You could not log on to the RSA Security Console or the RSA Self-Service Console if your authentication method was set to RSA_Password/(LDAP_Password+SecurID_Native).

AM-22755 In the RSA Security Console, you could not edit a user from an external identity source with double-byte characters in their user name or logon ID.

AM-22898 RADIUS migration from Authentication Manager 6.1 to Authentication Manager 7.1 failed if the migration package contained too much data.

AM-22899 Cross-realm (Remote Trust) from Authentication Manager 7.1 to Authentication Manager 6.1 was limited to a single port unless port-range limiting was specified. Now, cross-realm authentication is not limited to single port and uses any available port.

AM-22905 Authentication Manager now cleans up pending threads after completing cross-realm authentication.

AM-22920 Some countries in the GMT+3 time zone did not change their clocks after daylight savings time ended. As a result, they are now in the GMT+4 time zone, on-demand tokencode authentication failed, and incorrect times were logged for servers. This fix updates authentication manager to reflect these changes. This fix does not update your operating system.

AM-22929 RSA services did not start automatically after reboot in a Windows 2008 environment.

AM-22942 Corrects potential Java issues announced by Oracle in October of 2011. 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 October 2011. The update is cumulative, including all previously released fixes for this JRE.

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

AM-22974 Cross-realm authentication requests from Authentication Manager 6.1 to Authentication Manager 7.1 failed when primary realm IP addresses containing uninitialized data were not parsed correctly.

AM-22985 Cross-realm (Remote Trust) authentication failures between Authentication Manager 7.1 and Authentication Manager 6.1 caused by port unavailability for socket connection were not logged in the Authentication Activity Monitor.

AM-22990 In the RSA Security Console, some users did not display when you searched for users across all identity sources.

7.1 SP4 P10

Patch 10 contains fixes for the following issues:

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 APIs 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-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
   ```

   (On UNIX, enter "./" before **rsautil**.)

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
   ```

   (On UNIX, enter "./" before **rsautil**.)

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 PINs. If you used the SDK **API LoginCommand** to handle passcode authentication, user authentication requests failed if they entered their PINs with the incorrect case.

7.1 SP4 P9

Patch 9 contains fixes for the following issues:

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

Patch 8 contains fixes for the following issues:

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-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 user IDs 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 appear:

"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 appears.

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

Patch 7 contains fixes for the following issues:

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 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 plug-in 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.”

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

Patch 6 contains fixes for the following issues:

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

Patch 5 contains fixes for the following issues:

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-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-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.

7.1 SP4 P4

Patch 4 contains fixes for the following issues:

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 appears.

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

Patch 3 contains fixes for the following issues:

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,

"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 CLUs, such as rsautil store, from running. Trailing spaces no longer cause CLUs to fail.

7.1 SP4 P2

Patch 2 contains fixes for the following issues:

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

Patch 1 contains fixes for the following issues:

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" no longer appears.

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
   ```

   (On a UNIX platform, enter **./** before **rsautil**.)
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
```

(On a UNIX platform, enter **./** before **rsautil**.)

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.

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

Trademarks