RSA Authentication Manager Upgrade Process

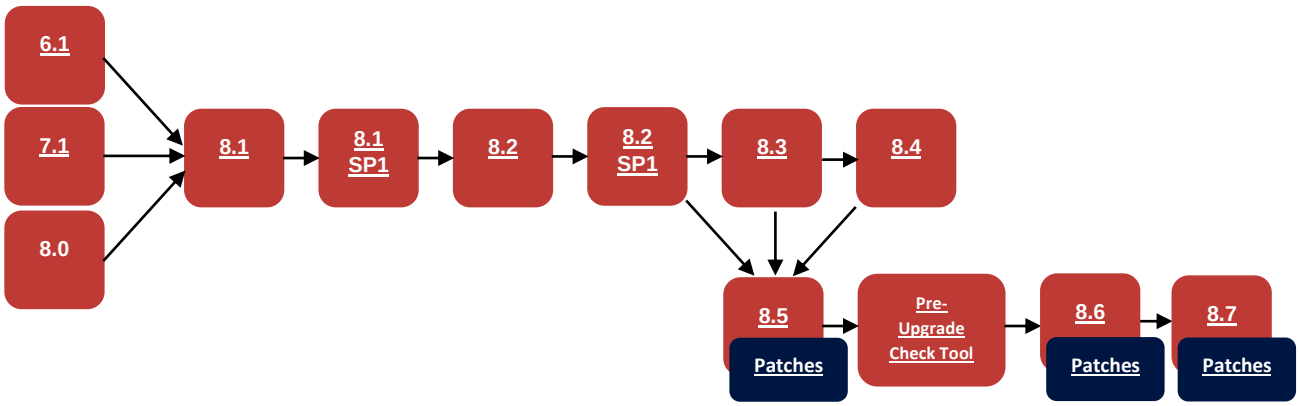
RSA Technical Support

Ahmed Hamza, Ahmed Ezzat, and *Farah Radwan*

Last modified: *January 9, 2023*

Contents

Authentication Manager Upgrade Path



Kindly check the Product Version Life Cycle for SecurID to note the end of support of each version.

Upgrade Example (from V8.2 to V8.7 P2):

In case of having one primary and one replica (both at the same version 8.2), upgrade one instance at a time, starting with the primary, then upgrade the replica to always be on the same version as the primary; therefore, the upgrade path will be as follows:

8.2 Primary > 8.2 SP1 Primary > 8.2 SP1 Replica > 8.5 Primary > 8.5 Replica > Run the Pre-Migration Script on the Primary instance > 8.6 Primary > 8.6 Replica > 8.7 Primary > 8.7 Replica > 8.7 P2 Primary > 8.7 P2 Replica

Note that you can upgrade from V8.2 SP1, V8.3, or V8.4, **directly to V8.5**.

Notes:

- For a smooth upgrade process and to avoid any service disruption, before upgrading any of the RSA Authentication Manager instances,
  - It is essential to check and follow the Pre-Upgrade Steps.
  - Make sure to follow the above RSA AM Upgrade Path.

Pre-Upgrade Steps

1. Take a Back-up/Virtual Machine Snapshot

- In case of a **hardware/virtual appliance**, take a backup of the AM database:

Procedure

1. In the Operations Console of the primary instance, click **Maintenance** > **Backup and Restore** > **Back Up Now**.

2. In the **Backup Name** field, accept the default name, or replace it with a backup name of your own.

   The default name consists of a timestamp and this extension: RSAbackup. The timestamp uses the following format: **YYYYMMDDHHMM**.

   In the default name **202208251230.RSAbackup**, for example, 2022 is the year, 08 is the month, 25 is the day, 12 is the hour, and 30 is the minute when the backup was created.

   If you replace the default filename, your name must use this extension: RSAbackup. This extension is case-sensitive.

3. In the **Backup Password** field, enter a valid password, and enter the same password in the **Confirm Backup Password** field.
   Note: carefully the backup password you specify. You need this password to restore the deployment.

4. Under **Backup Location**, do one of the following:
   - Select **Local Authentication Manager Server**. The backup is saved on the appliance in the directory **/opt/rsa/am/backup**.

   - Select **Windows Shared Folder**.
     - In the **Windows Shared Folder** field, enter the path to an existing Windows shared folder, for example, **\\primary.company.net\backup_path**.
     - If the shared folder requires a username, enter the username in the **Folder Username** field, for example, **Domain1\User1**.
     - If the shared folder requires a password, enter the password in the **Folder Password** field, for example, password1.

   - **Select NFS (Network File System) Shared Folder**. In the **NFS Shared Folder field**, enter the path to an NFS server and file directory, for example, **fileserver.company.net:/backup path**.

5. Click **Backup**.
   The Progress Monitor page displays the backup progress.

6. Click **Done** when the backup process completes.

- In case of a **hardware appliance**, use Clonezilla to backup and restore the RSA Authentication Manager 8.4 or later on the following models:
  - RSA SecurID Appliance 130 (Dell PowerEdge R230)
  - RSA SecurID Appliance 230 (Dell PowerEdge R240)
  - RSA SecurID Appliance 250 (Dell PowerEdge R630)
  - RSA SecurID Appliance 350 (Dell PowerEdge R640)
  - RSA SecurID Appliance 130 (Intel)

- In case of a **virtual appliance**, take a snapshot of each virtual machine in the deployment. When taking a snapshot of an Authentication Manager instance, the following settings must be specified:
  - Do not save the virtual machine's memory.
  - Choose the option to quiesce the guest file system to pause the running processes on the Authentication Manager instance.

2. Check the Replication Status

If you have replicated deployments, all replica instances must be running, replicating **successfully**, and are able to communicate when the upgrade is applied.

- From the primary instance **Operations Console**, click **Deployment Configuration** > **Instances** > **Status Report**.
- If a replication error occurs, you can download log files from Operations Console, click **Administration** > **Download Troubleshooting Files**, and contact RSA Support.

Note: It is preferable to have at least one replica up and running to handle the authentication during the upgrade process to avoid down time.

3. Check the Disk Space

- It is recommended that the free disk space is equal to the size of the current AM, plus 4 GB.
- For example, if the current database is 1 GB, you need 5 GB of free disk space. To determine the current size of the AM DB, run the below command:
  du -h --max-depth=0 /opt/rsa/am/rsapgdata

4. Check the Expiration Date of the Console Certificate(s) for each AM Instance

a. Login to the **Operations Console** of each AM instance.
b. Click on **Deployment Configuration** > **Certificates** > **Console Certificate Management.**

5. Check Port 8443/TCP

- Make sure that **port 8443/TCP** is **open for https traffic**.
- During a product update, the appliance opens this port in its internal firewall. The appliance closes this port when the update is complete.
- If an **external firewall blocks this port**, the browser displays an **inaccessible** or **blank web page**, but the update can successfully complete.

Upgrading the Authentication Manager

1. Specify the Product Update Source/Location

To allow RSA Authentication Manager to locate product updates, you must specify the location where updates are stored. Updates can be applied through your local browser, or you can store updates in an NFS share, Windows shared folder, a DVD/CD, or an ISO image on your client machine.

Before you begin

- Download the Authentication Manager upgrade file(s).
- If you intend to scan for updates on an RSA-supplied DVD or CD, do the following:
  - On a hardware appliance, use the DVD/CD drive or mount an ISO image.
  - On a virtual appliance, you must configure the virtual appliance to mount a DVD/CD or an ISO image. For information, see Hyper-V DVD/CD or ISO Image Mounting Guidelines or VMware DVD/CD or ISO Image Mounting Guidelines.

Procedure

1. In the Operations Console of the primary instance, click **Maintenance** > **Update & Rollback**.

2. On the **Update & Rollback** page, the default update source is your local browser. To change that setting, click **Configure Update Source**.

3. On the Configure Update Sources page, specify a location for updates.

   - To apply a specific update from your local machine, select **Use your web browser to upload an update**. You do not need to scan for updates.

   - If you want to scan for updates on an NFS share, select **Use NFS as the update source**. Enter the full path, including the IP address or hostname where updates are stored. For example: **192.168.1.2:/updates**

   - If you want to scan for updates on a Windows shared folder, select **Use Windows Share** as the update source.

     - In the **Windows Share Path** field, enter the full path, including the IP address or hostname where updates are stored. For example: **\\192.168.1.2\updates**
     - (Optional) In the **Windows Username** field, enter a username.
     - (Optional) In the **Windows Password** field, enter a password only if it is required by your Windows share configuration.

   - To scan for updates on an RSA-supplied DVD or CD, select **Use DVD/CD as the update source**.

4. To test the NFS or Windows share directory settings, click **Test Connection**. A message indicates whether the configured shared directory is available to the primary or replica instance.

5. Click **Save**.

2. Scan for Product Updates

- If you have configured an NFS share, a Windows shared directory or a DVD/CD as an update location, then you can scan for product updates. If you want to apply an update through your local web browser, then you do not need to scan for updates.

- Before you apply an update to an instance, you can review a list of available updates and a list of the updates that were applied. After you apply an update, the Authentication Manager removes the update from the **Available Updates** section and moves it to the **Update History** section.

- After you scan for updates, the new list displays for 24 hours. Logging out of the Operations Console does not remove the list from the system cache. If you restart the Operations Console, download additional updates, or change the product update locations, you must perform another scan to see the most current list.

Procedure

1. In the Operations Console of the primary instance, click **Maintenance** > **Update & Rollback**.

2. Click **Scan for Updates**. The system displays the progress of the scan on the **Basic Status View** tab. Detailed information displays on the **Advanced Status View** tab.

3. Click **Done** to return to the Update & Rollback page.

   The **Available Updates** section displays the following information for each update:

   - **Version**. The version of the update. To see the current Authentication Manager version, see the top of the Update and Rollback page.

   - **Reversible**. Indicates whether you can roll back (undo) the update.

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

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

   - **Action**. States whether the update is available to apply. Lists the minimum system requirement for the update.

4. In the **Applied Updates** section, click **Download Detailed History** Log for a complete update history.

   The **Applied Updates** section displays the updates applied to the instance. This section includes the update version numbers, the time and date that each update was applied, and who applied the update.

3. Apply Product Updates

You must apply updates to the primary instance before you apply updates to the replica instances.

Procedure

1. In the Operations Console of the primary instance, click **Maintenance** > **Update & Rollback**.
2. RSA recommends applying the most recent update.

   If you want to apply an update through your local web browser, do the following:

   a. Click **Upload & Apply**. Because browser uploads require additional processing, the Upload & Apply window may open slowly.

   b. Click **Choose File** to navigate to the location of the update. You cannot type the update location in the **Update Path** field.

   c. Click **Upload**.

   d. Verify the updated details and click **Apply**.

   If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, do the following:

   a. Click **Scan for Updates**. **Available Updates** displays all of the updates that can be applied.

   b. Next to the update that you want to apply, click **Apply Update**.

   c. Click **Confirm** to apply the update.
3. If prompted, enter the password for the operating system user **rsaadmin**, and click **Apply**.
4. (Optional) The basic status messages are displayed while the update is being applied. You can click the **Advanced Status View** tab to display detailed log messages.
5. If the update requires the system to restart the Operations Console or the appliance after the update is applied, the Operations Console or appliance automatically restarts. When the restart is complete, click **Done**.
6. The update is listed in the **Applied Updates** section. To save the high-level update history, click **Download Detailed History Log**.

4. Re-install the Web Tier

- If a Web Tier exists, it needs to be reinstalled **once all the Authentication Manager upgrades are completed**. (i.e., when upgrading the Authentication Manager from V8.5 to 8.7, wait until all the Authentication Manager instances are upgraded to V8.7, then install Web Tier V8.7)

- After uninstalling the Web Tier, you must **manually** check and delete any remaining files or folder in the Web-tier installation folder/directory.

- For more information, refer to the Web Tier Getting Started guide.

Note: there is **no upgrade path** for the web tier which means that if the RSA instance was on version 8.2 and you upgraded it to 8.7 P2, you will need to uninstall the web tier version 8.2 and install 8.7 P2 version on the web tier.

5. Re-install the Administration SDK

- If the Administration SDK is being used, it needs to be reinstalled **once all the Authentication Manager upgrades are completed**.

- For more information, refer to the Configure RSA Authentication Manager 8.x software developer kit (SDK) article.

Note:

- The **Authentication API** will not be affected by upgrading the RSA Instances from one version/patch to another.
- The **ADMIN SDK** is based on the **major versions only** which means that if your current version of the primary instance is 8.6 and
  - You applied patch 4, you DO NOT need to re-install the ADMIN SDK.
  - You applied the upgrade for 8.7 P2, you will need to download and re-install the new ADMIN SDK found in the extras folder of the base version (in this case will be the 8.7 extras folder).

Post-Upgrade

- You can download the detailed log file that contains the information that was displayed on the Advanced Status View tab.

- Check the **Replication Status Report** for each replica instance in the deployment:
    a. Login to the **Operations Console** of the primary instance.
    b. Navigate to **Deployment Configuration.**
    c. Click on **Instances.**
    d. Click on **Status Report**.

- Verify the **RADIUS Replication:**
    a. Login to the **Security Console** of the primary instance.
    b. Navigate to **RADIUS**.
    c. Click on **RADIUS Servers**.

Downloads & Documentation

- **Migration Document from V6.1 to V8.1:**
  - Download Migration from V6.1 to 8.1.

- **Migration Document from V7.1 to V8.1:**
  - Download Migration from V7.1 to 8.1.

- **Authentication Manager V8.1:**
  - Download AM V8.1 upgrade file.
  - Click here for the upgrade procedure.

- **Authentication Manager V8.1 SP1:**
  - Download AM V8.1 SP1 upgrade file.
  - Click here for the upgrade procedure.

- **Authentication Manager V8.2:**
  - Download AM V8.2 upgrade file.
  - Click here for the upgrade procedure.

- **Authentication Manager V8.2 SP1:**
  - Download AM V8.2 SP1 upgrade file.
  - Click here for the upgrade procedure.

- **Authentication Manager V8.3:**
  - Download AM V8.3 upgrade file.
  - Click here for the upgrade procedure.

- **Authentication Manager V8.4:**
  - Download AM V8.4 upgrade file.
  - Click here for the upgrade procedure.

- **Authentication Manager V8.5 and Patches:**
  - Download AM upgrade file: V8.5, V8.5 P1, V8.5 P2, V8.5 P3, V8.5 P4, V8.5 P5
  - Click here for the upgrade procedure.
  - Download Web Tier: V8.5, V8.5 P1, V8.5 P2, V8.5 P3, V8.5 P4, V8.5 P5
  - Re-install the Web-Tier.
  - Download RSA AM SDK (if you are using ADMIN SDK), download RSA Authentication Manager 8.5 – Extras
  - For the new features, enhancements, and defects fixed in each version, refer to the readme and release notes for AM: V8.5, V8.5 P1, V8.5 P2, V8.5 P3, V8.5 P4, V8.5 P5
  - AM V8.5 Known Issues.

- **Guides:**
  - V8.5 Setup and Configuration Guide
  - V8.5 Administrator's Guide

- **Pre-upgrade Check Tool:**

  Warning: You must run the RSA Authentication Manager 8.6 Pre-Upgrade Check Tool (download | readme) before upgrading to Authentication Manager 8.6, whether you use RADIUS or not. Failure to complete this task will result in losing the ability to manage RADIUS **and** may result in corruption of the Authentication Manager instance.

- **Authentication Manager V8.6 and Patches:**
  - Download AM upgrade file: V8.6, V8.6 P1, V8.6 P2, V8.6 P3, V8.6 P4
  - Click here for the upgrade procedure.
  - Download Web Tier: V8.6, V8.6 P1, V8.6 P2, V8.6 P3, V8.6 P4
  - Re-install the Web-tier.
  - Download RSA AM SDK (if you are using ADMIN SDK), download RSA Authentication Manager 8.6 – Extras

  - For the new features, enhancements, and defects fixed in each version, refer to the readme and release notes for AM: V8.6, V8.6 P1, V8.6 P2, V8.6 P3, V8.6 P4
  - AM V8.6 Known Issues.

  - **Guides:**
    - V8.6 Setup and Configuration Guide
    - V8.6 Administrator's Guide

  - **Note:**
    Authentication Manager V8.5, **with or without patches,** can be upgraded directly to V8.6, **only after running the Pre-upgrade Check tool.**

- **Authentication Manager V8.7 and Patches:**
  - Download AM upgrade file: V8.7, V8.7 P1, V8.7 P2.
  - Click here for the upgrade procedure.
  - Download Web Tier: V8.7, V8.7 P1, V8.7 P2.
  - Re-install the Web-tier.
  - Download RSA AM SDK (if you are using ADMIN SDK), download Authentication Manager 8.7 – Extras

  - For the new features, enhancements, and defects fixed in each version, refer to the readme and release notes for AM: V8.7, V8.7 P1, V8.7 P2
  - AM V8.7 Known Issues.

- **Guides:**
  - V8.7 Setup and Configuration Guide
  - V8.7 Administrator's Guide

- **Notes:**

a. Authentication Manager V8.6, **with or without patches,** can be upgraded directly to V8.7.
b. AM V8.7 includes **ONLY** the fixes for 8.6 P1 and **DOES NOT** include the fixes for V8.6 P2, 3 and 4. It is advised to upgrade to, at least, V8.7 P1 which contains the fixes for **ALL** the previous versions and patches.

Important Notes:

a. **Technical Support team** is a **break/fix** team that will only engage in case of upgrade-failure.
   i. To troubleshoot the upgrade-failure issue, kindly open a support case or call the support phone numbers to open a case for you.
   ii. **After the Upgrade Failure:**
      - In case you **have access** to the Operations Console, download the detailed Troubleshooting log files that contains the information that was displayed on the Advanced Status View tab and attach it to the case.

      - In case you do **NOT have access** to the Operations Console, follow the below steps to get the upgrade logs from the server itself using **WinSCP** or any transfer file protocol:
        a. Navigate to **/opt/rsa/am/server/logs** directory.
        b. Copy the upgrade file (***update-8.x.x.x.x-buildxxxx-YYYYMMDDhhmm.log***) to the desktop.

   iii. Upload the Troubleshooting logs to RSA SFTP Server.

b. If RSA's assistance is needed during the **whole upgrade process**, kindly contact the Sales Representative/Account Manager to engage the **Professional Services team**.


RSA