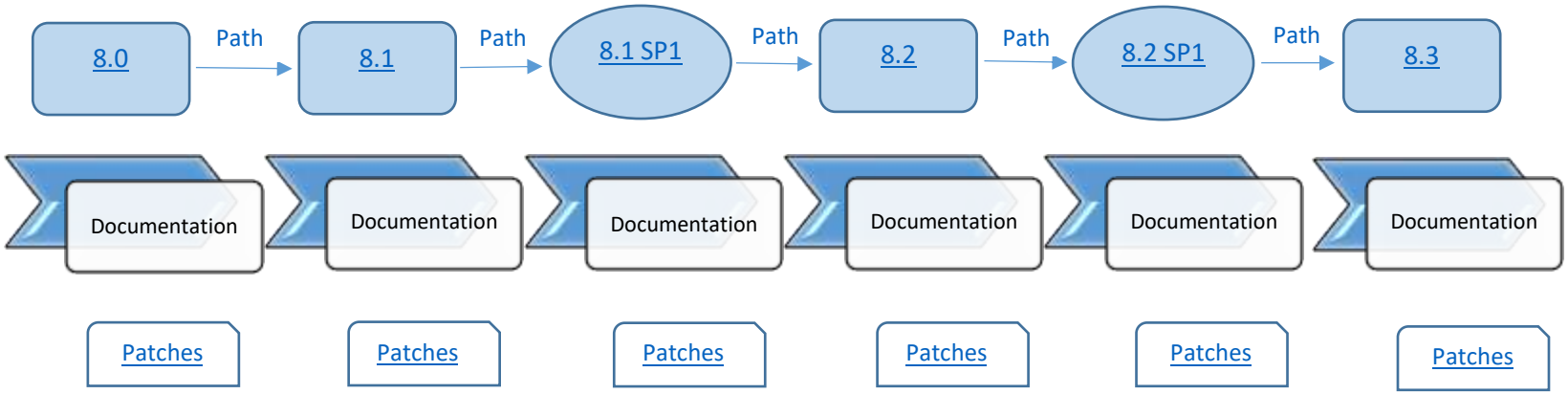
Authentication Manager Upgrade path



Pre-upgrade steps:

- Backup strongly recommended

  A-If you deployed a hardware appliance or a virtual appliance, you can back up the AM database. Use the Back Up Now feature in the Operations Console of the primary instance. See the Help topic

  "Create a Backup using Back Up Now."

  B-If you deployed a hardware appliance, RSA recommends using standard system disk imaging software to create a backup image in case you need to restore the hardware appliance.

  C-If you deployed a VMware virtual appliance, you can take a snapshot of each virtual machine in the deployment. When you take a snapshot of an Authentication Manager instance, you must specify the following settings:

  -Do not save the virtual machine's memory.
  -choose the option to quiesce the guest file system in order to pause the running processes on
  The Authentication Manager instance.

- Prepare the credentials for the rsaadmin user account and the Operations Console administrator account
- If you have replicated deployments, all replica instances must be running and replicating successfully and are able to communicate when the upgrade is applied.
- Make sure that the free disk space is equal to the size of the current AM plus 4 GB,
  For example, if the current db is 1 GB, you need 5 GB of free disk space.
  To determine the current size of the AM DB, run the below command:
  dua –h –d 0 /opt/rsa/am/rsapgdata
- Download the patch (source) to a location that a primary or replica instances can access.

Upgrade steps:

- In the Operations Console, click Maintenance > Update & Rollback.
- RSA recommends applying the most recent update. Do one of the following, depending on your Configuration:

To apply an update through your local web browser, do the following:

a. Click Upload & Apply Update.
b. Click Browse to navigate to the location of the update. You cannot type the update Location in the Update Path field.
c. Click Upload.
d. Verify the update details, and click Apply.

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

a. Click Scan for Updates. Available Updates displays all of the updates that can be applied.
b. Next to the update to apply, click Apply Update.
c. Click Confirm to apply the update.

- Authentication Manager moves the update from the Available Updates section to the Applied Updates Section.
- The Operations Console or Appliance automatically restarts. When the restart is complete, click done.
- When you return to the Update & Rollback page, the update is listed in the Applied Updates section.

To save the high-level update history, click Download Detailed History Log.

- The software version information is updated with the patch number. To view the software version Information, log on to the Security Console, and click Software Version Information.

NB: ***Apply the upgrade patch to the primary instance first then to each replica instance (as each replica instance is updated, all of the accumulated data on each replica instance is sent to primary instance)***

Post Upgrade steps

- You can download the detailed log file that contains the information that was displayed on the Advanced Status View tab
- Verify that the replication and radius replication is functioning correctly on the primary instance and the replica instance

Upgrading from 8.0 to 8.1

- RSA AM 8.0 with or without patches can be upgraded to version 8.1
- If you have applied patches 5,6,7 or 8 to version 8.0, then you should apply 8.1 SP1 after upgrading, version 8.1 SP1 includes the SW fixes in the version 8.0 patches 5 through 8
- Re-install the Web Tier

Upgrading from 8.1 to 8.1 SP1

- You can apply SP 1 to RSA AM 8.1 with or without patches
- The RSA Authentication Manager 8.1 SP1 ZIP file contains the following:
    - RSA AM 8.1 SP1 1 ISO file (am-update-8.1.1.0.0.iso)
    - RSA Authentication Manager 7.1 Migration Export Utility, if you plan to perform a migration from version 7.1
- If you deployed HW appliance or VMware virtual appliance, you can back up the version 8.1 DB,
- Use the Back Up Now feature in the Operations Console of the primary instance
- Update the Web tier

Upgrading from 8.1 SP1 to 8.2

- You can apply RSA AM 8.2 to any hardware appliance or virtual appliance that has the RSA AM 8.1 SP1 software
- The RSA Authentication Manager 8.2 ZIP file, am-update-8.2.0.0.0.zip, contains the RSA Authentication Manager 8.2 ISO file, am-update-8.2.0.0.0.iso, that is used to apply version 8.2 to Authentication Manager
- AM 8.2 includes a custom SSH banner, if you deployed a custom SSH banner for an earlier version, you must have a copy of the sshd_config file from /etc/ssh directory, so you can restore it after the upgrade is complete
- MD5 are no longer supported for identity sources, AM only connects to identity sources that use SHA-1 Or SHA-2 certificates. *See the Help topics "Delete an Identity Source SSL Certificate" and "Add an Identity Source SSL Certificate."*

Upgrading from 8.2 to 8.2 SP1

- You can apply RSA AM 8.2 SP1 upgrade patch to any HW appliance or virtual appliance that has RSA AM 8.2 SW
- The RSA Authentication Manager 8.2 SP1 ZIP file, **am-update-8.2.1.0.0.zip**, contains the RSA Authentication Manager 8.2 SP1 ISO file, **am-update-8.2.1.0.0.iso**, that is used to apply version 8.2 SP1 to Authentication Manager

Upgrading from 8.2 SP1 to 8.3

- You can apply RSA AM 8.3 upgrade patch to any HW appliance or virtual appliance that has RSA AM 8.2 SP1 SW
- The RSA Authentication Manager 8.3 ZIP file, **am-update-8.3.0.0.0.zip**, contains the RSA Authentication Manager 8.3 ISO file, **am-update-8.3.0.0.0.iso**, that is used to apply version 8.3 to Authentication Manager
- Re-install the Web Tier
- If AM is on Intel Hardware, please go through this article first https://community.rsa.com/docs/DOC-86959 And apply the hot fix.

Notes:

1-RSA AM upgrade is not handled by Customer Support, however we support post upgrade issues,
You can contact your account manager to engage RSA consultant for AM upgrades

2-If you faced any issues during the upgrade please call RSA technical support:

EMEA: Tel: +44 1344 781100 | US: 800-995-5095| AP: +800 7221 7221

3-Please go through the known issues document before AM upgrade

4-You can subscribe to "Product Advisory" to be aware of announcements of upcoming releases, patches and service packs https:/community.rsa.com/docs/DOC-81286

5-To create RSA Community account:

- Please go to https://community.rsa.com and click "Register" (in red, under the Search bar). Depending on the product you have, you will need to have your License Key/Serial Number/Contract Number or Site ID available to register successfully. Enter the required information and click "CONTINUE."
- To your company's product information: https://community.rsa.com/docs/DOC-40338
- Once the form is completed, you will be prompted to set up your security questions and On-Demand Authentication. After this is successfully completed, you will receive an email with a login link

6-For https://knowledge.rsasecurity.com downloads, please follow this URL:

- https://community.rsa.com/docs/DOC-65190