RSA® Authentication Manager 8.3 Hardware Appliance Getting Started

Welcome

Thank you for purchasing RSA® Authentication Manager 8.3 the world's leading two-factor authentication solution. This document describes how to deploy the RSA Authentication Manager hardware appliance.

Step 1: Prepare for Deployment

A: Verify the Package Contents

Refer to the packing list that is included with the appliance to verify that your package contains the listed items.

B: Download the License File

Download the license file (.zip) from RSA Download Central at **https://download.rsasecurity.com**. Do not unzip the file.

Use the credentials that RSA e-mailed to you to log on to the site and download the license file. If you did not receive an e-mail with the logon credentials, contact the License Seed Response Team by sending an e-mail with your contact information and license serial number (provided in your order confirmation) to the regional address for your area listed below:

- Americas: license_seed_response@rsa.com
- EMEA: support@rsa.com
- Asia Pacific: support@rsa.com

Before running Quick Setup for the primary appliance, locate the license file, and make sure it is accessible to the browser that is used to run the primary appliance Quick Setup. RSA recommends that you store the license file in a protected location that is available only to authorized administrative personnel.

C: Locate the Documentation Set

The documentation set is available on RSA Link at **https://community.rsa.com/community/products/securid**. RSA recommends that you store the user documentation in a network location that your administrators can access.

D: Read the Release Notes

Locate the *Release Notes* on RSA Link at **https://community.rsa.com/community/products/securid**. The *Release Notes* provide important information about this release, as well as workarounds for known issues.

E: Verify Your Web Browser Allows JavaScript and Cookies

Authentication Manager is managed through a web-based interface. Your supported web browser must allow JavaScript and cookies. For more information, see the *Setup and Configuration Guide*.

Step 2: Deploy the Appliance

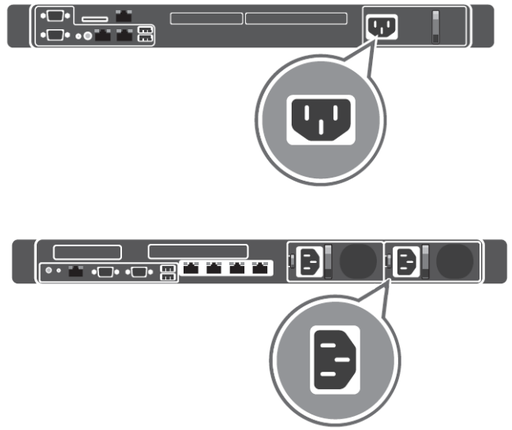
Follow these instructions to deploy the appliance.

Before You Begin

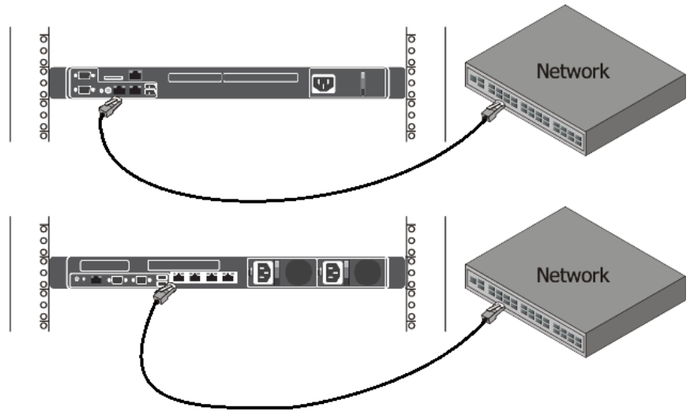
- Make sure that you have a keyboard and monitor.
- Collect the IPv4 network setting information.

Procedure

1. Connect a keyboard and monitor to the appliance.
2. Connect the power cord to the appliance.



3. Power on the appliance. When the appliance boot screen displays, select **Start RSA Authentication Manager** and press ENTER, or wait 10 seconds for Authentication Manager to load automatically.
   Do not use the F2 or F4 function key options that display on the boot screen.
4. By default, the keyboard is configured for **English (United States)**.To retain this setting, wait 30 seconds. To configure a new language, press any key, type the number that is associated with the language you want to configure, and press ENTER.
5. When prompted, configure the following network settings for the appliance:
   - Fully Qualified Hostname
   - IP Address
   - Subnet Mask
   - Default Gateway
   - (Optional) Primary DNS Server
   - (Optional) Secondary DNS Server
6. When prompted to confirm the network settings, verify the settings are correct. To accept the settings, type **y**.
7. Record the Quick Setup URL and the Quick Setup Access Code when they are displayed. This information is required to configure your appliance as an Authentication Manager instance.
8. If you have not done so already, connect the appliance to the network.



Next Step

RSA strongly recommends creating a backup image of the hardware appliance in case you need to restore the original settings. RSA has qualified PING. For more information, see "Using PING to Back Up and Restore the RSA Authentication Manager 8.2.x Hardware Appliance" on RSA Link at **https://community.rsa.com/docs/DOC-41697**.

RSA supports using an integrated Dell Remote Access Controller (iDRAC) to remotely restore the original system image to the hardware appliance. For more information, see "Configuring Remote Access to the RSA Authentication Manager Hardware Appliance" on RSA Link at **https://community.rsa.com/docs/DOC-67160**.

Step 3: Set Up the Primary Instance

Quick Setup configures the appliance as the primary instance.

Before You Begin

- Copy the license file into a location that is accessible to the web browser that is used to run the primary appliance Quick Setup.

  Note: Do not unzip the file.

- Understand that the following administrative accounts are creating during Quick Setup:
  - **Super Admin.** Super Admins can perform all Authentication Manager administrative tasks. Any Super Admin can create a new administrator in the Security Console.
  - **Operations Console administrator.** Operations Console administrators can perform administrative tasks in the Operations Console.
  - **Appliance Operating System Administrator.** Use the **rsaadmin** account if you need to access the appliance operating system for advanced maintenance or troubleshooting tasks.

  For more information, see the appendix "Administrative Accounts" in the *Setup and Configuration Guide*.

RSA® Authentication Manager 8.3 Hardware Appliance Getting Started

Procedure

1. Open a web browser and go to the following URL to launch Quick Setup:
   https://<*IP Address*>/
   where <*IP Address*> is the IP address of the appliance.
   If your web browser is configured for an enhanced security level, a warning states that this URL is not on the list of allowed or trusted sites. To continue, click the option that your browser presents that allows you to connect to an untrusted site. For example, your browser might ask you to click a link that reads "I Understand the Risks."
2. When prompted, enter the Quick Setup Access Code, and click **Next**.
3. Read the End User License Agreement (EULA). Click **Accept**.
4. Click **Start Primary Quick Setup**. Follow the instructions on each screen to complete Quick Setup.
   Record all of the passwords to the administrative accounts that you create during Quick Setup.
   The operating system password is required to access the appliance for advanced maintenance or troubleshooting tasks. For security reasons, RSA does not provide a utility for recovering the operating system password.
5. After the instance is configured, you can click the Security Console or Operations Console URL links to open these consoles. These URL links require a fully qualified domain name (FQDN).

   Note: The fully qualified domain name must resolve to your appliance. If you are having trouble connecting to the consoles, verify the DNS configuration.

   The first time you access the Security Console or the Operations Console, a warning appears because the default self-signed certificate created after Quick Setup is not trusted by your browser.
6. Accept the certificate to access the console and prevent the warning from appearing again. For more information, see the chapter "Deploying a Primary Appliance" in the *Setup and Configuration Guide*.
7. (Optional) You can download a text file that contains the network settings for the primary instance. You can refer to this information if you need to restore the original system image on the hardware appliance. For instructions, see the Help topic "Download Network Settings for a Primary or Replica Instance."

Logging On to the Consoles

After you have completed Quick Setup, you can use the following links to access a console. To view a complete list of URLs that are available for the consoles, see the *Setup and Configuration Guide*.

Console	URL
Security Console	https://<*fully qualified domain name*>/sc
Operations Console	https://<*fully qualified domain name*>/oc
Self-Service Console	If there is no web tier, enter: https://<*fully qualified domain name*>/ssc After installing a web tier, enter: https://<*fully qualified virtual host name*>/ssc If you change the default load balancer port, enter: https://<*fully qualified virtual host name*>:<*virtual host port*>/ssc

If your web browser is configured for an enhanced security level, add the URL for each console to the list of allowed or trusted sites. See your browser documentation for instructions.

To access the Security Console, enter the Super Admin User ID and password that you specified during Quick Setup. To access the Operations Console, enter the Operations Console user ID and password that were entered during Quick Setup.

Step 4: Set Up a Replica Instance

After you configure the primary instance, you can deploy another appliance and set up a replica instance.

Keep the appliance on a trusted network until Quick Setup is complete. The client computer and browser used to run Quick Setup should also be on a trusted network.

Before You Begin

A primary instance must be deployed on the network.

Procedure

1. On the primary instance, log on to the Operations Console, and click **Deployment Configuration** > **Instances** > **Generate Replica Package**. For instructions, see the Help topic "Generate a Replica Package."
2. Deploy the appliance. For instructions, see Step 2: Deploy the Appliance.
3. Open a browser and go to the following URL to launch Quick Setup:
   https://<*IP Address*>/
   where <*IP Address*> is the IP address of the replica appliance.
   If your web browser is configured for an enhanced security level, a warning states that this URL is not on the list of allowed or trusted sites. To continue, click the option that allows your browser to connect to an untrusted site.
4. When prompted, enter the Quick Setup Access Code, and click **Next**.
5. Read the End User License Agreement (EULA). Click **Accept**.
6. Click **Start Replica Quick Setup**. Follow the instructions on each screen to complete Quick Setup.
   Record the operating system password that is created during Quick Setup.
   The operating system password is required to access the appliance for advanced maintenance or troubleshooting tasks. For security reasons, RSA does not provide a utility for recovering the operating system password.
7. After the instance is configured, do one of the following:
   - Click **Begin Attach** to attach the replica instance to the primary instance.
   - Click **Defer Attach** to attach the replica instance at another time. When prompted, confirm your choice. The replica instance powers off. You can attach the replica instance the next time you power on the appliance.

   For instructions, see the Help topic "Attach the Replica Instance to the Primary Instance."
8. (Optional) You can download a text file that contains the network settings for the replica instance. You can refer to this information if you need to restore the original system image on the hardware appliance. For instructions, see the Help topic "Download Network Settings for a Primary or Replica Instance."

Web Tier Installation

Web tiers are not required, but your deployment might need them to satisfy your network configuration and requirements. Authentication Manager includes services, such as risk-based authentication, dynamic seed provisioning, and the Self-Service Console, that may be required by users outside of your corporate network. If your network includes a DMZ, you can use a web tier to deploy these services inside the DMZ. For more information, see the chapter "Planning Your Deployment" in the *Planning Guide*.

Next Steps

After setting up the appliance, consider which of the following tasks you want to perform for the Authentication Manager deployment. You must perform all post-setup tasks on the primary instance.

Task	Help Topic on RSA Link at https://community.rsa.com/community/products/securid/securid-access
Add Authentication Manager users	To add users to the internal database, see "RSA Authentication Manager Users." To link external identity sources, see "RSA Authentication Manager Identity Sources."
Assign authentication policies	"RSA Authentication Manager Policies."
Import tokens and assign users	"RSA SecurID Tokens."
Set up risk-based authentication	"Risk-Based Authentication."
Set up on-demand authentication	"On-Demand Authentication."
Configure end-user Self-Service for maintenance and troubleshooting.	"RSA Self-Service Overview."

Support and Service

You can access community and support information on RSA Link at **https://community.rsa.com**. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at **www.rsaready.com** provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

January 2018

P/N R300-000-006

P/N: RSA-509-5700-01 REV: 0A