SecurID

RSA® Authentication Manager 8.7 Hardware Appliance Getting Started

Welcome

Thank you for purchasing RSA® Authentication Manager 8.7.

Step 1: Prepare for Deployment

A: Download the License File

Download the license file (.zip) from https://my.rsa.com. Do not unzip the file.

Note: RSA recommends that you store the license file in a protected location that is available only to authorized administrative personnel.

B: Plan Your Depolyment and Meet the Prerequisites

See the documentation on RSA Link. Read the *Release Notes*.

Read the *Planning Guide* for deployment considerations. For example, if users outside of your network require access to resources, you might want to deploy a web tier.

Meet the prerequisites described in the *Setup and Configuration Guide*.

Step 2: Deploy the Appliance

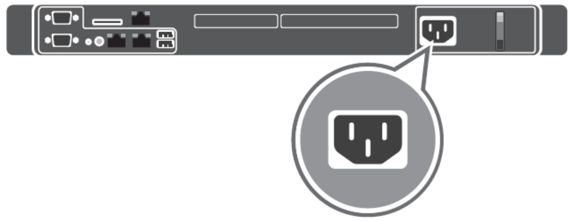
Follow these instructions to deploy the appliance.

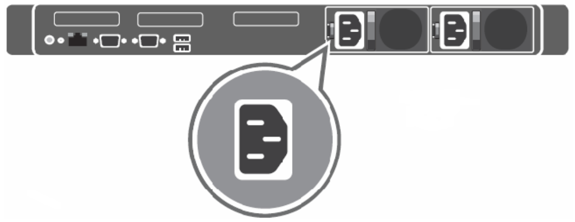
Before You Begin

- Make sure that you have a keyboard, a monitor, and an ethernet cable.
- Collect the IPv4 network setting information. Identify the fully qualified domain name and static IP address for the appliance, the subnet mask and default gateway, and the IP address or hostname of the DNS servers in the network.

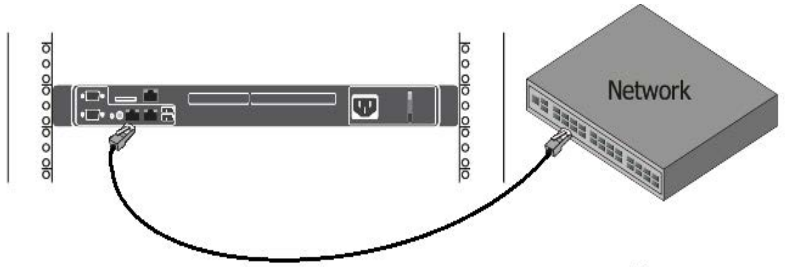
Procedure

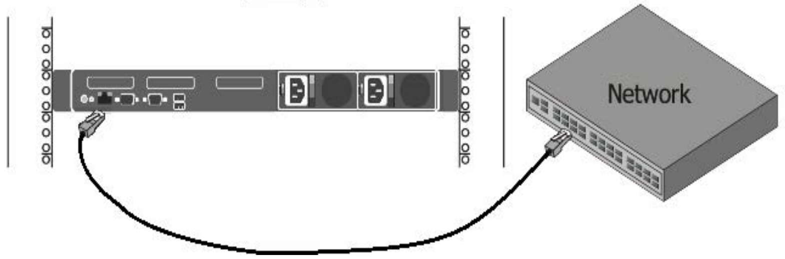
1. Connect a keyboard and monitor to the appliance.
2. Connect an active ethernet link. The hardware appliance does not need to be on the final destination network. You can connect it to any isolated switch or hub.
3. Connect the power cord to the appliance.





4. Power on the appliance. On the appliance boot screen, select **Start RSA Authentication Manager** and press ENTER, or wait for Authentication Manager to load automatically.
   Do not use the F2 or F4 function key options that display on the boot screen.
5. By default, the keyboard is configured for **English (United States)**. You can retain this setting or select a new language.
6. Configure the network settings for the appliance:
   - Fully Qualified Hostname
   - IP Address
   - Subnet Mask
   - Default Gateway
   - (Optional) Primary DNS Server and Secondary DNS Server
7. Verify the settings are correct. To accept the settings, type **y**.
8. Record the Quick Setup URL and the Quick Setup Access Code. This information is required to configure your appliance as an Authentication Manager instance.
9. If you have not done so already, connect the appliance to the final destination network.





Next Steps

RSA strongly recommends creating a backup image of the hardware appliance in case you need to restore the original settings. RSA has qualified Clonezilla. For more information, see Using Clonezilla to Back Up and Restore the RSA Authentication Manager 8.4 or Later Hardware Appliance on RSA Link.

RSA supports using an integrated Dell Remote Access Controller (iDRAC) to remotely restore the original system image. For more information, see Configuring Remote Access to the RSA Authentication Manager Hardware Appliance on RSA Link.

Step 3: Set Up the Primary Instance

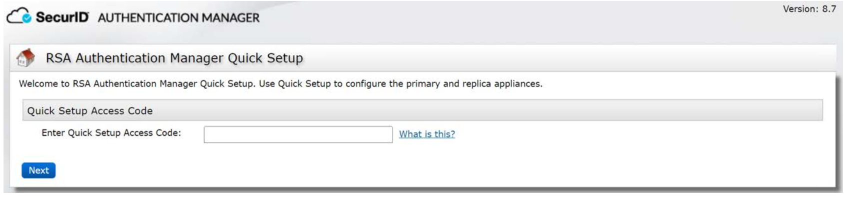
Quick Setup configures the appliance as the primary instance.

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. Do not unzip the file.

Procedure

1. Open a browser and navigate to the following URL to launch Quick Setup:
   https://<*primary appliance IP address*>/
   If a warning states that this URL is not on the list of allowed or trusted sites, click the browser option that allows you to connect to an untrusted site.
2. (Required) Enter the Quick Setup Access Code.



SecurID AUTHENTICATION MANAGER — Version: 8.7

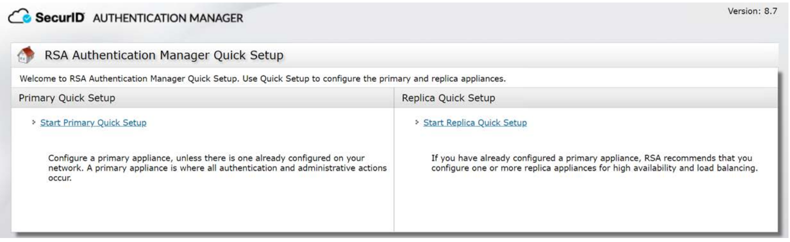
RSA Authentication Manager Quick Setup

Welcome to RSA Authentication Manager Quick Setup. Use Quick Setup to configure the primary and replica appliances.

Quick Setup Access Code

Enter Quick Setup Access Code: ____ What is this?

3. Accept the End User Licensing Agreement (EULA), and follow the prompts to configure the Authentication Manager primary instance.



SecurID AUTHENTICATION MANAGER — Version: 8.7

RSA Authentication Manager Quick Setup

Welcome to RSA Authentication Manager Quick Setup. Use Quick Setup to configure the primary and replica appliances.

Primary Quick Setup	Replica Quick Setup
Start Primary Quick Setup	Start Replica Quick Setup
Configure a primary appliance, unless there is one already configured on your network. A primary appliance is where all authentication and administrative actions occur.	If you have already configured a primary appliance, RSA recommends that you configure one or more replica appliances for high availability and load balancing.

4. Record all of the passwords to the administrative accounts that you create 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 security reasons, RSA does not provide a utility for recovering the operating system password.

   For more information, see the appendix “Administrative Accounts” in the *Setup and Configuration Guide*.
5. 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.
   Accept the certificate to access the console and prevent the warning from appearing again.
   If your web browser is configured for an enhanced security level, you must add the URL for each console to the list of allowed or trusted sites. See your browser documentation for additional instructions.

SecurID

RSA® Authentication Manager 8.7 Hardware Appliance Getting Started

6. (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** in the Operations Console or on RSA Link.

Logging On to the Consoles

You can access the consoles with the accounts that you specified during Quick Setup:

- The Super Admin account can access the Security Console and the Self-Service Console.
- The Operations Console administrator can access the Operations 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

Step 4: Set Up a Replica Instance

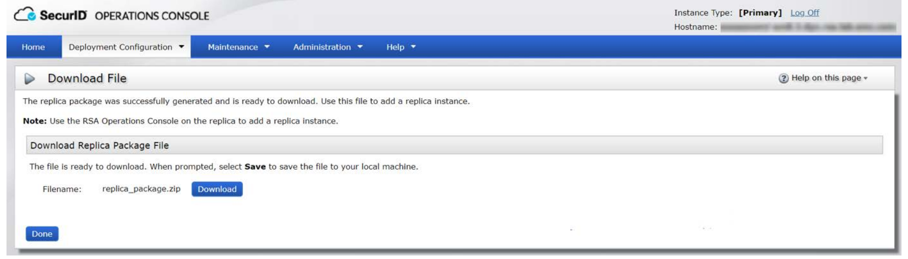
After you configure the primary instance, you can deploy another appliance and set up a replica instance.

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** in the Operations Console or on RSA Link.



Instance Type: **[Primary]** Log Off
Hostname: [redacted]

Download File

The replica package was successfully generated and is ready to download. Use this file to add a replica instance.

Note: Use the RSA Operations Console on the replica to add a replica instance.

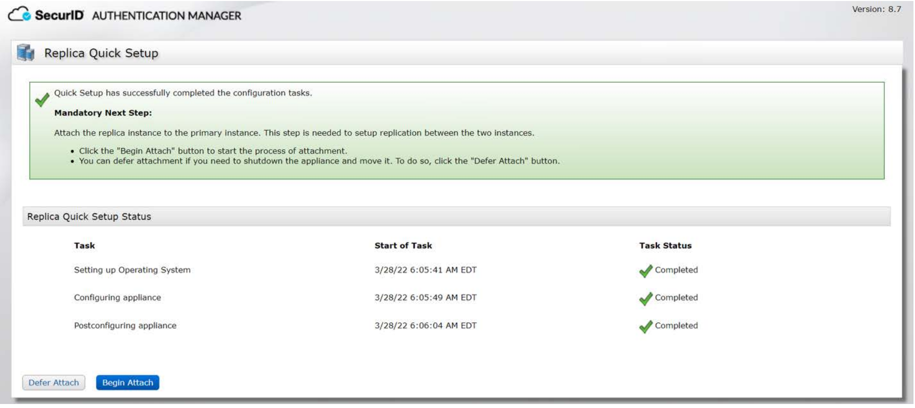
Download Replica Package File

The file is ready to download. When prompted, select **Save** to save the file to your local machine.

Filename: replica_package.zip

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://<*replica appliance IP address*>/
   If a warning states that this URL is not on the list of allowed or trusted sites, click the browser option that allows you to connect to an untrusted site.
4. When prompted, enter the Quick Setup Access Code.
   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.
5. 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** on RSA Link.



Replica Quick Setup

✓ Quick Setup has successfully completed the configuration tasks.

Mandatory Next Step:

Attach the replica instance to the primary instance. This step is needed to setup replication between the two instances.

- Click the "Begin Attach" button to start the process of attachment.
- You can defer attachment if you need to shutdown the appliance and move it. To do so, click the "Defer Attach" button.

Replica Quick Setup Status

Task	Start of Task	Task Status
Setting up Operating System	3/28/22 6:05:41 AM EDT	✓ Completed
Configuring appliance	3/28/22 6:05:49 AM EDT	✓ Completed
Postconfiguring appliance	3/28/22 6:06:04 AM EDT	✓ Completed

6. (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** in the Operations Console or on RSA Link.

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 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

See the *Setup and Configure Guide* for information on the next steps that you might perform for your deployment. You must perform all post-setup tasks on the primary instance.

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 **https://community.securid.com/t5/securid-integrations/tkb-p/securid-access-integrations** 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.

April 2022

Intellectual Property Notice

This software contains the intellectual property of RSA or is licensed to RSA from third parties. Use of this software and the intellectual property contained therein is expressly limited to the terms and conditions of the License Agreement under which it is provided by or on behalf of RSA.

Open Source License

This product may be distributed with open source code, licensed to you in accordance with the applicable open source license. If you would like a copy of any such source code, RSA or its affiliates will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. RSA or its affiliates may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to RSA Legal, 174 Middlesex Turnpike, Bedford, MA 01730, ATTN: Open Source Program Office.

R300-000-025 A0

P/N RSA-509-5700-04 **REV: 0A**