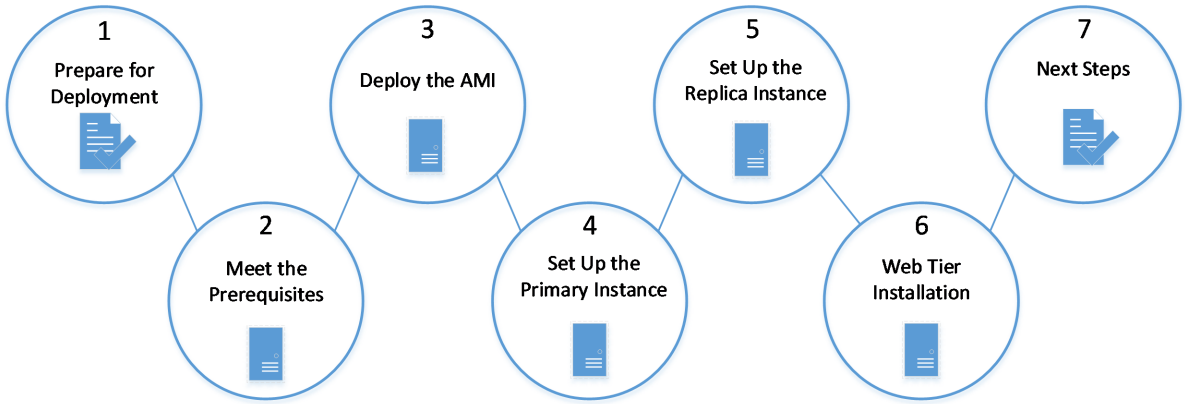
RSA® Authentication Manager 8.5

Amazon Machine Image Getting Started

Thank you for purchasing RSA® Authentication Manager 8.5. This document provides an overview of how to deploy the Authentication Manager Amazon Machine Image (AMI) on Amazon Web Services (AWS).



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 Deployment

See the documentation on RSA Link at https://community.rsa.com/community/products/securid/authentication-manager.

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.

Step 2: Meet the Prerequisites for Deploying the RSA Authentication Manager AMI

You must meet the following requirements for deploying the RSA Authentication Manager AMI.

Configuration

Before configuring AWS, do the following:

- Deploy a Virtual Private Cloud (VPC) on AWS.

The VPC is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud.

- Set up a private subnet and create a network interface in the private subnet.

  A private subnet has no direct route to the Internet gateway, uses private IP addresses, and is protected by an AWS security group.

- Have permission to deploy m4.large or better instance types.

For more information on VPCs and subnets, see the *Amazon Virtual Private Cloud User Guide* at https://docs.aws.amazon.com/vpc/.

DNS Server Configuration

For hostname resolution, the Authentication Manager AMI requires you to configure a DNS server in the Virtual Private Cloud (VPC):

1. Create a DHCP options set and associate it with the VPC.
2. Change the VPC properties by selecting **Yes** to editing DNS resolution and **No** to editing DNS hostnames.

Any on-premises RSA Authentication Manager primary and replica instances need to use the DNS server that is configured in the VPC.

The default DNS server for AWS uses the IP address 169.254.169.253. If you use the default DNS server, any subnet within the VPC can use 169.254.169.253 as the primary DNS server for Authentication Manager.

For more information on DNS servers, see the *Amazon Virtual Private Cloud User Guide* at https://docs.aws.amazon.com/vpc/.

Note: AWS also includes a default Network Time Protocol (NTP) server with the IP address 169.254.169.123 that you can specify during Quick Setup.

Create Security Groups

AWS security group rules control the inbound traffic to the Authentication Manager instance and the outbound traffic from the instance. By default, security groups allow all outbound traffic. Each port the user needs to access in the Authentication Manager instance must be configured in the security group rules for inbound traffic.

For more information on security groups for your Virtual Private Cloud (VPC), see the *Amazon Virtual Private Cloud User Guide* at https://docs.aws.amazon.com/vpc/.

Procedure

1. Log on to your AWS account.
2. On the Services tab, select **EC2**.
3. Select **Network and Security**.
4. Select **Security Groups**.
5. Create a security group that allows inbound traffic to the following ports, except where noted:

Port	Protocol	Purpose
22	TCP	Secure Shell (SSH)
49	TCP	TACACS authentication. Required for the TACACS client.
80	TCP	Quick Setup, Operations Console, Security Console
161	UDP	SNMP
443	TCP	Quick Setup, Operations Console, Security Console, Self-Service Console
If RADIUS clients only communicate to the RADIUS servers on ports 1812 and 1813, you can block the legacy RADIUS UDP ports 1645 and 1646. If RADIUS clients only communicate to the RADIUS servers on port 1812, you can block the legacy		

RADIUS UDP port 1645.		
1645	UDP	RADIUS authentication (legacy port)
1646	UDP	RADIUS accounting (legacy port)
If you do not use RSA RADIUS, but you have replica instances, you must allow connections between Authentication Manager instances on the TCP ports 1812 and 1813. These ports are required for tasks such as replica attachment, replica promotion, and IP address and hostname changes. You should restrict connections from other systems that are not Authentication Manager instances.		
1812	TCP	RADIUS replication port
1813	TCP	RADIUS administration
If you do not plan to use RSA RADIUS, you can close the UDP ports 1812 and 1813. If you do not plan to use RSA RADIUS, you can close the UDP port 1812.		
1812	UDP	RADIUS authentication
1813	UDP	RADIUS accounting
5500	TCP	Agent authentication
5500	UDP	Agent authentication
5550	TCP	Agent auto-registration
5555	TCP	RSA SecurID Authentication API agents
5580	TCP	Offline authentication service
7002	TCP, SSL-encrypted	Authentication Manager and the RSA Token Management snap-in for the Microsoft Management Console (MMC)
7004	TCP, SSL-encrypted	Security Console, Self-Service Console and risk-based authentication (RBA), and Cryptographic Token-Key Initialization Protocol (CT-KIP)
7022	TCP, SSL-encrypted	Authentication Manager, trusted realm network access point, or the web tier
7072	TCP, SSL-encrypted	Operations Console
7082	TCP, SSL-encrypted	RADIUS Configuration SSL
8443	TCP, SSL-encrypted	Authentication Manager patches and service packs
9786	TCP, SSL-encrypted	Embedded identity router

For more information about these ports, see the *Setup and Configuration Guide*.

Add any feature-specific ports to your security group. For example, an LDAP connection to an Oracle Directory Server instance might require you to add port 1389 in the security group. If you need to enable the connection to the Authentication API, then port number 5555 must be added to the security groups.

If you are using the ping command, you must enable the ICMP port in your security groups. RSA does not recommend opening the ICMP port on the cloud, but this port is required for ping to work.

For instructions on how to create security groups, see the Amazon Web Services documentation.

Step 3: Deploy the RSA Authentication Manager AMI

Deploy the RSA Authentication Manager AMI. When you run Quick Setup, you configure the AMI as an RSA Authentication Manager primary instance or replica instance.

Before you begin

- Request access to the RSA Authentication Manager Amazon Machine Image (AMI) file for your Amazon account ID. To request access to the AMI, contact RSA Customer Support.

  Note: RSA does not support the AWS feature for creating an AMI from an existing Authentication Manager primary or replica instance. Each Authentication Manager instance must be deployed from an AMI file that RSA provides.

- Manually configure network settings by creating a new network interface in the EC2 Dashboard. DHCP is not supported. Provide the appliance network settings for the AMI:

Description	Information
Default Gateway	This is the IP address of your AWS VPC Router. See: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html to determine the VPC Router IP for your subnet configuration.
Hostname (Fully Qualified Domain Name)	This is provided in the network interface configuration details.
IP Address	This is provided in the network interface configuration details.
Netmask	This must match the netmask of the subnet.
Primary DNS Server (Optional)	The default DNS server in AWS, 169.254.169.253, can be reached by any private subnet in the VPC.
Secondary DNS Server (Optional)	

  Note: If your region does not allow you to view the AWS console Instance Screenshot, you must provide your own Quick Setup Access Code along with the network settings. The Quick Setup Access Code is required to begin Quick Setup.

  The Quick Setup Access Code must contain eight of the following characters, including at least one number: abcdefghijkmnopqrstuvwxyzACDEFGHIJKLMNPQRSTUVWXYZ0123456789. For example, EgR7t4LR. If you do not meet these requirements, you cannot deploy the virtual appliance. Redeploy the appliance with a valid access code.

  You can record the appliance network settings in a text file, and paste it into AWS when you create the virtual appliance.

Procedure

1. Log on to your AWS account.
2. On the Services tab, select **EC2**.
3. In Images, select **AMIs**
4. Select the **Private Image** filter.
5. Search for the RSA Authentication Manager 8.5 AMI ID.
6. Right-click the AMI, and select **Launch**.
7. On the Choose an Instance Type page, select **m4.large**, **m4.xlarge**, or **m4.2xlarge**, and click **Next: Configure Instance Details**.
8. On the Configure Instance Details page, select a **Network** and a **Subnet** from the drop-down lists.
9. Expand the Network Interfaces section, and add the Primary IP address.
10. Expand the Advanced Details section. In the User data section, enter the appliance network settings as text. For example:

    gateway : 172.24.202.129

hostname : aws-am-001.example.com
ip : 172.24.202.187
netmask : 255.255.255.128
primarydns : 169.254.169.253
secondarydns : 0.0.0.0
accesskey : EgR7tbL7

11. Click **Next: Add Storage**.
12. Review the Add Storage page, but not modify the disk size parameter.
13. If this is a production instance, RSA recommends clearing the **Delete on Termination** checkbox. This ensures that the instance volume is retained when the instance is terminated.
14. Click **Next: Add Tags**.
15. On the Add Tags page, add any required tags. For example, you might enter "Instance Name" as the **Key** and "AM 8.5 primary instance" as the **Value**. Click **Next: Configure Security Group**.
16. On the Configure Security Group page, choose the appropriate configured security group, and click **Review and Launch**.
17. Review the settings on the Review Instance Launch page, and click **Launch**.
18. A key pair is not required for Authentication Manager. To log on to the appliance operating system, you need the password for **rsaadmin** account. You specify the operating system account password during Quick Setup.

    Select **Proceed without a key pair** from the drop-down list, and acknowledge that you will be able to connect to the appliance operating system with the operating system password.

19. Go to the Instances page, and right-click the new instance. Select **Instance Settings > Get Instance Screenshot** to view the console.

    If your region does not allow you to view the AWS console Instance Screenshot, proceed to step 21.

20. Click **Refresh** to view the updated screenshot.

    After to 10 to 15 minutes the Authentication Manager appliance boots and starts configuring network settings. When the Authentication Manager instance is deployed, the screenshot displays the Quick Setup URL and the Quick Setup Access Code.

21. Record the following required information:
    - The Quick Setup URL, which includes the IP address that you entered in step 7.
      `https://<IP Address>/`
      Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
    - The Quick Setup Access Code, which is required to initiate Quick Setup. The code is automatically generated, unless you entered it in step 10.
22. Enter the Quick Setup URL in the browser, including https, and press ENTER:

    `https://<IP Address>/`

23. To confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

Step 4: Set Up the Primary Instance

You must use Quick Setup to configure a primary instance before you deploy any replica instances.

RSA recommends a deployment containing both a primary instance and a replica instance. The RSA

Authentication Manager 8.5 Base Edition, Enterprise Edition, and Premium Edition all include permission to deploy a replica instance.

Do not cancel Quick Setup, or you will be unable to access the Quick Setup URL. In that situation, you must terminate the Amazon Web Services instance, and deploy the replica instance again.

Run Quick Setup on the Primary Instance

Keep the virtual 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

Copy the license file to a location that is accessible to the browser that is used to run the primary appliance Quick Setup. Do not unzip the file.

Procedure

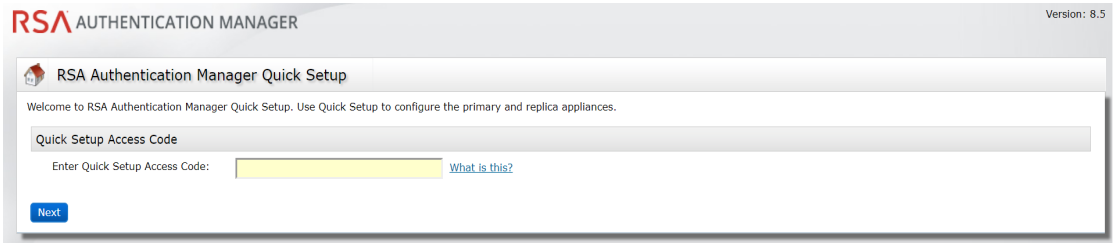
1. Launch Quick Setup with the URL provided at the end of virtual appliance deployment. Enter the Quick Setup URL in the browser, including **https**, and press **ENTER**:

   https://<*IP Address*>/

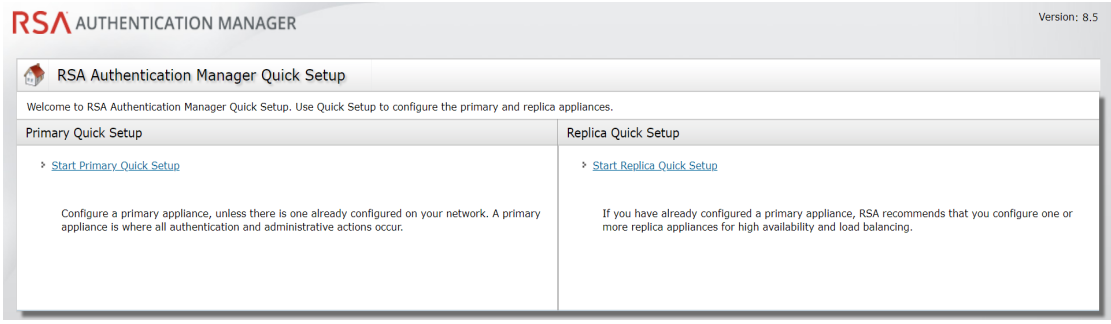
   where <*IP Address*> is the IP address of the appliance.

   If a browser warning states that this URL is not on the list of allowed or trusted sites, click the option that allows your browser to connect to an untrusted site.

2. You must enter the Quick Setup Access Code



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



4. Record all of the passwords for 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 require access to 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. After the instance is configured, 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 occurring again. For more information, see the chapter "Deploying a Primary Appliance" in the *Setup and Configuration Guide*

   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.

6. RSA recommends enabling SSH on the Amazon Web Services (AWS) virtual appliance, because SSH is the only way to log on to the operating system for this cloud-based appliance. For instructions, see the Enable Secure Shell on the Appliance topic in the Operations Console or on RSA Link.

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 replace a virtual appliance. For instructions, see the Download Network Settings for a Primary or Replica Instance topic in the Operations Console or on RSA Link.

Log 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 5: Set Up a Replica Instance

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

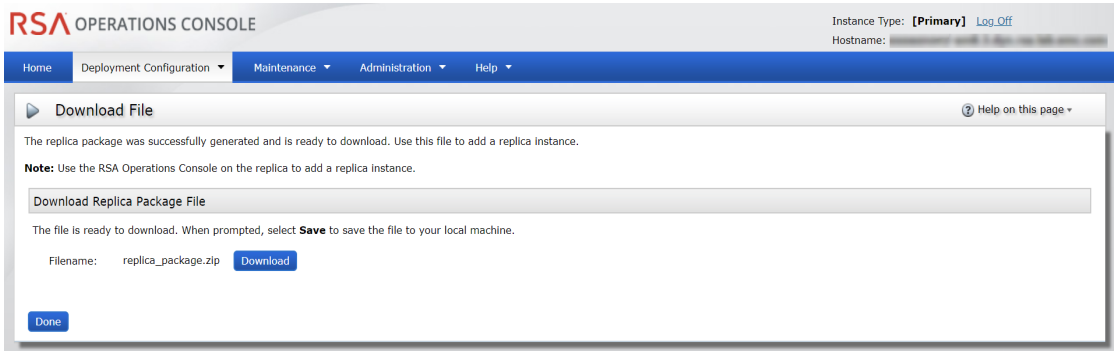
Do not cancel Quick Setup or defer replica attachment, or you will be unable to access the Quick Setup URL. In that situation, you must terminate the Amazon Web Services instance, and deploy the replica instance again.

Before you begin

A primary instance must be deployed on the network.

Procedure

1. On the primary appliance, log on to the Operations Console, and click **Deployment Configuration** > **Instances** > **Generate Replica Package**. For instructions, see the Generate a Replica Package topic in the Operations Console or on RSA Link.



2. Deploy a virtual appliance.

3. Launch Quick Setup with the URL provided at the end of the virtual appliance deployment. Enter the Quick Setup URL in the browser, including **https**, and press **ENTER**:

   https://<*IP Address*>/

   where <*IP Address*> is the IP address of the appliance.

   If a browser warning states that this URL is not on the list of allowed or trusted sites, 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**.

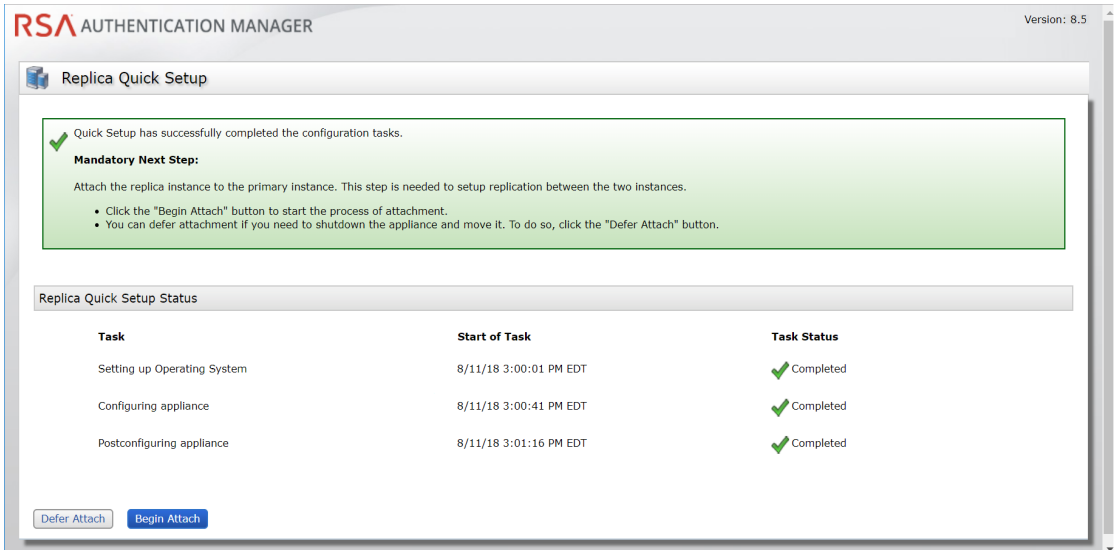
5. Follow the prompts to complete Quick Setup.

6. Record the operating system password that is created during Quick Setup.

   The operating system password is required to access your replica instance. For security reasons, RSA does not provide a utility for recovering the operating system password.

7. After the instance is configured, click **Begin Attach** to attach the replica instance to the primary instance. For instructions, see the Attach the Replica Instance to the Primary Instance topic on RSA Link.

Note: Do not defer replica attachment, or you will be unable to access the Quick Setup URL. In that situation, you must terminate the Amazon Web Services instance, and deploy the replica instance again.



8. RSA recommends enabling SSH on the Amazon Web Services (AWS) virtual appliance , because SSH is the only way to log on to the operating system for this cloud-based appliance. For instructions, see the Enable Secure Shell on the Appliance topic in the Operations Console or on RSA Link.

9. (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 replace a virtual appliance. For instructions, see the Download Network Settings for a Primary or Replica Instance topic in the Operations Console or on RSA Link.

Step 6: 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*.

Step 7: Next Steps

After setting up the appliance, see the *Setup and Configuration 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 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.

July 2020

Revised: May 2021

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.