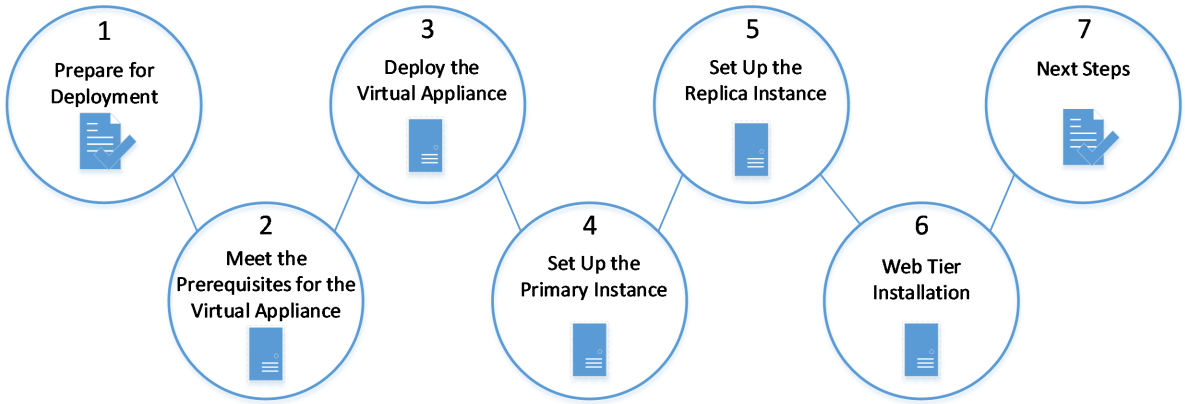
RSA SECURID® ACCESS

RSA® Authentication Manager 8.4

VMware Virtual Appliance Getting Started

Thank you for purchasing RSA® Authentication Manager 8.4. This document provides an overview of how to deploy Authentication Manager on the VMware virtual appliance.



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

Read the *Release Notes*, available at https://community.rsa.com/docs/DOC-99418.

Read the *Planning Guide*, available at https://community.rsa.com/docs/DOC-99427, for deployment considerations. For example, if users outside of your network require access to resources, you might want to deploy a web tier.

All of the documentation is available on RSA Link at https://community.rsa.com/community/products/securid/authentication-manager.

Step 2: Meet the Prerequisites for the Virtual Appliance

You must meet the following requirements for deploying RSA Authentication Manager 8.4 on a VMware virtual appliance.

Software Requirements

Deploy the virtual appliance on one of the following platforms:

- VMware ESXi 6.0 (also known as VMware vSphere Hypervisor 6.0)
- VMware ESXi 6.5 (also known as VMware vSphere Hypervisor 6.5)

- VMware ESXi 6.7 (also known as VMware vSphere Hypervisor 6.7)

RSA Authentication Manager 8.4 supports VMware ESXi 6.0, 6.5, and 6.7.

If you are using ESXi or vCenter Server 6.0, you must have any version of the VMware vSphere Client able to connect to and manage supported ESXi (Hypervisor) and vCenter Server deployments.

ESXi or vCenter Server 6.5 or 6.7 does not require a separate installed vSphere Client.

For VMware ESXi 6.5, Patch Release ESXi650-201801001 (52236) or later is required to deploy the virtual appliance directly on the VMware ESXi Server 6.5. You can check your ESXi Embedded Host Client version by logging on to the ESXi host with SSH, and running the following command:

```
"esxcli software vib get -n esx-ui"
```

To download the required software, go to https://my.vmware.com.

Software Support

(Optional) Versions of VMware vCenter Server that are compatible with the supported ESXi (Hypervisor) versions.

Primary or Replica Instance Requirements

The VMware virtual appliance for each RSA Authentication Manager instance requires hardware that meets or exceeds the following minimum requirements:

- 100 GB of disk space for storage and 4 GB for a swap file
- 4 GB of memory
- At least one virtual CPU

By default, each Authentication Manager instance is deployed with 8 GB of memory and two virtual CPUs.

The virtual appliance may require additional disk space for virtual machine operations, such as snapshots and memory management. Use the following formula to calculate the total amount of storage required:

Total disk space = 104 GB + (GB of memory allocated to the virtual appliance x 2) + (Number of snapshots x GB of memory allocated to the virtual appliance)

For example, a virtual appliance with 8 GB of memory and three snapshots requires about 150 GB of storage. The calculation 104 GB + (2 x 8 GB of memory) + (3 snapshots x 8 GB of memory) indicates that 144 GB is required, or 150 GB if you include a 6 GB buffer.

Automatic tuning on the virtual appliance supports 4 GB, 8 GB, 16 GB, or 32 GB of memory. For example, the appliance uses 32 GB of memory if more than 32 GB is available.

The VMware virtual appliance only supports the E1000 virtual network adapter. Do not change the default network adapter.

For additional hardware requirements for the physical server hosting the virtual appliances, see your VMware documentation.

Step 3: Deploy the Virtual Appliance

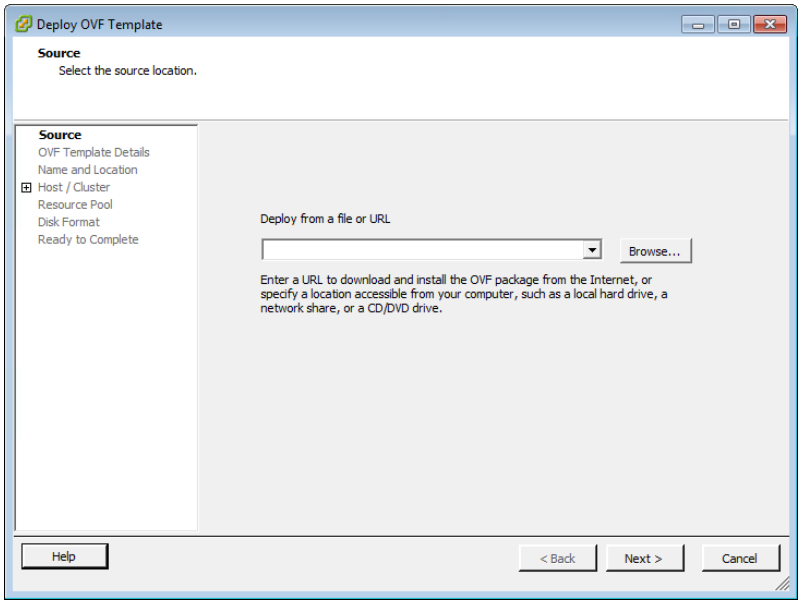
Follow this procedure to deploy a VMware virtual appliance. When you run Quick Setup, you configure the virtual appliance as an RSA Authentication Manager primary instance or replica instance.

Before you begin

Copy the RSA Authentication Manager OVA file from the directory in the kit to a location that the VMware vSphere Client can access.

Procedure

1. Depending upon your VMware version, do one of the following procedures:
   - For VMware vCenter Server or ESXi server 6.0, do the following :
     a. In the VMware vSphere Client, log on to VMware vCenter Server, or log on to the VMware ESX or ESXi server (VMware Hypervisor). VMware vCenter Server is not required to deploy the virtual machine.
     b. Select **File > Deploy OVF Template** to start the wizard.
     c. On the Source window, browse to RSA Authentication Manager OVA file.



   - For VMware vCenter Server 6.5 or 6.7, do the following:
     a. Use a browser to access the vCenter Server URL.
     b. On the Getting Started page, click either the **vSphere Client (HTML5)** or the **vSphere Web Client (Flash)**.
     c. On the VMware vCenter Single Sign-On page, log on to the VMware vCenter Server.
     d. Do one of the following:
        - (vSphere Client with HTML5) On the Navigator pane (left hand side), right-click the **VMware Datacentre/Cluster/Host** and select **Deploy OVF Template...** to start the deployment wizard.
        - (vSphere Web Client with Flash) On the Navigator pane, right-click on the vCenter server and select **Deploy OVF Template...** to start the deployment wizard.
     e. On the Select Template window, select **Local File**, click **Browse**, and locate the RSA Authentication Manager OVA file to deploy. Click **Next**.
   - For VMware ESXi server 6.5 or 6.7 (VMware Hypervisor), do the following:
     a. In a browser, log on to the VMware ESXi server.
     b. On the Navigator pane, right-click **Host** and select **Create/Register VM** to start the deployment wizard.
     c. On the Select creation type window, select **Deploy a virtual machine from an OVF or OVA file**. Click **Next**.
     d. On the Select OVF and VMDK files window, enter a Name for the virtual appliance, and locate the RSA Authentication Manager OVA file to deploy. Click **Next**.

2. Follow the wizard to deploy the template.

   Note: When deploying the virtual appliance directly to the VMware ESXi server 6.5 or 6.7, do not enter network settings on the Additional Settings window. Only enter network settings when prompted in the virtual machine console.

3. On the **Ready to Complete** window, review your settings, and click **Finish**. VMware requires approximately five minutes to deploy the virtual appliance.
4. Power on the virtual machine.
5. Select the virtual appliance, and click the **Console** tab. The VMware OS Console tab displays the progress of the virtual appliance deployment.
6. Wait 30 seconds to select the default keyboard layout, English (United States). To choose another keyboard layout, click any key and follow the instructions on the screen.
7. If you are deploying the virtual appliance directly on the ESXi platform, the OS Console prompts you to enter and verify the virtual appliance network settings.

   If you are deploying the virtual appliance through VMware vCenter, you already entered the network settings in the wizard.

8. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record the following required information:

   - The Quick Setup URL includes the IP address you provided for the virtual appliance:

     `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 is required to initiate Quick Setup.

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 8.4 Base Edition, Enterprise Edition, and Premium Edition all include permission to deploy a replica instance.

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

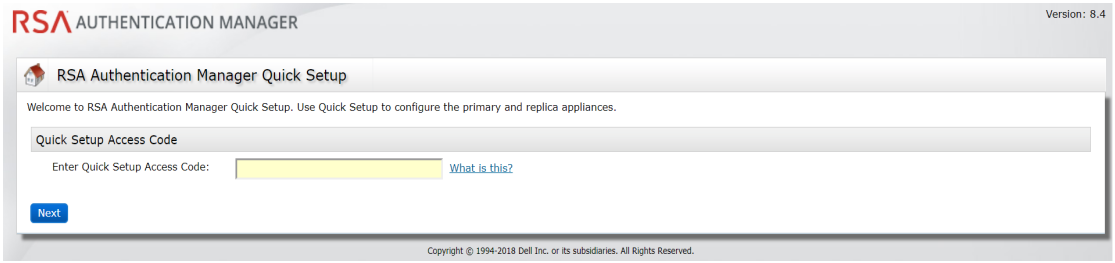
1. Launch Quick Setup with the URL provided at the end of virtual appliance deployment. Enter the Quick Setup URL in the browser, including **https**, and press **ENTER**:

   https://<*IP Address*>/

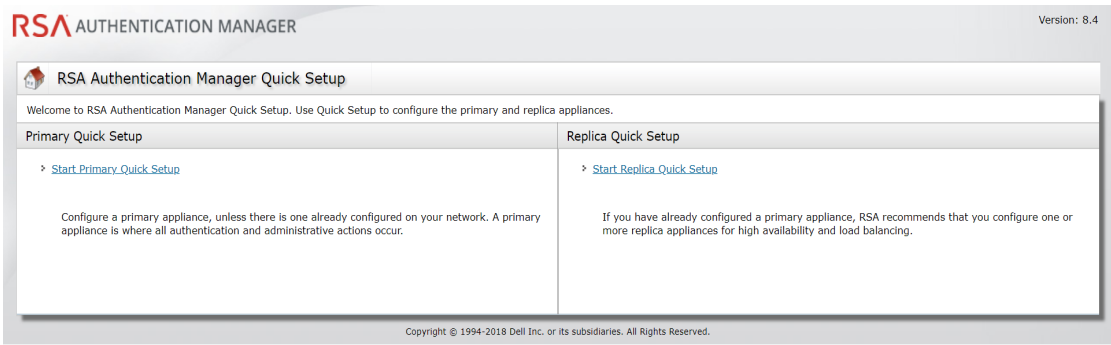
   where <*IP Address*> is the IP address of the appliance.

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 and the Azure virtual appliance, because SSH is the only way to log on to the operating system for these cloud-based appliances. Enabling SSH is optional on the VMware virtual appliance, the Hyper-V virtual appliance, and the hardware appliance. For instructions, see the "Enable Secure Shell on the Appliance" topic in the Operations Console or on RSA Link at https://community.rsa.com/docs/DOC-77019.

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 at https://community.rsa.com/docs/DOC-76799.

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

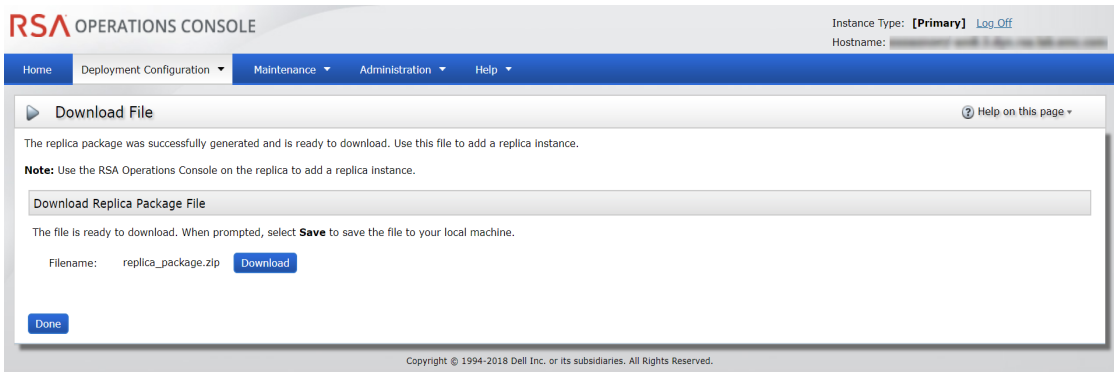
After you configure the primary instance, you can deploy another virtual appliance and set up a replica instance.

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 at https://community.rsa.com/docs/DOC-77158.



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.

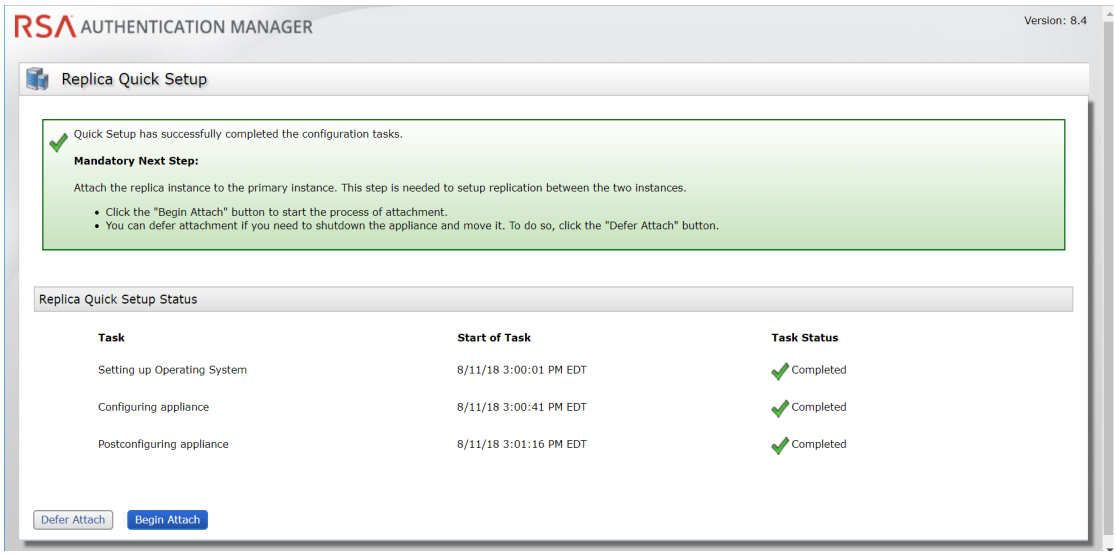
If a browser warning states that this URL is not on the list of allowed or trusted sites, click the option that allows your browser to connect to an untrusted site.

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, 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 replica instance.

   For instructions, see the "Attach the Replica Instance to the Primary Instance" topic on RSA Link at https://community.rsa.com/docs/DOC-76808.



8. RSA recommends enabling SSH on the Amazon Web Services (AWS) virtual appliance and the Azure virtual appliance, because SSH is the only way to log on to the operating system for these cloud-based appliances. Enabling SSH is optional on the VMware virtual appliance, the Hyper-V virtual appliance, and the hardware appliance. For instructions, see the "Enable Secure Shell on the Appliance" topic in the Operations Console or on RSA Link at https://community.rsa.com/docs/DOC-77019.
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 at https://community.rsa.com/docs/DOC-76799.

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.

December 2018

Revised: April 2019

Trademarks

Intellectual Property Notice

Open Source License