# RSA® Authentication Manager 8.1 Setup and Configuration Guide

*Revision 1*

### Contact Information

Go to the RSA corporate website for regional Customer Support telephone and fax numbers:
**www.emc.com/domains/rsa/index.htm**

### Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

### License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

### Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA SecurCare Online. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

### Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

### Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.


December 2013
Revised: February 2014

# Contents

# Revision History

| Revision Number | Date | Revision |
|---|---|---|
| 1 | February 2014 | Added instructions for upgrading RSA Authentication Manager 8.0 to 8.1.<br>Removed a reference to thin-provisioned storage on the virtual appliance. Thick-provisioned storage is also supported. |

# Preface

## About This Guide

This guide is intended for network and system administrators who are responsible for installing and securing the various components of an RSA® Authentication Manager deployment.

## RSA Authentication Manager 8.1 Documentation

For information about RSA Authentication Manager 8.1, see the following documentation. RSA recommends that you store the product documentation in a location on your network that is accessible to administrators.

***Release Notes.*** Describes what is new and changed in this release, as well as workarounds for known issues.

***Hardware Appliance Getting Started.*** Describes how to deploy a hardware appliance and perform the Authentication Manager Quick Setup process.

***Virtual Appliance Getting Started.*** Describes how to deploy a virtual appliance and perform the Authentication Manager Quick Setup process.

***Planning Guide.*** Describes the high-level architecture of Authentication Manager and how it integrates with your network.

***Setup and Configuration Guide.*** Describes how to set up and configure Authentication Manager.

***Administrator's Guide.*** Provides an overview of Authentication Manager and its features. Describes how to configure the system and perform a wide range of administration tasks, including manage users and security policies.

***Help Desk Administrator's Guide.*** Provides instructions for the most common tasks that a Help Desk Administrator performs on a day-to-day basis.

***Hardware Appliance SNMP Reference Guide.*** Describes how to configure Simple Network Management Protocol (SNMP) to monitor an instance of Authentication Manager on a hardware appliance.

***Virtual Appliance SNMP Reference Guide.*** Describes how to configure Simple Network Management Protocol (SNMP) to monitor an instance of Authentication Manager on a virtual appliance.

***Troubleshooting Guide.*** Describes the most common error messages in RSA Authentication Manager and provides the appropriate actions to troubleshoot each event.

***Developer's Guide.*** Provides information about developing custom programs using the RSA Authentication Manager application programming interfaces (APIs). Includes an overview of the APIs and Javadoc for Java APIs.

***Performance and Scalability Guide.*** Describes what to consider when tuning your deployment for optimal performance.

***6.1 to 8.1 Migration Guide***. Describes how to migrate from an RSA Authentication Manager 6.1 deployment to an RSA Authentication Manager 8.1 deployment.

***7.1 to 8.1 Migration Guide: Migrating to a New Hardware Appliance or Virtual Appliance.*** Describes how to migrate from an RSA Authentication Manager 7.1 deployment to an RSA Authentication Manager 8.1 deployment on a new hardware appliance or virtual appliance.

***7.1 to 8.1 Migration Guide: Upgrading RSA SecurID Appliance 3.0 on Existing Hardware.*** Describes how to migrate from an RSA Authentication Manager 7.1 deployment to an RSA Authentication Manager 8.1 deployment on existing, supported RSA SecurID Appliance 3.0 hardware.

**Security Console Help.** Describes day-to-day administration tasks performed in the Security Console.

**Operations Console Help.** Describes configuration and setup tasks performed in the Operations Console.

**Self-Service Console Help.** Describes how to use the Self-Service Console. To view the Help, on the **Help** tab in the Self-Service Console, click **Self-Service Console Help**.

**RSA Token Management Snap-In Help**. Describes how to use software that works with the Microsoft Management Console (MMC) for deployments that have an Active Directory identity source. Using this snap-in, you can enable or disable a token, assign a token, or perform other token-related tasks without logging on to the Security Console.

## Related Documentation

***RADIUS Reference Guide.*** Describes the usage and settings for the initialization files, dictionary files, and configuration files used by RSA RADIUS.

***Security Configuration Guide.*** Describes the security configuration settings available in RSA Authentication Manager. It also describes secure deployment and usage settings, secure maintenance, and physical security controls.

# Support and Service

| | |
|---|---|
| RSA SecurCare Online | https://knowledge.rsasecurity.com |
| Customer Support Information | www.emc.com/support/rsa/index.htm |
| RSA Solution Gallery | https://gallery.emc.com/community/marketplace/rsa?view=overview |

RSA SecurCare Online offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

The RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Secured by RSA Implementation Guides with step-by-step instructions and other information about interoperation of RSA products with these third-party products.

## Before You Call Customer Support

Please have the following information available when you call:

- ❑ Access to the RSA Authentication Manager appliance.
- ❑ Your license serial number. To locate the license serial number, do one of the following:
  - Look at the order confirmation e-mail that you received when your ordered the product. This e-mail contains the license serial number.
  - Log on to the Security Console, and click **License Status**. Click **View Installed License**.
- ❑ The Authentication Manager appliance software version information. You can find this information in the top, right corner of the Quick Setup, or in the Security Console. Log on to the Security Console, and click **Software Version Information**.

# 1 Preparing for Deployment

## Planning Decisions

Before you set up your RSA Authentication Manager 8.1 deployment, you must decide which Authentication Manager components you want to install. A deployment can include the following components:

**Primary Instance**. The instance on which all administration takes place. It can also service authentication requests.

**Replica Instance**. Provides redundancy of the primary instance and authenticates users.

**Web Tiers**. Allows the secure deployment of the RSA Self-Service Console, dynamic seed provisioning, and the risk-based authentication (RBA) service within the demilitarized zone (DMZ).

**Load Balancer**. Used to distribute authentication requests and to facilitate failover between the primary and replica web tiers.

**Authentication Agents**. Installed on any resource that you want to protect.

For more information on deployment planning topics, see the *Planning Guide*.

## Appliance Support

RSA Authentication Manager 8.1 supports a hardware appliance and a virtual appliance. Each type of appliance provides the same Authentication Manager features. You can use one or both types of appliance in your deployment.

Both a virtual appliance and a hardware appliance include a Linux operating system that is installed with Authentication Manager and RSA RADIUS server software. To configure an appliance as an Authentication Manager instance, you must complete Quick Setup.

The following differences apply:

- Before performing Quick Setup, the RSA-supplied hardware appliance is deployed by directly accessing the hardware, and connecting a keyboard and monitor to the machine to configure the network and keyboard language settings.
- You can only perform a factory reset on the hardware appliance.
- The virtual appliance is deployed with VMware vCenter Server or the VMware ESXi Server (VMware Hypervisor) on a host machine that you provide. You must use a host machine that meets the hardware requirements.
- The virtual appliance supports VMware features, such as VMware snapshots.

# VMware Virtual Appliance Requirements

If you deploy RSA Authentication Manager 8.1 on a virtual appliance, use the VMware vSphere Client to deploy a virtual appliance through VMware vCenter Server or directly on the VMware ESXi platform (also known as VMware vSphere Hypervisor 4.1 or later). VMware vCenter Server is not required to deploy the virtual appliance.

You must deploy a virtual appliance with the RSA Authentication Manager Open Virtualization Appliance (OVA) file that is located in the RSA Authentication Manager 8.1 download kit.

## VMware Software Requirements

| Required Software | Description |
|---|---|
| VMware Platforms | Deploy the virtual appliance on one of the following platforms:<br>• VMware ESXi 4.1 or later (VMware vSphere Hypervisor 4.1 or later)<br>• VMware ESXi 5.0 or later (VMware vSphere Hypervisor 4.1 or later) |
| VMware vSphere Client | Any version of the vSphere Client that works with supported ESXi (Hypervisor) and vCenter Server deployments. |

For the VMware host hardware requirements, see your VMware documentation.

## VMware Software Support

| Supported Software | Description |
|---|---|
| (Optional) VMware vCenter Server | VMware vCenter Server provides centralized management for multiple virtual machines and includes administrative features, such as vMotion.<br>The virtual appliance supports the versions of VMware vCenter Server that are compatible with the supported ESX and ESXi versions:<br>• VMware vCenter Server 4.1 or later<br>• VMware vCenter Server 5.0 or later |

## Primary or Replica Instance Hardware Requirements

The virtual appliance for each RSA Authentication Manager instance requires hardware that meets or exceeds the minimum requirements. Each instance is deployed with the default values.

| Description | Minimum Requirement | Default Value |
|---|---|---|
| Disk Space | 100 GB | 100 GB |
| Memory Requirements | 4 GB | 8 GB |
| CPU Requirements | One virtual CPU | Two virtual CPUs |

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

The virtual appliance only supports the E1000 virtual network adapter. Do not change the default network adapter or add a new virtual network adapter to the virtual appliance.

For the VMware host hardware requirements, consult your VMware documentation.

For information on ports used by Authentication Manager, see Port Usage on page 81.

## VMware Feature Support

RSA Authentication Manager supports VMware features, such as vMotion, Storage vMotion, High Availability, Fault Tolerance, Distributed Resource Scheduler (DRS), and Snapshots. Restrictions are described in the following table.

| Feature | Support |
|---|---|
| VMware Fault Tolerance | VMware Fault Tolerance in VMware vSphere 4.1 and 5.0 has the following requirements:<br>• Only virtual appliances with a single virtual CPU are compatible with Fault Tolerance. By default, each Authentication Manager instance is deployed with two virtual CPUs.<br>You can change the number of virtual CPUs. For instructions, see the VMware vSphere Client documentation.<br>• VMware Fault Tolerance does not support IPv6. If you use Fault Tolerance, do not create an IPv6 network address on an Authentication Manager primary or replica instance |

| Feature | Support |
|---|---|
| VMware snapshots | You can take a VMware snapshot of an Authentication Manager primary or replica instance, but snapshots do not replace the Operations Console backup feature.<br>When you take a snapshot of an Authentication Manager instance, specific settings are required. In a complex Authentication Manager deployment, restoring snapshots requires you to perform additional tasks.<br>For information, see the chapter "Disaster Recovery" in the *Administrator's Guide*. |
| VMware Distributed Resource Scheduler (DRS) | For security and redundancy, you can install primary and replica instances on separate hosts.<br>VMware DRS can move both instances onto the same host. Configure DRS to keep instances on separate physical hosts. |

# Supported Data Stores

You can store data in:

- The RSA Authentication Manager internal database
- One or more external directory servers that use LDAP (called an identity source within Authentication Manager).

## Internal Database

Authentication Manager is installed with an internal database. The following information is stored only in the internal database:

- Data that is specific to Authentication Manager, such as token data or policies for administrative roles and passwords.
- Data that links Authentication Managerwith LDAP directory user and user group records.

Users, user groups, and identity attribute data can be stored in an external LDAP directory or in the internal database.

## Supported Directory Servers

RSA Authentication Managersupports the following external LDAP directory servers for user, user group, and identity attribute data:

- Microsoft Active Directory 2008 R2
- Microsoft Active Directory 2012
- Sun Java System Directory Server 7.0
- Oracle Directory Server Enterprise Edition 11G

Active Directory Application Mode (ADAM) is not supported.

Authentication Manager has read-only access to all external directory servers. However, you can configure the system to allow users to change their passwords in LDAP during authentication.

Authentication Manager LDAP integration does not modify your existing LDAP schema, but rather creates a map to your data that Authentication Manager uses.

Authentication Manager supports Secure Socket Layer (SSL) for LDAP connections. SSL is required if you are allowing users to change their passwords from Authentication Manager. Non-SSL connections can expose sensitive data as it passes over the connection. For example, if bind LDAP operations to authenticate are performed over a non-SSL connection, the password is sent in the clear. The use of LDAP over SSL requires that the appropriate certificate is accessible by Authentication Manager.

For more information, see the chapter "Integrating LDAP Directories" in the *Administrator's Guide*.

## Supported Web Browsers

RSA Authentication Manager administration is managed through a web-based interface and must be accessed through a supported browser. Authentication Manager supports the following web browsers:

- Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox 10.0 or later.
- Google Chrome 18 or later
- Apple Safari 5.1 or later

The web browser must allow JavaScript and cookies. If your web browser does not have JavaScript and cookies enabled, see your web browser documentation for instructions on enabling JavaScript and cookies.

**Note:** To correctly display the web-based interface, you must have a screen resolution of 1024 X 768 or higher.

## Supported RSA Authentication Agents

Authentication agents are software applications that securely pass user authentication requests to and receives responses from RSA Authentication Manager. Authentication agents are installed on each machine, such as a domain server, web server, or a personal computer, that you protect with Authentication Manager. Any resource that is used with SecurID authentication, on-demand authentication (ODA) or risk-based authentication (RBA) requires an authentication agent.

The agent that you need depends on the type of resource you want to protect. For example, to protect an Apache web server, you need to download the RSA Authentication Agent for Apache. You may purchase products that contain embedded RSA Authentication Agent software. For example, these products include all the major brands of remote access servers and firewalls.

For a list of RSA authentication agents, go to **http://www.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings**.

For a list of third-party products that have embedded RSA agents, go to the RSA Secured® web site at **https://gallery.emc.com/community/marketplace/rsa?view=overview**.

For more information, see the chapter "Deploying Authentication Agents" in the *Administrator's Guide*.

## License Requirements

RSA Authentication Manager has one or more associated licenses. The license represents permission to use a specific version of the Authentication Manager software. RSA Authentication Manager 8.1 supports the use of an existing version 8.0 license, a new version 8.1 license, or a combination of version 8.0 and 8.1 licenses.

You can purchase and install one of the following license types:

- **Base Server.** A permanent license allowing 1 primary instance and 1 replica instance of Authentication Manager.
- **Enterprise Server.** A permanent license allowing 1 primary instance and up to 15 replica instances of Authentication Manager. The Enterprise Server license also includes the Authenticator Provisioning feature.

Each license type limits the number of instances of Authentication Manager that can be installed. User limits are based on the customer's usage requirements. For more information, see "Licenses" in the *Administrator's Guide*.

RSA provides the license files separately from your RSA Authentication Manager 8.1 download kit. Make sure that you know the location of the license file before running the primary appliance Quick Setup. The license file must be accessible to the browser that is used to run the primary appliance Quick Setup. Do not unzip the license file.

## Accurate System Date and Time Settings

RSA Authentication Manager requires accurate date and time settings for replication and authentication. If the token clock and the Authentication Manager system clock do not match, the generated tokencodes will not match, and authentication attempts can fail. Specifying a Network Time Protocol (NTP) server for the instance prevents replication and authentication issues that are caused by clock drift.

**Important:** An NTP server is required in a replicated deployment. RSA requires that all Authentication Manager instances have their time synchronized to an NTP server.

If you do not specify an NTP server in Authentication Manager, the virtual appliance uses the date and time provided by the physical machine hosting the virtual appliance. In this situation, the physical machine hosting the virtual appliance should be configured to obtain accurate date and time information from an NTP server.

Make sure that you have the hostname or IP address of an NTP server before running Quick Setup.

## Secure Appliance Deployment

After you deploy RSA Authentication Manager 8.1 on a hardware appliance or a virtual appliance, the operating system console screen displays a Quick Setup Access Code along with a Quick Setup URL. The Quick Setup Access Code is only available until Quick Setup is complete.

The Quick Setup Access Code is required to begin Quick Setup, which configures the appliance as an RSA Authentication Manager instance. This code makes it harder for a malicious user to access Quick Setup and take control of the appliance.

**Important:** You must have the Quick Setup Access Code to begin Quick Setup.

On a hardware appliance only, a factory reset puts the appliance into a pre-configured state. Any time you perform a factory reset on a hardware appliance, a new Quick Setup Access Code is displayed in the operating system console or the Factory Reset in Progress window in the Operations Console. The new code is required to run Quick Setup. The factory reset feature is not available for a virtual appliance.

RSA recommends the following guidelines when deploying an appliance:

- Deploy a hardware appliance in a test environment or in an isolated network. Only connect the appliance to your organization's network after Quick Setup is complete. Restrict physical and network access to the appliance to authorized individuals.

  For example, you can deploy a hardware appliance and run Quick Setup in a protected test environment that duplicates your production environment. After Quick Setup is complete, you can move the appliance into the production environment without changing the network settings, such as the hostname and the IP Address.

  Alternately, you can deploy the hardware appliance and run Quick Setup in a protected test environment and later change the network settings, such as the hostname and IP address, to attach the appliance to your production environment. For instructions, see the appendix "Changing the Instance Network Settings" in the *Administrator's Guide*.
- Deploy a virtual appliance on an isolated network until Quick Setup is complete. Use VMware to maintain full control over the appliance. Restrict network access to the appliance, and only allow authorized individuals to access the virtual appliance.
- If you access an appliance to run Quick Setup, and you discover that the appliance has already been configured or you receive error messages because Quick Setup is in progress, then do the following:

  a. Contact other administrators in your organization to ensure that a malicious user is not trying to take control of the appliance.

  b. If you believe that the appliance has been compromised, remove the primary or replica instance from your deployment. For instructions, see the chapter "System Maintenance and Disaster Recovery" in the *Administrator's Guide*.

  c. Do one of the following:

     - For a hardware appliance, shut down the appliance and remove the machine from service.
     - For a virtual appliance, suspend the appliance, and quarantine the machine for further investigation.

  d. Contact your IT department or RSA immediately.

# Deployment Checklist for the Primary Instance

Before you set up the RSA Authentication Manager primary instance, you must collect the following information. You enter this information during the appliance deployment and Quick Setup.

## Virtual Appliance Deployment

If you are deploying RSA Authentication Manager on a virtual appliance, you must collect the following items and information:

- ❑ **VMware vSphere Client computer.** You will use this computer to deploy the appliance through the vSphere Client and to run Quick Setup through a supported web browser. For a list of supported web browsers, see Supported Web Browsers on page 17.
- ❑ **RSA Authentication Manager Open Virtualization Appliance (OVA) file.** The OVA file is used to create your virtual appliance. Copy the OVA file to a location accessible to VMware.
- ❑ **IPv4 Network settings.** 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.

  You must provide this network information when deploying the appliance. The IP address that you specify for the appliance is used to access Quick Setup.

## Hardware Appliance Deployment

If you are deploying RSA Authentication Manager on a hardware appliance, you must collect the following items and information:

- ❑ **Keyboard and Monitor.** To deploy the hardware appliance and complete the initial configuration tasks that are required for the deployment process, you must attach a keyboard and monitor to the appliance.
- ❑ **IPv4 Network settings.** 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.

  You must provide this network information when deploying the appliance. The IP address that you specify for the appliance is used to access Quick Setup.

## Quick Setup Checklist

You must enter the following information during the Quick Setup process for a primary instance.

- ❑ **Appliance license file.** During Quick Setup, you must have access to the .zip license file. You download the license file (.zip) from RSA Download Central at **https://download.rsasecurity.com**.

  Use the credentials and the license serial number that were e-mailed to you to log on to the site and download the license file. If you did not receive this e-mail, contact the License Seed Response Team. Send an e-mail with your contact information and the license serial number provided in your order confirmation to the following address appropriate for your region:

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

  Make sure that you know the location of the license file before running the primary appliance Quick Setup. The license file must be in a location that is accessible to the browser that is used to run the primary appliance Quick Setup. Do not unzip the file. RSA recommends that you store the license file in a protected location available only to authorized administrative personnel.

- ❑ **Hostname or IP address of an NTP server.** RSA recommends that you specify a local or Internet Network Time Protocol (NTP) server, for example, nist.time.gov. During Quick Setup, you can enter the hostname or IP address of at least one NTP servers.

  **Important:** An NTP server is required in a replicated deployment. RSA requires that all Authentication Manager instances have their time synchronized to an NTP server.

- ❑ **Operating system password.** Choose a password to access the appliance operating system for troubleshooting and advanced administration. The password must be between 8 and 32 characters long, and contain at least 1 alphabetic character and at least 1 special character excluding ^, @, and ~. For example, gyz!8kMh is a valid password. For more information, see System Administrator Accounts on page 91.

- ❑ **User ID and password for initial administrator accounts.** Choose a User ID and password to create the following:

  – Initial Security Console administrator User ID and password for the Super Admin role

  – Operations Console administrator User ID and password

  For information on managing administrator accounts and passwords, see System Administrator Accounts on page 91.

# Deployment Checklist for a Replica Instance

Before you set up an RSA Authentication Manager replica instance, you must collect the following information about each replica that you want to set up. You enter this information during the appliance deployment and Quick Setup.

## Virtual Appliance Deployment

If you are deploying RSA Authentication Manager on a virtual appliance, you must collect the following items and information:

- ❑ **VMware vSphere Client computer.** You will use this computer to deploy the appliance through the vSphere Client and to run Quick Setup through a supported web browser. For a list of supported web browsers, see Supported Web Browsers on page 17.
- ❑ **RSA Authentication Manager Open Virtualization Appliance (OVA) file.** The OVA file is used to create your virtual appliance. Copy the OVA file to a location accessible to VMware.
- ❑ **IPv4 Network settings.** 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.

  You must provide this network information when deploying the appliance. The IP address that you specify for the appliance is used to access Quick Setup.

## Hardware Appliance Deployment

If you are deploying RSA Authentication Manager on a hardware appliance, you must collect the following items and information:

- ❑ **Keyboard and Monitor.** To deploy the hardware appliance and complete the initial configuration tasks that are required for the deployment process, you must attach a keyboard and monitor to the appliance.
- ❑ **IPv4 Network settings.** 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.

  You must provide this network information when deploying the appliance. The IP address that you specify for the appliance is used to access Quick Setup.

## Quick Setup Checklist

You must enter the following information during the Quick Setup process for a replica instance.

- ❑ **Replica package file location.** To set up a replica appliance, you must have access to the replica package file. If necessary, copy the replica package file onto the computer that you will use to run Quick Setup.

  For more information on creating a replica package, see Generate and Download a Replica Package File on page 41.

- ❑ **Hostname or IP address of an NTP server.** You must synchronize the time on the primary and replica appliances using a local or Internet Network Time Protocol (NTP) server. During Quick Setup, you can enter hostname or IP address of at least one NTP server.

- ❑ **Operating system password.** Choose a password to access the appliance operating system for troubleshooting and advanced administration. The password must be between 8 and 32 characters long, and contain at least 1 alphabetic character and at least 1 special character excluding ^, @, and ~. For example, gyz!8kMh is a valid password. Choose a unique password for each appliance. For more information, see System Administrator Accounts on page 91.

# Setup and Configuration Information List

Use the following list to specify setup and configuration information for RSA Authentication Manager. RSA recommends that you complete this list and distribute it to the appropriate personnel for your deployment. Save a copy of the completed list in a secure location for future reference.

**Note:** Some of the information that you enter in this list may be sensitive. Review your company's policies before entering sensitive information, such as a password, in this list.

## Appliance Deployment

| Element | Your Plan |
|---|---|
| RSA Authentication Manager OVA Package location (Virtual Appliance Only) | |
| Fully qualified domain name | |
| IPv4 Static IP address | |
| IPv4 Subnet mask | |
| IPv4 Default Gateway | |
| IP address of the DNS servers | |

**Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.

## Primary Appliance Setup

| Description | Your Plan |
|---|---|
| RSA Authentication Manager license file (.zip) location | |
| Hostname or IP address of an NTP server | |
| Operating System password | |
| Super Admin user name | |
| Super Admin password | |
| Operations Console Administrator user name | |
| Operations Console Administrator password | |

## Replica Appliance Setup

| Description | Your Plan |
|---|---|
| Replica package file location | |
| Hostname or IP address of an NTP server | |
| Operating system password | |

## Load Balancer Configuration

| Description | Your Plan |
|---|---|
| Load balancer IP address | |
| Load balancer hostname/virtual hostname | |
| Port number | |
| IP address of virtual host or load balancer on the DNS server | |

## Web Tier Installation

| Description | Your Plan |
|---|---|
| Web-tier server IP addresses | |
| Web-tier server hostnames | |
| IP address of the DNS server | |

# 2 Deploying a Primary Appliance

## Perform Deployment Tasks

Perform these steps to deploy an appliance and configure an RSA Authentication Manager primary instance.

**Procedure**

1. Deploy the appliance. Depending on your deployment, do one of the following:
   - For a virtual appliance, you must deploy the RSA Authentication Manager Open Virtualization Format (OVF) template. You can either Deploy the Virtual Appliance Through VMware vCenter Server or Deploy the Virtual Appliance Directly to the VMware ESXi Server.
   - For a hardware appliance, see Deploy the Hardware Appliance.
2. Configure the appliance with Quick Setup, a software wizard that creates access permission and specifies whether the appliance is a primary instance or a replica instance. See Run Quick Setup on the Primary Instance.
3. Accept the internal RSA certificate authority (CA) certificate. See Certificate Management for Secure Sockets Layer.
4. Log On to the Consoles.

## Deploying the Virtual Appliance

You can deploy the RSA Authentication Manager Open Virtualization Format (OVF) template through VMware vCenter or to the ESXi Server. For instructions, see the following:

- Deploy the Virtual Appliance Through VMware vCenter Server
- Deploy the Virtual Appliance Directly to the VMware ESXi Server

### Deploy the Virtual Appliance Through VMware vCenter Server

You can deploy a virtual appliance through VMware vCenter Server, if you are using this administrative tool to manage the virtual appliances.

**Note:** Depending on your VMware vCenter configuration and the version of the VMware vSphere Client, some of the windows that are described in the following procedure may not display. The window names may also vary.

### Before You Begin

- Collect the required information about each appliance instance being deployed. See Secure Appliance Deployment on page 19.
- Copy the RSA Authentication Manager Open Virtual Appliance (OVA) file to a location accessible to VMware.

#### Procedure

1. In the VMware vSphere Client, log on to VMware vCenter Server.
2. Select **File > Deploy OVF Template** to start the deployment wizard.
3. On the Source window, under **Deploy from a file or URL**, click **Browse**, and locate the RSA Authentication Manager OVA file to deploy. Click **Next**.
4. On the OVF Template Details window, verify that "RSA Authentication Manager" and the expected version number displays. Click **Next**.
5. On the End User License Agreement window, scroll to read the agreement. Click **Accept**, and **Next**.
6. On the Name and Location window, enter a **Name** for the virtual appliance, and click **Next**.
7. On the Host/Cluster window, select a host or cluster for the virtual appliance. Click **Next**.
8. On the Resource Pool window, select a resource pool. Resource pools let you manage your resources within a host or cluster. Click **Next**.
9. On the Storage window, select an existing VMware datastore for the virtual machine files. A VMware datastore can be a location such as a Virtual Machine File System (VMFS) volume, a directory on Network Attached Storage, or a local file system path. Click **Next**.
10. On the Disk Format window, select a format for storing virtual disks.
11. On the Network Mapping window, select the networks for the virtual appliance. Click **Next**.
12. On the Properties window, enter the IPv4 network settings for the virtual appliance, and click **Next**:
    - Fully Qualified Domain Name
    - IP Address.
    - Subnet Mask
    - Default Gateway
    - (Optional) Primary DNS Server
    - (Optional) Secondary DNS Server

**Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.

13. On the Ready to Complete window, review your settings, and click **Finish**. VMware requires approximately five minutes to deploy the virtual appliance.
14. Power on the virtual machine.
15. Click the **Launch Virtual Machine Console** button.

    The virtual machine console displays the progress of the virtual appliance deployment.
16. Wait for 30 seconds to select the default keyboard layout, English (United States). To choose another keyboard layout, press any key and follow the instructions on the screen.
17. Verify that the settings are correct. To accept the settings, type **y**, or wait 30 seconds.
18. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record this required information:
    - The Quick Setup URL includes the IP address that you entered in step 12.

      `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.
19. Enter the Quick Setup URL in the browser, including https, and press ENTER:

    `https://<IP Address>/`

**Note:** If you want 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.

## Deploy the Virtual Appliance Directly to the VMware ESXi Server

You can deploy a virtual appliance directly to the VMware ESXi server (VMware Hypervisor). VMware vCenter is not required to deploy the virtual machine.

Depending on your configuration of the VMware ESXi server and the version of the server, some of the windows that are described in the following procedure may not display. The window names may also vary.

### Before You Begin

- Collect the required information about each appliance instance being deployed. See Secure Appliance Deployment on page 19.
- Copy the RSA Authentication Manager Open Virtual Appliance (OVA) file to a location accessible to VMware.

### Procedure

1. In the VMware vSphere Client, log on to the VMware ESXi server.
2. Select **File > Deploy OVF Template** to start the deployment wizard.

3. On the Source window, under **Deploy from a File or URL**, click **Browse**, and locate the RSA Authentication Manager OVA file to deploy. Click **Next**.
4. On the OVF Template Details window, verify that "RSA Authentication Manager" and the expected version number displays. Click **Next**.
5. On the End User License Agreement window, scroll to read the agreement. Click **Accept**, and **Next**.
6. On the Name and Location window, enter a **Name** for the virtual appliance, and click **Next**.
7. On the Datastore window, select a directory for the virtual machine files. A VMware datastore can be a location such as a Virtual Machine File System (VMFS) volume, a directory on Network Attached Storage, or a local file system path. Click **Next**.
8. On the Disk Format window, select a format for storing virtual disks.
9. On the Network Mapping window, select the networks for the virtual appliance. Click **Next**.
10. On the Ready to Complete window, review your settings, and click **Finish**. VMware requires approximately five minutes to deploy the virtual appliance.
11. Power on the virtual machine.
12. For the virtual appliance, click the **Console** tab.

    The OS Console displays the progress of the boot sequence.
13. Wait for 30 seconds to select the default keyboard layout, English (United States). To choose another keyboard layout, press any key and follow the instructions on the screen.
14. When you are prompted by the OS Console, enter the IPv4 network settings for the virtual appliance:
    - Fully Qualified Hostname
    - IP Address
    - Subnet Mask
    - Default Gateway
    - (Optional) DNS Server Configuration

    **Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.
15. Verify that the settings are correct. To accept the settings, type **y**, or wait 30 seconds.

16. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record this required information:
    - The Quick Setup URL includes the IP address that you entered in step 14.

      `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.
17. Enter the Quick Setup URL in the browser, including https, and press ENTER:

    `https://<IP Address>/`

    **Note:** If you want 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.

## Deploy the Hardware Appliance

Use the following procedure to deploy the hardware appliance.

### Before You Begin

Collect the information and items that are required for a hardware deployment. For more information, see Secure Appliance Deployment on page 19.

### Procedure

1. Connect a keyboard and monitor to the hardware appliance.
2. Connect the power cord to the appliance and power on the appliance.
3. When the appliance boot screen displays, select **Start RSA Authentication Manager** and press ENTER, or wait 10 seconds for Authentication Manager to load automatically.

   **Note:** Do not use the F2 or F4 function key options that display for language and keyboard settings in the boot screen. After you start Authentication Manager, you can change the keyboard language when you are prompted for these settings.

4. By default, the keyboard is configured for **English (United States)**.To retain this setting, wait 30 seconds. To configure a new language, do the following:
   a. Press any key.
   b. Type the number that is associated with the language you want to configure, and press ENTER.

5. Review and accept the license agreement. Do the following:
   a. Press ENTER to view each proceeding line of the license agreement or press the spacebar key to view the next screen of text.
      You must press ENTER or the spacebar until you reach the end of the license agreement.
   b. When prompted, type **yes** to accept the license agreement, and press ENTER.
6. 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
7. When prompted to confirm the network settings, verify the settings are correct. To accept the settings, type **y**.
8. After the network settings are configured, the Quick Setup URL and the Quick Setup Access Code display. Record this required information:
   - The Quick Setup URL includes the IP address that you entered in step 6.

     `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.
9. If you have not done so already, connect the appliance to the network.

## Run Quick Setup on the Primary Instance

Quick Setup configures the appliance as an RSA Authentication Manager 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.

If you do not complete Quick Setup, you will be prompted to verify the network settings every time you power on the virtual or hardware appliance.

### Before You Begin

- You must have deployed a virtual appliance or hardware appliance.
- Verify that the browser on the local computer can access the license file (.zip) used during Quick Setup. For more information, see Secure Appliance Deployment on page 19.

### Procedure

1. Launch Quick Setup. Open a web browser and go to the following URL:

   https://<*IP ADDRESS*>

   where <*IP ADDRESS*> is the IP address of the appliance.
2. 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."
3. When prompted, enter the Quick Setup Access Code, and click **Next**.
4. On the Primary and Replica Quick Setup window, click **Start Primary Quick Setup**.
5. On the Primary Quick Setup page, click **Start Step 1**.
6. Specify the location of the license file (.zip), and click **Upload**.
7. Review the license summary, and click **Next**.
8. On the Date & Time page, do the following:
   a. In the **Time Zone** section, do the following in this order:
      - Select a region, for example, America.
      - Select a location. If the time zone uses Daylight Savings Time, two offsets from Coordinated Universal Time (UTC) are shown, for example, (UTC-05/UTC-04) New York.

   b. In the **Time Source** section, choose how you want the time to be set on the appliance, manually (hardware appliance only) or automatically (hardware or virtual appliance.

      To automatically synchronize the time on a hardware appliance or virtual appliance to an NTP server:

      a. Select **Sync to NTP Server**.

      b. Enter the hostname or IP address for a local or Internet Network Time Protocol (NTP) server.

         You may enter a second NTP server. If Quick Setup cannot connect to an NTP server, you can add an NTP Server in the Operations Console after Quick Setup is complete.

      c. To test the connection to the NTP server and verify that the correct time is selected, click **Preview Current Date & Time**.

      To automatically synchronize the time on a virtual appliance to the VMware host machine:

      a. Select **Sync to the physical machine hosting this virtual appliance**.

      b. To test the connection to the virtual host and verify that the correct time is selected, click **Preview Current Date & Time**.

To manually set the time on a hardware appliance:

a. Select **Set System Time**.

b. From the date box, select the date.

c. From the time drop-down boxes, select the hour and minute.

c. Click **Next**.

9. On the OS Password page, create and confirm the operating system password, and click **Next**.

**Note:** The operating system password is required to log on to the primary instance.

Record the operating system password, so that you can access it when you need it. For security reasons, RSA does not provide a utility for recovering the operating system password.

10. On the Initial Administration Accounts page, create the initial administration credentials for the Security Console Super Admin and the Operations Console (OC) administrator. Click **Next**.

**Important:** The User ID must be unique. It can contain 1 to 255 ASCII characters. The characters &% > < ` are not allowed. If a User ID contains unsupported characters, the user cannot authenticate.

Record these User IDs and passwords.

**Note:** After you complete Quick Setup, you can create additional Super Admin and Operations Console administrator accounts in the Security Console.

11. Review the information that you have entered. If you want to change anything, click **Back**, and make the change on the appropriate page. If necessary, use the navigation links at the top of the page.

12. Click **Start Configuration**.

After the instance is configured, direct links are provided to the Security Console and the Operations Console.

### Next Steps

- Web browsers used to administer Authentication Manager must have JavaScript enabled. See your web browser documentation for instructions on enabling JavaScript.
- After Quick Setup completes, you can change the appliance network settings in the Operations Console. Network Setting changes made in the VMware vSphere Client will no longer take effect.

## Certificate Management for Secure Sockets Layer

Secure Sockets Layer (SSL) is enabled by default for communication ports that are used for RSA Authentication Manager administration and replication. When you deploy an instance of Authentication Manager, communication is secured by a long-lived SSL certificate. This certificate is unique to your deployment, and it is signed by an internal RSA certificate authority (CA).

Because this SSL certificate is signed by an internal RSA CA, your browser may present a warning message that the default certificate cannot be verified. If an Online Certificate Status Protocol (OCSP) client is deployed, you may receive a message that revocation list information is not available. This is expected behavior.

To continue, click the option that your browser presents that allows you to proceed or to connect to an untrusted site. For example, your browser might ask you to click a link that reads “I Understand the Risks.”

To prevent this warning message from displaying, you must add the internal RSA CA to your browser’s trusted root certificate list, or replace the RSA certificate with one that is signed by a certificate authority that is trusted by your browser.

See your browser documentation for instructions about adding the internal RSA CA to your browser’s list of trusted root certification authorities.

## Log On to the Consoles

This procedure describes how to access the Security Console, Operations Console, and the Self-Service Console.

### Procedure

1. Open a supported web browser, and enter one of the URLs listed in the following table. Each console supports more than one URL.

| Console | URLs |
|---|---|
| Security Console | https://<*fully qualified domain name*><br>https://<*fully qualified domain name*>/sc<br>https://<*fully qualified domain name*>:7004/console-ims |
| Operations Console | https://<*fully qualified domain name*>/oc<br>https://<*fully qualified domain name*>:7072/operations-console |
| Self-Service Console | If there is no web tier, enter:<br>https://<*fully qualified domain name*>/ssc<br>https://<*fully qualified domain name*>:7004/console-selfservice<br><br>After installing a web tier, enter:<br>https://<*fully qualified virtual host name*><br>https://<*fully qualified virtual host name*>/ssc<br>https://<*fully qualified virtual host name*>/console-selfservice<br><br>If you change the default load balancer port, enter:<br>https://<*fully qualified virtual host name*>:<*virtual host port*>/<br>https://<*fully qualified virtual host name*>:<*virtual host port*>/ssc<br>https://<*fully qualified virtual host name*>:<*virtual host port*>/console-selfservice |

   For example, if the fully qualified domain name of your appliance installation is "host.mycompany.com," to access the Security Console, enter one of the following URLs in your web browser:

   https://host.mycompany.com

   https://host.mycompany.com/sc

   https://host.mycompany.com:7004/console-ims

2. If your web browser is configured for an enhanced security level, you must add an entry to the list of allowed or trusted sites. See your browser documentation for instructions about adding allowed or trusted sites.

3. 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.

   For more information on the Console accounts and passwords, see Administrative Accounts on page 91.

   **Important:** The Security Console may take up to 10 minutes to complete initial startup.

# 3 Deploying a Replica Appliance

## Perform Deployment Tasks

Perform these steps to deploy an appliance and deploy an RSA Authentication Manager replica instance.

### Procedure

1. Deploy the appliance. Depending on your deployment, do one of the following:
   - For a virtual appliance, you must deploy the RSA Authentication Manager Open Virtualization Format (OVF) template. You can either Deploy the Virtual Appliance Through VMware vCenter Server or Deploy the Virtual Appliance Directly to the VMware ESXi Server.
   - For a hardware appliance, see Deploy the Hardware Appliance.
2. Generate and Download a Replica Package File
3. Configure the appliance with Quick Setup, a software wizard that creates access permission and specifies whether the appliance is a primary instance or a replica instance. See Run Quick Setup on the Replica Instance.
4. Attach the Replica Instance to the Primary Instance

## Generate and Download a Replica Package File

Before you can add a replica instance to the deployment, you must create a replica package file on the primary instance. This file has configuration data that enables the replica instance to connect to the primary instance. The replica instance must have access to this file.

### Before You Begin

You must be an Operations Console administrator.

### Procedure

1. On the primary instance, log on to the Operations Console.
2. Click **Deployment Configuration > Instances > Generate Replica Package**.
3. Click **Download** to download the replica package file, and click **Save** to save the replica package to your local machine. The name of the replica package file is **replica_package.zip**.
4. Click **Done** to return to the Operations Console Home page.

# Run Quick Setup on the Replica Instance

Quick Setup performs the following tasks to add a replica appliance to the deployment:

- Quick Setup configures the appliance as an RSA Authentication Manager replica instance.
- Quick Setup attaches the replica instance to the primary instance.

After Quick Setup configures the replica instance, you can choose one of the following options:

- Attach the replica instance immediately to the primary instance.
- Defer attaching the replica instance until a later time.

If you choose to defer attaching the replica instance, Quick Setup powers off the replica instance. The next time you power on the replica instance, you can access Quick Startup to complete the attach process.

As a best practice, RSA recommends that you 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.

If you do not complete Quick Setup, you will be prompted to verify the network settings every time you power on the virtual or hardware appliance.

### Before You Begin

- Collect the required information about each replica instance that you want to set up. See Deployment Checklist for a Replica Instance on page 23.
- For a virtual appliance, you must have deployed the virtual appliance. For instructions, see Deploying the Virtual Appliance on page 29.
- For a hardware appliance, you must deploy the appliance. For instructions, see Deploy the Hardware Appliance on page 33.
- Generate and Download a Replica Package File on page 41.

### Procedure

1. Launch Quick Setup. Open a browser and go to the following URL:

   https://<*IP ADDRESS*>

   where <*IP ADDRESS*> is the IP address of the replica appliance.
2. 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.”
3. When prompted, enter the Quick Setup Access Code, and click **Next**.
4. On the Primary and Replica Quick Setup window, click **Start Replica Quick Setup**.

5. On the Replica Quick Setup page, click **Start Step 1**.
6. On the Date & Time Settings page, do the following in this order:
   a. In the **Time Zone** section, do the following in this order:
      - Select a region, for example, America.
      - Select a location. If the time zone uses Daylight Savings Time, two offsets from Coordinated Universal Time (UTC) are shown, for example, (UTC-05/UTC-04) New York.

   b. In the **Time Source** section, choose how you want the time to be set on the appliance, manually (hardware appliance only) or automatically (hardware or virtual appliance.

      To automatically synchronize the time on a hardware appliance or virtual appliance to an NTP server:

      a. Select **Sync to NTP Server**.
      b. Enter the hostname or IP address for a local or Internet Network Time Protocol (NTP) server.

         You may enter a second NTP server. If Quick Setup cannot connect to an NTP server, you can add an NTP Server in the Operations Console after Quick Setup is complete.

      c. To test the connection to the NTP server and verify that the correct time is selected, click **Preview Current Date & Time**.

      To automatically synchronize the time on a virtual appliance to the VMware host machine:

      a. Select **Sync to the physical machine hosting this virtual appliance**.
      b. To test the connection to the virtual host and verify that the correct time is selected, click **Preview Current Date & Time**.

      To manually set the time on a hardware appliance:

      a. Select **Set System Time**.
      b. From the date box, select the date.
      c. From the time drop-down boxes, select the hour and minute.

   c. Click **Next**.
7. Create and confirm the operating system password, and click **Next**.

   **Note:** The operating system password is required to log on to the replica instance.

   Record the operating system password for future use. For security reasons, RSA does not provide a utility for recovering the operating system password.
8. Review the information that you have entered. If you want to change anything, click **Back**, and make the change on the appropriate page. If necessary, use the navigation links at the top of the page.

9. Click **Start Configuration**.
   After the instance is configured, do one of the following:
   - Click **Begin Attach** to attach the replica instance to the primary instance. For more information, see Attach the Replica Instance to the Primary Instance on page 44.
   - 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.

### Next Step

- Replica Attachment Issues and Solutions on page 46.

## Attach the Replica Instance to the Primary Instance

Attaching the replica instance to the primary instance enables the replica instance to synchronize data with the primary instance. The replica instance records all authentications locally and sends the authentication and log data to the primary instance at regular intervals. When the primary instance is unavailable, the replica instance holds this data locally until the primary instance becomes available.

**Important:** The replica instance cannot authenticate users during the attachment process.

The instances use the TCP/IP protocol over an encrypted link for secure database synchronization. Instances can communicate over a local area network (LAN) or a wide area network (WAN). For information on firewalls, see Port Usage on page 81.

### Before You Begin

Confirm the following:

- You generated a replica package file on the primary instance and downloaded the replica package to your local machine. For instructions, see Generate a Replica Package on page 59.
- The primary and replica instances can resolve and connect to each other on the following ports:
  - 7002/TCP
  - 1812/TCP
  - 1813/TCP

  **Note:** Ports 1812 and 1813 are used by RSA RADIUS. If you do not plan to use RSA RADIUS, you must still open these ports on your network, for example, on any firewalls sitting between the primary instance and the replica instance, for attachment to succeed.

- The RSA RADIUS service is running on the primary instance.

  Even if you do not plan to use RADIUS, the service must be running for the replica attachment to succeed.
- The clocks on the primary and replica instances are synchronized. If the clocks are off by more than 10 minutes, the attachment fails.
- If you deferred attaching the replica instance after it was configured using Quick Setup, power on the replica instance and access Quick Setup. Quick Setup resumes at the Attach to Primary Instance page.

### Procedure

1. On the Attach to Primary Instance page under **Upload Replica Package**, click **Browse,** and select the replica package file to upload from your local machine. Click **Next**.
2. Under **Provide Credentials**, enter your Operations Console administrator User ID and password, and click **Next**.

### Next Steps

- Check the replication status by viewing the Replication Status Report for the replica instance. In the Operations Console for the replica instance, click **Deployment Configuration** > **Instances** > **Status Report**.
- If you are using RSA RADIUS, verify the replication status of the RADIUS server. In the Security Console for the replica instance, click **RADIUS > RADIUS Servers**.
- Make sure that the web browsers used to access the Security Console or the Operations Console have JavaScript enabled. See your web browser documentation for instructions on enabling JavaScript.
- After the replica instance is attached to the primary instance, network setting changes made in the VMware vSphere Client will no longer take effect. Use the Operations Console in the primary instance to change the network settings.

## Replica Attachment Issues and Solutions

If replica attachment requires additional information, perform the tasks listed in the following table.

| Issue | Solution |
|---|---|
| The replica instance cannot resolve the primary instance hostname. | In the **Associated Primary IP Address** field, enter the primary instance IP address, and click **Next**. |
| The replica instance cannot reach the primary instance. | In the **Retry Options** field, correct the primary instance IP address. Choose one of the following options:<br>• Address network connectivity issues, and then try to reach the primary instance again.<br>• Select the **Override IP Address** field, and enter the correct IP address for the primary instance. This information is saved in the hosts file of this appliance, and it overrides the DNS configuration, if a DNS server is available.<br>Click **Next**, and enter your Operations Console administrator credentials. |
| The primary instance cannot resolve the replica instance hostname | 1. Update the DNS server, if applicable, or use the primary instance Operations Console to edit the hosts file with the correct information for the replica instance.<br>For more information, see the Operations Console Help topic “Edit the Appliance Hosts File.”<br>2. Click **Next**. |

| Issue | Solution |
|---|---|
| The replica instance cannot communicate with the primary instance on the RADIUS ports. | Verify that the RSA RADIUS service is running on the primary instance. To do so:<br>1. Log on to the Operations Console on the primary instance.<br>2. Select **Deployment Configuration > RADIUS Servers**.<br>3. If prompted, enter your Super Admin user ID and password.<br>4. Click the server that you want to restart.<br>5. From the context menu, select **Restart Server**.<br>6. Select **Yes, restart RADIUS server**, and click **Restart Server**.<br>After less than one minute, the RSA RADIUS Service starts.<br>7. Verify that the network configuration permits remote connections over ports 1812/TCP and 1813/TCP.<br>8. Click **Next**. |
| The primary instance cannot communicate with the replica instance on the communication port 7002/TCP, and the RADIUS ports 1812/TCP and 1813/TCP. | 1. Verify that the network configuration permits remote connections over the communication port 7002/TCP, and the RADIUS ports 1812/TCP and 1813/TCP.<br>2. Click **Next**. |
| If the time difference between the primary instance and replica instance is greater than 10 minutes, replica attachment fails. | You can change the time.<br>On the primary instance, log onto the primary instance Operations Console and select **Administration > Date & Time**.<br>On the replica instance, redeploy the replica instance with the correct time. To do so:<br>1. Delete the failed replica instance from the Operations Console on the primary instance. For instructions, see the Operations Console Help topic “Delete a Replica Instance.”<br>2. Do the following:<br>• For a hardware appliance, perform a factory reset. For more information, see the Operations Console Help topic “Factory Reset.”<br>• For a virtual appliance, in VMware vCenter or on the ESXi server, shut down and delete the virtual appliance for the failed replica instance.<br>3. Deploy a new replica instance. |

# 4 Configuring a Virtual Host and Load Balancer

## Virtual Host and Load Balancer Overview

The virtual host is the gateway to the DMZ for users outside of the network who use risk-based authentication (RBA), the Self-Service Console, and dynamic seed provisioning. You must configure a virtual host and assign each web tier to the virtual host.

Load balancing distributes web tier traffic to the web tier servers. The web-tier deployment can include a load balancer or you can use round robin DNS. The virtual host can be associated with up to 2 load balancers.

For more information on network configurations that require a load balancer, see the *Planning Guide*.

## Load Balancer Requirements

A load balancer must meet the following requirements:

**User persistence.** The load balancer must send a client to the same server repeatedly during a session. The load balancer must send the client to the same Authentication Manager instance or web-tier server, depending on your deployment scenario, during an authentication session.

**X-Forwarded-For headers.** Load balancers in the application layer cause all requests to appear to come from the load balancer. You must configure load balancers to send the original client IP address in the "X-Forwarded-For" header. This is the default for most application layer load balancers.

In addition to the required features, consider the following:

**HTTPS Redirection.** The load balancer must be able to redirect HTTPS requests to another URL. This allows users to use the load balancer hostname to access the Self-Service Console.

## Configure a Load Balancer and Virtual Host

When adding a load balancer, you must configure a virtual hostname, IP address, and listening port. The load balancer acts as the virtual host providing an entry point to the demilitarized zone (DMZ). You must configure the virtual host before you can install a web tier.

If your deployment has a load balancer, the virtual hostname must resolve to the public IP address of the load balancer.

If your deployment does not have a load balancer, the virtual hostname must resolve to the public IP address of your web tier.

If you change the name of the load balancer or use another load balancer, you must change the virtual hostname accordingly.

### Before You Begin

- You must be a Super Admin.
- The virtual hostname must be configured in the Domain Name System (DNS) to point to the load balancer.

### Procedure

1. In the Operations Console on the primary instance, click **Deployment Configuration** > **Virtual Host & Load Balancing**.
2. If prompted, enter your Super Admin User ID and password.
3. On the Virtual Host & Load Balancing page, do the following:
   a. Select **Configure a virtual host and load balancers**.
   b. Enter a fully qualified virtual hostname unique to the deployment.
   c. (Optional) Change the default port number.
   d. Enter up to two load balancer IP addresses. If you are not using a load balancer, leave the IP address blank.
   e. Click **Add**.
4. Click **Save**.
   The system saves the virtual hostname and key material in the keystore file.
5. On the confirmation page, read **Mandatory Next Steps**.
6. Click **Done**.

### Next Steps

In the Operations Console, perform the appropriate mandatory next steps.

- If you updated load balancer details, you must reboot the primary and replica instances. In the Operations Console, click **Maintenance > Reboot Appliance** and reboot each instance.
- If you updated the virtual hostname, generate a new integration script for each web-based application using RBA, and then redeploy the integration scripts. For more information, see the *Administrator's Guide*.
- If the deployment includes a web tier, update the web tier. In the Operations Console, click **Deployment Configuration > Web-Tier Deployments > Manage Existing**. Click the update link for each web tier.
- If the deployment includes a web tier, replace the certificate on the load balancer and on the firewall with the virtual host certificate.

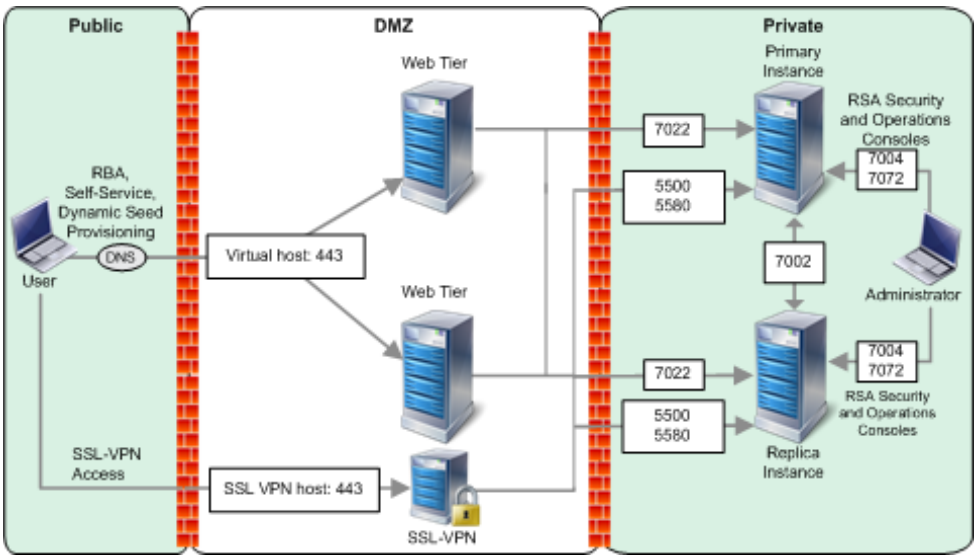
- If the deployment uses dynamic seed provisioning, update the hostname and port for the CT-KIP URL with the hostname and port that you specified for the virtual host. In the Security Console, go to **Setup** > **System Settings**. Click **Tokens**.
- If the deployment uses the RSA Self-Service Console, update the Self-Service Console URL with the hostname and port you specified for the virtual host. In the Security Console, go to **Setup** > **Self-Service Settings**. Click **E-Mail Notifications for User Account Changes**.

## Load Balance Using the Web Tier with Round Robin DNS

If you do not want to use a load balancer, you can set up the web-tier servers to distribute risk-based authentication (RBA) requests using round robin Domain Name System (DNS).

To set up load balancing using round robin DNS, associate the virtual hostname with the publicly accessible IP addresses of the web-tier servers in your DNS, and then enable round robin. The DNS server then sends RBA requests to web-tier servers.

The following figure shows a sample deployment of Authentication Manager using round robin DNS load balancing.



# 5 Installing Web Tiers

## Web Tier Overview

A web tier is a secure platform for installing and deploying the Self-Service Console, dynamic seed provisioning, and the risk-based authentication (RBA) service.

The web tier protects the private network by receiving and managing inbound internet traffic before it enters the private network. This prevents end users from accessing the private network through the Self-Service Console or web-based applications, such as SSL-VPNs, thin clients, or web portals. The web-tier server only sends a subset of the traffic, such as authentication traffic, securely to your private network.

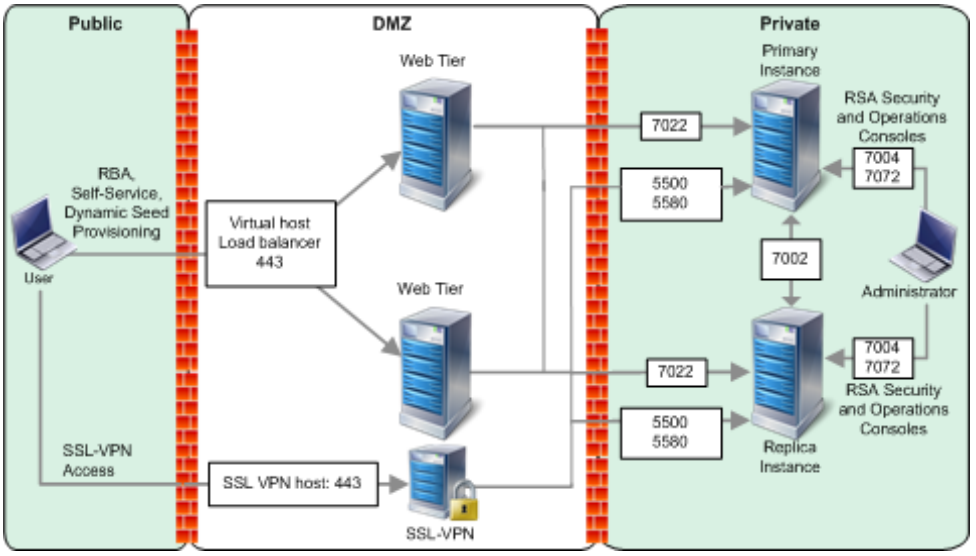
In addition to providing network security, deploying Authentication Manager on a web-tier server in your network demilitarized zone (DMZ) offers the following benefits:

- You can customize the end-user interface for the RBA service and web-based applications.
- Improves system performance by removing some processing tasks from the back end server.

Web-tier installation requires a primary instance. It is preferable that there is at least one replica instance of Authentication Manager located in your private network, as well as a load balancer and two web-tier servers located in your DMZ. An instance can have up to 16 web tiers. You need Super Admin permissions to manage the Authentication Manager and the web-tier servers.

Web tiers are not required, but your deployment might need them to satisfy your network configuration and requirements. For more information on the Authentication Manager deployment types, see the *Planning Guide*.

The following diagram shows traffic flow and ports in a typical web-tier deployment.

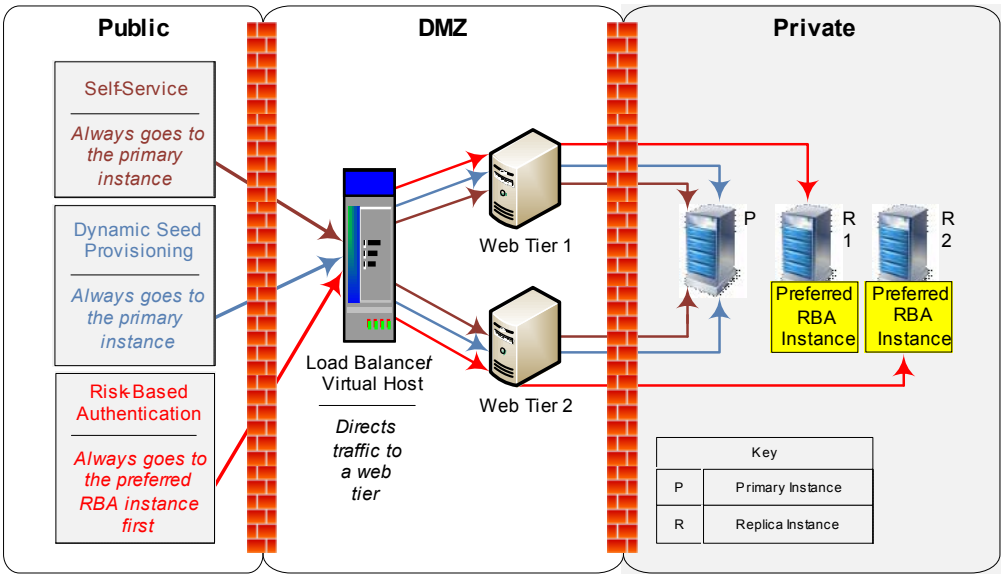



## Self-Service, Dynamic Seed Provisioning, and RBA Traffic in a Web Tier

In Authentication Manager, self-service and dynamic seed provisioning traffic is routed to the primary instance because these services can only run on the primary instance. RBA can run on any instance, but Authentication Manager always routes RBA traffic to the preferred RBA instance to distribute the workload.

The preferred RBA instance is the first instance to which Authentication Manager directs RBA traffic. You must choose a preferred RBA instance when you deploy a web tier. RSA recommends that you select a different preferred RBA instance for each web tier. You can select any Authentication Manager instance as a preferred RBA instance.

The following diagram shows how Self-Service, dynamic seed provisioning, and RBA traffic flows through a web tier.




If ever the preferred RBA instance is unavailable, Authentication Manager directs RBA traffic to the next instance on the server list.

Note that if you delete a replica that is a preferred RBA instance, the associated web tier is also deleted. RBA traffic flow through the deleted web tier is stopped. If the deployment has a load balancer and virtual host, make sure that they no longer point to the deleted replica and associated web tier.

## Web-Tier Hardware and Operating System Requirements

The following table lists the minimum requirements for the web-tier server. RSA recommends that you adjust these requirements upwards based on expected usage.

| Description | Requirements |
|---|---|
| Hardware | • Hard Drive: 2 GB for web tier installation<br>• Hard Drive: 4 GB-20 GB free space for logs and updated component downloads<br>• RAM: 2 GB<br>• CPU: A CPU with a dual-core processor or better, or 2 or more CPUs. |
| Ports | External Firewall: 443 HTTPS (TCP)<br>DMZ: 443 HTTPS (TCP)<br>Internal Firewall: 7022 T3S (TCP) |

| Description | Requirements |
|---|---|
| Operating Systems | • Red Hat Enterprise Linux 5 Server (64-bit)<br>• Red Hat Enterprise Linux 6 Server (64-bit)<br>• Windows Server 2008 R2 (64-bit)<br>• Windows Server 2012 (64-bit) |

## Performing Web Tier Pre-Installation Tasks

Before installing a web tier, perform the following tasks to set up the web-tier environment.

### Procedure

1. Verify that you have Super Admin permissions, and permissions to install software.
2. Verify that you have access to the Operations Console.
3. On Linux systems, verify that the open files hard limit for the local user is at least 4096.
4. Make sure that your web-tier servers meet the recommended hardware and operating system requirements. For more information, see Web-Tier Hardware and Operating System Requirements on page 55.
5. Set up the web-tier servers in the network DMZ.
6. Confirm that the date and time on the web-tier server match the date and time on the instance with which the web tier will be associated (primary or replica) within one minute. The time zones do not have to be the same. For example, the web-tier server time can be 7:00 am (GMT), and the associated instance time can be 9:00 am (GMT + 2).
7. Configure the virtual host. The virtual hostname can be a load balancer hostname or a round-robin Domain Name System (DNS). For instructions, see Chapter 4, Configuring a Virtual Host and Load Balancer.
8. (Optional) On the virtual host, replace the default certificate. For instructions, see the *Administrator's Guide*.
9. On the load balancer and on the firewall, replace the certificate with the virtual host certificate. For instructions, see your load balancer and firewall documentation.

# Installing the Web Tier

The following procedure lists the tasks for installing the web tier that is associated with the primary instance. You must perform these tasks before you associate a replica instance with a web tier.

**Before You Begin**

- Confirm that the virtual host and load balancer are configured.
- Decide which instance to select as the preferred RBA instance for each web tier.

**Procedure**

1. On the public and private DNS servers, enter the web-tier hostname and IP address.
2. On the primary instance, add a web-tier deployment record and generate a web-tier deployment package. For instructions, see Add a Web-Tier Deployment Record on page 57.
3. On the web-tier server, run the RSA Authentication Web-Tier Installer for your platform. For instructions, see the following:

   Install a Web Tier on Windows Using the Graphical User Interface on page 60.
   Install a Web Tier on Windows Using the Command Line on page 61.
   Install a Web Tier on Linux Using the Graphical User Interface on page 62.
   Install a Web Tier on Linux Using the Command Line on page 63.
4. Modify the Self-Service Console URL to point to the virtual host and virtual host port. For instructions, see the Security Console Help topic “Configure E-mail Notifications for Self-Service User Account Changes.”
5. If your deployment uses dynamic seed provisioning, modify the token-key generation URL to point to the virtual hostname, virtual host port, and self-service console. For instructions, see the Security Console Help topic “Configure Token Settings.”

# Add a Web-Tier Deployment Record

A web-tier deployment record must exist in the database on the primary instance before you can install a web tier. The web-tier deployment record establishes communication from the primary instance to web tier.

An instance can have up to 16 web tiers. Each web tier requires a web-tier deployment record.

In the last step of this procedure you can either generate the web-tier deployment package now or generate it at a later date. The web-tier deployment package contains the information that RSA Authentication Manager uses to connect a web tier to the associated instance. The web-tier deployment package is required prior to installing the web tier. If you generate the web-tier package now, you can install the web tier now.

### Before You Begin

- You must be a Super Admin.
- If you are installing a new web-tier deployment, configure a virtual hostname, listening port, and load balancer. For instructions, see Configure a Load Balancer and Virtual Host on page 49.

### Procedure

1. On the primary instance, in the Operations Console, click **Deployment Configuration** > **Web-Tier Deployments** > **Add New**.
2. If prompted, enter your Super Admin User ID and password.
3. On the Add New Web-Tier Deployment page, in the **Details** section, enter the following information:
   - **Deployment name.** The name you want for the web-tier deployment (0-255 characters. The & % > < ’ and ” characters are not allowed).
   - **Hostname.** Fully qualified hostname of the web-tier server where you are installing the web-tier deployment.
   - **Preferred RBA Instance.** The instance connected to this web-tier deployment to which risk-based authentication (RBA) traffic is directed.
4. In the **Web-Tier Service Options** section, turn any of the following services on or off.
   - Self-Service Console
   - Risk-based authentication
   - Dynamic seed provisioning
5. In the Virtual Host section, confirm the following information.
   - **Virtual Hostname**. Must be the fully qualified name of the virtual host.
   - **Port Number**. The default is 443.
6. Do one of the following:
   - Click **Save**. The system saves the record in the database on the associated primary instance. The trust certificate is updated when you generate a web-tier deployment package.
   - Click **Save & Generate Web-Tier Package**. The Generate Web-Tier Deployment Package screen is displayed.

**Note:** If the web-tier hostname is not resolved, a confirmation screen displays. Follow the instructions on the screen.

### Next Steps

- Confirm the details of this web-tier deployment record. For instructions, see the Operations Console Help topic “View Web Tier Deployments.”

- If you chose to save the web-tier deployment record without generating the web-tier deployment package, generate the web-tier deployment package before installing the web tier.
- Install the web tier. For instructions, see Installing the Web Tier on page 57.

## Web-Tier Installation Checklist

RSA Authentication Manager includes web-tier installers for Windows and Linux, which are located on the RSA Authentication Manager 8.1 download kit. Before you launch a web-tier installer, confirm the following:

- The web tier pre-installation tasks are completed.
- The web-tier server meets the system requirements.
- The public and private DNS servers are updated with the web-tier server IP address.
- A web-tier deployment package exists and has been transferred from the primary instance to the web-tier server.
- The Authentication Manager instance to which you will associate the web tier is running.
- You know the following information:
  - Directory name and location where you want the web-tier software installed
  - Fully qualified hostname of the web-tier server
  - Primary NIC IP address (IPv4) of the web-tier server
  - Web-tier deployment package name, location, and web-tier package password
  - For Linux, local user name (do not use root)
- The hostname in the web-tier deployment package matches the hostname on the target server.
- For Linux, you have root privileges.

After you confirm the items in the checklist, launch the installer you want to use and install the web tier.

- Install a Web Tier on Windows Using the Graphical User Interface
- Install a Web Tier on Windows Using the Command Line
- Install a Web Tier on Linux Using the Graphical User Interface
- Install a Web Tier on Linux Using the Command Line

## Install a Web Tier on Windows Using the Graphical User Interface

During installation, you run the RSA Authentication Web-Tier Installer on the web-tier server. This installs dynamic seed provisioning, the Self-Service Console and risk-based authentication (RBA) service.

Use only numbers and English characters when specifying paths and filenames. Single-byte and double-byte characters are not supported.

### Before You Begin

- Complete the Web-Tier Installation Checklist on page 59.
- Copy the RSA Authentication Manager 8.1 download kit to the appliance.

### Procedure

1. In the location where you copied the RSA Authentication Manager 8.1 download kit, go to **Webtier/windows-x86_64** and locate **install_webtier.bat**.
2. Do one of the following:
   - If User Access Control (UAC) is on, right click **install_webtier.bat** and select **Run As Administrator**.
   - If User Access Control (UAC) is off, double-click **install_webtier.bat**.
3. On the **Welcome** screen, read the overview and navigation instructions. Click **Next**.
4. On the **License Agreement** screen, read the license agreement, and click **Next**.
5. On the **Installation Folder** screen, specify the installation folder and click **Next**.
6. On the **Choose Web-Tier Package File** screen, do the following:
   a. Select the **Web-Tier Package** for the instance to which this web-tier server is associated.
   b. Type the **Password**.
   c. Click **Next**.
7. On the **Summary** screen, do one of the following:
   - If the summary is correct, click **Next**.
   - If the summary is incorrect, click **Previous**, and correct the information.
8. On the **Installation Progress** screen, wait for the progress bar to indicate that the installation is finished and click **Next**.
9. On the **Run Configuration** screen, wait for the configuration to complete and click **Next**.
10. On the **Installation Summary** screen, click **Done**.

### Next Steps

After you exit the web-tier installer, the Web-Tier Update Service connects to the primary server to install the necessary services. Use the Operations Console to check the status of this process.

In the Operations Console, click > **Deployment Configurations** > **Web-Tier Deployments** > **Manage Existing** to see the web tier installation status.

## Install a Web Tier on Windows Using the Command Line

During installation, you run the RSA Authentication Web-Tier Installer on the web-tier server. This installs dynamic seed provisioning, the Self-Service Console and risk-based authentication (RBA) service.

Use only numbers and English characters when specifying paths and filenames. Single-byte and double-byte characters are not supported.

### Before You Begin

Complete the Web-Tier Installation Checklist on page 59.

### Procedure

1. On the machine hosting the web-tier server, go to **Webtier/windows-x86_64** and launch **install.bat** in console mode.
2. On the command line, type the following and press ENTER.

   ```
   install.bat -console
   ```

3. On the **Welcome** screen, press ENTER.
4. On the **License Agreement** screen, press ENTER to continue.
5. On each successive **License Agreement** screen, you can do the following:
   a. Press ENTER to continue to the next page of the License Agreement.
      On the last screen, type **YES** and press ENTER to accept the terms of the license agreement.
   b. Type Q to quit the License Agreement.
      Type **YES** and press ENTER to accept the terms of the license agreement.
6. On the **Installation Folder** screen, enter the location of the installation folder and press ENTER.
7. On the **Choose Web Tier Package** screen, do the following:
   a. Enter the web-tier package location and file name, and press ENTER.
   b. Enter the web-tier package password, and press ENTER.
   c. Press ENTER.
8. On the **Summary** screen, review the summary and do one of the following:
   - If the summary is correct, type **1** to continue and press ENTER.
     The installation begins and the **Finish** screen displays when the installation is successful.
   - If the summary is incorrect, type **2** and press ENTER to quit.
     The installation terminates and you must begin again.
9. On the **Finish** screen, press ENTER to exit.

### Next Steps

After you exit the web tier installer, the Web-Tier Update Service connects to the primary server to install the necessary services. Use the Operations Console to check the status of this process.

In the Operations Console, click > **Deployment Configurations** > **Web-Tier Deployments** > **Manage Existing** to see the web tier installation status.

## Install a Web Tier on Linux Using the Graphical User Interface

During installation, you run the RSA Authentication Web-Tier Installer on the web-tier server. This installs dynamic seed provisioning, the Self-Service Console and risk-based authentication (RBA) service.

- Use only numbers and English characters when specifying paths and filenames. Single-byte and double-byte characters are not supported.
- The install user must have execute permission for the folder into which the web tier is installed.
- Do not save the web-tier installer and the web-tier package under the /root directory.
- Do not use spaces in the installation path.

### Before You Begin

- Verify that the open files hard limit for the local user is at least 4096.
- Complete the Web-Tier Installation Checklist on page 59.
- Copy the RSA Authentication Manager 8.1 download kit to the appliance.

### Procedure

1. Log on as root.
2. On the command line, change directories to the location where you copied the RSA Authentication Manager 8.1 download kit and do one of the following:
   - For Red Hat Enterprise Linux 5 Server (64-bit), type the following and press ENTER.

     ```
     Webtier/linux-x86_64
     ```
   - For Red Hat Enterprise Linux 6 Server (64-bit), type the following and press ENTER.

     ```
     Webtier/linux-x86_64
     ```
3. On the command line, type the following, and press ENTER:

   ```
   ./install_webtier.sh
   ```
4. On the RSA Authentication Manager Web-Tier Installer screen, click **Next**.
5. On the **Welcome** screen, read the overview and navigation instructions and click **Next**.
6. On the **License Agreement** screen, read the license agreement. Accept the terms, and Click **Next**.

7. On the **Installation Folder** screen, specify the installation folder and click **Next**.
8. On the **Choose Web-Tier Package File** screen, do the following:
   a. Select the **Web-Tier Package** for the instance to which this web-tier server is associated.
   b. Type the **Password**.
   c. Click **Next**.
9. On the Install User screen, enter the local user name and click Next.
10. On the **Summary** screen, do one of the following:
    - If the summary is correct, click **Next**.
    - If the summary is incorrect, click **Previous**, and correct the information.
11. On the **Installation Progress** screen, wait for the progress bar to indicate that the installation is complete and click **Next**.
12. On the **Run Configuration** screen, wait for the configuration to complete and click **Next**.
13. On the **Installation Summary** screen, click **Done**.

#### Next Steps

After you exit the web-tier installer, the Web-Tier Update Service connects to the primary server to install the necessary services. Use the Operations Console to check the status of this process.

In the Operations Console, click > **Deployment Configurations** > **Web-Tier Deployments** > **Manage Existing** to view the web tier installation status.

## Install a Web Tier on Linux Using the Command Line

During installation, you run the RSA Authentication Web-Tier Installer on the web-tier server. This installs dynamic seed provisioning, the Self-Service Console and risk-based authentication (RBA) service.

- Use only numbers and English characters when specifying paths and filenames. Single-byte and double-byte characters are not supported.
- The install user must have execute permission for the folder into which the web tier is installed.
- Do not save the web-tier installer and the web-tier package under the /root directory.
- Do not use spaces in the installation path.

#### Before You Begin

- Verify that the open files hard limit for the local user is at least 4096.
- Complete the Web-Tier Installation Checklist on page 59.

### Procedure

1. Log on as root.
2. On the command line, change directories to the location where you copied the RSA Authentication Manager 8.1 download kit and do one of the following:
   - For Red Hat Enterprise Linux 5 Server (64-bit), type the following and press ENTER.

     ```
     Webtier/linux-x86_64
     ```
   - For Red Hat Enterprise Linux 6 Server (64-bit), type the following and press ENTER.

     ```
     Webtier/linux-x86_64
     ```
3. On the command line, type the following and press ENTER.

   ```
   ./install_webtier.sh -console
   ```
4. On the **Welcome** screen, type **1** to continue and press ENTER.
5. On the **License Agreement** screen, press ENTER to continue.
6. On each successive **License Agreement** screen, you can do the following:
   - Press ENTER to continue to the next page of the License Agreement.
     On the last screen, type **YES** and press ENTER to accept the terms of the license agreement.
   - Type Q to quit the License Agreement.
     Type **YES** and press ENTER to accept the terms of the license agreement.
7. On the **Installation Folder** screen, do the following:
   a. Enter the location of the installation folder.
   b. Press ENTER.
8. On the **Choose Web Tier** screen, do the following:
   a. Enter the web-tier package location and file name, and press ENTER.
   b. Enter the web-tier package password, and press ENTER.
   c. Press ENTER.
9. On the **Installation User** screen, do the following:
   a. Enter the installation user, and press ENTER.
   b. Press ENTER.
10. On the **Summary** screen, review the summary and do one of the following:
    a. If the summary is correct, type **1** to continue and press ENTER.
       The installation begins and the **Finish** screen displays when the installation is successful.
    b. If the summary is incorrect, type **2** and press ENTER to quit.
       The installation terminates and you must begin again.
11. On the **Finish** screen, press ENTER to exit.

### Next Steps

After you exit the web tier installer, the Web-Tier Update Service connects to the primary server to install the necessary services. Use the Operations Console to check the status of this process.

In the Operations Console, click > **Deployment Configurations** > **Web-Tier Deployments** > **Manage Existing** to view the web tier installation status.

# 6 Next Steps for Your Deployment

After deploying RSA Authentication Manager, you must perform the required configuration tasks. You can perform additional configuration tasks based upon your deployment.

| Topic | Description | For More Information |
|---|---|---|
| **Required Steps for All Deployments** | | |
| Port Usage | Confirm that the ports on the primary and replica instances and the primary and replica web-tier servers are accessible to enable authentication, administration, replication, and other services on the network. | For more information, see Appendix B, Port Usage. |
| RSA Authentication Manager User Accounts | Each user must have an account in RSA Authentication Manager. You can create and store user accounts in the internal database, or you can link Authentication Manager directly to one or more external Lightweight Directory Access Protocol (LDAP) directories. | For more information on using the internal database, see the chapter "Administering Users" in the *Administrator's Guide*.<br>For more information on using your existing LDAP directories, see the chapter "Integrating LDAP Directories" in the *Administrator's Guide*. |
| Authentication Agents | An authentication agent is the component on the protected resource that communicates with RSA Authentication Manager to process authentication requests. Any resource that is used with SecurID authentication, on-demand authentication (ODA) or risk-based authentication (RBA) requires an authentication agent. | For a list of RSA authentication agents, go to **http://www.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings**.<br>For a list of third-party products that have embedded RSA agents, go to the RSA Secured® web site at **https://gallery.emc.com/community/marketplace/rsa?view=overview**. |

| Topic | Description | For More Information |
|---|---|---|
| **RSA RADIUS Configuration** | | |
| RSA RADIUS Configuration | In a RADIUS-protected network, RADIUS clients control user access at the network perimeter.<br>RADIUS clients, which can be VPN servers, wireless access points, or Network Access Servers connected to dial-in modems, interact with RSA RADIUS servers for user authentication and to establish appropriate access control parameters.<br>When authentication succeeds, RADIUS servers return a set of attributes to RADIUS clients for session control. | For more information, see the chapter "Administering RSA RADIUS" in the *Administrator's Guide*. |
| **Authentication Method Configuration** | | |
| Hardware and Software Tokens | **Hardware Token**<br>Device manufactured by RSA that generates and displays tokencodes. A tokencode is always displayed and changes automatically at intervals, such as every 60 seconds. The tokencode must be combined with the user's PIN to create a passcode, which enables authentication. Hardware tokens include PINPads, key fobs, and USB tokens.<br>**Software Token**<br>Software-based security token installed with an associated RSA SecurID application to a Windows desktop or laptop, web browser, an RSA Smart Card, a personal digital assistant (PDA), or a mobile device.<br>In most cases, software tokens are configured to request a user's PIN. The software token combines the PIN with the tokencode, and then displays the passcode, which enables authentication. | For more information, see the chapter "Deploying and Administering RSA SecurID Tokens" in the *Administrator's Guide*. |
| Risk-Based Authentication (RBA) | RBA identifies potentially risky or fraudulent authentication attempts by silently analyzing user behavior and the device of origin. RBA strengthens RSA SecurID authentication. | For more information, see the chapter "Deploying Risk-Based Authentication" in the *Administrator's Guide*. |
| On-Demand Authentication (ODA) | ODA delivers a one-time tokencode to a user by e-mail or text message. You must configure the on-demand tokencode delivery method. Install the authentication agent software on the resource that you want to protect, unless the agent is already embedded in the protected resource. | For more information, see the chapter "Deploying On-Demand Authentication" in the *Administrator's Guide*. |

| Topic | Description | For More Information |
|---|---|---|
| **Additional Deployment Steps** | | |
| Self-service configuration | You can configure RSA Authentication Manager to enable users to perform maintenance and troubleshooting tasks through the Self-Service Console. | For more information, see the chapter "RSA Self-Service" in the *Administrator's Guide*. |
| Securing Your Deployment | You may need to perform additional network and product configuration for secure operation, depending on your network topology and on the RSA Authentication Manager features that you intend to use.<br>In addition, each RSA Authentication Manager instance includes Clam Antivirus (ClamAV) software. ClamAV is an open-source software toolkit that is intended to reduce the risk of intrusion or malicious system or data access. | For more information, see the *Security Configuration Guide*. |

# A Upgrading RSA Authentication Manager 8.0 to 8.1

The RSA Authentication Manager 8.0 to 8.1 upgrade patch installs RSA Authentication Manager 8.1.

To install this upgrade, follow these procedures in order:

- Review the prerequisites. See Before Installing This Upgrade.
- Follow the standard steps to apply version 8.0 or 8.1 patches:
  - Specify an Upgrade Patch Location
  - Scan for Updates
  - Apply the Upgrade Patch
- Review the next steps that are specific to the upgrade.See After Installing this Upgrade on the Primary and Replica Instances.
- If your deployment includes a web tier, you must reinstall it. See Reinstall the Web Tier.

## Before Installing This Upgrade

Before installing this upgrade, review the following guidelines and requirements.

### VMware Snapshot Strongly Recommended

The RSA Authentication Manager 8.0 to 8.1 upgrade patch is not reversible.

**Note:** RSA strongly recommends taking a VMware snapshot of each virtual machine before upgrading.

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 running processes on the Authentication Manager instance.

For additional instructions, see the VMware vSphere Client documentation.

You can restore version 8.0 if you took a VMware snapshot before upgrading. Export your data or take other steps to preserve your data before reverting to a snapshot. See the *Administrator's Guide* for information about restoring snapshots.

## Required Credentials

The following credentials are required:

- The upgrade requires the operating system password for the rsaadmin user account on each virtual appliance.
- To apply the upgrade, you must have an Operations Console administrator account, with access to the Operations Console, for the primary instance and each replica instance.
- To reinstall the web tier, you must be a Super Admin.

## Replicated Deployments

If you have a replicated deployment, all replica instances must be running and replicating successfully when you apply the upgrade to the primary or replica instances. All instances must be able to communicate while the upgrade is applied. To verify the replication status, log on to the primary instance Operations Console, and then click **Deployment Configuration** > **Instances** > **Status Report**.

Apply this upgrade patch to the primary instance before upgrading the replica instances in your RSA Authentication Manager 8.0 deployment. On the primary instance, wait for the replication status to return to normal for all replica instances before upgrading the replica instances.

During the upgrade process, the upgraded version 8.1 primary instance and the existing version 8.0 replica instances can successful replicate. Be aware that you cannot attach a new version 8.0 replica instance to a version 8.1 primary instance.

## Required Disk Space

Each virtual appliance must have free disk space that is equal to the size of the current Authentication Manager database, plus 4 GB. For example, if the current database is 1 GB, then you need 5 GB of free disk space.

To determine the size of the current Authentication Manager database, log on to the appliance operating system using SSH or the VMware vSphere Client, and then run this command:

```
du -h -d 0 /opt/rsa/am/rsapgdata
```

The command displays output that is similar to the following example:

```
64M     /opt/rsa/am/rsapgdata
```

## Migrating From Version 7.1

Migrating from RSA Authentication Manager 7.1 to an upgraded version 8.1 deployment is not supported. If you attempt to do this, migration fails, and the RADIUS dictionary files are deleted.

After upgrading from version 8.0 to version 8.1, you cannot do a full migration. You can only choose to import data from version 7.1 while retaining the existing system settings and deployment topology. Migrate from version 7.1 before applying the version 8.0 to 8.1 upgrade patch, or migrate from version 7.1 to a new version 8.1 deployment. To recover the RADIUS dictionary files, see the Knowledgebase article **a63914** at **https://knowledge.rsasecurity.com/scolcms/knowledge.aspx?solution=a63914**.

## Patches for Version 8.0 and 8.1

RSA Authentication Manager 8.0 without patches or with any patch can be upgraded to version 8.1. The 8.0 to 8.1 upgrade kit installs the base version of 8.1, which includes the software fixes in the cumulative Patch 4 for version 8.0. After upgrading to version 8.1, you can obtain the fixes included in later 8.0 patches by applying the latest version 8.1 cumulative patch.

If you have applied Patch 5, 6, or 7 to version 8.0, then you should wait for RSA Authentication Manager 8.1 Patch 1 (P01) before upgrading. Version 8.1 Patch 1 will include the software fixes in the version 8.0 Patches 5 through 7.

# Specify an Upgrade Patch Location

To specify a product update location, or to edit a previously specified location, perform the following procedure to allow RSA Authentication Manager 8.0 to locate patches.

If you have already specified a location, see Scan for Updates on page 74.

### Before You Begin

Download the patch from **RSA SecurCare Online** to a location that the primary or replica instance can access.

To scan for updates on a DVD or CD, you must configure the virtual appliance to mount a DVD/CD or an ISO image. See the Operations Console Help topic "VMWare DVD/CD or ISO Image Mounting Guidelines."

### Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. On the **Update & Rollback** page, your local browser is configured as the method for applying an update. To change that setting, click **Configure Update Source**.
3. On the **Configure Update Sources** page, specify a location for updates.
   - To upload the update from your local machine, select **Use your web browser to upload an update**.
   - To scan for updates on an NFS share, select **Use NFS as the update source**. Enter the full path, including the IP address or hostname where updates are stored. For example: **192.168.1.2:/updates**

- To scan for updates on a Windows shared folder, select **Use Windows Share** as the update source.
  - In the **Windows Share Path** field, enter the full path, including the IP address or hostname where updates are stored. For example: **\\192.168.1.2\updates**
  - (Optional) In the **Windows Username** field, enter a username. If your Windows share configuration requires it, enter the domain and username.
  - (Optional) In the Windows Password field, enter a password only if it is required by your Windows share configuration.
- To scan for updates on a DVD or CD, select **Use DVD/CD as the update source**.

4. To test the NFS or Windows share directory settings, click **Test Connection**. A message indicates whether the configured shared directory is available to the primary or replica instance.
5. Click **Save**.

### Next Steps

Do one of the following:

- If you configured your local web browser as the method to apply an update, see Apply the Upgrade Patch on page 75.
- If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, see Scan for Updates on page 74.

## Scan for Updates

If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, you can scan to locate and review a list of available product updates.

### Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. Click **Scan for Updates**. You can view the progress of the scan on the **Basic Status View** tab. You can view more detailed information on the **Advanced Status View** tab.
3. Click **Done** to return to the **Update & Rollback** page.

   The **Available Updates** section displays a list of updates, with the following information for each update:

   - **Version**. The version of the update. To see the current Authentication Manager version, see the top of the Update and Rollback page.
   - **Reversible**. Indicates whether you can roll back (undo) the update. The upgrade patch is not reversible.

- **Automatic Appliance Reboot**. Indicates whether Authentication Manager automatically restarts the Appliance to apply the update. If the Appliance restarts, you must perform another scan to see a current list of updates.
- **Automatic Operations Console Reboot**. Indicates whether Authentication Manager automatically restarts the Operations Console to apply the update. If the Operations Console restarts, you must perform another scan to see a current list of updates.
- **Action**. States whether the update is available to apply. Lists the minimum system requirement for the update.

4. In the **Applied Updates** section, click **Download Detailed History Log** for a complete update history.

   The **Applied Updates** section displays the updates applied to the instance. This section includes the update version numbers, the time and date that each update was applied, and which administrator applied the update.

   After you scan for updates, the new list displays for 24 hours. Logging out of the Operations Console does not remove the list from the system cache. If you restart the Operations Console, download additional updates, or change the product update locations, you must perform another scan to see the most current list.

### Next Step

Apply the upgrade patch to the RSA Authentication Manager deployment.

## Apply the Upgrade Patch

Apply the upgrade patch to the primary instance first, and then to each replica instance. As each replica instance is updated, all of the accumulated data on each replica instance is sent to the primary instance.

### Before You Begin

- Specify an Upgrade Patch Location
- If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, Scan for Updates.
- In a replicated deployment, after upgrading the primary instance, wait for the replication status to return to normal for all replica instances before upgrading the replica instances. To verify the replication status, log on to the primary instance Operations Console, and click **Deployment Configuration** > **Instances** > **Status Report**.

### Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. 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.
3. In the **Password** field, enter the password for the operating system user **rsaadmin**, and click **Log On**.
4. The basic status messages appear while the update is applied. You can view more detailed information on the **Advanced Status View** tab.

After the patch is applied, the following occurs:

- 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**.

### Next Steps

- You can download a detailed log file containing the information that was displayed on the **Advanced Status View** tab. The file is named **update-*version-timestamp*.log**, where *version* is the update version number and *timestamp* is the time that the update completed. For instructions, see the Operations Console Help topic "Download Troubleshooting Files."
- Follow the steps in After Installing this Upgrade on the Primary and Replica Instances on page 77.
- If the deployment includes a web tier, see Reinstall the Web Tier on page 77.

## After Installing this Upgrade on the Primary and Replica Instances

After you have upgraded the primary instance and all of the replica instances, do the following:

- Verify that replication and radius replication is functioning correctly on the primary instance and the replica instance.
- The upgrade installs the base version of RSA Authentication Manager 8.1, which includes the fixes in the cumulative Patch 4 for version 8.0. As needed, obtain later software fixes by applying the latest version 8.1 patches to the upgraded Authentication Manager instances. For example, RSA Authentication Manager 8.1 P01 will include the fixes in RSA Authentication Manager 8.0 P5, P6, and P7.
- If you upgraded an RSA Authentication Manager 8.0 deployment that did not have any patches applied, then you should perform an additional step. RSA Authentication Manager 8.0 Patch 1 or later, and RSA Authentication Manager 8.1 at any patch level, prevent the syslog from logging the operating system password and the Simple Network Management Protocol (SNMP) passwords. To further secure these passwords, do the following:
  - Change the operating system account password and the passwords that are associated with your SNMP configuration. For instructions, see the Operations Console Help topics “Change the Operating System Account Password” and “Configure SNMP.”
  - Remove the operating system account password and the SNMP passwords from existing log entries. For instructions, see the knowledgebase article with the Solution ID a61380 on **RSA SecurCare Online**.

## Reinstall the Web Tier

If your deployment includes a web tier, after upgrading the primary and replica instances, you must upgrade the web tier. Follow these procedures to retain all existing web-tier configuration and customization settings:

1. Uninstall the Web Tier
2. Generate a New Web-Tier Deployment Package
3. Run the Web-Tier Installer for Your Platform
4. Update the Web Tier

### Uninstall the Web Tier

Uninstalling a web tier removes the web tier and all features and components of RSA Authentication Manager from the web-tier server. Uninstalling a web tier does not delete the web-tier deployment record.

For instructions, see the following:

Uninstall a Web Tier on Linux

Uninstall a Web Tier on Windows

## Uninstall a Web Tier on Linux

During uninstallation, run the RSA Authentication Web-Tier Uninstaller for Linux on the web-tier server.

### Before You Begin

- Confirm that you have root privileges.
- Verify that the open files hard limit for the local user is at least 4096.

### Procedure

1. Log on to the web-tier server.
2. Change directories to ***your-authentication-manager-web-tier-installation*/uninstall**.
3. On the command line, type:

   ```
   ./uninstall.sh
   ```

4. Press ENTER.
5. On the Welcome screen, type:

   ```
   yes
   ```

6. Press ENTER.

   The system uninstalls the web tier and displays “Uninstall Complete” when finished.

## Uninstall a Web Tier on Windows

During uninstallation, run the RSA Authentication Web-Tier Uninstaller for Windows on the web-tier server.

### Before You Begin

Confirm that you have Windows credentials to uninstall a program.

### Procedure

1. On the web-tier server, go to **Start** > **Control Panel** > **Programs and Features** > **Uninstall a Program**.
2. Right-click **RSA Authentication Web Tier**, and select **Uninstall**.
3. On the command line, type:

   ```
   y
   ```

   and press ENTER.

   When finished, the uninstaller screen displays Uninstall finished.
4. Press ENTER.

   The system removes the web-tier services and installation folders, except the top-level folder.

## Generate a New Web-Tier Deployment Package

On the primary instance, generate a new web-tier deployment package. The web-tier deployment package contains the information that Authentication Manager uses to connect the web tier to the preferred server.

### Before You Begin

- You must be a Super Admin.

### Procedure

1. In the Operations Console, click **Deployment Configuration** > **Web-Tier Deployments** > **Manage Existing**.
2. If prompted, enter your Super Admin User ID and password.
3. From the list of web-tier deployment records, click a web-tier deployment record to generate the package.
4. From the context menu, click **Generate Package**.
5. On the Generate Web-Tier Deployment Package page, verify the following information:
   - Hostname of the web-tier server
   - Preferred server hostname
6. Enter a web-tier package password.
7. Click **Generate Package**, and wait for the package to generate.
8. In the Download Web-Tier Deployment Package section, click **Download Package**.

## Run the Web-Tier Installer for Your Platform

On the web-tier server, run the RSA Authentication Web-Tier Installer for your platform. For instructions, see the following:

- Install a Web Tier on Windows Using the Graphical User Interface on page 60.
- Install a Web Tier on Windows Using the Command Line on page 61.
- Install a Web Tier on Linux Using the Graphical User Interface on page 62.
- Install a Web Tier on Linux Using the Command Line on page 63.

## Update the Web Tier

You must update the web tier when you make any changes such as updating your version of Authentication Manager and customizing the web-tier pages. Authentication Manager displays an update button in the Operations Console for each web tier that is not up-to-date. If you have multiple web tiers to update, update one web tier at a time. Each update can take up to 20 minutes to complete.

### Procedure

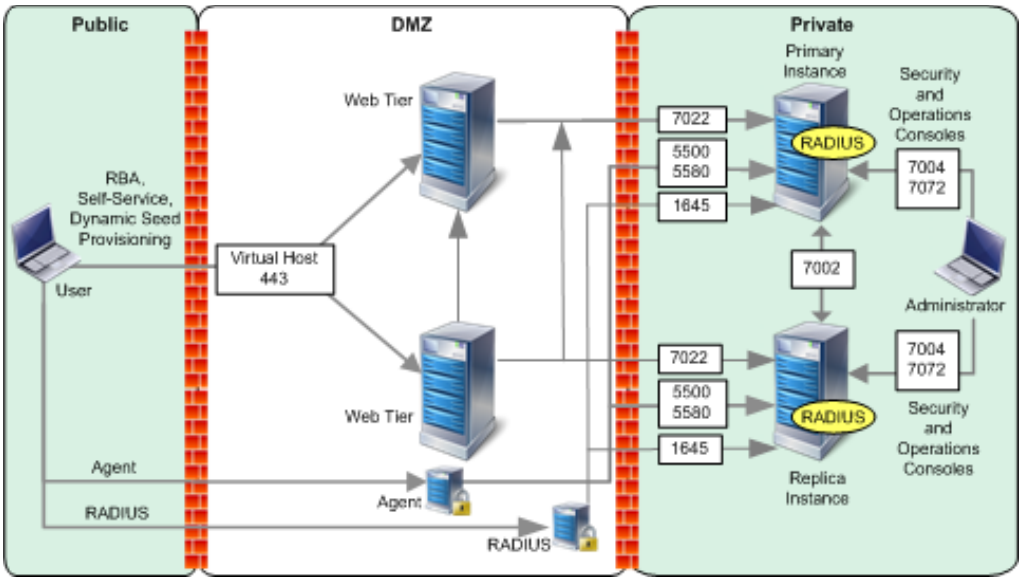
1. In the Operations Console, click **Deployment Configuration** > **Web-Tier Deployments** > **Manage Existing**.
2. On the Web Tiers page, in the **Status** column, click **Update** for the web tier that you want to update.

   When the update is complete, the **Status** column for the updated web tier displays **Online.**

# B Port Usage

## Port Traffic

The following figure represents a common RSA Authentication Manager deployment with primary and replica instances, web tiers, and a load balancer. An external firewall protects the primary and replica instances, and another external firewall protects the DMZ. For more information on RADIUS ports, see Ports for the RSA Authentication Manager Instance on page 82.



## Ports for the RSA Authentication Manager Instance

The RSA Authentication Manager instance has an internal firewall that limits traffic to specific ports. The internal firewall restricts inbound traffic to the hosts and services that provide product functionality. Outbound traffic is not restricted. RSA recommends that you deploy the instance in a subnet that also has an external firewall to segregate it from the rest of the network.

The following table lists ports used by the Authentication Manager instance. All ports support IPv4 only, unless IPv6 support is specified in the description.

| Port Number and Protocol | Function | Source | Description |
|---|---|---|---|
| 22, TCP | SSH | SSH client | Disabled by default. Allows the operating system account (rsaadmin) to access the operating system. |
| 49, TCP | TACACS authentication | TACACS client | Used to receive authentication requests from Network Access Device (NAD). |
| 80, TCP | Quick Setup<br>Operations Console, Security Console | Administrator's browser | Used for Quick Setup. After Quick Setup is complete, the appliance redirects connections from this port to the appropriate console. |
| 161, UDP | SNMP | SNMP client | Used by the Authentication Manager SNMP agent to listen for GET requests and send responses to a Network Management System (NMS).<br>This port is closed, unless SNMP is enabled. It can be configured in the Security Console. |
| 443, TCP | Quick Setup<br>Operations Console, Security Console, Self-Service Console | Administrator's browser | Used for Quick Setup. After Quick Setup is complete, the appliance redirects connections from this port to the appropriate console. |
| 1645, UDP | RADIUS authentication (legacy port) | RADIUS client | This port receives authentication requests from a RADIUS client. |

| Port Number and Protocol | Function | Source | Description |
|---|---|---|---|
| 1646, UDP | RADIUS accounting (legacy port) | RADIUS client | This port receives inbound accounting requests from a RADIUS client. |
| 1812, TCP | RADIUS replication port | Another RADIUS server | This port is used for communication between primary RADIUS and replica RADIUS services.<br>If you do not use RSA RADIUS, but you have replica instances, you must keep this port open. For more information, see Required RSA RADIUS Server Listening Ports on page 85. |
| 1812, UDP | RADIUS authentication | RADIUS client | This port receives authentication requests from a RADIUS client.<br>If you do not plan to use RSA RADIUS authentication, you can close this port. |
| 1813, TCP | RADIUS administration | RADIUS server | This port is used to administer RADIUS from the Security Console over the protected RADIUS remote administration channel.<br>If you do not use RSA RADIUS, but you have replica instances, you must keep this port open. For information, see Required RSA RADIUS Server Listening Ports on page 85. |
| 1813, UDP | RADIUS accounting | RADIUS client | This port receives accounting requests from a RADIUS client.<br>If you do not plan to use RSA RADIUS authentication, you can close this port. |
| 5500, TCP | Agent authentication | RSA SecurID Authentication protocol agents | Accepts requests from TCP-based authentication agents and sends replies. Required for RSA SecurID and on-demand authentication (ODA). This port supports both IPv4- and IPv6-compliant agents. |

| Port Number and Protocol | Function | Source | Description |
|---|---|---|---|
| 5500, UDP | Agent authentication | RSA SecurID Authentication protocol agents | Accepts requests from UDP-based authentication agents and sends replies. Required for RSA SecurID, ODA and risk-based authentication (RBA). This port only supports IPv4-compliant agents. |
| 5550, TCP | Agent auto-registration | RSA agents | Used for communication with authentication agents that are attempting to register with Authentication Manager. |
| 5580, TCP | Offline authentication service | RSA agents | Used to receive requests for additional offline authentication data, and send the offline data to agents. Also used to update server lists on agents.<br>This can be closed if offline authentications are not in use and no agents in your deployment use the Login Password Integration API. |
| 7002, TCP SSL-encrypted | Authentication Manager | Another appliance | Used for communication between an Authentication Manager primary and replica instances and for communication between replica instances (for replay detection).<br>Used by the RSA application programming interface (API).<br>Enable if you have at least one replica instance. |
| 7002, TCP SSL-encrypted | RSA Token Management snap-in for the Microsoft Management Console (MMC) | Microsoft Management Console | Enable this port if you plan to use the RSA Token Management snap-In to manage users and authenticators from MMC. |
| 7004, TCP SSL-encrypted | Security Console | Administrator's browser | Required for administering your deployment from the Security Console. Accepts requests for Security Console functions. |

| Port Number and Protocol | Function | Source | Description |
|---|---|---|---|
| 7004, TCP SSL-encrypted | Self-Service Console and RBA | User's browser | Required for using the elf-Service Console or RBA. Accepts requests for Self-Service Console functions and RBA authentication. |
| 7004, TCP SSL-encrypted | Cryptographic Token-Key Initialization Protocol (CT-KIP) | User's browser | Required for using dynamic seed provisioning. |
| 7022, TCP SSL-encrypted | Trusted realm network access point or the web tier. | Trusted realm, or the web tier and another appliance | Only enable this port if you have trusted realms or have a web tier. Used to communicate with trusted realms. Allows communication between the appliance and its web tier. |
| 7072, TCP SSL-encrypted | Operations Console | Super Admin's browser | Required for administering your deployment from the Operations Console. Accepts requests for Operations Console functions. |
| 7082, TCP SSL-encrypted | RADIUS Configuration SSL | Authentication Manager instance | Used for configuring RADIUS and restarting the RADIUS service from the Operations Console. |

## Restricting Access to the RSA Consoles

Access to the Security Console (port 7004) and the Operations Console (port 7072) should be restricted to internal administrators only. While port 7004 is used by the Security Console, dynamic seed provisioning, and the Self-Service Console, it should not be directly accessible outside the intranet. To allow access to the Self-Service Console or dynamic seed provisioning for external users, set up a web tier to help protect port 7004 and restrict access to the Security Console.

## Required RSA RADIUS Server Listening Ports

RSA RADIUS is installed and configured with RSA Authentication Manager. All the RADIUS-related ports (1645, 1646, 1812, 1813, and 7082) on the Authentication Manager server are open by default.

The RADIUS standard initially used UDP ports 1645 and 1646 for RADIUS authentication and accounting packets. The RADIUS standards group later changed the port assignments to 1812 and 1813. The Authentication Manager RADIUS server listens on all four ports for backward compatibility. If all the RADIUS clients are configured to talk to the RADIUS servers only on ports 1812 and 1813, you should block legacy ports 1645 and 1646 on the external firewall.

If you do not plan to use RSA RADIUS, but you have replica instances in your deployment, you must keep the TCP ports 1812 and 1813 open on your network. These ports are required for tasks such as replica attachment, replica promotion, and IP address and hostname changes. You can close the RADIUS authentication UDP ports 1812 and 1813.

## Port Considerations for Trusted Legacy Realms

RSA Authentication Manager 8.1 trusted realms communicate with RSA Authentication Manager 7.1 or 8.1 trusted realms using the ports listed in Ports for the RSA Authentication Manager Instance on page 82. To communicate with RSA Authentication Manager 6.1 trusted realms, you must configure a port range that Authentication Manager 8.1 uses for authentication. You configure this port range using the Security Console. The defaults are:

- Port range = 10 ports
- Minimum port = 10001
- Maximum port = 10010

These ports are closed unless an Authentication Manager 6.1 legacy trust relationship is established. You must configure any firewalls to allow access between the deployments.

You can change the default settings to improve performance or to coexist with other network services in the deployment. For example, if many users on Authentication Manager 8.1 are authenticating on several trusted legacy realms at the same time, RSA recommends that you increase the port range from the default.

To determine the number of ports to specify, multiply the number of trusted legacy realms by the number of legacy realm authentications that you expect to occur during a typical five-second window. For example, if you have 10 trusted legacy realms that expect two authentications to occur every five seconds, specify a port range of 20.

The Security Console does not verify if a port is already in use, so you must ensure that a port is available before you make any changes. Do not set the port range less than 10. A legacy realm requires at least 10 ports for authentication.

For instructions, see the Security Console Help topic “Configure Ports for Trusted Legacy Realm Authentication.”

## Ports on the Web Tier with a Load Balancer Deployed

The following table lists the default listening ports on the web-tier server when a load balancer is installed in a deployment.

If your environment has firewalls or proxy servers, make sure that they allow communication between the web tier and all other hosts and services that provide Authentication Manager functionality. These hosts and services, which are listed in the Source column, include Authentication Manager appliances, load balancers, and browsers.

| Port Number and Protocol | Function | Source | Destination | Description |
|---|---|---|---|---|
| 443, TCP | Self-Service Console, risk-based authentication (RBA), and dynamic seed provisioning | User's browser | Primary web-tier hostname | Accepts requests for Self-Service Console functions, RBA authentication, and dynamic seed provisioning. |
| 443, TCP | RBA | Load balancer | Web-tier virtual hostname | Accepts requests for RBA authentication that use the virtual hostname. |

## Ports on the Web Tier Without a Load Balancer

The following table lists the default listening ports on the web-tier server when a load balancer is not used in your deployment.

If your environment has firewalls or proxy servers, make sure that they allow communication between the web tier and all other hosts and services that provide Authentication Manager functionality. These hosts and services, which are listed in the Source column, include Authentication Manager appliances, load balancers, and browsers.

| Port Number and Protocol | Function | Source | Destination | Description |
|---|---|---|---|---|
| 443, TCP | Self-Service Console, risk-based authentication (RBA), and dynamic seed provisioning | User's browser | Primary web-tier hostname | Accepts requests for Self-Service Console functions, RBA authentication, and dynamic seed provisioning. |

| Port Number and Protocol | Function | Source | Destination | Description |
|---|---|---|---|---|
| 443, TCP | RBA | User's browser | Web-tier virtual hostname | Accepts requests for RBA authentication. |

**Important:** Keep port 443 (or another port number if you change the default) open on the replica web tier, so that a listening port is available.

## Access Through Firewalls

RSA recommends that you set up all RSA Authentication Manager instances in a subnet that has an external firewall to segregate it from the rest of the network. To enable authentication through external firewalls and to accommodate static Network Address Translation (NAT), you can configure alias IP addresses for Authentication Manager instances and alternate IP addresses for authentication agents. You can assign the following:

- Four distinct IP addresses (the original IP address and up to three aliases) to each Authentication Manager instance. For instructions, see the Security Console Help topic "Add Alternative IP Addresses for Instances."
- An unlimited number of alternate IP addresses (one primary IP address) to your agents. For instructions, see the Security Console Help topic "Add an Authentication Agent."

Each distinct IP address must be assigned to only one Authentication Manager instance. Authentication Manager instances must not share an IP address, even if it is hidden by NAT.

You must know the primary IP address and aliases for each Authentication Manager instance. If your deployment includes multiple locations, you must also know which ports are used for Authentication Manager communications and processes. You may need to open new ports in your firewall, or clear some existing ports for your deployment. Port translation is supported if the primary and replica instances are communicating on the standard Authentication Manager ports. For example, the primary and replica instances must communicate on port 7002, TCP. For more information on ports, see Port Traffic on page 81.

## Securing Connections Between the Primary and Replica Instances

Authentication Manager uses port 7002 to replicate data between the primary and replica instance databases. To secure this channel from unauthorized use, RSA recommends the following:

- If your deployment does not include a replica, or if your primary and replica instances are on the same LAN, close port 7002 on your external firewall (not the appliance firewall) so that it does not pass external traffic to the primary or replica instances.
- If your primary and replica instances are connected through a WAN and there is a firewall between them, open port 7002 on the firewall, but restrict traffic on this port to originate only from the IP addresses of the primary and replica instances.

# C Administrative Accounts

## System Administrator Accounts

The following accounts provide permission to modify, maintain, and repair the Authentication Manager deployment. Quick Setup creates these accounts with information that you enter.

- Authentication Manager Administrator Accounts
- Appliance Operating System Account

If you plan to record the logon credentials for these accounts, be sure that the storage method and location are secure.

### Authentication Manager Administrator Accounts

The following table lists the administrator accounts for Authentication Manager. The administrator who deploys the primary instance creates these accounts during Quick Setup.

| Name | Permissions | Management |
|---|---|---|
| Super Admin | Super Admins can perform all administrative tasks in the Security Console with full administrative permission in all security domains in the deployment. | Any Super Admin can create other Super Admin users in the Security Console.<br>An Operations Console administrator can recover a Super Admin account if no Super Admin can access the system. |

| Name | Permissions | Management |
|---|---|---|
| Operations Console administrator | Operations Console administrators can perform administrative tasks in the Operations Console. Operations Console administrators also use command line utilities to perform some procedures, such as recovering the Super Admin account. Command line utilities require the appliance operating system account password.<br><br>**Note:** Some tasks in the Operations Console also require Super Admin credentials. Only Super Admins whose records are stored in the internal database are accepted by the Operations Console. | Any Super Admin can create and manage Operations Console administrators in the Security Console. For example, you cannot recover a lost Operations Console administrator password, but a Super Admin can create a new one.<br><br>Operations Console administrator accounts are stored outside of the Authentication Manager internal database. This ensures that if the database becomes unreachable, an Operations Console administrator can still access the Operations Console and command line utilities. |

User IDs for a Super Admin and a non-administrative user are validated in the same way. A valid User ID must be a unique identifier that uses 1 to 255 ASCII characters. The characters & % > < ` are not allowed.

A valid User ID for an Operations Console administrator must be a unique identifier that uses 1 to 255 ASCII characters. The characters @ ~ are not allowed, and spaces are not allowed.

**Note:** Create an Operations Console administrator account for each Operations Console user. Do not share account information, especially passwords, among multiple administrators.

## Appliance Operating System Account

The appliance operating system account User ID is rsaadmin. This User ID cannot be changed. You specify the operating system account password during Quick Setup. You use this account to access the operating system when you perform advanced maintenance or troubleshooting tasks. The rsaadmin account is a privileged account to which access should be strictly limited and audited. Individuals who know the rsaadmin password and who are logged on as rsaadmin have sudo privileges and shell access.

Every appliance also has a root user account. This account is not needed for normal tasks. You cannot use this account to log on to the appliance.

You can access the operating system with Secure Shell (SSH) on a hardware appliance or a virtual appliance, or you can use the VMware vSphere Client on a virtual appliance. Before you can access the appliance operating system through SSH, you must use the Operations Console to enable SSH on the appliance.

An Operations Console administrator can change the rsaadmin password. For instructions, see the Operations Console Help topic "Change the Operating System Account Password." RSA does not provide a utility to recover the operating system password.

## Manage a Super Admin Account

Only a Super Admin can manage a Super Admin account.

### Procedure

1. In the Security Console, click **Identity > Users > Manage Existing**.
2. Use the search fields to find the user that you want to edit.
3. Click the user that you want to edit and select **Edit**.
4. Update the user settings.
5. Click **Save**.

# D Installing the RSA Authentication Manager Token Management Snap-In

## Overview

The RSA Token Management snap-in provides a convenient way to manage RSA SecurID tokens for deployments that have an Active Directory identity source. The RSA Token Management snap-in extends the context menus, property pages, control bars, and toolbars in the Active Directory Users and Computers snap-in for the Microsoft Management Console (MMC). You can use the RSA Token Management snap-in to enable or disable a token, assign a token, or perform other token-related tasks without logging on to the Security Console. For more information on the administrative actions enabled by this extension, see the *Administrator's Guide*.

## System Requirements

You can install the RSA Token Management Snap-In on the following platforms:

- Windows Server 2008 R2 Domain Controller
- Windows Server 2008 R2 Server with the Active Directory Domain Services (AD DS) Snap-Ins and Command Line Tools
- Windows Server 2008 Server with the Active Directory Domain Services Snap-Ins and Command Line Tools
- Windows 7 with the with the Active Directory Domain Services Snap-Ins and Command Line Tools

## Install the Token Management Snap-In for Local Access

Use this procedure if you want to administer the Authentication Manager through the Token Management Snap-In directly on the host where Active Directory is installed.

### Before You Begin

You must have the administrative permissions. These permissions (for example, domain level) depend on your Windows network configuration. At minimum, you must be a domain administrator and a local machine administrator.

**Procedure**

1. Obtain the RSA Token Management Snap-In installation files. The files are in the RSA Authentication Manager 8.1 – Token Management Snap-In for MMC.zip file that you can download from RSA SecurCare Online.
2. Unzip all of the installation files into a directory that is located on the same machine where you are installing the snap-in.
3. Do one of the following:
   - If you have a 32-bit operating system, run **setup32.exe**.
   - If you have a 64-bit operating system, run **setup64.exe**.

   **Note:** The installer also installs the Visual C++ redistributable package and Microsoft.NET framework if they are not already present.
4. Respond to the prompts for **Welcome**, **Select Region**, and **License Agreement**.
5. For Authentication Manager server settings, enter values for the following:
   - Authentication Manager server hostname
   - Authentication Manager server port number
   - Command Server Port
6. When prompted for **Destination Location**, either accept the default location or enter an alternative location.
7. Review the Pre-installation screen, and click **Next** to continue.
8. Click **Finish**.

## Install the Token Management Snap-In for Remote Access

Use this procedure if you want to administer the Authentication Manager through the Token Management Snap-In remotely from Windows 7 or a Windows Server 2008 without Active Directory.

Active Directory Domain Services (AD DS) Snap-Ins and Command Line Tools are part of the Remote Server Administration Tools and are used for remotely managing Active Directory Domain Controllers from Windows Server 2008 R2, Windows Server 2008 or Windows 7 machines.

For Windows 7, you can perform remote administration using the Remote Server Administration Tools. This tools package must be downloaded and installed separately, and can be installed only on Windows 7 (32-bit and 64-bit).

On Windows 2008, the Remote Server Administration Tools feature is part of the operating system and can be added from the Server Manager.

You can enable the AD DS Snap-Ins and Command Line Tools after installing the Remote Server Administration Tools.

### Before You Begin

- For Windows 7, download and install the Remote Server Administration Tools package from the Microsoft web site.
- You must have the appropriate permissions. These permissions (for example, domain level) depend on your Windows network configuration. At minimum, you must be a domain administrator and a local machine administrator.
- The administrator using the AD DS Snap-In and Command Line Tools to remotely administer the Active Directory must have appropriate administrative permissions. These permissions (for example, domain level) depend on your Windows network configuration.

### Procedure

1. Enable the **AD DS Snap-Ins and Command Line Tools** feature in Remote Server Administration Tools.
2. Obtain the RSA Token Management Snap-In installation files. The files are in the RSA Authentication Manager 8.1 – Token Management Snap-In for MMC.zip file that you can download from RSA SecurCare Online.
3. Unzip all of the installation files into a directory that is located on the same machine where you are installing the snap-in.
4. Do one of the following:
   - If you have a 32-bit operating system, run **setup32.exe**.
   - If you have a 64-bit operating system, run **setup64.exe**.
5. Respond to the prompts for **Welcome**, **Select Region**, and **License Agreement**.
6. For Authentication Manager server settings, enter values for the following:
   - Authentication Manager server hostname
   - Authentication Manager server port number
   - Authentication Manager Command Server Port
7. When prompted for **Destination Location**, either accept the default location or enter an alternative location.
8. Review the Pre-installation screen, and click **Next** to continue.
9. Click **Finish**.

# Performing Post-Installation Tasks

After a successful installation, perform the following tasks to complete the MMC Extension setup.

### Procedure

1. Make sure that the Authentication Manager is set up and running.
2. Make sure that Active Directory is configured and registered as an identity source. For more information see the chapter "Integrating an LDAP Directory" in the *Administrator's Guide*.
3. Start the Active Directory User and Computer Management Console to open the RSA Token Management Snap-In.
4. Configure the Connection with Authentication Manager
5. Make sure that the Windows user for the Token Management Snap-In is a valid Active Directory administrator and a valid Authentication Manager administrative user. For more information on administrator and administrative permissions, see the chapter "Preparing RSA Authentication Manager for Administration" in the *Administrator's Guide.*

## Start the Active Directory User and Computer Management Console

To use the Token Management Snap-In for Authentication Manager administration, you must start the Active Directory User and Computer Management Console.

### Before You Begin

Perform all of the preceding steps in Performing Post-Installation Tasks.

### Procedure

Do one of the following:

- Click **Control Panel > Administrative Tools > Active Directory Users and Computers**.
- From a command prompt, run **dsa.msc**.

## Configure the Connection with Authentication Manager

You must specify connection settings such as server information and authentication information to enable the Token Management snap-in to access Authentication Manager Server.

### Before You Begin

Perform all of the preceding steps in Performing Post-Installation Tasks

### Procedure

1. Access the Active Directory Users and Computers Management Console.
2. Click on any user. This makes the RSA button visible in the toolbar.

3. Click **RSA** in the toolbar.
   The RSA Token Management Setting page is displayed.
4. In the **Server Information** section, do the following:
   a. In the **AM Server Host** field, enter the name of the machine on which RSA Authentication Manager is running.
   b. In the **AM Server port** field, enter the port number on which RSA Authentication Manager is running.
   c. In the **Command Server Port** field, enter the port number on which the Command Server is running on the Authentication Manager Server.
5. In the **Authentication Information** section, do the following:
   a. Select the **UserID type** for the user.
      The format of the username displayed in the **Login User** field will be based on the chosen UserID type.

      **Important:** The UserID type must be the same as that defined for this identity source in the Authentication Manager.
      This user must be a member of the Domain Administrators group in Active Directory and must be assigned Super Admin privileges in Authentication Manager.

   b. In the **User Password** field, enter the user's password.
   c. Click **Test Authentication** to perform a test authentication.
      If the UserID exists in more than one identity source, you can choose the identity source to test. The chosen identity source will be displayed in the **Identity Source Name** field. When prompted to use the certificate for future communication, click yes.

# Glossary

**Active Directory**

The directory service that is included with Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2008, and Microsoft Windows Server 2008 R2.

**Active Directory forest**

A federation of identity servers for Windows Server environments. All identity servers share a common schema, configuration, and Global Catalog.

**administrative role**

A collection of permissions and the scope within which those permissions apply.

**administrator**

Any user with one or more administrative roles that grant administrative permission to manage the system.

**agent host**

The machine on which an agent is installed.

**appliance**

The hardware or guest virtual machine running RSA Authentication Manager. The appliance can be set up as a primary instance or a replica instance.

**approver**

A Request Approver or an administrator with approver permissions.

**assurance level**

For risk-based authentication, the system categorizes each authentication attempt into an assurance level that is based on the user's profile, device, and authentication history. If the authentication attempt meets the minimum assurance level that is required by the RBA policy, the user gains access to the RBA-protected resource. Otherwise, the user must provide identity confirmation to access the RBA-protected resource.

**attribute**

A characteristic that defines the state, appearance, value, or setting of something. In Authentication Manager, attributes are values associated with users and user groups. For example, each user group has three standard attributes called Name, Identity Source, and Security Domain.

**attribute mapping**

The process of relating a user or user group attribute, such as User ID or Last Name, to one or more identity sources linked to the system. No attribute mapping is required in a deployment where the internal database is the primary identity source.

**audit information**

Data found in the audit log representing a history of system events or activity including changes to policy or configuration, authentications, authorizations, and so on.

**audit log**

A system-generated file that is a record of system events or activity. The system includes four such files, called the Trace, Administrative, Runtime Audit, and System logs.

**authentication**

The process of reliably determining the identity of a user or process.

**authentication agent**

A software application installed on a device, such as a domain server, web server, or desktop computer, that enables authentication communication with Authentication Manager on the network server. See agent host.

**authentication method**

The type of procedure required for obtaining authentication, such as a one-step procedure, a multiple-option procedure (user name and password), or a chained procedure.

**authentication protocol**

The convention used to transfer the credentials of a user during authentication, for example, HTTP-BASIC/DIGEST, NTLM, Kerberos, and SPNEGO.

**authentication server**

A component made up of services that handle authentication requests, database operations, and connections to the Security Console.

**authenticator**

A device used to verify a user's identity to Authentication Manager. This can be a hardware token (for example, a key fob) or a software token.

**authorization**

The process of determining if a user is allowed to perform an operation on a resource.

**backup**

A file that contains a copy of your primary instance data. You can use the backup file to restore the primary instance in a disaster recovery situation. An RSA Authentication Manager backup file includes: the internal database, appliance-only data and configuration, keys and passwords used to access internal services, and internal database log files. It does not include all the appliance and operating system log files.

**certificate**

An asymmetric public key that corresponds with a private key. It is either self-signed or signed with the private key of another certificate.

**certificate DN**

The distinguished name of the certificate issued to the user for authentication.

**command line utility (CLU)**

A utility that provides a command line user interface.

**core attributes**

The fixed set of attributes commonly used by all RSA products to create a user. These attributes are always part of the primary user record, whether the deployment is in an LDAP or RDBMS environment. You cannot exclude core attributes from a view, but they are available for delegation.

**Cryptographic Token-Key Initialization Protocol (CT-KIP)**

A client-server protocol for the secure initialization and configuration of software tokens. The protocol requires neither private-key capabilities in the tokens, nor an established public-key infrastructure. Successful execution of the protocol results in the generation of the same shared secret on both the server as well as the token.

**custom attributes**

An attribute you create in Authentication Manager and map to a field in an LDAP directory. For example, you could create a custom attribute for a user's department.

**data store**

A data source, such as a relational database (Oracle or DB2) or directory server (Microsoft Active Directory or Oracle Directory Server). Each type of data source manages and accesses data differently.

**delegated administration**

A scheme for defining the scope and responsibilities of a set of administrators. It permits administrators to delegate a portion of their responsibilities to another administrator.

**delivery address**

The e-mail address or the mobile phone number where the on-demand tokencodes will be delivered.

**deployment**

An installation of Authentication Manager that consists of a primary instance and, optionally, one or more replica instances.

**demilitarized zone**

The area of a network configured between two network firewalls.

**device history**

For risk-based authentication, the system maintains a device history for each user. It includes the devices that were used to gain access to protected resources.

**device registration**

For risk-based authentication, the process of saving an authentication device to the user's device history.

**distribution file password**

A password used to protect the distribution file when the distribution file is sent by e-mail to the user.

**distributor**

A Token Distributor or an administrator with distributor permissions.

**DMZ**

See demilitarized zone.

**dynamic seed provisioning**

The automation of all the steps required to provide a token file to a device that hosts a software token, such as a web browser, using the Cryptographic Token-Key Initialization Protocol (CT-KIP).

**e-mail notifications**

Contain status information about requests for user enrollment, tokens, and user group membership that is sent to users who initiated the request. For token requests, e-mail notifications also contain information about how to download and activate tokens. Request Approvers and Token Distributors receive e-mail notifications about requests that require their action. See e-mail templates.

**e-mail templates**

Templates that administrators can use to customize e-mail notifications about user requests for user enrollment, tokens, user group membership, or the on-demand tokencode service. See e-mail notifications.

**excluded words dictionary**

A dictionary containing a record of words that users cannot use as passwords. It prevents users from using common, easily guessed words as passwords.

**fixed passcode**

Similar to a password that users can enter to gain access in place of a PIN and tokencode. The format for fixed passcodes is defined in the token policy assigned to a security domain. An administrator creates a fixed passcode in a users authentication settings page. Fixed passcodes can be alphanumeric and contain special characters, depending on the token policy.

**Global Catalog**

A read-only, replicated repository of a subset of the attributes of all entries in an Active Directory forest.

**Global Catalog identity source**

An identity source that is associated with an Active Directory Global Catalog. This identity source is used for finding and authenticating users, and resolving group membership within the forest.

**identity attribute**

Customer-defined attributes that are mapped to an existing customer-defined schema element. They are always stored in the same physical repository as the user's or user group's core attribute data. You can search, query, and report on these attributes. Each identity attribute definition must map to an existing attribute in an LDAP directory or RDBMS.

**identity confirmation method**

For risk-based authentication, an authentication method that can be used to confirm a user's identity.

**identity source**

A data store containing user and user group data. The data store can be the internal database or an external directory server, such as Microsoft Active Directory.

**instance**

An installation of RSA Authentication Manager that can be set up as a primary instance or a replica instance. An instance also includes a RADIUS server.

**internal database**

The Authentication Manager proprietary data source.

**keystore**

The facility for storing keys and certificates.

**load balancer**

A deployment component used to distribute authentication requests across multiple computers to achieve optimal resource utilization. The load balancer is usually dedicated hardware or software that can provide redundancy, increase reliability, and minimize response time. See Round Robin DNS.

**lower-level security domain**

In a security domain hierarchy, a security domain that is nested within another security domain.

**minimum assurance level**

See assurance level.

**node secret**

A long-lived symmetric key that the agent uses to encrypt the data in the authentication request. The node secret is known only to Authentication Manager and the agent.

**on-demand tokencode**

Tokencodes delivered by SMS or SMTP. These tokencodes require the user to enter a PIN to achieve two-factor authentication. On-demand tokencodes are user-initiated, as Authentication Manager only sends a tokencode to the user when it receives a user request. An on-demand tokencode can be used only once. The administrator configures the lifetime of an on-demand tokencode. See on-demand tokencode service.

**on-demand tokencode service**

A service that allows enabled users to receive tokencodes by text message or e-mail, instead of by tokens. You configure the on-demand tokencode service and enable users on the Security Console.

**Operations Console**

An administrative user interface through which the user configures and sets up Authentication Manager, for example, adding and managing identity sources, adding and managing instances, and disaster recovery.

**permissions**

Specifies which tasks an administrator is allowed to perform.

**preferred instance**

The Authentication Manager instance that the risk-based authentication service in the web tier communicates with first. Also, the instance that provides updates to the web tier. Any instance can be the preferred instance. For example, you can configure a replica instance as the preferred instance.

**primary instance**

The installed deployment where authentication and all administrative actions are performed.

**promotion, for disaster recovery**

The process of configuring a replica instance to become the new primary instance. During promotion, the original primary instance is detached from the deployment. All configuration data referring to the original primary instance is removed from the new primary instance.

**promotion, for maintenance**

The process of configuring a replica instance to become the new primary instance when all instances are healthy. During promotion, a replica instance is configured as a primary instance. The original primary instance is demoted and configured as a replica instance.

**provisioning**

See token provisioning.

**provisioning data**

The provisioning server-defined data. This is a container of information necessary to complete the provisioning of a token device.

**RADIUS**

See Remote Authentication Dial-In User Service.

**RBA**

See risk-based authentication.

**RBA integration script**

A script that redirects the user from the default logon page of a web-based application to a customized logon page. This allows Authentication Manager to authenticate the user with risk-based authentication. To generate an integration script, you must have an integration script template.

**realm**

A realm is an organizational unit that includes all of the objects managed within a single deployment, such as users and user groups, tokens, password policies, and agents. Each deployment has only one realm.

**Remote Authentication Dial-In User Service (RADIUS)**

A protocol for administering and securing remote access to a network. A RADIUS server receives remote user access requests from RADIUS clients, for example, a VPN.

**replica instance**

The installed deployment where authentication occurs and at which an administrator can view the administrative data. No administrative actions are performed on the replica instance.

**replica package**

A file that contains configuration data that enables the replica appliance to connect to the primary appliance. You must generate a replica package before you set up a replica appliance.

**requests**

Allows users to enroll, as well as request tokens, the on-demand tokencode service, and user group membership.

**Request Approver**

A predefined administrative role that grants permission to approve requests from users for user enrollment, tokens, or user group membership.

**risk-based authentication (RBA)**

An authentication method that analyzes the user's profile, authentication history, and authentication device before granting access to a protected resource.

**risk engine**

In Authentication Manager, the risk engine intelligently assesses the authentication risk for each user. It accumulates knowledge about each user's device and behavior over time. When the user attempts to authenticate, the risk engine refers to its collected data to evaluate the risk. The risk engine then assigns an assurance level, such as high, medium, or low, to the user's authentication attempt.

**round robin DNS**

An alternate method of load balancing that does not require dedicated software or hardware. When the Domain Name System (DNS) server is configured and enabled for round robin, the DNS server sends risk-based authentication (RBA) requests to the web-tier servers. See Load Balancer.

**scope**

In a deployment, the security domain or domains within which a role's permissions apply.

**Secure Sockets Layer (SSL)**

A protocol that uses cryptography to enable secure communication over the Internet. SSL is widely supported by leading web browsers and web servers.

**Security Console**

An administrative user interface through which the user performs most of the day-to-day administrative activities.

**security domain**

A container that defines an area of administrative management responsibility, typically in terms of business units, departments, partners, and so on. Security domains establish ownership and namespaces for objects (users, roles, permissions, and so on) within the system. They are hierarchical.

**security questions**

A way of allowing users to authenticate without using their standard method. To use this service, a user must answer a number of security questions. To authenticate using this service, the user must correctly answer all or a subset of the original questions.

**self-service**

A component of Authentication Manager that allows the user to update user profiles, change passwords for the Self-Service Console, configure life questions, clear devices enabled for risk-based authentication, change e-mail addresses or phone numbers for on-demand authentication, and manage on-demand authentication PINs. The user can also request, maintain, and troubleshoot tokens.

**Self-Service Console**

A user interface through which the user can update user profiles, change passwords for the Self-Service Console, configure life questions, clear devices enabled for risk-based authentication, change e-mail addresses or phone numbers for on-demand authentication, and manage on-demand authentication PINs. Users can also request, maintain, and troubleshoot tokens on the Self-Service Console.

**session**

An encounter between a user and a software application that contains data pertaining to the user's interaction with the application. A session begins when the user logs on to the software application and ends when the user logs off of the software application.

**shipping address**

An address used by distributors to distribute hardware tokens.

**silent collection**

For risk-based authentication, a period during which the system silently collects data about each user's profile, authentication history, and authentication devices without requiring identity confirmation during logon.

**SSL**

See Secure Sockets Layer.

**Super Admin**

An administrator with permissions to perform all administrative tasks in the Security Console. A Super Admin:

- Can link identity sources to system
- Has full permissions within a deployment
- Can assign administrative roles within a deployment

**system event**

System-generated information related to nonfunctional system events, such as server startup and shutdown, failover events, and replication events.

**System log**

A persistable store for recording system events.

**time-out**

The amount of time (in seconds) that the user's desktop can be inactive before reauthentication is required.

**token distributor**

A predefined administrative role that grants permission to act upon requests from users for tokens. Distributors record how they plan to deliver tokens to users and close requests.

**token provisioning**

The automation of all the steps required to provide enrollment, user group membership, RSA SecurID tokens, and the on-demand tokencode service to users. See also self-service.

**top-level security domain**

The top-level security domain is the first security domain in the security domain hierarchy. The top-level security domain is unique in that it links to the identity source or sources and manages the password, locking, and authentication policy for the entire deployment.

**Trace log**

A persistable store for trace information.

**trusted realm**

A trusted realm is a realm that has a trust relationship with another realm. Users on a trusted realm have permission to authenticate to another realm and access the resources on that realm. Two or more realms can have a trust relationship. A trust relationship can be either one-way or two-way.

**trust package**

An XML file that contains configuration information about the deployment.

**UDP**

See User Datagram Protocol.

**User Datagram Protocol (UDP)**

A protocol that allows programs on networked computers to communicate with one another by sending short messages called datagrams.

**User ID**

A character string that the system uses to identify a user attempting to authenticate. Typically a User ID is the user's first initial followed by the last name. For example, Jane Doe's User ID might be *jdoe*.

**virtual host**

Physical computer on which a virtual machine is installed. A virtual host helps manage traffic between web-based applications, web-tier deployments, and the associated primary instance and replica instances.

**virtual hostname**

The publicly-accessible hostname. End users use this virtual hostname to authenticate through the web tier. The system also generates SSL information based on the virtual hostname. The virtual hostname must be same as the load balancer hostname.

**web tier**

A web tier is a platform for installing and deploying the Self-Service Console, Dynamic Seed Provisioning, and the risk-based authentication (RBA) service in the DMZ. The web tier prevents end users from accessing your private network by receiving and managing inbound internet traffic before it enters your private network.

**workflow**

The movement of information or tasks through a work or business process. A workflow can consist of one or two approval steps and a distribution step for different requests from users.

**workflow participant**

Either approvers or distributors. Approvers review, approve, or defer user requests. Distributors determine the distribution method for token requests and record the method for each request. See also workflow.

# Index

## M



## N



## O



## P



## Q



## R



## S

## T



## U



## V



## W



## X