SecurID® Authentication Manager 8.7

Planning Guide

SecurID

Contact Information

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

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

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 Link. 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 RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA 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." RSA 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.

June 2022

Contents

Preface

About This Guide

This guide describes how to plan for a deployment of RSA® Authentication Manager 8.7. It is intended for system architects, network planners, security officers, and other trusted personnel whose responsibilities include system, network, and corporate security.

For a complete list of documentation, see "SecurID Product Documentation" on RSA Link at https://community.rsa.com/docs/DOC-60094.

For a description of common RSA Authentication Manager terms, see the "RSA Authentication Manager Glossary" on RSA Link at https://community.rsa.com/docs/DOC-76682.

SecurID Support and Service

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

Support for RSA Authentication Manager

Before you call Customer Support for help with the RSA Authentication Manager appliance, have the following information available:

- Access to the RSA Authentication Manager appliance.
- Your license serial number. To find this 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 appliance software version. This information is located in the top, right corner of the Quick Setup, or you can log on to the Security Console and click **Software Version Information**.

Support for the Cloud Authentication Service and Identity Routers

If your company has deployed identity routers and uses the Cloud Authentication Service, SecurID provides you with a unique identifier called the Customer Support ID. This is required when you register with SecurID Customer Support. To see your Customer Support ID, sign in to the Cloud Administration Console and click **My Account > Company Settings**.

RSA Ready Partner Program

The RSA Ready Partner Program website at https://community.securid.com/t5/securid-integrations/tkb-p/securid-access-integrations provides information about third-party hardware and software products that have been certified to work with SecurID products. The website includes Implementation Guides with step-by-step instructions and other information on how SecurID products work with third-party products.

Chapter 1: Planning Your Deployment

How RSA Authentication Manager Protects Your Resources

RSA Authentication Manager is a multifactor authentication solution that verifies authentication requests and centrally administers authentication policies for enterprise networks. Use Authentication Manager to manage security tokens, users, multiple applications, agents, and resources across physical sites, and to help secure access to network, Cloud, and web-accessible applications, such as SSL-VPNs and web portals.

Passwords are a weak form of authentication because access is protected only by a single factor - a string of characters that a user must remember. If the password is discovered by the wrong person, the security of the entire system is compromised. Multifactor authentication provides stronger protection by requiring two or more unique factors to verify a user's identity, for example, a user must know a PIN and have a mobile phone or laptop.

RSA Authentication Manager provides stronger protection for your resources:

RSA SecurID Tokens below

On-Demand Authentication below

RSA RADIUS below

Scalable and Interoperable on the facing page

Integrating Authentication Manager and the Cloud Authentication Service on the facing page

RSA SecurID Authentication with RSA Authentication Manager on page 10

RSA SecurID Authentication Examples on page 10

RSA SecurID Tokens

RSA SecurID hardware and software tokens provide tokencodes that enable users to authenticate and access resources protected by Authentication Manager and the Cloud Authentication Service.

A tokencode is a pseudorandom number. Tokencodes are time-based, changing at regular intervals. To gain access to protected resources, a user enters a personal identification number (SecurID PIN) + the number displayed on the token (tokencode). The combination of the SecurID PIN and the tokencode is called a passcode.

The user is granted access only if Authentication Manager validates the passcode. Otherwise, the user is denied access. Authentication Manager also supports PINless SecurID authentication.

On-Demand Authentication

Authentication Manager supports on-demand authentication (ODA) that provides strong two-factor authentication without the need for a physical token or dedicated authentication device. When a user enters a valid PIN to log on to the RSA authentication agent on a protected resource, the system delivers a one-time tokencode by way of e-mail or Short Message Service (SMS). The user then provides the tokencode to securely access the protected resource.

RSA RADIUS

You can use RSA RADIUS with Authentication Manager to directly authenticate users attempting to access network resources through RADIUS-enabled devices. RADIUS is automatically installed and configured during the Authentication Manager installation.

Scalable and Interoperable

Authentication Manager deployments are scalable and can authenticate up to one million users. Authentication Manager is interoperable with a wide variety of applications. For a list of supported applications, go to https://community.securid.com/t5/securid-integrations/tkb-p/securid-access-integrations.

Integrating Authentication Manager and the Cloud Authentication Service

Integrating Authentication Manager with the Cloud Authentication Service offers opportunities to expand the resources you protect and the authentication methods you make available to users. Authentication Manager is available with the Cloud Plus license and included with the Cloud Premier license. To deploy the Cloud Authentication Service, contact your RSA Sales representative at 1 800 995-5095 and choose Option 1. See Select an Integration Path for RSA Authentication Manager and the Cloud Authentication Service.

Multifactor Authentication

After installing the RSA SecurID Authenticate app on a supported device, users can authenticate with mobile-optimized push notification (Approve), Device Biometrics, or Authenticate Tokencode.

You do not need to replace or update your existing agents or RSA Ready products that use the UDP or TCP protocol. If you have deployed REST protocol authentication agents, your users will be able to authenticate to the Cloud with any form of multifactor authentication that is supported by the Cloud Authentication Service, including biometric methods such as fingerprint verification, RSA SecurID Token, and context-based authentication using factors such as the user's location and network.

RSA Authentication Manager provides high availability by allowing Authenticate Tokencode authentication to continue when the connection between Authentication Manager and the Cloud Authentication Service is not available.

If you deploy RSA Authentication Manager 8.5 or later with REST protocol authentication agents, you can configure RSA Authentication Manager as a proxy server that sends authentication requests to the Cloud Authentication Service. This creates one secure connection to the Cloud Authentication Service that supports all authentication methods supported by REST protocol authentication agents, whether verified by Authentication Manager or the Cloud Authentication Service.

You can connect in two ways:

- If you are using identity routers on other platforms in your on-premises network or in the Amazon Web Services cloud, see Connect RSA Authentication Manager to the Cloud Authentication Service.
- To connect with an embedded identity router, see Quick Setup - Connect RSA Authentication Manager to the Cloud Authentication Service with an Embedded Identity Router.

RSA SecurID Tokens

Users with RSA SecurID tokens can access SaaS and on-premises web applications and RADIUS clients protected by the Cloud Authentication Service. For more information, see Enable RSA SecurID Token Users to Access Resources Protected by the Cloud Authentication Service on RSA Link.

When Authentication Manager is not deployed, the Cloud Authentication Service can support authentication with the SID700 hardware token. If you have a Cloud-only deployment and you want to enable hardware token, contact your RSA Sales representative or Channel Partner.

RADIUS for the Cloud Authentication Service

If you have an RSA Authentication Manager RADIUS deployment, expand the authentication methods available

to users by moving to RADIUS for the Cloud Authentication Service. This path involves configuring a RADIUS client in the Cloud Authentication Service to protect the resources that are currently protected by RADIUS in Authentication Manager. For instructions, see RADIUS for the Cloud Authentication Service Overview on RSA Link.

RSA SecurID Authentication with RSA Authentication Manager

RSA SecurID authentication with RSA Authentication Manager involves the interaction of three distinct components:

- RSA SecurID authenticators, which generate one-time authentication credentials for a user.
- RSA Authentication Agents, which are installed on user's computers or client devices and send authentication requests to the Authentication Manager.
- RSA Authentication Manager, deployed on-premises or in the cloud, which processes the authentication requests and allows or denies access based on the validity of the authentication credentials sent from the authentication agent.

To authenticate a user with SecurID, Authentication Manager needs, at a minimum, the following information:

Element	Information
User record	Contains a User ID and other personal information about the user (for example, first name, last name, group associations, if any). The user record can come from either an LDAP directory server or the Authentication Manager internal database.
Agent record	Identifies the name of the machine where the agent is installed. This record in the internal database identifies the agent to Authentication Manager so that Authentication Manager can respond to authentication requests.
Token record	Enables Authentication Manager to generate the same tokencode that appears on a user's RSA SecurID token.
SecurID PIN	Used with the tokencode to form the passcode.

RSA Authentication Manager software, authentication agents, and RSA SecurID tokens work together to authenticate user identity. RSA SecurID patented time synchronization ensures that the tokencode displayed by a user's token is the same code that the RSA Authentication Manager software has generated for that moment. Both the token and the Authentication Manager generate the tokencode based on the following:

- The token's unique identifier (also called a "seed").
- The current time according to the token's internal clock, and the time set for the Authentication Manager system.

To determine whether an authentication attempt is valid, the RSA Authentication Manager compares the tokencode it generates with the tokencode the user enters. If the tokencodes do not match or if the wrong PIN is entered, the user is denied access.

RSA SecurID Authentication Examples

Authentication Manager software is scalable and can authenticate large numbers of users. It is interoperable with network, remote access, wireless, VPN, Internet, and application products. The following table lists some key examples.

Product or Application	Description
VPN Access	RSA SecurID provides secure authentication when used in combination with a VPN.
Remote dial-in	RSA SecurID operates with remote dial-in servers, such as RADIUS.
Web access	RSA SecurID protects access to web pages.
Wireless Networking	Authentication Manager includes an 802.1- compliant RADIUS server.
Secure access to Microsoft Windows	Authentication Manager can be used to control access to Microsoft Windows environments both online and offline.
Network hardware devices	Authentication Manager can be used to control desktop access to devices enabled for SecurID, such as routers, firewalls, and switches.

Deployment Components

An Authentication Manager deployment can include the following:

Primary Instance. The installed deployment where authentication and all administrative actions are performed. A single instance of Authentication Manager can handle administration and user authentication. The primary instance can be deployed on either a hardware appliance or a virtual appliance.

Replica Instance. (Optional) 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. Provides redundancy of the primary instance. A replica instance can be deployed on a hardware appliance or a virtual appliance. Mixed hardware appliance and virtual appliance deployments are supported.

Note: RSA recommends a deployment containing both a primary instance and at least one replica instance. The RSA Authentication Manager 8.7 Base Edition includes permission to deploy a replica instance. The Enterprise Edition and the Premium Edition both include permission to deploy up to 15 replica instances.

Web Tier. (Optional). 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. For more information, see Web Tier on the next page

Load Balancer. (Optional). A deployment component used to distribute authentication requests and to facilitate failover between the primary and replica web tiers. For more information, see Load Balancer on page 13.

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. For more information, see Authentication Agent on page 13.

Primary Instance

The primary instance is the initial Authentication Manager system that you deploy. Once you deploy a primary instance, you can add replica instances. It is possible to promote a replica instance to replace the primary instance in maintenance or disaster recovery situations.

The primary instance is the only system in the deployment that allows you to perform all Authentication Manager administrative tasks. Some administrative tasks can be performed on a replica instance, for example, replica promotion and log file collection.

The main functions of the primary instance include the following:

- Authenticating users.
- Enabling administration of Authentication Manager data stored in the internal database. You can perform tasks such as importing and assigning SecurID tokens, enabling risk-based authentication (RBA), adding LDAP identity sources, configuring self-service, generating replica packages, and generating agent configuration files and node secrets.
- Replicating changes due to administration and authentication activities.
- Handling self-service requests.
- Maintaining the most up-to-date Authentication Manager database.

Replica Instance

A replica instance provides deployment-level redundancy of the primary instance. With a few exceptions, you can view, but not update, administrative data on a replica instance.

A replica instance provides the following benefits:

- Real-time mirror of all user and system data
- Failover authentication if the primary instance becomes unresponsive
- Improved performance by load balancing authentication requests to multiple instances
- Ability to deploy a replica instance at a remote location
- Ability to recover administrative capabilities through replica promotion if the primary instance becomes unresponsive
- Administrators can clear PINs and provide emergency access to users

Note: If the primary instance has an "Out-of-Sync" replication status, for any reason, resynchronizing the deployment removes any administrative changes that occurred on a replica instance. For example, you may need to regenerate an offline emergency access tokencode that was generated on a replica instance.

Although a replica instance is optional, RSA recommends that you deploy both a primary and a replica instance. The RSA Authentication Manager 8.7 Base Edition includes permission to deploy a replica instance. The Enterprise Edition and the Premium Edition both include permission to deploy up to 15 replica instances.

Web Tier

A web tier is a platform installed in the DMZ that provides services to remote users without providing them with direct access to your private network. The web tier receives and manages inbound internet traffic before it enters your private network.

Authentication Manager includes risk-based authentication (RBA), dynamic seed provisioning, and the Self-Service Console, which may be needed by users outside of the corporate network. If the network includes a DMZ, you can use a web tier to deploy these services in the DMZ.

Note: On-demand authentication and SecurID do not require a web tier, even with a DMZ, when they are deployed as standalone authentication methods.

Deploying Authentication Manager applications and services in a web tier in the DMZ offers the following benefits:

- Protects your internal network from any unfiltered internet traffic from the Self-Service Console and RBA users. Web-tier servers receive and manage inbound internet traffic before it enters your private network.
- Allows you to customize the RBA logon pages and the Self-Service Console.
- Allows you to replace the default certificates with custom certificates that you request from a certificate authority.
- Improves system performance by removing some processing tasks from the back-end server.

A deployment can have up to 16 web tiers.

Load Balancer

If your deployment includes more than one web tier, you can add a third-party load balancer. The web-tier deployment can be used with a load balancer or you can use round robin DNS.

Adding a load balancer to your deployment provides the following benefits:

- The load balancer distributes authentication and RBA requests between the primary and the replica web tiers.
- The load balancer can be configured to forward Self-Service Console requests coming through the HTTPS port to the web tier or the primary instance hosting the Self-Service Console. If the primary instance is not functioning and a replica instance is promoted to take its place, users can continue to use the same URL for the Self-Service Console.
- The load balancer can verify the availability of each web tier.
- The load balancer provides failover if one of the Authentication Manager instances or web tiers experiences downtime.

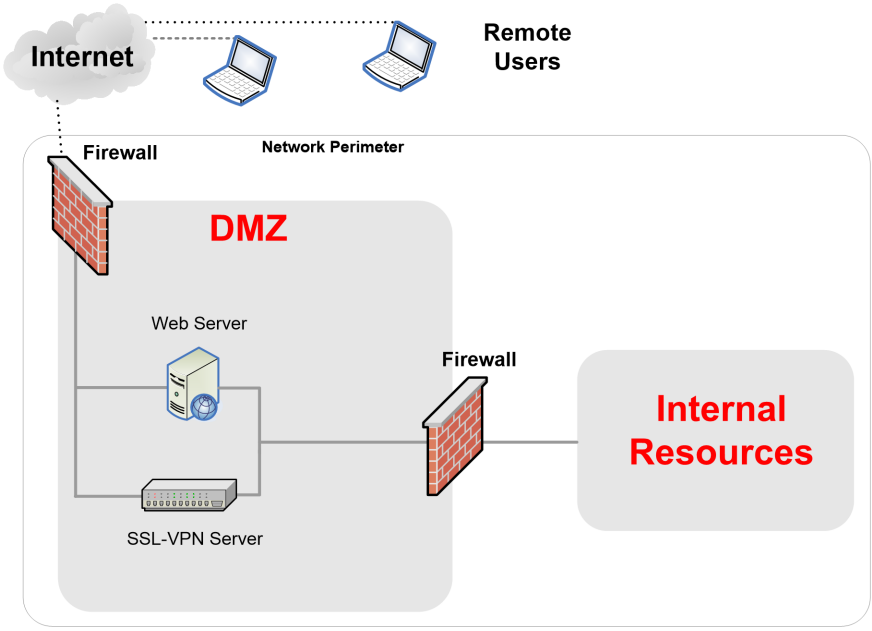
Authentication Agent

An authentication agent is software installed on the resource that you want to protect. The authentication agent communicates with Authentication Manager to process authentication requests. Authentication Manager works with many authentication agents.

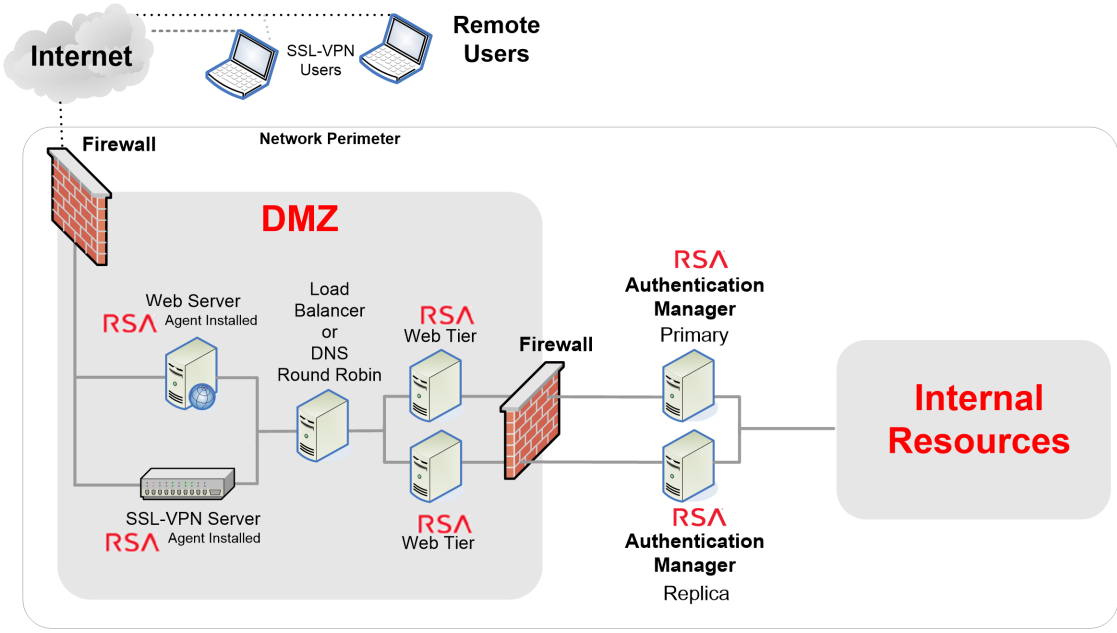
Different types of authentication agents protect different types of resources. For example, to protect an Apache Web server, you need RSA Authentication Agent for Web for Apache. RSA Authentication Agent software is also embedded in a number of products, such as web servers. Note that risk-based authentication works only with web-based agents. For more information about products with embedded RSA Authentication Agents, go to https://community.securid.com/t5/securid-integrations/tkb-p/securid-access-integrations.

Sample RSA Authentication Manager Deployment

The following figure shows a basic network configuration before Authentication Manager integration.



The following figure shows a basic network configuration after Authentication Manager integration.



Appliance Support

RSA Authentication Manager supports an Amazon Web Services (AWS) virtual appliance, an Azure virtual appliance, a VMware virtual appliance, a Hyper-V virtual appliance, and a hardware appliance. Each type of

appliance provides the same Authentication Manager features. You can use one type of appliance or both virtual and hardware appliances 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:

- AWS virtual appliance:
  - Deployed on AWS or AWS GovCloud (US) with an Amazon Machine Image (AMI) file that RSA provides.
  - Requires a Virtual Private Cloud (VPC) with a private subnet on AWS.
  - Supports a mixed deployment with cloud and on-premises appliances. For example, you can deploy your Authentication Manager primary instance on your local network and your replica instances in AWS.
- Azure virtual appliance
  - Deployed on the Azure Marketplace with an Azure Image file and an RSA Authentication Manager deployment JSON template that RSA provides.
  - Requires a Virtual Network with a private subnet on Azure.
  - Supports a mixed deployment with cloud and on-premises appliances. For example, you can deploy your Authentication Manager primary instance on your local network and your replica instances in Azure.
- VMware virtual appliance:
  - The VMware 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 VMware virtual appliance supports VMware features, such as VMware snapshots.
- Hyper-V virtual appliance:
  - The Hyper-V virtual appliance is deployed with the Hyper-V System Center Virtual Machine Manager (VMM) Console or the Hyper-V Manager on a host machine that you provide. You must use a host machine that meets the hardware requirements.
  - The Hyper-V virtual appliance supports Hyper-V features, such as Hyper-V checkpoints.
- Hardware appliance:
  - 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 use Clonezilla to create a backup image of the hardware appliance in case you need to restore the original settings for the hardware appliance. For instructions, "Using Clonezilla to Back Up and Restore the RSA Authentication Manager 8.4 or Later Hardware Appliance" on RSA Link at https://community.rsa.com/docs/DOC-97375.
  - If a backup image is not available, you can download and install the original hardware appliance system image from https://my.rsa.com.

  For a list of supported hardware appliance models, see the Product Version Lifecycle page on RSA Link.

Deployment Considerations

RSA Authentication Manager supports fault-tolerant deployments that include both a primary instance and a replica instance. Redundant deployments protect against unexpected failures, facilitate scheduled maintenance, and ensure availability of all authentication services. The RSA Authentication Manager 8.7 Base Edition, Enterprise Edition, and Premium Edition include permission to deploy a replica instance.

Do you require system-level redundancy?

- **Yes.** If you do require system-level redundancy, you must deploy both a primary instance and at least one replica instance.
- **No.** If you do not require system-level redundancy, you can deploy a single primary instance to meet your needs. Bear in mind that if the primary instance stops responding, authentication is not possible and protected resources are unreachable by your end users. For this reason, RSA strongly recommends the use of system-level redundancy for all business critical applications.

Deploying Web Tiers

Many corporate networks include a DMZ to filter unwanted or malicious Internet traffic from directly accessing protected resources on the internal network. RSA Authentication Manager supports such networks by allowing you to deploy the risk-based authentication (RBA) service, dynamic seed provisioning, and Self-Service Console on a separate web-tier server within the DMZ.

Do you plan to use RBA and dynamic seed provisioning? Do you plan to allow access to the Self-Service Console from outside your corporate network?

- **Yes.** In a DMZ environment, RBA, dynamic seed provisioning and the Self-Service Console must be deployed on a web tier to be accessible from outside the corporate network. You need to deploy one web tier for each instance (primary and replica). For more information, see Scenario 1: Primary Instance and Replica Instances with Web Tiers on page 18 or Scenario 3: Primary Instance with a Web Tier on page 21.
- **No.** If you plan to use on-demand authentication and SecurID as sole authentication methods and if you do not want the Self-Service Console accessible from outside the corporate network, you do not need to deploy web-tier servers. For more information, see or Scenario 4: Primary Instance Only on page 22.

Does your corporate network include a DMZ?

- **Yes.** If your network does include a DMZ, you may need to deploy one or more web tiers for each instance (primary and replica) depending on the services that you plan to offer.
- **No.** If your network does not include a DMZ, you do not need to deploy web-tier servers. Bear in mind that this may limit the services that you can offer and that it may also require you to open one or more ports in your corporate firewall. For more information, see or Scenario 4: Primary Instance Only on page 22.

Choosing a Load Balancing Strategy

In deployments consisting of a primary instance, replica instance, and web tiers, additional steps are required to distribute risk-based authentication (RBA) requests between the primary instance and the replica instance, and to ensure continuity of service in the event that either of the two servers stops responding.

DNS round robin is the easiest way to evenly distribute load between the two servers, but this strategy does not automatically handle situations where one of the two servers stops responding. If you require automatic failover for RBA, RSA recommends the use of a hardware or software load balancer.

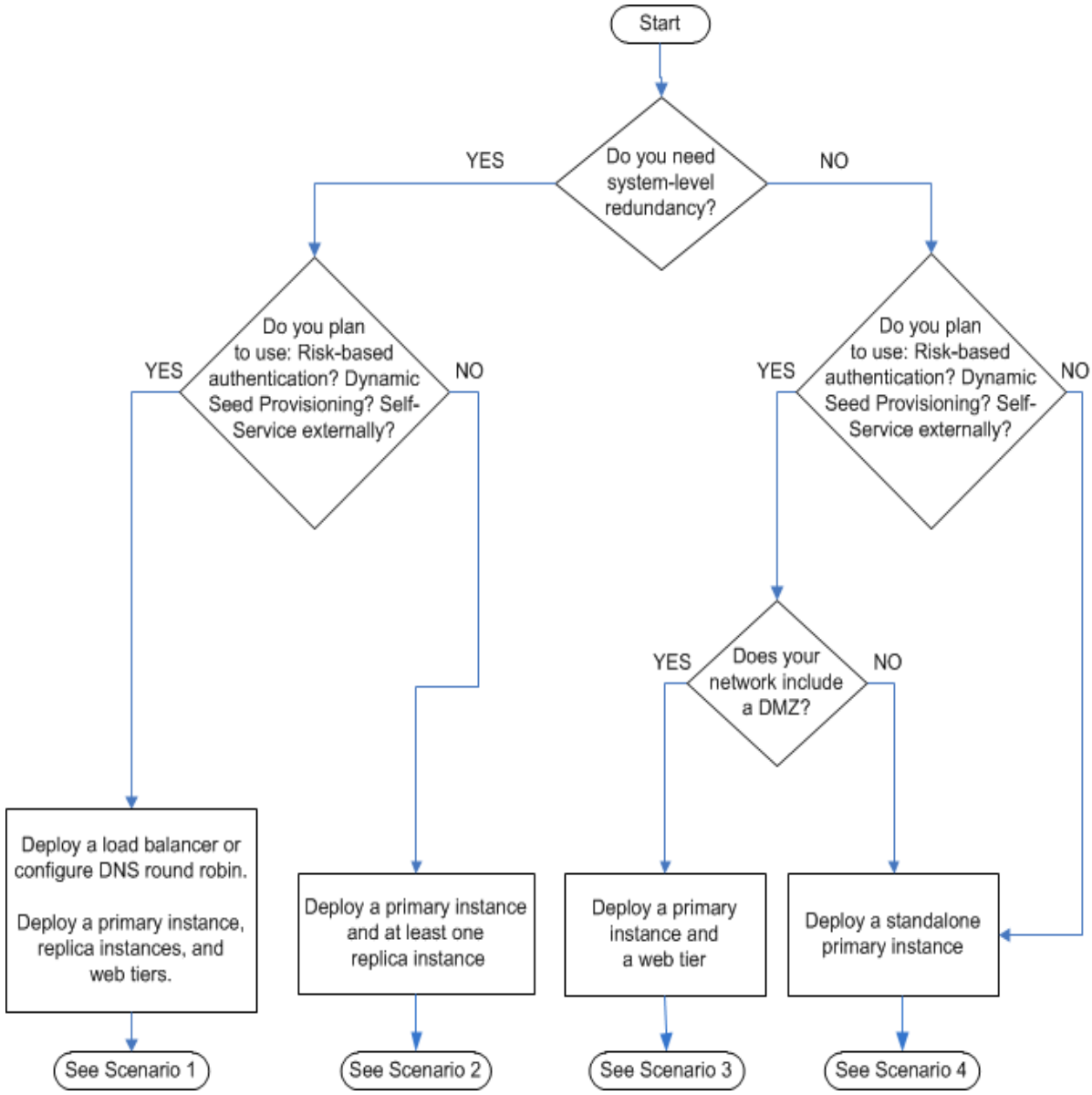
Selecting a Deployment Type

Authentication Manager supports hundreds of deployment options depending on your network topology and business requirements.

Before you deploy Authentication Manager, review the existing network. This review helps you determine which way to integrate Authentication Manager into your network.

Information to Review	Description
Diagrams of the network topology	Depict the physical location of all servers, other hardware, internal resources, firewalls, portals, and users' machines
Authentication process flow charts	Depict the existing authentication process

After gathering and reviewing information on your network topology, use the following decision tree to determine which Authentication Manager network configuration works best for your company.



Scenario 1: Primary Instance and Replica Instances with Web Tiers

A deployment consisting of a primary instance and replica instances with web tiers can include the following features:

- Authentication methods: on-demand authentication (ODA), risk-based authentication (RBA), and SecurID
- Failover in a disaster recovery situation
- Geographically dispersed deployments are possible

- Self-correcting web tier, if a primary or replica instance hostname changes, and redundancy on the web tier
- RBA logon screen customization
- Self-Service Console customization
- SSL certificate replacement for web tier servers

When you choose Scenario 1, consider these factors:

- RBA relies upon an external load balance or DNS round robin to distribute authentication requests between web tiers.
- In this configuration, both the individual web-tier hostnames and the shared virtual hostname must be addressable from the Internet.

Implementing Scenario 1

Perform the following tasks to implement the deployment of a primary instance and one or more replica instances with web tiers.

Procedure

1. Plan your deployment and complete the pre-installation checklists. For instructions, see the chapter "Preparing for Deployment" in the *Setup and Configuration Guide*.
2. Set up the primary appliance. For instructions, see the chapter "Deploying a Primary Appliance" in the *Setup and Configuration Guide*.
3. Set up the replica appliance. For instructions, see the chapter "Deploying a Replica Appliance" in the *Setup and Configuration Guide*.
4. Add a load balancer or configure DNS round robin. For instructions, see the chapter "Configuring a Virtual Host and Load Balancer" in the *Setup and Configuration Guide*.
5. Add web tiers. For instructions, see the chapter "Installing Web Tiers" in the *Setup and Configuration Guide*.
6. Secure your deployment, configure ports, add users, and configure authentication methods and Self-Service. For instructions, see the chapter "Next Steps for Your Deployment" in the *Setup and Configuration Guide*.

Scenario 2: Primary Instance with Replica Instances

In this example, a deployment consisting of a primary instance with replica instances can include the following features:

- Authentication methods: on-demand authentication (ODA) and SecurID
- Risk-based authentication (RBA) (with restrictions)
- Failover in a disaster recovery situation
- Geographically dispersed deployments are possible.

When you choose scenario 2, consider these factors:

- RSA recommends deploying a web tier to manage RBA logon attempts. Without a web tier, RBA can only exchange data with the primary instance. Because the replica instances are not available for RBA, system-level redundancy for RBA is not provided.
- On the primary instance, the Self-Service Console, the Security Console, and RBA all share port 7004. Consequently, using RBA, the Self-Service Console, and dynamic seed provisioning in this configuration makes the Security Console accessible from the Internet as well.

  RSA recommends limiting access to the Self-Service Console only to users inside your network, and not allowing users to clear their PIN with the Self-Service Console. Users that must clear their PIN should contact the Help Desk.

  Because RBA uses port 7004 rather than the standard SSL port (443), end users behind a client-side firewall, for example authenticating from a hotel, may not be able to access this service.

  If you intend to use RBA or the Self-Service Console, or if support for more restrictive client-side firewalls is required, RSA strongly recommends deploying a web-tier server. For more information on port considerations, see Port Traffic on page 24.
- Because the primary instance contains an SSL certificate signed by the Authentication Manager internal root certificate authority (CA), users may receive a certificate security warning when using RBA or when accessing the Self-Service Console. If you do not want users to see these warnings, you can use the Operations Console to replace the existing certificates with new certificates issued by a third-party certificate authority. For more information, see "Certificate Management for SSL" in the Authentication Manager Help.
- You must have Operations Console administrator credentials to attach a replica instance to the primary instance. Because the Operations Console administrator is able to perform many critical functions, you should provide these credentials to only the most trusted individuals. You can avoid providing these credentials when you set up a remote replica instance by having an administrator at the remote location deploy but not attach the replica instance. After the remote administrator deploys the replica instance, you can access the remote replica instance and perform the attach procedure.
- Deploying a replica instance requires a replica package file, which you create on the primary instance. If you choose to send a replica package to a trusted administrator, it is important to preserve the integrity of this file. When you send a replica package file, always use a secure and verifiable means of transit, such as a signed e-mail.

Implementing Scenario 2

Perform the following tasks to implement the deployment of a primary instance with one or more replica instances.

Procedure

1. Plan your deployment and complete the pre-installation checklists. For instructions, see the chapter "Preparing for Deployment" in the *Setup and Configuration Guide*.
2. Set up the primary appliance. For instructions, see the chapter "Deploying a Primary Appliance" in the *Setup and Configuration Guide*.
3. Set up the replica appliance. For instructions, see the chapter "Deploying a Replica Appliance" in the *Setup and Configuration Guide*.
4. Secure your deployment, configure ports, add users, and configure authentication methods and Self-Service. For instructions, see the chapter "Next Steps for Your Deployment" in the *Setup and Configuration Guide*.

Scenario 3: Primary Instance with a Web Tier

In this example, a deployment consisting of a primary instance with a web tier can include the following features:

- Authentication methods: on-demand authentication (ODA), risk-based authentication (RBA), and SecurID
- RBA logon screen customization
- Self-Service Console customization
- SSL certificate replacement for web-tier servers

When you choose scenario 3, consider these factors:

- There is no failover if the primary instance stops responding. If the primary instance stops responding, authentication is not possible and end users cannot reach protected resources.

  For this reason, RSA strongly recommends deploying both a primary instance and a replica instance for all business critical applications. The RSA Authentication Manager Base Server license includes permission to deploy a replica instance.
- There is no load balancing.

Implementing Scenario 3

Perform the following tasks to implement the deployment of a primary instance with a web tier.

Procedure

1. Plan your deployment and complete the pre-installation checklists. For instructions, see the chapter "Preparing for Deployment" in the *Setup and Configuration Guide*.
2. Set up the primary appliance. For instructions, see the chapter "Deploying a Primary Appliance" in the *Setup and Configuration Guide*.
3. Add the web tier. For instructions, see the chapter "Installing Web Tiers" in the *Setup and Configuration Guide*.
4. Secure your deployment, configure ports, add users, and configure authentication methods and Self-Service. For instructions, see the chapter "Next Steps for Your Deployment" in the *Setup and Configuration Guide*.

Scenario 4: Primary Instance Only

In this example, a standalone primary instance deployment can support the following authentication methods:

- On-demand authentication (ODA) (full support)
- Risk-based authentication (RBA) (with restrictions)
- SecurID (full support)

When you choose scenario 4, consider these factors:

- On the primary instance, the Self-Service Console, the Security Console, and RBA all share port 7004. Consequently, using RBA, the Self-Service Console, and dynamic seed provisioning in this configuration makes the Security Console accessible from the Internet as well.

  RSA recommends limiting access to the Self-Service Console only to users inside your network, and not allowing users to clear their PIN with the Self-Service Console. Users that must clear their PIN should contact the Help Desk.

  Because RBA uses port 7004 rather than the standard SSL port (443), end users behind a client-side firewall, for example authenticating from a hotel, may not be able to access this service.

  If you intend to use RBA or the Self-Service Console, or if support for more restrictive client-side firewalls is required, RSA strongly recommends deploying a web-tier server. For more information on port considerations, see Port Traffic on page 24.

- Because the primary instance contains an SSL certificate signed by the Authentication Manager internal root certificate authority (CA), users may receive a certificate security warning when using RBA or when accessing the Self-Service Console. If you do not want users to see these warnings, you can use the Operations Console to replace the existing certificates with new certificates issued by a third-party CA. For more information, see the Help topic "Certificate Management for Secure Sockets Layer."

Note: RSA recommends a deployment containing both a primary instance a replica instance. The RSA Authentication Manager Base Server license includes permission to deploy a replica instance.

Implementing Scenario 4

Perform the following tasks to implement the deployment of a standalone primary instance.

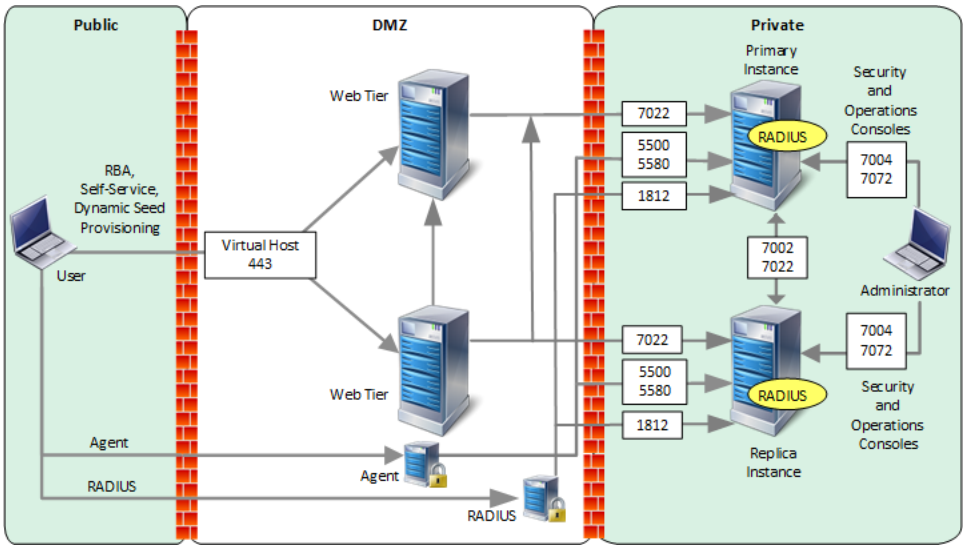
Procedure

1. Plan your deployment and complete the pre-installation checklist. For instructions, see the chapter "Preparing for Deployment" in the *Setup and Configuration Guide*.
2. Set up the primary appliance. For instructions, see the chapter "Deploying a Primary Appliance" in the *Setup and Configuration Guide*.
3. Secure your deployment, configure ports, add users, and configure authentication methods and self-service. For instructions, see the chapter "Next Steps for Your Deployment" in the *Setup and Configuration Guide*.

Chapter 2: Planning RSA Authentication Manager Network Integration

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 below.



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. Note the following:

- These ports are configured to be able to accept network traffic from remote systems. You should configure these ports for access on your local network.
- Authentication Manager uses other, internal network connections for communication between processes. Remote access to these ports is blocked by the internal firewall configured on the appliance.
- When blocking external access to ports on web-tier servers, do not block connections and traffic from services on the same system. For example, you can use a firewall to block external access to ports 7030, TCP, and 7036, TCP, but you must allow connections on the external NIC if the connections are from the same web-tier server.
- All ports support IPv4 only, unless IPv6 support is specified in the description.

Port Number and Protocol	Function	Source	Description
22, TCP	Secure Shell (SSH)	SSH client	Disabled by default. SSH can be enabled in the Operations Console. SSH allows the operating system account (rsaadmin) to access the operating system.
49, TCP	TACACS authentication	TACACS client	This port is closed unless TACACS is configured. Used to receive authentication requests from a Network Access Device (NAD).
80, TCP	Quick Setup 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). This port is closed, unless SNMP is enabled. It can be configured in the Security Console.
443, TCP	Quick Setup 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. For more information, see Required RSA RADIUS Server Listening Ports on page 28.
1812, UDP	RADIUS authentication	RADIUS client	This port receives authentication requests from a RADIUS client. 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.
5500, UDP	Agent authentication	RSA SecurID Authentication protocol agents	Accepts requests from UDP-based

Port Number and Protocol	Function	Source	Description
			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.
5555, TCP	Agent authentication	RSA SecurID Authentication API agents	Accepts requests from REST-based authentication agents and sends replies. Required for RSA SecurID and on-demand authentication (ODA). This port supports both IPv4- and IPv6-compliant agents.
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. 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). Used by the RSA application programming interface (API). 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.
7004, TCP	Self-Service Console and RBA	User’s browser	Required for using the Self-Service

Port Number and Protocol	Function	Source	Description
SSL-encrypted			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	Authentication Manager, trusted realm network access point, RBA, or the web tier	Another appliance, trusted realm, or the web tier and another appliance	Used for communication between Authentication Manager primary and replica instances and for communication between replica instances (for replay detection). Used to communicate with trusted realms and for RBA. 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.
8443, TCP SSL-encrypted	Authentication Manager patches and service packs	Administrator's browser	Access to this port is required for real-time status messages when applying Authentication Manager patches and service packs. During a product update, the appliance opens this port in its internal firewall. The appliance closes this port when the update is complete. If an external firewall blocks this port, the browser displays an inaccessible or blank web page, but the update can successfully complete.
9786, TCP SSL-encrypted	Embedded identity router	Authentication Manager	Used for communication between Authentication Manager and the embedded identity router for multifactor authentication (MFA) token verification over the Authentication Manager-identity router channel.

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, 1812, and 7082) on the Authentication Manager server are open by default.

Note: You must protect these ports by blocking the ones that are not used and restricting access to the ones that must be used only by Authentication Manager.

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

If you do not plan to use RADIUS, you can close the RADIUS authentication UDP ports 1645 and 1812.

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.
443, TCP	RBA	User's browser	Web-tier virtual hostname	Accepts requests for RBA authentication.

Note: 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 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 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 24.

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.

User Data Storage

You can store user data in:

- The internal databases
- An external directory server (called an identity source within Authentication Manager)

After integration with an external directory server is completed, administrators can use the RSA Security Console to do the following:

- View (but not add or modify) user and user group data that resides in the external directory server.
- Enable or disable Authentication Manager functions, such as SecurID authentication, on-demand authentication and risk-based authentication, for individual users who reside in the external directory server.
- Manage RSA-specific data, such as policy data, that is stored in the internal database.

Note: You must use the native user interface on the external directory server to modify user and group data. You cannot use the RSA Security Console to modify this data.

When choosing whether to use the internal database or an external directory server, consider your current network configuration and needs. Authentication Manager includes an internal database. The internal database contains all application and policy data. You can also store user and user group data in the internal database.

Using an External Directory Server

Authentication Manager supports the use of external directory servers for user and user group data. When you create an identity source, you provide Authentication Manager with the location of your user and user group data.

Know the following about integrating an external directory server:

- User data specific to Authentication Manager, for example registered devices, is stored in the internal database.
- Authentication Manager directory server integration does not modify your existing directory schema, but rather creates a map to your data that Authentication Manager uses.
- Authentication Manager has read-only access to external directory servers, with one exception: users may be permitted to change their own passwords during authentication.
- If users are permitted to change their own passwords, LDAP over SSL is required for external directory server connections to avoid exposing sensitive data passing over the connection. The use of LDAP over SSL requires that the appropriate certificate is accessible by Authentication Manager.
- For Active Directory, Authentication Manager supports Global Catalog identity sources and up to 30 non-Global Catalog identity sources per deployment. A Global Catalog identity source is used to look up users

and resolve group membership during authentications. You cannot use a Global Catalog identity source to perform administrative tasks.

Planning Physical Security

When you deploy Authentication Manager, you must have a plan to protect the physical assets in your deployment from unauthorized users and potential damage from the elements.

- **Equipment**. To ensure the physical security of the equipment running Authentication Manager, SecurID recommends that you locate the equipment in a locked location accessible to a minimum number of trusted personnel.
- **Connections and Ports**. Minimize the number and types of connections that can be made to the appliance. Block access through ports that are not necessary to system functionality.
- **Passwords and Key Material**. The Authentication Manager Quick Setup generates keys and passwords used to access internal services such as the internal database. These credentials are stored in a secure vault in Authentication Manager, protected both by a system-specific key for unattended startup as well as the Operations Console administrator credentials for interactive operations. The Operations Console administrator credentials are created during Quick Setup.

  You must secure the Operations Console administrator credentials, as they protect all of the system passwords required to run Authentication Manager.

  When you plan a failover and disaster recovery strategy, you can export the system keys and passwords to an encrypted, password-protected file as part of a backup of all of the system passwords. When recovering from a disaster, you can import the file back into the deployment. RSA strongly recommends storing the exported file in a safe and secure manner.
- **Hardware appliance or the physical machine hosting the virtual appliance.** Protect the hardware appliance. If you deploy a virtual appliance, protect the host where virtual disks, virtual memory, and any VMware snapshots or Hyper-V checkpoints are stored.

IPv4 and IPv6 Network Setting Requirements

IPv4 network settings are required to deploy RSA Authentication Manager. The IPv4 address that you specify for the appliance is used to access Quick Setup. IPv6-only deployments are not supported.

If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete. For each Authentication Manager instance, you can define IPv6 addresses to support authentication agents that use the REST protocol or the TCP protocol and IPv6 RADIUS clients.

IPv6 network settings are not supported for the following:

- **Web tier.** A web tier is a platform installed in the DMZ that provides services to remote users without providing them with direct access to your private network.
- **Replication.** At regular intervals, the primary instance sends administration and authentication data to each replica instance, and each replica instance sends authentication data to the primary instance.

- **Trusted or cross-realm authentication.** Two Authentication Manager deployments, each with a primary instance and, optionally, one or more replica instances, can trust one another and allow users to authenticate and access resources in the trusted deployment.
- **Azure deployments.** Microsoft Azure requires primary or replica instances deployed in the Azure cloud to only use static IPv4 addresses.
- **VMware Legacy Fault Tolerance feature.** If you use Legacy Fault Tolerance for your VMware virtual appliances, do not create an IPv6 network address on an Authentication Manager primary or replica instance.

Planning for Domain Name System Updates

To allow users to locate your web tier and optional load balancer, you must buy publicly resolvable names for these systems. Do the following:

- Define a domain name, for example, *mydomain.com*
- Define host names, for example, *myhost.mydomain.com*
- Contact a Domain Name registrar, and register the domain name and associated host names.

Clients using Self-Service and risk-based authentication (RBA) must be able to resolve to the virtual host name using Domain Name System (DNS).

- 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 addresses of each web tier.

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 below
- Appliance Operating System Account on the facing page

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. An Operations Console administrator can recover a Super Admin account if no Super

Name	Permissions	Management
		Admin can access the system.
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. **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. 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.

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.

RSA recommends the following best practices for administrative accounts:

- Create a separate administrative account for each administrator, for example, create a separate Operations Console administrator account for each Operations Console user. Do not share account information, especially passwords, among multiple administrators.
- RSA does not recommend associating administrative roles with external LDAP or Active Directory user accounts. Use separate administrative accounts with their own credentials for external identity source administrators and Authentication Manager administrators.
- If you have multiple administrators, restrict the scope and permissions of Authentication Manager administrative accounts, and restrict access by dividing your deployment into security domains. Separation of privileges is especially important if you are using LDAP or Active Directory users as administrators.
- If administrative roles in Authentication Manager are associated with an external LDAP account, a specific role. with appropriate limiting controls, should be used. For instructions, see the Help topic Administrative Role Scope and Permissions on RSA Link.

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. Before you can access the appliance operating system through SSH, you must use the Operations Console to enable SSH on the appliance.

On a virtual appliance, you can use the VMware vSphere Client, the Hyper-V System Center Virtual Machine Manager Console, or the Hyper-V Manager.

An Operations Console administrator can change the rsaadmin password. RSA does not provide a utility to recover the operating system password.

RSA RADIUS Overview

You can use RSA RADIUS with RSA Authentication Manager to directly authenticate users attempting to access network resources through RADIUS-enabled devices. A RADIUS server receives remote user access requests from RADIUS clients, for example, a VPN. The RADIUS server forwards the access requests to RSA Authentication Manager for validation. Authentication Manager sends accept or reject messages to the RADIUS server, which forwards the messages to the requesting RADIUS clients.

RADIUS is automatically installed and configured during the Authentication Manager installation. After installation, RADIUS is configured to run on the same instance with Authentication Manager.

You use the Operations Console to configure RSA RADIUS and manage settings that must be made on individual instances running RSA RADIUS.

You can use the Security Console to complete most tasks associated with managing RADIUS day-to-day operations.

Through the Security Console, you can manage the following objects:

- **RADIUS servers.** Server that receives users' access requests from RADIUS clients and forwards them to Authentication Manager for validation. A RADIUS server also forwards accept or reject messages from Authentication Manager to the requesting clients.
- **RADIUS clients.** RADIUS-enabled device at the network perimeter that enforces access control for users attempting to access network resources.
- **RADIUS profiles.** Named collection of checklist and return list attributes that specify session requirements for a user requesting remote network access.
- **RADIUS user attributes.** RADIUS attributes that you assign to a user or trusted user outside of a profile.

Trusted Realms

A deployment is an RSA Authentication Manager installation that consists of a primary instance and, optionally, one or more replica instances.

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.

For example, a corporation with headquarters in London has an office in New York. The London office and the New York office each has a deployment of Authentication Manager. The objects managed in each deployment constitute a realm: the London realm and the New York realm.

Two or more realms can have a trust relationship, which gives users on one realm permission to authenticate to another realm and access the resources on that realm.

For example, the London realm has a trust relationship with the New York realm. This means that the New York realm "trusts" users from the London realm and gives users from the London realm the same privileges as users in the New York realm. When users from the London office are in New York, they are able to able to authenticate at the New York office like all of the other New York users.

Note: You can create an SecurID trusted realm to allow users who are not in an Authentication Manager identity source or the internal database to use SecurID Authenticate Tokencodes on RSA authentication agents. For more information, see the Help topic "SecurID Authenticate Tokencodes."

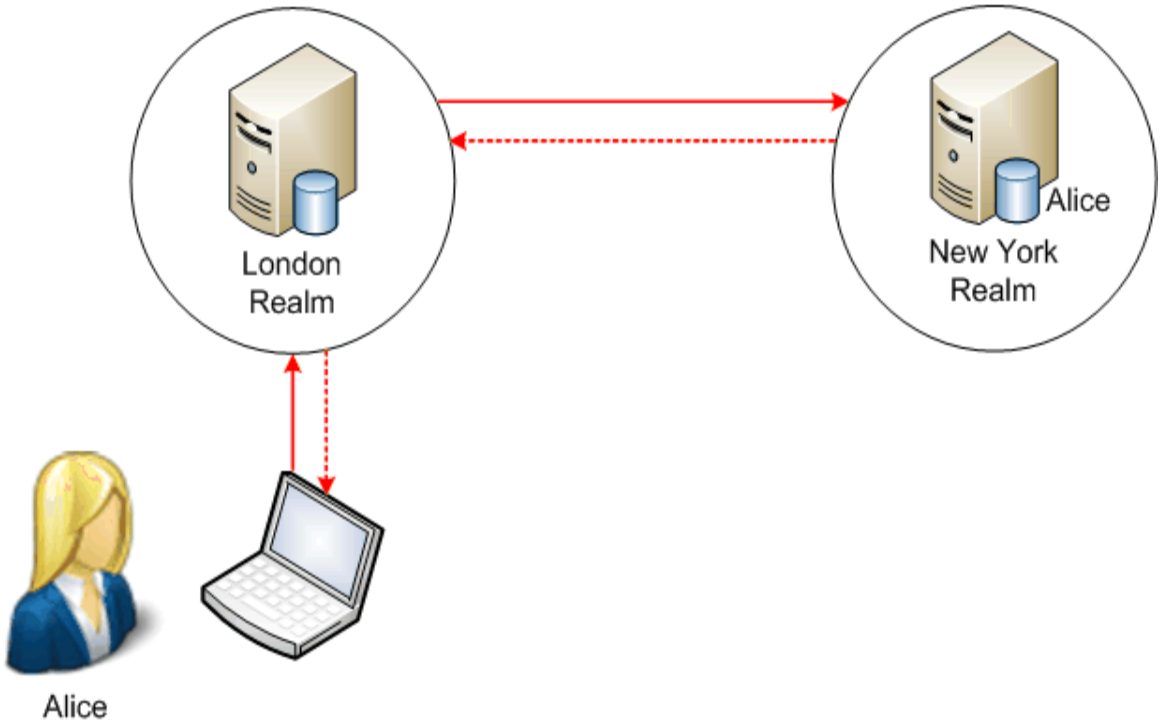
You create a trust relationship by performing the following tasks:

- Add an external realm as a trusted realm.
- Specify an agent to authenticate trusted users from the trusted realm.
- Specify the trusted users. You may not want to give all users from the trusted realm permission to authenticate on your realm, so you designate which users from the trusted realm are trusted users. Only trusted users have permission to authenticate.

A trust relationship can be either a one-way trust or a two-way trust. In a one-way trust, only trusted users on one realm are allowed to authenticate on the other realm.

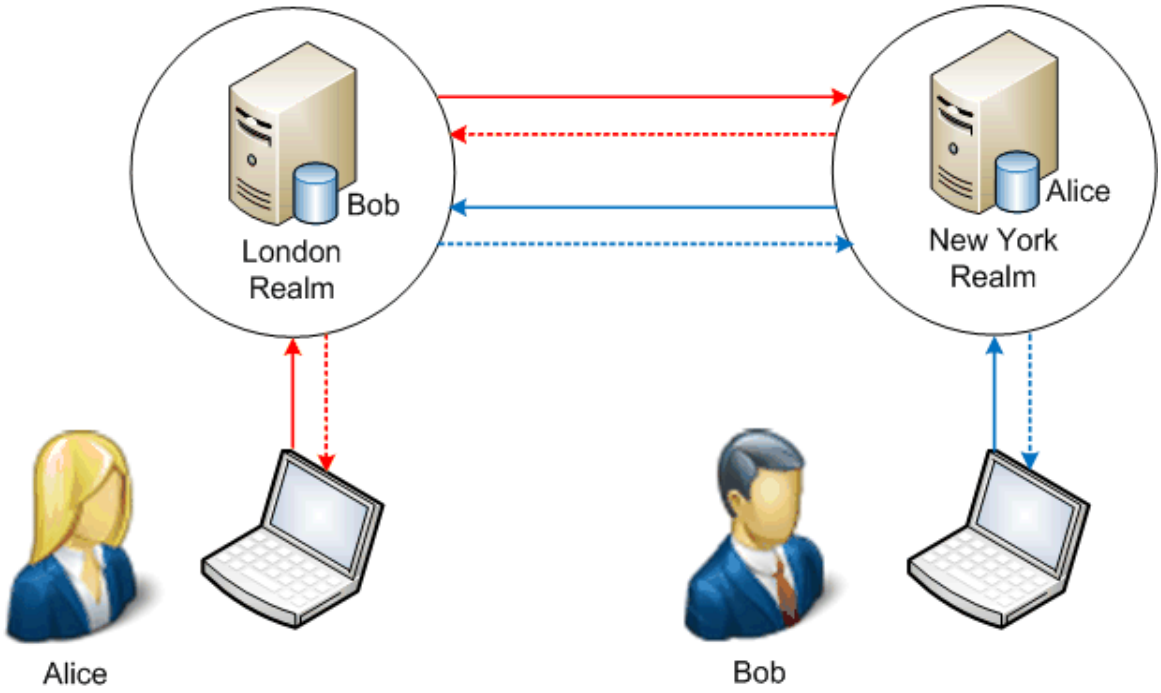
For example, if the trust relationship between London and New York is one way, either trusted London users can authenticate on New York or trusted New York users can authenticate on London. In a two-way trust, trusted users on each realm can authenticate on the other. For example, if the trust relationship between London and New York is two way, London users can authenticate on New York and New York users can authenticate on London.

The following figure shows a one-way trust. London has added New York as a trusted realm. This allows Alice, who is a trusted user in the New York realm, to authenticate to the London realm when she is in London on business.



While in London, Alice attempts to access London's virtual private network (VPN) using her New York realm credentials (user name and passcode). London's VPN server is protected by an agent that is configured to provide trusted realm authentications. This agent does not recognize Alice and looks for Alice in other realms. After the agent finds Alice in the New York realm, the New York realm verifies Alice's credentials, authenticates Alice, and tells the agent to grant Alice access.

The following figure shows a two-way trust. London has added New York as a trusted realm, and New York has added London as a trusted realm. This allows Alice, who is a trusted user in the New York realm, to authenticate to the London realm, and Bob, who is a trusted user in the London realm, to authenticate to the New York realm.



For more than two realms to trust each other, additional trust relationships must be established. Trusted realms cannot inherit or transfer trust from other realms. Trusted realm authentication only occurs between realms that have a direct, explicit trust relationship. In the previous example, even if the London realm were to add Paris as a trusted realm, New York and Paris would not trust each other unless you created a trust relationship between New York and Paris.

Chapter 3: Planning Guide Checklist

About This Checklist

Use the following checklist to specify planning and installation information. RSA recommends that you complete this checklist and distribute it to the appropriate personnel for your deployment. Save a copy of the completed checklist in a secure location for future reference.

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

Planning Your Deployment

Element	Your Plan
Determine whether you require one or more replica instances.	
Decide which authentication methods you want to use.	
Determine whether you need to install a web tier and which features you want to make available in the web tier.	
Determine whether you need a load balancer or round robin Domain Name System.	
Determine whether you need a time server to synchronize instances.	

Planning Network Configuration

Element	Your Plan
Determine what ports need to be open for the primary and replica instances.	
Determine whether to use the default port for the load balancer.	
Determine whether to use the default port for the web tier.	
Determine what you need to know to configure your firewall. For example: • Instance IP address • Agent IP addresses • Load balancer hostname and IP address • Load balancer port • Web-tier server hostname and IP address • Web-tier port • Virtual hostname	
Decide whether to keep the default certificates or to replace them with custom certificates.	
Determine where you will store user data: • Internal database • External directory server	

Element	Your Plan
• Both	

Directory Server
• Confirm that you have a supported version of the directory server.
• Establish an administrator's account in the directory server.
• Confirm the URL of your directory server.
• (Optional) Obtain the URL of the failover directory server.
• Determine if users will be allowed to change passwords from Authentication Manager.
• Obtain publicly (Internet) addressable DNS names and addresses for web-tier servers, the load balancer, and the virtual hostname.
• If password changes are allowed:
  • Enable Certificate Authority (CA) Services on Active Directory.
  • Make sure either the domain root CA certificate or a certificate signed by the same root CA as the certificate on the directory server is exported and available.	

Pre-Installation

Element	Your Plan
Locate the license file.	
Plan for securing name and password information: • Super Admin User ID • Super Admin password • Operations Console administrator name and password • OS password and emcrsv • Web-tier password	
Determine the physical location of the web-tier servers.	
Determine if agents are needed.	
Determine if a load balancer is needed.	

Installation

Element	Your Plan
Install the primary instance.	
Install one or more replica instances.	
Install web tiers.	
Install agent, if needed.	
Install load balancer, if needed.	