RSA® Authentication Manager 8.1
Planning 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.
Contents

Revision History .......................................................................................................................... 5
Preface ....................................................................................................................................... 7
About This Guide ......................................................................................................................... 7
RSA Authentication Manager 8.1 Documentation .................................................................. 7
Related Documentation ............................................................................................................... 8
Support and Service ................................................................................................................ 8
Before You Call Customer Support ....................................................................................... 9

Chapter 1: Planning Your Deployment ................................................................. 11
How RSA Authentication Manager Protects Your Network .............................................. 11
Deployment Components ....................................................................................................... 12
Primary Instance .................................................................................................................... 12
Replica Instance .................................................................................................................... 13
Web Tier ................................................................................................................................. 13
Load Balancer ....................................................................................................................... 14
Authentication Agent ............................................................................................................. 14
Sample RSA Authentication Manager Deployment ......................................................... 15
Appliance Support .................................................................................................................. 16
Deployment Considerations .................................................................................................... 17
Deploying Web Tiers .............................................................................................................. 17
Choosing a Load Balancing Strategy ..................................................................................... 18
Selecting a Deployment Type ............................................................................................... 18
Deployment Scenarios ........................................................................................................... 20
Scenario 1: Primary Instance and Replica Instances with Web Tiers .................................... 20
Implementing Scenario 1 ....................................................................................................... 21
Scenario 2: Primary Instance with Replica Instances .......................................................... 21
Implementing Scenario 2 ....................................................................................................... 23
Scenario 3: Primary Instance with a Web Tier ...................................................................... 23
Implementing Scenario 3 ....................................................................................................... 24
Scenario 4: Primary Instance Only ....................................................................................... 24
Implementing Scenario 4 ....................................................................................................... 25

Chapter 2: Planning RSA Authentication Manager Network Integration ................... 27
Port Traffic ............................................................................................................................... 27
Ports for the RSA Authentication Manager Instance .......................................................... 28
Restricting Access to the RSA Consoles .............................................................................. 31
Required RSA RADIUS Server Listening Ports ................................................................. 31
Port Considerations for Trusted Legacy Realms ................................................................. 32
Ports on the Web Tier with a Load Balancer Deployed ....................................................... 33
Ports on the Web Tier Without a Load Balancer ................................................................. 33
## Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Date</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>December 2014</td>
<td>Updated for RSA Authentication Manager 8.1 Service Pack 1 (SP1). Added information for Hyper-V support.</td>
</tr>
</tbody>
</table>
Preface

About This Guide

This guide describes how to plan for a deployment of RSA® Authentication Manager. It is intended for system architects, network planners, security officers, and other trusted personnel whose responsibilities include system, network, and corporate security. Do not make this guide available to the general user population.

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.
- **SNMP Reference Guide.** Describes how to configure Simple Network Management Protocol (SNMP) to monitor an instance of Authentication Manager on a hardware appliance or 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 Authentication Manager APIs and the related Javadoc.
- **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

<table>
<thead>
<tr>
<th>Service</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA SecurCare Online</td>
<td><a href="https://knowledge.rsasecurity.com">https://knowledge.rsasecurity.com</a></td>
</tr>
<tr>
<td>Customer Support Information</td>
<td><a href="http://www.emc.com/support/rsa/index.htm">www.emc.com/support/rsa/index.htm</a></td>
</tr>
<tr>
<td>RSA Solution Gallery</td>
<td><a href="https://gallery.emc.com/community/marketplace/rsa?view=overview">https://gallery.emc.com/community/marketplace/rsa?view=overview</a></td>
</tr>
</tbody>
</table>

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.
Planning Your Deployment

How RSA Authentication Manager Protects Your Network

RSA Authentication Manager protects resources on your network by requiring users to authenticate using multifactor authentication methods.

Authentication Manager offers the following multifactor authentication methods:

**RSA SecurID tokens.** Hardware and software tokens provide tokencodes that enable users to authenticate and access resources protected by Authentication Manager.

A tokencode is a pseudorandom number, usually six digits in length. 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, in which case a SecurID PIN is not required.

**Risk-based authentication (RBA).** Strengthens RSA SecurID authentication and traditional password-based authentication by discreetly analyzing user behavior and the device from which a user authenticates to identify potentially risky or fraudulent authentication attempts. When RBA is used to protect a network resource, the system determines the assurance level of each authentication attempt based on the user’s profile, authentication device, and authentication history.

**On-demand authentication (ODA).** Delivers a one-time tokencode to a user by way of e-mail or Short Message Service (SMS). This tokencode, combined with a PIN known only by the user, enables strong two-factor authentication without the need for a physical token or dedicated authentication device. You can use ODA as a standalone authentication method or as an identity confirmation method for RBA.

Authentication Manager is scalable and can authenticate up to one million users. It is interoperable with a wide variety of applications. For a list of supported applications, go to [https://gallery.emc.com/community/community/marketplace/rsa?view=overview](https://gallery.emc.com/community/marketplace/rsa?view=overview).
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 a replica instance. The RSA Authentication Manager Base Server license and the Enterprise Server license both include permission to deploy a replica instance.

**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 page 13.

**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 14.

**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 14.

**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.
- Hosting the primary RSA RADIUS server.
- 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. 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

Although a replica instance is optional, RSA recommends that you deploy both a primary and a replica instance. The RSA Authentication Manager Base Server license and the Enterprise Server license both include permission to deploy a replica instance.

**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**

A load balancer distributes authentication requests and facilitates failover between web tiers. Adding a load balancer to your deployment provides the following benefits:

- The load balancer distributes 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.
- 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 5.3 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://gallery.emc.com/community/marketplace/rsa?view=overview](https://gallery.emc.com/community/marketplace/rsa?view=overview).
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 8.1 supports a hardware appliance, a VMware virtual appliance, and a Hyper-V virtual appliance. Each type of appliance provides the same Authentication Manager features. You can use one type of appliance or both hardware and virtual 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:

- **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 only perform a factory reset on the hardware appliance.
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 Base Server license and the Enterprise Server license both 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 20 or Scenario 3: Primary Instance with a Web Tier on page 23.

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 Scenario 2: Primary Instance with Replica Instances on page 21 or Scenario 4: Primary Instance Only on page 24.

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 Scenario 2: Primary Instance with Replica Instances on page 21 or Scenario 4: Primary Instance Only on page 24.
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.

<table>
<thead>
<tr>
<th>Information to Review</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagrams of the network topology</td>
<td>Depict the physical location of all servers, other hardware, internal resources, firewalls, portals, and users’ machines</td>
</tr>
<tr>
<td>Authentication process flow charts</td>
<td>Depict the existing authentication process</td>
</tr>
</tbody>
</table>
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.

Start

Do you need system-level redundancy?

YES

Do you plan to use: Risk-based authentication? Dynamic Seed Provisioning? Self-Service externally?

YES

Deploy a load balancer or configure DNS round robin.

See Scenario 1

NO

Deploy a primary instance, replica instances, and web tiers.

See Scenario 2

NO

YES

NO

Deploy a load balancer or configure DNS round robin.

See Scenario 1

NO

YES

Deploy a primary instance and at least one replica instance

See Scenario 2

NO

YES

Deploy a primary instance and a web tier

See Scenario 3

NO

YES

Deploy a standalone primary instance

See Scenario 4

NO

Does your network include a DMZ?

YES

NO
Deployment Scenarios

The following Authentication Manager scenarios are examples of common deployments.

These examples are based upon the RSA recommendation that you deploy risk-based authentication and the Self-Service Console on a web tier.

<table>
<thead>
<tr>
<th>Scenario 1: Primary Instance and Replica Instances with Web Tiers on page 20</th>
<th>Load Balancing and Failover</th>
<th>Risk-Based Authentication (RBA)</th>
<th>On-Demand Authentication</th>
<th>RSA SecurID Authentication</th>
<th>Self-Service Console Customization</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenario 2: Primary Instance with Replica Instances on page 21</th>
<th>X</th>
<th>Only supported on the primary instance.</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Scenario 3: Primary Instance with a Web Tier on page 23</th>
<th>X</th>
<th>X</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
</table>

| Scenario 4: Primary Instance Only on page 24 | X | X | X |
|---|---|---|

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. 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 27.

- 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 RSA Authentication Manager 8.1 Administrator’s Guide.

- 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.

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 27.
• 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 “Certificate Management for Secure Sockets Layer” in the Administrator’s Guide.

• A primary instance-only deployment provides no redundancy or load balancing.

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.
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 on page 28.
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.

<table>
<thead>
<tr>
<th>Port Number and Protocol</th>
<th>Function</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22, TCP</td>
<td>SSH</td>
<td>SSH client</td>
<td>Disabled by default. Allows the operating system account (rsaadmin) to access the operating system.</td>
</tr>
<tr>
<td>49, TCP</td>
<td>TACACS authentication</td>
<td>TACACS client</td>
<td>Used to receive authentication requests from Network Access Device (NAD).</td>
</tr>
<tr>
<td>80, TCP</td>
<td>Quick Setup Operations Console, Security Console</td>
<td>Administrator’s browser</td>
<td>Used for Quick Setup. After Quick Setup is complete, the appliance redirects connections from this port to the appropriate console.</td>
</tr>
<tr>
<td>161, UDP</td>
<td>SNMP</td>
<td>SNMP client</td>
<td>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.</td>
</tr>
<tr>
<td>443, TCP</td>
<td>Quick Setup Operations Console, Security Console, Self-Service Console</td>
<td>Administrator’s browser</td>
<td>Used for Quick Setup. After Quick Setup is complete, the appliance redirects connections from this port to the appropriate console.</td>
</tr>
<tr>
<td>1645, UDP</td>
<td>RADIUS authentication (legacy port)</td>
<td>RADIUS client</td>
<td>This port receives authentication requests from a RADIUS client.</td>
</tr>
<tr>
<td>Port Number and Protocol</td>
<td>Function</td>
<td>Source</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1646, UDP</td>
<td>RADIUS accounting (legacy port)</td>
<td>RADIUS client</td>
<td>This port receives inbound accounting requests from a RADIUS client.</td>
</tr>
<tr>
<td>1812, TCP</td>
<td>RADIUS replication port</td>
<td>Another RADIUS server</td>
<td>This port is used for communication between primary RADIUS and replica RADIUS services. 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 31.</td>
</tr>
<tr>
<td>1812, UDP</td>
<td>RADIUS authentication</td>
<td>RADIUS client</td>
<td>This port receives authentication requests from a RADIUS client. If you do not plan to use RSA RADIUS authentication, you can close this port.</td>
</tr>
<tr>
<td>1813, TCP</td>
<td>RADIUS administration</td>
<td>RADIUS server</td>
<td>This port is used to administer RADIUS from the Security Console over the protected RADIUS remote administration channel. 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 31.</td>
</tr>
<tr>
<td>1813, UDP</td>
<td>RADIUS accounting</td>
<td>RADIUS client</td>
<td>This port receives accounting requests from a RADIUS client. If you do not plan to use RSA RADIUS authentication, you can close this port.</td>
</tr>
<tr>
<td>5500, TCP</td>
<td>Agent authentication</td>
<td>RSA SecurID Authentication protocol agents</td>
<td>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.</td>
</tr>
<tr>
<td>Port Number and Protocol</td>
<td>Function</td>
<td>Source</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>5500, UDP</td>
<td>Agent authentication</td>
<td>RSA SecurID Authentication protocol agents</td>
<td>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.</td>
</tr>
<tr>
<td>5550, TCP</td>
<td>Agent auto-registration</td>
<td>RSA agents</td>
<td>Used for communication with authentication agents that are attempting to register with Authentication Manager.</td>
</tr>
<tr>
<td>5580, TCP</td>
<td>Offline authentication service</td>
<td>RSA agents</td>
<td>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.</td>
</tr>
<tr>
<td>7002, TCP SSL-encrypted</td>
<td>Authentication Manager</td>
<td>Another appliance</td>
<td>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.</td>
</tr>
<tr>
<td>7002, TCP SSL-encrypted</td>
<td>RSA Token Management snap-in for the Microsoft Management Console (MMC)</td>
<td>Microsoft Management Console</td>
<td>Enable this port if you plan to use the RSA Token Management snap-In to manage users and authenticators from MMC.</td>
</tr>
</tbody>
</table>
## 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.

### Required RSA RADIUS Server Listening Ports

<table>
<thead>
<tr>
<th>Port Number and Protocol</th>
<th>Function</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7004, TCP SSL-encrypted</td>
<td>Self-Service Console and RBA</td>
<td>User’s browser</td>
<td>Required for using the Self-Service Console or RBA. Accepts requests for Self-Service Console functions and RBA authentication.</td>
</tr>
<tr>
<td>7004, TCP SSL-encrypted</td>
<td>Cryptographic Token-Key Initialization Protocol (CT-KIP)</td>
<td>User’s browser</td>
<td>Required for using dynamic seed provisioning.</td>
</tr>
<tr>
<td>7004, TCP SSL-encrypted</td>
<td>Trusted realm network access point or the web tier.</td>
<td>Trusted realm, or the web tier and another appliance</td>
<td>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.</td>
</tr>
<tr>
<td>7072, TCP SSL-encrypted</td>
<td>Operations Console</td>
<td>Super Admin’s browser</td>
<td>Required for administering your deployment from the Operations Console. Accepts requests for Operations Console functions.</td>
</tr>
<tr>
<td>7082, TCP SSL-encrypted</td>
<td>RADIUS Configuration SSL</td>
<td>Authentication Manager instance</td>
<td>Used for configuring RADIUS and restarting the RADIUS service from the Operations Console.</td>
</tr>
</tbody>
</table>
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 28. 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.

<table>
<thead>
<tr>
<th>Port Number and Protocol</th>
<th>Function</th>
<th>Source</th>
<th>Destination Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443, TCP</td>
<td>Self-Service Console, risk-based authentication (RBA), and dynamic seed provisioning</td>
<td>User’s browser</td>
<td>Primary web-tier hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accepts requests for Self-Service Console functions, RBA authentication, and dynamic seed provisioning.</td>
</tr>
<tr>
<td>443, TCP</td>
<td>RBA</td>
<td>Load balancer</td>
<td>Web-tier virtual hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accepts requests for RBA authentication that use the virtual hostname.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Port Number and Protocol</th>
<th>Function</th>
<th>Source</th>
<th>Destination Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443, TCP</td>
<td>Self-Service Console, risk-based authentication (RBA), and dynamic seed provisioning</td>
<td>User’s browser</td>
<td>Primary web-tier hostname</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accepts requests for Self-Service Console functions, RBA authentication, and dynamic seed provisioning.</td>
</tr>
</tbody>
</table>
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 27.

**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.
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.

Supported External Directory Servers

Authentication Manager supports:

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

**Note:** Active Directory Application Mode (ADAM) is not supported.

For a complete list of the information you need before integrating an external directory server, see Chapter 3: Planning Guide Checklist on page 43.
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, RSA 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.

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**
- **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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Permissions</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>Super Admins can perform all administrative tasks in the Security Console with full administrative permission in all security domains in the deployment.</td>
<td>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 Admin can access the system.</td>
</tr>
<tr>
<td>Operations Console administrator</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.

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. 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.

- **RADIUS accounting.** Usage statistics of the RADIUS servers and clients for billing or auditing purposes.

- **RADIUS replication.** RSA RADIUS sends changes that occur as a result of RADIUS activity to the RADIUS replica servers automatically, but you can manually cause the system to replicate as well.

---

**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.

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 information about trusted realms, see the chapter “Administering Trusted Realms” in the *RSA Authentication Manager 8.1 Administrator’s Guide*. 
### 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

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

### Planning Network Configuration

<table>
<thead>
<tr>
<th>Element</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine what ports need to be open for the primary and replica instances.</td>
<td></td>
</tr>
<tr>
<td>Determine whether to use the default port for the load balancer.</td>
<td></td>
</tr>
<tr>
<td>Determine whether to use the default port for the web tier.</td>
<td></td>
</tr>
</tbody>
</table>
## Element

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
- 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

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

## Installation

<table>
<thead>
<tr>
<th>Element</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the primary instance.</td>
<td></td>
</tr>
<tr>
<td>Install one or more replica instances.</td>
<td></td>
</tr>
<tr>
<td>Install web tiers.</td>
<td></td>
</tr>
<tr>
<td>Install agent, if needed.</td>
<td></td>
</tr>
<tr>
<td>Install load balancer, if needed.</td>
<td></td>
</tr>
</tbody>
</table>
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 tokencode 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.

thrusted 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

## A
- Active Directory, 36
- administration
  - external directory server, 35
- administrators
  - system administrator accounts, 38
- aliases
  - number allowed, 34
- alternate IP address, 34
- authentication
  - identity confirmation, 11
  - on-demand, 11
  - risk-based, 11
  - user history, 11
- authentication agents
  - alternate IP addresses, 34
  - overview, 12
  - types, 14

## C
- certificates
  - replace default with custom, 14
  - SSL-LDAP, 36
- customizing
  - RBA log on pages, 14

## D
- demilitarized zone
  - deploying web tiers, 13
- deployment
  - options, 12
  - planning, 11
  - primary and replica, 21
  - primary only, 24
  - primary with web-tier, 23
  - primary, replica, and web tiers, 20
  - selecting a type, 18
  - supported scenarios, 20
  - using a subnet, 28
  - using firewalls, 34
  - web tier, 17
- directory server integration
  - schema, 36

## E
- external directory servers
  - enable or disable user functions, 35
  - supported types, 36

## F
- failover
  - using a load balancer, 14
- firewalls
  - aliases, 34
  - Network Address Translation, 34
  - usage in a web tier, 17

## G
- Global Catalog
  - number supported, 36

## I
- identity source
  - using LDAP, 36
- installation
  - firewall access, 34
  - integration
  - planning, 27
- IP addresses
  - aliases, 34

## K
- keystores, 37

## L
- LDAP Directory
  - integration guidelines, 36
- license
  - ID, 9
  - serial number, 9
- load balance
  - deployment strategy, 18
  - load balancer
    - overview, 12
    - uses, 14

## M
- master password
  - export for backup, 37
  - recovery, 37
  - securing, 37
- multifactor authentication
  - overview, 11
N
NAT. See Network Address Translation
Network Address Translation, 34
agent IP address alias, 34
network protection, 11

O
on-demand authentication
definition, 11
overview, 11
using an agent, 14
one-way trust, 41
operating system
account, 39
Operations Console
administrator permissions, 38
Oracle Directory Server, 36

P
passcode
overview, 11
passwords
lost, 38–39
policy data
in an external directory server, 35
in the internal database, 35
port translation, 34
port usage
in a web tier, 17
list of ports, 28
on a web tier, 33
security, 37
traffic flow diagram, 27
primary instance
overview, 12
secure connection to a replica instance, 35

R
RADIUS
accounting, 40
clients, 40
profiles, 40
servers, 40
user attributes, 40
registered device
where data is stored, 36
replica instances
definition, 13
number allowed, 17
overview, 12
secure connection to a primary instance, 35
reviewing your existing network, 18
risk-based authentication
assurance level, 11
overview, 11
using an agent, 14
Round Robin DNS
deployment strategy, 18
ports, 33
RSA Self-Service Console
using a load balancer, 14

S
scalability, 11
schema
directory server integration, 36
Secure Shell
for accessing the appliance, 39
port, 28
SecurID
overview, 11
security
of connections, 37
of equipment, 37
of key material and system passwords, 37
security. See keystores, 37
SSH. See Secure Shell.
subnet
deploying appliance, 28
Sun Java System Directory Server, 36
Super Admin
permissions, 38
system administrator accounts, 38

T
tokens
SecurID overview, 11
types, 11
trusted realms
authentication, 40
one-way trust, 41
two-way trust, 42
trusts. See trusted realms
two-way trust, 42
Index

U
user group data
  administration, 35
  in the internal database, 35
User IDs
  valid characters, 38

V
valid characters
  for User IDs, 38
version
  viewing, 9

Virtual Private Network
  trusted realm, 41

W
web tiers
  benefits overview, 14
  customizing RBA log on pages, 14
  deployment, 17
  load balancer ports, 33
  number supported, 14
  overview, 12
  Round Robin DNS ports, 33
  using a load balancer, 14