RSA® Authentication Manager 8.1 Administrator’s Guide

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

Preface

About This Guide

This guide describes how to administer RSA® Authentication Manager 8.1. It is intended for administrators and other trusted personnel.

RSA® Authentication Manager 8.1 Documentation

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Documentation

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

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

Support and Service

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

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

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

Before You Call Customer Support

Please have the following information available when you call:

❑ Access to the RSA Authentication Manager appliance.

❑ Your license serial number. To locate the license serial number, do one of the following:

- Look at the order confirmation e-mail that you received when your ordered the product. This e-mail contains the license serial number.
- Log on to the Security Console, and click **License Status**. Click **View Installed License**.

❑ The Authentication Manager appliance software version information. You can find this information in the top, right corner of the Quick Setup, or in the Security Console. Log on to the Security Console, and click **Software Version Information**.

1 RSA Authentication Manager Overview

Introduction to RSA Authentication Manager

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

Multifactor Authentication

Passwords are a weak form of authentication because access is protected only by a single factor — a secret word or phrase selected by the user. If this password is discovered by the wrong person, the security of the entire system is compromised. Multifactor authentication provides stronger protection by requiring two or more unique factors to verify a user’s identity. Authentication factors in a multifactor system may include:

- Something the user knows (a password, passphrase, or PIN)
- Something the user has (a hardware token, laptop computer, or mobile phone)
- Something the user does (specific actions or a pattern of behavior)

Authentication Manager provides the following choices for strong authentication:

- RSA SecurID, which protects access using two-factor authentication with hardware and software-based tokens.
- On-demand authentication (ODA), which protects access using two-factor authentication by sending authentication credentials to users upon request through SMS text messaging or e-mail.
- Risk-based authentication (RBA), which protects access by assessing user behavior and matching the device being used to authenticate to assess the risk-level of an authentication attempt.

  By leveraging devices that the user already owns, for example, a mobile phone, PC, or laptop, RBA and ODA enable multifactor authentication with no tokens to manage.

Key Components for RSA Authentication Manager

An RSA Authentication Manager deployment may have the following components:

Primary Instance

Replica Instance

Identity Sources

RSA Authentication Agents

Risk-Based Authentication for a Web-Based Resource

RSA RADIUS Overview

Web Tier

Self-Service

SMS plug-ins. For more information see Deploying On-Demand Authentication on page 217.

Load Balancer

Note: RSA supports and certifies many third-party products for integration with RSA SecurID, risk-based authentication (RBA), on-demand authentication (ODA), or Short Message Service (SMS). For a list of supported products, go to **https://gallery.emc.com/community/marketplace/rsa** and search for Authentication Manager. Each certification has a step-by-step implementation guide for setting up the solution.

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
- Remote deployment must be done carefully to make sure that the replica instance is secure.For information about securely deploying a remote replica instance, see “Deployment Scenarios” in the *RSA Authentication Manager 8.1 Planning Guide*.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.

Identity Sources

All users and user groups in your deployment are stored in identity sources. RSA Authentication Manager supports the following as identity sources:

- LDAP directory servers, either Active Directory or Oracle Directory Server.
- Active Directory Global Catalogs, when some or all of the Active Directory servers in its Active Directory forest are used as identity sources. In such a case, the Global Catalog is used for runtime activities, for example, looking up and authenticating users, and resolving group membership within the Active Directory forest. The Global Catalog cannot be used to perform administrative functions.
- The Authentication Manager internal database, used for administrative operations, such as enabling users for on-demand authentication and risk-based authentication.

You can integrate LDAP directory servers as identity sources in Authentication Manager without modifying the schema of the directories.

RSA Authentication Agents

An authentication agent is a software application installed on a machine, such as a domain server, web server, or personal computer, that enables authentication.

The authentication agent is the component on the protected resource that communicates with RSA Authentication Manager to process authentication requests. Any resource that is used with SecurID authentication, on-demand authentication (ODA) or risk-based authentication (RBA) requires an authentication agent.

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. You may also purchase products that contain embedded RSA Authentication Agent software. The software is embedded in a number of products, such as remote access servers, firewalls, and web servers. Information about implementing such devices is available from the Secured By RSA Partner Program. For more information, see **http://www.emc.com/partnerships/rsa-partners/secured-rsa-partner-program-overview.htm**.

Note: RBA only works with web-based authentication agents.

Risk-Based Authentication for a Web-Based Resource

Risk-based authentication (RBA) protects access to web-based resources and applications. Deploying RBA requires integrating the resource with Authentication Manager. Authentication Manager provides a template to facilitate the integration process. Once integrated, the web-based resource automatically redirects users to Authentication Manager, which does either of the following:

- Authenticates the user and returns proof of authentication to the resource
- When the risk level is high, prompts the user to provide further credentials, such as the correct answers to pre-configured security questions, before returning proof of authentication.

The web-based resource presents the proof of authentication to Authentication Manager for verification and allows the user access to the resource.

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.

Web Tier

A web tier is a lightweight application server that hosts several Authentication Manager services securely in the network DMZ. Services such as risk-based authentication (RBA), the Cryptographic Token Key Initialization Protocol (CT-KIP) for the dynamic provisioning of software tokens, and the Self-Service Console may be required by users outside of your corporate network. If your network has a DMZ, you can use a web tier to deploy these services in the DMZ.

A web tier in your DMZ offers the following benefits:

- Protects your internal network from any unfiltered internet traffic from the Self-Service Console, the CT-KIP server and RBA users. Web-tier servers receive and manage inbound internet traffic before it enters your private network.
- Allows you to customize the RBA service and web-based application user interface.
- Improves system performance by removing some processing tasks from the back-end server.

The primary and replica instances are inside a firewall in your private network.

Self-Service

Self-Service is a web-based workflow system that provides user self-service options and automates the token deployment process. Self-Service has two components:

- **Self-Service**. Users can perform some token maintenance tasks and troubleshooting without involving administrators. This reduces the time that you need to spend servicing deployed tokens, such as when users forget their PINs, misplace their tokens, require emergency access, or require token resynchronization.
- **Provisioning**. Users can request RSA SecurID tokens and perform many of the steps in the token deployment process, and the system automates the workflow. This reduces administrative overhead typically associated with deploying tokens, especially in a large-scale token deployment. Provisioning is only available with the Enterprise Server license.

Users perform self-service and provisioning tasks through the Self-Service Console.The Self-Service Console is a browser-based interface that enables users to perform certain tasks without involving administrators or Help Desk personnel, thus reducing the time that your staff spends helping users. You can install the Self-Service Console inside your firewall on the Authentication Manager instance or in the DMZ (using a web-tier server) for greater security.

By default the Self-Service Console allows users to make requests to be added to the system after answering a set of security questions. Additionally, you can configure Authentication Manager to allow users to perform the following tasks on the Self-Service Console:

- Request an RSA SecurID token
- Manage their RSA SecurID PIN
- Configure security questions for identity confirmation

- Update their profile information, for example, a mobile phone number or e-mail address
- Change their Self-Service Console passwords
- Clear the risk-based authentication (RBA) device history to unregister devices
- Change e-mail address or phone number for on-demand authentication (ODA)
- Manage their ODA PIN
- View user group membership

Important: Users can only modify data that is stored in the internal database. Users cannot use the Self-Service Console to modify data that is stored in an LDAP directory, except when a password change is forced.

Load Balancer

RSA Authentication Manager includes a load balancer that provides the following capabilities:

- Distributes authentication requests between the primary and the replica web tiers.
- Provides failover in the event that one of the Authentication Manager instances or web tiers experiences downtime.
- Forwards Self-Service Console requests coming through the HTTPS port to the primary web tier or the primary instance hosting the Self-Service Console.

RSA SecurID Authentication Overview

RSA SecurID uses a patented, time-based two-factor authentication mechanism to validate users. It enables administrators to verify the identity of each user attempting to access computers, networks, and other resources.

RSA Authentication Manager software is the management component of RSA SecurID. It is used to verify authentication requests and centrally administer security policies for authentication, users, and groups for enterprise networks.

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

Product or Application	Description
VPN access	RSA SecurID provides secure authentication when used in combination with a VPN.
Remote dial-in	RSA SecurID operates with remote dial-in servers, such as RADIUS.
Web access	RSA SecurID protects access to web pages.

Product or Application	Description
Wireless networking	Authentication Manager includes an 802.1-compliant RADIUS server.
Secure access to Microsoft Windows	Authentication Manager can be used to control access to Microsoft Windows environments both online and offline.
Network hardware devices	Authentication Manager can be used to control desktop access to devices enabled for SecurID, such as routers, firewalls, and switches.

RSA SecurID Authentication Process

The RSA SecurID authentication process involves the interaction of three distinct products:

- RSA SecurID authenticators, also known as tokens, which generate one-time authentication credentials for a user.
- RSA Authentication Agents, which are installed on client devices and send authentication requests to the Authentication Manager.
- RSA Authentication Manager, which processes the authentication requests and allows or denies access based on the validity of the authentication credentials sent from the authentication agent.

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

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

RSA SecurID Tokens

An RSA SecurID token is a hardware device or software-based security token that generates and displays a random number is called a tokencode.

In addition to the tokencode, RSA SecurID typically requires a PIN, either created by the user or generated by Authentication Manager. Requiring these two factors, the tokencode and the PIN, is known as two-factor authentication:

- Something you have (the token)
- Something you know (the PIN)

In Authentication Manager, the combination of the tokencode and the PIN is called a passcode. When users try to access a protected resource, they enter the passcode at the logon prompt. (To protect against the use of stolen passcodes, Authentication Manager checks that a passcode has not been used in any previous authentication attempt.)

RSA SecurID also supports tokens that do not require a PIN. The user can authenticate with the current tokencode only. In such a case, an alternative second factor, for example, a user's network password, is used.

Each shipment of tokens includes token seed records that you must import into the Authentication Manager. Each token seed record corresponds to an individual RSA SecurID token, and is used by Authentication Manager to generate the correct tokencode when a SecurID authentication request is received from an authentication agent.

Authentication Manager logs the serial numbers of SecurID tokens used to authenticate. By default, Authentication Manager logs the serial number in the clear, but you can mask the serial numbers of tokens when logging to syslog or using SNMP if you want to avoid transmitting and recording the serial number in the clear. RSA recommends masking token serial numbers for added security. For more information, see Mask Token Serial Numbers in Logs on page 344.

You can assign up to three RSA SecurID tokens to each authorized user on a protected system.

RSA SecurID Hardware Tokens

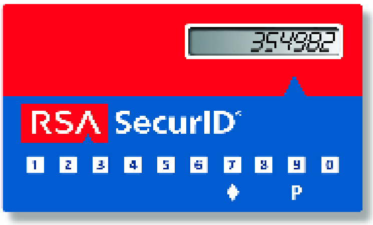
RSA SecurID hardware authenticators are available in a variety of convenient form factors.

- RSA SecurID 200 Authenticator

  This hardware token, the size of a credit card, is easily portable and extremely durable. It generates and displays a new tokencode at a predefined time interval, typically every 60 seconds.

- RSA SecurID 520 Authenticator

  With this device, the size of a credit card, the user enters the PIN on a 10-digit numeric keypad. The code displayed is a hash-encrypted combination of the PIN and the current tokencode. The RSA SecurID 520 Authenticator can offer protection against the key-logger type of malware, which may attempt to steal a user's PIN for other purposes.



- RSA SecurID 700 Authenticator

  This hardware device easily connects to any key ring. The user simply reads the changing display (typically every 60 seconds) and uses it as part of a dynamic and always-changing password.

- RSA SecurID 800 Hybrid Authenticator

  The RSA SecurID Authenticator SecurID 800 is both an RSA SecurID authenticator and a USB smart card (USB token) with a built-in reader. The two sets of electronics operate independently of each other.

When disconnected, the SecurID 800 generates and displays tokencodes used in RSA SecurID authentication. When connected to a computer, the token serves two functions:

- For RSA SecurID authentication, users obtain their tokencodes through the supporting middleware installed on their desktop instead of reading the number off the token.
- With the token's smart card capabilities, users can store credentials, including multiple X.509 digital certificates, which enable authentication, digital signature, and file-encryption applications, and Windows logon accounts.

RSA SecurID Software Tokens

RSA SecurID tokens are also available in a software form-factor that you can install into an RSA SecurID software token application on a client workstation, or a mobile device. The RSA Authentication Manager provides a centralized administration interface for issuing RSA SecurID software tokens to the supported device types. You can add information to software tokens such as device type, device serial number, or token nickname using token extension fields. For more information about the software token, see Chapter 9, Deploying and Administering RSA SecurID Tokens, and the documentation that accompanies individual RSA SecurID software token products.

The Role of RSA Authentication Manager In SecurID Authentication

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

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

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

On-Demand Authentication

On-demand authentication (ODA) delivers a one-time tokencode to a user's mobile phone or e-mail account. A tokencode is a randomly generated six-digit number. ODA protects company resources that users access through agent-protected devices and applications, such as SSL-VPNs and web portals.

ODA strengthens network security by requiring users to present two factors:

- Something only the user knows (a PIN)
- Something the user has (a tokencode)

ODA is easy to deploy because it does not require extra hardware, such as physical tokens. Employees already have and use mobile phones and e-mail accounts.

On-demand tokencodes can be used only once and expire after a specified time period, enhancing their security.

ODA relies on Short Message Service (SMS) or e-mail to deliver the tokencode. If you choose SMS, Authentication Manager sends the tokencode to SMS indirectly through an intermediary. You can customize SMS delivery to use an SMS modem (not included) or a third-party aggregation service.

On-Demand Authentication User Logon Example

When used as the sole authentication method, on-demand authentication (ODA) is especially suited for people who authenticate infrequently and from a variety of locations, or for people who need network access for a short time only, such as contractors. The following steps show how a user typically uses ODA to access a company web portal:

1. The user opens a browser window and accesses the company web portal.
2. When prompted, the user enters a User ID and PIN.

   A one-time tokencode is sent to the user’s mobile phone or e-mail account.
3. The user enters the tokencode into the browser.
4. The user gains access to the protected resource.

Risk-Based Authentication

Risk-based authentication (RBA) identifies potentially risky or fraudulent authentication attempts by silently analyzing user behavior and the device of origin. RBA strengthens RSA SecurID authentication and traditional password-based authentication. If the assessed risk is unacceptable, the user is challenged to further confirm his or her identity by using one of the following methods:

- On-demand authentication (ODA). The user must correctly enter a PIN and a one-time tokencode that is sent to a preconfigured mobile phone number or e-mail account.
- Security questions. The user must correctly answer one or more security questions. Correct answers to questions can be configured on the Self-Service Console or during authentication when silent collection is enabled.

RSA Authentication Manager contains a risk engine that intelligently accumulates and assesses knowledge about each user’s device and behavior over time. When the user attempts to authenticate, the risk engine refers to the 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. RBA compares this to the minimum acceptable level of assurance that you have configured. If the risk level is higher than the minimum assurance level, the user is prompted to confirm his or her identity by answering security questions or using ODA.

Risk-Based Authentication Prevents Data Loss from Stolen Passwords

Risk-based authentication (RBA) allows users who are accustomed to authenticating with passwords to continue doing so with little or no impact on their daily tasks. At the same time, RBA protects your company if passwords are stolen.

For example, consider John, a sales representative who regularly accesses the corporate SSL-VPN from his home office. John typically authenticates with just a user name and password using the same laptop every day. Suppose an unauthorized person steals John’s password and attempts to log on to the SSL-VPN from a different machine and location. RBA detects that the attacker is using an unrecognized device and challenges the attacker to confirm his identity by answering security questions. When the attacker fails the challenge, he is denied access.

Users who are accustomed to using passwords for authentication can continue to do so while RBA works in the background to protect sensitive company resources. The authentication experience is interrupted only if a user’s behavior is considered unusual.

In most cases, the typical user simply enters a password, as shown in the following steps:

1. The user opens a browser window and accesses the company web portal.
2. The user enters a password.
3. The user gains access to the protected resource.

After the password is entered, Authentication Manager analyzes the user’s risk level to determine if the user’s behavior and device are found to deviate from past attempts. Users who are considered suspicious or high risk are prompted to confirm their identity by performing these steps:

1. If the user is configured for more than one identity confirmation method, the user is prompted to choose either on-demand authentication (ODA) or security questions.
2. If the user selects ODA, the user enters a PIN. Authentication Manager sends a tokencode to the user by e-mail or SMS. The user enters the tokencode and is authenticated.

   If the user selects security questions, the user is prompted to answer predefined questions. If successful, the user is authenticated.

How Risk-Based Authentication Works

Risk-based authentication (RBA) intelligently assesses authentication risk for each user and accumulates knowledge about each user’s device and behavior over time to determine if an authentication attempt is legitimate. RBA has the following features:

Data Collection. RBA requires a learning period during which it builds up a profile of user devices and user behavior. After the initial learning period has expired, RBA continues to learn from the behavior of the user population and regularly customizes its risk model to adjust its definitions of “normal” and “abnormal” for your deployment.

Device Registration. The first time a user successfully authenticates from a device, RBA records characteristics about the device in the user’s device history and thus registers the device to the user. A registered device is one that Authentication Manager recognizes and that the user has previously used for authentication.

Device Matching. During authentication, RBA examines the characteristics of the user’s laptop or desktop computer and compares them with a list of previously used devices, in an attempt to find a close match.

Assurance Level. RBA uses the device characteristics and user behavior to calculate an assurance level, which is the likelihood that the access attempt is being made by a legitimate user. When the user attempts to authenticate, RBA refers to its collected data to evaluate the risk and then assigns an assurance level such as high, medium, or low to the user's authentication attempt.

For a full description of RBA, see Chapter 12, Deploying Risk-Based Authentication.

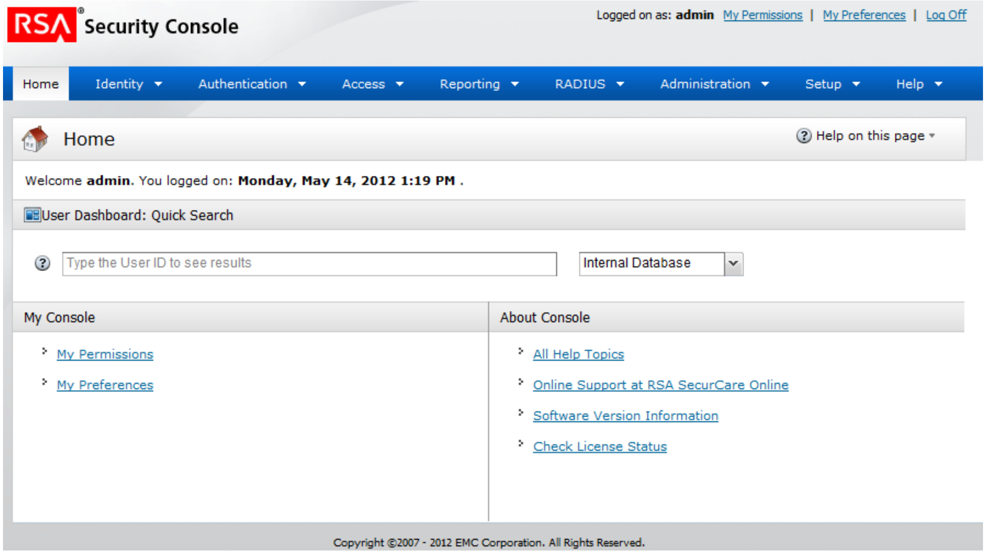
2 Preparing RSA Authentication Manager for Administration

Before you administer RSA Authentication Manager, you must prepare the deployment for administration. The following chapter explains the Security Console and the organizational hierarchy. The chapter also includes tasks for getting your deployment ready to administer.

Security Console

Authentication Manager includes an administrative user interface called the Security Console.

The following figure shows the Home page of the Security Console.



Logged on as: **admin**

Welcome **admin**. You logged on: **Monday, May 14, 2012 1:19 PM** .

Copyright ©2007 - 2012 EMC Corporation. All Rights Reserved.

You use the Security Console for most day-to-day administrative activities, and for some setup and configuration tasks. For example, you use the Security Console to:

- Add and manage users and user groups
- Add and manage administrators
- Assign and manage RSA SecurID tokens
- Enable and disable users for risk-based or on-demand authentication
- Add and manage security policies
- Add and manage authentication agents
- Designate which network resources you want to protect

During Authentication Manager Quick Setup, you define the User ID and password for the Security Console Super Admin account. The Super Admin account has permissions to perform all tasks within Authentication Manager.

You also specify the initial User ID and password for the Operations Console during Quick Setup. If you change the User ID or password for either the Security Console or the Operations Console in the future, the User ID and password for the other Console remains unchanged. These are separate accounts.

For more information on the Console accounts and passwords, see Authentication Manager Administrator Accounts on page 156.

Log On to the Security Console

If this is the first logon after Authentication Manager Quick Setup, use the User ID and password provided during setup. If this is not the first logon, enter the credentials required by the Security Console.

Note: Do not use the back button for your Internet browser to return to previously visited Console pages. Instead, use the Security Console navigation menus and buttons to navigate.

Procedure

To log on to the Security Console, go to the following URL:

```
https://fully qualified domain name:7004/console-ims
```

Important: If the Security Console is protected with RSA SecurID, the SecurID PIN is case sensitive.

For more information on protecting the Security Console with RSA SecurID, see Security Console Protection on page 37.

Security Console Customization

You can customize the Security Console by configuring the personal display preferences or the system-wide display options. The attributes are set on an administrator basis, so each administrator can configure his or her own Security Console sessions.

Set Personal Preferences

From the Security Console, you can specify the number of items displayed on list pages and the language used in the Security Console.

Procedure

1. In the Security Console home page, under My Console, click **My Preferences**.
2. To specify the default number of items that display on a list page, select a choice from the **Items Per List Page** drop-down menu.
3. To specify the language you want the Security Console to use, select a choice from the **Language** drop-down menu.

4. To change a shortcut key, type the new key next to the element, under Keyboard Shortcuts. Each shortcut must uniquely identify an element, therefore, you cannot repeat a character.
5. Click **Save**.

Next Step

You must log off and log back on before your preferences take effect.

System-Wide Display Options Customization

You can configure the following Security Console system-wide display options.

Option	Description
Items per list page	Set the number of items returned on each search results page. You can choose 25, 50, 100, 250, or All. The default value is 25.
Language	Set the language used in the Security Console. The default is English.
Identity attributes	By default, show only attributes with values within the user form display. Show or hide identity attributes that display in forms, for example, Mobile Phone Number.
Quick User Search Criteria	Configure the quick user search on the home page and user dashboard to search by last name or User ID. The default is last name
Table columns	Show or hide information in table columns in user lists.
Search criteria	Show or hide the attributes that display in the "Where" drop-down menu in the search panel of user list pages.
Basic user attributes	Show or hide user attributes that display in forms, for example, First Name.
Table columns	Show or hide information in table columns in token lists.
Search criteria	Show or hide the attributes that display in the "Where" drop-down menu in the search panel of token list pages.

Set Console Display Options

Security Console display options determine what information administrators can see when they use the Security Console. These options affect the entire deployment.

Some settings can be overridden by an individual administrator's personal preference settings. Only the administrator can see these changes.

All new identity attribute definitions that you add are hidden by default in the **Table Columns** field, but are displayed by default in the **Search Criteria** and **Identity Attributes** fields.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Under Console & Session Settings, click **Security Console Display Options.**
3. For **Items Per List Page**, select the number of items to display on each list page.
4. For **Language**, select the language for the Security Console.
5. For **Identity Attributes**, select the default to display only attributes with values on user forms. You can toggle the show and hide functions for individual users on the user form.
6. For **Quick User Search Criteria**, select whether to search by last name or User ID in the quick user search and the User Dashboard.
7. Under **User List Display,** do the following:
   a. For **Table Columns**, select which columns to display on pages that list users. For example, the columns you select display on the Users page when you click **Identity** > **Users** > **Manage Existing**. The User ID column is required.
   b. For **Search Criteria**, select which criteria to display in the search criteria drop-down menu on pages that list users. The User ID column is required.
8. Under **User Form Display**, do the following:
   a. For **Basic User Attributes**, select which items to display on user forms. Administrators cannot edit or view hidden attributes. The User ID and Last Name fields are required.
   b. For **Identity Attributes**, select which identity attributes to display on user forms. Administrators cannot edit or view hidden attributes. Make sure that all hidden identity attributes are removed from the identity attributes selected for display.
9. In the **Token List Display** section, do the following:
   a. Use the **Table Columns** fields to select which columns that you want to display on pages that show lists of SecurID Tokens. SecurID Token Serial Number is always shown in the SecurID Token list and is always the first column.
   b. In the **Search Criteria** fields, select which criteria that you want to display in the search criteria drop-down menu on pages that show lists of SecurID Tokens. SecurID Token Serial Number is always shown in the search criteria drop-down menu and is always the first column.
10. Click **Save**.

Security Console Protection

By default, an administrator can use an RSA password or an LDAP password to access the Security Console. To use an LDAP password for this purpose, the administrator's identity source must be an LDAP directory server.

For additional security, you can configure Authentication Manager to require administrators to present an RSA SecurID passcode before they can access the Security Console.

You can change the default settings by configuring one or more of the following authentication methods:

- RSA password
- LDAP password
- RSA SecurID passcode

Presenting a SecurID passcode before being allowed access ensures that the Security Console is protected by the same two-factor authentication that protects your network resources. If the Security Console is protected with a SecurID passcode, the SecurID PIN is case sensitive.

When you first enable a new Security Console authentication method, RSA recommends that you also continue to allow administrators to authenticate with the previous method for a period of time. This gives you time to ensure that all administrators can authenticate with the new method before you discontinue the previous method.

Configure Security Console Authentication Methods

Use this procedure to configure the authentication method an administrator must use to access the Security Console. For example, you can add security by requiring administrators to present an RSA SecurID passcode before they can access the Security Console.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Under Console & Session Settings, click **Security Console Authentication Methods**.
3. In the **Console Authentication** field, enter the authentication method(s) that administrators must use to log on to the Security Console. If you enter multiple authentication methods, use an available operator to create a valid expression. For example:
   - To require an RSA password or LDAP password, enter **RSA_Password/LDAP_Password**.
   - To require both an RSA SecurID passcode and LDAP password, enter **SecurID_Native+LDAP_Password**.
   - To require an RSA password, enter **RSA_Password**.

- To require an LDAP password, enter **LDAP_Password**.
- To require an RSA SecurID passcode, enter **SecurID_Native**.

If you enter an authentication method that is stronger than the current method, you are logged off and must authenticate with the new credential. For instance, if the original method was **RSA_Password/LDAP_Password** and you enter **(RSA_Password/LDAP_Password)+SecurID_Native**, you are logged off from the Security Console and must authenticate with an RSA Password or an LDAP Password, and an SecurID passcode. If you enter a method that is not stronger than the current method, the change only affects new authentication attempts.

4. (Optional) For **Non-Unique User IDs**, select **Identical User IDs may exist in more than one identity source** if you want to allow the same User ID to exist in more than one identity source. This can be useful if you have multiple identity sources that contain names for different types of users.

   Suppose that you have one identity source for employees and one for clients. This option allows identical User IDs that exist in both identity sources to be managed by the system, for example, if you have an employee with the User ID jsmith and a customer with the User ID jsmith.

5. (Optional) For **LDAP Password**, select **Enable LDAP Password authentication method** to enable the LDAP password as an authentication method.
6. Click **Save**.
7. Select **Yes, update authentication methods**.
8. Click **Update Authentication Methods**.

Identity Sources

An identity source is a repository that contains user and user group data. Each user and user group in a deployment is associated with an identity source.

Authentication Manager supports the following as identity sources:

- An LDAP directory

  Authentication Manager supports the following directories as identity sources:

  – Microsoft Active Directory 2008 R2

  – Microsoft Active Directory 2012

  – Sun Java System Directory Server 7.0

  – Oracle Directory Server Enterprise Edition 11G

  In Active Directory, you can add a Global Catalog as an identity source, which is used to look up users and resolve group membership during authentications. You cannot use a Global Catalog identity source to perform administrative tasks.

- The Authentication Manager internal database

Data from an LDAP Directory

Authentication Manager has read-only access to all LDAP directory identity sources. After a directory is integrated with Authentication Manager, you can use the Security Console to do the following:

- View (but not add or modify) user and user group data that resides in the directory.
- Perform Authentication Manager administrative tasks. For example, enable or disable the use of on-demand authentication (ODA) and risk-based authentication (RBA), or assign tokens or user aliases to individual users who reside in the directory.

You must use the LDAP directory native user interface to modify data in a directory.

Data from the Internal Database

Authentication Manager provides an internal database where you can create users and user groups. For users and user groups in the internal database, administrators can use the Security Console to do the following:

- Add, modify, and view user and user group data.
- Enable or disable Authentication Manager functions, such as ODA and RBA, for individual users, including users whose accounts are in an LDAP directory.

The following information is stored only in the internal database:

- Data that is specific to Authentication Manager, such as policies for administrative roles, and records for authentication agents and SecurID authenticators
- Data that links Authentication Manager with LDAP directory user and user group records

Security Domain Overview

Security domains represent areas of administrative responsibility. All Authentication Manager objects are managed by, and belong to, a security domain. Security domains allow you to:

- Organize and manage users.
- Enforce system policies.
- Limit the scope of administrators’ control by limiting the security domains to which they have access.

User Organization and Management

When you create a security domain, it is nested within a parent security domain. You can nest the security domains to create an administrative hierarchy. Organizing users in security domains also helps you find users and assign them tokens or add them to user groups. For example, you can search for all users in the Boston security domain and then assign a token to each member. Each user can exist in only one security domain.

By default, all users from an external LDAP identity source are added to the top-level security domain. You can use the Security Console to move these users to a lower-level security domain manually or you can configure domain mapping to add these users to a specific security domain. Make sure your mappings are in place before you manage users, so that you do not have to move users between security domains later. For more information, see Move Users Between Security Domains on page 122.

Users created in the internal database using the Security Console are created in the security domain to which the administrator has access.

Policy Enforcement

When you set up Authentication Manager a top-level security domain is automatically created. You cannot edit the name of the top-level security domain. By default, an installation of Authentication Manager supports up to 1,000 security domains.

Authentication Manager enforces authentication policies at the security domain level, so consider grouping users subject to the same policies together in the same domain.

Scope of Administrator's Control

By default, all SecurID tokens are managed in the top-level security domain. You can use the Security Console to transfer tokens from the top-level security domain to other security domains within the deployment.

Know the following about security domains:

- Security domains are organized in a hierarchy.
- Security domains are often created to mirror the departmental structure or the geographic locations of an organization.

For example, you can create separate security domains for each department, such as Finance, Research and Development (R&D), and Human Resources (HR), and then move users and user groups from each department into the corresponding security domain. To manage users in a given security domain, an administrator must have permission to manage that security domain.

In addition to making it easier to manager users, security domains allow you to limit the scope of an administrator's permissions. For example, suppose you have security domains named Boston, New York, and San Jose. When you set the administrative scope for your administrative roles, you might choose to limit the role to only the Boston security domain. This means that the administrator assigned that role only has permission to manage the Boston security domain, and not the New York and San Jose security domains.

An arrangement such as this allows you greater control over administrators. You can limit administrators by department, geographic location, or in any other way that you choose. Hierarchies also give administrators more flexible control over users and their access rights and restrictions.

Security Domains and Policies

You also use security domains to enforce system policies. Policies control various aspects of a user's interaction with Authentication Manager, such as password lifetime, length, format, frequency of change, and number of unsuccessful authentication attempts.

The following policies are assigned to security domains:

- Token Policy on page 76
- Lockout Policy on page 90
- Offline Authentication Policy on page 82
- Password Policy on page 85
- Self-Service Troubleshooting Policy on page 92
- Risk-Based Authentication Policies on page 94
- Risk-Based Authentication Message Policy on page 97

Authentication Manager provides a default of each policy type and assigns them to each new security domain. You can accept the default policies or create custom policies. If you designate a custom policy as the default, that policy will be used for all new security domains and for all existing security domains that are configured to use the existing default policy.

For example, suppose you create a custom policy named Finance Password Policy and designate it as the default password policy. Finance Password Policy is automatically assigned to all new security domains, and to all security domains configured to use the default password policy. A few months later, you create another custom policy named Miller and Strauss Password Policy, and designate it as the default password policy. The Miller and Strauss Password Policy is then used by all security domains configured to use the default password policy, and will automatically be applied to all new security domains.

Lower-level security domain do not inherit policies from upper-level security domains. New security domains are assigned the default policy regardless of which policy is assigned to security domains above them in the hierarchy. For example, if the top-level security domain is assigned a custom policy, lower-level security domains are still assigned the default policy.

Add a Security Domain

A security domain defines an area of management responsibility, typically corresponding to a company's internal business units, departments, and so on. A security domain represents a single unit in an organizational hierarchy. You build the hierarchy by creating relationships between security domains. You can create up to 1,000 security domains.

Before You Begin

- Learn about the custom and default policies available. For more information, see Security Domains and Policies on page 40.
- Follow these guidelines:
  - To use the default policy, select **Always Use Default** from the drop-down list. The default policy is automatically applied to the security domain.
  - To use a custom policy, select a policy name from the drop-down list. This policy applies to that security domain until you explicitly change it.

- When you apply a policy that is also the default policy, that policy remains assigned to the security domain even if you change the default policy. To use the default policy, you must explicitly specify **Always Use Default**.

Procedure

1. In the Security Console, click **Administration** > **Security Domains** > **Add New**.
2. In the **Security Domain Name** field, enter a unique name. Do not exceed 100 characters.
3. From the **Parent** drop-down list, select the parent security domain of the new security domain. The parent security domain is the security domain in which you want the new security domain to exist.
4. From the **Password Policy** drop-down list, select the password policy of the new security domain. Password policies enforce rules such as the required length of passwords, characters, and restricted words.
5. From the **Lockout Policy** drop-down list, select the lockout policy that you want to assign to the new security domain. Lockout policies lock out users after a designated number of consecutive unsuccessful logon attempts within a specified time period. Locked out users cannot authenticate.
6. From the **Self-Service Troubleshooting Policy** drop-down list, select a policy for the new security domain. This policy controls how users log on to the Self-Service Console if they cannot authenticate using primary methods such as passwords or passcodes.
7. From the **Risk-Based Authentication (RBA) Policy** drop-down list, select a policy for the new security domain. RBA policies include the minimum assurance level that is required for logon and the identity confirmation methods that are allowed when an authentication attempt does not meet the minimum assurance level.
8. From the **SecurID Token Policy** drop-down list, assign a SecurID token policy to the security domain. Token policies determine RSA SecurID PIN lifetime and format, and fixed passcode lifetime and format. The token policy also determines how to handle users or unauthorized people who enter a series of incorrect passcodes.
9. From the **Offline Authentication Policy** drop-down list, select an offline authentication policy for the security domain. Offline authentication policies define how users authenticate when they are not connected to the network.
10. (Optional) From the **Workflow Policies** drop-down list, select a workflow policy for the security domain. Workflow policies specify who receives e-mail, workflow definitions, the number of approval and distribution steps, and e-mail notifications for requests made through the Self-Service Console.
11. From the **Risk-Based Authentication (RBA) Message Policy** drop-down list, select a policy for the new security domain. This policy defines the message that users receive when they are challenged to configure their identity confirmation method.
12. Click **Save**.

Default Security Domain Mappings

By default, the system places all users from an external LDAP identity source in the top-level security domain. Configuring security domain mappings allows you to override the default behavior so that the system places users from a particular LDAP identity source, or from a specific organizational unit within the identity source, into a specific security domain.

For example, if you want to map the users in your sales force to the "Corporate" security domain and your salespeople are stored in your LDAP directory under "ou=sales,dc=example,dc=com" then you can create a mapping between the security domain named "Corporate" and "ou=sales,dc=example,dc=com" distinguished name (DN). After the mapping is created, users in the sales ou appear as being managed by the "Corporate" security domain instead of the top-level security domain.

Consider the following:

- When no security domain mappings exist, the system adds users to the top-level security domain.
- When multiple security domain mappings exist, the system applies the most specific mapping to a new user record.

  For example, suppose there are two mappings for users in the external identity source based on ou=sales and ou=commercial,ou=sales. A user in ou=commercial,ou=sales is created using the rule for ou=commercial,ou=sales, but a user in ou=retail,ou=sales is created using the rule for ou=sales.
- Security domain mappings are applied only to users who have never been managed in the deployment.
  - Prior to configuring security domain mapping, if an administrator performs an administrative action that affects a user, for example, enabling the user for on-demand authentication, that user is added to the top-level security domain.
  - After mapping, previously managed users remain in the security domain to which they currently belong. You must use the Security Console to move the users to another security domain manually. Updating the default security domain mappings for an identity source does not move all users in that identity source to the updated security domain.
- Delegated administration is enhanced by default security domain mappings. The mappings add users to security domains that are managed by specific administrators whose scope is restricted to the security domain. In this way, only administrators with the correct scope are allowed to manage users, and there is no need for a Super Admin to add the users to the security domain manually.
- Each security domain mapping points to a distinguished name in the external identity source, and the mapping applies to all objects within the DN except when a more specific mapping exists.

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.

Administrative Role Overview

Administrators manage all aspects of your deployment, such as users, tokens, and security domains. Each administrator is assigned an administrative role that has its own set of administrative privileges and areas of responsibility.

Administrative roles control what an administrator can manage. When an administrative role is assigned to a user, the user becomes an administrator.

Types of Administrative Roles

There are two types of administrative roles:

- **Predefined roles.** Authentication Manager provides predefined roles. You can assign predefined roles in their default form, or you can edit the permissions for each role.

  For example, if you do not want administrators with the Help Desk role to view authentication agents, you can use the Security Console to remove that permission from the role.

- **Custom roles.** You can create custom roles with different privileges and areas of administrative responsibility, depending on your organization's needs.

  For example, suppose your organizational hierarchy is divided into three security domains: HR, R&D, and Finance. Because financial data is sensitive, you might create a custom administrator who can run and view finance reports in the Finance security domain.

Administrative Role Assignment

After you have decided which roles you need for your deployment, and added any custom roles you require, you can assign the roles to administrators.

Know the following about assigning administrative roles:

- You can assign administrative roles to any user in your identity source. You will probably only assign administrative roles to members of your information technology (IT) organization and possibly a few other trusted individuals in your organization.
- When you assign a role to a user, the user becomes an Authentication Manager administrator and can use the Security Console to administer the deployment.
- When you assign a role to an administrator, the administrator is then able to perform the administrative actions specified by the role in the security domains specified by the scope of the role.
- You can only assign administrative roles with privileges equal to or less than those of your own role. That is, you cannot assign privileges that you do not have. For example, if your administrative role only allows you to add, edit, and delete users, and create and assign administrative roles, you cannot assign a role that enables users to receive on-demand tokencodes.
- You cannot edit an administrative role that has more permissions than your role.
- You can assign more than one role to an administrator. When you do this, the administrator can only perform administrative actions in a security domain that is included in the scope of the role that grants the permission.

  For example, suppose an administrator has one role that grants him permission to manage users in the San Jose security domain, and another role that grants him permission to manage authenticators in the New York security domain. In the Security Console, the administrator is allowed to manage users in the San Jose security domain, but not the New York security domain, so users in the New York security domain are not visible to the administrator. The same rule applies to authenticators. The administrator can manage and view authenticators in the New York security domain only.
- Be sure to assign roles that grant only enough permissions and include a scope just broad enough to accomplish their tasks. Avoid granting administrative roles to administrators who do not need them.

  For example, if an administrator's job only requires him to administer users in the Boston security domain, avoid including the San Jose and New York security domains in the scope of his role.

Administrative Role Components

An administrative role has two components:

- Permissions based on the function of the role
- The Scope (security domains and identity sources) in which the permissions can be applied

Permissions

The permissions in an administrative role determine the actions that an administrator can take on objects such as users, user groups, security domains, and policies. Be sure to assign permissions that allow administrators to manage all of the objects that are needed to accomplish their assigned tasks, but do not assign permissions that are not necessary.

You can modify the permissions to manage the following areas:

- Role basics
- Security domain administration
- Delegated administration
- Users
- User groups
- Reports
- RSA SecurID tokens
- User authentication attributes
- Authentication agents
- Trusted realms
- RADIUS
- On-demand tokencodes
- Provision requests

The following permissions are available for all objects in your deployment:

All. Perform any administrative action on the object.

Delete. Delete an object.

Add. Add an object.

Edit. View and edit an object, but not to add or delete.

View. View an object, but not to add, edit, or delete.

You can expand or reduce the scope of an administrator’s role by modifying permissions. For example, assume that you are the Super Admin for FocalView Software Company. The administrator in your Boston office has a role that limits him to assigning and managing authenticators. You want the administrator to also manage agents. You can modify the administrator’s current role instead of creating a new one.

These actions give the administrator permission within the Boston security domain and any of Boston’s lower-level security domains, if applicable. If the administrative scope only includes the Boston security domain, the administrator can only manage the objects, users, authenticators, and agents, for example, belonging to that domain.

Suppose that multiple administrators have the role that manages authenticators. If you modify the role so that one of the administrators can also manage agents, all administrators with that role can also manage agents. In this case, you may want to create a new role for the one administrator who manages both authenticators and agents.

Another option is to create a second role that allows agent management and then assign the role to the administrator. In this case, the administrator would have two assigned roles.

For example, if an administrator’s only task is assigning tokens to users, you would probably assign the following permissions to the role:

- View users
- View tokens
- Assign tokens to users
- Issue assigned software tokens
- Replace assigned tokens
- Import tokens (optional)
- Enable and disable tokens (optional)

The optional permissions above slightly expand the administrative role to complement the stated task of assigning tokens to users. You would not, however, assign the permissions to add and delete users, resynchronize tokens, or manage emergency offline authentication, as they are not related to the stated task of assigning tokens to users.

Permissions Required to Create Administrative Roles and Delegate Permissions

An administrator who creates a new administrative role must have the following permissions associated with their role:

- Permission to create administrative roles.
- The same permissions that he or she wants to add to the new administrative role.
- Permission to delegate the permissions granted to his or her role. This is determined by the Permission Delegation setting for the role assigned to the administrator who is creating the new role.
- Permission to manage the security domain that is associated with the new role.

When you assign permissions to a role, make sure the administrator has all the permissions necessary to perform assigned tasks. For example:

- An administrator who assigns tokens to user must have permission to view and assign tokens, and view users.
- An administrator who resets user passwords must have permission to reset passwords and view user records.
- An administrator who assigns administrative roles to users must have permission to assign roles and view user records.
- An administrator who assigns users to user groups must have permission to assign users to user groups and view user records.

You can delegate permissions to other administrators if your role permits you to create or assign existing roles to other users. For instructions on selecting Permission Delegation, see the Security Console Help topic "Duplicate an Administrative Role."

Permission Limits for Managing Identity Attribute Definitions

You can limit what permissions an administrative role grants to manage specific custom-defined identity attribute definitions. For any identity attribute definition, an administrative role can grant Modify, View, and None permissions. For more information, see the Security Console Help topic "User Attributes."

You can set permissions for specific identity attribute definitions on the Permissions page when you add or edit an administrative role. For more information, see the Security Console Help topics "Duplicate an Administrative Role" and "Edit Permissions for an Administrative Role."

Scope

The scope of an administrative role determines in what security domains an administrator may manage objects and from what identity sources an administrator may manage users and user groups. For more information, see Security Domain Overview on page 39.

Be sure to assign a scope broad enough so that the administrator can access the necessary security domains and identity sources. However, avoid assigning a scope that grants access to security domains and identity sources where the administrator has no responsibilities.

Also, avoid creating situations in which an administrator can view and manage a certain user group, but cannot at least view all the users in that user group. This happens when a user group from a security domain within the administrator's scope contains users from a security domain outside the administrator's scope. When the administrator views the user group members, he or she only sees the members from the security domain within his or her scope. This creates a situation in which administrators may take action on a group, for example, granting a group access to a restricted agent, without being aware of all the users affected. This can result in users being granted privileges that they should not have.

To avoid this situation, follow these guidelines:

- Allow all administrators to at least have view permission on all users in all security domains. This ensures that there are no cases where administrators are unaware of any members of a group they are administering.
- Make sure that a user group and all members of the user group are in the same security domain. This ensures that administrators who have permissions to view user groups and to view users are able to see all member users.
- If you want the administrator to run reports on the viewable information, grant the appropriate permission. Some reports require more than view permission.

Know the following about scoping administrative roles:

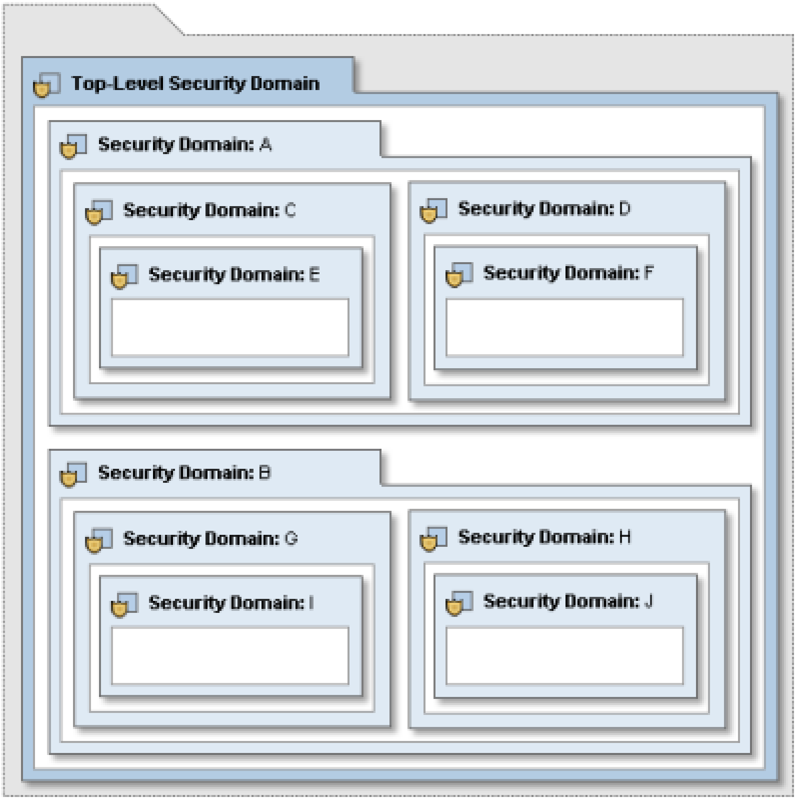
- When the scope of an administrative role is defined most broadly, the role can manage the security domain where the role definition was saved and all of the lower-level security domains beneath it.

- An administrative role that manages an upper-level security domain always manages the lower-level security domains beneath it.
- You can limit the scope of an administrative role to specific security domains, as long as those security domains are at or below the security domain that is associated with the role. An administrative role can only manage down the security domain hierarchy, never up.
- The security domain where you save the administrative role impacts the scope of the role. For example, suppose the top-level security domain is Boston, and the lower-level security domains are named New York and San Jose. If you save an administrative role to the New York security domain, administrators with that role can only manage objects in the New York security domain and in lower-level security domains within the New York security domain. Administrators with that role cannot manage objects in the Boston or San Jose security domains.

  You can save the Super Admin role in the top-level security domain, and then save all other administrative roles in a lower-level security domain. This prevents lower-level administrators, for example, Help Desk Administrators, from editing the Super Admin’s password and then using the Super Admin’s password to access the Security Console.

Scope Example

For example, consider the following hierarchy.



- An administrative role saved in the top-level security domain can be scoped to manage any security domain in the deployment. For example, it can manage only security domain F, or every security domain.
- An administrative role saved in security domain A can be defined to manage security domain A and all the lower-level security domains below it.
- An administrative role saved in security domain C can be defined to manage E, or both C and E.
- An administrative role saved in security domain E can be defined to manage only security domain E.

An administrative role can be defined so that it manages only users or user groups within a particular administrative scope who match certain criteria. These are called attribute-based roles. For example, if you have defined an identity attribute definition for location, an administrative role can manage all users in security domain A and down the hierarchy (C, D, E, and F).

You can also create a role that only allows an administrator to edit specified custom user identity attribute definitions. You configure permissions to a specific identity attribute definition as part of the role's permissions.

For a given attribute, the role can specify one of the following access permissions:

- None
- Read-Only
- Modify

Predefined Administrative Roles

The following are the predefined administrative roles:

- Super Admin
- Root Domain Administrator
- Security Domain Administrator
- RADIUS Administrator
- User Administrator
- Token Administrator
- Help Desk Administrator
- Privileged Help Desk Administrator
- Agent Administrator
- Request Approver
- Token Distributor
- Trust Administrator

Super Admin

The Super Admin role is the only role with full administrative permission in all security domains in your deployment. Use this role to create other administrators, and to create your security domain hierarchy.

Assign this role only to the most trusted administrators.

Only a Super Admin can manage the Super Admin role.

You cannot duplicate, edit, or delete the Super Admin role.

A Super Admin is the only administrator who can do the following:

- Configure external directories as identity sources so that users in the directories can be accessed through the Security Console.
- Upgrade a product license.

Use session lifetimes to limit administrative sessions. For more information, see the Security Console Help topic "Edit Session Lifetime Settings."

The number of Super Admins is based on the needs of your organization. You assign the Super Admin role in the same way that you assign all of the other administrative roles. For information, see Administrative Role Settings on page 55.

Your deployment should have at least two Super Admins. This ensures that you have full administrative control in situations where a Super Admin leaves for vacation or some other extended absence.

For example, if your organization has locations in Boston, New York, and San Jose, you might have four Super Admins: two in Boston, and one each in New York and San Jose. This arrangement allows for a vacation or extended-leave backup for the Super Admins in the Boston site, where most of the system management occurs. It also allows management of the deployment to occur from the New York or San Jose site if the Boston headquarters loses connectivity, or is otherwise unable to manage the deployment.

No one, including the administrators assigned the Super Admin role, can modify the Super Admin role.

The following occurrences can leave your deployment with no Super Admin:

- The only user assigned to the Super Admin role is deleted.
- The only user assigned to the Super Admin role is unassigned from the role.
- The only user assigned to the Super Admin role is locked out of the Security Console. This can happen if you change the Security Console logon requirement from password to SecurID, and you change the requirement before assigning a token to the Super Admin.

If any of these events occur, use the Super Admin Restoration utility to restore a Super Admin. For instructions, see Restore the Super Admin on page 408.

Root Domain Administrator

The Root Domain Administrator has complete responsibility for managing all aspects of the security domain tree including top-level objects such as policies and attribute definitions. This role does not include certain Super Admin permissions.

The default permissions for this role include complete management of the following:

- Policies
- Security questions
- Delegated administration
- Users
- User groups
- Reports
- Tokens
- User authentication attributes
- Authentication agents
- Trusted realm
- RADIUS
- On-demand authentication

Security Domain Administrator

The Security Domain Administrator manages all aspects of a branch of the security domain hierarchy. This administrator has all permissions within that branch except the ability to manage top-level objects, such as policies and attribute definitions. By default the scope of this role includes the entire deployment.

To limit the scope of this role scope to a lower-level security domain, edit the scope of the duplicate role. This role has the same permissions as the Super Admin, but is limited to the security domain in which it is created. The Security Domain Administrator can delegate some responsibilities of this role.

The default permissions for this role include complete management of the following:

- Security domains
- Administrative roles
- Permissions
- User groups
- Reports
- Tokens
- User accounts
- Agents

RADIUS Administrator

The RADIUS Administrator grants administrative responsibility to manage RADIUS servers. This administrator can not delegate the responsibilities of this role.

The default permissions for this role includes complete management of RADIUS and Agents.

User Administrator

The User Administrator manages users, assigns tokens to users, and accesses selected authentication agents. This administrator cannot delegate the responsibilities of this role.

The default permissions for this role include limited management of the following:

- Users—add, delete, edit, view, assign authentication methods (RBA or ODA)
- User groups—view user group, assign user group membership
- Reports—add, delete, edit, view, run, schedule
- Tokens—view, reset SecurID PINs, enable and disable SecurID tokens, resynchronize tokens, assign tokens to users, replace tokens, issue software tokens, manage online and offline emergency access tokencodes
- User accounts—manage fixed passcode, manage logon aliases, edit default shell manage incorrect passcode count, clear cached Windows credential, manage offline emergency access passcode
- Agents—view, grant user groups access to restricted authentication agents

User Administrators can run a subset of the Authentication Manager reports. For more information, see Reports on page 329.

Token Administrator

The Token Administrator can import and manage tokens, and assign tokens to users. This administrator cannot delegate the responsibilities of this role.

The default permissions for this role include limited management of the following:

- Users—view
- Reports—add, delete, edit, view report definition, run, schedule
- Tokens—import token, delete token, edit token, view token, reset SecurID PINs, resynchronize tokens, manage online and offline emergency access tokencodes, assign tokens to users, replace tokens, issue software tokens, manage incorrect passcode count.

Help Desk Administrator

The Help Desk Administrator resolves user access issues through password reset and unlocking or enabling accounts. This administrator cannot delegate the responsibilities of this role.

The default permissions for this role include limited management of the following:

- Users—view, reset passwords, enable and disable accounts, terminate active sessions.
- User groups—view user groups
- Tokens—view token, reset SecurID PINs, resynchronize tokens, enable and disable SecurID tokens
- Agents—view

Privileged Help Desk Administrator

The Privileged Help Desk Administrator resolves user access issues through password reset and unlocking or enabling accounts. In addition, this role grants the ability to view and provide both online and offline emergency access help. This administrator cannot delegate the responsibilities of this role.

The default permissions for this role include limited management of the following:

- Users—view, reset passwords, enable and disable accounts, terminate active sessions
- User groups—view user groups
- Tokens—view token, reset SecurID PINs, resynchronize tokens, enable and disable SecurID tokens
- Agents—view
- Fixed passcode—view and edit fixed passcodes
- Offline emergency access passcode—May manage offline emergency access passcode

Agent Administrator

The Agent Administrator manages authentication agents and grants access to selected authentication agents. This administrator cannot delegate the responsibilities of this role.

The default permissions for this role include limited management of the following:

- Users—view
- User groups—view user groups, assign user group membership
- Reports—add, delete, edit, view report definition, run, schedule
- Agents—add, delete, edit, view, manage node secret, grant user groups access to agents
- Security Domains—view

Agent Administrators can run a subset of the Authentication Manager reports. For more information, see Reports on page 329.

Request Approver

The Request Approver can view and approve requests. This administrator can not delegate the responsibilities of this role.

The default permissions for this role include limited management of the following:

- Requests—view and approve
- Users—view
- Tokens—view token

If a user requests enrollment in a security domain, the approver in that security domain can approve the request before the user is in the actual domain.

Token Distributor

The Token Distributor can view requests, distribute requested tokens, and determine how to assign and deliver tokens to users.

The default permissions for this role include limited management of the following:

- Requests—view and distribute
- Users—view
- Tokens—view token

Trust Administrator

The Trust Administrator can manage cross-deployment trusts, trusted users, and trusted user groups. This administrator can not delegate the responsibilities of this role.

The default permissions for this role include limited management of the following:

- Trusted users—add, delete, edit, and view trusted users
- Trusted user groups—add, delete, edit, and view trusted user groups
- Trusted user group restricted access—edit and view
- May assign trusted users to trusted user groups
- May grant trusted user groups access to an agent.
- May configure trusted realms.

Administrative Role Settings

The following table describes the settings of an administrative role.

Administrative Role Settings	Description
Administrative Role Name	Name of an administrative role. A role name must be unique in the security domain where it is defined, but does not have to be unique for the deployment. Administrative role names typically reflect administrators' functions within an organization, such as Help Desk, IT, or Human Resources.
Permission Delegation	Allows administrators to delegate their role permissions to other administrators. This selection only applies to administrators who also have the ability to create, edit, and assign administrative roles.
Notes	A brief explanation of the role.

Administrative Role Settings	Description
Security Domain Scope	Determines where an administrator assigned the role has administrative permissions. When an administrative role grants permissions in a security domain, permissions are also granted in each of its lower-level security domains in the security domain hierarchy.
Identity Source Scope	The identity sources where you want the administrative role to grant permissions.
General Permissions	Determines the actions an administrator can take on policies, security questions, delegated administration, users, user groups, and reports. If the scope of the role does not include the top-level security domain, the role cannot manage identity attribute definitions, password policies, lockout policies, self-service troubleshooting policies, security questions and Console display options.
Authentication Permissions	Determines the authentication related tasks an administrator can perform. These tasks include management of RSA SecurID, user authentication attributes, authentication agents, trusted realms, RADIUS and on-demand authentication. If the scope of the role does not include the top-level security domain, the role cannot manage RADIUS.
Self-Service Permissions	Determines the actions an administrator can take on provisioning requests.
Security Domain	The security domain that is associated with the administrative role. The new administrative role can only be managed by administrators whose scope includes the security domain that is associated with the role.

Administrative Role Scope and Permissions

The pre-defined administrative roles configured during Authentication Manager setup have scope over the top-level security domain by default. As a result, an administrator who is assigned to a pre-defined role can modify the account of a Super Admin, because the initial Super Admin account resides in the top-level security domain as well. This is because the top-level security domain is the only security domain in the deployment when Authentication Manager is initially set up.

Before assigning a pre-defined role to an administrator, consider whether you want to maintain the default behavior, or if you want to restrict the scope of the administrators assigned these roles to a lower-level security domain that does not include Super Admins or other higher-privileged administrators. There may be situations in which you want a lower-privileged administrator to modify the account of a higher-privileged administrator.

For existing deployments, you can use the Security Console to audit the permissions available to an administrator. For instructions, see the Security Console Help topic “View Available Permissions of an Administrator.”

If you do not want to use the default scope of the pre-defined administrative roles, you can avoid unintentionally granting additional privileges to an administrator by doing one of the following:

- Make sure that the scope of the administrator does not include the following:
  - A security domain that contains the user account or token of a higher-privileged administrator.
  - The security domain that contains the administrator’s own token so that the administrator cannot modify his own token or other credentials to provide additional privileges to his account.
  - The administrator’s own security domain so that the administrator cannot modify his own account.
- Create separate security domains to enforce your intended administrative scopes. For example, create one for Super Admins, one for other administrators, and one for users with no administrative role. Reduce the scope of the lower-privileged administrators to the security domains of users with no administrative role.

  Configure Authentication Manager according the following model:
  - Create a distinct security domain for Super Admins.
  - Place all other administrators, including those who have permission to edit users or authentication credentials, in lower-level domains.
  - Place all other users in another security domain.
  - Assign the appropriate role and scope to administrators. Make the lower-privileged administrator’s scope include only the security domain over which the administrator has authority. For example, make sure that the Help Desk administrator has scope only for the security domain of end users, and not for his own security domain or the security domain of the Super Admin. For instructions, see the Security Console Help topic, “Change the Scope of an Administrative Role.”

If you do want to allow administrators to manage the accounts of higher-privileged administrators, there are a number of ways you can configure your system to do this.

- Make sure that the lower-privileged administrator does not have permission to edit the following account settings of the higher-privileged administrator, by removing permissions from the lower level account to edit authentication data of the higher level account, such as:
  - The credential that is required to authenticate to the Security Console, for example, the user password of a Super Admin
  - Security questions
  - LDAP password
  - RSA Password
  - Assigned SecurID tokens
  - The ability to administer other users, including the ability to clear PINs, assign SecurID tokens and enable on-demand authentication

  Note: Make sure that the administrative role assigned to the administrator does not include tasks that are not required for the administrator to perform his job. For more information, see the Security Console Help topic, “Edit Permissions for an Administrative Role.”

- If you do not use the Self-Service Console or risk-based authentication in your deployment, do the following:
  - Remove the Reset Password permission from the Help Desk administrator who is helping end users.
  - Assign the Assign Token and Reset Password permissions to an administrator other than the Help Desk administrator.
- Configure Authentication Manager to require a combination of authentication credentials. If Authentication Manager requires multiple credentials, for example an on-demand tokencode and a password, at least one of which the lower-privileged administrator does not have permission to edit, the lower-privileged administrator cannot fully control the higher-privileged administrator’s authentication credentials and authenticate to the Security Console or Operations Console as the higher level administrator.

Add an Administrative Role

An administrative role is a collection of permissions that can be assigned to an administrator. A role determines what level of control the administrator has over users, user groups, and so on.

You can add administrative roles to your deployment, and assign these roles to users. If you assign multiple administrative roles to a user, the permissions are combined.

Before You Begin

To create an administrative role, you must have an administrative role that:

- Grants permission to create administrative roles.

- Includes the permissions he or she wants to add to the new administrative role.
- Allows the administrator to delegate the permissions granted to his or her role. This is determined by the Permission Delegation setting for the role assigned to the administrator who is creating the role.

Procedure

1. In the Security Console, click **Administration** > **Administrative Roles** > **Add New**.
2. In the **Administrative Role Name** field, enter a name for the new administrative role.
3. (Optional) If you want to allow administrators to delegate their role permissions to other administrators, select **Permission Delegation**.
4. In the **Security Domain Scope** tree, select the security domains in which the new administrative role grants permissions.
5. In the **Identity Source Scope** field, select the identity sources where you want this administrative role to grant permissions.
6. Click **Next**.
7. Assign general permissions to the administrative role.
8. (Optional) To restrict attributes, in the **User Attribute Restriction** field, select **May only access specific attributes**. An **Attributes** drop-down menu appears. Select **Modify, View**, or **None** for each attribute. If you select **None**, the attribute is hidden.

   The value in this field must be consistent with the value specified in the **Entry Type** field on the Add an Identity Attribute Definition page. If the attribute definition is read-only, do not select Modify for the User Attribute Restriction. If the attribute definition is required, do not specify View or None in the User Attribute Restriction. If you do, you cannot add the role. For more information, see the Security Console Help topic "Add an Identity Attribute Definition."
9. Click **Next**.
10. Assign authentication permissions to the administrative role.
11. Click **Next**.
12. Assign self-service permissions to the administrative role.
13. Click **Next**.
14. Use the **Security Domain** drop-down menu to select the security domain that is associated with the administrative role.
15. Review the summary of the administrative role, and click **Save**.

Assign an Administrative Role

You can assign an administrative role to a user so that the user can perform specified actions in a designated security domain. A user can have more than one administrative role.

Follow these guidelines:

- You can only assign and add administrative roles with the same or a narrower scope, and that have equal or fewer permissions to your own administrative role.
- You can assign administrative roles to a single user at a time or to multiple users at the same time.

If a password is required to access the Security Console, administrators use the password assigned to them in their user record.

Procedure

1. In the Security Console, click **Administration** > **Administrative Roles** > **Manage Existing**.
2. Use the search fields to find the administrative role that you want to assign.
3. Click the administrative role that you want to assign.
4. From the context menu, click **Assign More**.
5. Use the search fields to find the user that you want to assign to the administrative role.

   User searches are case sensitive.
6. Select the user that you want to assign to the administrative role, and click **Assign to Role**.

View Available Permissions of an Administrator

Under some configurations, a lower-privileged administrator, for example, an administrator assigned the default Help Desk Administrator role, may be able to modify the account of a higher-privileged administrator. To audit the permissions assigned to administrators and verify that lower-privileged administrators do not have permissions that allow them to modify the accounts of higher-privileged administrators, use the following procedure.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Identity > Users**.
2. Use the search fields to find Administrators.

3. Click the name of the administrator and select **Available Permissions** from the context menu.

   The user's assigned administrative roles are displayed. For each role, the following information displays:

   Security Domain. The security domain of the administrators who are allowed to manage the assigned role.

   Security Domain Scope. The scope of the administrator's role, i.e., where the administrator can perform the tasks for this administrative role.

   Identity Source Scope. The identity sources the administrator may access, if her administrative role includes managing users or user groups.

   Permission Delegation. Whether the assigned administrator can create new administrative roles that include this role's permissions.

   Administrative Tasks and Permissions. The permissions the administrator has to modify objects in the system, for example, permission to add users, or just view them.

Next Steps

If you find that an administrator has scope or permissions that give more privileges than appropriate, you can do the following:

- Add or remove roles from the set of roles assigned to the administrator. For more information, see Assign an Administrative Role on page 60.
- Edit one or more of the administrator’s roles to change the scope, set of permissions or both that role includes. This affects all administrators assigned the role. For more information, see the Security Console Help topic, “Edit an Administrative Role.”
- Create a new role having the correct scope and the exact set of permissions required, and assign it to the administrator. You can create a new role or duplicate an existing role and modify it. For more information, see Add an Administrative Role on page 58.

3 Deploying Authentication Agents

RSA Authentication Agents

Authentication agents are software applications that securely pass user authentication requests to and from RSA Authentication Manager. Authentication agents are installed on each machine, such as a domain server, web server, or a personal computer, that you protect with Authentication Manager.

For example, agent software residing on a web server intercepts all user requests for access to protected web pages. When a user attempts to access a protected URL, the agent requests the User ID and passcode and passes the User ID and passcode to the Authentication Manager for authentication. If the authentication is successful, the user is granted access to protected web pages.

Authentication Agent Types

When you deploy an agent, you specify whether the agent is unrestricted or restricted.

Unrestricted agents. Unrestricted agents process all authentication requests from all users in the same deployment as the agent.

However, to allow a user to authenticate with a logon alias, the user must belong to a user group that is associated with the logon alias and that is enabled on the unrestricted agent.

Restricted agents. Restricted agents process authentication requests only from users who are members of user groups that have been granted access to the agent. Users who are not members of a permitted user group cannot use the restricted agent to authenticate. Resources protected by restricted agents are considered to be more secure because they process requests only from a subset of users.

Obtaining RSA Authentication Agents

The agent that you need depends on the type of resource you want to protect. For example, to protect an Apache web server, you need to download the RSA Authentication Agent for Apache.

The download package includes an *Installation and Administration Guide* and a *Readme*. Read these documents before installing the agent. For information about installing agent software, see your agent documentation.

You may purchase products that contain embedded RSA Authentication Agent software. For example, these products include remote access servers and firewalls.

Procedure

Do one of the following.

- For an RSA agent and for a third-party agent that requires an RSA agent, go to **http://www.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings**.

  Locate the agent software for your platform and download the agent software and the RBA Integration Script Template.

- For a third-party agent that has an embedded RSA agent, go to the RSA Secured web site at **https://gallery.emc.com/community/marketplace/rsa?view=overview**, and locate the listing for *RSA Implementation Guide for Authentication Manager* for your agent.

  Download the *RSA Implementation Guide for Authentication Manager* for your agent. Save it to your desktop or a local drive that you can access during the integration process.

  Note: Only certified partner solutions have an implementation guide. For other agents that are certified as RSA SecurID Ready, you can create a custom implementation.

Next Steps

See Deploying an Authentication Agent on page 64.

Deploying an Authentication Agent

Authentication agents are software applications that securely pass user authentication requests to and from RSA Authentication Manager. Before an authentication agent can communicate with RSA Authentication Manager, you must deploy the agent.

Procedure

1. Use the Security Console to generate a configuration file for the agent. This allows the agent to locate Authentication Manager servers. For more information, see Generate the Authentication Manager Configuration File on page 65.
2. Install an authentication agent on each machine that you want to protect. See your agent documentation for installation instructions.
3. Use the Security Console to add a record for the new agent to the internal database. In this step, you can specify whether you are creating a restricted agent. The agent record identifies the agent to RSA Authentication Manager. This process is called registering the agent. For more information, see Add an Authentication Agent on page 66.

Generate the Authentication Manager Configuration File

You must configure communication between the authentication agents and RSA Authentication Manager. To do this, use the Security Console to generate a zip file (**AM_Config.zip**) that contains the RSA Authentication Manager configuration file, **sdconf.rec**. To configure communication, you copy **sdconf.rec** to each agent host. The **sdconf.rec** file contains a snapshot of the server topology as it was when the file was generated. The agent uses the data in the **sdconf.rec** file as a backup.

The generated zip file also contains a failover.dat file that can be configured on the agent. The failover.dat file allows agent auto-registration to complete when the primary instance is unavailable or separated from the agent host by a firewall that uses Network Address Translation (NAT).This file includes a list of the primary and replica instances, and their alias IP addresses.

Before You Begin

- Make sure an agent is connected to Authentication Manager.
- Review the configuration settings. See the Security Console Help topic "Configure Agent Settings."

Procedure

1. In the Security Console, click **Access** > **Authentication Agents** > **Generate Configuration File**.
2. From the **Maximum Retries** drop-down menu, select the number of times you want the authentication agent to attempt to establish communication with Authentication Manager before returning the message "Cannot initialize agent - server communications."
3. From the **Maximum Time Between Each Retry** drop-down menu, select the number of seconds that you want to set between attempts by the authentication agent to establish communications with Authentication Manager.
4. Click **Generate Config File**.
5. Click **Download Now**, and save **AM_Config.zip** to your local machine.

Next Steps

- Copy **AM_Config.zip**, containing the **sdconf.rec** file and the **failover.dat** file, to each agent host.
- Configure the agent with the new **sdconf.rec** file and if necessary, the **failover.dat** file. For instructions, see your agent documentation.

Add an Authentication Agent

Before an authentication agent can communicate with Authentication Manager, you must add the agent to the internal database. This process is called registering the agent. The agent record identifies the agent to Authentication Manager.

Deployments that use risk-based authentication (RBA) require additional configuration. If you use RBA to protect a web-based application, such as an SSL-VPN, web portal, or a thin client, you must integrate the web-based application with Authentication Manager. For more information, see Implementing Risk-Based Authentication on page 273.

Procedure

1. In the Security Console, click **Access** > **Authentication Agents** > **Add New**.
2. From the **Security Domain** drop-down menu, select the security domain to which you want to add the new agent.
3. Under **Authentication Agent Basics**, do the following:
   a. For **Hostname**, enter a new hostname for the agent host, and then click **Resolve IP**.

      The IP address is automatically entered. If you enter a new name, the name must be unique.

      Note: For IPv4/IPv6 agents, the hostname can be any agent descriptor and does not necessarily need to be a fully qualified host name. IP address resolution is not supported for IPv4/IPv6 agents.

   b. (Optional) In the **IP Address** field, enter the IP address of the agent.

      If you use an existing server name, this field is automatically populated and read-only. If no address is specified, UDP agents will use auto-registration to provide the address to the server.

      Note: Do not enter IP addresses in the IPv6 format. IPv4/IPv6 agents will use the hostname to provide the address to the server.

   c. (Optional) In the **Alternate IP Addresses** field, enter alternate IP addresses for the agent.

      You enter alternate IP addresses if the agent has more than one network interface card, or is located behind a static network address translation (NAT) firewall.

      If you use an existing server name, this field is automatically populated and read-only.
4. (Optional) Under **Authentication Agent Attributes,** you can select the following options:
   - To specify the type of agent, select the type from the **Agent Type** list.

     If the agent is a web agent, select **Web Agent**, otherwise keep the default selection **Standard Agent**. The populated agent types are labels, there is no functional difference by choosing Web Agent or Standard Agent.

- To disable the agent, select **Agent is disabled**.

  You might select this option to stop access to a resource temporarily.

- To add a restricted agent, select **Allow access only to members of user groups who are granted access to this agent**.

  Only users who are members of user groups that have permission to access a restricted agent can use this agent to authenticate. Any user can use an unrestricted agent to authenticate.

- To assign a manual or automatic contact list to the new agent, use the Authentication Manager Contact List buttons.

5. (Optional) To configure how users from a trusted realm authenticate to this agent, select **Enable Trusted Realm Authentication**, and then select whether you want to allow all trusted users to authenticate through the new agent or only those trusted users who belong to a trusted user group that has been granted explicit permission to use the agent.
6. (Optional) To allow users to authenticate to this agent using RBA, do the following.
   - Select **Enable this agent for risk-based authentication**.
   - If you want to restrict RBA access on this server agent, select **Allow access only to users who are enabled for risk-based authentication**.
   - Select an authentication method for RBA users.
7. Choose one of the following options to save the settings for this agent.
   - If you enabled this agent for RBA, click **Save Agent and Go to Download Page**.

     The system saves the settings and displays the Integration Script page, where you select and download the integration script for this agent.
   - If you did not enable this agent for RBA, click **Save**.

Note: If the hostname is not a fully qualified host name or the IP address is not specified, a Confirmation Required dialog, summarizing the hostname and the IP address is displayed. Here, you can either edit the agent details or save the agent information.

Next Steps

- Review the configuration settings. See the Security Console Help topic "Configure Agent Settings."
- (Optional) Generate an integration script. See the Security Console Help topic "Generate an integration Script for a Web-based Application."

Node Secret for Encryption

The node secret is a shared secret known only to the authentication agent and Authentication Manager. Authentication agents use the node secret to encrypt authentication requests that they send to Authentication Manager.

Authentication Manager automatically creates and sends the node secret to the agent in response to the first successful authentication on the agent.

The agent and the Authentication manager server must agree on the state of the node secret. For example, if the server expects the agent to have a node secret but the agent does not have one, or if the agent thinks it has a node secret and the server does not think the agent has one.

Manual Delivery of the Node Secret

In most deployments, automatically delivering the node secret is sufficient. However, you can choose to manually deliver the node secret for increased security. When you manually deliver the node secret, you must:

- Use the Security Console to create the node secret. For instructions, see Manage the Node Secret on page 69.
- Deliver the node secret to the agent, for example, on a disk, and use the Node Secret Load utility to load the node secret on to the agent.

The Node Secret Load utility does the following:

- Decrypts the node secret file.
- Renames the file after the authentication service name, usually **securid**.
- Stores the renamed file on your machine. For more information on where the renamed node secret file is stored, see your agent documentation.

When you manually deliver the node secret, take the following security precautions:

- Use the longest possible, alphanumeric password. The maximum length is 16 characters. The minimum length, required special characters, and excluded characters are determined by these default password policy for the deployment.
- If possible, deliver the node secret on external electronic media to the agent administrator, and verbally deliver the password. Do not write down the password. If you deliver the node secret through e-mail, deliver the password separately.
- Make sure that all personnel involved in the node secret delivery are trusted personnel.

For additional information about creating and sending the node secret file, see Manage the Node Secret on page 69.

Manage the Node Secret

To ensure a secure transaction the first time a user attempts to authenticate with a SecurID passcode, the authentication agent and Authentication Manager automatically communicate using a hashed value of the unique node secret and store it on the agent computer. From then on, each authentication interaction uses the node secret to encrypt the communication between the two systems.

Procedure

1. In the Security Console, click **Access** > **Authentication Agents** > **Manage Existing**.
2. Click the **Restricted** or **Unrestricted** tab, depending on whether the agent that you want to search for is restricted or unrestricted.
3. Use the search fields to find the agent with the node secret that you want to manage.
4. Click the agent with the node secret that you want to manage, and click **Manage Node Secret**.
5. If you want to clear the node secret from the Authentication Manager server, select the **Clear Node Secret** checkbox.

   To allow the agent to authenticate to the server, you must also clear the node secret on the agent.
6. (Optional) If you want to create a new node secret, select the **Create Node Secret** checkbox.
7. (Optional) If you chose to create a new node secret, enter and confirm a password to encrypt the node secret file.

   When you create a password, the maximum length is 16 characters. The minimum length, required characters, and excluded characters are determined by the default password policy for the deployment.
8. Click **Save**.
9. Click **Download Now.**

Refresh the Node Secret Using the Node Secret Load Utility

The node secret rarely needs to be refreshed, however there are times when it is necessary. Problems with the node secret can result in authentication or node verification errors. Refresh the node secret when:

- The node secret on the agent is lost, for example, when you perform a factory reset or reinstall the agent.
- The authentication agent record is either deleted or re-added.
- The node secret is deleted from one end of the connection but not the other, for example, the node secret is deleted from the Authentication Manager appliance but not from an associated agent.

You do not need to refresh the node secret when you:

- Change the agent name.
- Change the IP address.

The Node Secret Load utility, agent_nsload, is located in the RSA Authentication Manager 8.1 download kit.

Procedure

1. Create a node secret using the Security Console. For more information, see Manage the Node Secret on page 69.
2. From the RSA Authentication Manager 8.1 download kit, copy **agent_nsload** from the **rsa-ace_nsload** directory for the agent's platform to the agent host.

   RSA provides the following platform-specific versions of the utility:

   - Windows
   - LINUX
   - HP-UX
   - IBM AIX
3. From a command line on the agent host, run the Node Secret Load utility. Type:

   ```
   agent_nsload -f path -p password
   ```

   where:

   - *path* is the directory location and name of the node secret file.
   - *password* is the password used to protect the node secret file.

Automatic Agent Registration

The Automated Agent Registration and Update utility (**sdadmreg.exe)**, included with the RSA Authentication Agent software, enables new authentication agents to automatically add an agent record to the Authentication Manager internal database. This process is called registering the agent. Allowing authentication agents to self-register saves time and money by eliminating the need for an administrator to perform these tasks.

By default, when the agent host starts, the Automated Agent Registration and Update utility automatically runs to allow any IP address changes to be registered in the internal database. You can also run this utility whenever IP address of the agent host changes. This is useful for systems that use the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. If you use DHCP and do not enable this utility, you must manually update the IP addresses each time the agent host changes its IP address.

You can also run the Automated Agent Registration and Update utility manually whenever the IP address of an agent host changes, to update the IP address in the internal database.

Note: The RSA Authentication Agent 6.1.2 for Microsoft Windows automatically updates the internal database with any IP address changes. If you are using this agent, you do not need to manually run the utility.

It is important that you protect your critical IT infrastructure from potential Denial of Service (DOS) attacks. To reduce the vulnerability of your system:

- Disable agent auto-registration on critical machines, such as e-mail and VPN servers.
- In your IT infrastructure, give critical agents static IP addresses.
- Protect IP addresses within Authentication Manager. To do this, select Protect IP Address on the Authentication Agent page in the Security Console.

Allow an Agent to Auto-Register

Authentication agents can automatically add an agent record to the internal database. The process of adding an agent record is called registering the agent.

If your network uses Dynamic Host Configuration Protocol (DHCP) to assign IP addresses, consider enabling agent auto-registration. When enabled, agent IP addresses are automatically updated whenever the IP address of the agent host changes.

The Auto-Registration utility automatically registers users' computers in the Authentication Manager database the first time users start their computers with Authentication Agent installed. This utility and eliminates the need for an administrator to manually create the agent host record.

Before You Begin

- Install an authentication agent.
- Configure the agent host. See your agent documentation for information.

Procedure

1. In the Security Console, click **Setup** > **System Settings**> **Agents**.
2. Select **Allow authentication agent auto-registration**.
3. Click **Save**.

Download an RSA Authentication Manager Server Certificate

The RSA Authentication Manager server certificate is required to set up agent auto-registration.

Procedure

1. In the Security Console, click **Access** > **Authentication Agents** > **Download Server Certificate File**.
2. Click **Download Now**.
3. Select **Save it to disk**.

Next Step

To set up agent auto-registration, copy the file to the auto-registration installation directory on the agent host machine and run the **.exe** file.

Contact Lists for Authentication Requests

Contact lists are ordered lists of instances available to accept authentication requests, and are created either automatically by Authentication Manager, or manually by an administrator.

Authentication Manager uses contact lists to determine to which instance authentication requests are sent. Authentication Manager sends contact lists to each agent after the initial contact between the agent and Authentication Manager.

Depending on your license type, your Authentication Manager deployment can have a primary instance and up to 15 replica instances. To increase efficiency, use contact lists to route authentication requests from agents to the instances that can respond the quickest.

Agents request new contact lists as a part of subsequent authentications. Periodically, the agent reviews all the instances listed in the contact list to determine where to send authentication requests. The agent uses metrics, such as the amount of time it takes the instance to respond to authentication requests, to determine where to send requests.

If none of the servers on the contact list respond to authentication requests, the agent reverts to the Authentication Manager configuration file and uses an IP address in the configuration file to reconnect with Authentication Manager.

RSA RADIUS supports contact lists for the RADIUS server agent. RADIUS client agents do not support contact lists because there is no authentication agent software installed on RADIUS clients. The associated agent record in the internal database enables Authentication Manager to track RADIUS authentication attempts made through the RADIUS server. For more information, see RADIUS Clients on page 297.

IPv4/IPv6 agents do not support contact lists.

Automatic Contact Lists

An automatic contact list is assigned to each instance in your deployment. The list contains the IP addresses of each instance the contact list is assigned to, up to a limit of 11. Agents receive automatic contact lists by default.

Authentication Manager automatically updates these lists each time a new instance is added to the deployment. When the list is updated, a time stamp associated with the list is also updated. Agents use this time stamp to determine when to request an updated list.

The Super Admin can edit an automatic contact list in the Security Console on the Edit Authentication Manager Contact List page. Any edits that you make to an automatic contact list may be overwritten when a new instance is added to the deployment.

Manual Contact Lists

The Super Admin updates manual contact lists to reflect the most recent list of instances. Manual lists can contain the IP address of any instance in the deployment, up to a limit of 11.

For many organizations, automatic contact lists are sufficient. However, you may choose to create a manual contact list if you have a specific way that you want to route authentication requests.

For example, suppose that you are an administrator at a company that has Boston, New York, and San Jose locations. The New York and San Jose locations are small and all authentications are routed to Authentication Manager replica instances at each site. The Boston location, however, is largest, and the primary instance at that location handles all Boston location users, as well as all VPN requests from external users. You can create a manual contact list that routes authentication requests to the replica instances. This leaves the primary instance free to replicate data to the replica instances in New York and San Jose.

For instructions, see the Security Console Help topics, "Add a Manual Contact List," "Assign a Manual Contact List to an Authentication Agent," and "Edit a Manual Contact List."

4 Configuring Authentication Policies

Policies

Policies control various aspects of your deployment. Authentication Manager provides a default of each policy type and assigns them to each new security domain. You can also assign a custom policy. If you designate a new default policy, the new default policy is automatically assigned to existing security domains that use the default policy and to new security domains.

The policy assigned to a lower-level security domain is not inherited from upper-level security domains. New security domains are assigned the default policy that is in place at the time they are created, regardless of which policy is assigned to security domains above them in the hierarchy. For example, if the top-level security domain is assigned a custom policy, lower-level security domains are still assigned the default policy.

You can use the following policies to help administer your system.

Token Policy on page 76. A token policy defines users’ RSA SecurID PIN lifetime and format, and fixed passcode lifetime and format, as well as how a deployment handles users or unauthorized people who enter a series of incorrect passcodes. A passcode is a SecurID PIN + a tokencode. The tokencode is the number displayed on the front of a SecurID token.

Offline Authentication Policy on page 82. An offline authentication policy defines the way users authenticate when they are not connected to the network.

Password Policy on page 85. Password policies define the users' password length, format, and frequency of change.

Lockout Policy on page 90. Lockout policies define how many failed logon attempts users can make before the system locks their account. Lockout policies apply to the total number of logon attempts a user makes regardless of the type of credential used for each attempt. For example, if a user has two failures with a password and one failure with on-demand authentication, the policy counts three failed attempts and locks the user's account.

Self-Service Troubleshooting Policy on page 92. The self-service troubleshooting policy allows Self-Service Console users to troubleshoot routine authentication problems if they cannot access protected resources using primary methods, such as passwords or passcodes. This policy defines an alternative form of authentication, such as security questions, used to access the troubleshooting feature. The policy also specifies the circumstances that lock a user out of the troubleshooting feature.

Risk-Based Authentication Policies on page 94. Risk-based authentication (RBA) policies contain all RBA settings, including the minimum assurance level that is required for logon, and the identity confirmation methods that can increase the assurance level of a logon request.

Risk-Based Authentication Message Policy on page 97. The RBA message policy defines the message that users receive when they are challenged to configure their identity confirmation method.

Workflow Policy on page 248. Workflow policies determine how user requests are handled. They apply to the entire deployment. Each user request is governed by one workflow policy.

Token Policy

A token policy defines users' RSA SecurID PIN lifetime and format, and fixed passcode lifetime and format, as well as how a deployment handles users or unauthorized people who enter a series of incorrect passcodes. A passcode is a SecurID PIN + a tokencode. The tokencode is the number displayed on the front of a SecurID token.

You assign token policies to security domains. The token policy applies to all users assigned to that security domain.

When a user authenticates with a token, the token policy being enforced belongs to the users' security domain, rather than to the token's security domain. For example, if a user assigned to the New York security domain authenticates with a token assigned to the Boston security domain, the token policy of the New York security domain dictates policy requirements.

When you edit a token policy, existing PINs and fixed passcodes are not validated against the excluded words dictionary and history requirements. They are, however, validated against all other policy requirements.

Token policies assigned to upper-level security domains are not inherited by lower-level security domains. For example, if you assign a custom policy to the top-level security domain, all new security domains that you create below it in the hierarchy are still assigned the default token policy.

You need to balance security needs with consideration of what is reasonable to expect from users. Requiring a long PIN may be counterproductive and hard to remember, locking more users out of the network and generating calls to the Help Desk.

Token Policy Settings

The following table describes the token policy settings.

Token Policy Setting	Description
SecurID Token Policy Name	A unique name from 1 to 128 characters.
Incorrect Passcodes	Specifies how to handle situations where a user enters a number of incorrect passcodes before finally entering a correct passcode. You can allow users to enter a limited or unlimited number of incorrect passcodes. When the limit is exceeded and followed by a correct passcode, users are prompted to enter the next tokencode that displays on their tokens. This guards against situations in which an unauthorized person attempts to guess a passcode. In such a case, even if the person guessed a correct passcode, he or she is prompted for the next tokencode and has only one chance to enter it correctly. If the person enters the next tokencode incorrectly, authentication fails. You can allow unlimited incorrect passcodes. Do this if you never want users to be prompted to enter their next tokencode, regardless of how many incorrect passcodes they enter before finally entering one correctly. Be aware, however, that if the lockout policy assigned to the security domain is set to lock users out after a specified number of failed authentications, when the user exceeds this limit, the user is locked out. See Password Policy on page 85.
Default Policy	Designates the new policy as the default policy for the deployment. This security policy is then applied to all security domains in the deployment where **SecurID Token Policy** is set to **Always Use Default**. You can override the default policy at the individual security domain level.
Notes	Records any notes.
Periodic Expiration	An optional setting if you want to require users to change their SecurID PINs after a specified length of time. This enables the Maximum and Minimum Lifetime fields.

Token Policy Setting	Description
Maximum Lifetime	A fixed passcode can be used instead of a PIN and tokencode to authenticate. Fixed passcodes are not recommended because they eliminate the advantages of two-factor authentication. This setting determines the maximum amount of time that a user can keep a fixed passcode before being required to change it. For example, suppose the maximum fixed passcode lifetime is set to 90 days. If users change their fixed passcode on June 1, they must change it again on August 30. This setting prevents users from indefinitely keeping the same fixed passcode, which increases the likelihood that it might be guessed by an unauthorized person trying to access your network.
Minimum Lifetime	The minimum amount of time that a fixed passcode can exist before the user can change it. For example, suppose the minimum lifetime is set to 14 days. If users change their fixed passcode on June 15, they cannot change it again until June 29. This setting prevents users from circumventing restrictions on reusing old fixed passcodes that may have previously been set. For example, suppose you restrict users from reusing their five most recent fixed passcodes. The minimum fixed passcode lifetime prevents users from immediately changing their fixed passcode six times so that they can reuse a particular fixed passcode.
Restrict Reuse	Prevents users from using the same two or three fixed passcodes repeatedly. For example, if you restrict the last three fixed passcodes, users cannot enter those three fixed passcodes and must choose another. Reusing the same fixed passcodes increases the likelihood that an unauthorized person may guess a fixed passcode, especially if the fixed passcodes are all similar. The restriction forces users to move beyond those couple of fixed passcodes that they are most comfortable with, and choose more secure fixed passcodes.

Token Policy Setting	Description
PIN Creation Method	Selects the method by which SecurID PINs are generated. SecurID PINs can be system-generated or users can create their own PINs. **Note:** RSA RADIUS does not allow system-generated PINs by default. If you allow system-generated PINs, authentications will fail unless you change the RADIUS configuration file, **securid.ini**, to allow system-generated PINs. For instructions, see Password Policy on page 85.
Minimum Length	Prevents users from creating PINs that are too short and susceptible to brute force attacks.
Maximum Length	Prevents users from creating PINs that result in passcodes longer than the agent can accept. When you configure this field, make sure that your agent can accept the longest possible passcode.
Excluded Words Dictionary	A list of words that users cannot use as PINs. It includes common words that are likely to be included as part of any dictionary attacks on the system, for example, "password." The excluded words dictionary prevents users from using common, and therefore, easily guessed words as PINs. You can upload an excluded words dictionary into Authentication Manager. The maximum file size for an excluded words dictionary is 20 MB. A deployment can only have one excluded words dictionary. If a dictionary is already installed, you must delete it before adding a new one. For instructions, see the Security Console Help topic "Add a Password Dictionary."
Character Requirements	Requiring specific characters makes it more difficult to guess the fixed passcode. You can require alphabetic and numeric characters. You can also require a specific number of alphabetic or numeric characters.
Copy Settings from SecurID PIN Lifetime (Fixed Passcode)	Specifies whether you want the fixed passcode lifetime settings to be the same as the SecurID PIN settings, or whether you want to specify different settings.
Copy Settings from SecurID PIN Format (Fixed Passcode)	Specifies whether you want the fixed passcode format settings to be the same as the SecurID PIN settings, or whether you want to specify different settings.

Token Policy Setting	Description
Emergency Access Code Character Requirements	Emergency access tokencodes and passcodes are used to temporarily replace an assigned SecurID token or SecurID PIN if the user does not have access to his token or has forgotten his PIN. Required characters are included in each passcode and tokencode that is generated. You may require the following types of characters: • Numeric • Alphabetic • Special

Add a Token Policy

A token policy determines the lifetime and format of RSA SecurID PINs and fixed passcodes, as well as how to handle users who enter incorrect passcodes.

In a replicated deployment, changes to policies might not be immediately visible on the replica instance. This delay is due to the cache refresh interval. Changes should replicate within 10 minutes. For instructions to make changes take effect sooner on the replica instance, see Flush the Cache on page 369.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Token Policies** > **Add New**.
2. In the **SecurID Token Policy Name** field, enter a unique name with 1 to 128 characters. The characters & % > < ‘ are not allowed.
3. For **Incorrect Passcodes,** specify how the system responds when a user enters an incorrect passcode.

   You can allow users to enter a limited or unlimited number of incorrect passcodes. When the limit is exceeded and followed by a correct passcode, users are prompted to enter the next tokencode that displays on their tokens.

   This setting guards against an unauthorized person attempting to guess a passcode. Even if the person guesses a correct passcode, he or she is prompted for the next tokencode and given only one chance to enter it correctly. If the person enters the next tokencode incorrectly, the user account is locked.
4. For **Default Policy**, select **Set as default SecurID token policy** if you want to designate the new policy as the default policy for the deployment. This security policy is applied to all security domains in the deployment where **SecurID Token Policy** is set to **Always Use Default**. You can override the default policy for each security domain.

5. (Optional) For **Periodic Expiration**, select **Require periodic SecurID PIN changes** if you want to require users to change their SecurID PINs after a specified length of time. If you select this option, specify the following:
    - For **Maximum Lifetime**, specify how often SecurID PINs must be changed.
    - For **Minimum Lifetime**, specify how long users must wait between SecurID PIN changes. This prevents users from bypassing the Restrict Re-use specification by repeatedly changing their SecurID PINs.
6. (Optional) For **Restrict Reuse**, specify the number of recent SecurID PINs a user is restricted from reusing.
7. For **PIN Creation Method**, select the method by which SecurID PINs are generated. You can choose that SecurID PINs be system-generated or allow users to create their own PINs.

    Note: RSA RADIUS does not allow system-generated PINs by default. If you allow system-generated PINs, authentications will fail unless you change the RADIUS configuration file, **securid.ini**, to allow system-generated PINs. For instructions, see the Operations Console Help topic "Edit RADIUS Server Files."

8. For **Minimum Length**, specify the minimum number of characters that a SecurID PIN can contain.
9. For **Maximum Length**, specify the maximum number of characters that a SecurID PIN can contain.
10. (Optional) If you want certain words to be disallowed as PINs, select a dictionary from the **Excluded Words Dictionary** drop-down list.

    For more information on the Excluded Words Dictionary, see the Security Console Help topic "Add a Password Dictionary."
11. For **Character Requirements**, specify whether the SecurID PIN must be numeric or alphanumeric and the minimum number of each character type required for a valid SecurID PIN.
12. Under **Fixed Passcode Lifetime**, do one of the following:
    - Select **Use same settings from SecurID PIN** if you want the fixed passcode and SecurID PIN lifetime settings to be the same.
    - Select **Define separate settings** if you want to specify different lifetime settings for the fixed passcode, and specify the differences.
13. Under **Fixed Passcode Format**, do one of the following:
    - Select **Use same settings from SecurID PIN** if you want the fixed passcode and SecurID PIN format settings to be the same.
    - Select **Define separate settings** if you want to specify different format settings for the fixed passcode, and specify the length, dictionary, and character requirements.
14. Under **Emergency Access Code Format**, specify the types of characters that you want to include in emergency access codes.
15. Click Save.

Offline Authentication Policy

An offline authentication policy defines the way users authenticate when they are not connected to the network.

Offline authentication extends RSA SecurID authentication to users when the connection to RSA Authentication Manager is not available (for example, when users work away from the office or when network conditions make the connection temporarily unavailable).

An offline authentication policy is assigned to each security domain. A deployment can have multiple offline authentication policies.

Two policies can conflict if the user is in one security domain and the agent (their computer) is in a different security domain, and the security domains have different offline authentication policies.

RSA does not recommend offline authentication for the following authenticators:

- PINPad or software tokens
- Tokens that do not require PINs
- Fixed passcodes

These authenticators are likely to contain fewer characters than required by the minimum offline passcode length setting. You can override this setting to explicitly allow offline authentication using these authenticators.

Offline Authentication Policy Settings

The following table describes the password policy settings.

Offline Authentication Policy Setting	Description
Offline Authentication Policy Name	A unique name from 1 to 128 characters.
Offline Authentication	Allows users to authenticate with their tokens when their computer is not connected to the network.

Offline Authentication Policy Setting	Description
Windows Password Integration	Integrates RSA SecurID into the Windows password logon process. Users provide their Windows logon passwords only during initial online authentication. Passwords are then stored with the users’ authentication data in the internal database and, for offline authentication, in the offline data. During subsequent authentications, users enter only their user names and SecurID passcodes. The Authentication Manager gets the Windows password from Authentication Manager and passes it to the Windows logon system. • Enable Windows Password Integration - You enable Windows password integration on the Add Offline Authentication Policy and Edit Offline Authentication Policy pages in the Security Console. • Remove Windows Password Integration - To clear the cached copy of a user’s Windows credential, clear the Windows Password Integration checkbox on the Assigned SecurID Tokens & Authentication Attributes page in the Security Console. When you clear this checkbox, the user must enter his or her Windows password the next time he or she logs on.
Default Policy	An optional field that designates the new policy as the default policy for the deployment. When this option is selected, new security domains use this offline authentication policy.
Notes	A field to record any notes.
Minimum Passcode Length	Adjusts the cryptographic strength of the offline authentication policy. RSA recommends that the minimum passcode length setting be at least twelve characters. For example, if your RSA SecurID tokens display six characters, require users to specify PINs that are at least six characters. To download offline data, the user’s passcode (PIN + tokencode) length must be 8 to 16 characters.

Add an Offline Authentication Policy

An offline authentication policy defines the way users authenticate when they are not connected to the network. In a replicated deployment, changes to policies might not be immediately visible on the replica instance. This delay is due to the cache refresh interval. Changes should replicate within 10 minutes. If you want to make changes take effect sooner on the replica instance, see Flush the Cache on page 369.

Important: Any changes made to an offline policy cause all previously generated offline data to be discarded and regenerated.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Offline Authentication Policies** > **Add New**.
2. In the **Offline Authentication Policy Name** field, enter a unique name from 1 to 128 characters.
3. (Optional) If you want this policy to allow offline authentication, select **Enable Offline Authentication**. This allows users to authenticate with their tokens when their computers are not connected to the network.
4. (Optional) To allow Authentication Manager to automatically provide the user's Windows Login Password with a successful SecurID authentication, select **Enable Windows password integration**.
5. (Optional) If you want this policy to be the default offline authentication policy, select **Set as default offline authentication policy**. The default policy is applied to all new security domains.
6. From the **Minimum Online Passcode Length** drop-down menu, select the minimum length of the passcode (PIN + tokencode) a user must enter to download days of offline data.
7. (Optional) PINPad tokens, software tokens, and tokens that do not require PINs are likely to contain less characters than required by the minimum offline passcode length setting. RSA recommends that you do not allow offline authentication with these types of tokens. You can however, use the **Allow Offline Authentication Using** field to override the minimum length setting for users that authenticate with any of these tokens.
8. (Optional) Select the **Allow offline emergency codes to be generated** checkbox if you want RSA Authentication Manager to generate offline emergency codes for users.
9. Select the type of offline emergency codes that you want to generate:
   - **Offline emergency tokencodes**. Generate these for users who have misplaced their tokens. Users must enter their PIN followed by the emergency tokencode to gain entry to their computers.
   - **Offline emergency passcodes**. Generate these only for users who have forgotten their PINs and need a full passcode. In such cases, make sure you properly identify the users before providing them with emergency passcodes. Because emergency passcodes enable authentication without a PIN, RSA recommends that you use emergency tokencodes instead.
10. In the **Lifetime** field, enter the length of time, in days, for which emergency codes are valid. The default is thirty days.
11. In the **Maximum Days of Offline Data** field, enter the amount, in days, of offline data that you want to allow users to download.

12. In the **Days of Offline Data Warning** field, specify the number of remaining days of offline authentication data that triggers a warning to users. The default is seven days. Users who receive the warning must reconnect to the network and replenish their supply of offline logon days. If users run out of offline logon days, they must contact an administrator.
13. In the **Offline Authentication Failures** field, enter the number of allowable failed offline authentication attempts before users must use an emergency code to gain entry to their computers.
14. (Optional) Select the **Offline Logging** checkbox if you want authentication log entries uploaded to Authentication Manager when the user reconnects to the network.
15. Click **Save**.

Password Policy

A password policy defines users’ password length, format, and frequency of change. You assign password policies to security domains. The policy applies to all users who are assigned to that security domain. Note that user password policies do not apply to Operations Console administrators.

All RSA Authentication Manager users must have a password as part of their user record. If you use the Authentication Manager internal database as your identity source, the password is stored in the internal database.

Password characteristics are controlled by password policies.

Authentication Manager password policies only apply to users in the internal database. When users are stored in an LDAP directory, the directory password policy applies.

When you set up Authentication Manager, a default password policy is automatically created. You can edit this policy, or create a custom password policy and designate it as the default.

One password policy is always designated as the default policy. When you create new security domains, Authentication Manager automatically assigns the default password policy to the new security domains. You can use the default password policy or assign a custom policy to each security domain.

Password policies assigned to upper-level security domains are not inherited by lower-level security domains. For example, if you assign a custom policy to the top-level security domain, all new security domains that you create below it in the hierarchy are still assigned the default password policy.

Enabling system-generated passwords requires users to use passwords generated by Authentication Manager according to the password policy applied to the users’ security domain.

Enabling this option ensures that users’ passwords are random and therefore less likely to be guessed by an unauthorized person attempting to access your network.

When users are initially assigned their password, or when their passwords expire, they are prompted to choose from a list of system-generated passwords when they attempt to use their password.

You need to balance security needs with consideration of what is reasonable to expect from users. Requiring a long password may be counter productive and hard to remember, locking more users out of the network and generating calls to the Help Desk.

Password Policy Settings

The following table describes the password policy settings.

Password Policy Setting	Description
Password Policy Name	A unique name from 1 to 128 characters. The characters & % > < are not allowed in the policy name.
System-Generated Passwords	An optional field that requires users to use only system-generated passwords
Default Policy	An optional field that designates the new policy as the default for the deployment. When this option is selected, new security domains use this password policy.
Notes	Records any notes.
Periodic Expiration	An optional setting to require users to change their password after a specified length of time. This enables the Maximum and Minimum Lifetime fields.
Maximum Lifetime	The maximum amount of time a user can keep a password before being required to change it. For example, suppose this field is set to 90 days. If users change their password on June 1, they must change it again on August 30. Setting this field prevents users from indefinitely keeping the same password, which increases the likelihood that it might be guessed by an unauthorized person trying to access your network.

Password Policy Setting	Description
Minimum Lifetime	The minimum amount of time that a password must exist before the user can change it. For example, suppose the minimum password lifetime is set to 14 days. If users change their passwords on June 15, they cannot change it again until June 29. Setting this field prevents users from circumventing restrictions on the reuse of old passwords that you may have set. For example, suppose you restrict users from reusing their five most recent passwords. This field prevents them from immediately changing their password six times so they can reuse a particular password.
Restrict Re-Use	Prevents users from reusing a small set of passwords. For example, suppose you restrict the last twenty passwords, and the last twenty passwords are “password1,” “password2,” “password3,” up to “password20.” Users cannot enter those twenty passwords. Reusing the same passwords increases the likelihood that an unauthorized person may guess a password, especially if the passwords are all similar, for example, “favoritepet1” or “favoritepet11.” Restrictions force users to move beyond the passwords that they are most comfortable with (for example, a pet’s name or child’s birthday), and choose more secure passwords.
Minimum Length	Prevents users from creating passwords that are too short and easily guessed by an unauthorized person attempting to access your network.
Maximum Length	Prevents users from creating passwords that are too long and difficult for authorized users to remember.
Excluded Characters	You can configure Authentication Manager to exclude up to 50 characters, including a blank space, from use in passwords. The initial password policy excludes @ and ~ by default. You can change the excluded characters for this and any other policy.

Password Policy Setting	Description
Excluded Words Dictionary	A record of words that users cannot use as passwords. It includes commonly used words that are likely to be included as part of any dictionary attacks on the system, for example, "password." The excluded words dictionary prevents users from using common, and therefore, easily guessed words as passwords. You can upload an excluded words dictionary into Authentication Manager. The maximum file size for an excluded words dictionary is 20 MB. A deployment can only have one excluded words dictionary. If a password dictionary is already installed, you must delete it before adding a new one. For instructions to add a password dictionary, see the Security Console Help topic "Add a Password Dictionary."
Character Requirements	Requiring specific characters in passwords can make guessing the password more difficult, particularly when the required characters are not alphanumeric. Dictionary attacks on your system, in which unauthorized users use software to systematically enter all words in a dictionary in an attempt to guess valid passwords, are rendered less effective when passwords contain special characters. For example, the password "maryland" is more likely to be included in a dictionary attack than "mary%land" or "mary**land." You can require the following types of characters: • Alphabetic • Uppercase • Lowercase • Numeric • Special

Add a Password Policy

In a replicated deployment, changes to policies might not be immediately visible on the replica instance. This delay is due to the cache refresh interval. Changes should replicate within 10 minutes. To make changes take effect sooner on the replica instance, see Flush the Cache on page 369.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Password Policies** > **Add New**.
2. Under **Password Policy Basics**, do the following:

   a. In the **Password Policy Name** field, enter a unique name for the new password policy. Do not exceed 128 characters.

   b. (Optional) To require users to use only system-generated passwords, select **Require users to use system-generated passwords**.

   c. (Optional) To designate this policy as the default policy, select **Set as the default password policy**. When this option is selected, new security domains use this password policy.

3. Under **Lifetime**, do one of the following:

   a. Clear the default setting **Require periodic password changes**, and go to step c.

   b. Leave the default setting **Require periodic password changes** selected, and specify the following options:

      – For **Maximum Lifetime**, specify how long a password can be used.

      – For **Minimum Lifetime**, specify how long users must wait before changing a password. Specifying a minimum lifetime prevents users from bypassing re-use restrictions by immediately changing their passwords.

   c. To prevent users from using a password they have used previously, select **Restrict Re-use**. You can specify the number of previous passwords that cannot be used or prevent any previous passwords from being used again.

4. Under **Format**, do the following:

   a. In the **Minimum Length** field, enter the minimum number of characters required in a password. The default is 8.

   b. In the **Maximum Length** field, enter the maximum number of characters allowed in a password. The default is 32.

   c. (Optional) In the **Excluded Characters** field, enter any characters that you do not want to allow users to include in passwords. You can specify up to 50 excluded characters.

   d. From the **Excluded Words Dictionary** drop-down list, select which excluded words dictionary that you want to use. This dictionary contains a list of prohibited passwords.

   e. (Optional) In the **Character Requirements** fields, enter the minimum number of each character type required for a valid password.

5. Click **Save**.

Lockout Policy

A lockout policy defines how many failed logon attempts users can make before Authentication Manager locks their account, and how the account can be unlocked: either automatically or by administrator intervention. You assign lockout policies to security domains. This policy applies to all users assigned to that security domain.

When you set up Authentication Manager, a default lockout policy is automatically created. The default lockout policy locks the user out after five consecutive unsuccessful authentication attempts within one day and requires administrator intervention to unlock a user account. You can edit this policy, or create a custom lockout policy and designate it as the default. You can also assign custom policies to individual security domains

Lockout policies assigned to upper-level security domains are not inherited by lower-level security domains. For example, if you assign a custom policy to the top-level security domain, all new security domains that you create below it in the hierarchy still use the default lockout policy.

Lockout policies apply to all logon attempts regardless of how many different authentication methods a user uses to authenticate. The methods include tokens, fixed passcodes, password-based authentication to the Security Console or Self-Service Console, on-demand tokencodes, and risk-based authentication. For example, if a user has two failures with a software token and one failure with a hardware token, that counts as three failed attempts.

Lockout Policy Settings

The following table describes the lockout policy settings.

Lockout Policy Setting	Description
Lockout Policy Name	A unique name from 1 to 128 characters.
Default Policy	An optional field that designates the new policy as the default policy for the deployment. When this option is selected, new security domains use this lockout policy unless a custom policy is assigned to the security domain.
Notes	A field to record any notes.
Lock User Accounts	Specifies whether you want to allow users unlimited failed authentications, or limit the number of failed authentications before users are locked out. By default, the system locks accounts after five consecutive authentication attempts fail within one day.

Lockout Policy Setting	Description
Unlock	When a user is locked out of the deployment, the lockout policy governs how a user is re-enabled. If the policy is configured to automatically unlock the user account, the locked out user is re-enabled after a specified amount of time elapses. The time is specified in the lockout policy. If the policy is configured so that locked-out users must be unlocked by an administrator, the user remains locked out until an administrator explicitly re-enables the user.

Add a Lockout Policy

In a replicated deployment, changes to policies might not be immediately visible on a replica instance. This delay is due to the fact that policy data is cached for 10 minutes. For instructions on minimizing the delay so that changes take effect sooner on a replica instance, see Flush the Cache on page 369.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Lockout Policies** > **Add New**.
2. In the **Lockout Policy Name** field, enter a unique name for the new lockout policy. Do not exceed 128 characters.
3. (Optional) To make this the default policy for all new security domains, and for any existing security domains already assigned the default policy, select **Default Policy**.
4. In the **Lock User Accounts** field, specify whether you want to allow users unlimited failed authentications, or limit the number of failed authentications allowed before they are locked out. By default, the system locks accounts after five consecutive authentication attempts fail within one day.
5. To limit the number of failed authentications, use the **Unlock** field to specify that you want the system to automatically unlock users after a specified amount of time, or that locked out users must be unlocked by an administrator. The default is **Administrators unlock user accounts**.
6. Click **Save**.

Self-Service Troubleshooting Policy

The self-service troubleshooting feature allows Self-Service Console users to troubleshoot routine authentication problems when they cannot access protected resources using primary methods, such as passwords or passcodes.

The self-service troubleshooting policy defines an alternative form of authentication, such as security questions, used to access the Troubleshooting feature. The policy also specifies the circumstances that lock a user out of the Troubleshooting feature.

You must select one of the following methods to unlock users:

- System automatically unlocks user accounts after a specified amount of time
- Administrators unlock user accounts manually

You can manually unlock a user's account at any time.

You assign these policies to security domains. The policy applies to all users assigned to the security domain.

Self-service troubleshooting policies assigned to upper-level security domains are not inherited by lower-level security domains. For example, if you assign a custom policy to the top-level security domain, all new security domains that you create below it in the hierarchy are still assigned the default self-service troubleshooting policy.

Self-service troubleshooting policies allow you to define secondary authentication methods. A secondary authentication method allows a user to access the Self-Service Console even if the primary authentication method is not working.

Important: Self-service troubleshooting policies only determine the lockout criteria for the self-service troubleshooting feature. To set lockout requirements for the Self-Service Console, Security Console, and resources protected by Authentication Manager, see the Security Console Help topic "Lockout Policy."

Self-service troubleshooting policies apply to all logon attempts regardless of how many different tokens a user uses to authenticate. For example, if a user has two unsuccessful attempts with a software token and one unsuccessful attempt with a hardware token, that counts as three unsuccessful attempts.

Self-Service Troubleshooting Policy Settings

The following table describes the Self-Service troubleshooting policy settings.

Self-Service Troubleshooting Policy Setting	Description
Self-Service Troubleshooting Policy Name	A unique name from 1 to 128 characters.
Default Policy	An optional field that designates the new policy as the default policy for the deployment. When this option is selected, new security domains use this Self-Service troubleshooting policy.

Self-Service Troubleshooting Policy Setting	Description
Notes	A field to record any notes.
Authentication Method	Specifies the mode in which users will authenticate if they have trouble with their primary authentication method. Selecting "Security Questions" requires users to answer security questions upon enrollment or when they first access the Self-Service Security Console.
Lock User Accounts	Controls the number of failed authentication attempts a user is permitted to the Self-Service Console. You can allow an unlimited number of failed attempts, or a specified number of failed attempts within a specified number of days, hours, minutes, or seconds. After the number has been reached, this policy locks the user's account.
Unlock	When a user is locked out of the Self-Service Console, the lockout policy governs how a user is re-enabled. If the policy is configured to automatically unlock the user account, the locked out user is re-enabled after a specified amount of time elapses. If the policy is configured so that locked-out users must be unlocked by an administrator, the user remains locked out until an administrator explicitly re-enables the user.

Add a Self-Service Troubleshooting Policy

In a replicated deployment, changes to policies might not be immediately visible on the replica instance. This delay is due to the cache refresh interval. Changes should replicate within 10 minutes. For instructions to make changes take effect sooner on the replica instance, see Flush the Cache on page 369.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Self-Service Troubleshooting Policies** > **Add New**.
2. In the **Self-Service Troubleshooting Policy Name** field, enter the policy name. Use a unique name, and do not exceed 128 characters.
3. (Optional) To designate the new policy as the default policy for the system, select **Default Policy**. When this option is selected, new security domains use this policy.
4. (Optional) Select the **Authentication Method** with which users authenticate if they cannot use their primary authentication method.

5. The **Lock User Accounts** field controls the number of unsuccessful authentication attempts a user is permitted to make to the Self-Service Troubleshooting feature. You can allow an unlimited number of unsuccessful attempts, or a specified number of unsuccessful attempts within a specified number of days, hours, minutes, or seconds. After the number has been reached, this policy locks the user's account out of the troubleshooting feature.
6. In the **Unlock** field, you can either require administrators to unlock accounts after users have exceeded the limit specified in the **Lock User Accounts** field, or you can allow the system to automatically unlock accounts after a specified number of days, hours, minutes, or seconds.
7. Click **Save**.

Risk-Based Authentication Policies

To use RBA in your deployment, you must create an RBA policy, or edit the default policy, and associate the policy with a security domain. A policy can be associated with multiple security domains. For more information, see Add a Risk-Based Authentication Policy on page 95.

Risk-Based Authentication (RBA) Policy Settings

You use the Security Console to define a risk-based authentication (RBA) policy for a security domain. An RBA policy includes the following settings.

Risk-Based Authentication Policy Setting	Description
RBA Policy Name	A unique name from 1 to 128 characters.
Default Policy	Sets the default RBA policy for the deployment.
Notes	A field to record any notes.
Automatic Enablement	Determines whether the system automatically enables users for RBA during the first successful authentication to an RBA-protected resource.
Minimum Assurance Level	The confidence threshold that each authentication attempt must meet to avoid being challenged for identity confirmation. **Note:** If you increase the minimum assurance level, the system provides greater identity assurance, but users are more likely to be prompted for identity confirmation.

Risk-Based Authentication Policy Setting	Description
Silent Collection Period	Allows the system to establish a baseline authentication history for RBA users during a specified period of time. During silent collection, the system registers the users authentication device automatically, and does not require the user to use an identity confirmation method.
Identity Confirmation Methods	Methods that can be used to provide identity confirmation during logon.
New Device Registration	Determines the system response to unregistered authentication devices.
Total Registered Devices	Maximum number of registered devices preserved in each user's device history. If the number of registered devices exceeds the limit, the nightly cleanup job deletes the least recently used devices.
Unregister Devices	Length of time an inactive authentication device remains in the user device history.

Add a Risk-Based Authentication Policy

Risk-based authentication (RBA) is a multifactor authentication solution that strengthens traditional password-based systems by applying knowledge of the client device and user behavior to assess the potential risk of an authentication request. The RBA policy determines how RBA works in each security domain.

In a replicated deployment, changes to policies might not be immediately visible on the replica instance. This delay is due to the cache refresh interval. Changes should replicate within 10 minutes. To make changes take effect sooner on the replica instance, see Flush the Cache on page 369.

Before You Begin

Understand the concept of minimum assurance level. For more information, see Minimum Assurance Level on page 270.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Risk-Based Authentication Policies** > **Add New**.
2. Under **RBA Policy Basics**, do the following:
   a. In the **RBA Policy Name** field, enter a unique policy name. Do not exceed 128 characters.
   b. (Optional) If you want to make this the default RBA policy for the deployment, select **Set as default RBA policy**.
   c. (Optional) Add any notes in the **Notes** field.

3. Under **Enablement and Assurance Settings**, do the following:

   a. (Optional) If you want to automatically enable users for RBA after successful authentication, select **Allow system to enable users for RBA automatically during authentication** in the **Automatic Enablement** field.

   b. In the **Minimum Assurance Level** field, select the assurance level that is required to authenticate without prompting for identity confirmation. The system determines the assurance level of each authentication attempt based on the user's profile, authentication device, and authentication history. The higher the level, the greater the chance that the user will be prompted for identity confirmation. The default setting is **Medium**.

   Note: Changing this setting may affect how often users are prompted to confirm their identity.

4. Under **Device Registration and Identity Confirmation Settings**, do the following:

   a. For **Silent Collection Period**, do one of the following:

      - To enable silent collection, select **Allow silent collection**. Enter the number of days to enable silent collection for each user.
      - To disable silent collection, select **Do not allow silent collection**. This is the default setting.

   b. For **Identity Confirmation Methods**, select the methods to make available to users if an authentication request does not meet the minimum assurance level. You must select at least one method. If you select two methods, the user chooses which method to use.

   c. For **New Device Registration**, select one of the following to register a user's device.

      - To add a device automatically, select **Register the user authentication device automatically after successful authentication**.
      - To allow the user to choose whether to add a device to the device history, select **Prompt the user to choose whether the system registers the device after successful authentication**. This is the default setting.

   Important: Select this option if users will access RBA-protected resources from shared or public computers.

5. Under **Device Administration Settings**, do the following:

   a. In the **Total Registered Devices** field, enter the maximum number of registered devices preserved in each user's device history. If the number of registered devices exceeds the limit, the nightly cleanup job deletes the least recently used devices.

   b. In the **Unregister Devices** field, enter the number of consecutive days that a device can remain inactive before the system removes it from the user device history.

6. Click **Save**.

Risk-Based Authentication Message Policy

The risk-based authentication (RBA) message policy defines the message that users see when they are prompted to configure their identity confirmation method. You might use this message to inform users about why they need to configure an identity confirmation method. This message displays when all of the following conditions exist:

- The user authenticates to a web-based application, such as an SSL-VPN, thin client, or web portal.
- The user has not configured an identity confirmation method.
- The user attempts to authenticate using a high assurance device.

You can assign an RBA message policy to any security domain. A deployment can have multiple RBA message policies, which you assign by editing the security domain. Security domains use the deployment's default RBA message policy until you assign a different RBA message policy.

Risk-Based Authentication Message Policy Settings

The following table describes the risk-based authentication (RBA) message policy settings.

Setting	Description
RBA Message Policy Name	A unique name from 1 to 128 characters.
Default Policy	An optional field that designates the new policy as the default policy for the deployment. When selected, new security domains use this RBA message policy.
Notes	A field to record any notes.
Message text	Customized message for your company policies or business needs.

Add a Risk-Based Authentication Message Policy

The risk-based authentication (RBA) message policy defines the message that users see when they are prompted to configure their identity confirmation method. You can create multiple RBA message policies, for example, one for each security domain. This policy applies to all users in the security domain.

In a replicated deployment, changes to policies might not be immediately visible on the replica instance. This delay is due to the cache refresh interval. Changes should replicate within 10 minutes. To make changes take effect sooner on the replica instance, see Flush the Cache on page 369.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **RBA Message Policies** > **Add New**.
2. Under **RBA Message Policy Basics**, do the following:
   a. In the **RBA Message Policy Name** field, enter a unique name that does not exceed 128 characters.
   b. (Optional) To set this policy as the default policy, select **Set as the default RBA Message Policy**.
   c. (Optional) In the **Notes** field, enter any notes.
3. Under **Message Confirmation**, review the message in the **Message Text** field, and customize the message if necessary.
4. Click **Save**.

5 Integrating LDAP Directories

Identity Sources

An identity source is a repository that contains user and user group data. Each user and user group in a deployment is associated with an identity source.

Authentication Manager supports the following as identity sources:

- An LDAP directory

  Authentication Manager supports the following directories as identity sources:

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

  In Active Directory, you can add a Global Catalog as an identity source, which is used to look up users and resolve group membership during authentications. You cannot use a Global Catalog identity source to perform administrative tasks.

- The Authentication Manager internal database

Data from an LDAP Directory

Authentication Manager has read-only access to all LDAP directory identity sources. After a directory is integrated with Authentication Manager, you can use the Security Console to do the following:

- View (but not add or modify) user and user group data that resides in the directory.
- Perform Authentication Manager administrative tasks. For example, enable or disable the use of on-demand authentication (ODA) and risk-based authentication (RBA), or assign tokens or user aliases to individual users who reside in the directory.

You must use the LDAP directory native user interface to modify data in a directory.

Data from the Internal Database

Authentication Manager provides an internal database where you can create users and user groups. For users and user groups in the internal database, administrators can use the Security Console to do the following:

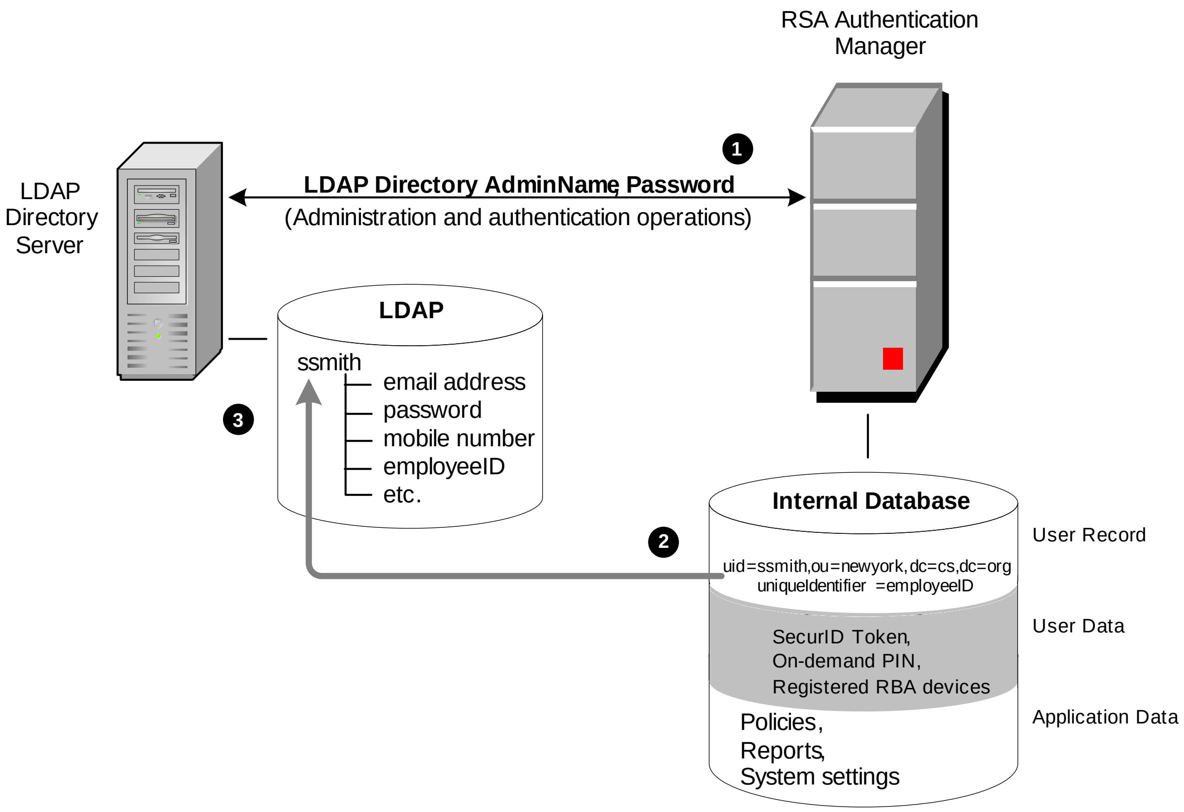
- Add, modify, and view user and user group data.
- Enable or disable Authentication Manager functions, such as ODA and RBA, for individual users, including users whose accounts are in an LDAP directory.

The following information is stored only in the internal database:

- Data that is specific to Authentication Manager, such as policies for administrative roles, and records for authentication agents and SecurID authenticators
- Data that links Authentication Manager with LDAP directory user and user group records

Identity Source Data Flow

The following figure shows how data elements (LDAP attributes and Authentication Manager attributes) may be distributed across external identity sources and the internal database. The figure also shows connections between Authentication Manager and LDAP external identity sources.



1. Authentication Manager communicates with the LDAP directory by using the LDAP administrator user name and password.

   If the administrator account is set to read/write access, end users may update their own passwords, responding directly to password renewal prompts received through Authentication Manager. If access is read-only, the users must contact their administrator for password updates.

2. The internal database contains a reference to every user's distinguished name and unique identifier to locate user records in the LDAP directory. It also contains user attributes defining properties that are specific to Authentication Manager, such as an on-demand PIN, security questions, and a user account enabled or disabled parameter.
3. Your directory servers may already contain typical LDAP user records and attributes. Authentication Manager can work with more than one directory server.

Identity Source Properties

You specify identity source properties when you add or edit an identity source. The Operations Console organizes the identity source properties in categories.

- Identity Source Basics
- Directory Connection - Primary and Replica
- Directory Settings
- Active Directory Options
- Directory Configuration - User Tracking Attributes
- Directory Configuration - Users
- Directory Configuration - User Groups

Identity Source Basics

Identity Source Name. Unique name for the identity source. This name is displayed in the Security Console to identify the identity source.

Type. The type of identity source. For example, an LDAP identity source type can be Microsoft Active Directory, Sun Java System Directory Server, or Oracle Directory Server. After an identity source is added to the deployment, you cannot change the identity source type. For the supported list of identity sources, see the Operations Console Help topic "View the Identity Sources in Your Deployment."

Notes. You can use up to 255 characters of text to add a note about the identity source.

Directory Connection - Primary and Replica

Directory URL. The URL of the new identity source. If you use the standard SSL-LDAP port 636, specify the value as ldaps://*hostname*/. For all other ports, you must specify the port number, for example, ldaps://*hostname:port*/. An SSL connection is required for password management.

For Active Directory, the Global Catalog can have the same directory URL as a another identity source that is not a Global Catalog.

Directory Failover URL. (Optional) The failover directory server is used if the connection with the primary directory server fails. The failover directory server must be a mirror of the primary directory server.

If you want to permit users to change their passwords during authentication, the LDAP directory administrator account must have write privilege for user records in the identity source. If you do not permit password changes, the directory administrator account does not need write privileges.

Directory User ID. The LDAP directory administrator's User ID.

For example, you might enter cn=Administrator,cn=Users,dc=domain,dc=com or Administrator@domain.com.

Directory Password. The LDAP directory administrator's password.

Make sure that this password is kept up-to-date. If this password expires, the connection fails.

Directory Settings

Use directory settings to narrow the scope of an identity source so that only a subset of the identity source is used. For more information, see Identity Source Scope Change Requirements on page 106.

If you narrow the scope of an identity source, you must schedule a cleanup job to remove references to unresolvable users and user groups from the internal database. For more information, see Schedule a Cleanup Job on page 149.

User Base DN. The base DN for directory user definitions. For example, for Active Directory, you might enter cn=Users, dc=domainName, dc=com.

User Group Base DN. The base DN for directory user group definitions. For example, for Active Directory, you might enter ou=Groups, dc=domain, dc=com.

It is important to follow these practices:

- Do not configure multiple identity sources with overlapping scope. If you have multiple identity sources that point to the same User Base DN or User Group Base DN, ensure that the User Search Filter and User Group Search Filter are configured so that each user and user group appears only in one identity source. Improper configuration may result in unresolvable users and authentication problems.
- If an attribute value contains a comma or an equal sign, you must escape these characters with a backslash. For example, if the attribute ou has the value of A=B, Inc, you must write this out as ou=A\=B\, Inc. If you do not escape these characters in an attribute value, the connection to the identity source fails. This only applies to commas or equal signs used in an attribute value. Do not escape commas separating elements of a distinguished name, for example, cn=Joe Smith, ou=Sales, or equal signs between a moniker and its attribute value, for example, ou=Sales.
- The default organizational unit “Groups” does not exist in the default Active Directory installation. Make sure you specify a valid container for the **User Group Base DN**.

Search Results Time-out. Limits how long a search will continue. If searches for users or groups are timing out on the directory server, either extend this time, or narrow individual search results. For example, instead of Last Name = *, use Last Name = G*.

User Account Enabled State. Specify where Authentication Manager looks for the enabled/disabled state of user accounts.

- Select **Directory** to look in the external identity source only.

  If the user account is disabled in the external identity source, the user cannot authenticate. The ability of the user to authenticate is based solely on the User Account Enabled State in the external identity source.

- Select **Directory and Internal Database** to look in the internal database in addition to the external identity source.

  The user account must be enabled in both the internal database and the external identity source for the user to authenticate. If the user account is disabled in either the internal database or the external identity source, the user cannot authenticate.

Validate Map Against Schema. Validates identity attribute definition mappings to the directory schema when identity attribute definitions are created or modified.

Active Directory Options

Global Catalog. Select this if the identity source is an Active Directory Global Catalog.

User Authentication. Select one of the following as the source for user authentication:

- **Authenticate users to this identity source.** Select this option if the identity source is not associated with a Global Catalog. If no Global Catalogs are configured as identity sources, this option is selected automatically.
- **Authenticate users to a global catalog.** Select this option if the identity source is associated with a Global Catalog, and select a Global Catalog from the drop-down menu.

Directory Configuration - User Tracking Attributes

User ID. Select one of the following to map the User ID:

- **Maps to.** Select this option to map the User ID to a specified attribute.
- **Uses the same mapping as E-mail.** Select this option to map the User ID to the e-mail attribute. If you choose this option, the User ID and e-mail fields have the same value. The e-mail attribute must already be defined in the directory.

When you change the User ID mapping, make sure that the new field is unique for all users and does not overlap with the old field. This prevents administrative data from being associated with the wrong user records for some users. For example, if the old mapping has the User ID “jdoe,” the new mapping should not contain the User ID “jdoe.” To ensure a smooth transition from the old User ID mapping to the new, you need to clean up unresolvable users to update the internal user records with the new User IDs. Perform this task immediately after you change the mapping. For instructions, see the *Administrator's Guide*.

Unique Identifier. A unique identifier to help the Security Console find users whose DNs have changed. For Active Directory, the default is ObjectGUID. For Oracle Directory Server (or Sun Java Directory Server), the default value is nsUniqueID.

You must specify the Unique Identifier before you move or rename LDAP directory users who are viewed or managed through the Security Console. Otherwise, the system creates a duplicate record for the users that you move or rename, and disassociates them from data the system has stored for them.

Enter an attribute from your directory that meets these requirements:

- The attribute must contain unique data for each user. For example, an employee ID number or badge number that is unique for each user in the deployment.
- The attribute must contain data for each user. The value cannot be empty.
- The attribute value cannot change. If the value for a user changes, Authentication Manager cannot track the user. You cannot map any other fields to the attribute that you map to the Unique Identifier.
- The attribute name can contain up to 64 characters.
- The attribute value can contain up to 42 characters.

Note: RSA does not recommend using the default value if you are using third-party directory management tools that handle moving users from one DN to another by deleting the users and adding them back to the directory.

Directory Configuration - Users

First Name. The directory attribute that maps to the first name attribute. By default, First Name maps to “givenName.”

Middle Name. The directory attribute that maps to the middle name attribute. By default, Middle Name maps to “initials.”

Last Name. The directory attribute that maps to the last name attribute. By default, Last Name maps to “sn.”

E-mail. The directory attribute that maps to the e-mail attribute. By default, E-mail maps to “mail.”

Certificate DN. Reserved for future use. By default, it is mapped to “comment.” Do not map certificate to critical fields, such as “cn” or “sAMAccountName.”

Password. The directory attribute that maps to the password attribute. By default, Password maps to “unicodePwd.”

Search Filter. The filter that specifies how user entries are distinguished in the LDAP directory, such as a filter on the user object class. Any valid LDAP filter for user entries is allowed, for example, (objectclass=inetOrgPerson).

Search Scope. The scope of user searches in the LDAP tree.

Object Classes. The object class of users in the identity source that are managed using the Security Console, for example, user,organizationalPerson,person.

Directory Configuration - User Groups

User Group Name. The directory attribute that maps to the user group name attribute. For example, the User Group Name might map to cn.

Search Filter. An LDAP filter that returns only group entries, such as a filter on the user group object class, for example, (objectclass=group).

Search Scope. The scope of user group searches in the LDAP tree.

Object Classes. The object class of user groups that are created or updated using the Security Console.

Membership Attribute. The attribute that contains the DNs of all the users and user groups that are members of a user group.

User MemberOf Attribute. Enables the system to resolve membership queries by using the value specified for the MemberOf attribute.

MemberOf Attribute. The attribute of users and user groups that contains the DNs of the user groups to which they belong.

Identity Source Scope

Identity source scope determines the subset of users and user groups in your LDAP directory that can be managed within the identity source.

Identity Source Scope Settings

When you add an identity source, you determine its scope, including the base DNs, the search filters, and the search scope (single level vs. all levels).

Setting	Description
User Base DN	Directory location where Authentication Manager searches for users.
User Group Base DN	Location in your LDAP directory where Authentication Manager searches for groups.
User Search Filter and User Group Search Filter	An LDAP filter that returns only user or group entries, such as a filter on the user group object class, for example, (objectclass=groupOfUniqueNames).
User Search Scope and Group Search Scope	Scope of user and user group searches in the LDAP tree.
User Object Classes and Group Object Classes	Object class of users and user groups that are accessed by Authentication Manager. Any custom attributes that are used in the mapping fields must be part of one of the object classes. For more information, see Custom Attribute Mapping on page 116.

Important: Do not configure multiple identity sources with overlapping scope. If you have multiple identity sources that point to the same User Base DN or User Group Base DN, verify that you correctly configured the User Search Filter and User Group Search Filter to include each user in only one identity source. Improper configuration may result in unresolvable users and authentication problems.

Identity Source Scope Change Requirements

You can make the scope of an identity source broader or narrower. If you narrow the scope of an identity source, some users and user groups may become unresolvable and unable to authenticate. Unresolvable users are users that Authentication Manager can no longer find in the LDAP directory that was designated as their identity source.

After you narrow the scope you need to run the scheduled cleanup job to delete references to unresolvable users and user groups from the internal database. For instructions, see Scheduling Cleanup for Unresolvable Users and User Groups on page 148.

When you run the scheduled cleanup job, you need to disable the Grace Period, the Cleanup Limit, or both if they are set, and re-enable those settings after this single cleanup runs.

Note: You do not need to perform a scheduled cleanup after broadening the scope of the identity source.

Active Directory Identity Sources that are Not Global Catalogs

In Active Directory, identity sources that are not Global Catalogs are used for administrative operations, such as enabling users for on-demand authentication and risk-based authentication. If you are not using a Global Catalog, this type of identity source is also used for finding and authenticating users. This type of identity source also maps to a domain controller.

If you want to administer Active Directory domain users in Authentication Manager, you must add an identity source for each domain that contains users who will authenticate with Authentication Manager.

For example, if an Active Directory forest has three domains and one Global Catalog, and you want to authenticate users in two of the domains, you must add an identity source for each of the two domains.

Important: Authentication Manager supports up to 30 identity sources that are not Global Catalogs per deployment. This limit does not include using the internal database as an identity source.

An identity source that is not a Global Catalog can use group membership data from all three types of Active Directory security groups: Universal Security, Global, and Domain Local. Authentication Manager does not support distribution groups of any kind for restricted agent access.

Support for Group-to-Group Membership in Active Directory

To support group-to-group membership in Active Directory, you must set the domain functional level to Windows 2003 or 2008. For more information about how to raise the domain functional level, go to **http://support.microsoft.com/kb/322692**.

Note: The default organizational unit "Groups" does not exist in the default Active Directory installation. Make sure you specify a valid container for the User Group Base DN when adding the identity source.

Active Directory Global Catalog Identity Sources

If you have an Active Directory forest, and you configure multiple identity sources within it, you can optionally configure an Active Directory Global Catalog as an identity source that the other Active Directory identity sources can use for finding and authenticating users, and resolving group membership within the forest. You need to:

- Add each Global Catalog to Authentication Manager as a separate identity source.
- Map the identity source to the Global Catalog port on the domain controller that hosts the Global Catalog.

RSA Authentication Manager does not use Global Catalogs for administrative operations, such as changing users' passwords. Administrative actions are only performed against non-Global Catalog identity sources.

Deployment Requirements for Global Catalogs

These requirements apply only to deployments that use restricted authentication agents.

To use a Global Catalog as an identity source, your deployment must meet all of the following requirements:

- All groups granted access to a restricted authentication agent must be Windows Universal Security groups.
- When you view the Active Directory groups from the Security Console, all types of groups (Universal Security, Domain Local, and Global) are displayed, but only Universal Security groups may be successfully used with restricted agents through a Global Catalog.
- All domains in the forest must run Windows 2008 R2.

Only the Windows administrator can change the group type in Active Directory.

Important: If you select a group from the list of Active Directory groups in order to activate users on restricted agents, make sure you select a Universal Security group. If you use any other type of group, the user cannot authenticate.

Data Replication for Global Catalogs

When you use the Active Directory Global Catalog as an identity source, individual Active Directory domain controllers replicate domain changes to the Global Catalog. For this type of deployment, you must integrate the following with Authentication Manager:

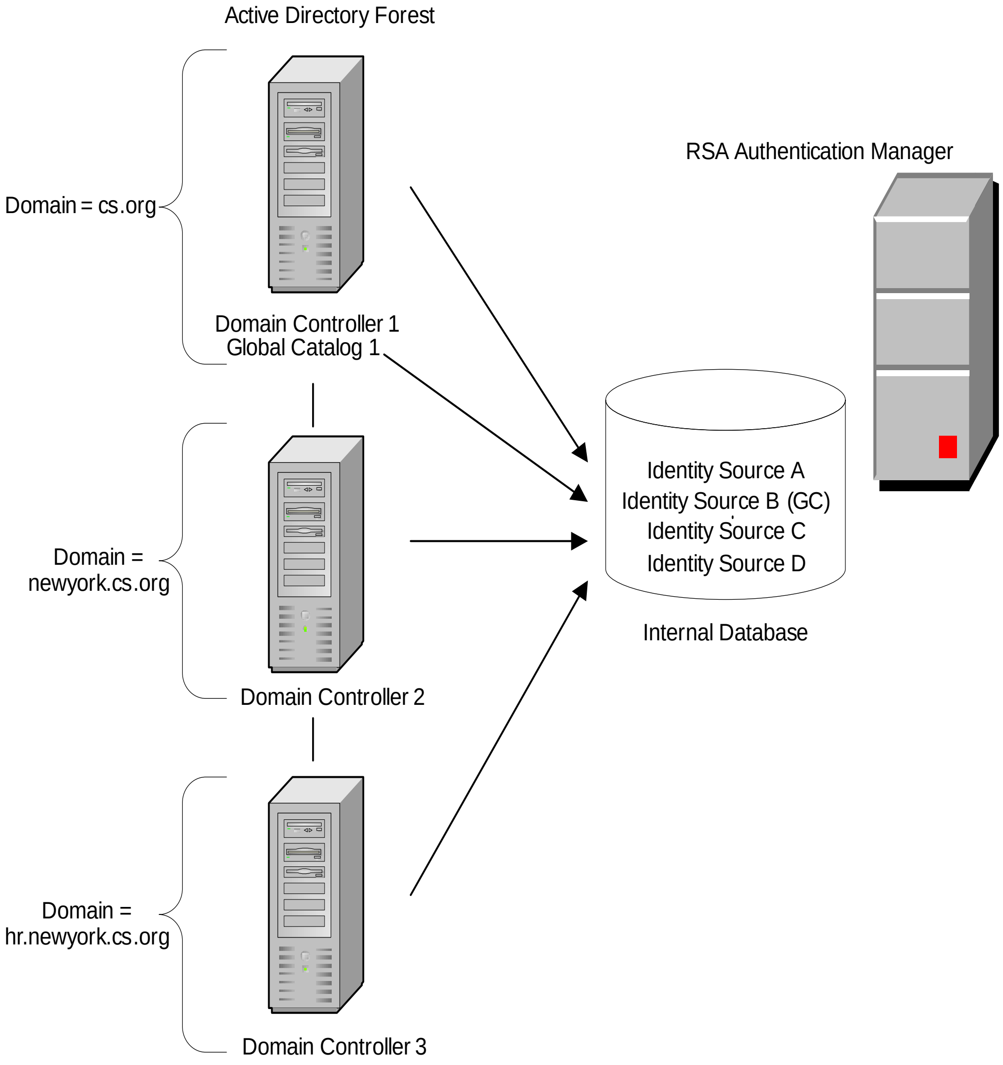
- The Global Catalog. If your forest has more than one Global Catalog, you can use one for failover. You do not need to create an identity source for the second Global Catalog. Instead, you can specify it as a failover URL when you create the identity source for the first Global Catalog.
- All domain controllers that contain users and user groups that you want to reference from Authentication Manager. Add each domain as an identity source.

For example, suppose that GC1 is the Global Catalog identity source for user authentication, and AD1, AD2, and AD3 replicate a subset of their data to GC1. You must map each Active Directory to an identity source. After integration is complete, Authentication Manager accesses GC1 for authentication requests and AD1, AD2, and AD3 for administration, such as updating the user password.

Global Catalog Deployment Example with Four Identity Sources

The following figure shows a forest composed of three domains, each consisting of one domain controller, and a single Global Catalog. In this example, you must enable at least four identity sources in Authentication Manager.

- Three identity sources for domain controllers, possibly with failover domain controllers
- One identity source for a Global Catalog, possibly with a failover Global Catalog server



Configure the Active Directory Connection Time-Out

In some situations, the default LDAP connection time-out is not long enough for Authentication Manager to establish a connection to the LDAP directory. If you need to adjust the length of time that Authentication Manager waits to establish the connection, use the Operations Console to edit the identity source and change the value in the **Search Results Time-out** field.

Integrating an LDAP Directory as an Identity Source

You can integrate LDAP directory servers as identity sources in Authentication Manager without modifying the directory schema. You perform the integration by adding identity sources, linking the identity source to Authentication Manager, and mapping identity attribute definitions to attribute names in the LDAP directory.

Follow these guidelines:

- You must have LDAP connection information and detailed knowledge of your LDAP schema.
- You must configure an identity source for each directory that contains users who will authenticate with Authentication Manager.
- The primary and replica instances should not use the same directory server for regular use, but they may share the same failover directory server. If both instances use the same directory server, a system or network outage for those systems may cause authentication to fail.
- If you have not configured a replica instance, but plan to in the future, you need to update the replica instance identity source connection information after you configure the replica instance.

The following high-level steps describe how to integrate an LDAP directory server as an identity source:

1. Set up SSL connections using the Operations Console. See Identity Source SSL Certificates on page 114. This step is required if you allow users to change their passwords from Authentication Manager.
2. (Optional) Review your password policy, and make adjustments if necessary. See Password Policy for Active Directory on page 116. This step is required only if you allow users to change their passwords from Authentication Manager.
3. If the directory server is Active Directory, verify if your domain functional level supports group-to-group membership. Check the System control panel on the domain controller, and see Support for Group-to-Group Membership in Active Directory on page 106.
4. Verify that the directory server hostname is a valid DNS name. Make sure:
   - The hostname is resolvable for both forward and reverse lookups.
   - The directory server can be reached from the Authentication Manager server.

5. Add the identity source, using the Operations Console. Make sure you configure the following:
   - The identity source name
   - The LDAP connection, including the directory URL, backup directory URL, directory User ID, and directory password
   - Attribute mapping
   - (Optional) Global Catalog (Active Directory only)
6. (Optional) You can define custom user attributes that are specific to your organization. For instructions, see the Security Console Help topic “Add Identity Attribute Definitions.”

   (Optional) Map the custom attributes that you previously defined from the LDAP directory to the identity source. If you choose to map custom attributes to the external identity source, Authentication Manager can read the attribute values from your directory.

   For instructions, see Custom Attribute Mapping on page 116.
7. Use the Security Console to link the identity source to the system. See Link an Identity Source to the System on page 112.
8. Verify that the identity source was added successfully. See “Verify the LDAP Directory Identity Source” on page 112.

Note: To disable or delete an identity source, it must be unlinked from the system. For instructions, see the Security Console Help topic “Unlink Identity Sources from the System.” For instructions about deleting the identity source, see the Operations Console Help topic “Remove an Identity Source.”

Add an Identity Source

To use an existing LDAP directory with RSA Authentication Manager, use the Operations Console to add the directory as a new identity source.

A deployment can have up to thirty identity sources. If you are using Active Directory, Global Catalogs configured as identity sources do not count against this limit.

Before You Begin

- You must be a Super Admin.
- For full functionality, establish an SSL connection between Authentication Manager and the identity source.

Note: Depending on the network or firewall configuration, you might not be able to validate the connection information from the primary server.

Procedure

1. Log on to the Operations Console on the primary instance.
2. Click **Deployment Configuration** > **Identity Sources** > **Add New**.

3. When prompted, enter your Super Admin User ID and password.
4. In the **Identity Source Basics** section, specify:
   - **Identity Source Name**. The name of the identity source that is displayed in the Security Console.
   - **Type**. The type of the identity source that you are adding.
   - **Notes.** Information about the identity source.
5. In the **Directory Connection - Primary** section, do the following:
   - Enter the requested information in the following fields. For detailed information, see Identity Source Properties on page 101.
     - **Directory URL**
     - **Directory Failover URL**
     - **Directory User ID**
     - **Directory Password**
   - Click **Test Connection** to ensure that the primary instance can connect to the specified directory. If the test fails, make sure that you have correctly imported the certificate for this identity source.
6. If you have a replica instance, complete the fields in the **Directory Connection - Replica** section, and click **Validate Connection Information** to verify that the primary instance can connect to the identity source. If the attempt fails, do the following:

   a. Verify that you entered the correct settings.

   b. If the settings are correct, make sure the primary instance is able to connect to the identity source.

   c. If the primary instance is able to connect to the identity source, make sure no other network issues are causing the connection failure.

   d. After you make any necessary changes, click **Validate Connection Information** again.
7. Click **Next**.
8. Provide the requested information for each of the following sections on the Add Identity Source - Map page. For detailed information, see Identity Source Properties on page 101.
   - **Directory Settings**
   - (Optional) **Active Directory Options**
   - **Directory Configuration - User Tracking Attributes**
   - **Directory Configuration - Users**
   - **Directory Configuration - Users Groups**
9. Click **Save**.

Link an Identity Source to the System

You must link all LDAP directory identity sources to the system. After linking, all users in the identity source can be viewed and managed through the Security Console. Users are visible in the top-level security domain by default, but you can move them to other security domains as necessary. Additionally, you can configure the system to place users from the identity source into a specific security domain automatically. For more information, see Default Security Domain Mappings on page 43.

Before You Begin

- You must be a Super Admin.
- If you link an Active Directory Global Catalog, you must also link each identity source that replicates user data to that Global Catalog. For example, if identity sources IS1 and IS2 replicate information to Global Catalog GC1, and you link GC1 as an identity source, you must also link IS1 and IS2 to the system.

Procedure

1. Log on to the Security Console as Super Admin.
2. Click **Setup** > **Identity Sources** > **Link Identity Source to System**.
3. From the list of available identity sources, select the identity sources that you want to link, and click the right arrow.
4. Click **Save**.

Verify the LDAP Directory Identity Source

To verify that you have successfully added and linked an identity source, you can view the users and groups from that identity source through the Security Console.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the appropriate identity source, and click **Search**.
3. View the list of users from the LDAP directory identity source.

Failover Servers

You can specify failover directory servers when you use the Operations Console to add an identity source. If the primary directory server stops responding, the deployment automatically connects to the failover server.

Follow these guidelines when configuring a failover directory server:

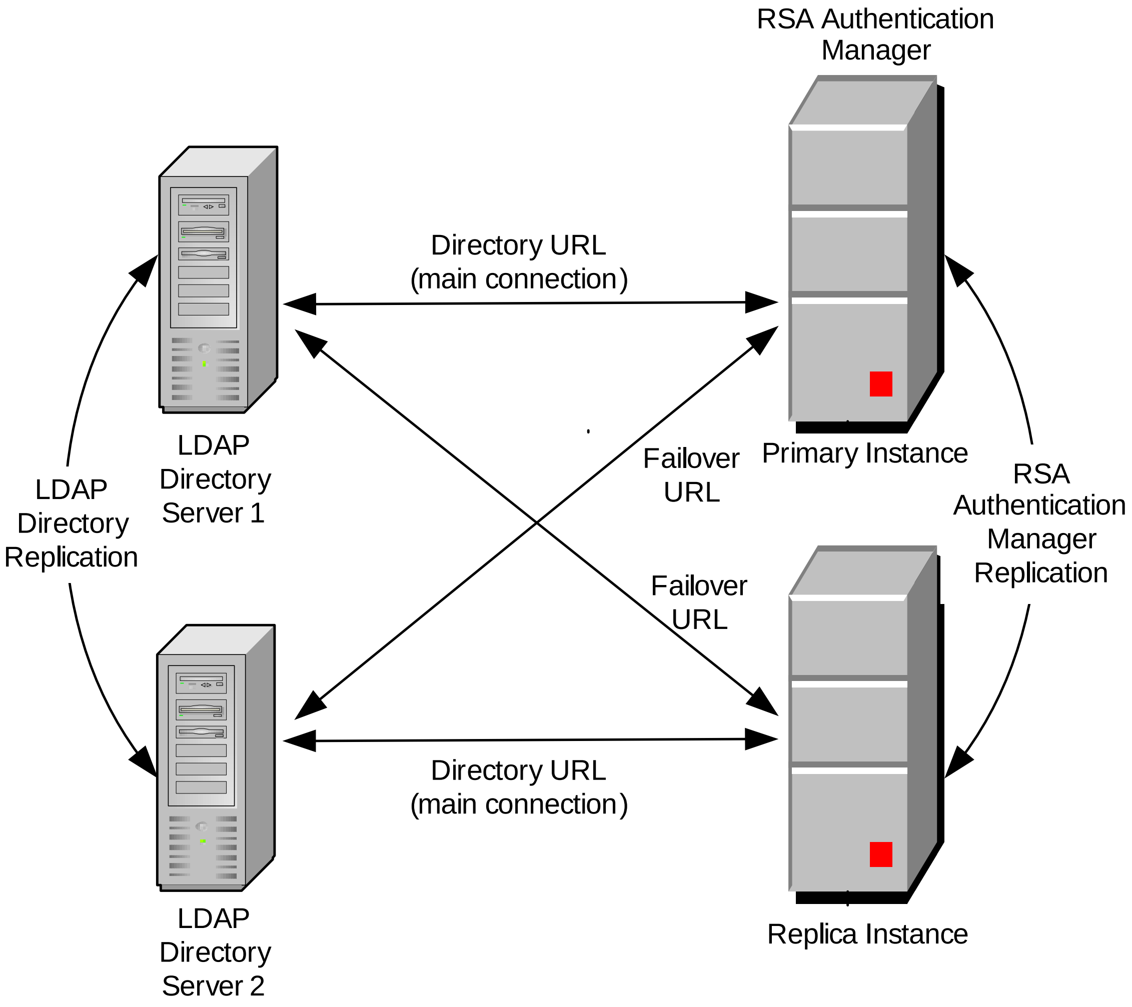
- Provide the failover URL in the Directory Failover URL field when you add an identity source. For instructions, see Custom Attribute Mapping on page 116.
- The failover directory server must be a replica of the primary directory server.
- The primary and replica instances should not use the same physical server. If no failover is provided and both servers use the same domain server, users cannot authenticate if that domain server becomes unavailable.
- Each failover URL should point to a different physical directory server.

Failover Active Directory Servers

For an Active Directory identity source, the failover server should not be a Global Catalog.

Deployment Example with Failover Directory Servers

The following example configuration eliminates any single-point-of-failure if one of the two available directory servers become unavailable. In this case, each directory server is in the same domain and provides a replicated copy of the same LDAP data.


RSA Authentication Manager
Directory URL (main connection)
LDAP Directory Server 1
LDAP Directory Replication
Failover URL
Primary Instance
RSA Authentication Manager Replication
Failover URL
Directory URL (main connection)
LDAP Directory Server 2
Replica Instance

Securing the Communications Path

RSA recommends that you use Secure Sockets Layer (SSL) to encrypt data in transit between Authentication Manager and the directory.

You must configure SSL for each directory server you plan to use with Authentication Manager. For more information, see Identity Source SSL Certificates on page 114.

For Active Directory there are additional considerations for password policies and group membership support. For more information, see Password Policy for Active Directory on page 116 and Support for Group-to-Group Membership in Active Directory on page 106.

Identity Source SSL Certificates

When you integrate an LDAP directory server as an identity source, use an identity source secure sockets layer (SSL) certificate to establish secure communication between the deployment and the external identity sources. Set up SSL connections using the Operations Console. Setting up an SSL connection also enables you to allow users to change their passwords from Authentication Manager.

When establishing an SSL connection, the identity source presents a certificate that identifies the server (for example, using the hostname). To accept the server certificate, either the certificate itself or its root certificate must be trusted by the deployment. For an SSL certificate to be trusted, you must add it to the deployment.

Add an Identity Source SSL Certificate

A secure sockets layer (SSL) certificate establishes secure communication between the deployment and the identity sources. You must add the identity source SSL certificate to the deployment as a trusted certificate.

Use the following procedure to add the identity source SSL certificate as a trusted certificate.

Before You Begin

You must be a Super Admin.

Procedure

1. Import the SSL server certificate or the CA root certificate to the primary appliance. The certificate must be in Distinguished Encoding Rules (.der) encoded format. Make sure you have access to these certificates.
2. Log on to the Operations Console on the primary instance.
3. Click **Deployment Configuration** > **Identity Sources** > **Identity Source Certificates** > **Add New**.
4. If prompted, enter your Super Admin User ID and password.
5. Enter a name for the new identity source certificate.

6. Browse to the directory where the SSL certificate is located. Certificates typically have .cer, .pem, or .der file extensions.
7. Click **Save**.

Access to User Passwords in an LDAP Directory

For users who are stored in an LDAP directory, you can configure your system to allow both Authentication Manager administrator's and the users themselves to modify the user password.

An administrator can modify the password of users whose accounts are stored in an LDAP directory if the identity source administration account has permission to write to user records in the LDAP directory. This account is specified in the Directory User ID and Directory Password account fields on the Identity Source Connections page in the Operations Console.

Users can change their passwords when prompted during authentication if the following conditions are met:

- The identity source administration account has permission to write to user records in the LDAP directory.
- The directory is configured to permit the users to change their passwords.

  Note: If you do not permit users to change their passwords during authentication, the identity source administration account does not need permission to write to the LDAP directory.

- An LDAPS connection is configured between Authentication Manager and the LDAP directory. For instructions on setting up an SSL connection, see Identity Source SSL Certificates on page 114.
- One of the following conditions applies:
  - The user's password has expired.
  - An Authentication Manager administrator has edited the user's user record to force a password change by checking the **Require the user to change password at next logon box**.
  - The LDAP directory is configured to require the user to reset the password the next time the user authenticates.

If these conditions are not met, users' attempts to change passwords will fail.

Password Policy for Active Directory

Active Directory has a default password policy that is more strict than the default Authentication Manager password policy. This can lead to errors such as “Will Not Perform” when adding and updating users.

To manage password policies with Active Directory identity sources, do one of the following:

- Make your Authentication Manager password policy password requirements more strict. See Chapter 4, Configuring Authentication Policies.
- Relax the complexity requirements in the Windows 2003, 2008, or 2008 R2 Group Policy Object Editor. For more information, see your Active Directory documentation.

Note: The Authentication Manager default password policy is already stricter than the default password policy of the Oracle Directory Server.

Custom Attribute Mapping

If you are using custom attributes, after adding the identity source, you need to explicitly map identity attribute definitions to physical attribute names in an LDAP directory identity source schema.

All user fields must map to non-null fields. However, the User ID can be mapped to any unique attribute for a user.

For complete mapping instructions, see the following Help topics in the Security Console.

Security Console Help Topic	Description
“User Attributes”	Overview of internal and default user attributes.
“Add Identity Attribute Categories”	Instructions for grouping related identity attributes together in categories. When you add identity attribute definitions, you assign each attribute to a category. For example, Address can be an attribute category used to group together the fields for Street, City, State, and Country. The default category is Attributes.
“Add Identity Attribute Definitions”	Instructions for mapping custom user attributes.

Identity Source User Attributes

To view LDAP data in the Security Console, you must map the Authentication Manager fields to corresponding fields in the LDAP directory. These fields are called attributes. There are two types of user attributes:

- Core attributes
- Custom attributes

Core Attributes

Core attributes include basic user attributes such as User ID, first name, and last name. You map these when you use the Operations Console to create an identity source.

Mapping the fields in the directory to the fields in Authentication Manager allows you to use the Security Console to view user and user group data stored in the directory. For example, when you create an identity source, you map the Authentication Manager User ID field to the appropriate field in the LDAP directory. You map core attributes when creating an identity source in the Operations Console.

All user fields must map to non-empty fields. For example, with Active Directory, User ID is mapped to sAMAccountName by default, but it can be mapped to any unique non-empty attribute for a user.

If you have multiple identity sources, try to map your attributes consistently. For example, if you map User ID to sAMAccountName in one identity source, do the same for your other identity sources.

Custom Attributes

In addition to the core attributes, you can define custom attributes, called identity attribute definitions, that contain information tailored to your organization. You can map these custom attributes to fields in the LDAP directory, allowing Authentication Manager to display these attribute values from the directory. You can use custom attributes to provide support information to your Help Desk personnel.

The attribute definition indicates whether the value should be stored in the directory or in the internal database. If stored in the directory, the field must already exist in the directory.

Use the Security Console to create and map custom attributes.

Unique Identifier Attribute

When you create an identity source and map the core attributes, you must map the Unique Identifier field. This field helps Authentication Manager map internal database records to their corresponding LDAP Directory records. Authentication Manager uses this field to find users whose distinguished name (DN) has changed. The default Unique Identifier is one of the following:

- For Active Directory, the default attribute is ObjectGUID.
- For Oracle Directory Server (and Sun Java Directory Server), the default attribute is nsUniqueID.

Map the Unique Identifier field on the Add New Identity Source page in the Operations Console. For more information, see Add an Identity Source on page 110.

The Unique Identifier attribute must meet these requirements:

- The attribute must contain unique data for each user. For example, an employee ID number or badge number that is unique for each user in your deployment.
- The attribute must contain data for each user. The value cannot be empty.
- The attribute value cannot change. If the value for a user changes, Authentication Manager cannot track the user. You cannot map any other fields to the attribute that you map to the Unique Identifier.
- The attribute name must not exceed 64 characters.
- The attribute value must not exceed 42 characters.

Follow these guidelines when mapping unique identifiers:

- You must specify the Unique Identifier before you move or rename directory users who are viewed or managed through the Security Console. Otherwise, the system creates a duplicate record for the users that you move or rename, and disassociates them from data the system has stored for them.
- After you have mapped the Unique Identifier field, you cannot change it.

User Account Enabled State Attribute

Each identity source contains an attribute, called the User Account Enabled State, that indicates where Authentication Manager looks to determine whether a user account is enabled or disabled. Authentication Manager always checks the external directory of an LDAP identity source, but you can configure it to check the setting in the internal database as well.

The Enabled attribute reports the enabled or disabled state of a user's account in Authentication Manager, as controlled in the Security Console. Unlike many other user attributes, you cannot alter the mapping of the Enabled attribute.

When you use the Operations Console to create an LDAP identity source, you can control how Authentication Manager determines whether a user is enabled for remote access. You can set the User Account Enabled State in either of two ways:

- When set to **Directory**, Authentication Manager consults the user's enabled state in the LDAP directory only.

  Use the Directory setting if you want LDAP alone to control whether a user is enabled in Authentication Manager. Disabling a user account in Authentication Manager requires disabling the user account in the directory.

- When set to **Directory and Internal Database**, Authentication Manager consults both the LDAP directory and the Authentication Manager internal database to determine a user's enabled state.

  Use the Internal Database setting if you want to disable the user in Authentication Manager, but allow the user to remain enabled in the LDAP. In this case, the user is not permitted to authenticate with Authentication Manager for remote access, but the state of the user's LDAP account does not change. For example, the user can still log on to Windows because the Windows Domain account remains enabled.

For both settings, the user's LDAP account must be enabled for the user to authenticate with Authentication Manager.

6 Administering Users

Common User Administration Tasks

You use the Security Console to provide and maintain authentication service for users. The Security Console enables you to perform the following common tasks:

- Manage user data
- Restrict access to specific resources
- Specify user access privileges
- Resolve user access problems
- Respond to user security issues
- Maintain user data

The administrative tasks that you can perform are defined by the scope of your administrative role.

Add a User to the Internal Database

You can use the Security Console to add users to the internal database even if an LDAP directory is the primary identity source. Adding users directly to the internal database allows you to create a group of users different from those in identity source. For example, you might store a group of temporary contractors or a specific group of administrators in the internal database. You might also use the internal database to store a small number of users for a pilot project.

User data in an LDAP directory is read-only. You must add users to the LDAP directory using the directory tools. However, you can use the Security Console to perform certain administrative functions, such as assigning tokens or enabling a user for risk-based authentication.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Add New**.
2. In the Administrative Control section, from the **Security Domain** drop-down list, select the security domain where you want the user to be managed. The user is managed by administrators whose administrative scope includes the security domain you select.

3. In the User Basics section, do the following:

   a. (Optional) In the **First Name** field, enter the user's first name. Do not exceed 255 characters.

   b. (Optional) In the **Middle Name** field, enter the user's middle name. Do not exceed 255 characters.

   c. In the **Last Name** field, enter the last name of the user. Do not exceed 255 characters.

   d. In the **User ID** field, enter the User ID for the user. The User ID cannot exceed 48 characters. Make sure the User ID is unique to the identity source where you save the user. Do not use multi-byte characters, for example:

   東

   Note: If you are creating an account for an administrator who requires access to the Security Console, the User ID must be unique within the deployment.

   e. (Optional) In the **Email** field, enter the user's e-mail address. Do not exceed 255 characters.

   f. (Optional) In the **Certificate DN** field, enter the user's certificate DN. The certificate DN must match the subject line of the certificate issued to the user for authentication. Do not exceed 255 characters.

4. In the Password section, do the following:

   Note: This password is not used for authenticating through authentication agents.

   a. In the **Password** field, enter a password for the user. Password requirements are determined by the password policy assigned to the security domain where the user is managed. This is the user’s identity source password, which may be different from alternate passwords provided by applications. For more information, see the Security Console Help topic “View a Password Policy.”

   b. In the **Confirm Password** field, enter the same password that you entered in the Password field.

   c. (Optional) Select **Force Password Change** if you want to force the user to change his or her password the next time the user logs on. You might select this checkbox, for example, if you assign a standard password to all new users, which you want them to change when they start using the system.

5. In the Account Information section, do the following:

   a. From the **Account Starts** drop-down lists, select the date and time you want the user’s account to become active. The time zone is determined by local system time.

   b. From the **Account Expires** drop-down lists, select the date and time you want the user’s account to expire, or configure the account with no expiration date. The time zone is determined by local system time.

   c. (Optional) Select **Disabled** if you want to disable the new account.
   d. If a Locked Status option is selected, you can unlock the user by clearing all selected options.
6. (Optional) Under **Attributes**, enter the user's mobile phone number in the **Mobile Number (String)** field.
7. Click **Save**.

User Status

To increase security, you can disable users who take an extended absence, and enable these users when they return to work.

Before enabling or disabling users, know the following:

- Disabling a user does not delete that user from the identity source.
- When a user account is disabled, any tokens belonging to the user remain assigned. Disabling a user account does not unassign the user's assigned tokens.
- Authentication Manager verifies whether a user is enabled or disabled each time a user authenticates. If a user in a linked identity source is disabled, that user cannot authenticate.

Disable a User Account

When you disable a user account, you suspend the user's permission to authenticate, which prohibits access to protected resources. Disabling a user does not delete the user from the identity source. To delete a user, see the Security Console Help topic "Delete a User."

If you want to disable a user in an LDAP directory that is linked to RSA Authentication Manager, you must use the native LDAP directory interface.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user that you want to disable. Some fields are case sensitive.
3. Click the user that you want to disable, and select **Edit**.
4. Under **Account Information**, select **Account is disabled**.
5. Click **Save**.

Enable a User Account

When you enable a user account, the user can authenticate and access protected resources.

To authenticate users to a directory server, you must enable the user in both the directory server and in the Security Console. Only users who are enabled in the directory server can authenticate to the directory server.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user that you want to enable. Some fields are case sensitive.
3. Click the user that you want to enable, and select **Edit**.
4. Under **Account Information**, clear **Account is disabled**.
5. Click **Save**.

Security Domains to Organize Users

After you create the security domain hierarchy and link the identity source to the system, all users are added to the top-level security domain. To help you organize users, manage the deployment, and limit administrative scope, you may want to move users to another security domain in the hierarchy.

Just as you have likely created security domains to match either your organization's structure or geographic locations, you can use the Security Console to transfer users from each department or location to their respective security domains.

For example, if the top-level security domain is named SystemDomain, and you have lower-level security domains named Boston, New York, and San Jose, you would likely move users from SystemDomain to their respective security domains.

For more information about security domains, see Security Domain Overview on page 39.

Move Users Between Security Domains

You can manually move users whose accounts are stored in the internal database to other security domains. You can also move user groups.

When you move users to another security domain, the policies for the new security domain take effect immediately. Also, after you move users, only administrators with permissions to manage users in that security domain can manage the users you moved.

When you move users, consider that users who are enabled for risk-based authentication (RBA) before the move retain their RBA user settings after the move. If users are disabled for RBA before the move, the users remain disabled for RBA after the move.

You can automatically move LDAP directory users to other security domains by mapping directory objects, such as organizational units, to the security domain of your choice. Authentication Manager uses security domain mappings to add users to the appropriate security domain when new user records are added to the database.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the users that you want to move. Some fields are case sensitive.

3. Select the users that you want to move.
4. From the Action menu, select **Move to Security Domain**, and click **Go**.
5. From the **Move to Security Domain** drop-down list, select the security domain where you want to move the user.
6. Click **Move**.

Duplicate User IDs

If two users with the same user name attempt to access the same protected resource, authentication will fail. This may occur if you link multiple identity sources to the same deployment and users with the same User ID exist in each identity source. In these cases, you have the following options:

- Map the User ID to another field where there are no duplicate values. For example, for an Active Directory identity source, you might be able to map to the UPN field or to a user's email address.
- Change one of the User IDs in the identity source so that both User IDs become unique. This option may not be practical if the User ID is used for other applications.
- Assign authenticators to only one of the users with the duplicate User ID. This option is not practical if authenticators must be assigned to more than one user with the duplicate User ID.
- You can allow one user to authenticate with a logon alias, and you can prevent this user from authenticating with the default User ID.

User Authentication

You use the Security Console to manage user authentication. You can:

- Modify user authentication settings
- Resolve user access problems

The user authentication tasks that you can perform are defined by the scope of the administrative role.

Manage User Authentication Settings

User authentication settings allow you to create exceptions to authentication policies for individual users. These settings also allow you to troubleshoot user authentication issues.

Before You Begin

You must have a restricted or unrestricted agent. If you plan to configure a logon alias, the user must belong to a user group that has access to a restricted agent or has been enabled on an unrestricted agent.

Procedure

1. In the Security Console, click **Identity** > **Users > Manage Existing**.
2. Use the search fields to find the user that you want to manage.
3. From the search results, click the user that you want to manage.
4. From the context menu, click **Authentication Settings**.
5. If you want to assign a fixed passcode to the user, select the **Fixed Passcode** checkbox.

   RSA recommends that you do not use fixed passcodes because they eliminate all the advantages of two-factor authentication.
6. Select the **Clear Incorrect Passcodes** checkbox to clear any incorrect passcodes. The count of incorrect passcodes is reset, and the user is not prompted for the next tokencode. However, if the user continues to enter incorrect passcodes and exceeds the number of failed logon attempts allowed by the lockout policy, the user is locked out of the system.
7. Select **Clear cached copy of selected user's Windows credential** to clear a cached version of a user's password.

   If your deployment uses RSA SecurID for Windows, Authentication Manager saves a cached version of the user’s Windows logon password. This information may need to be cleared, if the Windows password has been changed in Active Directory.
8. If you want to assign a default shell to the user, enter it in the **Default Shell** field.
9. To configure a logon alias for the user:
   a. Select whether you want to allow users to use their own User IDs and the alias.

      You can use this option to prevent a conflict between users who share the same default User IDs.

   b. Select the user group to which you want to assign the alias.

   c. In the **User ID** field, enter the User ID that you want to assign to the alias. In the **Shell** field, enter the shell that you want assigned to the alias. If you are using RADIUS, from the **RADIUS Profile** drop-down menu, select the RADIUS profile to assign to the alias. Click **Add**.
10. If you use RADIUS, select the RADIUS profile and RADIUS user attributes to assign to the user:
    a. From the **User RADIUS Profile** drop-down menu, select a RADIUS profile to assign to the user.

       If you set up logon aliases for the user and you do not specify a RADIUS profile for each alias in step 9, Authentication Manager assigns the user RADIUS profile to each alias.

    b. In **RADIUS User Attributes**, select the attribute that you want to assign to the user, enter the value for the attribute in the **Value** field, and click **Add**. RADIUS user attributes take precedence over attributes in a RADIUS profile.

A RADIUS user attribute can be mapped to an identity source attribute. For more information, see Map a RADIUS User Attribute Definition to an Identity Source Attribute on page 313.

11. Click **Save**.

Logon Alias

A logon alias allows users to log on with a user group ID. The user group ID is associated with a user group that has access to a restricted agent or that has been enabled on an unrestricted agent.

For example, users can have a User ID based on their first initial and last name, such as, "kmiller," as well as an administrative User ID with a specific name, for example "root." If a logon alias is established, Authentication Manager verifies the authentication using the user's passcode, regardless of the User ID that the user entered to log on to the operating system. For backward compatibility, a shell value is also maintained by the system.

A logon alias can also be used in deployments where there are users with the same User ID. An alias that further identifies the user may prevent conflicts when these users attempt to authenticate. In the authentication settings for a user, you can also prevent a user from authenticating with the default User ID and instead require that the user authenticate with an alias.

To allow a user to authenticate with a logon alias on a restricted agent, you must grant the user group that is associated with the alias access to the agent. Although all users within a deployment can access an unrestricted agent, a user cannot authenticate with a logon alias until you enable the user group that is associated with the alias on the unrestricted agent.

You can assign logon aliases on the Authentication Settings page in the Security Console. This page is accessed through the user Context menu.

For instructions, see Manage User Authentication Settings on page 123.

Unlock a User

RSA Authentication Manager locks out users who violate the lockout policy. Locked out users cannot authenticate until they are unlocked.

The lockout policy specifies the number of failed authentication attempts allowed before the system locks the account. A lockout policy can unlock users after a specific time period, or you can require an administrator to manually unlock the user.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user that you want to unlock. Some fields are case sensitive.
3. Click the user that you want to unlock, and select **Edit**.
4. Under **Account Information**, go to **Locked Status**, and clear all options that are selected.
5. Click **Save**.

Incorrect Passcode Count

The system counts each time the assigned user enters an incorrect passcode, clearing this count automatically with each correct passcode. If a user enters more incorrect passcodes than are allowed by the SecurID token policy and then enters a correct passcode, the user is prompted for the next tokencode. If you do not want a user to be prompted for the next tokencode, you can use the Security Console to clear the number of incorrect passcodes entered.

This operation only clears the existing count. To clear future counts, you must perform the procedure again.

For instructions, see Manage User Authentication Settings on page 123.

Managing Security Questions

Security questions is an authentication method that requires users to answer questions in order to authenticate. During enrollment or when users access the Self-Service Console for the first time, users are presented with several questions, which they must answer. Later when users authenticate, the users must answer a subset of these questions with the same answers that they provided during enrollment.

Security questions are used under the following conditions:

- when the primary authentication method results in a failed authentication
- to confirm identity for risk-based authentication (RBA)

If you want to allow users to change their answers, you must clear their existing answers. For example, you might need to do this when users forget their answers, or when users believe that their answers are compromised. After you clear a user's answers, the user is prompted to provide new answers at the next logon. For instructions, see the Security Console Help topic "Clear Security Question Answers."

A file of questions is provided for English-speaking users, which you can modify to create a new question file. You can also create a file of non-English questions in any supported language. When you create a new set of questions or modify just one question, the new file replaces the existing file.

You specify the number of questions that users must answer during enrollment or when accessing the Self-Service Console for the first time. You also specify the number of questions that users must answer during authentication. The number of questions that you specify for enrollment should be greater than the number of questions that you specify for authentication. If you specify fewer questions for authentication than you specify for enrollment, users can choose which questions to answer for authentication.

For self-service troubleshooting, the number of available questions must exceed the number of questions required for authentication.

Set Requirements for Security Questions

You specify the number of security questions that users must answer during enrollment or when they access the Self-Service Console for the first time, and the number of questions that users must answer correctly during authentication. If the total number of security questions specified for enrollment exceeds the number of questions specified for authentication, the user can choose which questions to answer for authentication.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Click **Security Questions Requirements**.
3. In the **Enrollment** field, specify the number of questions users must answer during enrollment. Modifying this setting does not affect users who are currently enrolled.
4. In the **Authentication** field, specify the number of questions users must answer correctly during authentication.
5. Click **Save**.

Custom Security Questions

You can customize the text and language of security questions by creating and importing a customized XML file into the database. When you create a new security questions file, you can make the following modifications:

- **Change the existing English text**. Edit the existing XML file to change the wording of the existing questions or add new questions of your own.
- **Change the language**. Create a new XML file using the provided template. Specify the language ID, and enter the security questions written in the selected language.

The RSA Authentication Manager 8.1 download kit includes a security questions sample file (**SecurityQuestionsSample.xml**) that you can use as a template. The file looks similar to the following example:

```
<?xml version=”1.0” encoding=”UTF-8”?>
 <SECURITY_QUESTIONS>
   <LANGUAGE id=”en_US”>
     <QUESTION>first question</QUESTION>
     <QUESTION>second question</QUESTION>
     <QUESTION>third question</QUESTION>
   </LANGUAGE>
 </SECURITY_QUESTIONS>
```

The **Security Questions Sample** folder on the RSA Authentication Manager 8.1 download kit also includes a security questions file schema (**SecurityQuestions.xsd**) for validating a modified or new security questions file.

A deployment can have only one active security questions file. If you modify the existing security questions and import the modified file, users must complete security questions enrollment again.

Follow these guidelines when customizing security questions:

- Create a separate XML file for each LANGUAGE. For example, if you need questions in three languages, you must create three language files.
- Each XML file must include the XML language attribute that identifies the language used to write the questions. For a list of supported language ID codes, see the Security Console Help topic “Language Codes for Security Questions.”
- You must type the text in the actual language. Authentication Manager does not translate languages.
- A security question can contain up to 255 characters.
- The security questions file must contain at least as many security questions as you have specified for enrollment. For more information, see the Security Console Help topic “Set Requirements for Security Questions.”
- You cannot delete a security questions file.

Modify the Security Questions File

Security questions are contained in an XML file that is saved in the database. A set of default questions is provided for English speaking users. You can modify the default questions by changing them or adding additional questions. Once your work is finished, you import the modified XML file into the database. When you import the new file, the language set in the new file replaces the corresponding set in the system. For example, all of the English questions in the new file replace all of the previous English questions. Therefore, if you modify even one question in the existing file, you must reimport the entire file.

Decide carefully whether to modify an existing security questions file. Each time you import a file to modify existing questions, all of the user answers to the previous questions are deleted. Users must reenter their answers. RSA recommends that you customize the security questions before any users answer the security questions.

Procedure

1. View the example in the security questions sample file (**SecurityQuestionSample.xml**) in the RSA Authentication Manager 8.1 download kit.
2. Create a separate security questions XML file for each LANGUAGE element. For example, if you need questions in three languages, create a file for each language.
3. Type the security questions in each file using the actual language. Authentication Manager does not translate languages. A security question can contain up to 255 characters. Add at least as many security questions as are required by your security questions enrollment setting.
4. Make sure that each XML file includes a language ID code that matches the language of the text. For a list of supported language ID codes, see the Security Console Help topic “Language Codes for Security Questions.”
5. Validate each file using the security questions file schema (**SecurityQuestions.xsd**) in the RSA Authentication Manager 8.1 download kit.

Next Step

Import each new security questions file. For instructions, see the Security Console Help topic “Import Security Questions.”

Emergency Online Authentication

Online authentication provides emergency access for users with missing or damaged tokens. Even with a missing token, users can continue to have two-factor authentication using an online emergency access tokencode, an 8-character alphanumeric code generated by Authentication Manager.

The format of the online emergency access tokencode is determined by the token policy of the associated security domain. For example, if the security domain’s token policy allows special characters, the online emergency access tokencode can include special characters.

If a user has an expired token, assign a new token, and then provide temporary access. An online emergency access tokencode cannot be assigned to a user with an expired token. For instructions, see Provide an Offline Emergency Passcode on page 133.

The following table lists the types of online emergency access tokencodes. Both tokencode types replace the tokencode generated by the user’s token.

Tokencode Type	Description
Temporary fixed tokencode	• Can be used more than once. • Must be combined with the user’s RSA SecurID PIN to create a passcode. • Is displayed on the Self-Service Console.
One-time tokencode	• Issued in sets. You can determine the number of tokencodes in a set. • Must be combined with the user’s RSA SecurID PIN to create a passcode. • Is displayed on the Self-Service Console. • Users can download the set of one-time tokencodes in a file. • Each tokencode in the set can only be used once.

Users can also use the Self-Service Console to request temporary access to Authentication Manager without the assistance of an administrator. For more information, see RSA Self-Service on page 233.

Assign a Set of One-Time Tokencodes

You can provide temporary access for a user whose token has been permanently lost or destroyed by assigning a set of one-time tokencodes. A one-time tokencode replaces the tokencode generated by the user's missing token. Users must enter their PIN and a one-time tokencode to perform two-factor authentication.

Each one-time tokencode in a set can be used once. A set of tokencodes allows a user to authenticate multiple times without contacting an administrator each time.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Use the search fields to find the appropriate token.
3. From the search results, click the token with which you want to work.
4. From the context menu, click **Emergency Access Tokencodes**.
5. On the Manage Emergency Access Tokencodes page, select the **Online Emergency Access** checkbox to enable authentication with an online emergency access tokencode.
6. Select **Set of One-Time Tokencodes**.
7. Enter the number of tokencodes that you want to generate.
8. Click **Generate Codes**. The set of tokencodes displays below the Generate Codes button.
9. Record the set of one-time tokencodes so you can communicate them to the user.
10. Select one of the following options for the **Emergency Access Tokencode Lifetime**:
    - No expiration.
    - Set an expiration date for the tokencode.
11. In the **If Token Becomes Available** field, configure how Authentication Manager handles lost or unavailable tokens that become available.
    - Deny authentication with the recovered token.

      If a token is permanently lost or stolen, deny authentication with the recovered token so that it cannot be used for authentication if recovered by an unauthorized individual. This is essential if the lost token does not require a PIN.
    - Allow authentication with the recovered token while simultaneously disabling the emergency access tokencode.
    - Allow authentication with the recovered token only after the emergency access tokencode has expired.
12. Click **Save**.

Assign a Temporary Fixed Tokencode

Occasionally, it is necessary to give a user temporary access to resources protected by RSA SecurID. For example, you can give temporary access to a user whose existing token has been lost or destroyed. Temporary access allows a user to access protected resources while waiting for a replacement token.

This procedure provides a user with temporary emergency access using a temporary fixed tokencode.

A temporary fixed tokencode replaces the tokencode generated by the user's token. Similar to the regular tokencode, the temporary fixed tokencode is entered with the user's PIN to create a passcode. By using a PIN with the temporary fixed tokencode, the user can still achieve two-factor authentication.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. On the **Assigned** tab, use the search fields to find the lost or destroyed token.
3. From the search results, click the lost or destroyed token, and from the context menu, select **Emergency Access Tokencodes**.
4. On the Manage Emergency Access Tokencodes page, select **Online Emergency Access**.
5. For **Type of Emergency Access Tokencode(s)**, select **Temporary Fixed Tokencode**.
6. Click **Generate New Code**. The tokencode displays next to the **Generate New Code** button.
7. Record the emergency access tokencode so that you can communicate it to the user.
8. For **Emergency Access Tokencode Lifetime**, select either **No expiration** or select **Expire on** and specify an expiration date.

   You may want to limit the length of time the one time tokencode can be used. Because the one-time tokencode is a fixed code, it is not as secure as the pseudorandom number generated by a token.
9. For **If Token Becomes Available**, select one of the following options:
   - **Deny authentication with token**.

     Select this option if the token is permanently lost or stolen. This option prevents the token from being used for authentication if recovered. This safeguards the protected resources in the event the token is found by an unauthorized individual who attempts to authenticate.
   - **Allow authentication with token at any time and disable online emergency tokencode**.

     Select this option if the token is temporarily unavailable (for example, the user left the token at home). When the user recovers the token, he or she can immediately resume using the token for authentication. The online emergency access tokencode is disabled as soon as the recovered token is used.
   - **Allow authentication with token only after the emergency code lifetime has expired and disable online emergency tokencode**.

     You can choose this option for misplaced tokens. When the missing token is recovered, it cannot be used for authentication until the online emergency access tokencode expires.
10. Click **Save**.

Emergency Offline Authentication

Offline authentication provides emergency access for RSA SecurID for Windows users who require emergency access while authenticating offline. These are users with lost or stolen tokens, or users who have forgotten their PIN. Temporary emergency access can be provided in two ways:

- **Offline emergency access tokencode.** Use this option if the user's token is unavailable. The Offline Emergency Access Tokencode is used with the user's PIN.
- **Offline emergency passcode.** Use this option if a user has forgotten his or her PIN. The offline emergency passcode is used in place of the user's PIN and tokencode.

RSA SecurID for Windows users may need temporary emergency access so that they can authenticate while working offline. Temporary emergency access is necessary for users with misplaced, lost, or stolen tokens, or users who have forgotten their PIN.

For offline authentication, the system generates and downloads an offline passcode or tokencode before the user needs it. Providing emergency offline authentication codes must be done in advance. Authentication codes cannot be sent to a user who is offline.

Provide an Offline Emergency Access Tokencode

An offline emergency access tokencode replaces the tokencode generated by the user's token. Similar to the tokencode used in non-emergency circumstances, the user enters the offline emergency access tokencode with a PIN to create a passcode, thus achieving two-factor authentication.

You can configure the following:

- Specify that a new offline emergency access tokencode is downloaded the next time the user authenticates online.
- Allow the offline emergency access tokencode to be used for online and offline authentication.

Before You Begin

- The user's security domain must allow offline authentication and permit the user to download offline emergency access tokencodes.
- The user must have authenticated to an agent that supports offline authentication and the agent has downloaded days of offline authentication data.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Use the search fields to find the token for the user who needs an offline emergency access tokencode.
3. From the search results, click the token.
4. From the context menu, click **Emergency Access Tokencodes**.

5. On the Manage Emergency Access Tokencodes page, note the Offline Emergency Access Tokencode and its expiration date.
6. Select **Reset Offline Emergency Access Tokencode**, if you want the user to download a new offline emergency access tokencode the next time he or she authenticates online. If selected, the new tokencode downloads automatically.
7. Click **Use offline code for online access**, if you want the offline emergency access tokencode used for online authentication.
8. Click **Save**.

Provide an Offline Emergency Passcode

An offline emergency passcode takes the place of the passcode (PIN + tokencode) that the user normally enters. The user does not need to possess the token or know the PIN to authenticate offline.

Before You Begin

Confirm the following:

- The user's security domain allows offline authentication and permits the user to download offline emergency access tokencodes.
- The user has authenticated to an agent that supports offline authentication and the agent has downloaded days of offline authentication data.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user who needs an offline emergency passcode.
3. From the search results, click the user.
4. From the context menu, click **Manage Emergency Offline Access**.
5. On the Manage Emergency Access Passcodes page, note the Offline Emergency Passcode and its expiration date.
6. Select **Reset Offline Emergency Access Passcode**, if you want the user to download a new offline emergency passcode the next time he or she authenticates online. If selected, the new passcode downloads automatically.
7. Click **Update**.

RSA SecurID PINs

A personal identification number (PIN) is a numeric password used to authenticate a user.

To increase security, you can set the token policy to require users to create PINs containing both letters and numbers and to change their PINs at regular intervals. See Token Policy on page 76.

Misplaced or stolen PINs puts protected resources at risk. For this reason, you should instruct users to report compromised PINs as soon as possible.

When a user reports a compromised PIN, you can require the user to change his or her PIN after the next successful authentication.

When a user is required to change a PIN, the user must know his or her current PIN. To change a PIN, the user authenticates using the existing PIN and tokencode. After successfully authenticating, the user is prompted to create and confirm a new PIN, and the PIN is associated with the user’s token.

For example, suppose a user reports that she used her computer at a local coffee shop, and now she is worried that someone may have seen her type her PIN. After you receive the report, you use the Security Console to require the user to change her PIN. For instructions, see Require Users to Change Their RSA SecurID PINs on page 135.

The token policy may require the user to use a system-generated PIN instead of creating one. After the next authentication, the system provides the user with a new, system-generated PIN. The user then authenticates again using the new, system-generated PIN.

If users forget their PINs, you cannot require them to change their PINS in order to obtain a new one because users need to know their PINs in order to change them. When a user forgets his or her PIN, you must clear the PIN before the user can create a new one. For instructions, see, Clear an RSA SecurID PIN on page 135.

Users can also use Self-Service to reset their PINs.

Set an Initial On-Demand Authentication PIN for a User

On-demand authentication (ODA) always requires a PIN to request a tokencode. You can set the initial PIN for the user. The following procedure is for a user who is not yet enabled for ODA.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user for whom you want to enable ODA and set an initial PIN.
3. Click the user.
4. Select **SecurID Tokens**.
5. Under **On-Demand Authentication**, select **Enable User**.
6. For **Expiration Date**, specify **No expiration** or the date when on-demand authentication expires.
7. For **Send On-Demand Tokencodes to**, specify the delivery method.
8. For **Associated PIN**, do one of the following:
   - Select **Require user to setup the PIN through RSA Self-Service Console**.
   - Select **Set initial PIN to**, and enter the initial PIN.
9. Click **Save**.
10. If you have set the initial PIN, securely communicate the initial PIN to the user.

Clear a User's On-Demand Authentication PIN

You might clear a user's on-demand authentication (ODA) PIN when the PIN is compromised, forgotten, or when your company policy requires the PIN change. You must always set a temporary PIN when you clear a user's PIN because ODA requires a PIN.

The user must change a temporary PIN the first time it is used.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user for whom you want to set a temporary PIN.
3. Click the user.
4. From the context menu, select **SecurID Tokens**.
5. Under **On-Demand Authentication**, for **Associated Pin**, select **Clear existing PIN and set a temporary PIN for the user**.
6. Enter a temporary PIN.
7. Click **Save**.
8. Securely communicate the temporary PIN to the user.

Require Users to Change Their RSA SecurID PINs

When you require a user to change a SecurID PIN, the user is prompted to create a new PIN after successfully authenticating with the token.

You can require a PIN change only when a user knows the existing PIN. For example, you might require a user to change a SecurID PIN if the current PIN has been compromised. If a user has forgotten the PIN, clear the PIN.

Procedure

1. In the Security Console, click **Authentication > SecurID Tokens > Manage Existing**.
2. Click the **Assigned** tab.
3. Use the search fields to find the token that you want to edit.
4. From the search results, click the token with the PIN that you want the user to change.
5. Select **Require SecurID PIN Change**.

Clear an RSA SecurID PIN

When a user forgets a SecurID PIN, you can clear the PIN so that the user can create a new one. When you clear a user’s PIN, the user can create a new PIN the next time the user authenticates.

For example, suppose a user has forgotten a PIN and calls for help. You verify the user’s identity and clear the PIN. You tell the user to enter just the tokencode when prompted for the passcode the next time user authenticates. After entering the tokencode, the user is prompted to create a new PIN for the user’s token.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user for whom you want to clear a PIN.
3. Click the user.
4. From the context menu, select **SecurID Tokens**.
5. Click the serial number for the user’s assigned token.
6. From the context menu, select **Clear SecurID PIN**.
7. Tell the user to enter only a tokencode at the next authentication. After the user enters the tokencode, the user is prompted to create a new PIN.

Obtain the PIN Unlocking Key for an RSA SecurID 800 Authenticator

Users with SecurID 800 authenticators need a PIN unlocking key to access their token if they have forgotten their PIN. Use the Security Console to view the smartcard details and obtain the PIN unlocking key.

Before You Begin

You must load the SecurID 800 authenticator data into RSA Authentication Manager before you can view it. For instructions, see Import PIN Unlocking Keys on page 136.

Procedure

1. In the Security Console, click **Authentication > SecurID Tokens > Manage Existing.**
2. Click the **Assigned** tab.
3. Use the search fields to find the smartcard that you want to view.
4. From the search results, click the smartcard that you want to view.
5. From the context menu, click **Edit**.
6. View the **SID800 Smart Card Details** section to obtain the PIN unlocking key.

Import PIN Unlocking Keys

Use the Import PIN Unlocking Key utility, import-puk, to import the PIN Unlocking Keys for the RSA SecurID 800 Hybrid Authenticator into Authentication Manager. After importing the XML data, you can view the PIN Unlocking Key on the Token Properties page in the Security Console.

Before You Begin

- You must have an administrator role with SecurID 800 Smart Card Details permission to perform this procedure. For more information, see the Security Console Help topic “Edit an Administrative Role.”
- Secure shell (SSH) must be enabled on the appliance. For instructions, see Enable SSH on the Appliance on page 403.

Procedure

1. Log on to the appliance using an SSH client. For instructions, see Log On to the Appliance Operating System with SSH on page 404.
2. Change directories to **/opt/rsa/am/utils**. Type:

   ```
   cd /opt/rsa/am/utils/
   ```

   and press ENTER.
3. Run import-puk to import the PIN unlocking keys. Type:

   ```
   ./rsautil import-puk -f filename
   ```

   where *filename* is the path to the PUK.xml file, for example:
   -f /opt/rsa/am/PUK.xml
4. When prompted, enter your administrator User ID, and press ENTER.
5. When prompted, enter your password, and press ENTER.
6. When the import process is complete, the following message displays:

   ```
   Status: IMPORTED <number> PIN UNLOCK KEY (PUK) RECORDS
   SUCCESSFULLY.
   ```

7. Close the SSH client. Type:

   ```
   exit
   ```

   and press ENTER.

User Groups

Grouping users makes it easy to manage access to protected resources. A user group is a collection of users, other user groups, or both. Users and user groups that belong to a user group are called member users and member user groups.

User Group Organization

You can organize groups according to your organizational needs:

- Geographic location. Groups can be created according to geography.
  - A city, state, or country
  - A region that includes several cities, states, or countries
- Company divisions. Groups can be created according to functional areas in a company.
  - Department
  - Project
  - Job
- Resources. Groups can be created according to particular resources.
  - Research and development files
  - Medical records

User Group Characteristics

User groups have the following characteristics:

- Each user group is stored in an identity source, either an LDAP directory or the internal database.
- Each user group is associated with a security domain.
- A user group can contain multiple users and user groups.

  User groups stored in an external identity source can contain only users and user groups contained in that identity source.
- A user group can include users and user groups that are managed in different security domains.

  For example, users in security domain A and users in security domain B can both be members of the same user group and thus access the same protected resources.
- User group names must be unique within a single identity source.

  Authentication Manager can have two user groups with the same name if they are stored in two different identity sources.
- Administrators can move user groups between security domains to transfer administrative responsibility for the group to a different administrator. For instructions, see the Security Console Help topic “Move User Groups Between Security Domains.”
- A user or user group can be a member of more than one user group.
- You can add and remove a user from user group using the User Dashboard page. For instructions, see the Security Console Help topic “User Dashboard.”

Creating User Groups

You can create user groups in the following ways:

- To create a user group in the internal database, use the Security Console. For instructions, see Add a User Group on page 140 and Add a User to a User Group on page 140.
- To create a user group in an external identity source, use the LDAP directory native interface.

Internal User Groups

You can add users and user groups from external identity sources to a user group in the internal database. This offers the following benefits:

- Improved authentication performance for users in an external identity source.

  Including these users directly in a group in the internal database reduces the need to access the external identity source when these users authenticate, which reduces network traffic to the directory server. Users in member groups within a user group do not benefit from this improved performance.
- Greater control over organizing users, especially users in an LDAP directory, where you cannot use the Security Console to control the group structure of the directory.

- Reduces administrative burden for the following reasons:
  - You can create a single user group for a restricted agent, and include all the users you want to grant access to the agent, rather than create separate groups for each identity source.
  - When an LDAP administrator modifies a group in the LDAP directory, you can minimize or eliminate the need to reconfigure restricted agents because access is granted through user groups residing in the internal database, and is unaffected by modifications to groups in the directory.

Membership in user groups residing in external identity sources is still restricted to member users and member users groups residing in the same external identity source as the user group.

Nested User Groups

When you configure user groups for restricted agents, you may want to add or "nest" multiple user groups within a single user group. This allows you to enable several groups on a restricted agent. Using nested groups eases the administrative burden of restricting access to authentication agents, but can affect authentication performance when groups are deeply nested or contain large numbers of users.

Nested user groups have the following characteristics:

- A user group in the internal database can contain user groups that reside in the internal database or an external identity source. A user group in an external identity source cannot contain user groups from any other identity source.
- You can nest user groups using one of the following means:
  - Using the Security Console to nest two or more user groups stored in the internal database.
  - Using the LDAP directory user interface to nest two or more user groups stored in the same external identity source.
  - Using the Security Console to nest a user group stored in an external identity source within a user group stored in the internal database.
- Members of nested groups inherit access to restricted agents from the parent user group that is granted access to the restricted agent. If a nested group is also granted access to the same agent, its members may have additional access permissions.

A user who is a member of a nested group can be granted access to a restricted agent for two reasons:

- Because the user is a member of a nested user group that has access to the restricted agent
- Because the user is a member of a user group that is nested in another user group that has access to a restricted agent

In general, members of nested user groups have the same access privileges as the parent user group. Members of the nested user group can access an agent when the group is nested inside another user group that can access the agent.

Add a User Group

You can add user groups to the internal database. You do not need to add a user group that already exists in an external identity source. Groups in external identity sources are added when the identity source is linked.

Procedure

1. In the Security Console, click **Identity** > **User Groups** > **Add New**.
2. From the **Security Domain** drop-down list, select the security domain to which you want to assign the new user group. The new user group is managed by administrators whose administrative scope includes this security domain.
3. In the **User Group Name** field, enter a unique name for the user group. Do not exceed 64 characters. The characters & % > < ‘ are not allowed.
4. Click **Save**.

Add a User to a User Group

You can add users from any identity source to a user group in the internal database only. To change the membership of a group in an external LDAP identity source you must use native tools.

You can add users to a single user group or to multiple user groups.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user that you want to add to a user group. Some search fields are case sensitive.
3. Select the checkbox next to the user that you want to add to a user group.
4. From the Action menu, select **Add to User Groups**, and click **Go**.
5. Use the search fields to find the user group to which you want to add the user. Some search fields are case sensitive.
6. Select the checkbox next to the user group to which you want to add the user. You can select multiple checkboxes to add the user to more than one group.
7. Click **Add to Group**.

Controlling User Access With Authentication Agents

After installing an agent, you configure the agent to control user access to protected resources. The following table describes how each agent configuration controls user access.

Agent Configuration	Who Can Authenticate	Benefits
Unrestricted	All users in the same deployment as the agent.	Less administrative burden because there is no need to configure an agent as a restricted agent, associate user groups with agents, or manage user membership of the user groups associated with the agent. However, you can grant a user group that is associated with a logon alias access to an unrestricted agent.
Restricted	Members of any group directly granted access to the restricted agent. Members of a group nested within a group granted access to the restricted agent.	Increases security because only a subset of users is allowed to authenticate to the agent, which allows you to limit access to specific network resources.
Restricted with group access time restrictions	Members of a group or nested group who authenticate during a specified time.	Further restricts access to the agent by prohibiting authentication outside of a specified time period.

Configuring a Restricted Agent to Control User Access

A restricted agent allows only members of one or more specified groups to access protected resources. For example, if you create a restricted agent to provide access to personnel data and allow only members of the human resources group to authenticate on this agent, only members of the human resources group can access personnel data. You can further restrict access by limiting authentication to a specified a time span.

This procedure lists the high-level tasks required to configure a restricted agent.

Procedure

1. Add an authentication agent, and configure the agent to be a restricted agent.

   For instructions, see Add an Authentication Agent on page 66.

2. Generate the Authentication Manager configuration file.

   For instructions, see Generate the Authentication Manager Configuration File on page 65.

3. Set up user groups.

   For instructions, see User Groups on page 137.

4. Allow a user group access to the restricted agent.

   For instructions, see Allow a User Group to Authenticate on an Agent on page 142.

5. (Optional) Set restricted access times for user groups.

   For instructions, see the Security Console Help topic "Set Restricted Access Times for User Groups."

Allow a User Group to Authenticate on an Agent

Use the following procedure to allow a user group to authenticate on a restricted agent or to enable the use of logon aliases on a restricted or unrestricted agent.

Restricted agents process authentication requests only from users who are members of user groups that have been granted access to the restricted agent. Users who are not members of an associated user group cannot use the restricted agent to authenticate.

Using restricted agents increases your control over who can authenticate to a resource. However, using restricted agents also increases your administrative overhead because administrators must explicitly associate user groups with the agents.

To authenticate on a restricted or unrestricted agent with a logon alias, a user must belong to a user group that is associated with the logon alias and that is enabled for authentication on the agent.

Procedure

1. In the Security Console, click **Access** > **Authentication Agents** > **Manage Existing**.
2. Click the **Restricted** or **Unrestricted** tab.
3. Use the search fields to find the agents to which you want to grant access or enable logon aliases.
4. Select the checkbox next to the agents to which you want to grant access or enable logon aliases.
5. Do one of the following:
   - For restricted agents, select **Grant Access to User Groups** from the Action menu, and click **Go**.
   - For unrestricted agents, select **Enable Logon Aliases** from the Action menu, and click **Go**.
6. Use the search fields to find the user groups to which you want to grant access or enable logon aliases.
7. Select the checkbox next to the user groups to which you want to grant agent access or enable logon aliases.
8. Do one of the following:
   - For restricted agents, click **Grant Access to User Groups**.
   - For unrestricted agents, click **Enable Aliases Associated with User Groups**.

Restricted Access Times for User Groups

You can assign restricted access times to user groups. Restricted access times allow you to control which days and hours members of a user group can access a restricted agent.

For example, suppose you have users in Boston who access company resources and you want to limit access to regular business hours. You can add the Boston users to a group and restrict access times from 8:00 a.m. to 5:00 p.m. To ease the burden of configuring time restrictions, Authentication Manager provides Access Time templates that reflect typical times you may want to restrict access to agents. In this example, you might choose to use the "8am - 5pm Weekdays" template for the group instead of configuring these times manually.

Be aware of the following behaviors and limitations of restricted access times:

- All times are relative to the time zone that you select when you configure restricted access times.

  Be aware of this behavior when applying restricted access times in a deployment containing users in geographically diverse locations. For more information, see Restricted Access Times for Users in Different Geographic Locations on page 143.

- Authentication Manager does not support fractional time zones. You must use an available time zone closest to the desired fractional time zone.

- Authentication Manager does not make automatic adjustments for Daylight Saving Time changes.

Restricted Access Times for Users in Different Geographic Locations

The times that you specify for restricted access are relative to the time zone of the primary instance. If you restrict access times for users in different geographic locations, you must account for the time differences between the locations. To accommodate the time differences, you can configure group membership and access time restrictions in two ways:

- **Configure two or more user groups based on geographic location and set a different access time for each group.** When you configure user groups according to the location of the members, you must compensate for the time difference between the primary instance and the location of the users by configuring different restricted access times for each group.

  For example, if the deployment has users in Boston and London, create a user group for Boston and another for London. Specify different restricted access times for each group. On the primary instance located in Boston, you restrict the Boston group from 8:00 a.m. to 5:00 p.m., and restrict the London group from 3:00 a.m. to 12:00 p.m. (which is 8:00 a.m. to 5:00 p.m. in London).

  Alternatively, you can select the local time zone when configuring restricted access times. In the previous example, you could specify the local time zone for each user group before configuring the restricted access times.

  RSA recommends using this method because it offers more administrative control over access times and over a user's ability to access the restricted agent.

- **Configure a single user group for users in multiple geographic locations and set the same access time for both groups.** When you configure a single group that contains members from different locations, you must make sure that the restricted access times include the entire work day for all members of the user group.

  For example, suppose your group contains users in Boston and London. On the primary instance located in Boston, which is set to Eastern Standard Time, you restrict the Boston access times to the hours of 8:00 a.m. to 5:00 p.m. Because users in London will only be able to access the agent from 1 p.m. to 10 p.m. London time, you must expand the access time for the group from 3:00 a.m. to 5:00 p.m. Eastern Standard Time. This allows users both in Boston and London to access the agent during the work day.

For more information, see Restricted Access Times for User Groups on page 143.

Restricted Access Times for Users in Multiple User Groups

When a user is a member of multiple user groups, more than one of the groups can be granted access to the same restricted agent. In such cases, the time restrictions of the groups are combined, which can expand the time that a user is allowed to access the agent.

For example, suppose that a user is a member of two user groups: Marketing and Sales. Both groups have access to the same restricted agent. If the restricted access time for the members of Marketing is from 8:00 a.m. to 5:00 p.m. and the restricted access time for members of Sales is from 9:00 a.m. to 7:00 p.m., the user can access the agent from 8:00 a.m. to 7:00 p.m.

For more information, see the Security Console Help topic "Set Restricted Access Times for User Groups."

Restricted Access Times for Users in Nested User Groups

In general, user groups nested in a parent group share the same restricted access times with the parent user group. However, when both the parent and the nested user groups are granted access to the same agent, time restrictions are combined in the same way that times are combined for users in multiple user groups.

For example, suppose that a user is a member of two user groups: Marketing and Sales. Marketing is nested within Sales, and both groups have access to the same restricted agent. If the restricted access time for members of Marketing is from 8:00 a.m. to 5:00 p.m. and the restricted access time for members of Sales is from 9:00 a.m. to 7:00 p.m., a member of Marketing can access the restricted agent from 8:00 a.m. to 7:00 p.m.

Access to Restricted Agents by Active Directory Groups

Active Directory supports multiple types of groups. When configured to use Active Directory as an identity source, Authentication Manager supports only Universal groups.

When you select an Active Directory group for access on a restricted agent, make sure that you select a Universal group. If you use any other type of Active Directory group, the user may not be able to authenticate. When you view the Active Directory groups from the Security Console, the Security Console displays all groups, regardless of type.

The Security Console cannot display a user's primary Active Directory user group, such as Domain Users. The group appears empty even though it has members.

View User Groups Allowed to Authenticate on a Restricted Agent

Use the Security Console to view user groups that are allowed to authenticate on a restricted agent. User groups directly granted access to the restricted agent are only displayed in the search results. Nested user groups are not displayed.

Procedure

1. In the Security Console, click **Access** > **Authentication Agents** > **Manage Existing**.
2. Click the **Restricted** tab.
3. Use the search fields to find the agent whose user groups you want to view.
4. Click the agent, and select **User Groups with Access**.
5. Click the user group that you want to view, and select **View**.

User Data in an LDAP Directory

Changes made to user data in an LDAP directory can affect authentication and administration of the user when the change in the directory modifies the user's distinguished name (DN), the user's User ID, or both. If a user's DN or User ID is changed, Authentication Manager can no longer find the user in the LDAP directory that was designated as his or her identity source. A user (or a user group) in this state is known as "unresolvable." RSA recommends removing references to unresolvable users and user groups because unresolvable users count against the license user limit if they have assigned authenticators.

How a User Becomes Unresolvable

Unresolvable users are users that can no longer be found in the LDAP directory that was designated as their identity source.

A user becomes unresolvable for any of the following reasons:

- The user is deleted from the LDAP directory.
- The user is moved outside the scope of the base DN of the identity source.
- The user is moved outside the scope of all identity sources.

- The scope of the identity source is narrowed so that it no longer includes the user.
- The Search Filter of the identity source is modified so that it no longer contains the user.
- The user is moved to an identity source in the same physical directory using the delete and add method, and the Unique Identifier is configured to use the default value.
- The user is moved to an identity source in a different physical directory.

Users who become unresolvable are reported as missing from the identity source.

After cleaning up users who have been moved to a different identity source, you re-establish these users in Authentication Manager by enabling them for authentication, or assigning them administrative roles.

Some directory management tools move users by deleting and re-adding them to the directory. In these cases, Authentication Manager cannot find the users after the move when the default Unique Identifier is used. Deleting and adding the user back to the directory creates a new value for ObjectGUID, the default Unique Identifier. To maintain the same value for your users, configure a customized attribute as the Unique Identifier.

How a User Group Becomes Unresolvable

Unresolvable user groups are user groups that can no longer be found in the LDAP directory that was designated as their identity source.

A user group becomes unresolvable for any of the following reasons:

- The user group is deleted from an LDAP directory.
- The user group is moved.
- The scope of the identity source is narrowed so that it no longer includes the user group.
- The Search Filter of the identity source is modified so that it no longer contains the user group.

Manual Cleanup for Unresolvable Users

RSA recommends cleaning up unresolvable users for the following reasons:

- Unresolvable users count against the license user limit. After cleaning up unresolvable users, the count is reduced, and you can register more users in your deployment.
- Tokens assigned to unresolvable users remain assigned to them. After cleaning up unresolvable users, you can assign their tokens to other users.

  If users are moved to an identity source in a different physical directory, reassign the tokens to the same users. You also need to reassign any fixed passcodes, on-demand tokencode settings, and administrative roles that users had prior to being moved.

The manual cleanup process removes the association between the users in an LDAP directory and RSA-specific data in the internal database. For instructions, see Clean Up Unresolvable Users Manually on page 147.

During a manual cleanup, RSA Authentication Manager generates a list of unresolvable users from linked identity sources. You can preview the users affected by the cleanup before removing all references to the users. By default, all unresolvable users in linked identity sources are cleaned up. A manual cleanup does not clean up user groups.

The manual cleanup process applies only to LDAP directory identity sources that are linked to the system. If an identity source is not linked, no users are unresolvable, and no manual cleanup is necessary.

Clean Up Unresolvable Users Manually

You can clean up unresolvable users manually on an as-needed basis. The cleanup process removes the association between the users in an LDAP directory and RSA-specific data in the internal database.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Setup** > **Identity Sources** > **Clean Up Unresolvable Users**.
2. Select the name of the identity source that you want to clean up, or select **All**.
3. In the **Grace Period** field, do one of the following:
   - If you want to clean up users who have been unresolvable for more than the specified number of days, select the checkbox.
   - If you want to clean up users immediately when they are found to be unresolvable, clear the checkbox.

   The Grace Period is used to prevent cleanup for any users and user groups that may have been mistakenly removed from the directory or moved to an OU out of scope of the identity source. You can specify how many days the users must be unresolvable before they are cleaned up, and take corrective action beforehand. By default, this field is enabled to clean unresolvable users after seven days.
4. Click **Next**.

   The list of unresolvable users builds and displays in the Preview panel when complete. The Preview displays up to 500 results at a time. If you see exactly 500 results, you may need to clean up additional users. In this case, RSA recommends running a report based on the Users and User Groups Missing From Identity Source report template to view a complete list of unresolvable users. For more information, see Add a Report on page 332.
5. In the Preview pane, review the list of users. Click the column names to sort the list. If the list is empty, there are no unresolvable users.
6. Click **Clean Up Now**.

Important: You cannot cancel the cleanup. When you click **Clean Up Now**, all associations between the users and objects in the internal database are removed.

When the clean up process completes, the Configure Settings pane displays a success message.

Scheduling Cleanup for Unresolvable Users and User Groups

The scheduled cleanup job deletes references to unresolvable users and user groups from the internal database.

The scheduled cleanup job runs against linked and unlinked identity sources and can be configured to run on a daily, weekly or monthly basis. The job is canceled if the number of unresolvable users exceeds the specified Cleanup Limit. The limit helps avoid accidentally disassociating a large number of users from their authentication data if changes are made to these users directly in an LDAP directory. The default limit is 50 users.

RSA recommends cleaning up unresolvable users for the following reasons:

- Unresolvable users count against the license user limit. After cleaning up unresolvable users, the count is reduced, and you can register more users in your deployment.
- Tokens assigned to unresolvable users remain assigned to them. After cleaning up unresolvable users, you can assign their tokens to other users.

  If users are moved to an identity source in a different physical directory, reassign the tokens to the same users. You also need to reassign any fixed passcodes, on-demand tokencode settings, and administrative roles that users had prior to being moved.

RSA recommends scheduling a cleanup for the following reasons:

- Before deleting an identity source

  To delete an identity source you must first unlink the identity source from the system, run the scheduled cleanup, and use the Operations Console to delete the identity source. The scheduled cleanup deletes all references to users and groups from the internal database that were associated with the unlinked identity source. For more information, see the Security Console Help topic "Unlink Identity Sources from the System."

  If you need to temporarily unlink an identity source (for example to add an associated Global Catalog) do not run a cleanup job. When you relink the identity source, all users from that identity source will be resolvable again. Authentication Manager will be able to locate those users as it did before the unlink operation.
- After narrowing the identity source scope

  After you narrow the scope of an identity source, some users and user groups may become unresolvable and unable to authenticate. You must run the scheduled cleanup job after editing the identity source. When you run the job, make sure that you disable the Grace Period and Cleanup Limit if they are set, and re-enable those settings after this single cleanup runs.

You can use the following options to modify the cleanup process:

Cleanup Limit. The Cleanup Limit cancels the automated cleanup when more than the specified number of unresolvable users are found in the database. This limit helps prevent accidentally disassociating a large number of users from their authentication data if changes are made to these users directly in the identity source.

When the cleanup is canceled, you can run the "Users and User Groups Missing From the Identity Source" report to see a list of unresolvable users. The list may contain users that you do not want to clean up. For example, these may be users who are mistakenly deleted from the directory or moved from location to another in the same directory.

Grace Period. The Grace Period restricts the cleanup to users who have been unresolvable for more than a specified number of days. Specifying a Grace Period gives you time to correct any unintended changes to users in the directory. For example, some users may have been deleted or moved accidentally.

Use the Grace Period to avoid cleaning up users when any of the following actions occur accidentally in linked identity sources:

- A user is deleted.
- A user is moved to an organizational unit (OU) outside of any identity source in your deployment.
- A user's name is changed.

Schedule a Cleanup Job

The schedule cleanup job repairs or deletes references to unresolvable users and user groups from the internal database. Unresolvable users are users whose designated identity source no longer contains any record of the user. When a user is moved to another identity within the same LDAP directory, the cleanup job repairs the references.

Procedure

1. In the Security Console, click **Setup** > **Identity Sources** > **Schedule Cleanup**.
2. To schedule the cleanup job to run, under **Cleanup Status**, select **Enable scheduled cleanup of unresolvable users and user groups from linked identity sources, and all users and user groups from unlinked identity sources**. By default, this checkbox is cleared, and the field is disabled.

   If you disable a cleanup that you have configured, the next time that you access this page, all of the fields are reset to the default values and all of the configuration changes that you made previously are lost.

3. In the **Cleanup Limit** field, do one of the following:
   - Leave the default.

     By default, this field is enabled and the limit is 50 users. The limit must be a positive number greater than zero. The cleanup is canceled when more than a specified number of unresolvable or unlinked user references are found. The limit helps avoid accidentally disassociating a large number of users from their authentication and authorization data if changes are made to these users directly in their identity source.
   - If you want to clean up all unresolvable users and user groups, clear the **Cleanup Limit** checkbox.

   Important: Before you delete an identity source that is unlinked, clear this checkbox when you run the cleanup.

4. In the **Grace Period** field, do one of the following:
   - Leave the default.

     By default this field is enabled and set to seven days. This value must be a positive number greater than zero. This field is ignored for unlinked identity sources. Only users who have been unresolvable for more than the specified number of days are cleaned. This field helps prevent the cleanup of users that may have been mistakenly removed from the directory or moved to an OU out of scope of the identity source. You have an opportunity to take corrective action before the cleanup.
   - If you want to clean users immediately when they are found to be unresolvable, clear the **Grace Period** checkbox.

   Note: The Grace Period does not apply to user groups. User groups are deleted immediately after they are found to be unresolvable.

5. If the Cleanup Limit is exceeded and the cleanup is canceled, run the Users and User Groups Missing From Identity Source report to determine which users you need to clean up. After viewing the report, you can specify a limit that allows the cleanup to run successfully or perform a manual cleanup. For more information, the Security Console Help topic "View a Report Template" and Scheduling Cleanup for Unresolvable Users and User Groups on page 148.

   Note: When you use Schedule Cleanup before deleting an unlinked identity source, make sure you clear the Cleanup Limit checkbox so that no limit applies. Also clear this checkbox when you run this job after narrowing the scope of an identity source.

6. Under Schedule, use the **Start** field to select the date you want the cleanup to run for the first time.
7. Use the **Frequency** fields to select how often, and on which days, you want the cleanup to take place.
8. Use the **Run Time** field to specify what time you want the cleanup to run.

9. Use the **Expire** fields if you want the settings to expire on a specific date. If you do not select a date, the settings do not expire.
10. When you are done scheduling cleanup, click **Save**.

Moving Users in an LDAP Directory

When a user is moved within an LDAP directory that is a linked identity source, Authentication Manager can detect the move and update the user when any of the following events occur:

- A scheduled cleanup is run.
- An administrator runs a manual cleanup of all identity sources or of the identity source containing the user.
- An administrator modifies a user's record in the Security Console.
- The user attempts to authenticate.

Next Steps

After cleaning up users who have been moved to a different identity source, you need to reestablish these users in Authentication Manager by assigning administrative roles and enabling them for authentication.

Moving Users within an Identity Source

If a user is moved within an LDAP directory and remains within the same identity source, the user can still authenticate and be administered unless the user's Unique Identifier changes. Some directory management tools change the Unique Identifier because the move is performed by deleting and re-adding the user to the directory.

In these cases, Authentication Manager cannot find the users after the move because deleting and adding the user back to the directory creates a new value for the attribute designated as the default Unique Identifier (ObjectGUID in Active Directory or nsUniqueID in Oracle Directory Server). To avoid this situation, configure a customized attribute as the Unique Identifier.

Moving Users Outside the Scope of the Original Identity Source

If a user is moved within an LDAP directory and is outside the scope of the original identity source, the user can still authenticate and be administered as long as the following criteria are met:

- The user still resides in the same physical directory.
- An identity source is configured in Authentication Manager that meets the following criteria:
  - The identity source exists in the same physical directory as the original identity source.
  - The identity source encompasses the user's new DN.
  - Both identity sources use the same attribute for the User ID.
  - Both identity sources use the same attribute for the Unique Identifier.

While you can configure the identity source after the user is moved, a user who attempts to authenticate before the identity source is configured is denied access for an hour after the authentication attempt.

- The method used to move the user must not delete and re-add the user when the identity source is configured to use the default Unique Identifier.

If these criteria are not met, the move causes the user to become unresolvable. For information about how to manage an unresolvable user, see Manual Cleanup for Unresolvable Users on page 146.

Impact of Moving a User Within an LDAP Directory

Moving a user in the directory affects Authentication Manager in the following ways:

- The user's first authentication attempt might fail. This failed attempt does not count against the user lockout policy.

  To minimize the number of users who experience this initial authentication failure, schedule a periodic cleanup. For instructions, see Schedule a Cleanup Job on page 149.

- When replication is out of sync, or a replica instance is unavailable, there can be a delay in updating the system with the user's new identity source. In these cases, the user is denied access until replication is restored.

- For users who authenticate with aliases, group associations are not retained when the user is moved to a different identity source.

  The user alias, shell, and any RADIUS profile assigned to the alias are retained from the old identity source.

  You must reassociate the alias, shell, and any RADIUS profile to a group in the new identity source. To do this, edit the alias in the user's authentication settings, and select a group in the new identity source to associate the alias with the group.

  For more information on updating authentication settings, see Manage User Authentication Settings on page 123.

- The ability to authenticate through restricted agents can be lost when the user is moved to a different identity source.

  If a user's distinguished name (DN) changes on the Oracle Directory Server/Sun Java System Directory Server, the user is removed from all LDAP group memberships. If this user belonged to a group with permission to authenticate on a restricted agent, the user can no longer authenticate through the restricted agent.

  If the user is a member of a group in the new identity source with permission to authenticate on a restricted agent, you do not need to take any action. If the user is not a member of a group in the new identity source with permission to authenticate on a restricted agent, you must add the user to the group in the directory location that is specified as the new identity source, and associate the group with the restricted agent.

  When group membership is changed directly in an LDAP directory, Authentication Manager may not immediately recognize these changes because group membership is cached. As a result, Authentication Manager sees the user as a member of the group in the original identity source until the cached value expires, typically after 10 minutes.

Users can authenticate through a restricted agent for a short time after they move, even though they are removed from all groups associated with the restricted agent. To ensure that the change in group membership is recognized immediately, flush the cache after making the changes in the directory. For more information, see Flush the Cache on page 369.

- The user can be modified by a different administrator.

  If the original administrator does not have privileges on the new identity source, he or she will no longer have the ability to administer the user. However, an administrator with privileges on the new identity source is able to administer the user.

- When a user is moved to a different identity source, the Security Console recognizes the user in the new identity source immediately.

  If administrators need to address any issues arising from the move, instruct them to search for the user in the new identity source, not the old identity source.

Modifying a User in an LDAP Directory

When a user's User ID is changed in an LDAP directory, Authentication Manager automatically detects the change and updates the user when any of the following events occur:

- A scheduled cleanup is run.
- An administrator runs a manual cleanup of all identity sources or of the identity source containing the user.
- An administrator modifies a user's record in the Security Console.
- The user attempts to authenticate using the old User ID.

Changing the User ID in the directory affects Authentication Manager in the following ways:

- The first authentication attempt made by the user can fail.

  If a user attempts to authenticate before another event has updated the User ID, he or she may experience an authentication failure. If users are denied access, instruct them to use the old User ID for the first authentication attempt after the change, and then use the new User ID for all subsequent authentication attempts.

  If User ID is mapped to a user's email, the initial authentication failure may not occur.

- The Security Console recognizes the new User ID immediately.

  If administrators need to deal with any issues arising from the User ID changing, instruct them to search for the user by the new User ID, not the old User ID.

  The User ID is updated and the user can authenticate using the new User ID after an administrator manages the user, for example, the administrator views the user record.

- The ability to authenticate through restricted authentication agents can be lost when default settings are used in Sun Java System Directory Server/Oracle Directory Server Enterprise Edition identity sources.

  The default settings in Sun Java System Directory Server/Oracle Directory Server Enterprise Edition use the uid attribute as the Naming Attribute. The default settings in Authentication Manager map User ID to the uid attribute. With these settings configured for Sun Java System Directory Server/Oracle Directory Server Enterprise Edition identity sources, any modification to the User ID (uid) changes the user's distinguished name, which removes all LDAP group memberships for the user.

If a user whose DN changed belonged to a group with permission to authenticate on a restricted agent, the user can no longer authenticate through the restricted agent. To enable this user to authenticate through the restricted agent, you must re-add the user to the group associated with the restricted agent.

Modifying Group Membership in an LDAP Directory

In order to optimize performance and minimize traffic between Authentication Manager and an LDAP directory, Authentication Manager caches information about user group memberships. When a user's group membership is changed in an LDAP directory, Authentication Manager cannot acknowledge the change until the cache is refreshed. As a result, these changes take effect after the cache refresh interval has elapsed. In the time between the change and the refresh, you may see the following behaviors:

- A user added to a group that has access to a restricted agent cannot authenticate to the restricted agent.
- A user who has been removed from a group that has access to a restricted agent can still authenticate to the agent.

You can flush the cache immediately using the Operations Console. For more information, see Flush the Cache on page 369.

For more information on configuring the cache, see the Security Console Help topic "Configure the Cache."

7 Administering RSA Authentication Manager

Delegated System Administration

The Super Admin and the Operations Console administrators are responsible for maintaining the components of the Authentication Manager system.

Super Admin

The Super Admin is the only role with full administrative permission in all security domains in the deployment. The Super Admin creates other administrators, the security domain hierarchy, and links identity sources to the deployment.

Operations Console Administrators

An Operations Console administrator is an administrative account that grants access to the Operations Console. Operations Console administrators can perform important command line utility procedures, including recovering a Super Admin account in the event that no Super Admin is able to access the system.

Like the Super Admin administrative role, an Operations Console administrator account should only be granted to the most trusted administrators. Many Operations Console tasks require both Super Admin and Operations Console administrator credentials.

You create an initial Operations Console administrator account during Quick Setup, and you can create and manage Operations Console administrators in the Security Console. Only a Super Admin can view or manage an Operations Console administrator account. Likewise, only a user with Operations Console administrator credentials can restore a Super Admin.

Authentication Manager stores Operations Console administrator accounts separately from the user database. User password policies do not apply to Operations Console administrators.

System Administrator Accounts

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

- Authentication Manager Administrator Accounts
- Appliance Operating System Account

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

Authentication Manager Administrator Accounts

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

Name	Permissions	Management
Super Admin	Super Admins can perform all administrative tasks in the Security Console with full administrative permission in all security domains in the deployment.	Any Super Admin can create other Super Admin users in the Security Console. An Operations Console administrator can recover a Super Admin account if no Super Admin can access the system.
Operations Console administrator	Operations Console administrators can perform administrative tasks in the Operations Console. Operations Console administrators also use command line utilities to perform some procedures, such as recovering the Super Admin account. Command line utilities require the appliance operating system account password. **Note:** Some tasks in the Operations Console also require Super Admin credentials. Only Super Admins whose records are stored in the internal database are accepted by the Operations Console.	Any Super Admin can create and manage Operations Console administrators in the Security Console. For example, you cannot recover a lost Operations Console administrator password, but a Super Admin can create a new one. Operations Console administrator accounts are stored outside of the Authentication Manager internal database. This ensures that if the database becomes unreachable, an Operations Console administrator can still access the Operations Console and command line utilities.

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

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

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

Appliance Operating System Account

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

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

You can access the operating system with Secure Shell (SSH) on a hardware appliance or a virtual appliance, or you can use the VMware vSphere Client on a virtual appliance. Before you can access the appliance operating system through SSH, you must use the Operations Console to enable SSH on the appliance. For instructions, see Enable SSH on the Appliance on page 403.

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

Add a Super Admin

Each deployment must have at least one Super Admin. You can assign another user as a Super Admin to share administrative responsibilities. You add a Super Admin in the Security Console.

Before You Begin

You must be a Super Admin to perform this procedure.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user that you want to assign a Super Admin role.
3. Click the user, and select **Administrative Roles**.
4. Click **Assign Role**, click **SuperAdminRole**, and click **Assign Role**.

Add an Operations Console Administrator

An Operations Console administrator is a user with permissions to perform administrative tasks in the Operations Console and to run some command line utilities. You create an Operations Console administrator in the Security Console.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Administration** > **Manage OC Administrators.**
2. Click **Add New**.
3. In the **Create User ID** field, enter the Operations Console administrator’s User ID. The User ID must be between 1 and 255 characters and may only contain characters in the basic ASCII character set, excluding space, @, and ~.
4. In the **Create Password** field, enter the Operations Console administrator’s password. The password must be between 8 and 32 characters, contain at least 1 alphabetic character, at least 1 special character, and may only contain characters in the basic ASCII character set, excluding space, @, and ~. The password can not match the corresponding user ID.
5. In the **Confirm Password** field, reenter the password.
6. Click **Save**.

Note: It can take from fifteen to thirty minutes for a new Operations Console administrator’s account to replicate to a replica instance.

Change an Operations Console Administrator's Password

Any Super Admin can change an Operations Console administrator password in the Security Console. You cannot recover a lost Operations Console administrator password, but a Super Admin can create a new one.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Administration** > **Manage OC Administrators.**
2. Next to the Operations Console administrator whose password you wish to modify, click **Change Password**.

3. In the **Create New Password** field, enter the Operations Console administrator’s new password.

   The password must be between 8 and 32 characters, contain at least 1 alphabetic character, at least 1 special character, and may only contain characters in the basic ASCII character set, excluding space, @, and ~. The password may not match the corresponding user ID.

4. In the **Confirm New Password** field, reenter the new password.
5. Click **Save**.

Note: It can take from fifteen to thirty minutes for changes to an Operations Console administrator’s account to replicate to a replica instance.

Operations Console

You use the Operations Console to add or manage the following Authentication Manager components:

- Identity sources
- Instances
- Certificates
- Web tiers
- Network settings

You also use the Operations Console to back up and restore deployment data to fix an unresponsive instance.

Log On to the Operations Console

Operations Console administrator credentials are required to log onto the Operations Console. An initial Operations Console administrator account is created during Quick Setup, and additional Operations Console accounts can be created by a Super Admin.

Navigation works best if you use the Operations Console menus and buttons instead of using the browser’s navigation controls.

Before You Begin

You must have Operations Console administrator credentials.

Procedure

1. Open the browser.
2. Go to the following URL:

   ```
   https://fully qualified host
   name:7072/operations-console/
   ```

   where *fully qualified host name* is the FQHN of the appliance.

Session Lifetime Limits

A session lifetime defines a session duration. Session lifetime is an important security feature because it prevents administrators from keeping sessions open indefinitely, leaving them vulnerable to unauthorized access. When you edit a session lifetime, you can change settings such as the maximum session lifetime, and how long a session can be idle before the system closes it.

Each time an administrator logs on to the Security Console, Operations Console, or Self-Service Console, the following sessions are created:

- Logon Session
- EAP32 Session Lifetime
- Console and Command API Session

Up to ten administrators can be logged on at the same time.

You can create different sets of session attributes for the primary instance and the replica instance.

Logon Session

Logon Session settings control the lifetime for sessions that are abandoned or have not completed the authentication process. These sessions affect the following types of logon sessions:

- Security Console (administrators)
- Operations Console (administrators)
- Self-Service Console (non-administrative)
- Users who are authenticating through risk-based authentication (non-administrative)

The defaults for these settings are three minutes idle time-out and eight minutes of total lifetime.

EAP32 Session Lifetime

Extensible Authentication Protocol (EAP) Session settings control the initial session lifetime for EAP32 Sessions.

Console and Command API Session

The Console and Command API Session settings control the authenticated or active sessions for administrators in the web-based consoles or the command application programming interface (API). The default settings are 30 minutes idle time-out and 8 hours of total lifetime.

The Authentication Manager web-based administrative consoles are the Security Console and the Operations Console. The command API is used by programmers, web developers, or systems engineers responsible for developing custom software applications that interact with the Authentication Manager system. For information on the command API, see the *RSA Authentication Manager 8.1 Developer’s Guide*.

Types of Session Lifetime Limits

Session settings apply to the logon pages for the web-based administrative consoles, the command API interface described in the *RSA Authentication Manager 8.1 Developer’s Guide*, and the risk-based authentication (RBA) logon attempts by end users. When a session times out or reaches the maximum lifetime, the logon page is redisplayed, and the user must log on again.

You can configure the following settings for sessions:

Time-out. The length of time that a session can be inactive before being terminated. The default setting is 30 minutes.

Maximum Lifetime. The maximum length of an session. When the console session reaches its session lifetime, the session is terminated and the administrator is logged off, regardless of whether the session is active. The default setting is eight hours.

These settings are independent of session inactivity. For example, if a console and command API session lifetime is eight hours, an administrator is automatically logged off after eight hours, even if there have been no periods of inactivity during the session.

Only a Super Admin can modify the console and command API session settings.

Edit Session Lifetime Settings

When you edit a session lifetime, you can change settings such as the maximum session lifetime, and the amount of time a session can be idle before the system closes it.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Under Console & Session Settings, click **Session Lifetime**.
3. Click the session type that you want to edit, and select **Edit**, from the context menu.
4. Under **Session Lifetime Settings**, do the following:
   a. Select **Time out idle sessions**, and enter the time-out duration, if you want to time out sessions after a period of inactivity.
   b. Select **Limit session lifetime**, and enter the maximum lifetime of a session.
5. Click **Save**.

Updating Identity Source Properties

Occasionally it is necessary to update the identity source properties after the identity source has been linked to Authentication Manager. The directory configuration mapping section of the identity source properties makes it possible for fields in the identity source to be used by the internal database. Use the Operations Console to edit directory configuration mapping.

You can also create custom user attributes with the Security Console. Use the Security Console to edit identity attribute definitions for custom user attributes. For information, see the Security Console Help topic “Edit Identity Source Attribute Mappings.”

Procedure

1. If you plan to change the User ID mapping, unlink the identity source from Authentication Manager. For instructions, see Unlink Identity Sources from the System on page 162.
2. Edit the identity source properties. For instructions, see Edit an Identity Source on page 163.
3. If you unlinked the identity source to change the User ID mapping, re-link the identity source to Authentication Manager after you have finished editing. For instructions, see Link an Identity Source to the System on page 164.

Unlink Identity Sources from the System

When you link an identity source to the system, all users and user groups in the identity source can be viewed and managed through the Security Console. When you unlink an identity source, those users and user groups can no longer be managed through the Security Console.

When you re-link the identity source, all users from that identity source will be resolvable again. Authentication Manager will be able to locate those users as it did before the unlink operation.

Before You Begin

You must be a Super Admin.

Note: You cannot unlink the internal database and the identity source to which you belong.

Procedure

1. In the Security Console, click **Setup** > **Identity Sources** > **Link Identity Source to System**.
2. From the list of linked identity sources under **Link Identity Source**, select the identity source that you want to unlink, and click the left arrow to unlink it.
3. Click **Save**.

4. On the Unlink Identity Source Confirmation screen, select **Yes, unlink the identity source(s)**.
5. Click **Unlink**.

Next Steps

Edit the identity source user attribute mappings. For instructions, see Edit an Identity Source on page 163.

Edit an Identity Source

You can edit identity source properties before or after the identity source is linked to the system. You must unlink the identity source from Authentication Manager before you edit User ID mapping.

Important: Use extreme caution when editing identity source properties. If you need to narrow the scope of an identity source or remap the User ID, see Identity Source Properties on page 101.

Before You Begin

You must be a Super Admin.

Procedure

1. In the primary instance Operations Console, click **Deployment Configuration** > **Identity Sources** > **Manage Existing**.
2. When prompted, enter your Super Admin User ID and password.
3. Click the identity source that you want to edit, and select **Edit**.
4. Click the **Connection(s)** tab or the **Map** tab to view the properties. Make any necessary changes to the fields. For a description of each field, see Identity Source Properties on page 101.
5. Click one of the following:
   - **Reset**. If you have not saved your edits, you can click **Reset** to reset the identity source as it was before you began editing.
   - **Save**. Saves your changes, and displays a confirmation message.
   - **Save and Finish.** Saves your choices, returns you to the list of identity sources, and displays a confirmation message.

Next Steps

If your changes cause a change in the set of users or groups, you may need to unlink the identity source, perform a manual cleanup, and relink the identity source. For more information, see User Data in an LDAP Directory on page 145.

Link an Identity Source to the System

You must link all LDAP directory identity sources to the system. After linking, all users in the identity source can be viewed and managed through the Security Console. Users are visible in the top-level security domain by default, but you can move them to other security domains as necessary. Additionally, you can configure the system to place users from the identity source into a specific security domain automatically. For more information, see Default Security Domain Mappings on page 43.

Before You Begin

- You must be a Super Admin.
- If you link an Active Directory Global Catalog, you must also link each identity source that replicates user data to that Global Catalog. For example, if identity sources IS1 and IS2 replicate information to Global Catalog GC1, and you link GC1 as an identity source, you must also link IS1 and IS2 to the system.

Procedure

1. Log on to the Security Console as Super Admin.
2. Click **Setup** > **Identity Sources** > **Link Identity Source to System**.
3. From the list of available identity sources, select the identity sources that you want to link, and click the right arrow.
4. Click **Save**.

Verify the LDAP Directory Identity Source

To verify that you have successfully added and linked an identity source, you can view the users and groups from that identity source through the Security Console.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the appropriate identity source, and click **Search**.
3. View the list of users from the LDAP directory identity source.

Certificate Management for Secure Sockets Layer

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

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

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

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

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

Console Certificate

When you deploy an instance of RSA Authentication Manager, communication between the browser and the Security Console, Operations Console, and Self-Service Console is secured by a long-lived secure socket layer (SSL) certificate. This certificate is signed by an internal RSA certificate authority (CA). Because this CA is self-signed, your browser may present a warning message that the default certificate cannot be verified.

Replacing the console certificate with a certificate issued by a third-party CA is optional. However, you might need to replace the console certificate for the following reasons:

- Your network policy requires that you use certificates issued by another CA.
- Your existing certificate is expired.

In the certificate chain you obtain from a third-party CA, each X.509 version 3 CA certificate must have the Basic Constraints extension CA field set to TRUE. If any X.509 version 3 CA certificate in the chain does not have the Basic Constraints extension properly set, Authentication Manager rejects the certificate. If this happens, contact the certificate authority to resolve the issue.

A certificate issued by a third-party CA may be valid for only 1 to 2 years. You must ensure that a third-party certificate is replaced before it expires.When the console certificate expires, you cannot start the Authentication Manager services after they are stopped.

If you stop the services on an instance with an expired certificate, you must replace the expired certificate with the default certificate that was installed when the instance was deployed. For instructions, see Replace an Expired Console Certificate on page 169.

For an overview of the replacement process, see Replacing the Console Certificate on page 165.

Replacing the Console Certificate

Complete this procedure to replace the existing secure socket layer (SSL) certificate that secures communication between the browser and the Security Console, Operations Console, and Self-Service Console.

Perform these tasks on any instance where you want to replace the existing SSL certificate.

Before You Begin

- You must be an Operations Console administrator.
- Consult your certificate authority (CA) to ensure that you have all of the required information for your certificate signing request (CSR).

Procedure

1. Generate a CSR by doing one of the following:
   - Use the Operations Console to have RSA Authentication Manager generate a key pair and a CSR.For instructions, see Generate a Certificate Signing Request Using the Operations Console on page 166.
   - Use a third-party tool of your choice to generate a key pair and a CSR.
2. Submit the CSR to your CA, and request an SSL server certificate.
   - If your CA does not provide an option for an SSL server certificate, make sure that your certificate includes the key-usage extension with Key Encipherment selected.
   - The key algorithm must be RSA Public Key.
3. Download the certificate file (either .cer or .p7b) from your CA. The certificate file typically contains the full signing chain of the certificate.
   - The issued certificate's subject must contain a common name (CN) whose value is the fully qualified hostname (FQHN) of the instance where you want to replace the current SSL certificate.
   - If the certificate file does not contain all the certificates in the signing chain, you must download the full signing chain of the certificate, either in a single file or individually.
4. If you generated a CSR using a third-party tool, create a PKCS#12 file (either .pfx or .p12) that includes the certificate file from your CA and the private key for the new certificate.
5. Import a Console Certificate on page 167 .
6. Activate a New SSL Console Certificate on page 168.

Generate a Certificate Signing Request Using the Operations Console

To replace a console certificate with a certificate by a third-party certificate authority (CA), you must generate a certificate signing request (CSR) and submit it to the CA. You may need to replace the console certificate for any of the following reasons:

- Your network policy requires that you use certificates issues by another CA.
- Your existing certificate is expired.

You submit a CSR to a CA to obtain a signed certificate. Use the Operations Console to generate a CSR.

Before You Begin

- You must be an Operations Console administrator.
- Consult your CA to ensure that you have all of the required information for the CSR.

Procedure

1. In the Operations Console, click **Deployment Configuration** > **Certificates** > **Console Certificate Management**.
2. In the Console Certificate Management page, click **Generate CSR**.
3. In the Generate Certificate Signing Request page, under **Certificate Basics**, enter the requested information.

   Depending on your CA, you are asked to supply some or all of the following information:

   - **(Required) Alias.** The name of this certificate. This name appears under **Alias** on the Console Management page. Only a-z, A-Z, space, and comma characters are allowed.
   - **Country Name.** The country where your organization is located. The value supplied to your CA is the two-letter country code.
   - **State or Province Name.** The state or province where your organization is located.
   - **City or Locality Name.** The city or town where your organization is located.
   - **Organization Name.** The legal name of your organization.
   - **Organizational Unit Name.** The division of your organization that is ordering the certificate, for example, engineering, accounting, marketing, and so on.
   - **E-mail Address.** An official e-mail address for verification, for example, administrator@mycompany.com.
4. Click **Generate File**.
5. In the Download File page, click **Download**.
6. Follow the browser prompts to save the CSR file.
7. In the Download File page, click **Done**.

Import a Console Certificate

After you import all of the certificates in the signing chain from your certificate authority (CA), you can replace the existing secure socket layer (SSL) certificate with a new certificate.

Before You Begin

- You must be an Operations Console administrator.
- Generate a certificate signing request (CSR), and submit the CSR to your CA.
- Download the CA root certificate.

- Download any other certificates that are part of the signing chain if the SSL certificate does not contain the complete chain.
- Download the new SSL certificate.

Procedure

1. In the Operations Console, click **Deployment Configuration** > **Certificates** > **Console Certificate Management**.

   Beginning with the root certificate, perform the following steps for each certificate in the signing chain.

2. In the Console Certificate Management page, click **Import Certificate**.
3. In the Import Certificate page under **Certificate Basics**, do one of the following:

   For a console certificate made in response to a CSR from the Operations Console:

   - In the **Import Certificate** field, browse to the location where the certificate is stored. This file contains either a CA root certificate or the SSL certificate from the CA.
   - For **Type of Certificate to Import**, select **PKCS #7 (*.cer or *.p7b)**.

   For a console certificate made in response to a CSR from a certificate tool of your choice:

   - In the **Import Certificate** field, browse to the location where the certificate is stored. This file contains one or more certificates and the private key for the new certificate. Do one of the following:
     - If the SSL certificate file contains the complete certificate chain up to the CA root certificate, then import the PKCS #12 file. In the **Password** field, enter the password for the PKCS#12 file.
     - If the SSL certificate file does not contain the complete certificate chain up to the CA root certificate, then import each of the CA certificates in the certificate chain in a PKCS #7 file before importing the SSL certificate in a PKCS #12 file. In the **Password** field, enter the password for the PKCS#12 file.

4. Click **Import**.

Next Steps

Activate the new certificate to replace the existing SSL certificate. For instructions, see Activate a New SSL Console Certificate on page 168.

Activate a New SSL Console Certificate

When you deploy an instance of RSA Authentication Manager, communication between the browser, and the Security Console, Operations Console, and Self-Service Console is secured by a long-lived secure socket layer (SSL) certificate. If you replace the console certificate, and in turn, import a new certificate, you must activate the certificate to make it available for use.

To activate a secure socket layer (SSL) certificate, the certificate must have a subject field that contains a common name (CN) with a value equal to the fully qualified hostname (FQHN) of the instance you are administering.

Before You Begin

- You must be a Super Admin and an Operations Console administrator.
- Import the SSL certificate that you want to activate. See Import a Console Certificate on page 167.

Procedure

1. In the Operations Console, click **Deployment Configuration** > **Certificates** > **Console Certificate Management**.
2. In the Console Certificate Management page, under Alias, click the name of the new SSL certificate.
3. From the context menu, select **Activate**.
4. In the Activate Certificate Confirmation page, review the **Certificate Details** to ensure that this is the certificate that you want to activate.
5. Select **Yes, make this the active certificate**, and click **Activate Certificate**.

   After the certificate is activated, the appliance services automatically restart to complete the activation process. This can take several minutes.
6. After all the services start, log on to the Operations Console.
7. In the Operations Console, click **Deployment Configuration** > **Certificates** > **Console Certificate Management**, and make sure that the new certificate status is **Active**.

Replace an Expired Console Certificate

If you replace the original console certificate with a certificate issued by a third-party certificate authority (CA), you must make sure that this third-party certificate is replaced before it expires. When the console certificate expires, you cannot start the Authentication Manager services after they are stopped.

If you stop Authentication Manager services on a deployment with an expired certificate, perform the following procedure. and then start the services.

Procedure

1. Use an SSH client (or the VMware vSphere client on a virtual appliance) to log on to the appliance with the User ID **rsaadmin** and the current operating system password.
2. Change the directory to utils. Type:

   ```
   cd /opt/rsa/am/utils
   ```

   and press ENTER.

3. Run the following command to change the console certificate from the third-party certificate to the original certificate. Type the following, and press ENTER:

   ```
   ./rsautil reset-server-cert -u oc_admin_UserID
   -p oc_admin_password
   ```

   where:

   - *oc_admin_UserID* is the user name for an Operations Console administrator
   - *oc_admin_password* is the Operations Console administrator's password

Next Step

Start the Authentication Manager Services. For instructions, see Manage RSA Authentication Manager Services Manually on page 406.

Licenses

Each Authentication Manager deployment must have a license installed. The license grants permission to use the Authentication Manager appliance. RSA Authentication Manager 8.1 supports the use of an existing version 8.0 license, a new version 8.1 license, or a combination of version 8.0 and 8.1 licenses.

These are the license types:

Base Server. A permanent license allowing 1 primary instance and 1 replica instance of Authentication Manager.

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

Each license type limits the number of instances of Authentication Manager that can be installed. User limits are based on the customer's usage requirements.

For example, a customer with 10,000 employees may purchase a license for 11,000 users in order to accommodate current employees and to allow for future hiring.

It is important to know:

- You can install multiple licenses.
- The Account ID must be the same for all licenses.
- The License ID, sometimes referred to as the Stack ID, must be unique for each license. You cannot install the same license twice.
- Only users with assigned authenticators count against the license limit. Users with multiple authenticators only count once.
- The Security Console displays warning messages as you approach your user limit. A message is displayed when you exceed 85, 95, and 100 percent of the user limit.
- The system updates the user counts every hour and each time that a user views the license status in the Security Console.

The following table shows the attributes for each license type.

License Feature	Base Server	Enterprise Server
Users with Assigned Authenticators	Specified by customer at time of purchase	Specified by customer at time of purchase
Number of instances	2[1]	16 (1 primary and 15 replica instances)
RBA/ODA	Optional	Optional
Business Continuity	Optional	Optional
RADIUS	Yes	Yes
Offline Authentication	Yes	Yes
Tokens	Yes	Yes
Self-Service	Yes	Yes
Authenticator Provisioning	No	Yes

[1] Licenses with a two-instance limit allow a third instance for disaster recovery situations.

The business continuity option allows you to temporarily enable more users to use RSA SecurID authentication than your license normally allows. RSA recommends that you enable the users created with the business continuity option to receive on-demand tokencodes so that you do not have to assign and deliver tokens to them. However, if you want, you can assign them RSA SecurID tokens.

If you need more users enabled for a specific feature, you must obtain an additional license from RSA.

For instructions, see Install a License and View Installed Licenses on page 172.

Install a License

You must install a new license when you want to do either of the following tasks:

- Upgrade from an evaluation license to a base or enterprise license.
- Upgrade the limits and features of an existing license.

When you purchase a license, you receive a .zip file containing the XML license file. You must install the XML license file through the Security Console.

When you install a new license, the License Status page displays the combined limits and features of all installed licenses.

Before You Begin

- You must be a Super Admin.
- When you upgrade from an evaluation license, you must uninstall the evaluation license before installing the new license. For more information, see the Security Console Help topic "Uninstall a License."
- The license version must be compatible with the current RSA Authentication Manager version.
- The license serial number must be the same as all other existing licenses in the deployment.
- The License ID, or Stack ID, must be unique among all licenses.

Procedure

1. Extract the license XML file from the .zip file.
2. In the Security Console, click **Setup** > **Licenses** > **Add New**.
3. Browse to the XML license file that you want to install, and select it.
4. Click **Next**.
5. Click **Install**.

   The License Status page displays the combined limits and features of all installed licenses.

View Installed Licenses

Viewing your license allows you to see the details about the license features, limits, and status. One important feature is the number of users that your license allows.

Users with assigned authenticators count against the license limit. Users with assigned authenticators that are disabled or expired also count against the license limit. Users with multiple authenticators only count once.

RSA Authentication Manager 8.1 supports the use of an existing version 8.0 license, a new version 8.1 license, or a combination of version 8.0 and 8.1 licenses.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Setup** > **Licenses** > **Status**.

   The License Status page in the Security Console provides the following information about all of the installed licenses:

   Status. Indicates the status of the license with respect to user limits and product features. Valid values are OK, Approaching Limit, or Limit Exceeded.

   License Features. Indicates the name of a feature that is enabled by the license.

   Limit. Indicates the maximum number of users who can use this feature. This field is not applicable to features that do not include a licensed limit, such as Self-Service.

Actual. For features that include a limit, such as the number of users with assigned authenticators, this field indicates the actual number of users who are using this feature and count against the license limit. For features that do not include a limit, such as Self-Service, this field indicates whether the feature is available with the license.

2. Click **View Installed Licenses**.
3. On the Installed Licenses page, click a license ID, and select **View** to view the following information for that license:

   License Details. Detailed information on the license, such as serial number, product, version, and issued and installed dates.

   License Features. Detailed information on the license features.

8 Administering Web Tier Deployments

Web Tier Deployment Administration

If you need to change the web tier configuration after installation, use the Operations Console to perform the tasks in this chapter. After you change the web tier configuration you must update the web tier. For instructions, see Update the Web-Tier on page 178.

For instructions to uninstall a web tier, see Uninstall a Web Tier on Windows on page 179 and Uninstall a Web Tier on Linux on page 179.

For instructions to replace the web-tier SSL certificate, see Replace the Default RSA Virtual Host Certificate on page 181.

Edit a Web-Tier Deployment Configuration

You can use the Operations Console to change the configuration and web tier service options of an existing web-tier deployment. For example, you can change the preferred RBA instance and turn on or off the Self-Service Console, risk-based authentication, and dynamic seed provisioning.

If you want to edit the virtual hostname or virtual host port number, see the Operations Console Help topic "Configure a Load Balancer and Virtual Host."

Before You Begin

- You must be a Super Admin.
- Consider the impact that downtime will have on users.
- On Linux systems, verify that the open files hard limit for the local user is at least 4096.

Procedure

1. On the Operations Console on the primary instance, click **Deployment Configuration** > **Web-Tier Deployments** > **Manage Existing**.
2. On the **Web Tier Name** list, click the deployment name.
3. On the context menu, select **Edit**.

4. On the Edit page, in the **Details** section, you can change the following information:
   - **Deployment name.** The name you want for the web-tier deployment (0-255 characters. The & % > < ’ and ” characters are not allowed).
   - **Hostname.** Fully qualified hostname of the web-tier server where you installed the web-tier deployment.
   - **Preferred RBA Instance.** The instance connected to this web-tier deployment to which RBA traffic is directed.
5. In the **Web-Tier Service Options** section, turn any of the following services on or off.
   - Self-Service Console
   - Risk-based authentication
   - Dynamic seed provisioning
6. Click **Save**.

Next Steps

If you changed the deployment name, preferred server, or turned services on or off, allow at least 3 minutes for the changes to take effect.

Changing the IP Address of a Web-Tier Server

You can change the IP address of a web-tier server, for example, when you reconfigure the network. When you change the IP address, you must reinstall the web tier. During this procedure, the web-tier server is unavailable.

Before You Begin

- Consider the impact that downtime will have on your users.
- You must be a Super Admin.
- On Linux systems, verify that the open files hard limit for the local user is at least 4096.

Procedure

1. Change the IP address of the web-tier server. For more information, see your server documentation.
2. Uninstall the web tier. For instructions, see the Uninstall a Web Tier on Windows on page 179 and Uninstall a Web Tier on Linux on page 179.
3. Reinstall the web tier using the Web-Tier Installer for your platform. For instructions, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

4. If you replaced the certificates with custom certificates, activate the custom certificates after reinstalling the web tier.
5. Update the DNS server or local host file with the new web-tier server IP address. For instructions, see your DNS server and local host documentation.

Update the Load Balancer and Virtual Host

Use the Operations Console to make changes to the virtual hostname, IP address, and listening port. For example, you might make changes if you want to rename the virtual host, resolve an IP address conflict, or use a different port.

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

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

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

Before You Begin

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

Procedure

1. In the Operations Console on the primary instance, click **Deployment Configuration** > **Virtual Host & Load Balancing**.
2. If prompted, enter your Super Admin User ID and password.
3. On the Virtual Host & Load Balancing page, change any of the following:
   a. The fully qualified virtual hostname
   b. The default port number
   c. The load balancer IP addresses. If you are not using a load balancer, leave the IP address blank.
4. Click **Save**.
   The system saves the virtual hostname and key material in the keystore file.
5. On the confirmation page, read **Mandatory Next Steps**.
6. Click **Done**.

Next Steps

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

- If you updated load balancer details, you must reboot the primary and replica instances. In the Operations Console, click **Maintenance > Reboot Appliance** and reboot each instance.

- If you updated the virtual hostname, generate a new integration script for each web-based application using RBA, and then redeploy the integration scripts. For more information, see the *Administrator’s Guide*.
- If the deployment includes a web tier, update the web tier. In the Operations Console, click **Deployment Configuration > Web-Tier Deployments > Manage Existing**. Click the update link for each web tier.
- If the deployment includes a web tier, replace the certificate on the load balancer and on the firewall with the virtual host certificate.
- If the deployment uses dynamic seed provisioning, update the hostname and port for the CT-KIP URL with the hostname and port that you specified for the virtual host. In the Security Console, go to **Setup** > **System Settings**. Click **Tokens**.
- If the deployment uses the RSA Self-Service Console, update the Self-Service Console URL with the hostname and port you specified for the virtual host. In the Security Console, go to **Setup** > **Self-Service Settings**. Click **E-Mail Notifications for User Account Changes**.

Verify the Web-Tier Version

The web-tier version must be the same as your Authentication Manager version. Make sure you check the web-tier version after you update Authentication Manager. You can find the web-tier version in the Operations Console or in the web-tier installation directory.

Procedure

To see the web tier version, do one of the following:

- In the Operations Console, click go to **Deployment Configuration** > **Web-Tier Deployments** > **Manage Existing**.
- In the web-tier installation directory, go to **webtierBootstrapper**// **webtier.properties** and look for **webtier.version=<VERSION NUMBER>**.

Update the Web-Tier

You must update the web tier when you make any changes such as updating your version of Authentication Manager and customizing the web-tier pages. Authentication Manager displays an update button in the Operations Console for each web tier that is not up-to-date. If you have multiple web tiers to update, update one web tier at a time. Each update may take up to 15 minutes to complete.

Procedure

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

   When the update is complete, which may take up to 20 minutes, the **Status** column for the updated web tier displays **Online.**

Uninstall a Web Tier on Windows

During uninstallation, run the RSA Authentication Web-Tier Uninstaller for Windows on the web-tier server. Uninstalling a web tier removes the web tier and all features and components of RSA Authentication Manager from the web-tier server.

Uninstalling a web tier does not delete the web-tier deployment record.

Before You Begin

Confirm that you have Windows credentials to uninstall a program.

Procedure

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

   ```
   y
   ```

   and press ENTER.

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

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

Next Steps

- On the primary instance, use the Operations Console to delete the web-tier deployment record. For instructions, see the Operations Console Help topic “Delete a Web-Tier Deployment Record.”
- (Optional) On the DNS server, delete the hostname and IP address for the web tier that you uninstalled.

Uninstall a Web Tier on Linux

During uninstallation, run the RSA Authentication Web-Tier Uninstaller for Linux on the web-tier server. Uninstalling a web tier removes the web tier and all features and components of RSA Authentication Manager from the web-tier server.

Uninstalling a web tier does not delete the web-tier deployment record.

Before You Begin

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

Procedure

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

   ```
   ./uninstall.sh
   ```

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

   ```
   yes
   ```

6. Press ENTER.

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

Next Steps

- On the primary instance, use the Operations Console to delete the web-tier deployment record. For instructions, see the Operations Console Help topic "Delete a Web-Tier Deployment Record."
- (Optional) On the DNS server, delete the hostname and IP address for the web tier that you uninstalled.

Managing the Web-Tier Service

The bootstrapper server and web-tier services start and run automatically when you install a web tier. You must start them manually after promoting a replica instance.

The bootstrapper must be running to report web-tier status and to push updates to the web tier. Web-tier services must be running to support web-tier functions such as Self-Service, risk-based authentication (RBA), and dynamic seed provisioning. You can stop, start, and re-start the bootstrapper and web-tier services manually, for example, if you want to stop the web-tier server to migrate to another machine.

For instructions, see the following procedures:

- Manage the RSA Web-Tier Bootstrapper Server on Windows on page 180
- Manage the RSA Web-Tier Bootstrapper Server on Linux on page 181

Manage the RSA Web-Tier Bootstrapper Server on Windows

Perform this procedure to stop, start, or restart the RSA Web-Tier Bootstrap Server. This procedure applies to all supported Windows versions.

Procedure

1. On the web-tier server, click **Start** > **Run**.
2. Type:

   services.msc

3. Press ENTER.
4. Right-click **RSA Webtier Bootstrapper Server**.
5. Click the following, as needed.
   - **Stop**
   - **Start**
   - **Restart**

Manage the RSA Web-Tier Bootstrapper Server on Linux

Perform this procedure to stop, start, or restart the RSA Web-Tier Bootstrap Server. This procedure applies to all supported Linux versions.

Before You Begin

- Log on as the local user you specified during installation.
- Verify that the open files hard limit for the local user is at least 4096.

Procedure

1. On the web-tier server, go to ***RSA_WT_HOME*****/webtierBootstrapper/server**.

   where *RSA_WT_HOME* is the web-tier installation directory.
2. Type the appropriate command:

   ./rsaserv start all
   ./rsaserv stop all
   ./rsaserv restart all
   ./rsaserv status all

Replace the Default RSA Virtual Host Certificate

Each web tier has a certificate based on the virtual hostname. Some features, such as risk-based authentication, use the virtual hostname to allow use of a load balancer. Other features, such as the Self-Service Console, use the virtual hostname so that the Console can connect to the web-tier server that is associated with the primary instance.

Replacing your default RSA virtual host certificate is optional. You might need to replace this certificate for the following reasons:

- Your network policy requires you to use certificates issued by a trusted root certificate authority (CA).
- Your current certificate issued by a trusted root CA is expired.
- You want to replace the default RSA certificate because your browser warns you that the default certificate is not trusted.

Certificate Authority Certificate Files

A certificate authority may send certificates in one or more files. There are three possible combinations:

One file. One certificate file that contains the entire chain of certificates from the parent trusted root certificate, to possible intermediate signing certificates, to the host certificate. This is the most convenient scenario, because everything is in one file. You may lose some flexibility because you cannot unbundle the certificates.

When you import the certificate file, the system warns you that it is not trusted because the imported root certificate is not yet saved in the trusted root store. After the import, the warning no longer appears.

Two files. A certificate file and a separate root certificate file containing the signed Virtual Host server certificate. This provides the following benefits:

- A trusted root certificate against which all future certificates are verified.
- A trusted root certificate that you can import into the trusted root stores of web browsers that do not trust the RSA default root certificate by default.

You must import the root certificate first.

Two or more files. Multiple files, each containing a separate certificate. This allows you to establish a trusted root and gives you the most flexibility. When you replace both the web-tier and virtual host certificates, and they are signed by the same trusted certificate authority, you only need to import the trust certificates once. You must import each certificate in the following order:

- Parent trusted root certificate
- Intermediate signing certificates
- Host certificate

Replacing the Default Virtual Host Certificate

The following is the procedure for replacing the default virtual host certificate.

1. Generate a certificate signing request using one of the following methods.
   - RSA Security Console. For instructions, see Generate a Certificate Signing Request (CSR) for the Web Tier on page 183.
   - Third-party tool. Ensure that the third-party tool generates a private key and a signing request. Ensure that you enter a common name (CN) where the value is the fully qualified hostname (FQHN) of the virtual host or you will not be able to activate the virtual host certificate. For instructions, see the third-party tool documentation.
2. Send the certificate signing request to the certificate authority (CA).
3. Import the trusted root and signed virtual host certificates and make it the active certificate. For instructions, see Import a Signed Virtual Host Certificate on page 183.
4. Update each web tier after importing the new certificate. For instructions, see Update the Web-Tier on page 178.

Generate a Certificate Signing Request (CSR) for the Web Tier

Before you can send a certificate signing request to a CA, you must generate the certificate signing request file in Authentication Manager. Authentication Manager generates the private key and certificate signing request.

Before You Begin

- You must be an Operations Console Administrator
- The virtual host must be defined

Procedure

1. In the Operations Console, go to **Deployment Configuration** > **Certificates** > **Virtual Host Certificate Management**, and click **Generate CSR**.
2. On the Generate Virtual Host Certificate Signing Request page, do the following:
   - Confirm the **Virtual Host** name.
   - Enter an **Alias**.
   - (Optional) Enter a **Country** name
   - (Optional) Enter a **State or Province** name.
   - (Optional) Enter a **City or Locality** name.
   - (Optional) Enter an **Organization** name.
   - (Optional) Enter an **Organizational Unit** name.
   - (Optional) Enter an E-mail Address
3. Click **Generate File**.
4. On the Download File page, click **Download**.
5. Save the certificate request file to your local machine.

Next Steps

- Send the certificate request file to the CA for signing and save the signed certificate request file on your local machine.
- Import the trusted root and signed certificates to the virtual host and activate them. For instructions, see Import a Signed Virtual Host Certificate.

Import a Signed Virtual Host Certificate

After you download all of the certificate files in the signing chain from your certificate authority (CA), you must import the files to replace the existing virtual host certificate with the new certificate.

Before You Begin

- You must be an Operations Console Administrator.
- Download the CA root certificate, all other certificates that are part of the signing chain, and the new virtual host certificate.

Procedure

1. In the Operations Console, click **Deployment Configuration** > **Certificates** > **Virtual Host Certificate Management**.

   Beginning with the root certificate, perform the following steps for each certificate in the signing chain.

2. In the Virtual Host Certificate Management page, click **Import Certificates**.

3. In the Import Certificate page under **Certificate Basics**, do one of the following:

   For a certificate made in response to a CSR from the Operations Console:

   - In the **Import Certificate** field, browse to the location where the certificate is stored. This file contains either a CA root certificate or the SSL certificate from the CA.
   - For **Type of Certificate to Import**, select **PKCS#7 (*.cer or *.p7b)**.

   For a certificate made in response to a CSR from a certificate tool of your choice:

   - In the **Import Certificate** field, browse to the location where the certificate is stored. This file contains one or more certificates and the private key for the new certificate.
   - For **Type of Certificate to Import**, select **PKCS#12 (*.pfx or*.p12)**.
   - In the **Password** field, enter the password for the PKCS#12 file.

4. Click **Import**.

Next Steps

Activate a Virtual Host Certificate on page 184

Activate a Virtual Host Certificate

Before the virtual host can use a new certificate, you must activate the certificate.

You can only activate a virtual host certificate that has a common name (CN) where the value is the fully qualified hostname (FQHN) of the virtual host.

Before You Begin

- You must be an Operations Console Administrator.
- Import a Signed Virtual Host Certificate that you want to activate.

Procedure

1. In the Operations Console, click **Deployment Configuration** > **Certificates** > **Virtual Host Certificate Management**.
2. In the Virtual Host Certificate Management page, under **Alias**, click the name of the new certificate.
3. Click **Activate**.
4. On the Activate Certificate Confirmation page, review the details, and select **Yes, make this the active default certificate**.
5. Click **Activate Certificate**.

Next Steps

Update the web tier. For instructions, see Update the Web-Tier on page 178.

Logout Error on the Self-Service Console in the Web Tier

If the web-tier server is more than 15 minutes out-of-sync with the associated instance, the user may see the following error when attempting to log out of the Self-Service Console:

"Error: Internal Server Error. The server encountered an unexpected condition, which prevented it from fulfilling your request."

The system log states the following:

"Caused by: com.rsa. common.SystemException: Logout request exceeds the configured time window. The web tier time is not in sync with the biz-tier or a possible replay."

The possible cause is a logout request that is outside of the allowable time window. To resolve this issue, do one of the following:

- If the deployment does not have a Network Time Protocol (NTP) server, synchronize the web-tier server time to the associated instance.
- If the deployment has an NTP server, synchronize the web-tier server to the NTP server.

The time zones do not need to be the same. For example, the web-tier server time can be 7:00 am (GMT), and the associated instance time can be 9:00 am (GMT + 2).

9 Deploying and Administering RSA SecurID Tokens

RSA SecurID Tokens

RSA SecurID tokens offer RSA SecurID two-factor authentication. An RSA SecurID token generates a 6-digit or 8-digit pseudorandom number, or tokencode, at regular intervals. When the tokencode is combined with a personal identification number (PIN), the result is called a passcode. Users enter passcode values, along with other security information, to verify their identity to resources protected by Authentication Manager. If Authentication Manager validates the passcode, the user is granted access. Otherwise, the user is denied access.

There are two kinds of SecurID tokens, hardware tokens and software tokens. Hardware tokens generate tokencodes using a built-in clock and the token's factory-encoded random key, known as the "seed." Hardware tokens come in several models, such as key fobs and PINPads. Software tokens consist of two components that are installed separately, an application specific to the intended device platform and a token seed record. Software token applications generate tokencodes on the device and offer the same passcode functionality as hardware tokens. Devices include smart phones, computers, and tablets.

Hardware and software tokens require similar administrative tasks. Following deployment, you can perform many token-related administrative tasks with the User Dashboard in the Security Console. For more information, see the Security Console Help topic "User Dashboard."

By default, RSA provides tokens that require a PIN and strongly recommends that you use PINs for all tokens. PINs provide the second factor in RSA SecurID two-factor authentication. RSA Authentication Manager also supports authentication with tokens that do not require an RSA SecurID PIN.

Deploying RSA SecurID Tokens

The following steps outline the tasks required to deploy RSA SecurID tokens.

Procedure

1. Import a Token Record File on page 188.
2. (Optional) Move a Token Record to a New Security Domain on page 189.
3. Assign Tokens to Users on page 189.
4. For software tokens, Add a Software Token Profile on page 192. Otherwise continue to step 5.
5. Distribute the token. Choose one of the following:

- Distribute a Hardware Token on page 194
- Distribute Multiple Software Tokens Using File-Based Provisioning on page 194
- Distribute One Software Token Using File-Based Provisioning on page 196
- Distribute Multiple Software Tokens Using Dynamic Seed Provisioning (CT-KIP) on page 197
- Distribute One Software Token Using Dynamic Seed Provisioning on page 198
- Distribute Multiple Software Tokens Using Compressed Token Format (CTF) on page 200
- Distribute One Software Token Using Compressed Token Format (CTF) on page 201

Import a Token Record File

RSA manufacturing provides an XML file that contains the token records that your organization has purchased. Before you can work with individual token records, you must import the token record XML file into Authentication Manager.

For hardware tokens, each token record in the file corresponds to a hardware token that your organization has purchased.

For software tokens, token record data will eventually be transferred into a software token application. Each token record contains the token seed and metadata such as the token serial number, expiration date, and the tokencode length and interval.

Before You Begin

- Decide which security domain will own the imported tokens. The security domain must be in the administrative scope of the administrator who will deploy and manage the tokens.
- Your administrative role must permit you to manage tokens.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Import Tokens Job** > **Add New**.
2. Enter a name for the import job. The job is saved with this name so that you can review the details of the job later. The name must be from 1 to 128 characters. The characters & % > < are not allowed.
3. From the **Security Domain** drop-down menu, select the security domain into which you want to import the tokens. The tokens are managed by administrators whose scope includes this security domain. By default, tokens are imported into the top-level security domain.
4. Browse to select the token files that you want to import.
5. In the **File Password** field, enter a password if the file is password protected.

6. Use the **Import Options** radio buttons to specify handling for duplicate tokens.
7. Click **Submit Job.**

Next Steps

Assign tokens to users. For more information, see Assign Tokens to Users on page 189.

Move a Token Record to a New Security Domain

You can select a new security domain to move token records. If you do not select a security domain, the token records are imported into the top-level security domain by default. You can move token records between security domains within a deployment using the Security Console. You can also change an administrator’s scope to manage token records, or you can move the records to a security domain that is associated with the location where the tokens will be used.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Use the search fields to find the tokens that you want to move.
3. Select the checkboxes next to the tokens that you want to move.
4. From the **Action** menu, click **Move to Security Domain**.
5. Click **Go**.
6. From the **Move to Security Domain** drop-down list, select the security domain to which you want to move the tokens.
7. Click **Move**.

Assign Tokens to Users

Assigning a token associates the token with a specific user. You must assign a token to a user before the user can authenticate. You can assign a maximum of three tokens to each user. RSA recommends that you do not assign more than one hardware token to a user as this may increase the likelihood that users will report a lost or stolen token. Some software token applications may not allow multiple tokens. For platform-specific information on token limitations, see the RSA SecurID software token documentation.

You can also assign tokens with the User Dashboard. For instructions, see the Security Console Help topic “User Dashboard.”

Before You Begin

- Import the token records from the token record file to the internal database. For more information, see Import a Token Record File on page 188.
- Make sure a user record exists in Authentication Manager for each user to whom you want to assign a token.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the users to whom you want to assign tokens.
3. From the search results, click the user(s) to whom you want to assign tokens.
4. From the context menu, under SecurID Tokens, click **Assign More**.
5. From the list of available RSA SecurID tokens on the Assign to Users page, select the checkboxes for the tokens that you want to assign. Record which tokens you assign so you can deliver them later.
6. Click **Assign**.

Next Steps

Add a Software Token Profile on page 192

Software Token Profiles

Software token profiles specify software token configurations and distribution processes. A software token profile is required for each platform for which you plan to distribute software tokens. Only a Super Admin can add software token profiles to the deployment. Software token profiles are available to the entire deployment and are not specific to a security domain.

Device Definition File

A device definition file is an XML file that defines the capabilities and attributes of software tokens used on a specific platform, for example, the Android platform or the iOS platform. The file identifies the supported tokencode characteristics, the token type, whether the token is CT-KIP capable, CT-KIP link format, whether the token is CTF capable, and the supported binding attributes.

When RSA releases applications for new software token types, the applications often require new device definition files. You must import the new device definition file when you create a software token profile using the new token type. To determine whether you need to import a new device definition file, see the *Administrator's Guide* for your software token application.

Software Token Configuration

RSA SecurID software tokens are factory-set as PINPad PIN type (PIN integrated with tokencode), 8-digit tokencode length, and 60-second tokencode interval. However, you can configure the tokencode interval, PIN type, and tokencode length of software tokens for each software token profile that you create. Depending on configuration options set in the device definition file, you can set the tokencode length to 6 or 8 digits and the tokencode interval to 30 or 60 seconds. You can change the PIN type so that the token behaves like a hardware fob. You can also reconfigure the token to be tokencode only.

Software Token Delivery Methods

The following methods are available for providing token data to a software token application:

Dynamic Seed Provisioning (CT-KIP). The dynamic seed provisioning method uses the four-pass Cryptographic Token Key Initialization Protocol (CT-KIP) to exchange information between an RSA SecurID client application running on a mobile device, desktop, or desktop, and the CT-KIP server, which is a component of the Authentication Manager server. The information exchanged between the client and server is used to generate a unique shared secret (token seed). Information critical to the seed generation is encrypted during transmission using a public-private key pair. The generated token seed value is never transmitted across the network. Dynamic seed provisioning is preferred over file-based provisioning because the four-pass protocol prevents the potential interception of the token's seed during the provisioning process.

If you configured activation codes to expire, a user must provide the activation code to the client application before the code expires. If the activation code is not used before the expiration time, you must redistribute the token, and provide the CT-KIP URL and the new activation code to the user.

The four-pass CT-KIP protocol is initiated by a request from the client application to the CT-KIP server when the user selects an import token option on the client device. Dynamic seed provisioning uses a unique one-time provisioning activation code to ensure that the request is legitimate The client application must be provided with the activation code, either through manual user entry or as part of a URL string sent to the user's device e-mail. The CT-KIP server evaluates the activation code, and if the server determines that the request is valid, the four-pass process continues, ultimately resulting in a successful import operation.

File-Based Provisioning. With file-based provisioning, Authentication Manager generates token data contained within a file, which is added to a ZIP file for download. Software token files provisioned using this method have the extension .sdtid. The data in the token file includes the seed used by the SecurID algorithm and other metadata, including the token serial number, expiration date, number of digits in the tokencode, and so on. To protect the seed against attack, the seed is encrypted using the AES encryption algorithm and an optional password that you can assign during the configuration process. RSA recommends protecting file-based tokens with a strong password that conforms to guidelines provided in the *RSA Authentication Manager 8.1 Security Configuration Guide.*

Compressed Token Format (CTF) Provisioning. E-mail programs on some mobile device platforms cannot interpret .sdtid file attachments. In such cases, you can deliver file-based tokens using Compressed Token Format (CTF). Authentication Manager generates token data in the form of a CTF URL string, which you deliver to the user's device by e-mail as a URL link. CTF URL strings contain the encoded token data needed by the software token application. This encoded data includes the seed used by the SecurID algorithm and other metadata, including the token serial number, expiration date, number of digits in the tokencode, and so on. The URL format signals the device that the URL link contains data relevant to the software token application. RSA recommends protecting CTF format tokens with a strong password that conforms to guidelines provided in the *RSA Authentication Manager 8.1 Security Configuration Guide*.

Device Attributes

Device attributes are used to add information to software tokens. You can use the **DeviceSerialNumber** field to restrict the installation of a token to a device platform or to a specific device. The default **DeviceSerialNumber** value associated with the device type binds the token to a specific platform. Binding to a device platform allows the user to install the token on any device that runs on that platform, for example, any supported Android device. The user cannot install the token on a different platform, such as Apple iOS.

For additional security, you can bind a token to a single, device-specific identification number, for example, a separate, unique device ID assigned by the RSA SecurID software token application. In this case, the token can only be installed on the device that has the device-specific ID. If a user attempts to import the token to any other device, the import fails. You must bind tokens before you distribute them. In some cases, you must obtain the device binding information from the user. The user must install the software application before providing the binding information. For more information, see your RSA SecurID software token documentation.

The **Nickname** field allows you to assign a user-friendly name to the token. When the token is installed into the application on the device, the application displays the token nickname. If you do not assign a nickname, the application displays a default name, for example, the token serial number. Not all software token applications support nicknames.

Add a Software Token Profile

Software token profiles specify software token configuration and distribution options. You must configure a software token profile for each platform to which you plan to distribute software tokens.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Authentication** > **Software Token Profiles** > **Add New**.
2. Enter the **Profile Name**. Try to include the device type or distribution method in the profile name. For example, “Android_CT_KIP.”
3. Do one of the following:
   - To choose an existing device type, select one from the **Device Type** drop-down list.
   - To load a new device type, click **Import New Device Definition File**, browse to the device definition file, and click **Submit**.
4. Complete the specific fields for the device type. You may have to configure these settings:
   a. In the **Tokencode Duration** field, select the duration for the tokencode display.
   b. In the **Tokencode Length** field, select the number of digits in the tokencode.

c. Select the **Authentication Type**. The following authentication types are available:

  - PINPad-style. The user must enter a PIN in the software token application to generate the passcode.
  - Fob-style. The user must enter the PIN, followed by the tokencode when logging on to the resource protected by SecurID.
  - Tokencode. The user enters a tokencode. No PIN is required.

d. Select the **Delivery Method**. You can distribute the software token file in one of three ways:

  - Dynamic Seed Provisioning. Uses the Cryptographic Token-Key Initialization Protocol (CT-KIP). Use this method only with CT-KIP-capable SecurID software tokens. A CT-KIP-capable SecurID software token is always a 128-bit token.
  - Compressed Token Format (CTF) Provisioning. Authentication Manager generates a URL, which you deliver to the user’s device. This URL contains the encoded token information needed by the software application. Use this method only with CTF-capable SecurID software tokens. CTF provisioning is not available to 64-bit tokens.
  - File-based Provisioning. Authentication Manager generates a software token distribution file (.sdtid), which is added to a .zip file for download. This software token distribution file contains the shared secret (“seed”) used by the SecurID algorithm, and other metadata such as expiration date, serial number, and number of digits in the tokencode.

e. In the **Device Specific Attributes** section, do one of the following:

  - If you want to bind all software tokens intended for this device type to the device class, leave the default value (classGUID) in the **DeviceSerialNumber** field.
  - If you do not want to bind all software tokens intended for this device type to the device class, you can clear the **DeviceSerialNumber** field or leave the default value. Then, when you distribute the token, you can replace the default value with a device-specific ID.

f. Enter a nickname if you want all tokens that you deliver to have the same nickname (for example, your company name). You can set a nickname for a specific token when you distribute the token.

5. Click **Save**.

Next Steps

Deliver the token to the user using the selected method. For instructions, see one of the following:

- Distribute Multiple Software Tokens Using File-Based Provisioning on page 194
- Distribute One Software Token Using File-Based Provisioning on page 196

- Distribute Multiple Software Tokens Using Dynamic Seed Provisioning (CT-KIP) on page 197
- Distribute One Software Token Using Dynamic Seed Provisioning on page 198
- Distribute Multiple Software Tokens Using Compressed Token Format (CTF) on page 200
- Distribute One Software Token Using Compressed Token Format (CTF) on page 201

Distribute a Hardware Token

Before You Begin

Assign Tokens to Users on page 189

Procedure

Do one of the following:

- If users are located within close proximity, instruct the users to physically collect the tokens.
- If your organization is large and geographically dispersed, distribute tokens by mail.

Distribute Multiple Software Tokens Using File-Based Provisioning

When you distribute software tokens using file-based provisioning, token data is stored in a token distribution file (SDTID file). The SDTID file is added to a ZIP file for download.

Before You Begin

- Instruct users to install the software token application on their devices. For installation instructions, see the *Administrator's Guide* for your software token application.
- Add a Software Token Profile on page 192.
- Assign Tokens to Users on page 189.

Important: When you redistribute tokens using this method, any existing users of these tokens may no longer be able to authenticate. Users must import the new token data before they can authenticate.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Distribute Software Tokens in Bulk** > **Generate Software Token Files**.
2. In the **Job Name** field, enter a name for the job, or accept the default name. The job is saved with this name so that you can review the details of the job later. Enter a unique name from 1 to 128 characters. The characters & % > < are not allowed.

3. From the **Software Token Profile** drop-down list, select a software token profile with file-based provisioning as the delivery method.
4. In the **DeviceSerialNumber** field, do one of the following:
   - To bind the token to the device class, leave the default setting.
   - To bind the token to a specific device, clear the field and enter the device ID you obtained from the user.
5. Enter a nickname or leave the **Nickname** field blank.
6. You can choose to **Password Protect** the token file. The user must enter the password when adding the token to the SecurID application on the device. Select an option:
   - **Password.** Enter a password of your choice. This password applies to all software tokens in the token distribution file. A password can be up to 24 characters long for 128-bit tokens and 8 characters long for 64-bit tokens.
   - **No password**. The user does not enter a password.
   - **User ID**. The user enters his or her user ID.
   - **Combination User ID followed by Password**. The user enters his or her user ID and the password that you set. The user ID and password combination can be up to 24 characters long for 128-bit tokens and 8 characters long for 64-bit tokens.
7. If you selected **Password**, enter the password in the **Password** and **Confirm Password** fields.
8. Click **Next**.
9. Enter the token selection criteria to find the tokens that you want to distribute. For example, enter the range of serial numbers for the tokens that you want to distribute.
10. Click **Next**.
11. Review the distribution summary and click **Submit Job**.
12. Click the **Completed** tab to view completed jobs.
13. From the context menu, click **Download Output File**.
14. Save the output file to your machine.
15. Safely deliver the token files to users.

Distribute One Software Token Using File-Based Provisioning

When you distribute software tokens using file-based provisioning, token data is stored in a token distribution file (SDTID file). The SDTID file is added to a ZIP file for download.

Before You Begin

- Instruct the user to install the software token application on a device. For installation instructions, see the *Administrator's Guide* for your software token application.
- Add a Software Token Profile on page 192. Only a Super Admin can add software token profiles.
- Assign Tokens to Users on page 189.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Use the search fields to find the software token that you want to distribute.
3. From the search results, click the software token that you want to distribute.
4. From the context menu, click **Distribute**.
5. From the **Select Token Profile** drop-down list, select a software token profile with file-based provisioning as the delivery method.
6. In the **DeviceSerialNumber** field, do one of the following:
    - To bind the token to the device class, leave the default setting.
    - To bind the token to a specific device, clear the field and enter the device ID you obtained from the user.
7. Enter a nickname or leave the **Nickname** field blank.
8. You can choose to **Password Protect** the token file. The following options are available:
    - **Password.** Enter a password of your choice. This password applies to all software tokens in the token distribution file. A password can be up to 24 characters long for 128-bit tokens and 8 characters long for 64-bit tokens.
    - **No password**. The user does not enter a password.
    - **User ID**. The user enters his or her user ID.
    - **Combination User ID followed by Password**. The user enters his or her user ID and the password that you set. The user ID and password combination can be up to 24 characters long for 128-bit tokens and 8 characters long for 64-bit tokens.
9. If you select **Password or Combination**, create a password, and enter it in the **Password** and **Confirm Password** fields.
10. Click **Save and Distribute**.
11. Click **Download Now.**

12. Securely deliver the token file to the user.
13. Click **Done**.

Distribute Multiple Software Tokens Using Dynamic Seed Provisioning (CT-KIP)

Dynamic Seed Provisioning uses the CT-KIP protocol to generate token data without the need for a token file. After you complete the provisioning steps, RSA Authentication Manager displays the URL link of the CT-KIP server and a unique, one-time token activation code. You need these two pieces of information to deliver the token to a device as a URL. Authentication Manager 8.1 now generates custom CT-KIP URLs for certain mobile platform device types. For example, Android, iPhone, Nokia, Browser Toolbar, and Windows Phone.

Before You Begin

- Decide how to safely deliver the URL link of the CT-KIP server and the CT-KIP activation code to users. RSA Authentication Manager does not encrypt e-mail. For secure delivery, you can do the following:
  - Provide the information offline, such as by calling the users on the telephone.
  - Copy the information into e-mail that you encrypt.
  - Use a Simple Mail Transfer Protocol (SMTP) e-mail encryption gateway if the end-user device supports encrypted e-mail.
- Instruct users to install the software token application on their devices. For installation instructions, see the documentation for the software token application.
- Add a Software Token Profile on page 192.
- Assign Tokens to Users on page 189
- RSA recommends that you replace the default certificates in Authentication Manager with trusted certificates. If you do not replace the default certificates, end users are prompted to accept untrusted certificates before proceeding. If you want to use dynamic seed provisioning with CT-KIP, you must have a trusted certificate on the Authentication Manager server or web-tiers.

Important: When you redistribute tokens using this method, any existing users of these tokens may no longer be able to authenticate. Users must import the new token data before they can authenticate.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Distribute Software Tokens in Bulk** > **Generate Dynamic Seed Provisioning Credentials**.
2. In the **Job Name** field, enter a name for the job, or accept the default name. The job is saved with this name so that you can review the details of the job later. The name must be a unique name from 1 to 128 characters. The characters & % > < are not allowed.
3. From the **Software Token Profile** drop-down list, select a software token profile with dynamic seed provisioning as the delivery method.

4. In the **DeviceSerialNumber** field, do one of the following:
   - To bind the token to the device class, leave the default setting.
   - To bind the token to a specific device, clear the field and enter the device ID you obtained from the user.
5. Enter a nickname or leave the **Nickname** field blank.
6. Click **Next.**
7. Enter the token selection criteria to find the tokens that you want to distribute. For example, enter the range of serial numbers for the tokens that you want to distribute.
8. Click **Next.**
9. Review the distribution summary and click **Submit Job**.
10. Click the **Completed** tab to view completed jobs.
11. Click the job with which you want to work.
12. From the context menu, click **Download Output File**.
13. Save the output file to your machine.
14. Open the output file, copy the activation codes and CT-KIP URL and safely deliver them to the users.

   Note: When you download the output file, some spreadsheet applications will remove the leading zeroes from the activation codes. To import activation codes successfully, open the file in an application that does not remove any characters, such as a text editor, to copy the activation code accurately.

15. Instruct users on how to import tokens.

   If you configured activation codes to expire, advise users to import tokens before the expiration time. If the activation codes are not used before the expiration time, you must redistribute the tokens, and provide the CT-KIP URL and the new activation codes to users.

   For more information, see the software token *Administrator's Guide* for your platform.

Distribute One Software Token Using Dynamic Seed Provisioning

Dynamic seed provisioning uses the CT-KIP protocol to generate token data without the need for a token file. After you complete the provisioning steps, RSA Authentication Manager displays the URL link of the CT-KIP server and the unique, one-time token activation code. You need these two pieces of information to deliver the token to a device as a URL. Authentication Manager 8.1 now generates custom CT-KIP URLs for certain mobile platform device types. For example, Android, iPhone, Nokia, Browser Toolbar, and Windows Phone.

Before You Begin

- Decide how to safely deliver the URL link of the CT-KIP server and the CT-KIP activation code to the user. RSA Authentication Manager does not encrypt e-mail. For a more secure delivery option, you can do the following:
  - Provide the information offline, such as by calling the user on the telephone.
  - Copy the information into an e-mail that you encrypt.
  - Use a Simple Mail Transfer Protocol (SMTP) e-mail encryption gateway.
- Instruct users to install the software token application on their devices. For installation instructions, see the documentation for the software token application.
- Add a Software Token Profile on page 192. Only a Super Admin can add software token profiles.
- Assign Tokens to Users on page 189.
- RSA recommends that you replace the default certificates in Authentication Manager with trusted certificates. If you do not do this, end users are prompted to accept untrusted certificates before proceeding. Certain mobile device platforms only support an SSL certificate with a server that has a trusted certificate installed. If you want to use dynamic seed provisioning with CT-KIP, you must have a trusted certificate on your Authentication Manager server.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Use the search fields to find the software token that you want to distribute.
3. From the search results, click the software token that you want to distribute.
4. From the context menu, click **Distribute**.
5. From the **Select Token Profile** drop-down list, select a software token profile with dynamic seed provisioning as the delivery method.
6. In the **DeviceSerialNumber** field, do one of the following:
   - To bind the token to the device class, leave the default setting.
   - To bind the token to a specific device, clear the field and enter the device ID you obtained from the user.
7. Enter a nickname or leave the **Nickname** field blank.
8. From the **CT-KIP Activation Code** drop-down list, select an activation code for the software token.
9. Click **Save and Distribute**.

10. Copy the activation code and CT-KIP URL and safely deliver them to the user.
11. Instruct the user on how to import the token.

    If you configured the activation code to expire, advise the user to import the token before the expiration time. If the activation code is not used before the expiration time, you must redistribute the token, and provide the CT-KIP URL and the new activation code to the user.

    For more information, see the software token *Administrator's Guide* for your platform

Distribute Multiple Software Tokens Using Compressed Token Format (CTF)

When you distribute software tokens using Compressed Token Format (CTF), you generate a URL, which you deliver to the user. This URL contains the token data needed by the software token application.

Before You Begin

- Instruct users to install the software token application on their devices. For installation instructions, see the documentation for the software token application.
- Add a Software Token Profile on page 192. Only a Super Admin can add software token profiles.
- Assign Tokens to Users on page 189.

Important: If you use this method to redistribute existing tokens, the users of these tokens cannot authenticate until they import the new token data.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Distribute Software Tokens in Bulk** > **Generate Compressed Token Format Credentials**.
2. In the **Job Name** field, enter a name for the job, or accept the default name. The job is saved with this name so that you can go back and review the details of the job later. The name must be a unique name containing 1 to 128 characters. The characters & % > < are not allowed.
3. From the **Software Token Profile** drop-down list, select a software token profile with CTF as the delivery method.
4. In the **DeviceSerialNumber** field, do one of the following:
    - To bind the token to the device class, leave the default setting.
    - To bind the token to a specific device, clear the field and enter the device ID you obtained from the user.
5. Enter a nickname or leave the **Nickname** field blank.

6. You can choose to **Password Protect** the token file. The following options are available:
   - **Password.** Enter a password of your choice. This password applies to all software tokens in the token distribution file. A password can be up to 24 characters long for 128-bit tokens and 8 characters long for 64-bit tokens.
   - **No password**. The user does not enter a password.
   - **User ID**. The user enters his or her user ID.
   - **Combination User ID followed by Password**. The user enters his or her user ID and the password that you set. The user ID and password combination can be up to 24 characters long for 128-bit tokens and 8 characters long for 64-bit tokens.
7. If you select **Password or Combination**, create a password, and enter it in the **Password** and **Confirm Password** fields.
8. Click **Next.**
9. Enter the token selection criteria to find the tokens that you want to distribute. For example, enter the range of serial numbers for the tokens that you want to distribute.
10. Click **Next.**
11. Review the distribution summary and click **Submit Job**.
12. Click the **Completed** tab to view completed jobs.
13. Click the job with which you want to work.
14. From the context menu, click **Download Output File**.
15. Save the output file to your machine.
16. Open the output file, copy the CTF URLs and safely deliver them to the users.
17. Instruct users on how to import the token. For more information, see the software token *Administrator's Guide* for your platform.

Distribute One Software Token Using Compressed Token Format (CTF)

When you distribute a software token using Compressed Token Format (CTF), you generate a URL, which you deliver to the user. This URL contains the token data needed by the software token application.

Before You Begin

- Instruct users to install the software token application on their devices. For installation instructions, see the documentation for the software token application.
- Add a Software Token Profile on page 192. Only a Super Admin can add software token profiles.
- Assign Tokens to Users on page 189.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Click the **Assigned** tab.
3. Use the search fields to find the software token that you want to distribute.
4. From the search results, click the software token that you want to distribute.
5. From the context menu, click **Distribute**.
6. From the **Select Token Profile** drop-down list, select a software token profile with Compressed Token Format (CTF) as the delivery method.
7. In the **DeviceSerialNumber** field, do one of the following:
   - To bind the token to the device class, leave the default setting.
   - To bind the token to a specific device, clear the field and enter the device ID you obtained from the user.
8. Enter a nickname or leave the **Nickname** field blank.
9. You can choose to **Password Protect** the token file. The following options are available:
   - **Password.** Enter a password of your choice. This password applies to all software tokens in the token distribution file. A password can be up to 24 characters long for 128-bit tokens and 8 characters long for 64-bit tokens.
   - **No password**. The user does not enter a password.
   - **User ID**. The user enters his or her user ID.
   - **Combination User ID followed by Password**. The user enters his or her user ID and the password that you set. The user ID and password combination can be up to 24 characters long for 128-bit tokens and 8 characters long for 64-bit tokens.
10. If you select **Password or Combination**, create a password, and enter it in the **Password** and **Confirm Password** fields.
11. Click **Save and Distribute**.
12. Copy the CTF URL and safely deliver it to the user.

    Note: If you navigate away from this page before you copy the CTF URL, you must perform the distribution process from the beginning to generate a new URL.

13. Instruct the user on how to import the token. For more information, see the software token *Administrator's Guide* for your platform.

Administering RSA SecurID Tokens

Administering a token includes token management and providing temporary emergency access for users. You can perform the following tasks with tokens:

- Enable a Token on page 203
- Disable a Token on page 204
- Delete a Token on page 204
- Edit a Token on page 204
- Assign a Replacement Token on page 205

Enabled and Disabled Tokens

An enabled token can be used for authentication. A disabled token cannot be used.

After Authentication Manager is installed, tokens must be imported into the deployment. All imported tokens are automatically disabled. This security feature protects the deployment if the tokens are lost or stolen.

Tokens are automatically enabled when they are assigned by an administrator.

Tokencode-only software tokens that are provisioned through Self-Service are disabled by default. Users can enable these tokens through the Self-Service Console.

A disabled token does not lock a user's account. Lockout applies to a user's account, not to a user's token. Disabling a token does not remove the user's account from the deployment. You can view disabled tokens using the Security Console.

You can enable and disable tokens only in security domains that are included in your administrative scope.

You should disable an assigned token in the following situations:

- Before a hardware token is mailed to a user. Re-enable the token after you know that it has been successfully delivered to the user to whom it has been assigned and the user is ready to use it.
- If you know that a user does not need to authenticate for an extended period of time. For example, you may want to disable a token before a user takes a short-term leave or an extended vacation. After you disable the token, that user cannot authenticate with that token until it is re-enabled.

Enable a Token

Before a user can use an assigned token to authenticate, you must enable the token.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Click the **Assigned or Unassigned** tab to view the list of tokens that you want to enable.
3. Select the checkbox next to the tokens that you want to enable.

4. From the Action menu, click **Enable**.
5. Click **Go**.

Disable a Token

When you disable a token, the assigned user can no longer use the token to authenticate.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Click the **Assigned or Unassigned** tab to view the list of tokens that you want to disable.
3. Select the checkbox next to the tokens that you want to disable.
4. From the Action menu, click **Disable**.
5. Click **Go**.

Delete a Token

When you delete a token, the token is removed from the internal database and can no longer be assigned. If it is already assigned to a user, the user cannot use the token to authenticate.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage**
2. **Existing**.
3. Click the **Assigned or Unassigned** tab, depending on whether the tokens you want to delete are assigned to a user or are unassigned.
4. Use the search fields to find the token that you want to delete.
5. From the Search results, select the checkbox next to the token or tokens that you want to delete.
6. From the Action menu, click **Delete**.
7. Click **Go**.
8. Click **OK** in the delete dialog box to confirm deletion.

Edit a Token

Edit a token to update information about the token, such as the security domain to which the token is assigned. You can also:

- Enable or disable the token.
- Clear the SecurID PIN.

- Require the user to change the SecurID PIN the next time he or she authenticates with the token. The user can view, clear, and change the PIN options only when the token is assigned.
- Specify whether the user must enter a SecurID PIN.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Click the **Assigned** or **Unassigned** tabs, depending on whether the token you want to edit is assigned to a user.
3. Use the search fields to find the token that you want to edit.
4. From the search results, click the token that you want to edit.
5. From the context menu, click **Edit**.
6. Make any necessary changes to the token record.
7. Click **Save**.

   If you did not save your edits, you can click **Reset** to reset the token record to be as it was before you began editing.

User Assistance for Lost, Stolen, Damaged, or Expired Tokens

Users can request replacement tokens and temporary emergency access tokencodes using the Self-Service Console.

You can provide temporary emergency access tokencodes for users whose tokens are damaged, lost, temporarily misplaced, stolen, or expired. Authentication Manager generates emergency access tokencodes and provides two-factor authentication so that users can authenticate until their token issue is resolved. For more information, see Exporting and Importing Users and Tokens Between Deployments.

Note: You cannot assign emergency access tokencodes to an expired token. Replace the token before providing temporary access.

You must replace permanently lost, stolen, damaged, or expired tokens. For more information, see Assign a Replacement Token.

Assign a Replacement Token

You can assign a replacement token to a user if a user's token has been permanently lost or destroyed, or if the current token has expired.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.
2. Use the search fields to find the token that you want to replace.
3. From the search results, click the token that you want to replace.
4. Click **Replace with Next Available Token**.

Resynchronize a Token

A token must be resynchronized when the tokencode displayed on the token does not match the tokencode generated by Authentication Manager. When the tokencodes do not match, authentication attempts fail. Depending on your configuration, users can resynchronize tokens with the Self-Service Console. You can also use the Security Console to resynchronize tokens.

Before You Begin

You need access to the tokencodes. The user can read tokencodes to you over the phone.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user whose token needs to be resynchronized.
3. Click the **Assigned** or **Unassigned** tab.
4. From the search results, click the user whose token needs to be resynchronized.
5. From the context menu, click **SecurID Tokens.**
6. Click the token that you want to resynchronize.
7. Click **Resynchronize Token**.
8. Enter the tokencode that is displayed on the user's token.
9. Wait for the tokencode to change, and then enter the new tokencode.
10. Click **Resynchronize**.

Exporting and Importing Users and Tokens Between Deployments

You can export and import token records and user records between two Authentication Manager 8.1 deployments. You might do this when merging two deployments or to move tokens from one deployment to another. You can export and import tokens, or you can export and import users with tokens. You export from the source deployment and import to the target deployment.You can move tokens that are assigned or unassigned, and reassign the tokens to different users on the target deployment. Authentication Manager encrypts the export file to ensure that the process is secure.

Impact of Export and Import on Authentication

Moving users to a new deployment does not interrupt authentication because the exported data from the source deployment is not deleted. Users can still authenticate to the source deployment even after you have imported their records to the target deployment. You must manually delete the users from the source deployment.

Impact of Export and Import on Identity Sources

Authentication Manager handles the export and import of users differently for internal and external identity sources.

Note: You select identity sources on the identity source mapping page.

Exporting from an External Identity Source and Importing to an External Identity Source

If the source and target deployments both store user records in external identity sources (an LDAP directory server), Authentication Manager creates reference records in the target deployment that point to each user’s record in the LDAP directory sever. The users being moved must have the same User IDs in the source and target deployments.

The following apply:

- If the user record already exists and a user is already assigned one or more tokens in the source deployment, Authentication Manager does not import the user and token(s). Instead, Authentication Manager logs an exception message.
- If the user record already exists and the user has no assigned tokens in the target deployment, Authentication Manager updates the user record on the target deployment and imports the tokens. Authentication Manager writes a warning message to the system logs.

Exporting from an Internal Identity Source and Importing to an Internal Identity Source

If the user records are stored in the internal database in both the source and target deployments, Authentication Manager adds new records to the internal database in the target deployment only if the records do not already exist. If the user record already exists in the target deployment, the record is not duplicated and the user and all linked tokens are ignored.

Exporting From an Internal Identity Source and Importing to an External Identity Source

When the source deployment uses an internal identity source and the target deployment uses an external identity source, the following apply:

- If the user record already exists and a user is already assigned one or more tokens, Authentication Manager does not import the user and token(s). Instead, Authentication Manager logs an exception message.
- If the user record already exists and the user has no assigned tokens in the target deployment, Authentication Manager updates the user record on the target deployment and imports the tokens. Authentication Manager writes warning message to the system logs.

Exporting From an External Identity Source and Importing to an Internal Identity Source

When the source deployment uses an external identity source, users’ LDAP passwords are not exported. The user records are imported to the internal database without a password and password authentication is disabled. If the users need password authentication, you must reset the passwords, or the user must use the Self-Service Console to create a password. For more information, see the Security Console Help topic “Enable Users to Reset Passwords After User and Token Export.” If the user record already exists in the target deployment, the record is not duplicated and the user and all linked tokens are ignored.

Impact of Export and Import on Users

The export and import operations affect user records in the following ways.

- If the exported users are enabled for risk-based authentication (RBA) on the source deployment but the target deployment does not have an RBA license, the users are disabled for RBA after the import. If the target deployment has an RBA license, the user is imported with the same status as on the source deployment, either enabled or disabled for RBA.
- If exported users have a RADIUS profile or a user alias on the source deployment, the users are disabled for RADIUS profiles and aliases on the target deployment. Users will not be able to authenticate using RADIUS. For more information, see RADIUS Profiles on page 303 and the Security Console Help topic “Assign a User Alias to a RADIUS Profile.”
- If the source and target deployments have different PIN policies, each user may need to change his or her PIN when logging on to the target deployment for the first time to conform to the different PIN standards.
- Users’ security questions and answers are exported if the following conditions are met on the target deployment:
  - The language is the same on both deployments. If the language does not match, the user is imported without the security question answers. RSA recommends that the source and the target deployments use the same language.
  - The same security questions must exist on both deployments. If the questions are not the same, the user is imported without the security question answers.
  - If the number of questions the user must answer on the target deployment is less than or equal to the required number on the source deployment, the users and answers are imported. If the target deployment requires users to answer more questions than the source deployment requires, the users are imported without the answers. Users will have to reconfigure security questions and answers when they log on to the target deployment for the first time. For more information, see Managing Security Questions on page 126.
  - If a user in external identity source is already registered on the target deployment, the user and the user’s answers are not imported.

- On-demand authentication (ODA) is supported if the Mobile Number attribute definition is part of the identity attribute definitions and have a Short Message Service (SMS) service provider. Mobile Number is the only extended attribute that is exported. If Mobile Number is part of the user record, it is exported and cannot be excluded. If SMS is configured on the target deployment, users can authenticate using the mobile number.
- Software token profiles are not imported. The association between the profile and the token is imported if the same profiles exist on the source and target deployments. Authentication Manager handles the import of software token profiles as follows:
  - If the names of the software token profiles on the source and target deployments match, the tokens are imported with the software token profile association preserved.
  - If the names of the software token profiles on the source and the target deployments do not match, the tokens are imported, but the software token profile is not associated with the tokens. The software token profile does not affect authentication, but it does affect token distribution. By default, if these tokens are either lost or damaged or need replacement, they cannot be replaced through the Self-Service Console. RSA recommends that users request a new token when these tokens need to be replaced. As an alternative, the administrator can redistribute them from the Security Console using a new profile, so replacements can be requested. However, this would affect authentication for the redistributed token. For more information, see Software Token Profiles on page 190.
  - If the software token profile on the source deployment contains new Device Types that cannot be found on the target deployment, the new Device Type is removed from the token when it is imported.
  - If an assigned token is imported with no associated user, the software token profile association is removed and the Device Type is reset to the default device definition type.

Download the Encryption Key

The encryption key is the public key corresponding to an RSA public-private key pair. The key ensures the following:

- Token and user records being exported can be imported only to the target deployment.
- The export data is encrypted, thus preventing data from being read or tampered with in transit.
- The source and target deployments communicate only with each other.

You must download the encryption key from the target deployment before exporting users or tokens from a source deployment.

Procedure

1. In the Security Console of the target deployment, click **Administration** > **Export/ Import Tokens and Users** > **Download Encryption Key**.
2. Click **Download Now**.
3. Use the File Download dialog box to select a location for the encryption key, and click **Save**.
4. Complete the save operation to your local directory, as required by your browser.
5. Click **Done**.

Next Steps

and Export the tokens or users and tokens from the source deployment. See Export Tokens on page 210 and Export Users with Tokens on page 212.

Export Tokens

Use the Security Console to export token records from a deployment. The records can subsequently be imported into another deployment.

Important: If the tokens are assigned to a user on the source deployment, they are imported to the target deployment in an unassigned state.

Before You Begin

- Download the encryption key from the target deployment where you will import these tokens. See Download the Encryption Key on page 209.
- Select the security domain where the tokens being exported are located. All tokens from that security domain will be exported. If you want to export specific tokens, move the tokens into a temporary security domain and export only that security domain.

Procedure

1. In the Security Console of the source deployment, click **Administration > Export/Import Tokens and Users > Export Tokens and Users**.
2. In the **Encryption Key Location** field, browse to the encryption key that you downloaded from the target deployment.
3. In the **Export Job Name** field, specify the name of the job that will handle the export task. RSA recommends you keep the default job name. If you edit the job name, it must be unique.
4. In the **Export Type** field, select **Tokens Only**.
5. Click **Next**.
6. From the Token Selection page, in the **Security Domain** field, select the source security domain. Only tokens from this security domain will be exported.
7. In the **Subdomains** field, select **Include subdomains** only if you want to include the subdomains of the selected security domain.

8. In the **Status** field, select the status of the tokens to export.
9. Click **Export**.

   You are directed to the Export/Import Status page. The progress of the export is automatically refreshed. You do not need to refresh the page.
10. Click **Download File** to download and save the export file to your local machine.
11. Run the System Log Report to view the results of the export. For more information, see Reports on page 329.

Next Steps

Import tokens to the target deployment. See Import Tokens from Another Deployment on page 211.

Import Tokens from Another Deployment

You can import tokens that were exported from another deployment. Custom token attributes will not be imported with the token data. Standard token attributes are imported. Software token profiles are not imported. The association between the profile and the token is imported if the exact same profiles exist on the source and target deployments. For information on how importing tokens affects software token profile association, see Impact of Export and Import on Users on page 208. Duplicate tokens that are not assigned in the source deployment are not imported to the target deployment.

This topic describes how to import tokens that were exported from a different deployment. To import a new token record file, see Import a Token Record File on page 188.

Before You Begin

- Export the tokens from the source deployment. See Export Tokens on page 210.
- RSA recommends that you create a new security domain on the target deployment for the tokens being imported. This makes it easier to isolate the new data and to verify its accuracy. After you are satisfied that the import is correct, you can move this data to another suitable security domain.

Procedure

1. In the Security Console of the target deployment, click **Administration > Export/Import Tokens and Users > Import Tokens and Users.**
2. In the **Import Job Name** field, specify the name of the import job.
3. Select the import file location.
4. Click **Next**.
5. On the **Security Domain Selection** page, select the target security domain for the imported tokens. You can only select one security domain.
6. Click **Next**.
7. On the **Pre-Import Summary** page, review the import operation details for accuracy.

8. Click **Import**. You are directed to the Export/Import Status page. The status of the import is automatically refreshed.

   When the import is complete, the tokens are in the security domain that you selected in an unassigned state.

9. Run a report to view the results of the import job. Use the **Imported Users and Tokens Report** template. For more information, see Reports on page 329.

   Note: In the Imported Users and Tokens Report template, in the **Job Name** field, RSA recommends that you do not select a name of the import job in the template. Only select the name of the import job when you run the report. If you select a name of the import job in the template, every report you run will have the same name.

Export Users with Tokens

Use the Security Console to export users with tokens from a deployment. The records can subsequently be imported into another deployment. Only users with assigned tokens will be exported.

You can add users to groups and choose only those groups at export time. You can use groups to filter users, but the groups are not exported, and group memberships are not exported.

For information on how exporting users affects risk-based authentication (RBA), on-demand authentication (ODA), and RADIUS usage, see Impact of Export and Import on Identity Sources on page 207.

Before You Begin

- Download the encryption key from the target deployment where you will import these users and tokens. See Download the Encryption Key on page 209.
- Make sure you understand how this operation will affect the identity sources. See Impact of Export and Import on Identity Sources on page 207.
- Select the security domain where the user records being exported are located. It is possible for the tokens to reside in a different security domain than the user records. Tokens follow their user records.

Procedure

1. In the Security Console of the source deployment, click **Administration** > **Export/Import Tokens and Users** > **Export Tokens and Users**.
2. In the **Encryption Key Location** field, browse to the encryption key that you downloaded from the target deployment.
3. In the **Export Job Name** field, specify the name of the export job. RSA recommends you keep the job name default. If you edit the job name, the new name must be unique.
4. In the **Export Type** field, select **Users with Tokens.**
5. Click **Next**.

6. From the User Selection page, in the **Security Domain** field, select the security domain where the users being exported are located.
7. In the **Subdomains** field, select **Include subdomains** only if you want to include the subdomains of the selected security domain.
8. In the **User Selection** field, do one of the following:
   - Export all users in the selected security domain.
   - Search for groups of users to export. Within these groups, only users in the selected security domain and its subdomains are exported. Users in other security domains are ignored. Tokens associated with the users being exported are exported regardless of security domain.

   If you export by group, find and move the groups with the users you want to export from the **Available Groups** box to the **Selected Groups** using the arrow buttons.
9. Click **Export**.

   You are directed to the Export/Import Status page. The progress of the export is automatically refreshed.
10. From the Export/Import Status page, click **Download File** to download and save the export file to your local machine.
11. Run the System Log Report to view the results of the export. For more information, see Reports on page 329.

Next Steps

Import users with tokens to the target deployment. See Import Users with Tokens on page 213.

Import Users with Tokens

You can import token records and user records that were previously exported from another deployment. Users are imported into a single security domain, without group memberships. An unassigned token on the target deployment gets overwritten by a matching assigned token in the export file.

For information on how exporting users affects risk-based authentication (RBA), on-demand authentication (ODA), and RADIUS usage, see Impact of Export and Import on Identity Sources on page 207.

Software token profiles are not imported. The association between the profile and the token is imported if the same profiles exist on the source and target deployments. For information on how to retain software token profile association for importing users with tokens, see Impact of Export and Import on Users on page 208.

The following information is not also imported:

- Custom token attributes
- Extended user attributes
- Risk-based authentication device history

Before You Begin

- Understand how this operation will affect identity sources. See Impact of Export and Import on Identity Sources on page 207.
- Export the users and tokens from the source deployment.
- If the users being imported will be stored in an external identity source on the target deployment, make sure the users already exist in the LDAP directory server that the target deployment uses.
- Make sure you use the same User ID naming conventions on the source and the target deployments.
- RSA recommends that you create a new security domain on the target deployment for the users and tokens being added. This makes it easier to isolate the new data and to verify its accuracy. Once you are satisfied that the import is correct, you can move this data to another suitable security domain.

Procedure

1. In the Security Console of the target deployment, click **Administration** > **Export/Import Tokens and Users** > **Import Tokens and Users**.
2. In the **Import Job Name** field, specify the name of the import job.
3. Select the import file location.
4. Click **Next**.
5. On the Security Domain Selection page, select the target security domain for these users and tokens. You can only select one security domain.
6. Click **Next**.
7. From the Identity Source Mapping page, select the identity source(s) on the target deployment where the system can find the associated user. If you select internal database, the user is created in the internal database on the target deployment.
8. Click **Next**.
9. On the Pre-Import Summary page, review the import operation details for accuracy.
10. Click **Import**. You are directed to the Export/Import Status page. The import status is automatically refreshed.

    When the import is complete, the users are in the security domain that you selected with their assigned tokens.
11. Run a report to view the results of the import job. Use the **Imported Users and Tokens Report** template. For more information, see Reports on page 329.

    Note: Make sure you specify the name of the import job when you run the report. Do not specify the name in the Job Name field in the Imported Users and Tokens template. Specifying it in the template will cause every report using that template to have the same name.

Next Steps

Inform users that they must configure security questions and answers when they log on to the target deployment for the first time.

10 Deploying On-Demand Authentication

On-Demand Authentication

On-demand authentication (ODA) is a service that allows users to receive on-demand tokencodes delivered by text message or e-mail. You can use ODA to protect resources, such as an SSL-VPN, thin client, or web portal.

When a user logs on to an agent with a valid PIN, the system sends a tokencode to the user by either text message or e-mail. The user is prompted for the tokencode to gain access to the protected resource.

If you use ODA as a primary authentication method, you must install the RSA Authentication Agent software on the resource that you want to protect.

Note: To use SMS delivery, you must establish a relationship with an SMS provider, and integrate SMS with RSA Authentication Manager.

Planning for On-Demand Authentication

If you plan to use on-demand authentication (ODA), you must configure the deployment to send on-demand tokencodes. Users must be enabled to receive on-demand tokencodes.

Authentication Manager can deliver on-demand tokencodes in two ways:

- To mobile phones by text message. You can configure an SMS provider or modem to integrate with Authentication Manager to deliver on-demand tokencodes to a user’s mobile phone. Use the parameters required by the SMS provider or modem vendor. For instructions, see Configuring On Demand Tokencode Delivery by Text Message on page 218.
- To e-mail accounts. You must configure a connection to a Simple Mail transfer Protocol (SMTP) server. For instructions, see Configuring On-Demand Tokencode Delivery by E-mail on page 224.

Note: You can select only one delivery method, either mobile phone or e-mail, per user.

You must enable ODA for users so that they can receive on-demand tokencodes. For instructions, see Configuring Users for On-Demand Authentication on page 228.

Configuring On Demand Tokencode Delivery by Text Message

To send on-demand tokencodes to mobile phones by text message, perform the following tasks:

1. Ensure that Authentication Manager has access to the identity source attributes where you store mobile phone numbers. Authentication Manager automatically maps to the mobile attributes in the internal database and an LDAP directory.

   (Optional) Using the Security Console, you can map to custom attributes in the internal database and an LDAP directory. See Identity Attribute Definitions for On-Demand Tokencode Delivery by Text Message on page 218.

2. Configure the HTTP Plug-In for On-Demand Tokencode Delivery on page 219.

Identity Attribute Definitions for On-Demand Tokencode Delivery by Text Message

Authentication Manager 8.1 must have access to the identity source attributes where you store mobile phone numbers and e-mail addresses. Authentication Manager automatically maps to the e-mail and mobile attributes in the internal database and an LDAP directory. Using the Security Console, you can also map to custom attributes in the internal database and an LDAP directory.

If you want to deliver on-demand tokencodes by text message, use the following table to determine the necessary attribute configuration to ensure that Authentication Manager can access user mobile phone numbers.

Identity Sources In Your Deployment	Configuration
Internal database	No attribute mapping required.
At least one LDAP directory identity source, and you want to use the mobile number value in the LDAP directory “mobile” field.	No attribute mapping required. When you add an external identity source, Authentication Manager automatically links to the “mobile” attribute in an LDAP directory. When you configure on-demand tokencode delivery, select Mobile Number from the User Attribute to Provide SMS Destination drop-down menu on the SMS Configuration page.

Identity Sources In Your Deployment	Configuration
At least one LDAP directory identity source, and you want to use the mobile number value in an LDAP directory field other than the “mobile” field.	You may edit the identity attribute definition, Mobile Number, so that it maps to the LDAP directory attribute where you store users’ mobile numbers, or you can create a new identity attribute definition. When you configure on-demand tokencode delivery, select Mobile Number from the User Attribute to Provide SMS Destination drop-down menu on the SMS Configuration page.
At least one LDAP directory, and you want to store user mobile numbers in the internal database because the LDAP directory does not contain mobile numbers.	You must create an identity attribute definition for user mobile numbers that is always stored internally. When you configure on-demand tokencode delivery, choose the attribute that you created from the User Attribute to Provide SMS Destination drop-down menu on the SMS Configuration page.

Configure the HTTP Plug-In for On-Demand Tokencode Delivery

You can configure a deployment to integrate with Short Message Service (SMS) providers or modems using HTTP, HTTPS, or XML-over-HTTP to deliver on-demand tokencodes to a user’s mobile phone.

The HTTP request communicates the following delivery information to your SMS provider or modem:

- The text message, which includes the on-demand tokencode
- The mobile phone number
- Any other information required by your SMS provider or modem

The maximum length of the text message is 140 bytes and the number of characters depends on the type of character encoding used by the SMS provider. The full payload of 140 bytes can support 160 7-bit characters, 140 8-bit characters, or 70 16-bit characters. The $OTT and $Lifetime variables are replaced with the actual values, which uses some of the available characters.

Important: HTTP connections are not secure. Sensitive information, such as a tokencode, may be exposed. For secure connections, configure HTTPS.

Before You Begin

- Go to https://gallery.emc.com/community/marketplace/rsa?view=overview to download the implementation guide that contains configuration values and parameters for supported SMS providers and modems. Each SMS provider has its own implementation guide. You can search for providers by name or get the full list by browsing to **Product Category > SMS Providers** on the site. You can find the implementation guide on the **Collateral** tab for each provider.
- If your SMS provider requires digital certificates or if HTTP connections are redirected to an HTTPS site, secure the certificate from your provider and save it locally. Importing the certificate enables Authentication Manager to validate the server to which the on-demand tokencodes are sent. Authentication Manager accepts all connections signed by this certificate. For instructions, see the Security Console Help topic "Import a Digital Certificate."
- Make sure that all users' destination mobile phone numbers meet the following requirements:
  - The mobile phone numbers must include country codes. If they are not already stored with country codes, select a country code when you configure on-demand tokencode delivery to mobile phones.
  - End the mobile phone number with a number.
  - The mobile phone number may begin with the plus (+) character.
  - Use the following characters or a blank space for separators: . - ( ).
  - Do not use alphabetic characters or any other characters not mentioned in this list.

  The following are examples of valid destination mobile phone numbers:

  +1 123 123 1234
  +44 1234-123-123-1
  123 123 1234
  123.123.1234
  (123) 123-1234

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Under Authentication Settings, click **On-Demand Tokencode Delivery**.
3. Click the **SMS Configuration** tab.
4. Under **Tokencode Delivery by SMS**, do the following:
   a. Select **Enable the delivery of on-demand tokencodes using SMS service**.
   b. From the **User Attribute to Provide SMS Destination** drop-down menu, select the user attribute that provides the mobile phone numbers used to deliver on-demand tokencodes to users.

If you use the internal database for user information, you can map to an attribute there, such as telephone number, or create a custom attribute. If you use an external identity source, you can choose an attribute that is mapped to an attribute in the external identity source (for example, telephone number).

c. From the **Default country code** drop-down menu, select a country code to prepend to the destination mobile phone numbers.

   Country codes are required for all on-demand tokencode destination mobile phone numbers. Select a country code only when the mobile phone numbers to which you send on-demand tokencodes are not already stored with country codes.

d. From the **SMS Plug-In** drop-down menu, select **HTTP.**

5. Under **SMS Provider Configuration**, do the following:

   a. In the **Base URL** field, enter the base URL for your SMS provider or modem.

   b. Import a certificate when your SMS provider requires digital certificates or for when HTTP connections are redirected to an HTTPS site. For instructions, see the Security Console Help topic "Import a Digital Certificate."

   Note: If your SMS provider does not require digital certificate or the base URL does not use HTTPS, this step is not required.

   c. From the **HTTP Method** drop-down menu, select the method required by your SMS provider, and configure one of the following.

      – For GET or POST. Enter the parameters supplied by your SMS provider.

      – For XML. Enter the XML request body supplied by your SMS provider.

   Note: If your SMS provider uses XML-over-HTTP, select **XML** for the **HTTP Method**.

   d. In the **Parameters** field, enter the parameters required by Authentication Manager and your SMS provider or modem. For more information, see SMS HTTP Plug-In Configuration Parameters on page 222.

   e. In the **Account User Name** field, enter the user name for your SMS service provider account. This is provided by your service provider.

   f. In the **Account Password** field, enter the password for your SMS service provider account. This is provided by your service provider.

   g. In the **Connection Timeout** field, enter a connection time-out between 1,000 and 3,600,000 milliseconds. The default value is 5,000 milliseconds.

   h. In the **Success Response Code** field, enter the success response code required by your SMS provider.

   i. In the **Response Format** field, enter the success response format required by your SMS provider.

Note: See your standard JDK documentation for more information on regular expressions.

6. (Optional) Under **SMS HTTP(S) Proxy Configuration**, do the following:
   a. In the **Proxy Hostname** field, enter a hostname for your HTTP proxy.
   b. In the **Proxy Port** field, enter your proxy port number.
   c. In the **Proxy User** field, enter your proxy user name.
   d. In the **Proxy Password** field, enter your proxy password.
7. (Optional) Under **Test SMS Provider Integration**, do the following:
   a. In the **Mobile phone number to test** fields, select a country code, and enter the number for mobile phone that receives the test message.
   b. Click **Send Test Text Message**.

      The system saves all of your changes before the test is conducted. If the connection is unsuccessful, you see an error message.
8. On the **Tokencode Settings** tab, configure the following:
   a. In the **On-Demand Tokencode Message** field, enter the text that you want to display in the text message that contains the on-demand tokencode.

      You must leave the $OTT variable in the message. The on-demand tokencode is inserted in place of this variable.
   b. In the **On-Demand Tokencode Lifetime** field, enter the length of time that on-demand tokencodes are valid after they are delivered to the user.
9. Click **Save**.

SMS HTTP Plug-In Configuration Parameters

Configuration values for the parameters contain variable elements, which are replaced with corresponding values during SMS transmission. For example, ${cfg.user} is replaced with the “Account User Name” configuration value.

The following elements are required in the parameters string.

Element	Field Corresponding to Element
$msg.address	User Attribute to Provide SMS Destination
$msg.message	On-Demand Tokencode Message
$cfg.user	Account User Name
$cfg.password	Account Password

The +, &, and = characters are reserved for use with value pairs in the parameters string, for example, text=${msg.message}&clientid=${cfg.user}.

If the +, &, or = characters are used in any name value data that is retrieved by the parameters string, you must enter the following elements in the parameter string:

Character	Element
+	${plus}
&	${ampersand}
=	${equal}

For example, if you want to include the + character with a foreign phone number, use the ${plus} element as follows: destaddr=${plus}${msg.address}

Configuration Example

In this example, an SMS provider requires message data in the following format:

```
https://sms.rsa.com/http/send?user=john&password=doe123&extr
aparam=123456&to=2223334444&text=Meet+me+at+home
```

This example requires the following configuration:

Configuration Parameter	Value
Base URL	https://sms.rsa.com/http/send
HTTP Method	GET
Parameters	user=$cfg.user&password=$cfg.password&extraparam=123456&to=$msg.address&text=$msg.message
Account User Name	john
Account Password	doe123
Success Response Code	RESULT:OK
Response Format	RESULT:OK

Change the SMS Service Provider

You can change the SMS service provider.

Procedure

Do one of the following:

- Reconfigure the HTTP Plug-In. For more information, see Configure the HTTP Plug-In for On-Demand Tokencode Delivery on page 219.
- Implement a custom plug-in. For more information, contact your RSA sales representative.

Configuring On-Demand Tokencode Delivery by E-mail

To send on-demand tokencodes to e-mail accounts, perform the following tasks:

1. Configure the SMTP Mail Service on page 224
2. Ensure that Product Name (Short) can access the database attribute where you store users' e-mail addresses. See Identity Attribute Definitions for On-Demand Tokencode Delivery by E-Mail on page 225
3. Configure E-mail for On-Demand Tokencode Delivery on page 227

Configure the SMTP Mail Service

If you plan to use e-mail to deliver on-demand tokencodes, you must configure all Authentication Manager instances to send Simple Mail Transfer Protocol (SMTP) messages.

SMTP settings might not be immediately visible through the replica instance. Data should replicate within 10 to 20 minutes.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Click **E-Mail (SMTP)**.
3. Select an instance**.**
4. Click the **Next** tab.
5. In the **Hostname** field, enter the hostname of the mail server to which this instance will send messages.
6. In the **Port** field, enter the destination port number for the mail server.
7. In the **From E-mail Address** field, enter the e-mail address that you want to display in all outgoing e-mail from this instance. Use an e-mail address to which users can respond.
8. (Optional) If your mail server connection requires a User ID and password, select **Logon Required**.
9. If logon is required, do the following:
   a. Enter the administrator's User ID in the **User ID** field. This User ID must already be defined in the SMTP mail server.
   b. Enter the password defined for the User ID in the **Password** field.
   c. Re-enter the password in the **Confirmed Password** field.
10. In the **Test E-mail Address** field, enter the e-mail address to use for testing this instance.
11. Click **Test Connection** to test the mail service.

12. If you configured the primary instance, you can choose to apply the same settings to the replica instance.
13. After you receive the test e-mail, click **Save**.

Identity Attribute Definitions for On-Demand Tokencode Delivery by E-Mail

If you want to deliver on-demand tokencodes by e-mail, you must ensure that Authentication Manager 8.1 can access the database attribute where you store users’ e-mail addresses.

Use the following table to determine whether additional configuration is required.

Identity Sources In Your Deployment	Configuration
Internal database	Select **E-Mail** to use the e-mail configured for the user and stored in the internal database. Make sure that the configured e-mail address does not require the user to authenticate using an on-demand tokencode. If the e-mail address requires the user to authenticate with an on-demand tokencode, the user cannot retrieve the tokencode. In this case, create an identity attribute definition in the internal database that can store an e-mail address that does not require the user to authenticate with an on-demand tokencode.
At least one LDAP directory identity source that contains e-mail addresses	Select **E-Mail** to use the attribute you mapped to the **E-Mail** field when you configured the identity source. Make sure that the configured e-mail address does not require the user to authenticate using an on-demand tokencode. If the e-mail address configured in your directory requires the user to authenticate with an on-demand tokencode, the user cannot retrieve the tokencode. In this case, create an identity attribute definition, and map it to an LDAP attribute where you store a user e-mail address that does not require the user to authenticate with an on-demand tokencode.

Identity Sources In Your Deployment	Configuration
At least one LDAP directory identity source, and you want to use the e-mail address value in the LDAP directory "mail" field.	No attribute mapping required. When you add an LDAP directory, Authentication Manager 8.1 automatically links to the "mail" attribute in an LDAP directory. When you configure on-demand tokencode delivery, select "mail" from the **User Attribute to Provide SMS Destination** drop-down menu on the SMS Configuration page.
At least one LDAP directory identity source, and you want to use the e-mail address value in an LDAP directory field other than the "mail" field.	You may edit the "E-mail" identity attribute definition in Authentication Manager 8.1 or create a new one, so that it maps to the LDAP directory attribute that you want to use for e-mail addresses. For more information, see the Operations Console Help topic "Edit LDAP Directory Identity Sources." When you configure on-demand tokencode delivery, select "mail" from the **User Attribute to Provide SMS Destination** drop-down menu on the SMS Configuration page.
At least one LDAP directory identity source, and you want to store user e-mail addresses in the internal database because the LDAP directory does not contain e-mail addresses.	You must create an identity attribute definition for user e-mail addresses that is always stored internally. When you configure on-demand tokencode delivery, select the attribute that you created from the **User Attribute to Provide SMS Destination** drop-down menu on the SMS Configuration page.

Configure E-mail for On-Demand Tokencode Delivery

You can configure a deployment to send on-demand tokencodes to a user's e-mail address. First you must configure the e-mail server connection for each instance.

Before You Begin

- Confirm that you have the following information:
  - **Hostname.** The hostname of the server you will use to send e-mail notifications.
  - **SMTP port.** The port you will use for e-mail transmissions.
  - **E-mail address.** The address from which the e-mail notifications will be sent.
  - **Logon.** Whether your e-mail server requires a User ID and password.
- Configure a destination e-mail address for each user.

  Use an e-mail address other than the one for which on-demand authentication enables access. For example, make the user's personal e-mail address the destination when the user needs the tokencode to access his or her e-mail account at work.
- See Configure the SMTP Mail Service on page 224. You must do this for each instance in your deployment.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Click **On-Demand Tokencode Delivery**.
3. Click the **E-mail Configuration** tab.
4. Select **Enable the delivery of On-demand Tokencodes through e-mail**.
5. From the **User Attribute to Provide E-mail Destination** drop-down menu, select the attribute that provides the e-mail addresses used to deliver on-demand tokencodes to users.
6. Click **Save**.
7. (Optional) On the **Tokencode Settings** tab, do the following:
   a. In the **On-Demand Tokencode Message** field, enter the text that you want to display in the text message that contains the on-demand tokencode.

      You must leave the $OTT variable in the message. The on-demand tokencode is inserted in place of this variable.

   b. In the **On-Demand Tokencode Lifetime** field, enter the length of time that on-demand tokencodes are valid after they are delivered to the user.
8. Click **Save**.

Configuring Users for On-Demand Authentication

Users who will receive on-demand tokencodes must be enabled for on-demand authentication (ODA). When a user is enabled, you can specify a delivery method for the tokencodes, the length of time that the user can request on-demand tokencodes, and whether users can set initial PINs using the Self-Service Console. For instructions, see Enable On-Demand Authentication for a User on page 228.

An administrator can clear a PIN that is forgotten, expired, or compromised, and then provide a temporary PIN to the user. An administrators can require PIN changes. For more information, see PINs for On-Demand Authentication on page 229.

You can configure the Self-Service Console to allow users to update their destination phone numbers and e-mail addresses. This configuration option saves time and effort for the administrators. For instructions, see Enable Users to Update Phone Numbers and E-mail Addresses on page 230.

Enable On-Demand Authentication for a User

On-demand authentication (ODA) delivers a one-time tokencode to a user's mobile phone or e-mail account. On-demand tokencodes expire after a specified time period, enhancing their security. ODA protects company resources that users access through SSL-VPNs, web portals, or browser-based thin clients.

Enable ODA for users so they can receive on-demand tokencodes.

Before You Begin

Configure On-Demand Tokencode Delivery. For more information, see Configuring On Demand Tokencode Delivery by Text Message on page 218 and Configuring On-Demand Tokencode Delivery by E-mail on page 224.

Procedure

1. In the Security Console, click **Authentication** > **On-Demand Authentication** > **Enable Users**.
2. Use the search fields to find the user for whom you want to enable ODA. Some fields are case sensitive.
3. Enable users for ODA.

   To enable one user, do the following:

   a. From the search results, click the user that you want to enable for ODA.

   b. From the context menu, click **Enable for ODA**.

   To enable multiple users, do the following:

   a. From the list of available users, select the checkboxes next to the ones that you want to enable for ODA.

   b. Click **Enable for ODA**.
4. Use the **Send On-Demand Tokencodes to** options to select a delivery method for on-demand tokencodes if applicable. Specify an e-mail address or phone number if necessary.

Important: If you elect to send an on-demand tokencode to a user's e-mail address, make sure that the user does not need the on-demand tokencode to access the e-mail account.

5. Use the **Expiration Date** options to specify the length of time the user can request on-demand tokencodes. You can specify an exact date or no expiration date.
6. Use the **Associated PIN** options to specify how the user's initial PIN is created. Create an initial PIN if necessary.
7. Click **Save**.

PINs for On-Demand Authentication

Users must have a PIN for on-demand authentication (ODA). These PINs are governed by the user’s security domain PIN policy. Be aware of the following tasks related to PINs for ODA:

- Setting a PIN

  Users can set initial PINs using the Self-Service Console. If you want users to do this, you must configure this option when you configure ODA for the user. If you do not want users to set their initial PINs, you can use the Security Console to set users’ initial PINs.

- Clearing a PIN

  You might clear a PIN that is forgotten, expired, or compromised. If you clear a user’s PIN, you must assign the user a temporary PIN before the user can attempt to log on to a resource protected with ODA. Use the Security Console to clear a PIN and provide the temporary PIN to the user.

- Changing a PIN

  Users who are enabled for ODA can change their ODA PINs after logging on to the Self-Service Console or during authentication. Users need to change their PINs when the PINs expire or when you force a PIN change. You might force a PIN change when you think that the PIN is compromised. If you want to force a PIN change, use the Security Console to clear the user’s PIN and set a temporary PIN.

For instructions on how to require users to set their initial PIN, see Enable Users to Set Their Initial On-Demand Authentication PINs on page 229. For instructions on how to clear a temporary PIN and force users to change their initial PIN, see Set a Temporary On-Demand Tokencode PIN for a User on page 230.

Enable Users to Set Their Initial On-Demand Authentication PINs

Users need a PIN before attempting to use on-demand authentication (ODA) to access a protected resource. You can either set the initial PIN for the user or you can enable users to set their initial PINs and thus relieve administrators of this task.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user for whom you want to enable.

3. Click the user for whom you want to enable.
4. Click **SecurID Tokens**.
5. Under **On-Demand Authentication**, if the user is not enabled for ODA, select **Enable user for on-demand authentication**.
6. Select **Require user to set the PIN through the RSA Self-Service Console**.
7. Click **Save**.

Set a Temporary On-Demand Tokencode PIN for a User

Use the Security Console to clear a user's on-demand tokencode PIN and assign a temporary PIN.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user for whom you want to set an initial on-demand tokencode PIN.
3. Click the user.
4. Click **SecurID Tokens**.
5. Select **Clear existing PIN and set a temporary PIN for the user**.
6. Enter a temporary PIN.
7. Click **Save**.
8. Securely communicate the temporary PIN to the user.

Enable Users to Update Phone Numbers and E-mail Addresses

You can configure the Self-Service Console to allow users to update their destination phone numbers and e-mail addresses for on-demand tokencode delivery.

Note the following:

- Users can update their phone numbers and e-mail addresses only if this information is stored in the internal database.
- All user attributes that are stored in an external identity source are read-only. Users cannot modify this information through the Self-Service Console.
- Required fields are editable.

Before You Begin

- Configure Authentication Manager 8.1 to display the Change Delivery Option link on the Self-Service Console. The link displays on the My Account page when the user is enabled for on-demand authentication.
- Verify that at least one attribute (either SMS phone number or e-mail address) is editable and viewable, or that both attributes (SMS phone number and e-mail addresses) are viewable, but not editable.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. Under **Customization**, click **User Profile**.
3. From the **Choose an Identity Source** drop-down list, select **Internal Database**.
4. Click **Next**.
5. Do one or both of the following:

   To enable users to update a phone number:

   a. Under **Custom Attributes**, select **View and manage user profile attribute details** for **Mobile Number**.

   b. From the **Make Field (for Update Profile)** drop-down list, select **Editable**.

   c. For **Display Label**, accept the default label or replace it with one of your own.

   To enable users to update an e-mail address:

   a. Under **Core Attributes**, select **View and manage user profile attribute details** for **Email**.

   b. From the **Make Field (for Update Profile)** drop-down list, select **Editable**.

   c. For **Display Label**, accept the default label or replace it with one of your own.
6. Click **Save**.

On-Demand Authentication with an Authentication Agent or a RADIUS Client

Using an on-demand tokencode requested through an authentication agent or RADIUS client differs from the same process when using a tokencode requested through the Self-Service Console, or an RSA SecurID hardware or software token. In each case, the authentication agent prompts the user to enter a User ID and passcode. However, with an on-demand tokencode, the following process occurs:

1. The user accesses a protected resource, and the agent prompts the user for a User ID and passcode.
2. The user enters his or her User ID and, at the passcode prompt, an on-demand authentication (ODA) PIN, not passcode.

   When a user who is enabled for the on-demand tokencode service enters an ODA PIN at the passcode prompt, Authentication Manager recognizes that the user is actually making a request for an on-demand tokencode.
3. Authentication Manager sends a tokencode to the user.
4. The authentication agent prompts the user to enter the next tokencode.
5. The user enters the received on-demand tokencode.

RSA recommends that you inform your users that they cannot simply follow the prompts. Some agents may support changing the prompts to make this less confusing, although this only works if you have an ODA-only user population.

Additionally, if a user cancels out of the next tokencode prompt or waits too long to enter the on-demand tokencode, the tokencode can still be used (with the PIN) to authenticate. For example, the user can attempt to authenticate again, and when the authentication agent or RADIUS client prompts the user for the passcode, the user may enter the PIN and on-demand tokencode as the passcode and successfully authenticate.

New PINs and On-Demand Tokencodes for Authentication Agents and RADIUS Clients

On-demand tokencodes always require a PIN. As a result, an administrator cannot clear the PIN of a user with an on-demand tokencode without assigning a temporary PIN. The user experience of changing the PIN of an on-demand tokencode depends on the method used to request the tokencode.

For a tokencode requested through an authentication agent or RADIUS client:

1. The user attempts to access a protected resource, and the agent prompts the user to enter a User ID and passcode.
2. When prompted for the passcode, the user enters the current PIN, which could be an expiring PIN or a temporary PIN assigned by the administrator.
3. The agent prompts the user to enter a new PIN and to confirm the new PIN.
4. The user enters a new PIN and confirms the new PIN.
5. The agent prompts the user to enter a passcode.
6. The user enters the new PIN.
7. Authentication Manager sends the on-demand tokencode to the user.
8. When the agent prompts the user for next tokencode, the user enters the received on-demand tokencode.

Restrictions of On-Demand Tokencodes

The following restrictions apply to users of on-demand tokencodes:

- Users cannot perform trusted-realm authentications.
- Users cannot authenticate using an alias, except when authenticating through an authentication agent.
- The PIN for an on-demand tokencode should not be the same as a fixed passcode assigned to the user.
- EAP32-enabled authentication agents do not support on-demand tokencodes.

11 RSA Self-Service

RSA Self-Service Overview

RSA Self-Service automates the authenticator deployment process and provides a Self-Service Console. The Self-Service Console is a web-based interface that you configure to provide a variety of services to Authentication Manager users.

RSA Self-Service includes the following components:

Self-Service. A configurable console where users can manage many day-to-day tasks related to authentication, token, and user accounts without calling the Help Desk. Self-Service can reduce the call volume to your Help Desk and aid in providing 24-hour support for your users.

Provisioning. A web-based workflow system for the rapid deployment and lifecycle management of RSA SecurID authenticators. Users can perform many of the steps in the authenticator deployment process, and the system automates the workflow. Provisioning can reduce administrative overhead associated with deploying authenticators, especially in large-scale deployments.

RSA recommends installing the Self-Service Console on a secure server on a web tier in the DMZ. This installation offers the convenience of Self-Service to remote users, while protecting your internal resources. Self-Service configuration menus are integrated into the RSA Security Console. You can customize the Self-Service Console, for example to display your logo, and the Self-Service features that it displays.

The tasks that users can perform from the Self-Service Console depend on the license installed, the options that you enable, and whether the user’s data is stored in an internal or external identity source. For more information, see Select Security Domains for Self-Service on page 236.

Self-Service Console User Experience

Depending on the configuration, users may perform these tasks from the Self-Service Console:

- Enroll as Self-Service user
- Configure security questions for identity confirmation
- Request authenticators
- Update user profile
- Change Self-Service Console password
- Clear the risk-based authentication (RBA) device history to unregister devices
- Change e-mail address or phone number for on-demand authentication (ODA)

- Manage the ODA PIN
- View user group membership
- Test and resynchronize tokens
- Troubleshoot and report problems with tokens
- Request emergency access for lost, broken, or temporarily unavailable tokens
- Unblock and reset PINs
- Request on-demand authentication

User Enrollment

You can configure the system to allow new users to request an account in the internal database. This is known as enrollment. Users who already have accounts in the internal database or any other identity source do not need to enroll. By default, such users can access the Self-Service features that you configure.

At enrollment, users must select a security domain into which they want to be enrolled. You configure Self-Service to determine whether users must also do the following.

- Configure a user profile.
- Configure security questions.
- Select a user group.

Identity Sources for Self-Service Users

The identity source where the users' accounts are stored affects which actions users can perform using the Self-Service Console. You can use the internal database, Active Directory, and Oracle Directory Server as identity sources.

If an Active Directory or Oracle Directory Server has the "change password during next logon" option set, you cannot enroll users in Self-Service.

Using the Internal Database as an Identity Source

Authentication Manager can read and write data to the internal database. Users whose accounts are in the internal database can use the Self-Service Console to perform all actions for which their administrator has configured permissions. For example, these actions may include resetting passwords or entering phone numbers or e-mail addresses on the Identity Confirmation Method configuration page for on-demand authentication with risk-based authentication (RBA).

Using Active Directory as an Identity Source

Users whose accounts are in Active Directory cannot use the Self-Service Console to perform any actions that require Authentication Manager to access Active Directory. For example, users whose accounts are stored in Active Directory cannot use the Self-Service Console to change their Self-Service passwords. Authentication Manager has read-only access to Active Directory for all user and user group data.

Using Oracle Directory Server as an Identity Source

Users whose accounts are in Oracle Directory Server cannot use the Self-Service Console to perform any actions that require Authentication Manager to access Oracle Directory Server. Authentication Manager has read-only access to Oracle Directory Server for all user and user group data.

Configuring Self-Service

You must configure Self-Service to provide the features and services that you want for your Self-Service Console users. You can specify which users will have access to the Self-Service Console and the credentials that they need to log on. The following list is a guide to configuring Self-Service.

Procedure

1. Enable Enrollment by Selecting Identity Sources on page 235.
2. Select Security Domains for Self-Service on page 236.
3. Select User Groups for Self-Service on page 237.
4. User Profile Configuration for Self-Service on page 238.
5. Set the Authentication Method for the Self-Service Console on page 239.
6. Security Questions for Self-Service on page 240.
7. Configure E-mail Notifications for Self-Service User Account Changes on page 240.

Enable Enrollment by Selecting Identity Sources

Enabling enrollment allows new users to request accounts in the internal database. By default, the only identity source that you can select to enable enrollment is the internal database. Users cannot enroll in any external identity sources.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. Click **Select identity sources**.
3. In the **Display Name for Identity Source Selection Component** field, enter user-friendly text about choosing an identity source.
4. Select **Allow users to request accounts in this identity source** to make the internal database available to users at enrollment.
5. Click **Save**.

Select Security Domains for Self-Service

You must select the security domains from which users can enroll in Self-Service. The security domain in which a user enrolls determines which administrators manage the user, and which security policies are applied to the user.

Consider the following:

- Any security domains that get many Help Desk calls or deploy a large number of tokens would benefit from self-service and provisioning.
- Do not select security domains that contain users who should not use Self-Service or provisioning.

To clarify the selection process for users, you can customize the names and descriptive text of all available security domains that appear on the Self-Service Console. For example, if the security domains represent departments in your company, you can label each security domain with the department name and instruct users to pick their departments.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. Click **Select Security Domains**.
3. In the **Display Name for Security Domain Selection Component** field, enter user-friendly text about choosing a security domain.

   For example, if you have a security domain for each department in your organization, you might enter “Select your department.”
4. Click **Select More Domains** to view a tree showing all lower-level security domains.
5. Select the security domains you want to make available.
6. Click **Make Available**.
7. In the **Display Name** field, optionally add a descriptive name for the security domain. For example, enter “Human Resources.”

   The display name appears on the Self-Service Console and can be helpful to users when they select a security domain.
8. Click **Save**.

Select User Groups for Self-Service

If you use provisioning and restricted agents, you can select the user groups that you want to make available to users when they enroll in Self-Service. The user groups in which a user enrolls determine which restricted agents the user can use to authenticate. The user groups that you select are displayed on the Self-Service Console. If you select no user group, the User Group Selection page does not display during enrollment.

When selecting user groups for Self-Service, consider the following:

- Users can request membership in internal groups only. Authentication Manager cannot add users to groups in external identity sources.
- Which user groups provide users with the access to resources that they need
- Whether there are any user groups that you do not want users to access
- Whether there a user group that you want all users to access
- If you set a default group, users can only belong to the default group.
- If you do not use restricted agents, you do not need to select user groups for provisioning.

Note: Users can request additional user group membership after enrolling in Self-Service, as long as the user group resides in the internal database.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. Click **Select User Groups**.
3. Click **Next** to select the internal database, the only identity source that contains user groups that you can make available to users for enrollment.
4. In the **Display Name for User Group Selection Component** field, enter user-friendly text about choosing a user group. For example, if remote access is protected by a restricted agent, you might enter “Select your access method.”
5. Click **Select More Groups** to view a list of available groups for the identity source you selected.
6. Select the user groups you want, and click **Make Available**.
7. (Optional) In the **Display Name** field, add a descriptive name for the user group. For example, enter “VPN.”
8. (Optional) Click the Default Group check box for each user group that you want assigned by default to all new users who enroll through the Self-Service Console.
9. Click **Save**.

User Profile Configuration for Self-Service

User profiles are required for Self-Service enrollment. They contain user attributes such as name, User ID, e-mail address, Self-Service Console password, and mobile number. If you are using the internal database for self-service users, you can specify which user attributes are required, editable, read-only, or hidden from the user in the Self-Service Console. For example, you can allow users to edit their e-mail addresses and mobile numbers, but not their User IDs. All user attributes stored in external identity sources are read-only. Users can view these attributes and report any discrepancies to the administrator.

Before users can view or edit their user profiles, you must populate the users’ profiles, as follows:

New user. If a user is not in the internal identity source or in an external identity source, you must enter the required information into the user’s profile.

User not in Authentication Manager, but in a directory server. The directory server populates the user profile.

In the Security Console, you can use the default user profile or customize it for each identity source that you use. When deciding whether to customize user profiles, consider the following:

- Does your company have different names for some fields in the default user profile, for example, “User name” instead of “User ID”?
- Do you need to add descriptive text to instruct users about what to enter in any fields?
- Do you need to add custom attributes, for example, a home address for users?

If you create custom attributes for an identity source, you can add custom attributes to the user profile. Optionally, you can customize the labels for each attribute.

Customize Self-Service User Profiles

If you are using the internal database for self-service users, you can specify which user attributes are required, editable, read-only, or hidden from the user in the Self-Service Console. You can also customize display labels for each attribute.

Remember:

- All user attributes that are stored in an external identity source are read-only. Users cannot modify this information through the Self-Service Console.
- Required fields are editable.
- If you create custom user attributes for an identity source, you can specify which fields display in the user profile.
- If the e-mail address attribute is editable and Self-Service is configured to send e-mail notifications for changes to the user’s profile or the on-demand authentication delivery option, Authentication Manager sends notification to both the old and new e-mail addresses when the e-mail address is changed.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. Click **User Profiles**.
3. From the **Choose an Identity Source** drop-down list, select an identity source.
4. Click **Next**.
5. In the **Core Attributes** section, select **View and manage user profile attribute details** for the attributes that you want to customize.
6. In the **Custom Attributes** section, select **View and manage user profile attribute details** for the attributes that you want to customize.
7. Click **Save**.

Set the Authentication Method for the Self-Service Console

Users must provide credentials to access the Self-Service Console. If users are not required to have a password, configure one or more other credentials. You can configure one or more of the following types:

- **RSA Password**. For users whose identity source is the Authentication Manager internal database. To use this credential, an RSA password must be assigned to the user’s account.
- **RSA SecurID**. For users who have RSA SecurID authenticators.
- **On-Demand**. For users who use on-demand tokencodes.
- **LDAP Password**. For users whose identity source is an LDAP directory server.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**> **Self-Service Console Authentication**.
2. In the **Console Authentication Method** field, enter the authentication method that users must use to log on to the Self-Service Console.

   For example, to require an on-demand tokencode and an LDAP password, enter OnDemand+LDAP_Password.
3. Click **Save**.

Next Steps

If you change the authentication method, notify the users because all users currently logged on to the Self-Service Console must re-authenticate using the new method.

Security Questions for Self-Service

If security questions are enabled in the Self-Service troubleshooting policy, users are prompted to create answers to security questions during Self-Service enrollment or when they log on to the Self-Service Console. If enrolled users cannot log on to the Self-Service Console with their primary method, they are prompted to answer these questions to verify their identity. After providing correct answers, users can use the Self-Service Console troubleshooting screens to resolve authentication problems.

Security questions cannot be used as a primary authentication method to access the Self-Service Console. Primary methods are RSA Password, LDAP Password, On-Demand Authentication, and SecurID.

You determine how many security questions users must answer during enrollment and during troubleshooting. For instructions, see Set Requirements for Security Questions on page 127.

Configure E-mail Notifications for Self-Service User Account Changes

To improve the security of Self-Service accounts, you can configure Self-Service to send e-mail notifications to users when selected events occur.

You can enable the following Self-Service events to send e-mail notifications:

- Profile changes
- Password changes (RSA or LDAP passwords only when changed by the user through the Self-Service Console)
- PIN changes and when a blocked PIN is unblocked
- On-demand authentication delivery option changes
- Emergency access requests
- Token resynchronization requests

E-mail notifications to users about changes to their accounts can contain a link to the Self-Service Console on the web tier. This link enables users to go directly to the Self-Service Console where they can check their accounts.

The URL used to access the Self-Service Console varies depending on your deployment type. By default, Authentication Manager assumes that end users connect directly to the Self-Service Console installed on the primary instance. If your deployment includes a web tier where the end users connect through a load balancer or virtual host, your end users must use the appropriate URL for the Self-Service Console.

To include a link to the Self-Service Console in an e-mail notification, change the default URL in the notification to point to the virtual host or load balancer. This does not change the actual URL of the Self-Service Console, nor does it validate that the Self-Service Console is reachable through the specified URL.

In the e-mail notifications template, you can customize the field labels, message text, and add, remove, or reorder the e-mail tags. For more information, see E-mail Template Example for the Self-Service Console on page 241.

If the e-mail address attribute is editable and Self-Service is configured to send e-mail notifications for changes to the user’s profile or on-demand authentication delivery option, Authentication Manager sends a notification to both the old and new e-mail addresses when the e-mail address is changed.

Before You Begin

Configure the SMTP Mail Service on page 224

Procedure

1. In the Security Console, go to **Setup** > **Self-Service Settings**.
2. Under **Customization**, click **E-Mail Notifications for User Account Changes**.
3. To change the default URL for e-mail notifications for user account changes, do one of the following.
   - If you do not have a web tier. Under **Configure Default Self-Service Console URL**, enter the primary instance URL and port.

     The format for the URL is:

     https://*hostname:7004*/console-selfservice

     where:

     – *hostname* is the fully qualified hostname of the primary instance.
   - If you have a web tier. Under **Configure Default Self-Service Console URL**, enter the virtual host URL and port.

     The format for the URL is:

     https://*virtualhostname:port*/console-selfservice

     where:

     – *virtual-hostname* is the fully qualified hostname of the virtual host.

     – *port* is the virtual host port.
4. Under **E-mail Notifications**, select one or more events to initiate an e-mail notification to users.
5. Under **E-mail Template**, edit the **Subject** and **Body** fields.

   You cannot use angle brackets (< >) in e-mail templates.
6. Click **Save**.

E-mail Template Example for the Self-Service Console

The following example shows the default e-mail template for an account change with customized changes indented.

Recent account change:${MailComposer.NL}${MailComposer.NL}

> Account change: ${MailComposer.RequestType}${MailComposer.NL}
>
> Performed by: #(${Principal.UserID})${MailComposer.NL}

Date of account change:
${MailComposer.RequestDate}${MailComposer.NL}${MailComposer.NL}

If you have not authorized this change, contact your administrator with the information in this e-mail.

E-mail Template Tag Syntax

The syntax for e-mail template tags is:

${*objectname.propertyname*}

where:

- *objectname* is the name of a Self-Service object.
- *propertyname* is the property name of the object.

For example:

```
${Principal.UserID}
```

is the user’s identification.

Important: Do not modify e-mail tag syntax, for example, ${objectname.propertyname}.

E-mail Template Tag Default Values

Use the default e-mail template tags to customize the e-mail notifications. The following table lists the default e-mail template tags.

Object Name	Property Name	Type	Description
Principal	UserID	String	User ID
Principal	E-mail	String	User e-mail ID
Principal	FirstName	String	User’s first name
Principal	LastName	String	User’s last name
MailComposer	RequestType	String	Type of request
MailComposer	RequestDate	Date	Date of account change
MailComposer	NL	String	Adds a new line

Customizing the Self-Service Console

You can customize the Self-Service Console to meet your business needs and to enhance the user experience.

Enable or Disable Self-Service Features. Display only the features that meet your business needs.

Customize Self-Service Console Web Pages. Brand the Self-Service Console with your logo. Customize the header text and footer text with messages to your users.

Customizing the Self-Service Console User Help. Customize the content of the Self-Service Console Help file to reflect how your company uses self-service.

Enable or Disable Self-Service Features

You can customize your Self-Service deployment by enabling or disabling Self-Service features. For example, suppose you do not want users to recover their lost or forgotten passwords by themselves. You can hide the **Forgot your password** link, which allows users to change their passwords

The following features are disabled by default.

- Display Forgot Your Password link
- Display Troubleshoot SecurID Token link
- Display I Forgot My PIN option

All settings are global and apply to your entire deployment.

Before You Begin

RSA recommends that you carefully consider the security implications before enabling these features.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. On the Settings page, under **Customization**, click **Enable or Disable Self-Service Features**.
3. Under **Set Display Options for Self-Service Console - Home Page**, select the links and sections that you want to show or hide on the Home page of the Self-Service Console.

   Note: If you clear **Display Log On Section,** users cannot log on from the Home page or view their profile information on the My Account page of the Self-Service Console.

4. Under **Set Display Options for Self-Service Console - My Account Page**, select the links and sections that you want to show or hide on the My Account page of the Self-Service Console.

5. Under **Set Display Options for Troubleshooting**, select the links that you want to show or hide on the Self-Service Console.
6. Click **Save**.

Next Steps

If you enabled the **I Have Forgotten My Smart Card PIN or it is Blocked Option** under **Set Display Options for Troubleshooting**, you must import the PIN unlocking keys before users can use this option. For instructions, see Clear an RSA SecurID PIN on page 135.

Customize Self-Service Console Web Pages

You can customize the following elements of the Self-Service Console web pages and risk-based authentication (RBA) logon pages.

Procedure

1. In the Operations Console, go to **Deployment Configuration** > **Web-Tier Deployments** > **Customization**.
2. On the Web Tier Customization page, do the following.
   - (Self-Service Console and RBA logon pages) Select a new logo file for Self-Service Console and RBA logon pages. You can replace the RSA logo with your own. The logo file must be a .gif file that is less than 5 MB. The image must fit within 500 pixels wide by 50 pixels high.
   - (Self-Service Console) Enter text for the header for Self-Service Console only. You can add some user information, such as "Welcome to the *your company name* Self-Service Console, where you can request an on-demand tokencode and update your user profile."
   - (Self-Service Console) Enter text for footer 1 for Self-Service Console only. You can add up to three lines of text.
   - (Self-Service Console) Enter text for footer 2.
   - (Self-Service Console) Enter text for footer 3.
3. Click **Save**.

Next Steps

See Update the Web-Tier on page 178.

Customizing the Self-Service Console User Help

You can customize the content of the Self-Service Console Help file to reflect how your company uses self-service.

By editing the Self-Service Console Help HTM files, you can customize the Help to:

- Reflect any changes that you make to the Self-Service Console when editing the **properties** file.
- Add information that is specific to your company, for example, terminology.
- Remove information that is not applicable to your company.

The location of the HTM files on the Authentication Manager appliance is **/opt/rsa/am/server/apps/rsa-help/eclipse/plugins/com.rsa.ucmuserconsole.help/console-help**.

The location of the HTM files on the web tier is **RSA_WT_HOME/server/apps/rsa-help/eclipse/plugins/com.rsa.ucmuserconsole.help/console-help**.

Modifying the Self-Service Console Help file on the Authentication Manager appliance does not modify the Self-Service Console Help file on the web tier. Copy the Self-Service Console Help file from the **console-help** directory on the appliance to the **console-help** directory on each web-tier server where you want the customized Help to display.

Provisioning Overview

The Provisioning feature of Self-Service automates workflows for distributing authenticators and allows users to perform many of the provisioning tasks from the Self-Service Console.

Note: The Provisioning feature is included with the Authentication Manager Enterprise Server license. If you have a Base Server license, and you want provisioning, you must upgrade to the Enterprise Server license.

You can configure provisioning so that users can request, enable, and troubleshoot authenticators, as well as use emergency access. Provisioning includes predefined administrative roles that you can assign for managing authenticators, approving requests, and distributing authenticators.

Users can perform the following provisioning actions from the Self-Service Console:

- Request enrollment
- Request new or additional tokens
- Enable a token
- Request the on-demand tokencode service
- Request replacement tokens if tokens are lost, broken, temporarily unavailable, or about to expire
- Request user group membership for access to protected resources
- Request on-demand authentication

Administrative Roles in Provisioning

Provisioning includes the following predefined administrative roles, which you can customize.

Token Administrator. Imports and manages tokens, and assigns tokens to users.

Request Approver. Approves, updates, and rejects Self-Service provisioning requests including new user accounts, user group membership, and token requests.

Token Distributor. Manages token provisioning requests. Determines how to assign and deliver tokens to users.

For each predefined role, you can configure the permissions shown in the following table for each administrator.

General Permissions	Authentication Permissions	Self-Service Permissions
• Manage Policies • Manage Security Questions • Manage Delegated Administration • Manage Users • Manage User Groups • Manage Reports	• Manage SecurID Tokens • Manage User Groups • Manage User Authentication Attributes • Manage Authentication Agents • Manage Trusted Realms • Manage On-Demand Authentication	Provisioning Requests

You can limit the administrative scope of each role to a security domain and a identity source. You can also allow a provisioning administrator to delegate the role’s permissions to other administrators. For example, the Request Approver for a corporate division might want to delegate approval permissions to department-level administrators.

You can also assign provisioning permissions to any administrative role in Authentication Manager. Use the Security Console to configure administrative roles.

Scope for Request Approvers and Token Distributors

Request Approvers can approve requests under the following conditions.

Type of Request	Approval Conditions
Authenticators	Unassigned authenticators are available within the approver’s scope.
Group Membership	Both the user and group are in the Approver’s scope.
Default Group	Approver has scope for the user, regardless of scope over the group.
Any Request	User must be in the Approver’s security domain.

For Request Approver workflow instructions, see the Security Console Help topic “Approve and Reject User Requests.”

Token Distributors can only review and close requests in their security domain.

Privileges for Request Approvers and Token Distributors

Request Approvers and Token Distributors can change the type of token requested by users. For example, they can change a request for a keyfob token to a request for a USB token.

Request Approvers and Token Distributors cannot:

- Change hardware token requests to software token requests, or the reverse.
- Change requests for the on-demand tokencode service to hardware or software token requests, or the reverse.

RSA recommends that Request Approvers and Token Distributors do not change a request for a keyfob to a PINPad-style token because the PIN for a keyfob is not compatible with the PINPad-style token and the PIN fails when users try to use it.

If you change the PIN policy, verify that it does not affect any of the pending token requests. RSA recommends that you take appropriate action on pending requests before you change the PIN policy for any tokens.

For Token Distributor workflow instructions, see the Security Console Help topic “Complete User Requests.”

Workflow for Provisioning Requests

Provisioning uses workflows to automate token deployment. A workflow defines the number of steps or work tasks required for each type of user provisioning request. The users and administrators who perform tasks in a workflow are called workflow participants.

The following table lists the types of workflow participants and the tasks they can perform.

Workflow Participant	Tasks
User	From the Self-Service Console, the user initiates a request that starts a workflow. The types of user requests are: • Enrollment • New or additional SecurID tokens • Replace hardware and software tokens that are about to expire • Replace broken or permanently lost tokens • On-demand tokencode service • Additional user group membership

Workflow Participant	Tasks
Request Approver	From the Security Console, the Request Approver: • Views all requests. • Approves, rejects, cancels, or defers action on requests. • Comments on requests, if necessary. • Changes the token type, if necessary.
Token Distributor	From the Security Console, the distributor: • Views user requests that require distribution. • Determines how to assign and deliver tokens to users. • Records how tokens are delivered to users.

Assigning Administrative Roles

If you use workflows for provisioning requests, you need to assign the Token Administrator, Request Approver, and Token Distributor Administrator roles. For more information about administrative roles in provisioning, see Administrative Roles in Provisioning on page 246. For instructions, see Assign an Administrative Role on page 60.

Workflow Policy

Self-Service uses workflow policies to automate deployment of authenticators and to fulfill other requests from users, for example, on-demand authentication (ODA). Workflow policies determine how user requests are handled. They apply to the entire deployment. Each user request is governed by one workflow policy. The workflow policy includes:

- General workflow settings
- User and group settings
- Hardware and software token request settings
- On-demand tokencode request settings
- The number of steps for each type of request
- List of e-mail notification recipients for provisioning requests
- The content of e-mail notifications for each type of request

For more information about ODA and RBA, see Chapter 10, Deploying On-Demand Authentication and Chapter 12, Deploying Risk-Based Authentication.

Configuring Provisioning

You must enable provisioning and configure the features and services that you want for your Self-Service Console users. You can specify workflow policies and customize e-mail notifications for user requests. If you need to create multiple token and user group membership requests, advanced users can run a bulk import utility. The following list is a guide to configuring provisioning.

Procedure

1. Enable Provisioning on page 249.
2. Change the Default Workflow Policy on page 249.
3. Assign a Workflow Policy to a Security Domain on page 250.
4. Change Workflow Definitions on page 250.
5. Using E-mail Notifications for Provisioning Requests on page 251.
6. Configure Authenticators for Self-Service Users on page 253.
7. Configure Shipping Addresses for Hardware Authenticators on page 254.
8. (Optional) Creating Multiple Requests and Archiving Requests on page 254

Enable Provisioning

You must enable provisioning to allow users to request enrollment, user groups, authenticators, and on-demand authentication on the Self-Service Console.

Procedure

1. In the Security Console, go to **Setup** > **Self-Service Settings** > **Enable or Disable Self-Service Features**.
2. Select **Enable Provisioning Features**.
3. Click **Save**.

Change the Default Workflow Policy

If your company wants to change the number of Request Approvers in a workflow definition, who receives e-mail, or the content of the e-mails sent to workflow participants, you can change the default workflow policy for your company as needed.

Each deployment has a default workflow policy that is assigned to all new security domains. You can change the default policy. The default policy applies to all security domains that are configured to use the default policy.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. Under Provisioning, click **Workflow Policies**.
3. Use the search fields to find the policy you want to set as the default.

4. From the search results, click the policy you want to set as the default and click **Edit** from the context menu.
5. Under Workflow Policy Basics, select the **Default Policy** check box to designate the new policy as the default policy for the deployment.
6. Click **Save**.

Assign a Workflow Policy to a Security Domain

When you install Authentication Manager or create a new deployment, a default workflow policy is created. When you create a security domain, you can use the default policy, or you can create custom policies and assign them to security domains. The policy that you choose applies to all users owned by the security domain.

Procedure

1. In the Security Console, click **Administration** > **Security Domains** > **Manage Existing**.
2. From the security domain tree, select the security domain that you want to edit and click **Edit** from the context menu.
3. Under Policies, in the **Workflow Policy** field, use the drop-down menu to select a policy for the security domain.
4. Click **Save**.

Change Workflow Definitions

Each type of user request has a default workflow definition, which you can customize to meet the needs of your organization. A workflow definition defines the number of steps or work items for each type of request. Each approval step requires a unique Request Approver. A workflow definition consists of the following:

- Zero to four approval steps: Request Approvers view all requests, and approve or reject the requests.
- Zero to one distribution step: Token Distributors view user token requests and determine how to assign and deliver the tokens.

For example, suppose a company requires all new employees to enroll in Self-Service and request new tokens so they can access the company network. If your company policy requires two people—a manager and a system administrator—to approve token requests from new employees, you can customize the workflow definition to accommodate this requirement.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. Under Provisioning, click **Workflow Policies**.
3. Use the search fields to find the policy that you want to edit.
4. Select the policy that you want to edit.
5. From the context menu, click **Edit**.

6. To change the workflow definition for a particular type of request, click one of the following tabs:
   - **User and User Group.** Requests for a Self-Service account from users in a directory server, users not in a directory server, and user group membership.
   - **Hardware Token.** Requests for hardware tokens.
   - **Software Token.** Requests for software tokens.
   - **On-Demand Authentication.** Requests for on-demand authentication.
7. Under **Workflow Definitions**, click the drop-down arrow to change the number of approval or distribution steps for a request.
8. Click **Save**.

Note: If you have not saved your edits, you can click **Reset** to change the policy back to its original setting.

Using E-mail Notifications for Provisioning Requests

Provisioning workflow participants can receive e-mail notifications when a request is submitted, waiting for approval, approved, cancelled, rejected, or is unsuccessful. You can allow the following workflow participants to receive e-mail notifications:

- All workflow participants. Users, Request Approvers, Token Distributors
- Super Admin
- Workflow participants in parent security domain

You can add a comment to the request properties configuration that will be included in the e-mail notification, for example, to explain why a request is denied.

Before Authentication Manager can send e-mail notifications, you must configure SMTP. For more information, see the Security Console Help topic "Configure the SMTP Mail Service."

If you enable e-mail notifications to workflow participants in the parent security domain, all Request Approvers and Token Distributors in security domains above the security domain where a request originates receive workflow e-mail notifications.

You can deselect the default setting that enables workflow e-mail notifications to all workflow participants (Users, Request Approvers, Token Distributors). You cannot disable workflow e-mail notifications by participant type, except for Super Admin.

Configure E-mail Notifications for Provisioning Workflow Participants

Self-Service can automatically send e-mail to workflow participants to notify them that they need to take action on requests, for example, when a request is submitted, waiting for approval, cancelled, rejected, or unsuccessfully submitted. You can specify who receives workflow e-mail notifications.

Self-Service sends e-mail notifications automatically to users about their requests. You cannot disable e-mail notifications to users.

Procedure

1. In the Security Console, click **Setup** > **Self-Service**.
2. Under Provisioning, click **Workflow Policies**.
3. Use the search fields to find the policy you want to change.
4. From the search results, click the policy you want to change and click **Edit** from the context menu.
5. Under **E-mail Notification Settings**, select one or more of the following options:
   - **Enable e-mail notifications for all workflow participants** - All workflow participants (managers, or administrators with permission to approve requests or distribute tokens) receive e-mail notifications.
   - **Enable e-mail notifications for Super Admin** - Super Admins receive e-mail notifications.
   - **Enable e-mail notifications for parent workflow participants** - All approvers and distributors in the parent security domain of the user that made the request receive e-mail notifications.
6. Click **Save**.

Managing Authenticators for Self-Service Users

Users can request authenticators and emergency access through the Self-Service Console. You can use the Security Console to manage the types of authenticators available, emergency access tokencodes, and requests to replace expiring tokens.

Hardware Token Types Available for Request. You can select which types of tokens are available, the authentication method, and a default type for Self-Service users.

Software Token Profiles Available for Request. You can select which software token profiles are available. The software token profile designates the authentication method and the token delivery method. You can allow users to edit token attribute details, and to select a default type for Self-Service users.

On-Demand Authentication (ODA) Settings. You can allow users to request the ODA service as a primary authentication type. You need to configure the ODA settings to enable provisioning users to request this service.

Token File Password Settings. You can require users to provide a password to protect the software token file.

Emergency Access Tokencode Settings. Users whose tokens are temporarily or permanently unavailable may require emergency access. Self-Service users can obtain emergency access themselves rather than calling the Help Desk. You can configure the type of emergency access to make available to users.

Expiring Token Parameters. Users can request a replacement token through the Self-Service Console if a token is about to expire. You can configure the number of days before expiration that users can make this request. The default is within 30 days of expiration.

If you want reports about authenticator distribution and use, you can use the Authentication Manager standard reports or you can create custom reports. For more information about reports, see Reports Permitted for Each Administrative Role on page 330 and Custom Reports on page 332.

Configure Authenticators for Self-Service Users

Users can request authenticators and emergency access through the Self-Service Console. You can manage the types of authenticators available and configure the settings for emergency access tokencodes.

Before You Begin

Add a Software Token Profile on page 192. Only a Super Admin can add software token profiles.

Procedure

1. In the Security Console, go to **Setup** > **Self-Service Settings**.
2. Under **Provisioning**, click **Manage Authenticators,** and do the following, as needed:
   - Under **Hardware Token Types Available for Request**, select one or more types and define the settings for each type. For detailed instructions, see the Security Console Help topic “Select Hardware Tokens for Provisioning.”
   - Under **Software Token Profiles Available for Request**, select one or more software token profiles and define the settings for each type. For detailed instructions, see the Security Console Help topic “Select Software Tokens for Provisioning.”
   - Under **On-Demand Authentication Settings**, select **Allow users to request the on-demand tokencode service,** and define the settings. For detailed instructions, see the Security Console Help topic “Select On-Demand Authentication for Provisioning.”
   - Under **Token File Password Settings**, select **The user needs to provide the password, to protect the token file**, and select a file format.
3. (Optional.) Configure emergency access settings. For detailed instructions, see the Security Console Help topic “Configure Emergency Access for Provisioning.”
   - Under **Emergency Access Tokencode Settings**, define the settings.
   - Under **Emergency Access Tokencode Settings for Permanently Lost or Broken Tokens**, define the settings.
   - Under **Emergency Access Tokencode Settings for Temporarily Unavailable Tokens**, define the settings.
   - Under **Expiring Token Parameters**, enter the number of days in advance of expiration that a user can request a replacement token.
4. Click **Save**.

Configure Shipping Addresses for Hardware Authenticators

When you configure provisioning, you can configure a shipping address where hardware authenticators are sent for each user. Each user can have a separate shipping address. The shipping address appears on the user profile.

If you store shipping data in the internal database, the user must enter a shipping address for each request for an authenticator that requires a distribution step.

If you use a directory server as the identity source, you can map the shipping address to existing identity attributes. The identity source automatically fills in the address information for the user. The user can view the shipping address, but cannot modify it.

Any changes made to the shipping address are only for the current authenticator request. Changes to the shipping address do not change the user’s record in the identity source.

Procedure

1. In the Security Console, click **Setup** > **Self-Service Settings**.
2. Under **Provisioning**, click **Set Shipping Addresses**.
3. (Optional) Under **Shipping Address Mapping and Display Options**, specify if you want the fields in the shipping address to be **Required**, **Optional**, **Read-only**, or **Hidden**.
4. (Optional) For each of the options, do one of the following:
   - If you store data in the internal database, under **Map to**, select **Unmapped**.
   - To use information from an identity source for the shipping address, under **Map To**, select one of the available identity attributes.
5. Click **Save**.

Creating Multiple Requests and Archiving Requests

If you need to create multiple requests, you can use the User Groups and Token Bulk Requests utility, import-bulk-request. For example, if you want every salesman in your organization to receive a SecurID token, you can create a bulk request on their behalf. The system acts as if each salesman made a separate request using the Self-Service Console.

If you want to free up disk space, you can use the Archive Requests utility, archive-ucm-request, to export closed Self-Service Console requests with their associated attributes and process data. If you need to retrieve the information, you can use the Archive Requests utility to import the archived requests. For example, you might want to resend an approval e-mail to a user who has lost the approval e-mail that contained a token file.

User Groups and Token Bulk Requests Utility

Use the User Groups and Token Bulk Requests utility, import-bulk-request, to import token and user group membership requests. The RSA Authentication Manager self-service feature runs this task as a batch job.

When you run the User Groups and Token Bulk Requests utility, the time that it takes for bulk request operations to complete depends on the number of requests in the comma-separated value (CSV) input file. If you receive time-out errors, it may be that your CSV input file has too many requests. You should create multiple CSV input files and import them separately.

Import Bulk Requests for User Groups and Tokens

You must run the import-bulk-request utility on the appliance. The input file must also be on the appliance operating system. For example, you can use Secure FTP to copy the .csv file into the **/home/rsaadmin** directory.

Important: This procedure assumes a knowledge of Linux commands. Do not attempt this procedure without the necessary knowledge.

Before You Begin

- You must have Super Admin and Operations Console administrator privileges to run the User Groups and Token Bulk Requests utility.
- You must create an input file that lists all of the bulk requests. For instructions, see Create Input Files for Bulk Requests on page 257.

Procedure

1. Log on to the appliance using an SSH client. For instructions, see Enable SSH on the Appliance on page 403.
2. Change directories to **/opt/rsa/am/utils**.
3. Do the following:
   - To import bulk token requests, type:

     ```
     ./rsautil import-bulk-request -u admin_UserID -o
     oc_admin_UserID -f /home/rsaadmin/TokenRequests.csv -r
     TOKEN
     ```

     where

     – *admin_UserID* is the user name for the Super Admin running the utility.

     – *oc_admin_UserID* is the user name for an Operations Console administrator.

     – */home/rsaadmin/TokenRequests.csv* is the request input file (CSV) with pathname and filename.

     – TOKEN is the request type.

- To import bulk on-demand tokencode service requests using the mobile device delivery method, type:

  ```
  ./rsautil import-bulk-request -u admin_UserID -o
  oc_admin_UserID -f /home/rsaadmin/TokenRequests.csv -r
  TOKEN -d SMS
  ```

  where *SMS* is the delivery method.

  When you import on-demand tokencode service bulk requests, the delivery method follows these guidelines:

  – You can use only one delivery method for each on-demand tokencode service bulk request.

  – If you configure one delivery method for the on-demand tokencode service, either mobile device or e-mail, all on-demand tokencode service bulk requests use that delivery method.

  – If you configure both mobile device and e-mail as the delivery methods for the on-demand tokencode service, you can set the delivery method for on-demand tokencode service bulk requests using the (-d) option flag. If you do not use the `-d` option flag, the default delivery method is e-mail.

  – If the CSV file does not contain any on-demand tokencode service bulk requests, the delivery method (-d) option flag is ignored.

  For information on configuring delivery methods, see Configuring On Demand Tokencode Delivery by Text Message on page 218 and Configuring On-Demand Tokencode Delivery by E-mail on page 224.

- To import bulk user group membership change requests, type:

  ```
  ./rsautil import-bulk-request -u admin_UserID -o
  oc_admin_UserID -f /home/rsaadmin/GroupRequests.csv -r
  GROUP
  ```

  where

  – *admin_UserID* is the user name for the Super Admin running the utility.

  – *oc_admin_UserID* is the user name for an Operations Console administrator.

  – */home/rsaadmin/GroupRequests.csv* is the request input file (CSV) with pathname and filename.

  – GROUP is the request type.

4. When prompted, enter the Super Admin and Operations Console administrator passwords.

Important: Although it is possible to enter the Super Admin and Operations Console administrator passwords on the command line along with the other options, this creates a potential security vulnerability. RSA recommends that you enter passwords only when the utility presents a prompt.

Create Input Files for Bulk Requests

You must create a CSV(comma-separated values) input file that lists all of the bulk requests that you want to input into the Self-Service Console using the User Groups and Token Bulk Requests utility.

To create a CSV input file:

1. Do one of the following:
   - Create an ASCII text file. Separate the header information and request information with commas.
   - Use spreadsheet software, such as Microsoft Excel, and enter the values in each column of the spreadsheet.

   Note: You must create a separate CSV input file for token requests and a separate CSV input file for user group membership requests. You cannot put token requests and user group membership requests in the same CSV input file.

2. Enter header information (attribute names) for requests, on the first line, separated by commas, or in different columns, if you use a spreadsheet.
3. Enter request information (attribute values) in the second and following lines, separated by commas, or in different columns, if you use a spreadsheet.

   Each line, after the header, is a separate request.

   Note: The request information (attribute values) must follow the same order as the header information (attribute names) in each line of the input file.

   For information about attribute names and attribute values, see CSV Format for Token Requests Input File on page 258 and CSV Format for User Group Membership Requests Input File on page 259.
4. Do one of the following:
   - Save the text file with the .csv extension.
   - If you use spreadsheet software, save the input file as a .csv file.
5. Copy the .csv file to the RSA Authentication Manager instance. For example, use Secure FTP to copy the .csv file into the /**home/rsaadmin** directory.
6. Run the import-bulk-request utility.

   For more information, see Import Bulk Requests for User Groups and Tokens on page 255.

CSV Format for Token Requests Input File

The following table lists the attribute names (header information) and attributes values (request information) for the token requests input file.

Attribute Names	Attribute Values
USER_ID	Logon ID of the user for whom the bulk request is created.
IDENTITY_SOURCE_NAME	Identity source name of the user for whom the bulk request is created. **Note:** Do not use the user-friendly display name. Use the exact identity source name.
TOKEN_TYPE	Use the token type name that appears on the Security Console Self-Service Settings: Provisioning - Manage Authenticators page. For software tokens, use the display names listed under the section **Software Token Types Available for Request**. You enter the display name when you add a new software token profile. For instructions, see Add a Software Token Profile on page 192. Input to the import-bulk-request CLU is based on the display name. **Note:** Use **On-Demand Tokencodes** to create bulk requests for the on-demand tokencode service. You cannot send on-demand tokencodes to users using bulk requests.

Sample CSV Input File for Token Requests

```
USER_ID,IDENTITY_SOURCE_NAME,TOKEN_TYPE
SDoe,Internal Database,STDCARD
PPorter,Internal Database,PINPAD
FKing,Internal Database,KEYFOB
LMathews,Internal Database,SID800
RKapur,Internal Database,Android_CT_KIP
DCohen,Internal Database,iPhone
RBouvier,Internal Database,Windows Mobile
ADoyle,Internal Database,Toolbar
GWilliams,Internal Database,CT KIP
TKennedy,Internal Database,On Demand Tokencode Service
```

CSV Format for User Group Membership Requests Input File

The following table lists the attribute names (header information) and attributes values (request information) for the user group membership requests input file.

Attribute Names	Attribute Values
USER_ID	Logon ID of the user for whom the bulk request is created.
IDENTITY_SOURCE_NAME	Identity source name of the user for whom the bulk request is created. **Note:** Do not use the user-friendly display name. Use the exact identity source name.
USER_GROUP_NAME	User group name. You can request membership in more than one group by using “;” for a delimiter. **Note:** You must use the exact name for each user group member. Do not use the user-friendly display name.

Sample CSV Input File for User Group Membership Requests

```
USER_ID,IDENTITY_SOURCE_NAME,USER_GROUP_NAME
GWilliams,Internal Database,Managers
TKennedy,Internal Database,Managers; HR
DCohen,Internal Database,Doc
RBouvier,Internal Database,Customers
```

Log Files for Bulk Requests

A log file is created for each bulk request batch job. View the log file to verify that the batch job successfully created all requests in the input file.

The location of the log file is:

/opt/rsa/am/server/logs/CLU

The log file uses the following naming conventions:

- For bulk token requests:
  UCM Requests_BulkToken_YYYY_MM_DD_HH_MIN_SEC.log
- For bulk user group membership requests:
  UCM Requests_BulkGroup_YYYY_MM_DD_HH_MIN_SEC.log

PIN and Protection of Distribution Files for Software Tokens

The CSV output file stores PINs and passwords for protection of distribution files in text format. There is no protection of passwords or PINs in this file. Administrators can use this file to send PINs and passwords to users by e-mail. The CSV output file has the same name as the corresponding log file, except with the .csv extension, and it is generated in the same location as the log file.

For tokens with PINs, the system generates PINs to protect distribution files. The system uses the setting to password protect distribution files set by the administrator.

For tokens without PINs, which have one-factor authentication, the system protects distribution files with passwords (8 alphanumeric characters).

Archive Requests Utility

Use the Archive Requests utility, archive-ucm-request, to export and import RSA Self-Service closed requests, such as new user and token requests, with their associated attributes and workflow data.

You can export closed requests if you want to free up disk space and if you want to increase the speed of search operations in the system. You can import archived requests if you want to resend an approval e-mail to a user who has lost the approval e-mail that contained a token file.

This utility exports the associated attributes and process instance data into the file **Request_YYYY_MM_DD_HH_MIN_SEC.ZIP** in the directory **/tmp/archivedRequest**. The .zip file contains the following files:

- Request Data - **Request_YYYY_MM_DD_HH_MIN_SEC.CSV**
- Request Attribute Data - **Request_Att_YYYY_MM_DD_HH_MIN_SEC.CSV**
- Process Instance Data - **Request_WF_YYYY_MM_DD_HH_MIN_SEC.CSV**
- Process Instance Activity Data - **Request_WF_ACTYYYY_MM_DD_HH_MIN_SEC.CSV**

Export and Import Closed Requests

The Archive Requests utility, archive-ucm-request, can only export RSA Self-Service closed requests. When you import archived requests, you must use the same .zip file that you use to export requests. Do not change the name of the .zip file.

Important: This procedure assumes a knowledge of Linux commands. Do not attempt this procedure without the necessary knowledge.

Before You Begin

You must have Super Admin and Operations Console administrator privileges to run the Archive Request utility.

Procedure

1. Log on to the appliance using an SSH client. For instructions, see Enable SSH on the Appliance on page 403.
2. Change directories to **/opt/rsa/am/utils**.

3. Do the following:

   - To export requests from a range of dates and delete the requests after exporting them, type:

     ```
     ./rsautil archive-ucm-request -u admin_UserID -o
     oc_admin_UserID -d /tmp/archivedRequest -a EXPORT
     -S 07/03/2013 -E 07/07/2013 -D
     ```

     where

     – *admin_UserID* is the user name for the Super Admin running the utility.

     – *oc_admin_UserID* is the user name for an Operations Console administrator.

     – */tmp/archivedRequest* is the directory path for archived requests.

     – EXPORT is the archive option.

     – *07/03/2013* is the start date. Requests created on or after this date are exported. [mm/dd/yyyy].

     – *07/07/2013* is the end date. Requests created on or before this date are exported. [mm/dd/yyyy].

     – -D deletes records after exporting.

     The archived requests are saved in a .zip file in the directory **/tmp/archivedRequest**.

     To save disk space, you can move the .zip file to a secure location on the network. For example, use Secure FTP.

   - To import archived requests and the associated process instance data, copy the archive .zip file to the appliance operating system. For example, you can use Secure FTP to copy the .zip file into the /**tmp/archivedRequest** directory.

     Type:

     ```
     ./rsautil archive-ucm-request -u admin_UserID
     -o oc_admin_UserID -d /tmp/archivedRequest -a IMPORT
     -j Request_2013_03_06_15_48_26.zip
     ```

     where

     – *admin_UserID* is the user name for the Super Admin running the utility.

     – *oc_admin_UserID* is the user name for an Operations Console administrator.

     – */tmp/archivedRequest* is the directory path for archived requests.

     – IMPORT is the archive option.

     – *Request_2013_07_03_06_15_48_26.zip* is the file for import. The .zip file must have the same filename as it had when the data was exported.

4. When prompted, enter the Super Admin and Operations Console administrator passwords.

Important: Although it is possible to enter the Super Admin and Operations Console administrator passwords on the command line along with the other options, this creates a potential security vulnerability. RSA recommends that you enter passwords only when the utility presents a prompt.

Self-Service Troubleshooting

The self-service troubleshooting feature allows Self-Service Console users to troubleshoot routine authentication problems when they cannot access protected resources using primary methods such as passwords or passcodes.

Users can troubleshoot the following problems, if their records are stored in the internal database.

- Reset passwords
- Reset token PINs
- Resynchronize tokens
- Request a new tokens (if they lost the old one)
- Request emergency access tokencodes

You associate Self-Service troubleshooting policies with security domains. The default policy is automatically assigned to each new security domain that you create. You can override the default policy by selecting a custom policy.

Add a Self-Service Troubleshooting Policy

In a replicated deployment, changes to policies might not be immediately visible on the replica instance. This delay is due to the cache refresh interval. Changes should replicate within 10 minutes. For instructions to make changes take effect sooner on the replica instance, see Flush the Cache on page 369.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Self-Service Troubleshooting Policies** > **Add New**.
2. In the **Self-Service Troubleshooting Policy Name** field, enter the policy name. Use a unique name, and do not exceed 128 characters.
3. (Optional) To designate the new policy as the default policy for the system, select **Default Policy**. When this option is selected, new security domains use this policy.
4. (Optional) Select the **Authentication Method** with which users authenticate if they cannot use their primary authentication method.

5. The **Lock User Accounts** field controls the number of unsuccessful authentication attempts a user is permitted to make to the Self-Service Troubleshooting feature. You can allow an unlimited number of unsuccessful attempts, or a specified number of unsuccessful attempts within a specified number of days, hours, minutes, or seconds. After the number has been reached, this policy locks the user's account out of the troubleshooting feature.
6. In the **Unlock** field, you can either require administrators to unlock accounts after users have exceeded the limit specified in the **Lock User Accounts** field, or you can allow the system to automatically unlock accounts after a specified number of days, hours, minutes, or seconds.
7. Click **Save**.

12 Deploying Risk-Based Authentication

Risk-Based Authentication

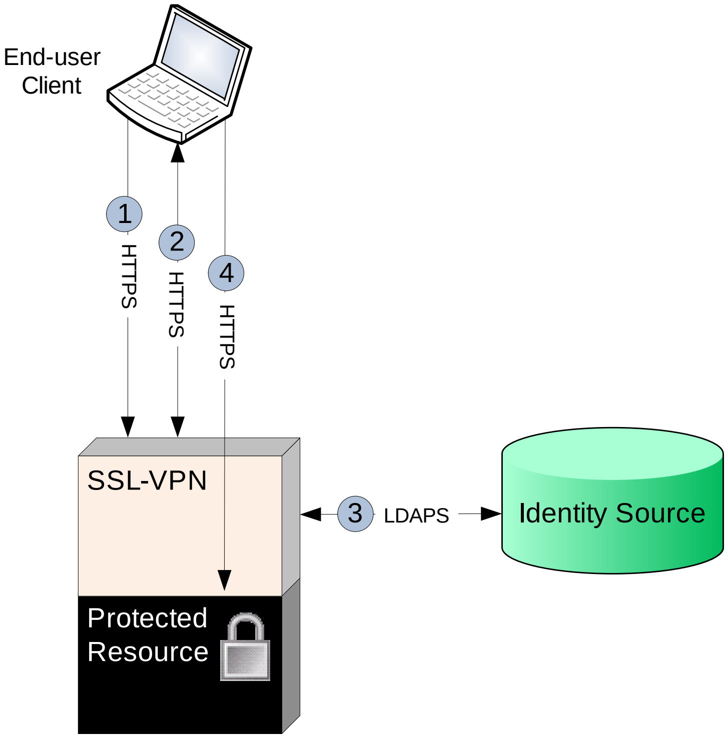
Risk-based authentication (RBA) identifies potentially risky or fraudulent authentication attempts by silently analyzing user behavior and the device of origin. RBA strengthens RSA SecurID authentication and traditional password-based authentication. If the assessed risk is unacceptable, the user is challenged to further confirm his or her identity by using one of the following methods:

- On-demand authentication (ODA). The user must correctly enter a PIN and a one-time tokencode that is sent to a preconfigured mobile phone number or e-mail account.
- Security questions. The user must correctly answer one or more security questions. Correct answers to questions can be configured on the Self-Service Console or during authentication when silent collection is enabled.

RSA Authentication Manager contains a risk engine that intelligently accumulates and assesses knowledge about each user’s device and behavior over time. When the user attempts to authenticate, the risk engine refers to the 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. RBA compares this to the minimum acceptable level of assurance that you have configured. If the risk level is higher than the minimum assurance level, the user is prompted to confirm his or her identity by answering security questions or using ODA.

Risk-Based Authentication Data Flow

The following figure shows a web-based application before it is configured for risk-based authentication (RBA). In this example, the network resource is protected by an SSL-VPN, and the SSL-VPN is configured to validate user logon credentials using an LDAP directory.



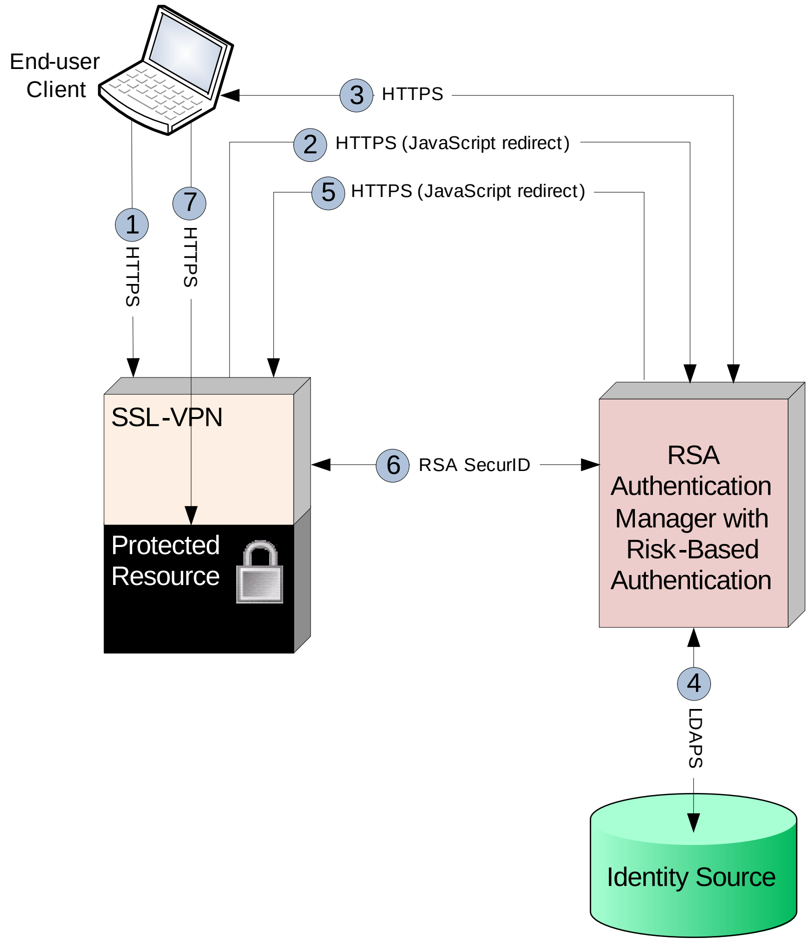
Data flow occurs in the following sequence:

1. The user browses to the SSL-VPN logon page over an HTTPS connection.
2. The user provides a user name and password.
3. The SSL-VPN validates the user’s identity using an LDAP directory, the identity source, over an LDAPS connection.
4. The SSL-VPN grants the user access to the protected resource.

When RBA is enabled, the logon page for the web-based application redirects the user to the Authentication Manager logon page. The user enters logon credentials, and Authentication Manager validates the user’s credentials using an LDAP directory as an identity source.

You can deploy RBA so that the workflow is transparent to the user. The redirect is immediate. Also, you can customize the Authentication Manager logon page.

The following figure shows RBA integrated with the SSL-VPN.


End-user Client
3 HTTPS
2 HTTPS (JavaScript redirect)
5 HTTPS (JavaScript redirect)
1 HTTPS
7 HTTPS
SSL-VPN
Protected Resource
6 RSA SecurID
RSA Authentication Manager with Risk-Based Authentication
4 LDAPS
Identity Source

Data flow occurs in the following sequence:

1. The user browses to the SSL-VPN logon page over an HTTPS connection.
2. The SSL-VPN redirects the user's browser to an Authentication Manager logon page.
3. The user provides a user name and password.
4. Authentication Manager validates the user's identity using an LDAP directory, the identity source, over an LDAPS connection.

Also, Authentication Manager assesses the assurance level (the confidence level that determines when the user is challenged for identity confirmation) of the authentication attempt. One of the following occurs:

- If the assurance level meets the level that is required by the RBA policy, the workflow continues at step 5.
- If the assurance level does not meet the level that is required by the RBA policy, the user is prompted to confirm his or her identity. One of the following happens:
  - If the user provides identity confirmation, the workflow continues at step 5.
  - If the user does not provide identity confirmation, Authentication Manager returns a message to the user's browser that access is denied, and the workflow ends.

5. Authentication Manager redirects the user's browser to the SSL-VPN with an authentication artifact to confirm that the user's credentials are valid.
6. The SSL-VPN validates the authentication artifact over the RSA SecurID protocol, which is the native authentication protocol for Authentication Manager.
7. The SSL-VPN grants the user access to the protected resource.

Deployment Considerations for Risk-Based Authentication

Before you deploy risk-based authentication (RBA), consider these aspects when you plan your RBA deployment strategy and establish RBA policies:

- Do you want to use RBA for all users in a security domain? If yes, you can configure Authentication Manager to enable all users automatically. If no, the administrator enables users individually.
- Do you have a web tier? RSA recommends a web tier for RBA. You can have multiple web tiers handling RBA traffic.
- Which server do you want to select as the preferred server for RBA? RBA requires a preferred server. You must select a unique preferred server for each web tier handling RBA traffic.
- Do you want to integrate RBA with your web-based authentication agents? RSA supports specific web-based agents for integration with RBA. You may integrate other web-based agents that support either the RSA SecurID protocol or the RADIUS protocol.
- Do you want to use silent collection, which allows the system to establish a baseline authentication history for each user and register authentication devices automatically to users during the data accumulation period?
- How often do users access protected resources from public computers or devices? Consider this when you are choosing a minimum assurance level, deciding whether you want to enable silent collection, and configuring device settings. You may want to select a higher assurance level if users frequently use public computers or devices.

- Do users typically access protected resources using multiple devices or from changing locations? How sensitive should Authentication Manager be to changes in the user’s location, device, and behavior? Consider this when you choose a minimum assurance level and configure device settings.
- Which identity confirmation methods should be available to users? For example, if users carry mobile phones that your organization authorizes for business use, you might choose on-demand authentication. For laptop or desktop users, you might choose security questions.
- How many devices should be associated with each user? How long should each device remain registered to the user? Consider these when you are configuring device settings.
- Do you want your company’s logo on the RBA logon pages? For more information, see Customize Self-Service Console Web Pages on page 244.
- Do your users use RSA SecurID authenticators? When RBA is enabled, the following authenticator-related events can cause the system to raise the risk level.
  - User exceeds your threshold for unsuccessful logon attempts
  - User uses a temporary tokencode or fixed passcode
  - Administrator clears a user’s PIN
  - Administrator changes a user’s PIN
  - Administrator marks a token as lost and a user attempts to logon with it

  You may want to educate the SecurID users about these additional risk contributors to help them understand why the system challenges them for identity confirmation.

Risk Engine Considerations for Risk-Based Authentication

The risk-based authentication (RBA) risk engine creates a profile for each user based on the client device and user behavior. Before you deploy RBA, consider these factors regarding the RBA risk engine:

- The RBA risk engine requires a learning period during which it acquires the data needed to build profiles on users and their devices, and general user population behavior. During this learning period, users may be challenged more frequently for risk until the profiles are built to establish baseline assurance levels. For user convenience, you can configure the silent collection option to avoid risk-based challenges while the data for baseline assurance levels is acquired. See Silent Collection on page 272.
- The RBA risk engine employs soft matching techniques based on statistical probability. If the risk engine has insufficient data to match a device, it can use forensic tools to assess the match probability and adjust the assurance level accordingly.
- The RBA risk engine is self-tuning and learns to ignore parameter values that most authentications in your deployment have in common. Self-tuning improves security and reduces overall user challenge rates.

Minimum Assurance Level

The minimum assurance level is the confidence threshold that each authentication attempt must meet to avoid a challenge to the user for identity confirmation. The setting is in the risk-based authentication (RBA) policy for each user's security domain.

Each time a user attempts to authenticate, the risk engine evaluates the device match and user behavior in real-time to produce an assurance level. The risk engine compares the user's assurance level with the minimum assurance level in the RBA policy. If the user's level is lower than the minimum, the user is prompted for identity confirmation.

For an authentication attempt to be considered high assurance, most or all device characteristics must match those that were recorded during a previous authentication attempt. Device characteristics include, but are not limited to, the IP address, the browser type and version, and the HTTP and Flash cookies that identify the device.

If the device is not in the user's device history (and silent collection is expired or is disabled), the authentication attempt is considered low assurance and the user must confirm his or her identity to access the RBA-protected resource. When the user's assurance level is below the threshold, and the user has not configured an identity confirmation method, the user cannot access the protected resource.

Recommendations for Determining the Minimum Assurance Level

Before you deploy risk-based authentication (RBA), consider these factors regarding the minimum assurance level:

- Many factors are involved in calculating the risk level. Results may vary based on your network, users, and specific situations.
- The best minimum assurance level for your deployment depends on:
  - The sensitivity of the resources being protected
  - The acceptable user challenge rate
- If strength-of-authentication is your primary objective, start with a higher assurance level, and adjust it to a lower level if users are being challenged too often.
- If ease-of-use is your primary objective, start with a lower assurance level, and adjust it to a higher level if you want more security.
- RSA recommends starting with a Medium-High assurance level.

Because assurance increases when the device is known and the user behavior is predictable, some user populations are better suited to higher assurance levels than others. For example, employees authenticating regularly from the same device and location usually have much higher assurance than employees who travel frequently. Adjust the minimum assurance level to match the majority of your user population.

The Impact of User Behavior on Risk-Based Authentication

A user’s behavior affects how often the user is challenged to confirm identity. The system calculates and assigns users a Behavioral Risk Assurance Level that indicates the degree of confidence that the user is known to the deployment. The Behavioral Risk Assurance Level is based on the user’s typical behavior. Abnormal user behavior, such as attempting to authenticate several times in a row using the wrong password, lowers the Behavioral Risk Assurance Level and increases the assessed risk of the authentication attempt.

The system also calculates and assigns a client device a Device Assurance Level that indicates the degree of confidence that the device is known to the deployment. The Device Assurance Level is based on a specified device matching technique.

Low-risk behaviors include common activities that are perfectly valid under most circumstances but could be associated with fraud. For example:

- The user’s account was recently modified.
- The user is authenticating from a previously unknown IP address.

Medium-risk behaviors may include multiple activities that are combined in a suspicious way. For example:

- The user authenticates from an unknown IP address soon after a failed identity confirmation challenge.
- The user authenticates from an unknown IP address after changing his profile through the Self-Service Console.

Any clearly identified fraudulent activity constitutes high-risk behavior. For example, authentication attempted from a machine with an invalid or compromised cookie is a high-risk behavior.

The effect of user behavior on the device and behavioral risk assurance level is shown in the following table.

Device Matching Technique	**Device Assurance Level**	**Behavioral Risk Assurance Level**			
		Low	**Medium**	**Medium-High**	**High**
Based on two or more unique attributes and statistical data	High	High	High	Medium-High	Very Low
Based on one unique attribute plus statistical data	Medium-High	Medium-High	Medium	Low	Very Low

Device Matching Technique	Device Assurance Level	Behavioral Risk Assurance Level			
		Low	Medium	Medium-High	High
Based on one unique attribute	Medium	Medium	Medium	Low	Very Low
Based on statistical data	Low	Very Low	Very Low	Very Low	Very Low
Unregistered device	Very Low	Very Low	Very Low	Very Low	Very Low

Silent Collection

Silent collection is an optional feature that facilitates the process of collecting profile and behavioral data for users without the need for user or administrator intervention.

When silent collection is enabled, the risk engine passively monitors user behavior for a defined period without actively challenging users based on risk. During this period, the risk engine automatically registers user devices and observes behavioral patterns. Once the risk engine has gathered enough information to have high assurance about a particular user, that user is prompted to provide any missing information. For example, the user may need to configure security questions or on-demand authentication.

You enable the silent collection period in the risk-based authentication (RBA) policy for all users in a security domain. Using silent collection helps the risk engine build a baseline profile for each user.

Silent collection affects your deployment in the following ways:

- During silent collection, authentication is based only on the authentication method required by the agent. Users are never challenged for identity confirmation.
- All devices are registered to the user's RBA profile. This may include unwanted devices such as internet kiosks.

For configuration instructions, see the Security Console Help topic "Configure Silent Collection for a Risk-Based Authentication Policy".

Implementing Risk-Based Authentication

Complete the following tasks to implement risk-based authentication (RBA).

Before You Begin

Choose a backup authentication method so that users can continue to access network resources if Authentication Manager is unavailable or user authentication is unsuccessful. See Backup Authentication Method for Risk-Based Authentication on page 273.

Procedure

1. Update the Domain Name System (DNS) with entries for Authentication Manager. For instructions, see Planning for Domain Name System Updates on page 44.
2. Specify the RBA policy for your deployment integration. For instructions, see, Add a Risk-Based Authentication Policy on page 95.
3. Ensure high availability for RBA. See Backup Authentication Method for Risk-Based Authentication on page 273.
4. Obtain the RSA Authentication Agent software or third party product. See Obtaining RSA Authentication Agents on page 274.
5. Deploy the RSA Authentication Agent software or third party product. See Deploying an Authentication Agent on page 64.
6. Install the RBA Integration Script Template on page 275.
7. Configure the Authentication Agent for Risk-Based Authentication on page 275.
8. Use the implementation guide that you downloaded when you obtained the agent to configure your agent to pass authentication requests to and from Authentication Manager.
9. Test the RBA integration. See Testing Your Risk-Based Authentication Integration on page 277.

Backup Authentication Method for Risk-Based Authentication

RSA recommends that you set up a replicated deployment of Authentication Manager. A replica instance ensures high availability for risk-based authentication (RBA). If you do not use a replica instance, configure your web-based application to use a backup authentication method. A backup authentication method allows users to continue accessing network resources if Authentication Manager becomes unavailable or user authentication is unsuccessful.

When RBA is configured for your web-based application, Authentication Manager authenticates the user using the directory server and internal database in your environment. To ensure an effective backup method, plan to revert authentication configuration of the web-based application so that it authenticates users directly using the directory server.

The backup method that you use depends on your web-based application and the other products in your environment that are involved in user authentication workflow. Consider the following methods:

- Use the original logon page for your web-based application.

  Redirect users to the original logon page, or replace the modified logon page with the original version.
- Using your web-based application, create a backup method that is specific to the user population that uses RBA.

  Change the authentication workflow only for the user population, group, or domain that uses RBA.
- Using your web-based application, create a backup method that is specific to the network resource that you are protecting with RBA.

  Change the profile or policy for the network resource that you are protecting with RBA.

For more information, see your agent documentation.

Obtaining RSA Authentication Agents

The agent that you need depends on the type of resource you want to protect. For example, to protect an Apache web server, you need to download the RSA Authentication Agent for Apache.

The download package includes an *Installation and Administration Guide* and a *Readme*. Read these documents before installing the agent. For information about installing agent software, see your agent documentation.

You may purchase products that contain embedded RSA Authentication Agent software. For example, these products include remote access servers and firewalls.

Procedure

Do one of the following.

- For an RSA agent and for a third-party agent that requires an RSA agent, go to **http://www.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings**.

  Locate the agent software for your platform and download the agent software and the RBA Integration Script Template.
- For a third-party agent that has an embedded RSA agent, go to the RSA Secured web site at **https://gallery.emc.com/community/marketplace/rsa?view=overview**, and locate the listing for *RSA Implementation Guide for Authentication Manager* for your agent.

  Download the *RSA Implementation Guide for Authentication Manager* for your agent. Save it to your desktop or a local drive that you can access during the integration process.

Note: Only certified partner solutions have an implementation guide. For other agents that are certified as RSA SecurID Ready, you can create a custom implementation.

Next Steps

See Deploying an Authentication Agent on page 64.

Install the RBA Integration Script Template

If the RBA integration script template that you downloaded from RSA SecurCare Online is newer than the integration script template that is installed in Authentication Manager, use the newer one. You must perform this procedure to find the version number in your deployment. The version number is located in the integration script template header, for example, <Version>1.0</Version>.

Before You Begin

If you want to use SSH, enable SSH connectivity on the Authentication Manager appliance. For instructions, see Enable SSH on the Appliance on page 403.

Procedure

1. Using an SSH client or an SCP client, log on to the appliance using the operating system account User ID **rsaadmin** and password.
2. Copy the downloaded integration script template to the **/opt/rsa/am/utils/rba-agents** directory on the appliance.

   Wait a few minutes for Authentication Manager to refresh the list of integration script templates.
3. Verify that the version number in the header of the generated integration script (.js file) is the same as the version number in the header of the downloaded integration script template (.xml file). For example, look for <Version>1.0</Version> near the top of the generated .js file or the .xml template.
4. Repeat step 1 through step 3 for each agent.

Next Steps

Configure the Authentication Agent for Risk-Based Authentication on page 275

Configure the Authentication Agent for Risk-Based Authentication

To protect a web-based application with risk-based authentication (RBA), you must configure the authentication agent for RBA and generate an integration script to deploy to the web-based application’s default logon page. The integration script redirects the user from the web-based application's default logon page to a customized logon page that allows Authentication Manager to authenticate the user with RBA.

Procedure

1. On the primary instance Security Console, click **Access > Authentication Agents > Manage Existing**.
2. Click the appropriate agent, and click **Edit**.
3. In the **Risk-Based Authentication (RBA)** section, select **Enable this agent for risk-based authentication**.
4. To enable RBA as the only authentication method for this agent, select **Allow access only to users who are enabled for risk-based authentication**. If a user is not enabled for RBA, the agent will deny access to the resource.
5. From the **Authentication Method** drop-down list, select **Password** or **SecurID**. This field determines the authentication method that the agent requires when using RBA.
6. Click **Save Agent & Go to Download Page**.
7. From the **Agent Type** drop-down list, select the appropriate agent, and click **Download File.**

   The system generates the JavaScript integration file based on the .xml integration script template that is stored in Authentication Manager.
8. When prompted, save the JavaScript file locally.

Next Steps

- Verify that components such as the web tier and load balancer are installed and configured correctly. For more information, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*
- Use the *RSA Implementation Guide for Authentication Manager* for the agent that you downloaded. Configure the agent to pass authentication requests to and from Authentication Manager by uploading the generated script to the agent.
- Test the RBA integration. For instructions, see Testing Your Risk-Based Authentication Integration on page 277.

Testing Your Risk-Based Authentication Integration

Test your risk-based authentication (RBA) integration to verify that Authentication Manager can authenticate users for the agent. If the test is unsuccessful, troubleshoot the setup, and repeat the test until it succeeds.

The Authentication Activity Monitor logging detail can be used for troubleshooting if the test is unsuccessful.

Procedure

1. Create a test user in the Security Console by adding a new user to the internal database and the default security domain (SystemDomain).

   For instructions, see Add a User to the Internal Database on page 119.

2. Verify that the RBA policy associated with the default security domain (SystemDomain) has the following configuration and edit the policy if necessary:

   - Automatic enablement is allowed.
   - Silent collection is allowed.

   For instructions on editing an RBA policy, see the Security Console Help topic "Edit a Risk-Based Authentication Policy."

3. Start the Authentication Activity Monitor in the Security Console.

   Click **Start Monitor** to view real-time authentication activity.

4. Do one of the following:

   - Go to another computer on the same network, start the browser, and go to the logon page for your web-based application.
   - Start a different browser application on the same machine if you have more than one installed. For example, if you used Firefox to access the Security Console, you may use Internet Explorer to access the logon page for your web-based application.

   The logon page for your web-based application automatically redirects you to the Authentication Manager logon page. If you are not redirected to this page, troubleshoot the test. For more information, see Troubleshooting the Authentication Test on page 278.

5. Enter the logon credentials for the test user.

6. Verify that your browser loads the correct landing page for the network resource that you are trying to access.

7. Review authentication logging in the Authentication Activity Monitor. If the test succeeded, familiarize yourself with entries that are logged for successful authentication. If the test is unsuccessful, review the entries and review Troubleshooting the Authentication Test on page 278.

Troubleshooting the Authentication Test

If the authentication test is unsuccessful, follow the recommended troubleshooting methods in the following table based on the system behavior that you observed during the test.

System Behavior	Action
Browser displays the default logon page for your web-based application instead of the Authentication Manager logon page.	• Verify that you generated and deployed the RBA integration script correctly. For more information, see the implementation guide for your web-based application. • Verify that the integration script file for your web-based application is encoded as ISO-8859-1 (also referred to as Latin-1) or ASCII. Other file encoding formats are not supported.

System Behavior	Action
Web-based application redirects you to a logon page that does not load.	• Verify that your browser allows JavaScript. For more information, see your browser documentation. • Verify that your browser has cookies enabled. For more information, see your browser documentation. • Verify that you are using a supported browser. For a list of supported browsers, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*. • Do one of the following: – For a deployment with a web tier, verify that the URL resolves to the virtual host and virtual host port. – For a deployment without a web tier and with a load balancer, verify that the URL resolves to the load balancer and the load balancer port. – For a deployment without a web tier and a load balancer, verify that the URL resolves to the primary instance and primary instance port. • Verify that all firewalls are configured to allow inbound traffic to the host and port that are specified in the URL. • Verify that the Domain Name System (DNS) server has the appropriate hostnames and IP addresses for RBA. See Planning for Domain Name System Updates on page 44. • Also, verify that any Network Address Translation (NAT) or load balancers do not interfere with requests that must be routed to an Authentication Manager host, which is either the web tier or an Authentication Manager instance, depending on your deployment scenario. These actions can resolve issues in which the browser enters a redirect loop. • Verify that web tier instances can communicate with the primary and replica instances. Also, if your deployment includes a load balancer, verify that it can communicate with the web tier instances. If none of these methods resolves the issue, RSA recommends that you generate and redeploy the integration script to the logon page for your web-based application. For more information, see the implementation guide for your web-based application.

System Behavior	Action
The web-based application redirects you to a page with the error message “Agent Integration Error”.	• Verify that you created an agent record in Authentication Manager. For more information, see Add an Authentication Agent on page 66. • Generate and redeploy the integration script to the logon page for your web-based application. For more information, see the implementation guide for your web-based application. • If your deployment includes a load balancer, verify that the load balancer has persistence configured. Persistence, which is also called “session affinity” or “sticky sessions,” allows a load balancer to send a client to the same server during a session. For Authentication Manager, the load balancer must send the client to the same Authentication Manager instance or web tier during an authentication session. For more information, see your load balancer documentation. • Find a more detailed error message in **rsa-console.log**. For instructions, see the Operations Console Help topic “Download Troubleshooting Files.
Page error occurs after you log on as the test user.	Verify that you are using a supported deployment scenario for RBA. For supported deployment scenarios, see the *RSA Authentication Manager 8.1 Planning Guide*.
After you enter the logon credentials for the test user, you are prompted to log on again.	Do the following: • Verify that the account settings in Authentication Manager allow the test user to log on. The user must exist and belong to the default security domain (SystemDomain), and the account must be enabled. The account must not be expired, and the user must not be locked out. For more information, see Enable a User Account on page 121. • Verify that the RBA policy for the default security domain (SystemDomain) allows automatic enablement and silent collection. For more information, see Risk-Based Authentication Policies on page 94. • Verify that the user is enabled for RBA, if RBA does not allow automatic enablement. • Verify that the Authentication Activity Monitor displays all the required log entries. You will see the following entry types: authentication method success with password and SecurID, authentication method success with RBA, artifact generation success, and artifact delivery success. If this does not resolve the issue, RSA recommends clearing the node secret for Authentication Manager and your web-based application. For more information on clearing the node secret for Authentication Manager, see Manage the Node Secret on page 69. For more information on clearing the node secret for your web-based application, see your web-based application documentation.

User Enablement for Risk-Based Authentication Users

You enable users for risk-based authentication (RBA) using one of the following methods:

Automatic. When a user accesses an RBA-protected resource, the user becomes enabled for RBA automatically after the first successful authentication. For instructions, see the Security Console Help topic "Enable Users Automatically for Risk-Based Authentication."

Manual. Only specified users can access RBA-protected resources. An administrator must manually enable these users for RBA. For instructions, see the Security Console Help topic "Enable Users Manually for Risk-Based Authentication."

Enabling Identity Confirmation Methods for a Risk-Based Authentication Policy

If your deployment uses risk-based authentication (RBA), you must enable at least one identity confirmation method. RBA is a multifactor authentication solution that strengthens traditional password-based systems by applying knowledge of the client device and user behavior to assess the potential risk of an authentication request. If the assessed risk is high, the user is challenged to further confirm his or her identity using one of the following methods:

- **On-demand authentication (ODA).** The user must correctly enter a PIN and a one-time tokencode that is sent to a preconfigured mobile phone number or e-mail account.
- **Security questions.** The user must correctly answer one or more pre-enrolled security questions.

If you enable both security questions and ODA, the user can choose to configure one or both methods. With both methods configured, the user can choose a method when prompted to confirm identity.

How a User Configures an Identity Confirmation Method

To configure an identity confirmation method, a user must do one of the following:

- Complete the configuration process inline during silent collection.

  During silent collection, if the user's assurance level meets the required assurance level, the user is prompted to configure an identity confirmation method.
- Complete the configuration process by invitation using the Self-Service Console.

  After an administrator sends users the link to the Self-Service Console with instructions on how to configure a method, users log on to the Self-Service Console and configure an identity confirmation method.

Device Settings for Risk-Based Authentication

For risk-based authentication (RBA), the system uses device history as a factor in determining risk. The device history is a list of user authentication devices from previous, successful logons. The system maintains a device history for each user. Once added to the list, the device is considered to be registered. When the user tries to access an RBA-protected resource using a registered device, the authentication attempt is likely to have a higher assurance level. When the user attempts to logon with an unknown device, the system challenges the user for identity confirmation. If the logon is successful, the new device is added to the user's device history list.

You specify how the system registers and manages user's devices for RBA. You can configure the following client device settings.

Setting	Description
New device registration	Authentication Manager can register a new device automatically or ask users if they want to register the device. If you expect users to access RBA-protected resources from public or shared devices, allow them to decide which devices they want to register.
Total registered devices	You can set the maximum number of registered devices preserved in each user's device history. If the number of registered devices exceeds the limit, the nightly cleanup job deletes the least recently used devices.
Unregister devices	You can specify when inactive devices are removed from a user's device history. For example, you can specify that devices are removed from a user's device history after 60 days of inactivity. Consider the needs of all your users. Although most users might use the same client devices frequently to access RBA-protected resources, some users might only use public client devices infrequently.

Configure Device Registration for a Risk-Based Authentication Policy

Device registration is the process of saving a user's authentication device in the user's device history list. Each device in the list was used during a previous, successful logon. When the user tries to access an RBA-protected resource using a registered device, the authentication attempt is likely to have a higher assurance level.

The system can register a new device automatically, or users can choose to register the device. If you expect users to access RBA-protected resources from public or shared devices, you may want to allow them to decide which devices they want to register.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Risk-Based Authentication Policies** > **Manage Existing**.
2. Click the policy that you want to configure, and select **Edit**.
3. In the **Device Registration and Identity Confirmation Settings** section, select one of the following for **New Device Registration**:
   - To add the device to the user device history automatically after authentication, select **Register the user authentication device automatically after successful authentication**.
   - To prompt the users to choose if they want to add the device to the device history, select **Prompt the user to choose whether the system registers the device after successful authentication**.
4. Click **Save**.

Configure Device History Settings for a Risk-Based Authentication Policy

For risk-based authentication (RBA), the system maintains a device history for each user. The device history is a list of user authentication devices from previous successful logons. Once added to the list, the device is considered to be registered. When the user tries to access an RBA-protected resource using a registered device, the authentication attempt is likely to have a higher assurance level.

You can set the maximum number of registered devices preserved in each user’s device history. If the number of registered devices exceeds the limit, the nightly cleanup job deletes the least recently used devices.

Also, you can specify when inactive devices are removed from a user’s device history. For example, you can specify that devices are removed from a user’s device history after 30 days of inactivity.

Procedure

1. In the Security Console, click **Authentication** > **Policies** > **Risk-Based Authentication Policies** > **Manage Existing**.
2. Click the policy that you want to configure, and select **Edit**.
3. Under **Device Administration Settings**, enter numbers for the following fields:
   - In the **Total Registered Devices** field, enter the maximum number of registered devices preserved in each user’s device history.
   - In the **Unregister Devices** field, enter the number of consecutive days that a device can remain inactive before the system removes it from the user device history.
4. Click **Save**.

Custom Solutions for Web-Based Applications for Risk-Based Authentication

For web-based applications that have been certified as RSA SecurID Ready but not supported by RSA Authentication Manager for risk-based authentication (RBA), you can create your own custom solution. To create a custom solution, you must create your own RBA integration script using the XML template that RSA provides. For a complete list of RSA SecurID Ready products, go to **https://gallery.emc.com/community/marketplace/rsa?view=overview**.

For instructions on creating an RBA integration script for an RSA SecurID Ready application, see the *RSA Authentication Manager Custom Implementation Guide*. You can download the ISO image from RSA SecurCare Online at **https://knowledge.rsasecurity.com**. (Access to this site requires an RSA SecurCare Online logon account.)

13 Administering RSA RADIUS

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.

RSA RADIUS Authentication Process

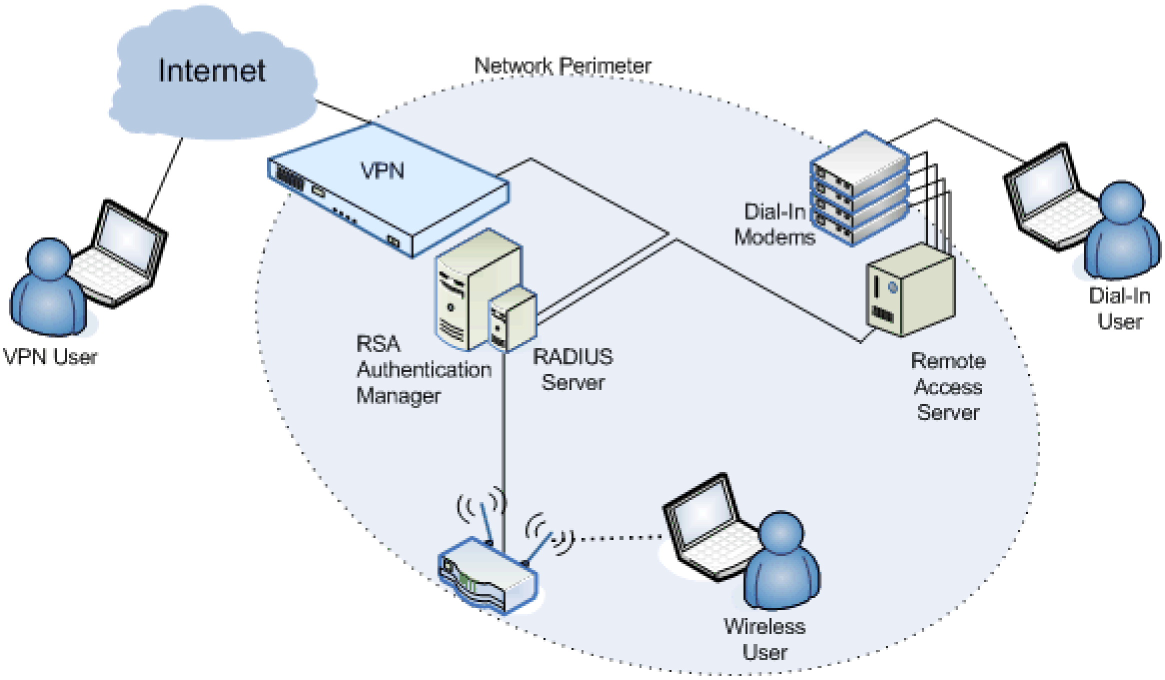
In a RADIUS-protected network, the authentication process works as follows:

1. The user provides authentication information to a RADIUS client.
2. The RADIUS client sends an "Access-Request" to server, which could include the following:
   - User ID
   - User password (encrypted)
   - Client ID
   - Port ID
3. RSA RADIUS validates the client using a shared secret. If no secret exists, the request is ignored.
4. RSA RADIUS checks requirements that must be met for the user to access the resource. The requirements are known as RADIUS attributes and may include the following:
   - Password
   - Clients through which the user can access a resource
   - Ports on which the user can access
5. RSA RADIUS forwards the request to Authentication Manager.

6. Authentication Manager allows or denies the request.
7. RSA RADIUS sends one of three responses:
   - Access-Accept. RSA RADIUS allows access and returns a set of RADIUS attributes to the client.
   - Access-Challenge. RSA RADIUS issues a challenge to which the user must respond, for example, with a passcode.
   - Access-Reject. The conditions are not met so access is denied.

RADIUS clients control user access at the network perimeter. RADIUS clients, which can be VPN servers, wireless access points, or Network Access Servers connected to dial-in modems, interact with RSA RADIUS for user authentication and to establish appropriate access control parameters. When authentication succeeds, RSA RADIUS returns a set of attributes to RADIUS clients for session control.

The following figure shows how an RSA RADIUS server runs as a service on an Authentication Manager instance. The RADIUS service handles the requests from the clients and communicates with the Authentication Manager, which processes the authentications and grants or denies access to the user.



RADIUS Network Topology

Firewalls typically separate the VPN server from the RADIUS server and the Internet. In most cases, multiple RADIUS replica servers are configured with a primary server for load balancing and failover. Additional RADIUS clients may also be configured, for example, as multiple wireless access points in strategic locations throughout a site. These details are somewhat hidden from administrators because most routine administration is applied to a primary server that replicates some of those changes to replica servers.

Some administration operations that are performed less frequently require administrators to know about replica servers for failover, disaster recovery, and other system maintenance purposes.

Remote users with direct Internet connections can access network resources using a RADIUS-enabled VPN server. Remote users without direct Internet connections can connect using telephone lines and dial-in modems connected to a RADIUS-enabled network access server. Wireless users can access the network over RADIUS-enabled wireless access points.

For all of these access methods, RADIUS provides the following capabilities:

- Fine-grained access controls that allow administrators to tightly manage individual user access, restricting users to a specific network access device, session length, IP address or range, or other restriction.
- Comprehensive and flexible accounting that allows administrators to tailor event log data to meet specific needs, whether in support of Sarbanes-Oxley or any other auditing requirement. You can save your log data to a flat file.

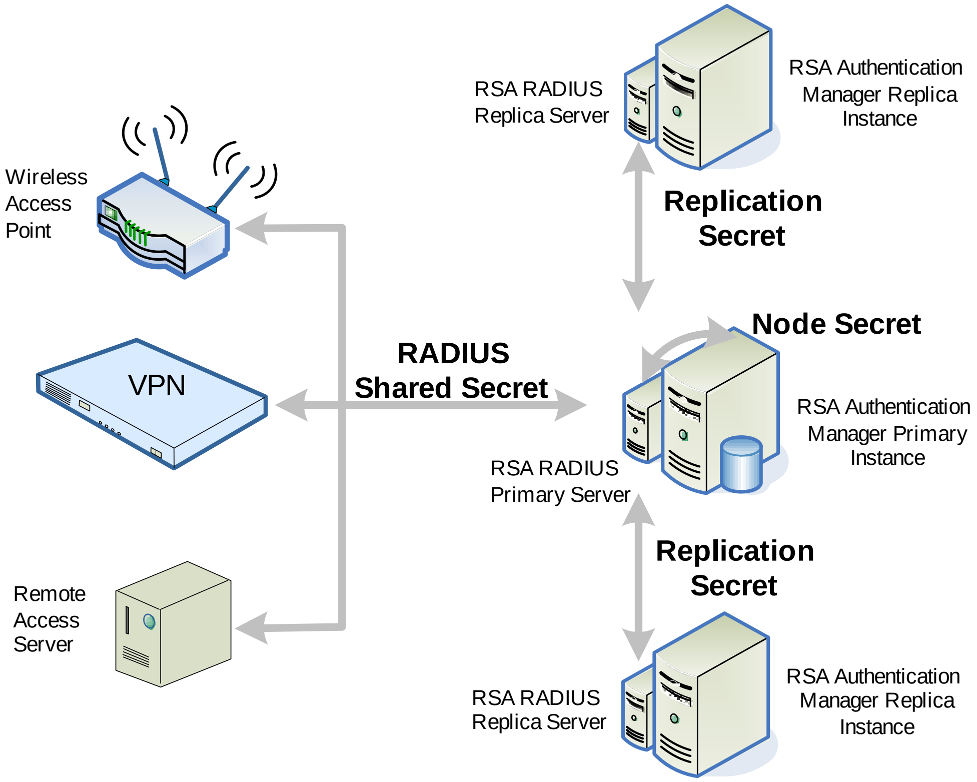
Communication Between RADIUS Servers and Clients

Communication between the RADIUS server and Authentication Manager always uses HTTPS. Communication between RADIUS servers and clients always uses the RADIUS protocol. Authentication Manager uses the security features available in the RADIUS protocol, namely, sensitive fields are encrypted with a shared secret.

A shared secret is a text string that serves as a password between hosts. RADIUS servers use the following types of shared secrets:

- **RADIUS shared secret.** Used to secure communication between a RADIUS server and a RADIUS client.
- **Accounting secret.** (This is not shown in the following figure) Used to secure accounting traffic passed between the RADIUS primary server and a RADIUS client. The RADIUS server uses the accounting secret of the RADIUS client. If no accounting secret exists on the client, the RADIUS server uses the RADIUS shared secret of the client.
- **Replication secret.** Used to secure communication between a RADIUS primary server and a RADIUS replica server. This secret is generated during installation of the Authentication Manager. You cannot manage this secret.
- **Node secret.** Used to secure communication between a RADIUS server and an Authentication Manager server. The RADIUS primary and all replicas use the node secret. This secret is generated during installation of the Authentication Manager. You cannot manage this secret.

You can configure the RADIUS shared secret and the accounting shared secrets through the Security Console. After the RADIUS shared secret is created, you must set the secret in the RADIUS client using the RADIUS client's administrative interface.


Wireless Access Point
VPN
Remote Access Server
RADIUS Shared Secret
RSA RADIUS Replica Server
RSA Authentication Manager Replica Instance
Replication Secret
Node Secret
RSA Authentication Manager Primary Instance
RSA RADIUS Primary Server
Replication Secret
RSA RADIUS Replica Server
RSA Authentication Manager Replica Instance

Managing RSA RADIUS Servers

This topic describes how to manage RSA RADIUS servers throughout their life cycle and includes the following topics:

- Management Consoles for RSA RADIUS Administration
- View RADIUS Servers
- RADIUS Data Replication
- Configure RSA RADIUS to Use System-Generated PINs
- Restart a RADIUS Server
- RSA RADIUS Server Maintenance

Management Consoles for RSA RADIUS Administration

You use the Security Console and Operations Console to manage RSA RADIUS.

Use the Security Console to perform the following routine RADIUS administrative tasks:

- View the RADIUS servers in your deployment, and the IP address and replication status of each RADIUS server.
- Manage RADIUS clients and RADIUS client agents.
- Manage RADIUS profiles, including assigning profiles to users, user groups and agents, and specifying a default profile.
- Manage RADIUS user attributes and custom attributes.
- View RADIUS server and RADIUS client statistics.
- Initiate replication to the replica RADIUS servers.
- Configure periodic replication to the replica RADIUS servers.

Use the Operations Console for non-routine maintenance of the RADIUS servers. You perform the following tasks using the Operations Console:

- View the RADIUS servers in your deployment, and the IP address and replication status of each RADIUS server.
- Manage the certificates used by RSA RADIUS, including the RADIUS server certificate and the trusted root certificates for Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) authentications.
- Manage RADIUS server files, including RADIUS dictionary files and configuration files.

When using the Operations Console to modify RADIUS servers, the following restrictions apply:

- Changes made to one RADIUS server are not replicated to the other RADIUS servers in your deployment, except for changes made to the following:
  - root certificates
  - peapauth.aut
  - ttlsauth.aut
- You must restart the RADIUS server for the changes to take effect.

View RADIUS Servers

You can view a list of all RADIUS servers in RSA Authentication Manager. For example, you might view the list of all servers to quickly determine the number of RADIUS replica servers in Authentication Manager.

You can view the list of all RADIUS servers and the following properties of each:

- **Type.** Primary or Replica.
- **IP Address.** IP address that RADIUS clients and other RADIUS servers use to communicate with this server. This is the same IP address used by Authentication Manager.
- **Replication Status.** The state of RADIUS data on a RADIUS server. For more information see RADIUS Replication Status on page 291.

Procedure

In the Security Console, click **RADIUS** > **RADIUS Servers**.

RADIUS Data Replication

RADIUS synchronizes data on the RADIUS replica servers with the data on the RADIUS primary server. The primary server detects when an administrator changes RADIUS data through the Security Console and sends all RADIUS data that can be replicated to the replica servers. If no changes have been made, data is not replicated.

The RADIUS primary server does not replicate RADIUS configuration files or RADIUS dictionary files. Each RADIUS server has its own set of these files. When you make changes to the files of the RADIUS primary server, you must make the same changes to the files of each RADIUS replica server in your deployment.

You must log on to the Operations Console on the RADIUS server you want to modify to view and edit the RADIUS configuration files. For more information about the configuration files, see the *RSA Authentication Manager 8.1 RADIUS Reference Guide*. For more information about the dictionary files, see the documentation for your RADIUS device.

You use either of two methods to replicate RADIUS data:

- Configure periodic replication
- Initiate replication

By default, the deployment is configured to use periodic replication.

Configure Periodic Replication Method

Periodic replication is the default method. When this is enabled, the RADIUS primary server performs these steps:

1. Searches for changes to the RADIUS data on the primary server every 15 minutes.
2. Replicates any changes to each RADIUS replica server.
3. Verifies that each RSA RADIUS replica server has the latest data.

If an RSA RADIUS replica server fails to update after replication, the RADIUS primary server logs a message to the system log and to the Authentication Manager Critical System Event Notification system, which can be configured to send e-mail to designated personnel. The failure notification can take up to 15 minutes to be logged and sent.

Important: There is no failure notification when you disable periodic replication.

Initiate Replication Method

The initiate replication method requires that administrators use the Security Console to start replicating RADIUS data to the RADIUS replica servers. You can use this method regardless of whether periodic replication is enabled or RADIUS data has been changed. If a RADIUS replica server is offline for a period of time and therefore not up-to-date, once the RADIUS server is available, initiating replication sends the latest RADIUS data to all RADIUS replica servers in the deployment.

Out-of-Date RADIUS Replica Servers

Data on a RADIUS replica server becomes out-of-date when the RADIUS replica server is unavailable for an extended period of time, for example, it is offline or the RADIUS primary server cannot connect to the replica due to a network issue.

A replica server that is unavailable cannot receive data from the RADIUS primary server. However, once the RADIUS replica server becomes available, it checks for missed updates once per hour and initiates replication when it finds more up-to-date data.

If the RADIUS data changes before the hour interval, the RADIUS replica server can still receive the updates through the replication method you configured.

RADIUS Replication Status

RADIUS replication synchronizes data on the RADIUS replica servers with the data on the RADIUS primary server. The primary server detects when an administrator changes RADIUS data through the Security Console and sends all RADIUS data that can be replicated to the replica servers. If no changes have been made, the primary server does not replicate any data.

The following table lists the possible values of the status for RADIUS servers:

Server	Status	Description	Action
Primary	Cannot determine status	The RADIUS primary server may be down.	Verify that the primary instance running the RSA RADIUS service is up. Verifying RSA RADIUS Replication on page 293
	Out-of-Sync	The data on the RADIUS primary server has changed and needs to be replicated to the RADIUS replica servers.	If periodic replication is enabled, none. If periodic replication is not enabled, initiate replication.
	Synchronized	In a deployment with RADIUS replicas, the RADIUS primary has no changes to replicate. **Note:** In a deployment with a RADIUS primary only, there are never any changes to replicate.	None.

Server	Status	Description	Action
Replica	Cannot determine status	Communication between the RADIUS primary server and the RADIUS replica is not working.	Verify that the primary instance running the RSA RADIUS service is up. Verify that the replica instance running the RSA RADIUS service is up and can connect to the primary instance. For more information, see Verifying RSA RADIUS Replication on page 293.
	Initiating Data Transfer	The RADIUS primary is attempting to start replication of data to the replica.	None.
	Out-of-Sync	Changes to data on the RADIUS primary need to be replicated to the replica server.	If periodic replication is enabled, none. If periodic replication is not enabled, initiate replication.
	Synchronized	The data on the RADIUS primary server and the replica server is the same. The replica has the most current RADIUS data.	None.
	Unreachable	The RADIUS primary server cannot connect to the replica server.	Verify that the primary and replica instances can connect. For more information, see Verifying RSA RADIUS Replication on page 293.

Verifying RSA RADIUS Replication

To ensure proper communication between the RADIUS primary and RADIUS replicas, verify the following:

- The Authentication Manager instances are connected to the network.
- All hostnames and IP addresses are correctly configured so that the primary instance can resolve the replica instances by hostname and IP address, the replica instances can resolve the primary instance by hostname and IP address.
- The firewalls between primary and replica instances allow communication on ports 1812 and 1813.
- The system clocks on primary and replica instances are within ten minutes of each other. If the difference in time is greater than ten minutes the RADIUS primary cannot replicate data to the RADIUS replica.

You can check the replication status of a RADIUS server in the RADIUS Servers page of the Security Console.

Enable Periodic RADIUS Replication

When you enable periodic replication, every 15 minutes the RADIUS primary server checks for changes to the RADIUS data and, when changes are found, replicates the RADIUS data to all of the available RADIUS replica servers in your deployment. After replicating the data, the primary server verifies that each RADIUS replica server is up-to-date. If a RADIUS replica server fails to update, the RADIUS primary server logs a message to the system log and to the Critical System Event Notification system, which can be configured to send e-mail messages to designated personnel.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Under Advanced Settings, click **RADIUS**.
3. Under **RADIUS Replication Configuration**, for **Periodic RADIUS Replication**, select **Enable periodic RADIUS Replication every 15 minutes**.
4. Click **Save**.

Initiate Replication to RADIUS Replica Servers

You can initiate replication of the RADIUS database from the primary RADIUS server to all the replica RADIUS servers in your deployment. For example, you might initiate replication to all replica RADIUS servers when you add an important RADIUS client to your network.

Procedure

1. In the Security Console, click **RADIUS** > **RADIUS Servers**.
2. Click **Initiate Replication**.

Configure RSA RADIUS to Use System-Generated PINs

RSA RADIUS does not allow system-generated PINs by default. If you choose to allow system-generated PINs, authentication will fail unless you change the RADIUS configuration file, **securid.ini**, on each RADIUS server to allow system-generated PINs, and then restart RADIUS.

Before You Begin

You must be a Super Admin.

Procedure

1. Log on to the Operations Console on the RSA Authentication Manager instance hosting the RADIUS server.
2. Click **Deployment Configuration > RADIUS Servers**.
3. If prompted, enter your Super Admin User ID and password.

4. Select the server hosted on this instance, and click **Manage Server Files** from the context menu.
5. In the **Configuration Files** tab, select the **securid.ini** file, and click **Edit** from the context menu.
6. Find the following line:

   ```
   AllowSytemPins = 0
   ```

   The 0 indicates that system-generated PINs are not allowed. To allow system-generated PINS, change the setting to the following:

   ```
   AllowSystemPins = 1
   ```

   The 1 indicates that system-generated PINs are allowed.
7. Click **Save and Restart RADIUS**.
8. Restart the RADIUS server for the changes to take effect.

Restart a RADIUS Server

RSA RADIUS servers start automatically when the RSA Authentication Manager starts. You need to restart the RADIUS server in the following situations:

- After changing the port assignments on a RADIUS server.
- After making changes to RADIUS server files (.ini, .dct, or .aut).
- After replacing the RADIUS server certificate.
- If the RADIUS server stops.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Operations Console that is on the RSA Authentication Manager instance hosting the RADIUS server, click **Deployment Configuration > RADIUS Servers**.
2. If prompted, enter your Security Console User ID and password, and click **OK**.
3. Click the RADIUS server that you want to restart, and select **Restart Server** from the context menu.
4. In the Restart RADIUS Server page, under Confirmation, select **Yes, restart RADIUS Server**, and click **Restart Server**.

RSA RADIUS Server Maintenance

You can maintain and modify RSA RADIUS servers for such purposes as servicing a host system, improving authentication response time, or recovering if a RADIUS server becomes unavailable. This section describes the following maintenance tasks:

- RSA RADIUS Server File Customization
- Edit RADIUS Server Files

RADIUS is installed on a primary or replica instance and configured to run on the same instance with Authentication Manager. You can modify the RADIUS server configuration using the Operations Console on the primary or replica instance.

RSA RADIUS uses the same hostname and IP address as the RSA Authentication Manager. To change the hostname or IP address of the RADIUS server, you must change the hostname and IP address of the RSA Authentication Manager.

For information, see Appendix A, Changing the Instance Network Settings.

RSA RADIUS Server File Customization

Each RSA RADIUS server has a set of configuration, initialization, and dictionary files for customizing the server within its working environment. For many situations, the default files provide sufficient functions without any modification. However, you may need to modify these files if any of the following situations apply to your deployment:

- You are modifying logging options, for example accounting attributes.
- You are configuring a RADIUS client that has special attribute names that need to be included in RADIUS profiles. Dictionary files provided with the RADIUS client must be added to each RADIUS server that will handle requests from that client. You may need to edit the **mapping.ini** file to properly associate attribute names across different RADIUS clients.

Use the Operations Console to view the RADIUS server files (the configuration, initialization and dictionary files) and open the files for editing. For a detailed explanation of the syntax used in the configuration files, see the *RSA Authentication Manager 8.1 RADIUS Reference Guide*.

Edit RADIUS Server Files

You may need to modify one or more RSA RADIUS server files. For example, you may need to edit these files if you are modifying logging options or configuring a RADIUS client that has special attribute names that need to be included in the RADIUS profiles.

Edits apply only to the RADIUS server on which you make the changes.

Important: Be cautious when editing the configuration files. The changes that you make are not validated, and the existing file is overwritten with the new content. For a detailed explanation of the syntax used in the configuration files, see the *RSA Authentication Manager 8.1 RADIUS Reference Guide*.

Before You Begin

You must have Super Admin and Operations Console administrator credentials.

Procedure

1. Log on to the Operations Console on the RSA Authentication Manager instance hosting the RADIUS server.
2. Click **Deployment Configuration** > **RADIUS Servers**.

3. If prompted, enter the Super Admin User ID and password, and click **OK**.
4. Select the RADIUS server hosted on this instance, and select **Manage Server Files** from the context menu.
5. On the Manage Server Files page, do one of the following:
    - Click the **Configuration Files** tab to see the configuration files, such as .conf, .aut, and .ini.
    - Click the **Dictionary Files** tab to see the RADIUS dictionary files.
6. Select the file that you want to edit, and select **Edit** from the context menu.
7. Edit the text file, and click **Save**.
8. Click **Save & Restart RADIUS Server** for the changes to take effect.

Next Steps

You must copy to other RADIUS servers any edits that must be synchronized across the environment, such as edits to .dct files. To copy edits to another RADIUS server in the deployment, select the appropriate RADIUS server from the Manage RADIUS Server page, and copy or make the edits to the replica.

RADIUS Clients

A RADIUS client is a RADIUS-enabled device at the network perimeter that enforces access control for users attempting to access network resources.

A RADIUS client can be one of the following:

- VPN server
- Wireless access point
- Network access server supporting dial-in modems
- Dial-in modem

A RADIUS client sends a user's access request to the RADIUS server. The RADIUS server forwards the request to RSA Authentication Manager for validation.

If Authentication Manager validates the access request, the RADIUS client accepts the user's request for network access. Otherwise, the RADIUS client rejects the user's request for network access.

You can configure RADIUS clients with or without an assigned authentication agent. The difference between the two methods is in the level of access control and logging you want to have.

> **RADIUS client with an agent.** Adding an agent to a RADIUS client allows Authentication Manager to determine which RADIUS client is used for authentication and to save this information in log files.

When you add a RADIUS client, you have the option to create an associated agent. If you manually configure an agent with the same hostname and IP address as the RADIUS client, the agent is automatically recognized as a RADIUS client agent.

For more information, see Add a RADIUS Client.

RADIUS client without an agent. Without an assigned RADIUS client agent, Authentication Manager cannot track which RADIUS client sends authentication requests and you cannot assign a profile to the client. The RADIUS server simply confirms that the shared secret from the RADIUS client matches the shared secret stored in RSA RADIUS, and then forwards the request without any client information to Authentication Manager.

All authentication requests appear to be coming from the RADIUS server through its assigned authentication agent. While using this method, if you add an agent to a RADIUS client in the Security Console, Authentication Manager does not associate the agent with the client, so it does not apply any of the agent properties that you specify to the client.

To allow the system to authenticate users from clients with no assigned agent, you must set the **SecurID.ini** file parameter CheckUserAllowedByClient to 0. By default, this parameter is set to 1, which allows the system to authenticate users from clients with an assigned agent. For more information, see the *RSA Authentication Manager 8.1 RADIUS Reference Guide*.

If you need to add a large number of RADIUS clients to Authentication Manager, you might not want to assign agents to RADIUS clients. For example, you are an ISP administrator and need to add and configure one thousand network access servers with the RSA RADIUS server. Instead of adding an agent to each RADIUS client, you select **ANY RADIUS client**, and enter the same shared secret for each RADIUS client. When an *ANY* client sends a network request to its associated RADIUS server, the RADIUS server confirms the shared secret and forwards the request without any client information to Authentication Manager.

Add a RADIUS Client

You must add a RADIUS client to the deployment for each RADIUS device that is configured to use RSA SecurID as its authentication method. The RADIUS client sends authentication requests to the RSA RADIUS server, which then forwards the request to Authentication Manager.

If you want to use risk-based authentication (RBA), RBA must be enabled for the agent associated with the RADIUS client.

Procedure

1. In the Security Console, click **RADIUS** > **RADIUS Clients** > **Add New**.

   In the **Client Name** field, enter the name of the client, for example, VPN-London. You can enter letters, digits, hyphens (–), and underlines(_). Spaces, tabs, @ signs, most symbols, and non-printable characters are not allowed. This field is limited to 50 characters.

   If you do not want RSA Authentication Manager to track which RADIUS client sends authentication requests (for example, because you want to quickly add many RADIUS clients), you do not need to enter a name.

2. (Optional) In the **ANY Client** field, select

   If you select this option, you also need to disable proxy authentication so that the RADIUS server does not authenticate on behalf of this RADIUS client. For more information, see RADIUS Clients on page 297.

   After you save the client, you cannot change its name. If you want to rename the client, you must delete it and then add a new client with the new name.

3. In the **IP Address** field, enter the IP address of the RADIUS client, for example, 111.222.33.44.

   You cannot enter an IP address if you select **ANY Client** in the previous step because the IP address is not applicable.

4. In the **Make/Model** drop-down list, select the type of RADIUS client. If you are unsure of the make and model of the RADIUS client, select **Standard Radius**.

   The RADIUS server uses the make and model to determine which dictionary of RADIUS attributes to use when communicating with this client.

5. In the **Shared Secret** field, enter the authentication shared secret (case-sensitive password) that you specified during the RADIUS client installation and configuration.

   The RADIUS client uses the same shared secret when communicating with the RADIUS primary server or RADIUS replica server.

6. If you want to use a different shared secret (other than the one specified in step 5) for accounting transactions between the RADIUS client and RADIUS server, select **Accounting**.

   In the **Accounting Shared Secret** field, enter the accounting shared secret that you entered during the RADIUS client installation and configuration. The RADIUS client uses the same shared secret when communicating with the RADIUS primary server or RADIUS replica server.

7. Select **Client Status** to specify how many seconds the RADIUS server maintains the client connection without receiving a keepalive packet from the RADIUS client.

   In the **Inactivity Time** field, enter the number of seconds. Enter a slightly higher value than the keepalive value specified in the RADIUS client configuration. If you choose a time frame that is too short, the server might close valid connections. For more information, see the RADIUS client documentation.

8. In the **Notes** field, enter any notes for this client, for example, "Located at London site."

9. To save your changes, do one of the following:

   - Click **Save and Create Associated RSA Agent**. This choice allows Authentication Manager to determine which RADIUS agent is used for authentication and to log this information. This option is required if you want to use risk-based authentication (RBA).

   - Click **Save** only if you have disabled proxied authentication (by setting the **securid.ini** file parameter CheckUserAllowed ByClient to 0). In this case, you cannot assign a profile to this client, and all authentications appear to Authentication Manager as though they are coming from the RADIUS server.

Next Steps

- If you created an associated RSA agent for this RADIUS client, you must configure the agent. For instructions, see the Security Console Help topic "Add a RADIUS Client Agent" and begin at step 8.
- Once configured, replication takes place every 15 minutes. If you want to manually initiate replication to notify the RADIUS replica servers about this new client, see Initiate Replication to RADIUS Replica Servers on page 294.

EAP-POTP Settings

Extensible Authentication Protocol (EAP) is an authentication framework that supports multiple authentication methods. This allows RADIUS to support new authentication methods without requiring any changes to the RADIUS protocol or RADIUS servers. EAP-POTP defines the method for one-time password (RSA SecurID) authentication and provides the following capabilities within RSA RADIUS:

- End-to-end protection of one-time password
- Mutual authentication
- Session key derivation for 802.1x (wireless)
- Support for token exception cases (for example, New PIN or Next Token code)
- Fast session resumption if a wireless connection is lost

EAP-POTP settings define basic parameters for keying material (and keys) protecting one-time passwords used for authentication.

The default values balance security (cryptographic strength) with system responsiveness and are considered satisfactory for most environments. You may increase or decrease EAP-POTP default values. However, even slight changes to values used for key generation may cause a large change in response time during authentication. EAP-POTP settings affect the entire deployment.

Note: RSA RADIUS does not support the Filter-ID attribute when using EAP authentication methods.

EAP-TTLS Configuration

You can configure the RSA RADIUS server to handle Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) authentications. RSA RADIUS requires the following certificates to handle authentication requests made using the EAP-TTLS protocol:

- A server certificate for each RADIUS server, which is used by a RADIUS client to verify the identity of the RADIUS server. A server certificate is installed on each RADIUS server by default.
- A trusted root certificates, which is used by a RADIUS server to verify the identity of a RADIUS client. Root certificates are not installed on the RADIUS server by default.

Replace a RADIUS Server Certificate

A RADIUS server certificate is presented to a RADIUS client by RSA RADIUS so that the client can verify the identity of the RADIUS server. You can use the Operations Console to replace the existing server certificate of a RADIUS Server with a different certificate. For example, you might prefer to assign a certificate that has your organization as its trusted root signer. RSA RADIUS does not replicate the server certificate. You must access each RADIUS server directly and perform the following procedure.

Before You Begin

- You must be a Super Admin.
- Make sure you have a keystore (.pfx) file that contains the new server certificate and the associated private key. This file should be in PKCS #12 file format and contain the replacement certificate and private key only. If the keystore contains more than one certificate, the wrong certificate may be used as the replacement server certificate.
- Add a Trusted Root Certificate to the system. Add the certificate used to sign the replacement server certificate. The signing certificate must be in DER format and have a .der extension. If the replacement certificate is self-signed, you do not need to add the signing certificate.

Procedure

1. On the primary instance Operations Console, click **Deployment Configuration** > **RADIUS Servers**.
2. If prompted, enter your Security Console User ID and password, and click **OK**.
3. Click the RADIUS server whose certificate you want to replace, and select **Manage EAP Certificates** from the context menu.
4. In the Manage EAP Certificates page, click the **Server Certificate** tab.
5. Under **Replace Server Certificate**, click **Browse** to locate the keystore file containing the replacement certificate and associated private key.

   You must select a keystore that is in PKCS #12 certificate store format, with a .pfx suffix.
6. Enter the password for the keystore file containing the replacement certificate in the **Keystore Password** field.
7. Click **Save & Restart RADIUS Server**.

   The RADIUS server must restart for the change to take effect.
8. Repeat this procedure for each RSA RADIUS server in the deployment.

Add a Trusted Root Certificate

A trusted root certificate is used by a RADIUS server to verify the identity of a RADIUS client. Use the Operations Console to add trusted root certificates for RSA RADIUS. By default, RSA RADIUS contains no trusted root certificates. You can add as many certificates as you need. You need to add a trusted root certificate on the primary instance only. RSA RADIUS replicates trusted root certificates to all RSA RADIUS servers in the deployment.

Before You Begin

- You must be a Super Admin.
- Verify that the certificate meets the following requirements:
  - certificate is in DER format.
  - certificate file has a .der extension.

Procedure

1. Log on to the Operations Console on the Authentication Manager primary instance.
2. Click **Deployment Configuration** > **RADIUS Servers**.
3. If prompted, enter your Super Admin User ID and password.
4. Select the primary RADIUS server, and click **Manage EAP Certificates** from the context menu.
5. In the Manage EAP Certificates page, click the **Trusted Root Certificates** tab.
6. Click **Browse** to locate and select the certificate that you want to add.
7. Click **Add** to add the certificate to the server.
8. When you are finished adding trusted root certificates, click **Done**.

Managing User Access

RSA RADIUS administrators manage RADIUS user access through the use of attribute-value pairs. During a RADIUS authentication attempt, the RADIUS client and server exchange lists of attributes and their values. The server sends a checklist and the client replies with a return list.

You can assign an attribute in two ways:

- Add the attribute to a RADIUS profile and assign the profile to a user or agent.

  For more information, see Add a RADIUS Profile on page 305 and RADIUS Profile Associations on page 306.
- Assign a user attribute, either a standard user attribute or a custom user attribute, to a user directly.

  For more information, see RADIUS User Attributes on page 310.

This section contains the following topics:

RADIUS Profiles

A RADIUS profile is a named collection of attributes that specify session requirements for users authenticating using RADIUS. When you create or update a profile, you can add, remove, or modify attributes and their values within checklists and return lists.

Profiles support easy administration of groups of users. An administrator creates a profile with a checklist and a return list of attributes suitable for a specific group of users, and then assigns the profile to relevant user identities defined within Authentication Manager. Available checklist and return list attributes appear in the Security Console in the drop-down list on the management pages for creating and updating profiles.

Profiles are synchronized across all RSA RADIUS servers in the deployment. The profile names reside on Authentication Manager so that they can be centrally managed from the Security Console. RSA RADIUS, when shipped, contains no profiles. You create profiles using the Security Console.

RADIUS Attributes

RSA RADIUS provides more flexibility in controlling system behavior during authentication through the use of single-value and multiple-value attributes and orderable multiple-value attributes.

- Single-Value and Multiple-Value Attributes

  Attributes can be single-value or multiple-value. Single-value attributes appear only once in the checklist or return list. Multiple-value attributes may appear several times. If an attribute appears more than once in the checklist, this means that any one of the values is valid. For example, you can set up a checklist to include multiple telephone numbers for the attribute Calling-Station-ID. Because all of the telephone numbers are valid, a user trying to dial in to your network can call from any of the designated telephone numbers and still authenticate successfully.

  If an attribute appears more than once in the return list, each value of the attribute is sent as part of the response packet. For example, to enable both IP and IPX header compression for a user, the Framed-Compression attribute must appear twice in the return list: once with the value VJ-TCP-IP-header-compression and once with the value IPX-header-compression.

- Orderable Multiple-Value Attributes

  Certain multiple-value return list attributes are also orderable, which means that the attribute can appear more than once in a RADIUS response, and the order in which the attributes appear is important. For example, the Reply-Message attribute allows text messages to be sent back to the user for display. A multiline message is sent by including this attribute multiple times in the return list, with each line of the message in its proper sequence.

RADIUS Checklist

The RADIUS checklist is the set of attributes that must be sent from a RADIUS client to a RADIUS server as part of an authentication request. If a required attribute is not present, the request is rejected. For example, the checklist attribute, NAS-IP-Address, specifies the IP address of a RADIUS client that the user is allowed to use. If this attribute is not in the access request, the request is rejected.

The RADIUS server examines authentication requests from RADIUS clients to confirm that attributes and values defined in a profile as checklist attributes are contained in the authentication request.

By default, a RADIUS client sends all available attributes and values with authentication requests. If a RADIUS client is configured to not send some attribute and that attribute is defined as a checklist attribute, the authentication request fails. See the RADIUS client device documentation for procedures on how to configure a RADIUS client.

You can assign an attribute to the checklist by adding the attribute to a RADIUS profile and then assigning the profile to a user or agent.

RADIUS Return List

The RADIUS return list is the set of attributes that a RADIUS server returns to a RADIUS client when a user is authenticated. Return list attributes provide additional parameters, such as VLAN assignment or IP address assignment, that the RADIUS client needs to connect the user. When authentication succeeds, RADIUS sends return list attributes to the RADIUS client along with the Access-Accept message for use in setting session parameters for that user.

You can add an attribute to the return list in two ways:

- Add the attribute to the return list in a profile and assign the profile to a user or agent. For more information, see Add a RADIUS Profile on page 305 and RADIUS Profile Associations on page 306.
- Assign a user attribute, either a standard user attribute or a custom user attribute, to a user directly. For more information, see RADIUS User Attributes on page 310.

Note: The purpose and use of specific attributes is described in the documentation for particular RADIUS client devices and is outside the scope of this guide.

Default Profile

RSA RADIUS supports a default profile. When a RADIUS user authenticates and has no assigned profile, the user receives the attributes and values that are defined in the default profile, if one is specified.

There is no default RADIUS profile specified during installation. Administrators must create the default profile and specify it as the default. Once you have added one or more RADIUS profiles to Authentication Manager, you can specify the default profile on the System Settings page in the Security Console. However, you can also specify a default profile in the **securid.ini** RADIUS configuration file. The default profile specified in Authentication Manager always overrides any default profile specified in the **securid.ini** file.

Administrators can add, remove, or modify attributes and their values within checklists and return lists for the default profile in the same manner as for regular profiles.

For more information on setting a default RADIUS profile, see the Security Console Help topic "Configure RADIUS Settings."

Dictionary Files to Customize Attributes

RSA RADIUS provides standard RADIUS attributes defined in dictionary files provided with the server. These standard attributes are sufficient to support most major brands of RADIUS client devices. If you purchase a new or specialized RADIUS client device, that device may also have its own dictionary file that contains client-specific attributes. You can install that dictionary file on each of the RADIUS servers so that new or changed RADIUS client attributes are available for inclusion in profiles.

In some rare cases, attribute names in RADIUS may differ from attribute names used by a particular RADIUS client. The Operations Console allows administrators to modify attributes defined in dictionary files.

Add a RADIUS Profile

A RADIUS profile is a named collection of attributes that specify session requirements for a user requesting remote network access. Attributes are contained in a checklist or return list.

You can add a profile to create a collection of checklist and return list attributes that you want to assign to users, user aliases, trusted users, or agents.

Procedure

1. In the Security Console, click **RADIUS** > **RADIUS Profiles** > **Add New**.
2. In the **Profile Name** field, enter a unique name that identifies the purpose for this profile, for example, SALES.

   After you save the profile, you cannot change its name. If you want to rename the profile, you must delete it and then add a new profile with the new name.
3. In the **Notes** field, enter any notes for this profile, for example, Use this profile for all employees in Sales.
4. In **Return List Attributes**, do one of the following:

- If you want to add an attribute, select each return list attribute, enter its corresponding value for this profile, and click **Add**. For more information about the attributes and their values, see the RADIUS client documentation.
- If you want to remove an attribute, select the attribute from the list box, and click **Remove**.
- If you want to update an attribute, select the attribute from the list, enter the updated value in the field, and click **Update**. If you enter a multivalued return list attribute (marked with an M) that is orderable (marked with an O), click **Up** or **Down** to specify the necessary order for the attribute and its value.
- If you do not want to specify a particular value, but want to make sure that the attribute value in the RADIUS request is echoed to the client in the RADIUS response, select **Echo** for the attribute.

5. In **Checklist Attributes**, do one of the following:
   - If you want to add an attribute, select each checklist attribute, enter its corresponding value for this profile, and click **Add**. For more information about the attributes and their values, see the RADIUS client documentation.
   - If you want to remove an attribute, select the attribute from the list box, and click **Remove**.
   - If you want to update an attribute, select the attribute from the list, enter the updated value in the field, and click **Update**.
   - If a RADIUS client does not send one of these attributes (for example, Port-Limit), and you select **Default** for the attribute (for example, Port-Limit), the RADIUS server still processes the authentication request. If a RADIUS client does not send one of these attributes, and you do not select **Default** for the attribute, the RADIUS server rejects the authentication request.
6. Click **Save**.
7. To notify the RADIUS replica servers about this new profile, initiate replication to the replica servers. Once configured, replication takes place every 15 minutes. For instructions, see Initiate Replication to RADIUS Replica Servers on page 294.

RADIUS Profile Associations

You can associate RADIUS profiles with users and agents in your deployment by assigning a profile to them. When you assign a profile to a user or agent, the RADIUS server uses the checklist and return list contained in the profile whenever the user or agent attempts a RADIUS authentication. Assigning a profile designates the checklist and return list contained in the profile as the set of attributes to be used when a RADIUS authentication attempt is made.

An administrator can assign or unassign a profile to the following:

- **User.** An account managed by the system that is usually a person, but may be a computer or a web service.
- **User Alias.** Allows users to authenticate with their RSA SecurID tokens, but using User IDs other than their own. For example, suppose you assign the alias "root" to certain administrators. The administrators can log on using the User ID "root" and their own tokens.

- **Trusted User.** A user from a different, trusted RSA Authentication Manager 8.1 deployment that can authenticate to Authentication Manager through your deployment.
- **Agent.** A software application installed on a RADIUS client or server, which enables authentication with Authentication Manager on the network server.

You can specify a default RADIUS profile that Authentication Manager assigns to a user's network request, if the user and the agent (that the user sends the network request to) do not have an assigned RADIUS profile.

User Assignment

Users are defined within Authentication Manager and their association with the correct RSA SecurID token record is maintained there. On the RADIUS pages in the Security Console, an administrator can associate a User ID with a profile. This action applies the attributes of that profile to that user.

User Alias Assignment

User aliases allow a user to have multiple roles if necessary. For example, user Alice has a user identity Alice_User and a user alias identity Alice_Admin. When Alice logs on as Alice_User, all of the attributes associated with users are applied to her because her user identity is associated with a profile set up for users. When Alice_Admin logs on, attributes more appropriate for administrators are applied to her because her user alias identity is associated with a profile set up for administrators, for example, she can access IP addresses needed to manage routers and VPN servers.

Trusted User Assignment

Within a trusted realm, users from another version 8.1 realm may attempt to access resources using RSA RADIUS. How RADIUS profiles are associated with these users depends on how these remote “trusted users” are defined in the local realm.

Note: Using RSA_RADIUS to authenticate trusted users requires that trusted realms are running Authentication Manager 7.1 or later. Trust relationships between Authentication Manager 8.1 and 6.1 realms do not support authentications using RSA RADIUS.

A trusted user identity may be defined in Authentication Manager in advance, with a RADIUS profile associated with that trusted user identity. That profile may be set up especially for trusted users giving them attributes appropriate for trusted users. When that trusted user’s access request succeeds, RADIUS returns the associated profile attributes to the RADIUS client device along with any assigned RADIUS user attributes.

If the trusted user identity is not set up in advance, the authentication agent on the RADIUS server creates a trusted user account dynamically in Authentication Manager. In turn, Authentication Manager forwards the authentication request to other trusted realms until a success or failure is returned. When the request is successful, Authentication Manager adds the trusted user’s home realm to the trusted user identity (to speed up future authentication requests) and returns a passcode accepted message to RADIUS.

If an agent profile is associated with the RADIUS client (the VPN server, wireless access point, or network access servers supporting dial-in modems) used by the trusted user, the trusted user receives the attributes of that profile. Otherwise, the user receives the default profile, if one is specified.

Authentication Agent Assignment

Assigning a profile to an authentication agent causes the attributes in the profile to be assigned to all users authenticating using that specific RADIUS client device.

For example, a remote user authenticating through a VPN server could have access to one set of resources while that same user authenticating over a wireless access point could access a reduced set of services. RSA RADIUS allows administrators to choose whether an agent profile takes precedence over a user profile. This avoids conflicts in the case where a profile for users and a profile for an agent could both be applied to a user. For instructions, see the Security Console Help topic "Configure RADIUS Settings."

Profile Priority

To avoid conflicts in cases where a profile for users and a profile for an agent could both be applied to a user, for example, you assign a RADIUS profile to a user, and the user requests network access from a RADIUS client with an agent that has a different assigned profile. To prevent profile conflicts, specify the profile precedence.

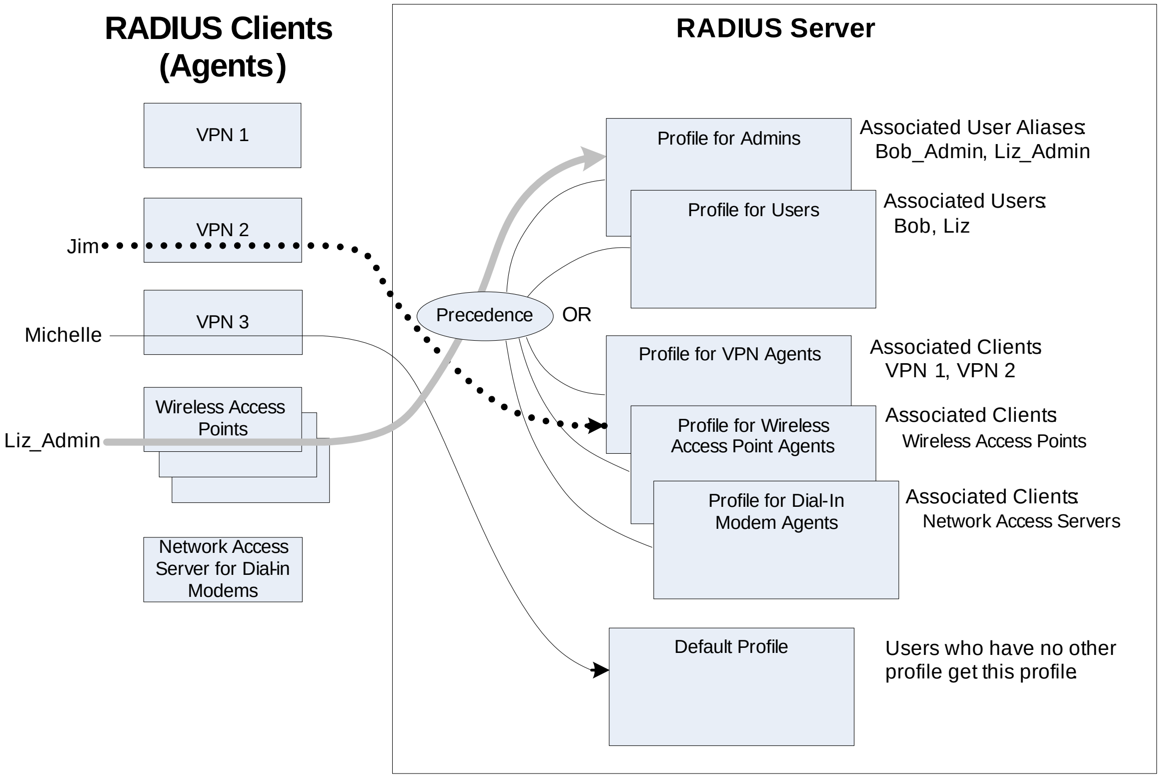
For instructions, see the Security Console Help topic "Choose the Priority of Agent or User RADIUS Profiles."

Profile Assignment Example

The following figure shows how RADIUS applies profiles to users based on associations of profiles to users and agents (RADIUS clients).

- Jim is not explicitly associated with a profile. He authenticates through VPN2 that does have an explicitly associated profile, so he gets the profile for VPN agents.
- Liz_Admin is explicitly associated with the profile for Administrators. She is authenticating through a wireless access point that also has an explicitly associated profile. As both profiles could be applied to Liz Admin, the precedence mechanism determines which profile is applied.

- Michelle does not have an associated profile. She is authenticating through VPN3 that also does not have an explicitly associated profile for agents. RADIUS applies the default profile because no other profile applies to Michelle.


RADIUS Clients (Agents)
RADIUS Server
VPN 1
VPN 2
VPN 3
Wireless Access Points
Network Access Server for Dial-In Modems
Jim
Michelle
Liz_Admin
Precedence
OR
Profile for Admins
Associated User Aliases Bob_Admin, Liz_Admin
Profile for Users
Associated Users Bob, Liz
Profile for VPN Agents
Associated Clients VPN 1, VPN 2
Profile for Wireless Access Point Agents
Associated Clients Wireless Access Points
Profile for Dial-In Modem Agents
Associated Clients Network Access Servers
Default Profile
Users who have no other profile get this profile

Specify the Default RADIUS Profile

Specify the default RADIUS profile that the RADIUS server assigns to a user's network request, if the user and the agent (that the user sends the network request to) do not have an assigned RADIUS profile.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Under Advanced Settings, click **RADIUS.**
3. Select the profile from the **Selected RADIUS Profile** drop-down menu for **Default RADIUS Profile**.
4. Click **Save**.

RADIUS User Attributes

RSA RADIUS supports standard and custom RADIUS attributes.

- **Standard.** Attributes with fixed names and assigned ID numbers specified by the RADIUS protocol. For more information, see the RADIUS client device documentation.
- **Custom.** Attributes defined by a RADIUS client manufacturer that are not included in the RADIUS protocol. If you want to use these custom attributes, you define them through the Security Console, and then assign them to a user or trusted user. The user alias of a user is also assigned these custom attributes. For more information, see the Security Console Help topic, Edit a Custom RADIUS User Attribute Definition.

If you have attributes that you want to assign to more than one user, user alias, trusted user, or agent, you can create a profile with the attributes and assign the profile to the object.

If you want to assign specific standard or custom attributes to only one user or trusted user, you can assign these RADIUS attributes to a user or trusted user outside of a RADIUS profile. RADIUS attributes that you assign to a user or trusted user outside of a profile are called RADIUS user attributes. When you can assign RADIUS user attributes to a user, any user alias of the user is also assigned the attributes. You cannot assign user attributes to an agent. RSA Authentication Manager automatically assigns the attribute with its value to user aliases associated with the user object.

You can define a RADIUS user attribute in two ways:

- Without an actual value

  When this attribute is assigned to a user, the administrator can enter the value appropriate for that user. For example, if the RADIUS user attribute is Callback Number, the administrator enters the user’s callback phone number when he or she applies the attribute to the user. (RADIUS can use a callback number to ensure that a user is calling from a specific phone number). RADIUS user attributes override profile attributes with the same name.
- Mapped to data stored in an identity source

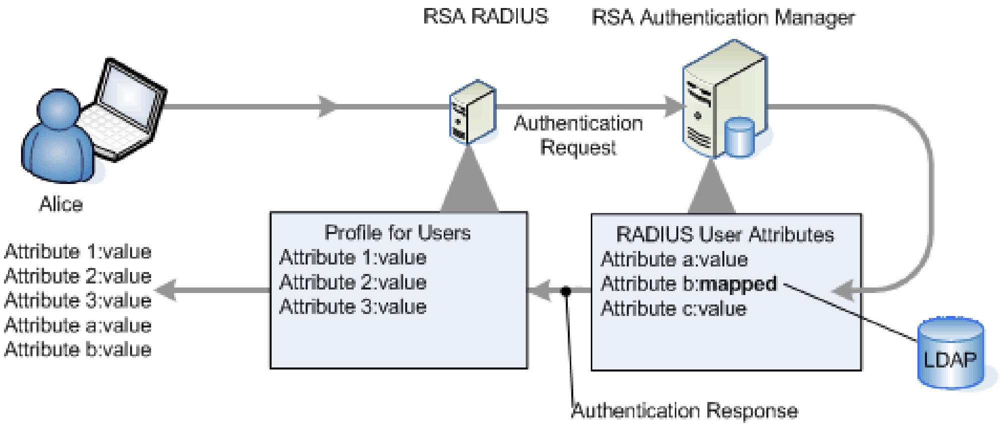
  In this case, the attribute returns information that is already stored in an identity source, such as an LDAP corporate identity database, avoiding the need to maintain attribute values in multiple places.

The RADIUS server sends RADIUS user attributes along with the profile return list attributes to a RADIUS client. These assigned RADIUS user attributes override attributes assigned to the user or trusted user through profiles.

You can also map a RADIUS user attribute definition to an identity source attribute. The RADIUS server applies the value of the identity source attribute to the RADIUS user attribute definition. For example, you can map the RADIUS Callback-ID attribute to the Phone Number attribute in the LDAP corporate database. If you do not map a RADIUS user attribute definition to an identity source attribute, when you assign the RADIUS attribute to the user or trusted user, you must enter the attribute value.

User Attribute Assignment Example

The following figure shows the relationship of profile return list attributes and RADIUS user attributes when user Alice authenticates using RADIUS. Alice is assigned RADIUS user attributes a and b (attribute c is assigned to someone else). When Alice authenticates successfully, she gets all of the profile attributes and RADIUS user attributes a and b. The value for RADIUS user attribute b is taken from an LDAP identity store.



Add a Custom RADIUS User Attribute Definition

RADIUS user attributes can be assigned to user outside of the user's assigned RADIUS profile. For example, you might want to add a callback telephone number attribute to later individually assign to users with their specific telephone numbers.

A custom RADIUS user attribute can be either of the following:

- A new, non-standard RADIUS attribute (value of 64 to 255) that you add a to a RADIUS dictionary.
- A non-standard RADIUS attribute that exists in a RADIUS dictionary.

You can add a custom user attribute definition with or without an actual value, or map it to an attribute in an LDAP directory.

Before You Begin

- When the custom RADIUS attribute is a new attribute, make sure that it does not conflict with an existing attribute in the dictionary. If the dictionary contains an attribute that uses the same name or number as the attribute that you want to add, comment out the conflicting attribute.
- When you create a new custom attribute, for each RADIUS client type that uses the attribute, add a RADIUS attribute definition to the RADIUS dictionary for that client type. You must add the attribute to the dictionary on each RSA RADIUS server. For instructions, see the Operations Console Help topic "Add a RADIUS Attribute Definition to a Dictionary."

Procedure

1. In the Security Console, click **RADIUS** > **RADIUS User Attribute Definitions** > **Add New**.
2. In the **Number** field, enter a number between 64 and 225.
3. In the **Attribute Name** field, enter a name that describes the function of the attribute.

   Enter a name that is different from the standard RADIUS attribute names.
4. In the **Map to Identity Attribute** section, select whether to map the custom attribute to an identity source attribute or to manually enter the attribute value, and do one of the following:
   - If you select **Yes**, select the identity attribute to which you want to map the RADIUS attribute, and enter any notes about this attribute mapping, for example, Mapped to telephone number in HR database.
   - If you select **No**, enter the default value and any notes about this attribute, for example, User's office telephone number as of October 1, 2012.
5. Click **Save**.

Next Step

If you do not enter the value when you add the definition, you must enter the attribute value when you assign the attribute to a user or trusted user. For more information, see Assign RADIUS User Attributes to Users.

Assign RADIUS User Attributes to Users

You can assign standard or custom RADIUS attributes to a user. For example, you might assign the Callback-Number attribute to a user with the value as the user's individual office telephone number. RSA Authentication Manager automatically assigns the attribute with its value to user aliases associated with the user object.

If you assign a user to a RADIUS attribute both in a RADIUS profile and as a RADIUS user attribute, the RADIUS server applies the value that you specify in the RADIUS user attribute definition.

Before You Begin

Enable RADIUS user attributes. For more information, see the Security Console Help topic "Enable or Disable RADIUS User Attributes."

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Click the user to which you want to assign an attribute.
3. From the context menu, click **Authentication Settings**.

4. In **RADIUS User Attributes**, do one of the following:
   - If you want to add an attribute, select the attribute that you want to assign to the user, enter the value for the attribute in the **Value** field, and click **Add**.
   - If you want to remove an attribute, select the attribute from the list, and click **Remove.**
   - If you want to update an attribute, select the attribute from the list, enter the value in the field, and click **Update**.

     A RADIUS user attribute can be mapped to an identity source attribute. For more information, see Map a RADIUS User Attribute Definition to an Identity Source Attribute.
5. Click **Save**.

Map a RADIUS User Attribute Definition to an Identity Source Attribute

You can map a RADIUS user attribute definition to an identity source attribute. For example, you can map the RADIUS Callback-ID attribute to the Phone Number attribute in the corporate LDAP directory.

If you do not map a RADIUS user attribute definition to an identity source attribute, when you assign the RADIUS attribute to the user, you must enter the attribute value.

Procedure

1. In the Security Console, click **RADIUS** > **RADIUS User Attribute Definitions** > **Manage Existing**.
2. Click **Standard Attributes** or **Custom Attributes**.
3. Click the attribute that you want to map.
4. From the context menu, click **Edit**.
5. In **Map to an Identity Attribute**, select **Yes**.
6. From the **Select an Identity Attribute** list, select the identity attribute for which you want to map the RADIUS attribute.
7. Click **Save**.

Monitoring and Analyzing System Usage

After the initial deployment is installed and configured, you may need to actively monitor RSA RADIUS system usage for the purposes of detecting attacks, auditing, and troubleshooting.

This section explains RSA RADIUS system usage analysis in detail. The following tasks are described:

- View RADIUS Server Statistics
- View RADIUS Client Authentication and Accounting Statistics

RADIUS Server Authentication Statistics

Authentication statistics summarize the number of authentication acceptances and rejections, with summary totals for each type of rejection or retry.

The following table describes the authentication statistics fields and the possible causes for some authentication rejections.

Authentication Statistic	Meaning
Transactions	
Accepts	The current, average, and peak number of RADIUS transactions that resulted in an accept response.
Rejects	The current, average, and peak number of RADIUS transactions that resulted in a reject response. These are detailed in the Reject Details section.
Overall	
Total Transactions	The sum of the accept, reject, and silent discard totals.
Silent Discards	The number of requests in which the client could not be identified. This might occur if a RADIUS client entry cannot be found for a device with the name, IP address, or both of a device requesting authentication services.
Challenges	The number of challenges received from RADIUS clients.
Reject Details	
Dropped Packet	The number of RADIUS authentication packets dropped by RADIUS because the server was flooded with more packets than it could handle.
Invalid Request	The number of invalid RADIUS requests made. **Possible Cause:** A device is sending incorrectly formed packets to RADIUS. Either there is a configuration error or the device does not conform to the RADIUS standard.
Failed Authentication	The number of failed authentication requests, where the failure is due to invalid user name or password. **Possible Cause:** If all transactions are failing authentication, the problem might be that the shared secret entered into RADIUS does not match the shared secret entered on the client device.
Failed on Checklist	The number of requests that were authenticated but failed to meet the checklist requirements.
Insufficient Resources	The number of rejects due to a server resource problem.

Authentication Statistic	Meaning
Rejects Sent	
Transactions Retried	The number of requests for which one or more duplicates was received.
Total Retry Packets	The number of duplicate packets received.

View RADIUS Server Statistics

The Security Console begins tracking the statistics after a RADIUS server starts. When an administrator restarts the RADIUS server, the Security Console clears the statistics and begins the tracking again. You can record statistics in RADIUS log files.

Procedure

1. In the Security Console, click **RADIUS** > **RADIUS Statistics** > **RADIUS Server Statistics**.
2. From the **Select a RADIUS Server** drop-down list, select the server for which you want to view statistics.
3. Select a transaction type:
   - **Authentication.** The number of accepts, rejects, silent discards, and challenges, and details about rejects and retries.
   - **Accounting.** The number of starts, stops, ons, offs, and interim requests, and details about failures and retries.

RADIUS Client Statistics

The Security Console displays statistics for the RSA RADIUS clients in RSA Authentication Manager. The statistics contain authentication and accounting data for RADIUS clients.

The Security Console begins tracking the statistics after an administrator starts the RADIUS server that is associated with the RADIUS client. When an administrator restarts the RADIUS server, the Security Console clears the statistics and begins the tracking again. You can record statistics in RADIUS log files.

When displaying RADIUS client statistics, the Security Console allows you to choose from the following four types:

- Accounting Request Diagnostics
- Account Request Types
- Authentication Request Diagnostics
- Summary

To view RADIUS client statistics, see the Security Console Help topic “Edit a Standard RADIUS User Attribute Definition.” You can view subsets of authentication and accounting statistics.

Authentication Statistics

Authentication confirms that valid users request network services. Authentication statistics include the following.

Statistic	Description
Authentication Request Diagnostics	
Retry packets	Number of duplicate messages sent by the client to its associated RADIUS server.
Invalid secrets	Number of messages with invalid accounting secrets sent by the client to its associated RADIUS server.
Challenges	Number of challenges sent by the client to its associated RADIUS server.
Invalid requests	Number of invalid RADIUS requests made by this RADIUS client. For example, the client is sending incorrectly formed packets to the RADIUS server because there is a configuration error or the device does not conform to the RADIUS standard.
Invalid types	Number of invalid accounting types sent by the client to its associated RADIUS server. For example, the client sends a RADIUS packet on the server accounting port that is not a RADIUS Accounting-Request packet.
Dropped Packets	Number of RADIUS accounting packets dropped by the RADIUS client because it received more packets than it could handle.

Accounting Statistics

Accounting tracks the network resources used by users. Accounting statistics include the following.

Statistic	Description
Accounting Request Diagnostics	
Retry packets	Number of duplicate packets sent by the client to its associated RADIUS server.
Invalid secrets	Number of failed authentication requests sent by this client, where the failure is due to using an invalid secret.
Invalid requests	Number of invalid RADIUS requests that this client sent to its associated server. For example, the client sends a request that does not parse properly.
Invalid types	Number of invalid authentication types sent by the client to its associated RADIUS server. For example, the client sends a request to the wrong port on the server.

Statistic	Description
Dropped packets	Number of RADIUS authentication packets sent by the client to its associated RADIUS server that the server drops for various reasons, such as a resource error.
Accounting Request Types	
Starts	Number of accounting start messages sent by the client to its associated RADIUS server.
Stops	Number of accounting stop messages sent by the client to its associated RADIUS server.
Interim requests	Number of interim accounting packets sent by the client to its associated RADIUS server.
Ons	Number of Accounting-On messages sent by the client to its associated RADIUS server when the RADIUS client restarts.
Offs	Number of Accounting-Off messages sent by the client to its associated RADIUS server when the RADIUS client shuts down.
Acks	Number of acknowledgement messages that the associated RADIUS server sent to this client.

Summary Statistics

Summary statistics include information about authentication and accounting requests, accepts and rejects.

Statistic	Description
Auth reqs	Total number of authentication requests sent by this client to its associated RADIUS server.
Accepts	Number of accept messages that the client received from its associated RADIUS server.
Rejects	Number of reject messages that the client received from its associated RADIUS server.
Acct Reqs	Total number of accounting requests sent by the client to its associated RADIUS server.
Starts	Number of transactions handled by this client in which a dial-in connection was started following a successful authentication.
Stops	Number of transactions handled by this client in which a dial-in connection was terminated by the RADIUS client.

View RADIUS Client Authentication and Accounting Statistics

You can view authentication and accounting statistics for the RSA RADIUS clients in RSA Authentication Manager.

Procedure

1. In the Security Console, click **RADIUS** > **RADIUS Statistics** > **RADIUS Client Statistics**.
2. From the **Select RADIUS Client** drop-down list, select the client for which you want to view statistics, and select the RADIUS server with which the client is associated.
3. Select a transaction type:
   - **Accounting Request Diagnostics.** The number of duplicate messages, messages with invalid secrets, malformed messages, messages with incorrect types, and dropped requests for each RADIUS client.
   - **Accounting Request Types.** The number of accounting start messages, accounting stop messages, interim messages, Accounting-On messages, Accounting-Off messages, and acknowledgement messages sent for each RADIUS client.
   - **Authentication Request Diagnostics.** The number of duplicate messages, challenges, messages containing invalid authentication information, bad authentication requests, bad types, and dropped requests for each RADIUS client.
   - **Summary.** The number of authentication requests, Access-Accept messages, Access-Reject messages, and the total number of accounting requests, starts, and stops for each RADIUS client.

Accounting Attributes and Administrator Actions to Record

When users authenticate, RADIUS clients send attributes for each user authentication attempt. RADIUS servers collect this information and can save as much or as little as needed for billing or monitoring purposes. The server writes the information to a comma-delimited file suitable for inclusion in a spreadsheet or other application.

RADIUS log files record administrator actions including authentications and any changes made using the Security Console or Operations Console.

The following table describes the files that establish settings for accounting and logging. For more information on modifying configuration files, see the *RSA Authentication Manager 8.1 RADIUS Reference Guide*.

File Name	Function
account.ini	Controls how RADIUS accounting attributes are logged.
radius.ini	Controls (among other things) the types of messages that RADIUS records in the server log file and the location of the log directory.

RADIUS Server Log Files

The server log file records RADIUS events, such as server startup or shutdown or user authentication or rejection, as a series of messages in an ASCII text file. Each line of the server log file identifies the date and time of the RADIUS event, followed by event details. You can open the current log file while RADIUS is running.

You can specify a maximum size for a server log file by entering a non-zero value for the LogfileMaxMBytes setting in the [Configuration] section of the **radius.ini** file.

- If a maximum file size is set, the server log filename identifies the date and time it was opened (YYYYMMDD_HHMM.log). When the current server log file approaches the specified number of megabytes (1024 x 1024 bytes), the current log file is closed and a new one is opened. The closed file will be slightly smaller than the specified maximum file size.
- If the maximum file size is set to 0 (or if the LogfileMaxMBytes setting is absent), the server log file size is ignored, and log filenames are date stamped to identify when they were opened (YYYYMMDD.log).

Note: The size of the log file is checked once per minute, and the log file cannot roll over more than once a minute. The log file may exceed the specified maximum file size temporarily (for less than a minute) after it passes the LogfileMaxMBytes threshold between size checks.

You can control the level of detail recorded in server log files by use of the LogLevel, LogAccept, LogReject, and TraceLevel settings.

The LogLevel setting determines the level of detail given in the server log file. The LogLevel can be the number 0, 1, or 2, where 0 is the least amount of information, 1 is intermediate, and 2 is the most verbose. The LogLevel setting is specified in the [Configuration] section of **radius.ini** and in the [Settings] sections of .aut files.

The LogAccept and LogReject flags allow you to turn on or off the logging of Access-Accept and Access-Reject messages in the server log file. These flags are set in the [Configuration] section of **radius.ini**. A value of 1 causes these messages to be logged, and a value of 0 causes the messages to be omitted. An Accept or Reject is logged only if LogAccept or LogReject, respectively, is enabled and the LogLevel is “verbose” enough for the message to be recorded.

The TraceLevel setting specifies whether to log packets when they are received and being processed, and what level of detail to recorded in the log.

Using the Accounting Log File

RADIUS accounting events are recorded in the accounting log file. Accounting events include START messages, indicating the beginning of a connection; STOP messages, indicating the termination of a connection, and INTERIM messages, indicating that a connection is ongoing.

Accounting log files use comma-delimited, ASCII format, and are intended for import into a spreadsheet or database program. Accounting log files are located in the RADIUS database directory by default. Accounting log files are named *yyyymmdd*.ACT, where *yyyy* is the 4-digit year, *mm* is the month, and *dd* is the day on which the log file was created.

The current log file can be opened while RADIUS is running.

Accounting Log File Format

The first six fields in every accounting log entry are provided by RADIUS for your convenience in reading and sorting the file:

- **Date.** The date when the event occurred
- **Time.** The time when the event occurred
- **RAS-Client.** The name or IP address of the RADIUS client sending the accounting record
- **Record-Type.** START, STOP, INTERIM, ON, or OFF, the standard RADIUS accounting packet types
- **Full-Name.** The fully distinguished name of the user, based on the authentication performed by the RADIUS server
- **Auth-Type.** A number that indicates the class of authentication performed:

  10—SecurID User

  11—SecurID Prefix

  12—SecurID Suffix

By default, the standard RADIUS attributes follow the Auth-Type identifier. For more information, see Standard RADIUS Accounting Attributes on page 321.

You can edit the **account.ini** initialization file to add, remove, or reorder the standard RADIUS or vendor-specific attributes that are logged. For more information, see the *RSA Authentication Manager 8.1 RADIUS Reference Guide*.

Accounting Log File Headings and Placeholders

The first line of the accounting log file is a file header that lists the attributes that have been enabled for logging in the order in which they are logged. The following example of a first line shows the required headings in bold italic, the standard RADIUS headings in bold, and the vendor-specific headings in regular text:

```
"Date","Time", "RAS-Client", "Record-Type", "Full-Name",
"Auth-Type", "User-Name", "NAS-Port", "Acct-Status-Type",
"Acct-Delay-Time", "Acct-Input-Octets", "Acct-Output-Octets",
"Acct-Session-Id", "Acct-Authentic","Acct-Session-Time",
"Acct-Input-Packets", "Acct-Output-Packets",
"Acct-Termination-Cause", "Acct-Multi-Session-Id",
"Acct-Link-Count","Acc-Err-Message",
"Nautica-Acct-SessionId","Nautica-Acct-Direction",
"Nautica-Acct-CauseProtocol","Nautica-Acct-CauseSource",
"Telebit-Accounting-Info","Last-Number-Dialed-Out",
"Last-Number-Dialed-In-DNIS","Last-Callers-Number-ANI",
"Channel","Event-Id","Event-Date-Time",
"Call-Start-Date-Time","Call-End-Date-Time",
"Default-DTE-Data-Rate","Initial-Rx-Link-Data-Rate",
"Final-Rx-Link-Data-Rate","Initial-Tx-Link-Data-Rate",
"Final-Tx-Link-Data-Rate","Sync-Async-Mode",
"Originate-Answer-Mode","Modulation-Type",
"Equalization-Type","Fallback-Enabled","Characters-Sent",
"Characters-Received","Blocks-Sent","Blocks-Received",
"Blocks-Resent","Retrains-Requested","Retrains-Granted",
"Line-Reversals","Number-Of-Characters-Lost",
"Number-of-Blers","Number-of-Link-Timeouts",
"Number-of-Fallbacks","Number-of-Upshifts",
"Number-of-Link-NAKs","Back-Channel-Data-Rate",
"Simplified-MNP-Levels","Simplified-V42bis-Usage", "PW_VPN_ID"
```

RSA RADIUS writes accounting events to the accounting log file. If an event recorded in the accounting log file does not have data for every attribute, a comma placeholder marks the empty entry so that all entries remain correctly aligned with their headings. For example, based on the “first line” of headings shown in the example above, the following is a valid accounting log entry, in which the value of the Acct-Status-Type attribute is 7:

```
"12/23/1997","12:11:55","RRAS","Accounting-On",
,,,,7,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,
```

Standard RADIUS Accounting Attributes

The following table lists the standard RADIUS accounting attributes defined in RFC 2866, “RADIUS Accounting.”

RADIUS Accounting Attributes	Description
User-Name	Name of the user as received by the client.
NAS-Port	Port number on the client device.
Acct-Status-Type	A number that indicates the beginning or ending of the user service: 1—Start 2—Stop 3—Interim-Acct 7—Accounting-On 8—Accounting-Off
Acct-Delay-Time	Number of seconds the client has been trying to send this record, which can be subtracted from the time of arrival on the server to find the approximate time of the event generating this request.
Acct-Input-Octets	Number of octets (bytes) received by the port over the connection. This is present only in STOP records.

RADIUS Accounting Attributes	Description
Acct-Output-Octets	Number of octets (bytes) sent by the port over the connection. This is present only in STOP records.
Acct-Session-Id	Identifier used to match START and STOP records in a log file.
Acct-Authentic	Indicates how the user was authenticated by RADIUS, the network access device (local) or another remote authentication protocol: 1—RADIUS 2—Local 3—Remote
Acct-Session-Time	Elapsed time of connection in seconds. This is present only in STOP records.
Acct-Input-Packets	Number of packets received by the port over the connection. This is present only in STOP records.
Acct-Output-Packets	Number of packets sent by the port over the connection. This is present only in STOP records.

RADIUS Accounting Attributes	Description
Acct-Termination-Cause	Number that indicates how the session was terminated. This is present only in STOP records: 1—User Request 2—Lost Carrier 3—Lost Service 4—Idle Timeout 5—Session Timeout 6—Admin Reset 7—Admin Reboot 8—Port Error 9—NAS Error 10—NAS Request 11—NAS Reboot 12—Port Unneeded 13—Port Preempted 14—Port Suspended 15—Service Unavailable 16—Callback 17—User Error 18—Host Request
Acct-Multi-Session-Id	Unique accounting identifier to make it easy to link together multiple related sessions in a log file.
Acct-Link-Count	The count of links that are known to have been in a given multilink session at the time the accounting record is generated.

14 Logging and Reporting

Log Messages Overview

RSA Authentication Manager generates log messages for all events. These messages are stored in log and database files according to the origin of the message. You can use these log files to monitor deployment activity and produce a record of events such as user logon requests or administrative operations.

Most log settings are instance-based, unless you choose to replicate logging configuration changes. The exception is log rotation settings, which are configured in the Operations Console on each instance.

The system does not log most successful read actions.

Log Types

Authentication Manager maintains the following types of logs:

- **Administrative Audit.** Log messages that record administrative actions, such as adding and editing users. This category does not include system level failures of administrative actions. Those messages are captured in the system log.
- **Runtime Audit**. Log messages that record any runtime activity, such as authentication and authorization of users.
- **System**. System level messages, such as "Server started" and "Connection Manager lost db connection." This category includes system level failures of administrative actions.

Logging Levels

For each type of log, you can use the Security Console to configure the level of detail written to the log files. For example, you might choose to record only fatal errors in the Administrative Audit log, while recording all messages in the System log. For instructions, see the Security Console Help topic "Log Configuration Parameters.

If you change the logging levels and want to return to the default values, select the values listed in the following table.

Log	Default Setting
Administrative Audit Log	Success
Runtime Audit Log	Success
System Log	Warning

Download Troubleshooting Files

You can use the Operations Console to download logs and reports to use for troubleshooting. Since these log files are not included in the product backup, you can archive them by periodically downloading them. You can also download troubleshooting files to access migration log files, including the migration report.

The log files are bundled into a .zip file for downloading. RSA Customer Support may ask to see the .zip file for troubleshooting. This .zip file contains sensitive information about hosts file, IP address, database schemas, and so on. The .zip file is password-protected. Use Winzip version 9 and above to view the contents of the .zip archive file.

Note: If you do not want to share a log containing sensitive information, delete it before making the .zip archive file available to RSA Customer Support. Do not share the .zip archive file with non-RSA personnel.

Before You Begin

You must be a Super Admin. However, if the RSA Runtime Server is down, you can access this page using Operations Console credentials.

Procedure

1. In the Operations Console, click **Administration > Download Troubleshooting Files**.
2. If prompted, enter your Super Admin credentials, and click **OK**.
3. Select the logs to download. Different options may display depending on whether the instance is a primary or replica. The following table shows all available options.

Option	Description
Product Information	Files that detail the configuration of Authentication Manager, such as information related to licensing, the version of Authentication Manager and the operating system, configured identity sources, and more.
Authentication Manager Log Files	Logs that detail deployment activity such as administrative operations and user actions. Log files include: Authentication Manager instance log Quick Setup log Operating system files Replication log files Migration log files

Option	Description
System Log Report (primary instance only)	A report that displays deployment activity, administrative operations, and the results of any activity in a Comma Separated Value (CSV) file.

Note: If the internal database or the RSA Runtime Server is down, only a subset of files from the Product Information option are downloaded., and the System Log Report option is unavailable on the primary instance.

4. In the **Create Password** field, enter a valid password.
5. Confirm the password.

   Carefully note the password. You need this password to view the contents of the .zip archive file. If you share the .zip archive file with RSA Customer Support, you will have to provide this password.
6. Click **Generate and Download Zip File**.

   Progress is displayed in the **Progress Monitor** page. This may take a few minutes to complete.
7. In the **Progress Monitor** page, click **Download Zip File**.

Real-time Monitoring

You can monitor your deployment in real time using any of the following tools.

Tool	Further Information
Activity Monitors	Real-time Monitoring Using Activity Monitors on page 328
Remote and Local Syslog	Configure Appliance Log Settings on page 338 Configure the Remote Syslog Host for Real Time Log Monitoring on page 351
Simple Network Management Protocol (SNMP)	SNMP Overview on page 345
Runtime Activity Monitor in the User Dashboard	Security Console Help topic “User Dashboard”

Real-time Monitoring Using Activity Monitors

You can use Activity Monitors to view RSA Authentication Manager activity, such as log entries, in real time. There are three Activity Monitors, each of which opens in a separate browser window and displays a different type of information.

Monitor	Information Displayed
Authentication Activity	• Which user is authenticating • Source of the authentication request • Server used for authentication
System Activity	• Time of an activity • Description of activity • Whether the activity succeeded • Server where the activity took place
Administration Activity	Changes such as when users are added or deleted.
Runtime Activity Monitor in the User Dashboard	• Log entries for real-time authentication activity over the past seven days for one user • Time of activity, result of activity, and description of activity

You can customize the information displayed. For example, you can use the Administration Activity Monitor to view the activity of a specific administrator, User ID, authentication agent, or security domain.

You can open multiple Activity Monitor windows at the same time. For example, you can simultaneously monitor a specific administrator, an entire user group, and an entire security domain.

You can pause the Activity Monitor and review specific log messages. When you resume monitoring, all log messages generated while the Activity Monitor was paused are added at the top of the Activity Monitor display.

If the number of new messages exceeds the number of messages selected for display, only the most recent are displayed. For example, if you configured the monitor to display 100 messages, but there are 150 new messages, only the 100 most recent are displayed.

You can also view a user's authentication activity through the User Dashboard page in the Security Console. For more information, see the Security Console Help topic "User Dashboard."

View Messages in the Activity Monitor

Use this procedure to view messages in the Activity Monitor to troubleshoot problems.

Procedure

1. In the Security Console, click **Reporting** > **Real-time Activity Monitors**, and select an available Activity Monitor.
2. Specify the criteria of the log messages that you want the Activity Monitor to display. Leave these fields blank to view all activity.
3. Click **Start Monitor**.
4. When a message displays that you want to view, click **Pause Monitor**.
5. Click the date and time of the message that you want to view.

Reports

Reports provide access to logged information, and current information about the users, administrators, and system activity in a deployment. This information is useful for troubleshooting, auditing security issues, and demonstrating compliance with various policies.

You create a report using one of the supplied templates. Each template allows you to choose the types of information being reported and the parameters to apply in order to refine that information. For example, you can use the All Users template to create a report that generates a list of all the users in your deployment by first and last name who are enabled for risk-based authentication.

After you have created and saved a report, an administrator can run the report manually at any time. For instructions, see the Security Console Help topic “Run a Report Job.” You can also schedule the report to run automatically on a given day and time. For instructions, see the Security Console Help topic “Schedule a Recurring Report Job.”

You can view the report output in the Security Console, or download the report as a CSV, XML, or HTML file.

Reports Permitted for Each Administrative Role

Administrative permissions determine which reports each administrator can run. Each predefined administrative role has default reporting permissions.The following table lists the default permissions for the predefined administrative roles, and the reports that each role has permission to run. You can modify a predefined role if you want it to have broader scope.

Note: Administrators who do not have view permissions for security domains have limited reporting capabilities. RSA recommends that you allow administrators to view security domains.

Administrator Role					
Report Name	**Help Desk Admin**	**User Admin**	**Agent Admin**	**Security Domain Admin**	**Super Admin**
Administrator Activity					X
Administrators of a Security Domain		X	X	X	X
Administrators with a Specified Role				X	X
Administrators with Fixed Passcode		X	X	X	X
Agents not updated by auto-registration more than a given number of days		X	X	X	X
Agents with Unassigned IP Address		X	X	X	X
All User Groups		X	X	X	X
All Users		X	X	X	X
Authentication Activity					X
Distributed Token Requests					X
Expired User Accounts		X	X	X	X
Imported Users and Tokens Reports		X	X	X	X
List all RADIUS clients				X	X
List all RSA Agent with assigned RADIUS client/RADIUS server		X	X	X	X
List all RSA Agents with assigned RADIUS profile		X	X	X	X
List all User Alias		X	X	X	X

Administrator Role					
Report Name	**Help Desk Admin**	**User Admin**	**Agent Admin**	**Security Domain Admin**	**Super Admin**
List all Users with assigned RADIUS profile		X	X	X	X
Object Lifecycle Activity (Non User/User Group)					X
Risk-Based Authentication (RBA) Activity					X
Risk-Based Authentication (RBA) Users		X	X	X	X
Software Token		X	X	X	X
System Log Report					X
Token Expiration Report		X	X	X	X
User and User Group Lifecycle Activity					X
User and User Groups Missing from Identity Source		X	X	X	X
Users Enabled for On-Demand Authentication		X	X	X	X
Users Enabled for On-Demand Authentication Who Have Never Logged In		X	X	X	X
Users never logged in with token		X	X	X	X
Users with days since last login using specific token		X	X	X	X
Users with Disabled Accounts		X	X	X	X
Users with Tokens		X	X	X	X
Users with tokens set to online emergency access tokencode		X	X	X	X

Scheduled Report Jobs

A scheduled report job creates a report according to a specified schedule. When creating a scheduled report job, you can configure these parameters.

Job Starts. The date to run the first instance of the recurring report job.

Frequency. The frequency of the recurring report:

- Daily or Weekly - You can run the report each day, or on a specific day or multiple days.
- Monthly **-** You can run the report every month, or on certain months. You can also specify the day on which the report is run.

Run Time. The time of day that the report is run.

Job Expires. The date when the recurring report job expires. You can choose a job that does not expire, or you can enter a specific date.

Input Parameters. Filter the report results. The available values vary depending on the report. For example, for a report on disabled user accounts, the report can show only disabled accounts belonging to users with a certain first name.

Custom Reports

You can create and run customized reports describing system events and objects.

For example, you might create a report that shows all user accounts that are disabled. You can design the report to include relevant information such as User ID, name, identity source, and security domain.

You can create a report that shows administrator activities. For example, you can report on activities for all administrators, or you can display detailed information on one administrator.

You can create custom reports using the predefined report templates provided with Authentication Manager. Each template includes predefined variables, column headings, and other report information. For a list of templates, see Reports Permitted for Each Administrative Role on page 330.

The template is the foundation for your custom report. The template offers a starting point for sets of data, including input parameters and output columns. You can decide which columns to show, apply data filters, and modify run options.

Add a Report

Add a report to generate information about your deployment. You select a report template for the type of report you want to add, and customize the template for the specific information you want the report to provide.

Procedure

1. In the Security Console, click **Reporting** > **Reports** > **Add New**.
2. On the Select Template page, select a template for the report.

   Each template contains different input parameters and output columns. The **Description** column provides a summary of each template.
3. Click **Next**.

4. From the **Security Domain** menu, select the security domain where you want the report to be managed.

   The security domain designates which administrators can manage the report.

5. In the **Report Name** field, enter a unique name for the report.

   Do not exceed 64 characters. The characters & % > < are not allowed.

6. Select one of the following options for **Run As**:

   - **The administrator running the report job**. The report data is limited to the scope of the administrator who runs the report.
   - **The report creator**. The report data is limited to the scope of the administrator who created the report. If the administrator running the report has a narrower scope than the report creator, the report will include data from the broader scope of the report creator.

   Only the administrator who created the report can change the **Run As** option.

7. Under Output Columns, move the items that you want to display in the report from the **Available** column to the **Show in Report** column.

8. Under Input Parameter Values, either enter values or leave the fields blank.

   If you leave the fields blank, administrators can set values when they run the report. If you enter values, the administrator must use these values when running the report. To include administrators with a specific role in a report, you must specify the role name. This name is case sensitive.

9. Click **Save**.

Next Steps

You can run the report manually, or schedule the report to run at specified times.

Completed Reports

In the Security Console, you can view and download completed reports, as well as a list of reports that are in progress or waiting in the report queue. On the Report Output page, the report jobs are grouped as Completed and In Progress. You can view the report jobs based on status, or use the search criteria to search for a specific report job.

You can view completed reports in the following ways:

- In a separate browser window, you can save the report after you view it.
- Download and save to a CSV file.
- Download and save to an XML file.
- Download and save to an HTML file.

For instructions, see the Security Console Help topic "View In Progress Report Jobs and Completed Reports."

Sample Reports

This section provides sample reports using the following report templates:

- All Users
- Users with Tokens
- Authentication Activity
- System Log

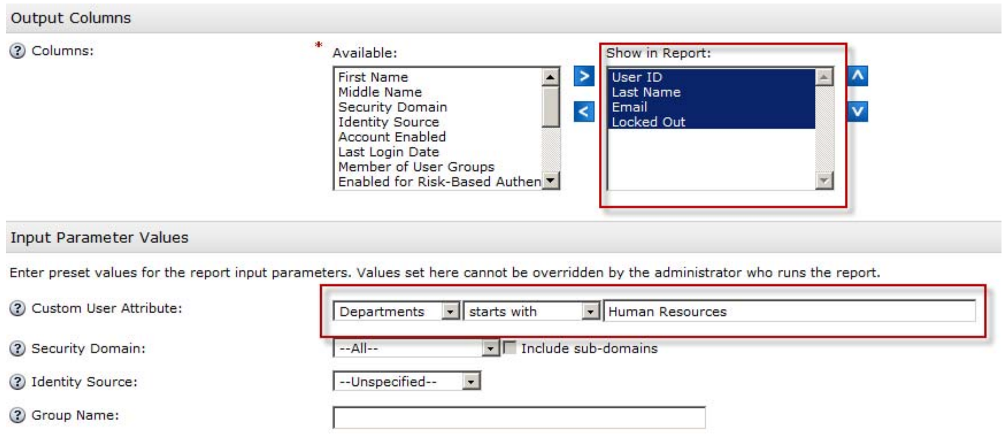
Sample All Users Report

The All Users report provides information about users in your deployment. You can filter results based on input values such as custom user attributes, security domain, or group.

For example, you can generate a report to list all users in a specific department, if the department is defined as a custom user attribute.

In this example, Departments is a custom user attribute with Human Resources, Finance and IT as pre-defined values.

Suppose you want to generate a report that lists all users in the Human Resources department along with their User ID, Last Name, Email, and Lockout Status. On the Add a New Report page, select Departments and Human Resources in the Custom User Attribute field. Enter the search string as Human Resources. Include the following columns under Show in Report:



Output Columns

Columns: * Available:

- First Name
- Middle Name
- Security Domain
- Identity Source
- Account Enabled
- Last Login Date
- Member of User Groups
- Enabled for Risk-Based Authen

Show in Report:

- User ID
- Last Name
- Email
- Locked Out

Input Parameter Values

Enter preset values for the report input parameters. Values set here cannot be overridden by the administrator who runs the report.

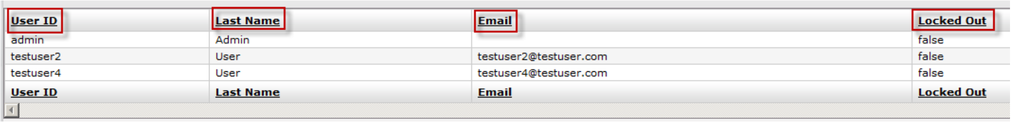
Custom User Attribute: Departments | starts with | Human Resources

Security Domain: --All-- ☐ Include sub-domains

Identity Source: --Unspecified--

Group Name:

The following figure shows the report output. The column headers highlighted in red are the same as those defined in the Add Report page.

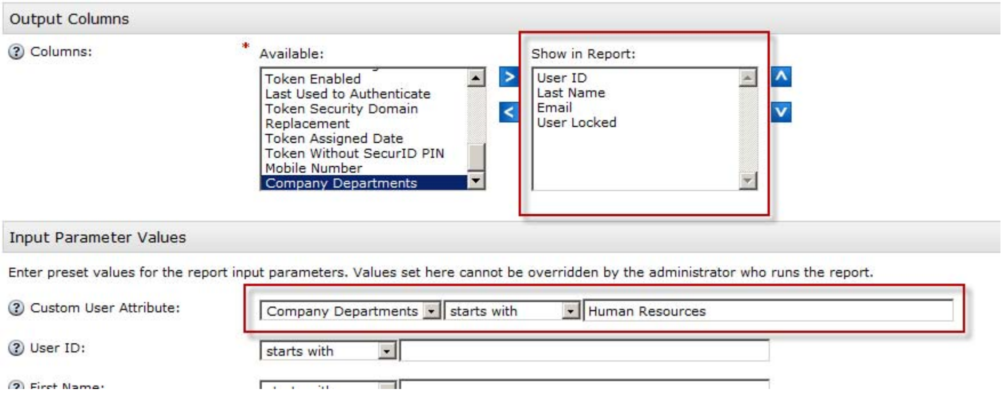


User ID	Last Name	Email	Locked Out
admin	Admin		false
testuser2	User	testuser2@testuser.com	false
testuser4	User	testuser4@testuser.com	false
User ID	Last Name	Email	Locked Out

Sample Users with Tokens Report

The Users with Tokens report provides a list of users who are assigned tokens.You can narrow the search using input parameter values such as customer user attributes.

For example, suppose you want to generate a report that lists the User ID, First Name, Last Name of users in the Human Resources department, and the lockout status of each account. Specify the output columns and input parameters as shown in the following figure.



Output Columns

Columns: * Available:

- Token Enabled
- Last Used to Authenticate
- Token Security Domain
- Replacement
- Token Assigned Date
- Token Without SecurID PIN
- Mobile Number
- Company Departments

Show in Report:

- User ID
- Last Name
- Email
- User Locked

Input Parameter Values

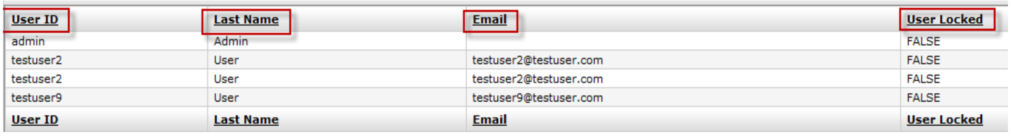
Enter preset values for the report input parameters. Values set here cannot be overridden by the administrator who runs the report.

Custom User Attribute: Company Departments | starts with | Human Resources

User ID: starts with

First Name:

The following figure shows the report output. The column headers highlighted in red are the same as those defined in the Add New Report page.



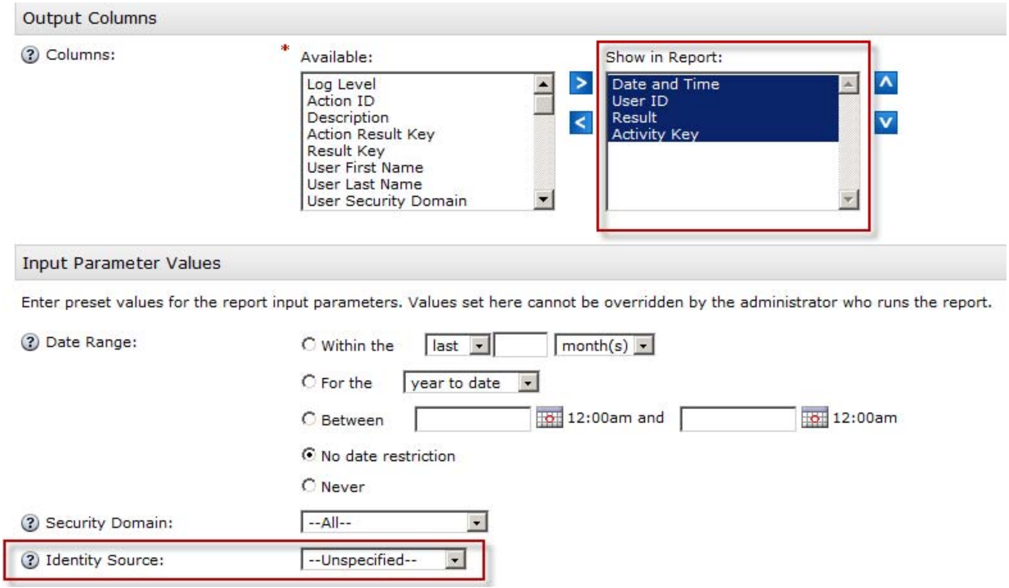
User ID	Last Name	Email	User Locked
admin	Admin		FALSE
testuser2	User	testuser2@testuser.com	FALSE
testuser2	User	testuser2@testuser.com	FALSE
testuser9	User	testuser9@testuser.com	FALSE
User ID	Last Name	Email	User Locked

Sample Authentication Activity Report

The Authentication Activity report helps you track the following types of authentication activities:

- Security and Operations Console login
- Users with tokens
- Agents on the server

For example, suppose you want to generate an authentication activity report that lists the user ID, date and time of authentication, result of the attempt, and type of activity that took place across multiple identity sources. Specify the output columns and input parameter values as shown in the following figure.



Output Columns

Columns: * Available:

Log Level
Action ID
Description
Action Result Key
Result Key
User First Name
User Last Name
User Security Domain

Show in Report:

Date and Time
User ID
Result
Activity Key

Input Parameter Values

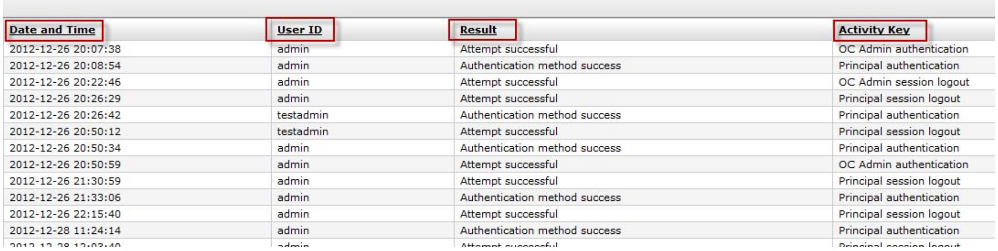
Enter preset values for the report input parameters. Values set here cannot be overridden by the administrator who runs the report.

Date Range:
○ Within the last [ ] month(s)
○ For the year to date
○ Between [ ] 12:00am and [ ] 12:00am
● No date restriction
○ Never

Security Domain: --All--

Identity Source: --Unspecified--

The following figure shows the report output. The column headers highlighted in red are same as those defined in the Add New Report page.

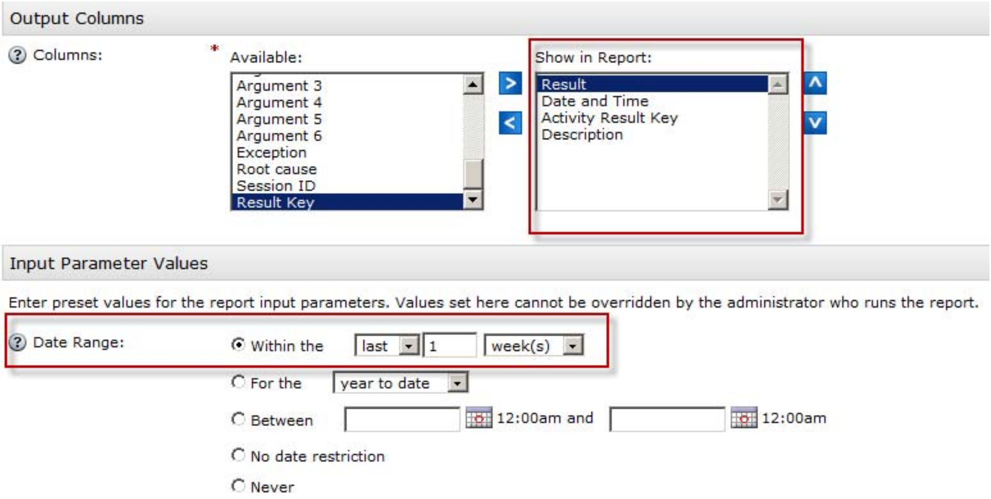


Date and Time	User ID	Result	Activity Key
2012-12-26 20:07:38	admin	Attempt successful	OC Admin authentication
2012-12-26 20:08:54	admin	Authentication method success	Principal authentication
2012-12-26 20:22:46	admin	Attempt successful	OC Admin session logout
2012-12-26 20:26:29	admin	Attempt successful	Principal session logout
2012-12-26 20:26:42	testadmin	Authentication method success	Principal authentication
2012-12-26 20:50:12	testadmin	Attempt successful	Principal session logout
2012-12-26 20:50:34	admin	Authentication method success	Principal authentication
2012-12-26 20:50:59	admin	Attempt successful	OC Admin authentication
2012-12-26 21:30:59	admin	Attempt successful	Principal session logout
2012-12-26 21:33:06	admin	Authentication method success	Principal authentication
2012-12-26 22:15:40	admin	Attempt successful	Principal session logout
2012-12-28 11:24:14	admin	Authentication method success	Principal authentication
2012-12-28 12:03:40	admin	Attempt successful	Principal session logout

Sample System Log Report

The System Log report lists log entries from the system log.You can narrow the search to a specific time period using input parameter values.

For example, suppose you want to generate a report that lists the Result, Activity Result Key, Date and Time and Description of events in the system log for the last one week. Specify the output columns and input parameters as shown in the following figure.



Output Columns

Columns: * Available: Argument 3, Argument 4, Argument 5, Argument 6, Exception, Root cause, Session ID, Result Key

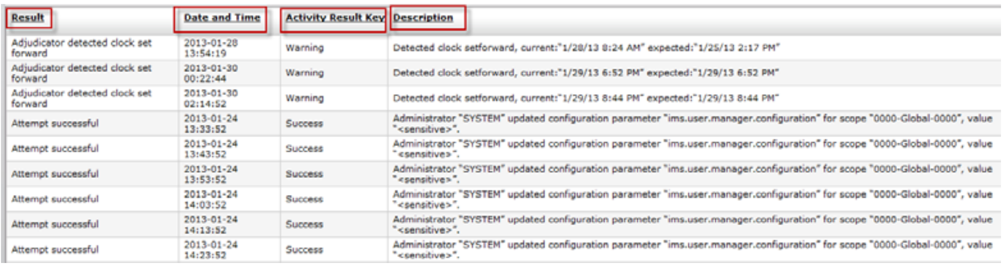
Show in Report: Result, Date and Time, Activity Result Key, Description

Input Parameter Values

Enter preset values for the report input parameters. Values set here cannot be overridden by the administrator who runs the report.

Date Range:
● Within the last 1 week(s)
○ For the year to date
○ Between 12:00am and 12:00am
○ No date restriction
○ Never

The following figure shows the report output. The column headers highlighted in red are same as those defined in the Add New Report page.



Result	Date and Time	Activity Result Key	Description
Adjudicator detected clock set forward	2013-01-28 13:54:19	Warning	Detected clock setforward, current:"1/28/13 8:24 AM" expected:"1/25/13 2:17 PM"
Adjudicator detected clock set forward	2013-01-30 00:22:44	Warning	Detected clock setforward, current:"1/29/13 6:52 PM" expected:"1/29/13 6:52 PM"
Adjudicator detected clock set forward	2013-01-30 02:14:52	Warning	Detected clock setforward, current:"1/29/13 8:44 PM" expected:"1/29/13 8:44 PM"
Attempt successful	2013-01-24 13:33:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 13:43:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 13:53:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 14:03:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 14:13:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".
Attempt successful	2013-01-24 14:23:52	Success	Administrator "SYSTEM" updated configuration parameter "ims.user.manager.configuration" for scope "0000-Global-0000", value "<sensitive>".

Log Rotation Policy for the Appliance Logs

The appliance log files contain operating system messages. To simplify log data management, the appliance uses a log rotation policy that creates multiple files for each appliance log. You can define this policy.

The appliance creates one initial file for each appliance log. After this file reaches its specified size or time limit (daily, weekly, or monthly), the appliance adds the date to the filename, and then starts a new file for new log messages. For example, the syslog file is initially named messages and becomes messages-20120630 when it is rotated on June 30, 2012. After the rotation, the system creates a new file named messages for the most recent log messages.

You can compress log files to reduce the amount of storage space they require. For example, if you choose to compress rotated log files with bzip2, the rotated file from the previous example would be named **messages-20120630.bz2**.

Shredding overwrites deleted appliance log files to help prevent the recovery of confidential information. For example, you can specify that the system overwrite deleted files seven times. Higher numbers are more secure, but lower numbers require fewer system resources.

After the appliance creates the maximum number of log files, it deletes the oldest rotated log files before rotating the current file. For example, if the maximum number of files is five, and five rotated **messages** files have been created, the appliance deletes the oldest file and then rotates the current **messages** file.

Configure Appliance Log Settings

Log rotation settings prevent the appliance operating system logs from growing indefinitely. You can configure how and when the appliance logs are rotated.

The appliance logs track items such as syslog entries, appliance SNMP messages, and Network Time Protocol (NTP) server updates. RSA Authentication Manager logs track product-specific activity, such as adding a replica instance or authenticating users.

The log settings for RSA Authentication Manager are configured in the Security Console. For more information, see the Security Console Help topic “Configure Logging.”

Procedure

1. In the Operations Console, click **Administration** > **Log Rotation Settings**.
2. In the **Log Rotation Options** field, do one of the following:
   - Select **Rotate when the maximum file size reached is** 4,096 **KB** to rotate log files by size. Enter the maximum file size.

- Select **Rotate** daily, weekly, or monthly to rotate the log files by date intervals.

After each log file reaches the specified size, or after the specified time frame, the appliance renames the rotated file with the month, day, and year. The appliance starts writing a new log file.

3. In the **Compression Options** field, you can select **Compress rotated log files** to reduce the amount of storage space required by the rotated log files.
4. In the **Shred Options** field, you can choose to overwrite deleted log files to make them more difficult to recover later.
5. In the **Maximum Number of Files Allowed** field, specify the maximum number of rotated files kept by the system.

   After the appliance creates the maximum number of rotated log files, it deletes the oldest rotated log files before rotating the current files. The maximum number of files does not include the active log files.
6. Click **Save**.

If you have not saved your changes, you can click **Reset** to reset the log rotation settings to be as they were before you began editing.

Working with Log Files

You can perform operations on log files.

- Log Archives
- Verify the Integrity of an Archived Log File
- Log Messages in Local Files
- Set the Maximum Number of Local Log Files
- Set the Maximum Size of Each Local Log file
- Mask Token Serial Numbers in Logs

Log Archives

By archiving log files, you can maintain a history of all deployment activity, such as logon attempts and Security Console administrative operations. You can examine archived log files to troubleshoot problems or to audit security issues.

You use the Security Console to archive log files in the following ways:

- Schedule a one-time log archive job. For instructions, see the Security Console Help topic "Archive Logs Using Archive Now."
- Schedule a recurring log archive job. Recurring archive jobs run automatically on specified days, weeks, or months. For instructions, see the Security Console Help topic "Archive Logs Using Schedule Log Archival."

You can perform the following operations to manage log archives:

- Purge and export online log data stored for more than a specified number of days
- Export online log data stored for more than a specified number of days
- Purge online log data stored for more than a specified number of days
- Not purge or export online log data

Verify the Integrity of an Archived Log File

Use the Verify Archive Log utility, verify-archive-log, to ensure that a log file has not been tampered with.

Before You Begin

The system must validate the log files to ensure that the sequence of log events are intact. To determine if a log file has been validated, look in the directory where the log file exists. A validated log file has a *.log file and a *.sig file with the same filename.

Procedure

1. Log on to the appliance.
2. Switch users to become the rsaadmin user:
   a. Type the following, and press ENTER:
      ```
      sudo su rsaadmin
      ```
   b. When prompted, type the operating system account password, and press ENTER.
3. Change directories to the Authentication Manager utilities directory. Type the following, and press ENTER:
   ```
   cd /opt/rsa/am/utils
   ```
4. Type the following and press ENTER:
   ```
   ./rsautil verify-archive-log -f log_filename
   ```
   where *log_filename* is the filename and extension of the log file that you want to verify.
5. When prompted enter the Operations Console administrator username and password.

After you enter the Operations Console administrator password, the utility returns the verification status of the log file. The status is “VERIFIED” if verification is successful, or “TAMPERED” if verification fails.

If the utility returns an error that it cannot verify the integrity of the file, confirm that the file has been validated by the system.

Log Messages in Local Files

You can collect log messages to maintain an audit trail of all logon requests and operations performed using the Security Console. You need to configure Authentication Manager to send log messages to a local file.

Local log files are kept in the following locations:

- Admin: **RSA_AM_HOME/server/logs/imsAdminAudit.log**
- Runtime: **RSA_AM_HOME/server/logs/imsRuntimeAudit.log**
- System: **RSA_AM_HOME/server/logs/imsSystem.log**

These locations cannot be changed.

Configure All Instances to Send Log Messages to a Local File

Perform this procedure to configure all instances in the deployment to send log messages to a local file.

Before You Begin

This procedure assumes knowledge of the Linux operating system. Do not attempt this procedure without the necessary knowledge.

Procedure

1. On the primary instance, log on to the appliance with the user name **rsaadmin** and the operating system password that was specified during Quick Setup.
2. Change directories to **RSA_AM_HOME/utils**. Type one of the following commands, and press ENTER:

   For the Admin log:

   ```
   ./rsautil store -a config_all
   ims.logging.audit.admin.datastore database,file
   ```

   For the Runtime log:

   ```
   ./rsautil store -a config_all
   ims.logging.audit.runtime.datastore database,file
   ```

   For the System log:

   ```
   ./rsautil store -a config_all
   ims.logging.system.datastore database,file
   ```

3. When prompted, type the Operations Console administrator password, and press ENTER.

Configure One Instance to Send Log Messages to a Local File

Perform this procedure to configure in one instance of the deployment to send log messages to a local file.

Before You Begin

This procedure assumes knowledge of the Linux operating system. Do not attempt this procedure without the necessary knowledge.

Procedure

1. On the primary instance, log on to the appliance with the user name **rsaadmin** and the operating system password that was specified during Quick Setup.
2. To obtain the fully qualified hostname, log on to the Security Console, and click **Setup** > **System Settings** > **Basic Settings** > **Logging.**
3. Change directories to **RSA_AM_HOME/utils**. Type one of the following commands, and press ENTER:

   For the Admin log:

   ```
   ./rsautil store -a update_config
   ims.logging.audit.admin.datastore database,file host_name
   ```

   where *host_name* is the fully qualified name of the primary instance or replica instance.

   For the Runtime log:

   ```
   ./rsautil store -a update_config
   ims.logging.audit.runtime.datastore database,file
   host_name
   ```

   where *host_name* is the fully qualified host name of the primary instance or replica instance.

   For the System log:

   ```
   ./rsautil store -a update_config
   ims.logging.system.datastore database,file host_name
   ```

   where *host_name* is the fully qualified name of the primary instance or replica instance.
4. When prompted, type the Operations Console administrator password, and press ENTER.

Set the Maximum Number of Local Log Files

You can configure how many local log files are saved. After the maximum is reached, the oldest files are automatically deleted as new log files are saved. You change the maximum backup file index to set this limit. The default is 100 files.

Before You Begin

The following procedure assumes knowledge of the Linux operating system. Do not attempt this procedure without the necessary knowledge.

Procedure

1. On the primary instance, log on to the appliance with the user name **rsaadmin** and the operating system password that was specified during Quick Setup.
2. To obtain the fully qualified hostname, log on to the Security Console, and click **Setup** > **System Settings** > **Basic Settings** > **Logging**.

3. Change directories to **RSA_AM_HOME/utils**. Type one of the following commands, and press ENTER:

   For the Admin log:

   ```
   ./rsautil store -a update_config
   ims.logging.audit.admin.file.max_backup_index n host_name
   ```

   where:

   - *n* is the maximum number of local log files
   - *host_name* is the name of the primary instance or replica instance

   For the Runtime log:

   ```
   ./rsautil store -a update_config
   ims.logging.audit.runtime.file.max_backup_index n
   host_name
   ```

   where:

   - *n* is the maximum number of local log files
   - *host_name* is the name of the primary instance or replica instance

   For the System log:

   ```
   ./rsautil store -a update_config
   ims.logging.system.file.max_backup_index n host_name
   ```

   where:

   - *n* is the maximum number of local log files
   - *host_name* is the name of the primary instance or replica instance

   If you want to change the setting for all instances, use the config_all option instead of update_config and omit the *host_name*. For example, to change the setting for System log to 5 log files for all instances, you type the following:

   ```
   ./rsautil store -a config_all
   ims.logging.system.file.rotation_size 5
   ```

Set the Maximum Size of Each Local Log file

By default, the maximum size of a local log file is 10 MB. You can increase or decrease this limit.

Before You Begin

This procedure assumes knowledge of the Linux operating system. Do not attempt this procedure without the necessary knowledge.

Procedure

1. On the primary instance, log on to the appliance with the user name **rsaadmin** and the operating system password that was specified during Quick Setup.
2. Change directories to **RSA_AM_HOME/utils**. Type one of the following commands, and press ENTER:

   For the Admin log:

   ```
   rsautil store -a update_config
   ```

```
ims.logging.audit.admin.file.rotation_size n host_name
```

where:

- *n* is the maximum size in MB of the local log files
- *host_name* is the fully qualified host name.

For the Runtime log:

```
./rsautil store -a update_config
ims.logging.audit.runtime.file.rotation_size n host_name
```

where:

- *n* is the maximum size in MB of the local log files
- *host_name* is the host name

For the System log:

```
./rsautil store -a update_config
ims.logging.system.file.rotation_size n host_name
```

where:

- *n* is the maximum size in MB of the local log files
- *host_name* is the host name

If you want to change the setting for all instances, use the config_all option instead of update_config and omit the *host_name*. For example, to change the setting for System log to 5 MB for all instances, you type the following:

```
./rsautil store -a config_all
ims.logging.system.file.rotation_size 5
```

Mask Token Serial Numbers in Logs

You can configure RSA Authentication Manager to include only part of the token serial number in log data that is sent to applications outside of the Authentication Manager instance. For example, you might do this when logging data to syslog, a local file, or a Network Management Server using Simple Network Management Protocol (SNMP).

You can configure Authentication Manager to include zero to twelve digits of the token serial number. The default value is twelve, which includes the entire token serial number.

Procedure

1. On the primary instance, log on to the Security Console.
2. Click **Setup** > **System Settings** > **Basic Settings** > **Logging**.
3. Under **Select Instance,** choose the primary instance and click **Next**.
4. In **Configure Settings**, under **Log Data Masking,** in the **Number of digits of the token serial number to display** box, enter the number of digits.
5. Click **Save**.

   The setting applies to all instances in your deployment.

Advanced Logging and Troubleshooting

This section describes advanced tasks for logging and troubleshooting.

- SNMP Overview
- Configure SNMP
- Log Files for Troubleshooting
- Trace Logs
- Configure the Remote Syslog Host for Real Time Log Monitoring
- Configure Critical System Event Notification
- Critical System Event Types

SNMP Overview

RSA Authentication Manager supports a third-party network management system (NMS) using Simple Network Management Protocol (SNMP). An NMS reveals how Authentication Manager is functioning in a production environment, making it easier to configure the deployment for optimal performance.

You can define the information that you want an NMS to provide by specifying GETS and traps. The NMS requests information using GETS and receives messages that are triggered by traps. The NMS obtains network information from the Management Information Base (MIB).

GETS and traps differ in two ways:

- A GET requests information, whereas a trap automatically sends information.
- A GET is composed of aggregate data, but a trap is an individual piece of data.

For example, assume that Authentication Manager is configured to send a notification each time a successful authentication occurs. If there are 100 successful authentications, 100 trap messages are sent. If you were to do a GET for successful authentications, you would receive one message showing a value of 100.

You can configure the NMS to receive Authentication Manager error, warning, or success notifications. Notifications can be intercepted and filtered based on the data sent in the trap message (message ID, for example).

You can also set traps to monitor disk usage, memory usage, and the CPU system load. You can select an interval at which to check the instance and send a notification to the NMS if too many resources are being used.

SNMP settings are instance-based. Changes that you make to one instance do not affect the other instances.

In Authentication Manager, SNMP obtains values only from the internal database, not from external identity sources. For example, suppose you have 2000 users in an external identity source but only 1000 users in the Authentication Manager internal database. If you have a GET for the total number of users, the value returned is 1000.

To view the Authentication Manager message IDs that an NMS can filter and their causes, see the *RSA Authentication Manager 8.1 Hardware Appliance SNMP Reference Guide* or the *RSA Authentication Manager 8.1 Virtual Appliance SNMP Reference Guide*.

Configure SNMP

You can configure Simple Network Management Protocol (SNMP) GETs and traps for RSA Authentication Manager.

You must log on to the primary instance to configure SNMP settings for each instance. The Security Console of the replica instance allows you to only view SNMP settings. You can apply the primary instance settings to all instances.

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console of the primary instance, click **Setup** > **System Settings**.
2. Under Advanced Settings, click **Network Monitoring (SNMP)**.
3. Select an instance.
4. Click **Next**
5. Under **Network Monitoring using SNMP v3**, select **On**. This enables the SNMP agent. If you do not select **On**, skip the rest of this procedure.

   You can change this setting to temporarily disable SNMP. Selecting **Off** does not clear the other SNMP settings on this page.
6. In the **Request Port** field, enter the port number the SNMP agent listens on for GET requests. The default port number is 161.

   Note: Do not enter port number 8002. The appliance uses port 8002 for an internal SNMP agent.
7. In the **Security Name** field, define a user name for the appliance SNMP agent. The SNMP agent uses this user name to authenticate GET requests and to send traps.
8. In the **Security Level** field, select a security level for SNMP communication:
   - **No Authentication** does not authenticate or encrypt SNMP communication. Go to step 11.
   - **Authentication, No Privacy** authenticates the sender of a GET or trap, but does not encrypt SNMP data communication.
   - **Authentication and Privacy** authenticates the sender of a GET or trap and encrypts SNMP data communication.

9. If you are using authentication, do the following:

   a. In the **Authentication Password** field, enter a password for authenticating the sender of a GET or trap. Some SNMP clients use the term "passphrase."

   b. From the **Authentication Protocol** list, select the protocol for authenticating the sender of a GET or trap.

10. If you are using encryption, do the following:

    a. In the **Privacy Password** field, enter the password for encrypting SNMP data communication. Some SNMP clients use the term "passphrase."

    b. In the **Privacy Protocol** field, select the algorithm for encrypting SNMP data communication.

11. Click **Download** to save the Management Information Base (MIB) .zip file.

    The .zip file contains MIB files for Authentication Manager and the appliance operating system. On a hardware appliance, the .zip file contains MIB files for the appliance hardware.

12. In the **Trap Settings** section, specify the type and severity of log events to be trapped.

Log Event Type	Description	Severity
Administrator Activity	Administrative actions in the deployment, both from the Security Console and through the API.	Severity levels are cumulative: • **Success** traps success, warning, and error events. • **Warning** traps both warning and error events. • **Error** only traps errors.
Authentication Activity	All events related to user authentication, such as User ID, authentication time, authenticating agent, and account lockout.	
System Log Report	Authentication Manager information related to the environment, internal processes, state or events such as activation, connections made or dropped, and refresh events.	

13. Under **Send Traps for Operating Systems** events, choose whether to monitor the appliance for resource utilization:

    For all of the OS Attributes, enter threshold values at which the system will send a trap. All attributes require values, but you can set a high threshold value for a specific attribute that you do not want to trap.

14. Under **Traps Receiver Settings**, add the IP address or hostname of the machines that receive SNMP trap notifications. You can keep or change the default port number of 162.

    You may enter multiple trap receivers, update existing trap receivers, or remove trap receivers from the list.

15. If you configured the primary instance and you want to apply these settings to the replica instance, click **Apply the above settings to the replica instance(s) upon save** to apply the same settings to the replica instance.

16. Click **Save**.

Next Step

SNMP configuration changes can require up to 10 minutes to take effect on a replica instance. To replicate the SNMP configuration changes sooner, you can log on to the Operations Console of the replica instance, and flush the cache. For more information, see Flush the Cache on page 369.

Log Files for Troubleshooting

The log messages that display in the Security Console are also written to files in your Authentication Manager directory. This directory also contains other logs for your appliance, which can be valuable for troubleshooting Authentication Manager.

You can access the log files after logging on to the appliance operating system via a secure shell (SSH) client. You can also download these logs using the Operations Console. For more information, see Download Troubleshooting Files on page 326.

Authentication Manager Logs

The following table lists the log files available.

Log Filename	Contents
imsAdminAudit.log	Messages written to the Administrative Audit log. These messages record any administrative actions, such as adding and editing users. **Note:** Only contains data not written to the Administrative Audit log stored in the internal database.
imsRuntimeAudit.log	Messages written to the Runtime Audit log. These messages record runtime activity, such as authentication and restricted agent access checks. **Note:** Only contains data not written to the Runtime Audit log stored in the internal database.

Log Filename	Contents
imsSystem.log	Messages written to the System log. These messages record system level activity, such as system startup and add replica. **Note:** Only contains data not written to the System log stored in the internal database.
imsTrace.log	Messages written to the Trace log. Use these messages to debug your system.
AdminServer.log	Messages about the administration server, which also hosts the Operations Console.
AdminServer_access.log	Messages about the HTTP traffic to and from the administration server, which also hosts the Operations Console.
biztier.log	Messages about the primary instance. Includes information about server startup, environment, which server components are running, networking services, and server errors.
biztier_access.log	Messages about the primary Authentication Manager HTTP interface.
console.log	Messages about the Console server. Includes information about server startup, environment, which server components are running, networking services, and server errors.
console_access.log	Messages about the HTTP traffic to and from the Console server. This includes the Security Console and, if no web tier is configured, the Self-Service Console.
rsa-console.log	Messages about the Security Console.
BiztierServerWrapper.log	Messages about service startup information for the biz tier Authentication Manager server.
AdminServerWrapper.log	Messages about service startup information for the administration server.
ConsoleServerWrapper.log	Messages about service startup information for the Console server.
imsOCAdminAudit.log	Messages about the information written to the Administrative Audit log in the Operations Console. These messages record administrative action such as adding and editing users.

Log Filename	Contents
imsOCRuntimeAudit.log	Messages about the information written to the Runtime Audit log in the Operations Console. These messages record runtime activity such as authentication and authorization of users.
imsOCSystem.log	Messages about the information written to the System log in the Operations Console. These record system level activity, such as “Authentication Manager Server started” and “Connection Manager lost db connection.”
imsOCTrace.log	Messages about the information written to the Trace log in the Operations Console. Use these messages for debugging.
ops-console.log	Messages about the Operations Console.
PlannedPromotion log	Messages about the promotion for maintenance feature.
radius-console.log	Messages about the RADIUS server.
radiusoc.log	Captures the RADIUS server related log messages in the Operations Console that you can use to debug your system.
radiusoc-access.log	Messages about the HTTP traffic to and from the RADIUS server.
radiusOCServerWrapper.log	Messages about the RADIUS server HTTP interface.
rsa-runtime.log	Messages about service startup information for the RADIUS server.
imsRadiusTrace	Messages written to the Trace log. Use these messages to debug the RADIUS server.

Internal Database Related Log Files

The following table lists the database related log file available at **/opt/rsa/am/rsapgdata/pg_log**.

Log Filename	Contents
postgresql-yyyy-mm-dd_064308.log **Note:** The log filename contains the current date in yyyy-mm-dd format.	An ongoing log of low-level database failures such as "out of disk space" or "disk hardware error." Also captures all Authentication Manager related activity that is written to the database.

Trace Logs

Trace logs help you debug problems in the application. You can configure the level of detail written to the Trace log files on the Log Configuration page in the Security Console. The following logging levels are available for the Trace log.

Fatal. Captures only log messages that imply the imminent crash of the application or the relevant subcomponents. Fatal messages require immediate attention.

Error. Captures all fatal messages, as well as error conditions that must be addressed, but may not necessarily cause the application to crash.

Warning. Captures all fatal and error messages, as well as log messages for minor problems while the application is running.

Information. Captures all fatal, error, and warning messages, as well as log messages for significant events in the normal life cycle of the application.

Verbose. Captures all fatal, error, warning, and information messages, as well as log messages associated with minor and frequently occurring events.

Important: Do not set the trace logging level to "verbose" for extended periods of time unless instructed to do so by RSA Customer Support. Trace logs may occupy large amounts of disk space and this can impact system performance.

Some routine system activity is only written to the System log when the logging level is set to "information" or "verbose." Use either of those logging levels if you want to see this information written to the internal database. Certain infrequent, important System log messages, such as system startup, are logged regardless of the log level.

Configure the Remote Syslog Host for Real Time Log Monitoring

You can configure a remote Syslog host to log messages from Authentication Manager. The remote host must be a valid UNIX or Linux machine with Syslog capabilities. The remote Syslog manages logs from multiple systems in the network, including RSA Authentication Manager. Configure the remote host to log messages from Authentication Manager. The location of files and IP tables used in configuration may vary depending on your remote host. For instructions, see your UNIX or Linux documentation.

After you have configured the remote Syslog host, you must identify the remote host as a destination for logs in the Security Console. For instructions, see the Security Console Help topic “Configure Logging.”

Configure Critical System Event Notification

RSA Authentication Manager can notify administrators by email if a critical system event occurs, for example, if a replica instance replication status changes to unsynchronized.

RSA recommends that you configure Authentication Manager to send critical system event notifications to key administrators. This enables administrators to resolve a condition before before it becomes a problem.

Before You Begin

- You must be a Super Admin.
- You must have SMTP mail service configured on the Security Console. For instructions, see the Security Console Help topic “Configure the SMTP Mail Service.”

Procedure

1. In the Security Console, click **Set Up** > **System Settings**.
2. Under **Basic Settings**, click **Critical System Event Notification**.
3. For **Enable Notifications**, select **On**.
4. For **Send Notifications for**, select one or more of the following items:
   - **Backup Events.** A new backup is needed because a backup was not made during the past 7 days, or a scheduled backup is unsuccessful.
   - **Identity Source Connection Events.** An identity source directory is unavailable.
   - **Low Disk Space Events.** Disk space is below 5 GB.
   - **RADIUS Configuration Events.** RADIUS configuration is unsuccessful during Quick Setup, attach, rebalance, hostname change, or IP address change.
   - **RADIUS Replication Events.** RADIUS replication is unsuccessful.
   - **Realm Certificate Removal Events.** Realm certificate removal during hostname change is unsuccessful.
   - **Replication Events.** The replication status has changed, for example, a replica instance replication status changes to out of sync.
5. For **Send Notifications to**, select one or both of the following items:
   - **Super Administrators**
   - **Individual Email Addresses**

     After you select **Individual Email Addresses**, enter the email address for each recipient in the related field. Separate each email address with a semicolon.
6. Click **Save**.

Critical System Event Types

Critical system event notifications alert administrators to undesirable conditions in the deployment. This allows administrators to resolve a condition before it becomes a problem. You use the Security Console to enable email notifications when the following events occur.

Event Type	Notification Cause
Backup Events	A new backup is needed because a backup was not made during the past 7 days, or a scheduled backup is unsuccessful. For more information on backups, see Deployment Backup on page 369.
Identity Source Connection Events	An identity source directory is unavailable. For more information about identity sources, see the Operations Console Help topic "Add an Identity Source."
Low Disk Space Events	Disk space is below 5 GB. For more information about disk space problems, see Chapter 15, System Maintenance and Disaster Recovery.
RADIUS Configuration Events	RADIUS configuration is unsuccessful during Quick Setup, attach, rebalance, hostname change, or IP address change. For information about RADIUS, see Chapter 13, Administering RSA RADIUS.
RADIUS Replication Events	RADIUS replication is unsuccessful. For information about RADIUS, see Chapter 13, Administering RSA RADIUS.
Realm Certificate Removal Events	Realm certificate removal during hostname change is unsuccessful.
Replication Events	The replication status has changed, for example, a replica instance replication status changes to out of sync. For information about replication status, see Check Replication Status on page 366.

15 System Maintenance and Disaster Recovery

Deployment Maintenance

RSA Authentication Manager 8.0 includes features that enable you to perform system maintenance and disaster recovery. Both the hardware appliance and the virtual appliance support these features, with the exception of VMware snapshots and the hardware appliance factory reset option.

This chapter discusses the following features:

Replica Instance Promotion. You can promote a replica instance for maintenance if the primary instance and all of the replica instances in the deployment are online and functioning normally. For more information, see Promotion for Maintenance on page 356.

If the primary instance is not functional, then you can promote a replica instance for disaster recovery. For more information, see Replica Instance Promotion for Disaster Recovery on page 380.

Performing Backups. Authentication Manager can back up your deployment with a manual, one-time backup, or a scheduled regular backup for the days and times that you specify. RSA recommends that you use the Operations Console to maintain a current backup of Authentication Manager to restore your deployment in a production environment. For instructions, see Create a Backup Using Back Up Now on page 370 and Create a Backup Using Schedule Backups on page 371.

VMware Snapshots. On the virtual appliance, you can take a VMware snapshot to capture the state of a primary or replica instance at a particular point in time. Snapshots do not replace the Authentication Manager backup feature. For more information, see Primary or Replica Instance Snapshots on page 373.

Factory Reset. If a malfunctioning primary or replica instance cannot be recovered, performing a factory reset restores the hardware appliance to a pre-configured state. You can run Quick Setup to configure the reset hardware appliance as a primary or replica instance. A factory reset is not supported on the virtual appliance. For more information, see Factory Reset on page 396.

Restoring the Web Tier. If the primary and replica instances are functioning normally, but the web tier stops responding, you can restore the web tier. For instructions, see Restore Web Tier on page 389.

Repairing Trusted Realm Relationships. If you change the hostname on a primary instance, then you must repair any previously existing trust relationships with other realms. For more information, see Trusted Relationship Repair on page 390.

Promotion for Maintenance

Promotion for maintenance promotes a replica instance to a primary instance while the original primary instance is online and functioning. An Operations Console administrator can initiate promotion for maintenance from the Operations Console of the replica instance that is to be promoted. After promotion, the original primary instance is demoted to a replica instance.

To perform a promotion for maintenance, the primary instance and all replica instances must be online and functioning. During this promotion process, authentication, administration, and self-service on the primary and replica instance involved in promotion will be unavailable, but authentication remains available on additional replicas in your deployment. After promotion, the original primary instance is demoted to a replica instance and is automatically synchronized with the new primary instance. All additional replica instances are automatically connected to the new primary instance.

If your deployment includes a web tier, you must restart services for each web tier after promotion. You must also initiate RADIUS data replication to synchronize the RADIUS server on each replica instance with the RADIUS server on the new primary instance. For more information, see RADIUS Data Replication on page 290.

Note: If your primary instance is not functioning, use the disaster recovery method option. For more information, see Deployment Problem Troubleshooting on page 364.

Things to Consider

Before you promote a replica instance to a primary instance, consider the following:

- If you have only one replica instance in your deployment, deploying another replica instance prior to promotion allows authentication to remain available during the promotion process.
- There are two ways to transfer and copy log data. If you choose to automatically transfer and copy log data, consider archiving logs to an NFS to conserve time and disk space during promotion. If you choose to manually transfer and copy log data, SSH must be enabled. In this case, you must copy and transfer the backup file from the original primary instance to a location supported by the backup and restore feature on the new primary instance. You must also import the logs using the Operations Console of the new primary instance.
- Back up the data in your current primary and save the backup file to a location outside of the appliance, such as a Network File System (NFS) or Windows shared folder.
- If you have enabled critical system notifications, you may receive notifications for replication events.
- Download completed reports using the Security Console on the primary instance. The report results will not be available on the new primary instance after promotion. For more information, see the Security Console Help topic, "View a Completed Report."

- If there are any completed Users/Tokens export jobs, download the export data files using the Security Console on the primary instance. The export data files will not be available on the new primary instance after promotion. For more information, see the Security Console Help topic, "Exporting and Importing Users and Tokens Between Deployments."
- Using the Security Console on the primary instance, disable any scheduled jobs such as reports, log archival, unresolvable users cleanup that may be scheduled to run during the period of planned promotion. If there are any scheduled jobs currently running, wait until they complete before beginning a promotion for maintenance. Any jobs that are in progress during the promotion are automatically cancelled. For more information, see the Security Console Help Topics, "Scheduled Report Jobs," "Archive Logs Using Schedule Log Archival," and "Schedule a Cleanup Job."

Promote a Replica Instance Using Promotion for Maintenance

For maintenance purposes, you can promote a replica instance to a primary instance while the original primary instance is online and functioning.

Before you Begin

- Ensure that the replica instance being promoted can reach the primary and all other replica instances. The primary and all other replica instances must be able to reach the replica instance being promoted. Ports 7072, 7002, 1812, and 1813 must be reachable from the replica. For more information, see "Securing Connections Between the Primary and Replica Instances" in Port Usage in the *RSA Authentication Manager 8.1 Setup and Configuration Guide.*
- Communicate to all other Operations Console administrators that you are going to promote the replica.
- In the Operations Console on the original primary instance, click **Maintenance** > **Backup and Restore** > **Progress Monitor** to ensure that backup or restore jobs are not running on the original primary instance. If a backup or restore job is running, wait for it to complete before promoting the replica instance.
- Disable any scheduled backup jobs on the original primary instance. To disable a scheduled backup job, go to **Maintenance > Backup and Restore** > **Schedule Backups**.
- If there are any completed reports, download report results using the Security Console of the original primary instance. The report results will not be available on the new primary instance after promotion. For more information, see the Security Console Help topic "View a Completed Report."
- If there are any completed Users/Tokens export jobs, download the export data files using the Security Console of the original primary instance. The export data files will not be available on the new primary instance after promotion. For more information, see the Security Console Help topic, "Exporting and Importing Users and Tokens Between Deployments."

- Using the Security Console on the primary instance, disable any scheduled jobs such as reports, log archival, unresolvable users cleanup that may be scheduled to run during the period of planned promotion. If there are any scheduled jobs currently running, wait until they complete before beginning a promotion for maintenance. Any jobs that are in progress during the promotion are automatically cancelled. For more information, see the Security Console Help Topics, "Scheduled Report Jobs," "Archive Logs Using Schedule Log Archival," and "Schedule a Cleanup Job."

Procedure

1. In the Operations Console, go to **Deployment Configuration** > **Replica Promotion** > **For Maintenance** > **Promote to Primary**.
2. Select the radio button for the log transfer option you want to use.
   a. If you choose the manual log transfer option, you must enter and confirm a log backup password. After promotion, you must manually transfer and add logs to the new primary instance using the same password.

   b. If you choose the automatic log transfer option, logs are copied and transferred during promotion. Consider archiving log data to conserve time during promotion. To archive now, in the Security Console, click **Administration** > **Archive Audit Logs** > **Archive Now.**
3. Verify the instance details and click **Run Pre-Promotion Check**.
4. After the pre-promotion checks are complete, review the status. Depending on the status, do one of the following:
   a. If the pre-promotion check completed successfully and you choose to promote this instance, select the **Yes, Promote this instance** checkbox and click **Start Promotion**.

      The Progress Monitor displays. You can only view the progress of the promotion operation on the replica instance that you are promoting.

   b. If one or more of the pre-promotion checks fail, do the following in this order:
      - Review the **Advanced Status View** to determine the errors that occurred.
      - After reviewing the **Advanced Status View**, click **Close** to exit the window.
      - On the Pre-Promotion Checks page, click the **Cancel** button.
      - Fix any issues that caused the failure and return to this procedure to retry the promotion.
5. After promotion completes, do one of the following:
   - If promotion completes successfully, click **Next** to view the mandatory next steps.
   - If promotion completes with warnings, review the warnings and click **Next** to view the mandatory next steps.
   - If promotion fails, complete the steps mentioned in the error message.

6. Review the **Summary** page and complete the **Required Next Steps**.
7. To save a copy of the required next steps, click **Download Next Steps**.

Next Steps

View the Next Steps for Promotion for Maintenance

View the Progress Monitor for Promotion for Maintenance

View the Next Steps for Promotion for Maintenance

After promotion completes, you can view the Next Steps on the new primary instance. You cannot view these Next Steps on any other instance besides the promoted instance.

The Next Steps differ based on your promotion process and deployment.

RSA recommends that you download the Next Steps for future reference. If you restart services on the instance, these steps are no longer available for viewing or downloading.

Before you Begin

Promote a Replica Instance Using Promotion for Maintenance on page 357

Procedure

1. In the Operations Console on the new primary instance, click **Deployment Configuration > Promotion > For Maintenance > Progress Monitor**, and then click **Next.**
2. Complete the next steps that display.

   RSA recommends that you click **Download Next Steps** to save a copy of the steps for future reference.

   The following next steps are always required after a promotion for maintenance:

Task	Instructions
Restore RADIUS replication on the new primary instance	In the Security Console on the new primary instance, go to **RADIUS > RADIUS Servers** and click **Initiate Replication** to synchronize the replica RADIUS servers with the new primary instance.
If your deployment includes web tiers, restart services for each web tier.	See Managing the Web-Tier Service on page 180.

Task	Instructions
Review the instance-specific system settings for the new primary instance and update any setting as needed. **Note:** The new primary instance does not inherit these settings from the original primary instance.	In the Security Console, go to **Setup** > **System Settings**, and review the settings that are configured by instance. For example, you may want to review and update the following instance-specific settings: • SNMP • SMTP • Caching • Logging • Session Handling
Verify your dynamic seed provisioning configuration	1. In the Security Console, go to **Setup** > **System Settings**, and under **Authentication Settings**, click **Tokens**. 2. Review the dynamic seed provisioning settings. If the fully qualified hostname of the demoted primary instance is used, update the setting with the fully qualified hostname of the new primary instance. For further instructions, see the Security Console Help topic "Configure Token Settings."

Depending on the outcome of the promotion, additional steps may also display.

If any of the following scenarios apply to the promotion that you completed, you must perform the corresponding task:

Scenario	Task	Action
You chose to manually copy and transfer log data after promotion	Restore logs	The log backup file is created on the original primary instance. Using methods like FTP, transfer the backup file to a supported backup location. For instructions on restoring from a backup, see Restore from Backup on page 375. **Note:** SSH must be enabled to access the local file system on the instance. To enable SSH, go to the Operations Console for the instance and click **Administration** > **Operating System Access.**

Scenario	Task	Action
One or more additional replica instances could not be updated to point to new primary instance	Enable communication with replica instances	For each additional replica instance that could not be updated, log on to the Operations Console of the replica instance, click **Administration > Network > Update Primary Hostname** and update the Primary Hostname field to that of the new primary instance.
The original primary instance cannot be demoted	Reset and configure the original primary instance as a replica	See Manually Reset the Original Primary Instance as a Replica Instance on page 363.
The original primary instance was demoted, but services could not be started successfully	Reuse the original primary instance as a replica instance	Start services on the original primary instance and synchronize with the new primary instance. For more information, see Start and Synchronize the Original Primary Instance on page 363.
Synchronization of the original primary instance does not succeed	Synchronize original primary instance	See Synchronize a Replica Instance on page 368.

3. Verify the following settings on the new primary instance.

Task	Reference
Make sure that the identity sources that you use are accessible from the new primary instance.	See the Operations Console Help topic "View the Identity Sources in Your Deployment."
Review the backup schedule for the new primary instance. Make sure that the new primary instance can communicate with the backup location.	See Create a Backup Using Schedule Backups on page 371.
Make sure that the link that is included in e-mail notifications for Self-Service user account changes contains the correct URL for the Self-Service Console.	See Configure E-mail Notifications for Self-Service User Account Changes on page 240.

View the Progress Monitor for Promotion for Maintenance

If you navigate away from the Promotion for Maintenance page or log out of the Operations Console during promotion, you can still view the progress monitor. The progress monitor displays on the replica instance that you are promoting.

After promotion, the progress monitor information is still available on the promoted instance. However, if you restart services on the new primary instance, you can no longer access this information.

Procedure

Do one of the following:

- To view the progress monitor during promotion, in the Operations Console on the replica instance being promoted to primary, go to **Deployment Configuration > Replica Promotion > For Maintenance > Progress Monitor**.
- To view the progress monitor after promotion, in the Operations Console on the new primary instance, **Deployment Configuration > Replica Promotion > For Maintenance > Progress Monitor**.

Restore Administration on the Primary Instance

If promotion for maintenance was unsuccessful, use the following procedure to restore administration on the original primary instance.

Before you Begin

Restart all services on the original primary instance. For instructions, see Reboot the Appliance on page 366.

Procedure

1. In the Operations Console on the original primary instance, click **Deployment Configuration > Instances > Status Report**.
2. Select the replica instance that did not promote from the list and click **Delete**.
3. Do one of the following:
   - If the replica instance is deployed on a hardware appliance, you must complete a factory reset. For more information, see Factory Reset on page 396.
   - If the replica instance is deployed on a virtual appliance, you must delete the replica appliance and deploy a new replica instance on a virtual appliance. For more information, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide.*
4. Run Quick Setup to configure the instance as a replica. For more information, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

Manually Reset the Original Primary Instance as a Replica Instance

If you successfully promoted a replica instance to a primary instance for maintenance purposes, but you were unable to demote the original primary instance to a replica instance, complete the following procedure to manually configure the original primary instance as a replica instance.

Procedure

1. Do one of the following:
   - If the original primary instance is deployed on a hardware appliance, you must complete a factory reset. For more information, see Factory Reset on page 396.
   - If the original primary instance is deployed on a virtual appliance, you must delete the old primary instance using the vSphere client. For more information, see the vSphere documentation. Deploy a new virtual machine with the RSA Authentication Manager image.
2. Run Quick Setup to configure the instance as a replica. For more information, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

Start and Synchronize the Original Primary Instance

If services did not start and synchronization did not complete on your original primary after promotion for maintenance, you must start the RSA Runtime Server (biztier) on the original primary instance and synchronize this instance with the new primary instance. If the biztier service cannot be started, reset and configure the appliance as a replica instance.

Procedure

1. Log on to the original primary instance using SSH with the User ID **rsaadmin** and the current operating system password. For instructions, see Log On to the Appliance Operating System with SSH on page 404.
2. Verify that the RSA Runtime Server (biztier) service is running. Do the following.
   a. On the original primary instance, change the directory. Type:
      ```
      cd /opt/rsa/am/server
      ```
      and press ENTER.
   b. Type the following command and press enter.
      ```
      ./rsaserv status biztier
      ```
3. If the biztier is not running, try to restart the service by typing the following command.
   ```
   ./rsaserv start biztier nodep
   ```

4. If the RSA Runtime Server (biztier) service does not start, reset the original primary instance and configure it as a replica instance. For more information, see Manually Reset the Original Primary Instance as a Replica Instance on page 363.
5. If you can start the RSA Runtime Server, synchronize the original primary instance using Operations Console of the new primary instance. In the Operations Console, select **Deployment Configuration > Instances > Status Report** and click **Sync** to synchronize the original primary instance with the new primary instance.

Deployment Problem Troubleshooting

When a deployment is not working properly, it exhibits symptoms that help you troubleshoot what is wrong. Once you determine the problem, you can choose the appropriate solution to restore the deployment.

Symptoms of Missing Data on the Primary or Replica Instance

When RSA Authentication Manager data is accidentally deleted, the following events occur:

- Some users can no longer authenticate because their records are missing.
- Policy settings no longer function as expected.
- Restricted agents no longer function as expected.
- Trusted realm authentication no longer functions as expected.

When the deployment shows symptoms of missing data, you can fix the problem by restoring data from a backup. For more information, see Primary Instance Data Restoration on page 373.

Symptoms of an Unresponsive Primary Instance

When the primary instance stops responding, the following events occur:

- Any replica instances continue to process authentication requests, but overall authentication requests take more time than usual.
- You cannot administer the deployment.
- Users in an LDAP directory who have moved to a different Distinguished Name (DN) or who have never authenticated or been edited in Authentication Manager cannot authenticate or be edited.
- If the deployment includes a replica instance, risk-based authentication (RBA) continues if the deployment includes a load balancer. If not, RBA is unavailable until you promote the replica instance.
- If the deployment does not have a replica instance, authentication stops.
- A Help Desk solution does not work.
- Users who are locked out cannot be unlocked.
- The database on the primary instance is unavailable.

- The Self-Service Console is unavailable.
- The primary instance is not generating log files.

When the primary instance is unresponsive, you can fix the problem by restoring the primary instance. For more information, see Primary Instance Restoration on page 377.

Symptoms of an Unresponsive Replica Instance

When the replica instance stops responding, the following events occur:

- The primary instance and any other replica instances continue to process authentication requests, but authentication takes more time than usual.
- All database updates that occurred on the primary and were not yet propagated to the replica are queued in the primary instance database server until the disk is full or the replica is removed or recovered. Depending on the number of transactions queued in the primary instance, the system may mark the replica **Out of Sync** to prevent running out of disk space.
- The replica instance is not generating log files.

When the replica instance is unresponsive, you can fix the problem by replacing the replica instance. For more information, see Replacing a Replica Instance on page 387.

Symptoms of an Unresponsive Web Tier

When a web tier stops responding, the following events occur:

- The Self-Service Console is unavailable if the web tier is connected to the primary instance.
- In a non-replicated deployment, risk-based authentication (RBA) stops.

When the web tier is unresponsive, you can fix the problem by removing the current web tier and adding a new web tier. For more information, see Restore Web Tier on page 389.

Symptoms of Replication Problems

When data replication between the primary instance and the replica instance stops working, an instance can stop authenticating users because the allotted disk space is full. If critical event notification messages are enabled, you receive a message when replication stops working.

You can fix the problem by synchronizing the replica instance with the primary instance. For more information, see Synchronize a Replica Instance on page 368.

Deployment Problem Solutions

Deployment problems can often be solved by performing one or more of the following tasks:

- Reboot the Appliance
- Check Replication Status
- Synchronize a Replica Instance
- Flush the Cache

Reboot the Appliance

You may need to reboot the appliance as part of a software update.

The reboot process can take approximately 10 minutes. When complete, you are redirected to the Operations Console logon page.

Before You Begin

You must be an Operations Console administrator.

Procedure

1. On the appliance instance that you want to reboot, launch and log on to the Operations Console.
2. Click **Maintenance** > **Reboot Appliance**.
3. On the Reboot Appliance Confirmation page, select **Yes, reboot the appliance**, and click **Reboot**.
4. On the Reboot Appliance Progress page, wait until the reboot process is complete.
5. When the Operations Console logon page displays, log on to the Operations Console.

Check Replication Status

You can view the Replication Status Report for each replica instance in the deployment and if necessary, delete or synchronize a replica instance.

The deployment must contain at least one replica instance to display any replication status data.

On a primary instance, the Replication Status Report displays the following information:

- **Disk Space Available.** The free disk space available on the primary instance. Replication stops when the free disk space is insufficient.
- **Minimum Disk Space for Replication.** The amount of free disk space on the primary instance that is required for replication.

- **Replication Status.** The replication status between the primary instance and each replica instance in the deployment.

  On a replica instance, the Replication Status report displays the replication status between that replica instance and the primary instance. For more information about each status, see Replication Status on page 367.

If you shut down a replica instance, you must wait approximately three minutes before restarting to see the replication status. If you restart immediately and the process takes less than three minutes, you might not see any messages in the System Activity Monitor. However, you can run a report to see the events.

If a replication error occurs, you can download log files to assist with troubleshooting. For more information, see Download Troubleshooting Files on page 326.

Procedure

On the primary instance Operations Console, click **Deployment Configuration** > **Instances** > **Status Report**.

Replication Status

The Replication Status Report displays the replication status for each replica instance in the deployment.

The following table describes each possible replication status. If you enable critical system notifications for replication status, you receive an e-mail notification when the replication status changes. The status term used for each critical notification message is provided in the description for each status.

Status	Description
Attachment in Progress (only on the primary instance)	The replica instance is currently attaching to the primary instance. Critical notification: ATTACHING.
Attachment Unsuccessful	The replica instance did not attach successfully. Critical notification: FAILED.
Instance Offline (only on the primary instance)	The replica instance has stopped updating its status and might be shut down or disconnected from the network. Critical notification: OFFLINE.
Internal Replication Error	An error has occurred. Critical notification: UNHEALTHY.
Normal	Replication is occurring successfully. Critical notification: HEALTHY.

Status	Description
Out of Sync	The replica instance is not synchronized with the primary instance and must be manually synchronized. Critical notification: OUT_OF_SYNC.
Synchronization in Progress	The replica instance is in the process of synchronizing with the primary instance. Critical notification: SYNCHRONIZING.

Synchronize a Replica Instance

The primary instance data is replicated frequently on each replica instance in the deployment. You can view the replication status of each replica instance in the Operations Console Replication Status Report page. When a replica instance shows an **Out of Sync** status, you must manually synchronize this replica instance. The synchronization process brings the replica instance data back into sync with the primary instance data. When you manually synchronize a replica instance with the primary instance, the replica instance can contain data that is waiting to be sent to the primary instance. This pending data is lost during the synchronization process.

Perform the following procedure to synchronize an out-of-sync replica instance with the primary instance.

Before You Begin

You must be an Operations Console administrator.

Procedure

1. On the primary instance Operations Console, click **Deployment Configuration** > **Instances** > **Status Report**.
2. For a replica instance with an **Out of Sync** status, click **Sync**.

   Note: You can synchronize only one replica instance at a time.

   The synchronize progress displays.

   If the synchronization process does not finish after 30 minutes, or if the synchronize progress displays an error, you can troubleshoot the problem by downloading the troubleshooting files on the replica instance. For instructions, see Download Troubleshooting Files on page 326.
3. After the synchronization tasks are completed, click **Done**.

Flush the Cache

Flush the cache to remove old information from memory. When you flush the cache, each selected object is refreshed from the database the next time it is accessed.

Cache contents are refreshed every 10 minutes. Depending on cache settings, database replicated changes to cached data may take up to 10 minutes to display on all instances after a change occurs on the primary. If you do not want to wait for the automatic 10-minute refresh, you can flush the cache on each individual instance.

Before You Begin

You must be an Operations Console administrator and a Super Admin.

Procedure

1. In the Operations Console, on the machine where you want to flush the cache, click **Maintenance** > **Flush Cache**.
2. If prompted, enter your Super Admin User ID and password, and click **OK**.
3. Under Flush Cache, do one of the following:
    - Select **Flush all cache objects** to flush all the caches, and click **Flush**.
    - Select **Flush specific cache objects**, select the specific caches that you want to flush, and click **Flush**.

Deployment Backup

You use the Operations Console to create a backup of the deployment data. This backup can be used to repair a deployment in the following ways:

- Restore data that is accidentally deleted
- Restore a malfunctioning primary instance

You can back up deployment data using one of the following methods:

- **Back Up Now.** A manual, one-time backup of the deployment. For instructions, see Create a Backup Using Back Up Now on page 370.
- **Schedule Backups.** Regular backups of the deployment according to a schedule that you specify. For instructions, see Create a Backup Using Schedule Backups on page 371.

RSA recommends that you maintain a current backup. If a successful backup has not been created during the past seven days and Critical System Event notifications are configured, the deployment sends a Critical System Notification.

Authentication continues while you create a backup. However, backup operations can slow the authentication process. RSA recommends that you back up the deployment data when authentication traffic is low and no batch jobs are running.

The deployment encrypts backups because backups contain sensitive information. During the backup process, you must specify a password that is used for encryption. During the restore process, you provide this password so that the backup can be decrypted and checked for integrity.

The size of the internal database determines the time required to create a backup. If the internal database is large, the process can take a long time.

You can save the backup on the appliance or at a remote location. RSA recommends saving a current backup in a remote location so that you can restore the deployment to recover from a disaster.

Backup File Contents

The backup file (.RSAbackup) contains the following data:

- **Internal database.** Includes configuration, policy, users, and groups.
- **Authentication Manager files.** Data and configuration files, such as update logs, bootloader settings, keys, and passwords used to access internal services, such as the internal database.
- **RADIUS.** All data and configuration files necessary to restore the RADIUS primary, including any imported trusted root certificates for Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) clients. All RADIUS data is included in the backup. You cannot back up or restore RADIUS data separately.
- **Internal database log file data.** Administrative Audit Log, Runtime Audit Log, and System Log.
- **Console SSL certificates.** The certificates that secure communication between a browser and the Operations, Security, and Self-Service Console.

The backup does not contain any files used to deploy the appliance. The backup only contains data that is added or changed after the appliance is deployed.

The backup does not contain any files that were generated by an export of users and tokens to another deployment. When the export is complete, download the file locally and delete the export job.

Create a Backup Using Back Up Now

Back Up Now creates a manual, one-time backup of a deployment.

Use Back Up Now before you perform significant maintenance tasks so that you can restore the deployment if necessary. For example, you should use Back Up Now at the following times:

- Immediately after deploying the primary instance
- After completing migration
- Before and immediately after applying an update
- After changing the arrangement of the deployment, for example, adding or deleting a replica instance, or promoting a replica instance for maintenance.

Procedure

1. In the Operations Console of the primary instance, click **Maintenance** > **Backup and Restore** > **Back Up Now**.
2. In the **Backup Name** field, accept the default name, or replace it with a backup name of your own.

   The default name consists of a timestamp and this extension: .RSAbackup. The timestamp uses the following format: YYYYMMDDHHMM.

   In the default name 201208251230.RSAbackup, for example, 2012 is the year, 08 is the month, 25 is the day, 12 is the hour, and 30 is the minute when the backup was created.

   If you replace the default filename, your name must use this extension: .RSAbackup. This extension is case sensitive.
3. In the **Backup Password** field, enter a valid password, and enter the same password in the **Confirm Backup Password** field.

   Note carefully the backup password you specify. You need this password to restore the deployment.
4. Under **Backup Location**, do one of the following:
   - Select **Local Authentication Manager Server**. The backup is saved on the appliance in the directory **/opt/rsa/am/backup**.
   - Select **Windows Shared Folder**.
     - In the **Windows Shared Folder** field, enter the path to an existing Windows shared folder, for example, **\\primary.company.net\backup_path**.
     - If the shared folder requires a user name, enter the user name in the **Folder User Name** field, for example, **Domain1\User1**.
     - If the shared folder requires a password, enter the password in the **Folder Password** field, for example, password1.
   - Select **NFS (Network File System) Shared Folder**. In the **NFS Shared Folder** field, enter the path to an NFS server and file directory, for example, **fileserver.company.net:/backup_path**.
5. Click **Backup**.

   The Progress Monitor page displays the backup progress.
6. Click **Done** when the backup process completes.

Create a Backup Using Schedule Backups

Schedule Backups creates regular backups of the deployment data according to the days and times that you specify. Use Schedule Backups to ensure that you always have a current backup. This makes it possible to restore a deployment with a minimal loss of data.

Authentication takes place during the backup process. However, backup operations slow general system performance. RSA recommends that you schedule the backups to take place during off-peak periods.

If you promote a replica instance to a primary instance, you must configure Schedule Backups on the new primary instance.

The deployment also sends a Critical System Notification if a scheduled backup is not successful.

Procedure

1. In the Operations Console of the primary instance, click **Maintenance** > **Backup and Restore** > **Schedule Backups**.
2. Under **Schedule Backup Status**, select **On**.
3. Under **Backup Configuration**, do the following:
   a. In the **Backup Password** field, enter a valid password. In the **Confirm Backup Password** field, enter the same password.

      Carefully note the backup password you specify. You need this password to restore the deployment.

   b. For **Maximum Number of Archived Backups**, accept the default of 4, or select a new number from the drop-down list.

      RSA recommends that you select a minimum of 4 backups. When the total number of scheduled backups reaches the maximum number, the next scheduled backup will delete the oldest scheduled backup.
4. Under **Backup Location**, do one of the following:
   - Select **Local Authentication Manager Server**. The backup is stored on the appliance in the directory **/opt/rsa/am/backup**.
   - Select **Windows Shared Folder**.
     - In the **Windows Shared Folder** field, enter the path to an existing Windows shared folder, for example, **\\primary.company.net\backup_path**.
     - If the shared folder requires a user name, enter the user name in the **Folder User Name** field, for example, **Domain1\User1**.
     - If the shared folder requires a password, enter the password in the **Folder Password** field, for example, password1.
   - Select **NFS (Network File System) Shared Folder**. In the **NFS Shared Folder** field, enter the path to an NFS server and file directory, for example, **fileserver.company.net:/backup_path**.
5. Under **Schedule**, accept the default settings, or specify a different backup schedule.

   For example, you can create backups on every Monday and Wednesday at 2:00 A.M.
6. Click **Save**.

Primary or Replica Instance Snapshots

You can take a VMware snapshot of a virtual appliance to capture the state of an RSA Authentication Manager primary or replica instance at a particular point in time. Snapshots, however, do not replace the Operations Console backup feature. Snapshots are very useful in a test environment because they allow you to revert quickly any changes you make to the deployment. RSA recommends that you use the Operations Console to maintain a current backup of Authentication Manager in order to restore your deployment in a production environment.

When you take a snapshot of an Authentication Manager instance, you must specify the following settings:

- Do not save the virtual machine's memory.
- Choose to quiesce the guest file system. This option pauses running processes on the Authentication Manager instance.

For additional instructions, see the VMware vSphere Client documentation.

Additional tasks are required to revert an Authentication Manager instance to a snapshot. For more information, see Reverting the Primary Instance to a Snapshot on page 385 and Reverting a Replica Instance to a Snapshot on page 388.

Primary Instance Data Restoration

If the primary instance data is accidentally deleted, but the primary instance is functioning properly, you can use the Operations Console to restore the deleted data using Restore from Backup.

Important: Restoring deleted data does not restore a malfunctioning primary instance, and can cause additional problems. To restore a malfunctioning primary instance, see Primary Instance Restoration on page 377.

When you use Restore from Backup, the following activities take place:

- The RSA Authentication Manager services stop so that no other processes can connect to the database. No administration or authentication operations can be performed on the primary instance during the restore operation.
- All backup data that is saved in a remote location is copied to the primary instance.
- The backup data overwrites all the existing data.
- Some protected data, such as system passwords and database passwords, is restored.

The Restore from Backup operation does not restore data for changes that were made after the backup was created. Those changes are lost. For this reason, users must provide the credentials they used before the backup was created. Similarly, a risk-based authentication user might be challenged to confirm identity because the behavioral and device data collected after the backup was created are unavailable. All of the console certificates imported from a third-party certificate authority (CA) that are in the backup are restored, but none of these imported console certificates are active. The restore process does not change the active certificate on the deployment. The active certificate on the deployment remains active when the restore process finishes.

After you restore the deployment data from a backup, you can use the Operations Console to activate any of the restored certificates. For example, if you had replaced the default certificate on the old deployment with a certificate signed by a third-party certificate authority (CA), this certificate is restored but not active. You can use the Operations Console to activate this certificate on the restored deployment. For instructions, see Replacing the Console Certificate on page 165.

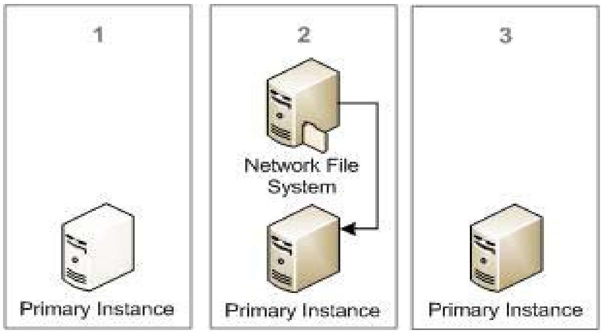
Restoring Primary Instance Data on a Standalone Deployment

Data that has been accidentally deleted on a standalone deployment can be restored by completing the following tasks.

Procedure

1. Troubleshoot the primary instance to determine that data is missing but the primary instance is still functioning properly.
2. Perform the Restore from Backup procedure. For instructions, see Restore from Backup on page 375.

The following figure shows the process.



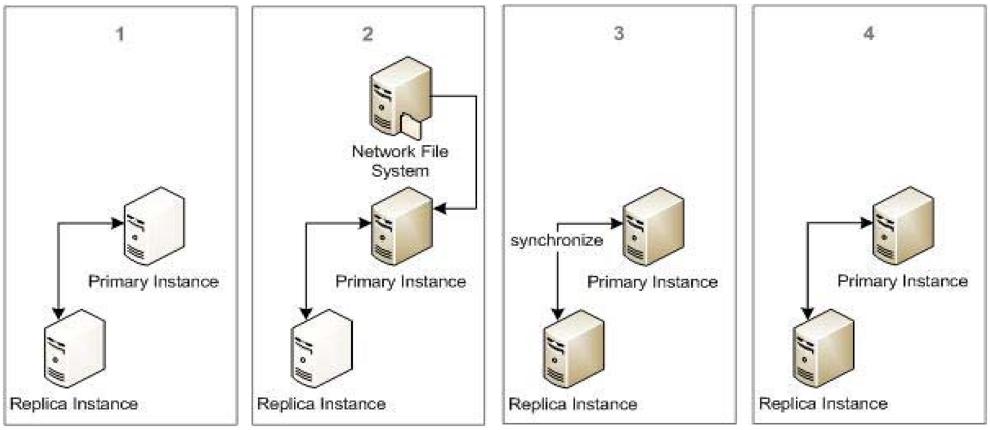
Restoring Primary Instance Data on a Replicated Deployment

When data has been accidentally deleted on a primary instance and the lost data has been replicated to the replica instance, you can restore the primary instance data by completing the following tasks.

Procedure

1. Troubleshoot the primary instance to determine that data is missing but the primary instance is still functioning properly.
2. Perform the Restore from Backup procedure. For instructions, see Restore from Backup on page 375.
3. Manually synchronize each replica instance. For instructions, see Synchronize a Replica Instance on page 368.

The following figure shows the process.



Restore from Backup

This procedure restores deployment data from a backup.

No administration or authentication operations can be performed while the data is restored. The restore process takes longer to complete than the backup process because the authentication services are stopped and started. The size of the internal database also determines the amount of time required to restore data. If the internal database is large, the process can take a long time.

Before You Begin

- You must have a backup created on your deployment.
- You must be an Operations Console administrator.

Procedure

1. In the Operations Console, click **Maintenance** > **Backup and Restore** > **Restore from Backup**.
2. Under **Backup Location**, do one of the following:
   - Select **Local Authentication Manager Server**.
   - Select **Windows Shared Folder**.
     - In the **Windows Shared Folder** field, enter the path to an existing Windows shared folder, for example, **\\primary.company.net\backup_path**.

  - If the shared folder requires a user name, enter the user name in the **Folder User Name** field, for example, Domain1\User1.
  - If the shared folder requires a password, enter the password in the **Folder Password** field, for example, password1.

- Select **NFS (Network File System) Shared Folder**.

  In the **NFS Shared Folder** field, enter the NFS server host name and path to a NFS shared folder, for example, **fileserver.company.net:/backup_path**.

3. Under **Restore Options**, do one of the following:

   - Select **All Data** to restore deployment data.

     If you select the All Data option, no administration or authentication operations can be performed while the deployment is being restored.

   - Select **Log Data Only** to restore just the Administrative Audit, Runtime Audit, and System log data.

     Select this option after you promote a replica instance to transfer the historical log data from the previous primary instance to the new primary instance.

4. Click **Next**.

   A list of backups is displayed. If you select **Log Data Only**, the backups created only on the current deployment are displayed.

5. Select the backup (.RSAbackup) that you want to use, and click **Next**.

   You should use the last good backup created on the current deployment.

6. On the Restore from Backup page, confirm that you selected the correct backup, and do one of the following:

   - To select a different backup, click **Back**.
   - To restore with the selected backup, enter the password for this backup, and click **Restore**. The Progress Monitor page is displayed.

7. Click **Done** when the restore process is complete.

Next Steps

- In a replicated deployment, synchronize each replica instance with the restored primary instance. For instructions, see the Operations Console Help topic “Synchronize a Replica Instance.”

  If you restored the primary instance with a backup that came from a different deployment, then the restore operation automatically deletes each replica instance from the current deployment. A backup that is restored from the original primary instance in the current deployment retains each replica instance.

- If the replica instance includes a web tier, generate a web-tier package for the web tier associated with the replica instance, and run the Web-Tier Installer. For instructions, see the chapter “Installing Web Tiers” in the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

Primary Instance Restoration

If the primary instance malfunctions either because the database schema is altered or a critical application file is deleted, the primary instance can become unavailable.

When the primary instance is unavailable, you cannot administer the deployment. For example, without the primary instance, you cannot add users.

If you suspect that the primary instance is malfunctioning, you can restore the primary instance using one of the following methods:

- Primary Instance Replacement
- Replica Instance Promotion for Disaster Recovery
- Reverting the Primary Instance to a Snapshot

Primary Instance Replacement

You can restore a malfunctioning primary instance by replacing the primary instance with a new appliance and restoring the primary instance using Restore from Backup.

If you use a backup to restore a primary instance with an IP address or hostname that is different from the malfunctioning primary instance, you must generate the **Authentication Manager** host configuration file (**sdconf.rec**) and install this file on each authentication agent after replacing the appliance.

Replacing the malfunctioning primary instance can take a long time. In a replicated deployment, if a replica instance runs out of storage space because data cannot be sent to the primary instance, the replica instance might also become unresponsive. When this happens, the replica instance cannot authenticate users.

Replacing the Primary Instance in a Standalone Deployment

Perform the following tasks to replace a malfunctioning primary instance in a standalone deployment.

Procedure

1. Do one of the following:
   - For a virtual appliance, deploy and configure a new primary appliance to replace the malfunctioning primary instance. For instructions, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.
   - For a hardware appliance, shut down the appliance and remove the machine from service. You can perform a factory reset to restore the appliance to a pre-configured state. For more information, see Factory Reset on page 396.
2. Restore the old primary instance on the new appliance using Restore from Backup. For instructions, see Restore from Backup on page 375.

3. (Optional) Generate and install the Authentication Manager host configuration file (**sdconf.rec**) on each authentication agent if you use a backup to restore a primary instance with a different IP address or hostname.

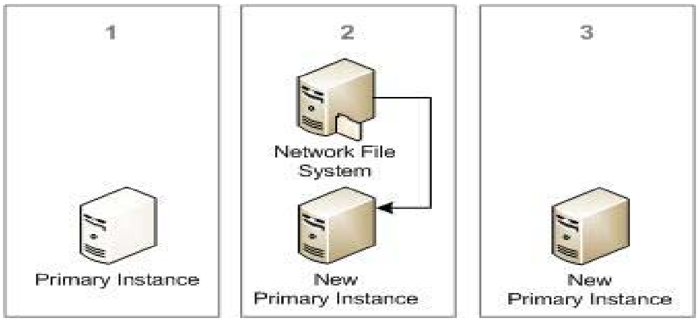
   For instructions on generating a host configuration file, see Generate the Authentication Manager Configuration File on page 65.

   For instructions on installing a host configuration file, see the agent documentation.

4. (Optional) If the deployment has a trust relationship with another realm and you restore the primary instance on a machine with a new hostname, you must repair the trust relationship. For instructions, see Trusted Relationship Repair on page 390.

5. For a virtual appliance, delete the old primary instance virtual machine from the disk using the vSphere client. For instructions, see the vSphere documentation.

The following figure shows the process.



Replacing the Primary Instance in a Replicated Deployment

Perform the following tasks to replace a malfunctioning primary instance in a replicated deployment.

Procedure

1. Do the following:
   - For each virtual appliance, use the vSphere client to suspend the virtual machine. For instructions, see the vSphere documentation.
   - For each hardware appliance, press the power button to shut down the physical machine.

2. Deploy and configure a new primary instance to replace the malfunctioning primary instance. For instructions, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

3. Restore the old primary instance on the new appliance using Restore from Backup. For instructions, see Restore from Backup on page 375.

   If you are restoring the primary instance with a backup that comes from a different deployment, then the restore operation automatically deletes each replica instance from the current deployment. A backup that is restored from the original primary instance in the current deployment retains each replica instance.

4. Do the following:

    - In a virtual environment or a mixed virtual and hardware environment, delete the virtual machine for the original primary instance and the virtual machine for each of the original replica instances from the disk using the vSphere client. For instructions, see the vSphere documentation.

    - For a primary instance on a hardware appliance, shut down the malfunctioning primary instance and remove the machine from service.

5. Do the following:

    - For each virtual appliance, deploy and configure a new replica instance to replace each deleted replica instance, and attach each replica instance to the primary instance. For instructions, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

    - For each hardware appliance, turn on each replica instance.

      You can perform a factory reset to restore the replica instance to a pre-configured state, and then you can run Quick Setup to configure a replica instance. For more information, see Factory Reset on page 396.

      Attach each replica instance to the primary instance. For instructions, see the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

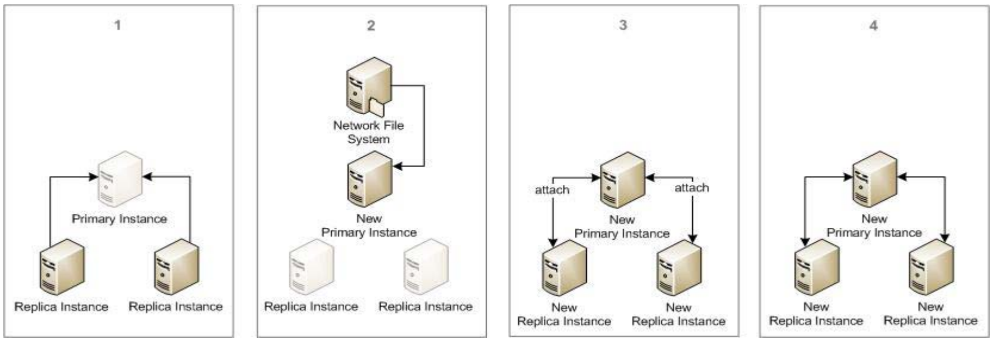
6. (Optional) Generate and install the Authentication Manager host configuration file (**sdconf.rec**) on each authentication agent if you use a backup to restore a primary instance with a different IP address or hostname.

   For instructions on generating a host configuration file, see Generate the Authentication Manager Configuration File on page 65.

   For instructions on installing a host configuration file, see the agent documentation.

7. (Optional) If the deployment has a trust relationship with another realm and you restore the primary instance on a virtual machine with a new hostname, you must repair the trust relationship. For instructions, see Trusted Relationship Repair on page 390.

The following figure shows the process.



Replica Instance Promotion for Disaster Recovery

You can restore a malfunctioning primary instance by promoting a replica instance to become the primary instance.

Promoting a replica instance restores the primary instance more quickly than replacing the primary instance with a new appliance, but the replica instance available for promotion needs to be physically accessible to an Operations Console administrator to facilitate ongoing administration.

Promoting a replica instance to be the primary instance changes the topology of a deployment in the following ways:

- The malfunctioning primary instance is deleted from the deployment.
- The promoted replica instance becomes the new primary instance.
- The RADIUS server on the new primary instance becomes the RADIUS primary. You cannot perform a separate promotion of a replica RADIUS server.
- If web tiers are associated with the old primary instance, you must restart the web tiers that are associated with the old primary instance.
- If web tiers are associated with any replica instance in the deployment, you must restart the web tiers that are associated with any replica instance.

Promoting a Replica Instance in a Deployment with One Replica Instance

Perform the following tasks to promote the replica instance to be the primary instance.

Before You Begin

Make sure that the primary instance is unresponsive before you promote the replica instance.

If the primary instance is partially functional, then do the following:

- For a virtual machine, use the vSphere client to shut down the primary instance virtual machine. For instructions, see the vSphere documentation.
- For a hardware appliance, press the power button to shut down the primary instance.

Procedure

1. Promote a replica instance to primary instance.

   For instructions, see Promote a Replica Instance for Disaster Recovery on page 383.

2. If web tiers are associated with the deployment, do the following.

   a. If web tiers are associated with the old primary instance, restart all the web tiers.

      For instructions, see Promote a Replica Instance for Disaster Recovery on page 383.

b. If web tiers are associated with replica instances, wait for the web-tier status to display **Offline**. This can take about 30 minutes. Restart the bootstrapper server and web-tier services on each web tier, and wait for the web-tier status to display **Online** before attempting to access the web-tier services.

   For instructions, see Promote a Replica Instance for Disaster Recovery on page 383.

3. (Optional) Restore the log data from the last good backup of the old primary instance to make the historical log data on the old primary instance available on the new primary instance.

   For instructions, see Restore from Backup on page 375.

4. (Optional) Generate and install the Authentication Manager host configuration file (**sdconf.rec**) on each authentication agent if you use a backup to restore a primary instance with a different IP address or hostname.

   For instructions on generating a host configuration file, see Generate the Authentication Manager Configuration File on page 65.

   For instructions on installing a host configuration file, see the agent documentation.

5. Do the following:

   - For a virtual appliance, deploy and configure a new replica instance to replace the promoted replica instance, and attach the new replica instance to the new primary instance.
   - For a hardware appliance, you can perform a factory reset to restore the malfunctioning primary instance to a pre-configured state. You can then run Quick Setup to configure a replica instance. Attach the replica instance. For more information, see Factory Reset on page 396.

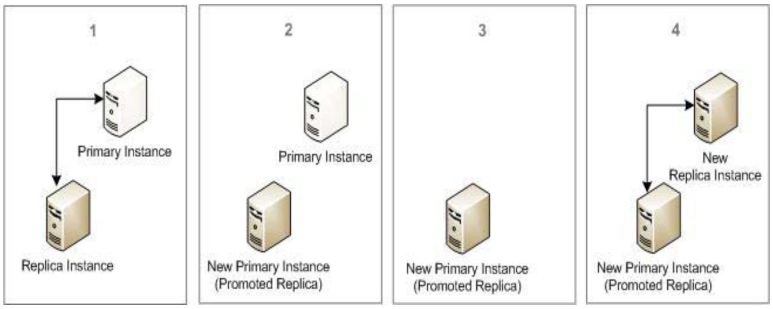
   For instructions, see the chapter “Deploying a Replica Appliance” in the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

6. Back up the new primary instance.

   For instructions, see Create a Backup Using Back Up Now on page 370.

7. For a virtual appliance, delete the old primary instance from the disk using the vSphere client. For instructions, see the vSphere documentation.

The following figure shows the process.



Promoting a Replica Instance in a Deployment with More Than One Replica Instance

Perform the following tasks to promote a replica instance to be the primary instance.

Before You Begin

Make sure that the primary instance is unresponsive before you promote the replica instance.

If the primary instance is partially functional, then do the following:

- For a virtual machine, use the vSphere client to shut down the primary instance virtual machine. For instructions, see the vSphere documentation.
- For a hardware appliance, press the power button to shut down the primary instance.

Procedure

1. Promote a replica instance to be the primary instance.

   For instructions, see Promote a Replica Instance for Disaster Recovery on page 383.

2. If web tiers are associated with the deployment, do the following.

   a. If web tiers are associated with the old primary instance, restart all the web tiers.

      For instructions, see Promote a Replica Instance for Disaster Recovery on page 383.

   b. If web tiers are associated with replica instances, wait for the web-tier status to display **Offline**. This can take about 30 minutes. Restart the bootstrapper server and web-tier services on each web tier, and wait for the web-tier status to display **Online** before attempting to access the web-tier services.

      For instructions, see Promote a Replica Instance for Disaster Recovery on page 383.

3. (Optional) Restore the log data from the last good backup of the old primary instance to make the historical log data on the old primary instance available on the new primary instance.

   For instructions, see Restore from Backup on page 375.

4. (Optional) Generate and install the Authentication Manager host configuration file (**sdconf.rec**) on each authentication agent if you use a backup to restore a primary instance with a different IP address or hostname.

   For instructions on generating a host configuration file, see Generate the Authentication Manager Configuration File on page 65.

   For instructions on installing a host configuration file, see the agent documentation.

5. Do the following:

   - For a virtual appliance, deploy and configure a new replica instance to replace the promoted replica instance, and attach the new replica instance to the new primary instance.

   - For a hardware appliance, you can perform a factory reset to restore the malfunctioning primary instance to a pre-configured state. You can then run Quick Setup to configure a replica instance. Attach the replica instance. For more information, see Factory Reset on page 396.

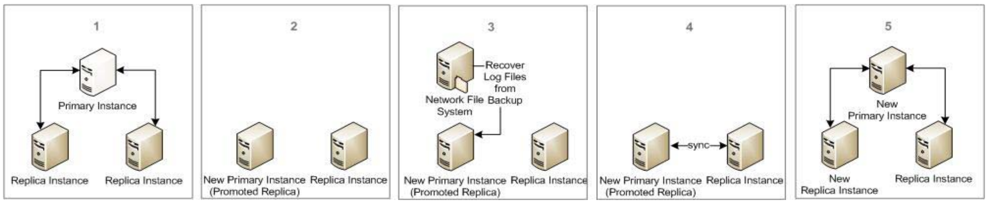
   For instructions, see the chapter "Deploying a Replica Appliance" in the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

6. Back up the new primary instance.

   For instructions, see Create a Backup Using Back Up Now on page 370.

7. For a virtual appliance, delete the old primary instance from the disk using the vSphere client. For instructions, see the vSphere documentation.

The following figure shows the process.



Promote a Replica Instance for Disaster Recovery

This procedure removes a malfunctioning primary instance from the deployment and promotes a replica instance to be the new primary instance. Promoting a replica instance restores the ability to administer a deployment.

While the replica instance is being promoted, users cannot authenticate to the replica, and you cannot perform any administrative functions, such as adding users.

If the original primary instance and all replica instances are online and functional, then you can perform a promotion for maintenance. For more information, see Promotion for Maintenance on page 356.

Before You Begin

You must be an Operations Console administrator.

Procedure

1. Log on to the Operations Console of the replica instance that you are promoting, and click **Deployment Configuration** > **Replica Promotion> For Disaster Recovery**.

2. On the Promote Replica to Primary page under **Current Replica Instance Details**, review the information to verify that this is the replica instance that you want to promote.

3. Under **Confirmation**, select **Yes, promote the replica**, and click **Promote**.

   The promotion progress displays. For detailed information about this process, click **Advanced Status View**.

4. After all the promotion tasks are completed, click **Next**.

5. Review the information under **Summary/Results** and **Proposed Next Steps**, and click **Done**.

Next Steps

- Check the following items on the new primary instance after you finish the promotion process, and make any necessary changes.

Item	Instructions
Primary Instance Web Tiers. If web tiers are associated with the old primary instance, perform these steps: 1. Check the replication status of each replica instance to verify that the replica status displays **Normal**. 2. After the status of all of each replica instance displays **Normal**, wait five minutes to make sure that the server list check has taken place. 3. Restart the bootstrapper server and web-tier services on each web tier.	See the Operations Console Help topic “Check Replication Status.” See Managing the Web-Tier Service on page 180.
Replica Instance Web Tiers. If web tiers are associated with any replica instance, perform these steps: 1. Wait for the web-tier status to display **Offline**. This can take about 30 minutes. 2. Restart the bootstrapper server and web-tier services on each web tier. 3. Wait for the web-tier status to display **Online** before attempting to access the web-tier services.	See the Operations Console Help topic “View Web-Tier Deployments.” See Managing the Web-Tier Service on page 180.
Identity Sources. Make sure that the identity sources that you use are connected to the new primary instance.	See the Operations Console Help topic “View the Identity Sources in Your Deployment.”
Schedule Backups. Review the backup schedule for the primary instance. Make sure that the new primary instance can communicate with the backup location.	See Create a Backup Using Schedule Backups on page 371.

Item	Instructions
Self-Service Console URL. Make sure that the link that is included in e-mail notifications for Self-Service user account changes contains the correct URL for the Self-Service Console.	See the Security Console Help topic “Configure E-mail Notifications for Self-Service User Account Changes.”
Critical Notifications. Check SMTP configuration for critical notifications and other purposes, like dynamic seed provisioning.	See the Security Console Help topic “Configure SNMP.”

- To make the historical log data from the former primary instance available on the new primary instance, use the Operations Console to restore the log data from the last good backup of the old primary instance. For instructions, see Restore from Backup on page 375.

Reverting the Primary Instance to a Snapshot

The following information about reverting the primary instance to a snapshot is only for the virtual appliance. Reverting the primary instance to a snapshot is not supported for the hardware appliance.

You can restore a malfunctioning primary instance by reverting the primary instance to a snapshot of a previous virtual machine state.

If you attempt to attach or synchronize a replica instance while reverting to a snapshot, the replica instance status becomes **Attachment Unsuccessful**. This status displays on the Replication Status Report page of the Operations Console. If this happens, you must delete this replica instance and attach a new one. For instructions, see the Operations Console Help topic “Delete a Replica Instance.”

You do not need to revert a replica instance when you revert a primary instance to a snapshot.

Reverting the Primary Instance to a Snapshot in a Standalone Deployment

In a standalone deployment, you can take snapshots of the primary instance and revert the primary instance to a snapshot at any time. For information on taking snapshots, see Primary or Replica Instance Snapshots on page 373.

Reverting the Primary Instance to a Snapshot in a Replicated Deployment

In a replicated deployment, you can take snapshots of the primary instance and revert the primary instance to a snapshot at any time. For information on taking snapshots, see Primary or Replica Instance Snapshots on page 373.

After you revert to a snapshot, all attached and working replica instances are out of sync with the primary instance and must be synchronized. For instructions, see Synchronize a Replica Instance on page 368.

Additional Snapshot Tasks

Because a snapshot preserves the virtual machine state at a particular point in time, you might need to perform some additional tasks:

- If you revert the primary instance to a snapshot that was taken before you changed the primary instance hostname, the primary instance cannot communicate with any of the replica instances. To restore communication, delete all the replica instances in the Operations Console of the primary instance, and delete each replica instance virtual machine from the deployment. For instructions, see the Operations Console Help topic "Delete a Replica Instance." You can replace the deleted replica instances with new ones.
- If you revert the primary instance to a snapshot that was taken before you changed a replica instance hostname, the primary instance cannot communicate with that replica instance. To restore communication, delete that replica instance in the Operations Console of the primary instance, and delete that replica instance virtual machine from the deployment. For instructions, see the Operations Console Help topic "Delete a Replica Instance." You can replace this deleted replica instance with a new one.
- If you take a snapshot of a replica instance before it is promoted to the primary instance, you cannot use that snapshot to restore the new primary instance if it malfunctions. If the new primary instance malfunctions, either promote a replica instance to be the primary instance or deploy a new primary instance and restore the primary instance with a backup. If necessary, delete the malfunctioning primary instance virtual machine. For instructions, see Primary Instance Restoration on page 377.
- If you revert the primary instance to a snapshot that includes replica instances that were deleted after the snapshot was taken, the Operations Console of the primary instance shows those replica instances as still attached. To show the actual state of the deployment, delete these replica instances from the Operations Console, and, if necessary, delete each replica instance virtual machine. For instructions, see the Operations Console Help topic "Delete a Replica Instance."
- If you take a snapshot of the primary instance in a deployment that has an unattached replica instance and this replica instance is attached after this snapshot is taken, this replica instance does not appear in the Operations Console of the primary instance after you revert the primary instance to this snapshot. To restore the actual state of the deployment, delete the virtual machine for this replica instance.

Replica Instance Restoration

If a replica instance malfunctions either because the database schema is altered or a critical application file is deleted, the replica instance can become undependable or unresponsive. When the replica instance is unavailable, you lose authentication failover and the ability to restore administration quickly if the primary instance becomes unavailable.

If you suspect that a replica instance is malfunctioning, you can restore the malfunctioning replica instance using one of the following methods:

- Replacing a Replica Instance
- Reverting a Replica Instance to a Snapshot

Replacing a Replica Instance

Perform the following tasks to replace an unresponsive replica instance.

Before You Begin

Make sure that the replica instance is unresponsive before you replace the replica instance.

If the replica instance is a virtual appliance and is partially functional, use the vSphere client to shut down the replica instance virtual machine. For instructions, see the vSphere documentation.

Procedure

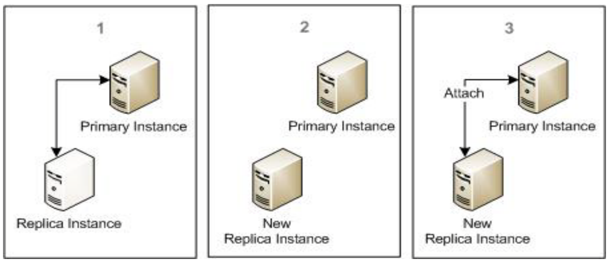
1. Delete the unresponsive replica instance from you deployment. For instructions, see the Operations Console Help topic "Delete a Replica Instance."
2. Deploy a new replica instance to replace the deleted replica instance, and attach it to the primary instance.

   For instructions, see the chapter "Deploying a Replica Appliance" in the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.
3. Back up the primary instance.

   For instructions, see Create a Backup Using Back Up Now on page 370.
4. Do one of the following:
   - For a virtual appliance, delete the old replica instance from the disk using the vSphere client.

     For instructions, see the vSphere documentation.
   - For a hardware appliance, shut down the old replica instance and remove the machine from service. You can perform a factory reset to restore the appliance to a pre-configured state. For more information, see Factory Reset on page 396.

The following figure shows the process.



Reverting a Replica Instance to a Snapshot

The following information about reverting the replica instance to a snapshot is only for the virtual appliance. Reverting the replica instance to a snapshot is not supported for the hardware appliance.

You can restore a malfunctioning replica instance by reverting the replica instance to a snapshot of a previous virtual machine state.

When you revert a replica instance to a snapshot, any replica data that has not been sent to the primary instance is lost. Replica data sent to the primary instance after the snapshot was taken is preserved.

You do not need to revert the primary instance when you revert a replica instance to a snapshot.

Reverting a Replica Instance to a Snapshot

In a replicated deployment, you can take snapshots of any replica instance and revert that replica instance to a snapshot at any time. For information on taking snapshots, see Primary or Replica Instance Snapshots on page 373.

After you revert to a snapshot, the replica instance is out of sync with the primary instance and must be synchronized . For instructions, see Synchronize a Replica Instance on page 368.

Additional Snapshot Tasks

Because a snapshot preserves the virtual machine state at a particular point in time, the primary instance might not be able to communicate with a replica instance after you revert the replica instance to a particular snapshot. This happens if you revert to a replica snapshot that is taken before you make these changes:

- You give the primary instance or replica instance a new hostname.
- You promote a replica instance to replace the primary instance.

To restore communication between the primary instance and the replica instance, delete the replica instance in the Operations Console of the primary instance, and delete the replica instance virtual machine from the deployment. For instructions, see the Operations Console Help topic “Delete a Replica Instance.” Replace the deleted replica instance with a new replica instance.

Restore Web Tier

Perform the following procedure to restore a web tier when it stops responding. These procedures apply when you need to restore only the web tier, and the primary and replica instances are functioning normally.

Procedure

1. On the web-tier server, run the RSA Authentication Web-Tier Uninstaller for the platform. For instructions, see one of the following:
   - Uninstall a Web Tier on Windows on page 179.
   - Uninstall a Web Tier on Linux on page 179.
2. Remove the web-tier deployment record:
   a. In the Operations Console, click **Deployment Configuration** > **Web-Tier Deployments** > **Manage Existing**.

   b. On the Web-Tier page, select the web-tier to remove, and click **Delete**.

   For complete instructions, see the Operations Console Help topic "Delete a Web-Tier Deployment Record."
3. In the Operations Console, click **Deployment Configuration** > **Web-Tier Deployments** > **Add New** to add a new web-tier deployment record. For instructions, see the Operations Console Help topic "Add a Web-Tier Deployment Record."
4. On the primary instance, generate a web-tier deployment package:
   a. In the Operations Console, click **Deployment Configuration** > **Web-Tier Deployments** > **Manage Existing**.

   b. On the Web-Tier Deployments page, select the web tier for which to generate a web-tier package.

   c. On the Generate Web-Tier Deployment Package page, enter a password for the web-tier package file.

   d. Click **Generate Web-Tier Package**.

   e. Click **Download**.
5. Run the RSA Authentication Web-Tier Installer for the platform. For instructions, see the chapter "Installing Web Tiers" in the *RSA Authentication Manager 8.1 Setup and Configuration Guide*.

Trusted Relationship Repair

When you restore an RSA Authentication Manager 8.1 primary instance on a machine with a new hostname or perform a migration, and you had a trust relationship previously with another realm, the following trust relationships must be repaired:

- **Trusted Realm.** A trust relationship between two Authentication Manager 8.0 or 8.1 deployments or between an Authentication Manager 8.0 or 8.1 and an Authentication Manager 7.1 deployment. For instructions, see Repair a Trust Relationship with a Version 8.0 or 8.1 Realm on page 390 or Repair a Trust Relationship with a Version 7.1 Realm on page 392.

  For a trusted realm, the repair process ensures that the original trusted realm information, such as trusted users and groups, is preserved. The process is similar to adding a trusted realm. Both the administrator of the migrated or restored version 8.0 or 8.1 deployment, and the administrator of the version 8.0, 8.1, or 7.1 deployment participate in the repair process. However, only the administrator of the previously trusted realm imports a trust package. The administrator of the migrated or restored deployment provides a trust package to the administrator of the deployment where the trust will be repaired. This package is used to repair the trusted realm.

- **Cross Trust.** A legacy trust relationship between a version 8.0 or 8.1 and a version 6.1 deployment. For instructions, see Repairing a Trusted Legacy Realm on page 395.

  For a legacy trust relationship, the repair process requires updating the host name and IP address in the realm record on the Authentication Manager 6.1 deployment.

Repair a Trust Relationship with a Version 8.0 or 8.1 Realm

If you restore the version 8.1 primary instance on a machine with a new hostname, and you had a trust relationship previously with another version 8.0 or 8.1 realm, perform the following procedure to repair the trust between the two RSA Authentication Manager 8.0 or 8.1 deployments.

Before You Begin

The administrator of the restored deployment and the administrator of the deployment where the trust will be repaired must be able to communicate directly while they perform this procedure.

Procedure

1. The administrator of the restored deployment performs the following steps to generate a trust package.

   a. In the Security Console, click **Administration** > **Trusted Realms** > **Manage Existing**.

   b. Under **Trusted Realm Name**, click the trusted realm name to repair.

   c. From the context menu, click **Generate Trust Package,** and save the file (**TrustPackage.xml**).

   d. After the trust package is saved, use a secure method to send the trust package to the administrator of the deployment where the trust will be repaired.

2. The administrator of the deployment where the trust will be repaired performs the following steps to import the trust package.

   a. After receiving the trust package, click **Administration** >**Trusted Realms** > **Manage Existing**.

   b. Under **Trusted Realm Name**, click the trusted realm name to repair.

   c. From the context menu, click **Repair Trust**.

   d. In the **Trust Package from Trusted Realm** field, enter the path to the new trust package by browsing to the package file, and click **Open**.

   e. Click **Next**, and contact the restored realm administrator.

3. The administrator of the restored deployment performs the following steps to share the confirmation code with the administrator of the deployment where the trust will be repaired.

   a. In the Security Console, click **Administration** > **Trusted Realms** > **Manage Existing**.

   b. Under **Trusted Realm Name**, click the trusted realm name to repair.

   c. From the context menu, click **View**, locate the confirmation code under **Current Realm Confirmation Code**, and read the code to the administrator of the deployment where the trust will be repaired to confirm that the trust package is valid.

      The Current Realm Confirmation Code must match the administrator's Trusted Realm Confirmation Code.

4. The administrator of the deployment where the trust will be repaired performs the following steps to repair the trust.

   a. On the Update Trusted Realm page under **Trusted Realm Confirmation Code**, read the **Trust Package Confirmation Code** to the restored realm administrator to confirm that the trust package is valid.

      The Trusted Realm Confirmation Code must match the restored realm administrator's Current Realm Confirmation Code.

      If the confirmation code does not match, ask the restored realm administrator to generate and send a new trust package.

   b. Click **Confirm and Next**.

   c. (Optional) For **Authentication Status**, select **Authenticate Trusted Users** if you want your realm to authenticate users from the trusted realm.

   d. For **Create Trusted Users in Security Domain**, select the security domain that will own users from the trusted realm.

      After your realm authenticates users from the trusted realm, the users must belong to a security domain in your realm. The security domain that you select must be configured to use the internal database as an identity source.

e. (Optional) In the **Trusted User Name Identifier** field, enter a unique identifier that your realm can recognize for the trusted user, and click **Add**. The unique identifier could be the user's domain name or e-mail address, such as jsmith@company.com. The value must be unique among trusted realms.

   For example, suppose John Smith from Realm A is jsmith in his local realm. Your realm does not know the identity of jsmith. If you enter yourcompany.com in this field, this user will be identified within your realm as jsmith@yourcompany.com.

f. Click **Save**.

Repair a Trust Relationship with a Version 7.1 Realm

If you restore a version 8.0 or 8.1 primary instance on a machine with a new hostname, and you had a trust relationship previously with a version 7.1 realm, perform the following procedure to repair the trust between the RSA Authentication Manager 8.0 or 8.1 deployment and the RSA Authentication Manager 7.1 deployment.

Before You Begin

You and the version 7.1 administrator must communicate directly while performing this procedure.

Procedure

1. On version 8.0 or 8.1, generate a trust package, and securely send this package to the 7.1 administrator. To generate a trust package, do the following:
   a. In the version 8.0 or 8.1 Security Console, click **Administration** > **Trusted Realms** > **Manage Existing**.
   b. Under **Trusted Realm Name**, click the version 7.1 trusted realm to repair.
   c. From the context menu, click **Generate Trust Package,** and save the file (**TrustPackage.xml**).
2. Instruct the version 7.1 administrator to import the version 8.1 trust package and record the **Current Realm Confirmation Code**. For instructions, advise the version 7.1 administrator to see the Security Console Help topic "Reimport a Trust Package."
3. As part of import, the version 7.1 administrator must verify the **Trusted Realm Confirmation Code**. On version 8.0 or 8.1, do the following to locate the confirmation code for your realm and share the confirmation code with the version 7.1 administrator:
   a. In the version 8.0 or 8.1 Security Console, click **Administration** > **Trusted Realms** > **Manage Existing**.
   b. Under **Trusted Realm Name**, click the version 7.1 realm to repair.

c. From the context menu, click **View**, and locate the confirmation code for **Current Realm Confirmation Code**. Read the code to the version7.1 administrator to confirm that the trust package is valid.

The version 8.0 or 8.1 **Current Realm Confirmation Code** and the 7.1 **Trusted Realm Confirmation Code** must match. If the confirmation codes do not match, you must generate a new trust package, and securely send the package to the version 7.1 administrator.

Repair Trusted Realm Discrepancy When the Backup is Incomplete

When you use a backup to restore a primary instance on a new machine, the connection information for trusted realm authentication is contained in the backup. If you restore a primary instance with a backup that does not match the deployment, you must repair the discrepancy. For example, if you create a backup and then add a trusted realm, the backup will not contain the connection information for the trusted realm. If you restore a primary instance with this backup, you need to perform additional tasks to remove any discrepancy.

The following table shows the tasks required to restore the discrepancies in the deployment when the backup does not reflect the current state of the deployment.

Deployment Relationship	Backup	Type of Restoration	Required Tasks
Deployment A (version 8.0, 8.1, or 7.1) has a trust relationship with Deployment B (version 8.0 or 8.1).	Backup does not contain trust relationship data.	Deployment B is restored with backup on the same virtual machine or hardware appliance.	1. Regenerate the trust package on Deployment A. 2. On Deployment B, add a new trust for Deployment A.
Deployment A (version 8.0, 8.1, or 7.1) has a trust relationship with Deployment B (version 8.0 or 8.1).	Backup does not contain trust relationship data.	Deployment B is restored with backup on a different virtual machine or hardware appliance.	1. Regenerate trust package on Deployment A. 2. Generate a trust package on Deployment B. 3. If Deployment A is version 7.1, delete and add a new trust for Deployment B. If Deployment A is version 8.0 or 8.1, repair the trust for Deployment B. 4. On Deployment B, repair the trust for Deployment A.

Deployment Relationship	Backup	Type of Restoration	Required Tasks
Deployment A (version 6.1) has a trust relationship with Deployment B (version 8.0 or 8.1).	Backup does not contain trust relationship data.	Deployment B is restored with backup on the same virtual machine or hardware appliance.	On Deployment A, delete the realm (Deployment B).
Deployment A (version 6.1) has a trust relationship with Deployment B (version 8.0 or 8.1).	Backup does not contain trust relationship data.	Deployment B is restored with backup on a different virtual machine or hardware appliance.	On Deployment A, delete the realm (Deployment B).
Deployment A (version 8.0, 8.1, or 7.1) does not have a trust relationship with Deployment B (version 8.0 or 8.1).	Backup contains trust relationship data.	Deployment B is restored with backup on the same virtual machine or hardware appliance.	1. Generate the trust package on Deployment A. 2. Regenerate the trust package on Deployment B. 3. On Deployment A, add a new trust. 4. On Deployment B, repair the new trust for Deployment B.
Deployment A (version 8.0, 8.1, or 7.1) does not have a trust relationship with Deployment B (version 8.0 or 8.1).	Backup contains trust relationship data.	Deployment B is restored with backup on a different virtual machine or hardware appliance.	1. Generate the trust package on Deployment A. 2. Regenerate the trust package on Deployment B. 3. On Deployment A, add a new trust for Deployment B. 4. On Deployment B, repair the new trust for Deployment A.

Deployment Relationship	Backup	Type of Restoration	Required Tasks
Deployment A (version 6.1) does not have a trust relationship with Deployment B (version 8.0 or 8.1).	Backup contains trust relationship data.	Deployment B is restored with backup on the same virtual machine or hardware appliance.	1. On Deployment B, delete the old cross realm authentication with Deployment A. 2. On Deployment A, enable cross realm authentication with Deployment B.
Deployment A (version 6.1) does not have a trust relationship with Deployment B (version 8.0 or 8.1).	Backup contains trust relationship data.	Deployment B is restored with backup on a different virtual machine or hardware appliance.	1. On Deployment B, delete the old cross realm authentication with Deployment A. 2. On Deployment A, enable cross realm authentication with Deployment B.

For more information about enabling cross-realm authentication, see the chapter “Realm Administration” in the *RSA Authentication Manager 6.1 Administrator's Guide*. For more information about creating a trusted realm, see Administering Trusted Realms on page 413.

Repairing a Trusted Legacy Realm

After you use a backup to restore a primary instance on a new appliance, the connection information in the internal database for cross-realm authentication is obsolete. You must repair the connection information to restore cross-realm authentication.

When you restore a primary instance on a new appliance, the Progress Monitor displays a message if you must also repair a trusted realm. If cross-realm authentication was previously enabled on an Authentication Manager 6.1 legacy realm, you repair the trust relationship by updating the host name and IP address in the realm record on the Authentication Manager 6.1 deployment.

For more information, see the RSA Authentication Manager 6.1 Host Mode Console Help topic “Edit a Trusted Realm.”

Factory Reset

If you cannot recover a malfunctioning instance, or if you want to restore an instance to a pre-configured state, you can perform a factory reset. You can only perform this operation on the hardware appliance. A factory reset is not supported on the virtual appliance.

A factory reset restores the original settings on a hardware appliance. This operation removes all data associated with an RSA Authentication Manager instance, including all data, logs, and configured settings, except for possibly the network settings. The factory reset also removes any files that you saved on the hardware appliance.

You can perform a factory reset remotely through the Operations Console or through a command line. If you have direct access to the hardware, you also perform a factory reset by restarting the appliance and choosing the **Factory Reset** option in the appliance boot menu. Depending on the type of factory reset that you perform, the operation preserves or removes the network settings from the appliance. A factory reset from the Operations Console or the command line automatically preserves network settings. If you perform a factory reset by directly accessing the physical appliance and the appliance boot menu, network settings are removed.

After you perform a factory reset, you can reconfigure the appliance as an Authentication Manager instance by completing Quick Setup. To initiate Quick Setup, you must enter the Quick Setup Access Code. A new Quick Setup Access Code is displayed each time you perform a factory reset. This code prevents a malicious user from accessing Quick Setup.

To access Quick Setup, open a web browser and go to the following URL:

https://*IP_Address_of_Appliance*

where *IP_Address_of_Appliance* is the IP address that you configured for the appliance.

If you directly access the physical hardware and perform a factory reset through the appliance boot menu, you must reconfigure network settings before you can access Quick Setup.

Consequences of a Factory Reset

Before performing a factory reset, RSA recommends that you consider the consequences.

The following applies when performing a factory reset on the primary instance:

- You cannot administer the deployment until a primary instance is available. If a primary instance is unresponsive, RSA recommends that you promote a replica instance to reduce administrative downtime. For more information, see Replica Instance Promotion for Disaster Recovery on page 380.
- Authentication requests are redirected to a replica instance when the primary instance is unavailable. If replica instances are not available, users cannot authenticate until a primary instance is available.
- Data that accumulates on the replica instance while the primary instance is unavailable is lost.

- If you restore a backup file on a reset primary instance, the primary instance will not contain data for changes that were made after the backup file was created. For more information, see Deployment Backup on page 369.
- You cannot reattach the replica instances to the reset primary instance. In this case, you must redeploy new replica instances and attach the replica instances to the deployment.

If you perform a replica instance promotion for disaster recovery, you avoid redeploying and reattaching the replica instances. You also reduce the total amount of data that is lost. In this case, the data that exists on the promoted replica instance is preserved. However, the promotion process requires that you synchronize the remaining replica instances with the new primary instance. Any data that was recorded on the these replica instances while the original primary instance was unavailable is lost during synchronization. For more information, see Replica Instance Promotion for Disaster Recovery on page 380.

The following applies when performing a factory reset on a replica instance:

- Data on the replica instance that did not replicate to the primary instance is lost.
- Authentication requests are redirected to other available instances.
- You must remove the replica instance from your deployment before performing a factory reset.

When performing a factory reset on an instance and then adding an instance to your deployment, you also must consider how these actions affect your network topology. For example, if you promote a replica instance and perform a factory reset on the original primary instance, you may decide to configure the reset appliance as a new replica instance. These actions may require that you restore RADIUS replication or restart the web tiers.

Because a factory reset removes any files that are saved on the appliance, you must transfer any files that you wish to access following the factory reset, such as backup files, from the hardware appliance to an external, accessible location. This is especially required if you wish to restore a reset machine with a backup file that is stored on the appliance.

Perform a Factory Reset Using the Appliance Boot Menu

If you have direct access to the hardware appliance, you can perform a factory reset by accessing the boot menu that loads after restarting the appliance. This operation removes all data, logs, and settings that are associated with an Authentication Manager instance. In this procedure, the appliance is restored to its original factory settings. The network settings are not preserved.

If you need to perform a factory reset remotely and you want to preserve the network settings, see Perform a Factory Reset Using a Command Line Utility on page 399 or Perform a Factory Reset Using the Operations Console on page 400.

Important: You can only perform this procedure on the hardware appliance. This operation is not supported on the virtual appliance.

Before You Begin

Transfer any files that you want to save, for example, backup files, from the hardware appliance to an external, secure location.

Procedure

1. Attach a monitor and keyboard to the hardware appliance.
2. Do one of the following:
   - Restart the hardware appliance with a command. Do the following:
     - In a command prompt, log on as **rsaadmin** and enter the operating system account password.
     - Type the following command to log on as the root user and press ENTER:

       ```
       sudo su -
       ```

     - When prompted, type the operating system account password, and press ENTER.
     - Type the following command.

       ```
       reboot
       ```

     After the hardware appliance restarts, a boot menu displays.
   - At the physical machine, press the power button to shut down the appliance, and press the power button again to restart it.

     A boot menu displays.
3. Using the down-arrow key, immediately select **Factory Reset** from the boot menu. Another boot menu displays.

   If you do not select **Factory Reset** within 10 seconds, Authentication Manager starts automatically. If this happens, go to step 2.
4. In the boot menu, use the down-arrow key to select **Perform a Factory Reset**. The factory reset begins. A factory reset takes up to 15 minutes to complete.

Next Steps

To configure the hardware appliance as an Authentication Manager instance after the factory reset, do the following:

- Perform the following initial configuration tasks on the hardware appliance:
  - Confirm the keyboard layout settings. The keyboard is automatically set to **English (United States)**. You can change the language that is associated with the keyboard by clicking any key.
  - Accept the RSA license agreement.
  - Configure the network settings.
  - Record the Quick Setup URL and the Quick Setup Access Code. This information is required to configure your appliance as an Authentication Manager instance.

  For complete instructions, see the *Setup and Configuration Guide*.

- Complete Quick Setup. Go to the Quick Setup URL at https://*IP_Address_of_Appliance*.

  where *IP_Address_of_Appliance* is the IP address of the appliance.

  For Quick Setup instructions, see the *Setup and Configuration Guide*.

Perform a Factory Reset Using a Command Line Utility

Use the following procedure to perform a factory reset with a command line utility. This operation removes all data, logs, and settings, except for network settings, that are associated with an Authentication Manager instance.

To complete this procedure, you must enable SSH. If the Operations Console is not available and you cannot enable SSH, you must perform a factory reset using the appliance boot menu. For instructions, see Perform a Factory Reset Using the Appliance Boot Menu on page 397.

Important: You can only perform this procedure on the hardware appliance. This operation is not supported on the virtual appliance.

Before You Begin

- Transfer any files that you want to save, such as backup files, from the hardware appliance to an external, secure location.
- Enable SSH on the appliance. For instructions, see Enable SSH on the Appliance on page 403.

Procedure

1. Log on to the primary or replica appliance. Do the following:
   a. Launch the SSH client, and connect to the appliance using the IP address or fully qualified hostname.
   b. When prompted for the user name, type the operating system User ID, **rsaadmin**, and press ENTER.
   c. When prompted for the password, type the **rsaadmin** operating system account password, and press ENTER.
2. Change directories to the Authentication Manager utilities directory. Type the following, and press ENTER:

   ```
   cd /opt/rsa/am/utils
   ```
3. Type the following and press ENTER

   ```
   ./rsautil factory-reset
   ```
4. When prompted, enter the Operations Console username and password.
5. Confirm that you want to perform the factory reset. Type **y**.

   When the factory reset starts, the SSH connection automatically closes. The factory reset takes up to 15 minutes to complete.

6. Record the Quick Setup URL and the Quick Setup Access Code. This information is required to configure your appliance as an Authentication Manager instance.

   Do not close the SSH connection or reboot the appliance without recording the Quick Setup Access Code. If you do not have the code, then you must perform a second factory reset to generate a new code. To do so, you must have direct access to the hardware appliance. For instructions, see Perform a Factory Reset Using the Appliance Boot Menu on page 397.

Next Steps

To configure the hardware appliance as an Authentication Manager instance, complete Quick Setup. After factory reset, you can access Quick Setup at

https://*IP_Address_of_Appliance*.

where *IP_Address_of_Appliance* is the IP address of the appliance.

For Quick Setup instructions, see the *Setup and Configuration Guide*.

Perform a Factory Reset Using the Operations Console

Use the following procedure to perform a factory reset on the hardware appliance. This operation removes all data, logs, and settings, except for network settings, that are associated with an Authentication Manager instance.

Important: You can only perform this procedure on the hardware appliance. This operation is not supported on the virtual appliance.

Before You Begin

Transfer any files that you want to save, such as backup files, from the hardware appliance to an external, secure location.

Procedure

1. On a primary instance or replica instance, click **Maintenance** > **Factory Reset Appliance**.
2. Review the text on the screen.
3. Select the confirmation checkbox, and click **Begin Factory Reset**.

   The factory reset begins. Wait approximately 15 minutes for the operation to complete.
4. The Factory Reset in Progress window displays the Quick Setup URL and the Quick Setup Access Code. Record this required information.

   Do not close the Factory Reset in Progress window without recording the Quick Setup Access Code. If you do not have the code, then you must perform a second factory reset to generate a new code. To do so, you must have direct access to the hardware appliance. For instructions, see Perform a Factory Reset Using the Appliance Boot Menu on page 397.

5. After the process completes, you can access Quick Setup at the following location:

   https://*IP_Address_of_Appliance*.

   where *IP_Address_of_Appliance* is the IP address of the appliance.

Next Steps

To configure the hardware appliance as an Authentication Manager instance, complete Quick Setup. For instructions, see the *Setup and Configuration Guide*.

16 Advanced Administration

Troubleshooting and Advanced Administration Using the Appliance Operating System

Although you use the Operations Console and the Security Console to administer Authentication Manager, there are times when you need to access the appliance operating system to perform the following advanced administration tasks:

- Run RSA Authentication Manager command line utilities (CLUs).
- Stop and start Authentication Manager services.
- Troubleshoot appliance problems.

You access the appliance operating system with a Secure Shell (SSH) client, a software application that uses SSH to connect with a remote computer. The client is installed on a local computer that has a network connection to the appliance. Before you can access the appliance operating system through an SSH client, you must enable SSH on the appliance.

You can also access the operating system on a virtual appliance with the VMware vSphere Client.

Enable SSH on the Appliance

Before you can log on to the appliance operating system using an SSH client, you must enable SSH on the appliance.

You can define session lifetime settings for logging on to the appliance operating system. Session lifetime is an important security feature because it prevents administrators from keeping sessions open indefinitely, leaving them vulnerable to unauthorized access. The session lifetime settings apply when you access the appliance operating system with an SSH client and when you access a virtual appliance with the VMware vSphere Client.

Procedure

1. In the Operations Console, click **Administration** > **Operating System Access**.
2. Select **Enable SSH**. In the **SSH Settings** section, select the checkbox for each NIC on which you want to enable SSH. If you have multiple NICs configured, you can enable SSH on more than one NIC.
3. Under **Session Lifetime Settings**, select **Time out idle sessions**, and enter the time out duration, if you want to time out sessions after a period of inactivity.
4. Click **Save**.

Log On to the Appliance Operating System with SSH

Use the following procedure to log on to the hardware appliance or virtual appliance operating system using an SSH client.

Before You Begin

- Obtain the rsaadmin operating system password.
- Obtain the hostname for the appliance virtual machine.
- Enable SSH on the appliance.

Procedure

1. Launch the SSH client, and connect to the appliance using the IP address or fully qualified hostname.
2. When prompted for the user name, type the operating system User ID, **rsaadmin**, and press ENTER.
3. When prompted for the password, type the rsaadmin operating system account password, and press ENTER.

Log On to the Appliance Operating System with the VMware vSphere Client

Use the following procedure to log on to the virtual appliance operating system using the VMware vSphere Client.

Before You Begin

You can define session lifetime settings for logging on to the appliance operating system. Session lifetime settings prevent administrators from keeping sessions open indefinitely. For more information, see Enable SSH on the Appliance on page 403.

Procedure

1. Log on to the VMware vSphere Client.
2. Right click the virtual appliance name, and select **Open Console** from the context menu.
3. When prompted for the user name, type the operating system User ID, **rsaadmin**, and press ENTER.
4. When prompted for the password, type the rsaadmin operating system account password, and press ENTER.

Run Clam Antivirus Software

Each RSA Authentication Manager instance includes Clam Antivirus (ClamAV) software. ClamAV is an open-source software toolkit that is intended to reduce the risk of intrusion or malicious system or data access. Apply software updates to ClamAV only as part of RSA-delivered updates. You are responsible for updating antivirus definition files and running ClamAV in order to scan any Authentication Manager instance for known malware.

Before You Begin

- This procedure assumes a knowledge of Linux commands.
- For the operating system account User ID **rsaadmin**, obtain the operating system password.
- To access the operating system with a secure shell (SSH) client, you must enable SSH. You can also access the operating system on a virtual appliance in the VMware vSphere client. For instructions on using SSH, see Enable SSH on the Appliance on page 403.

Procedure

1. On each instance in your deployment, use an SSH client (or the VMware vSphere client for a virtual appliance) to access the operating system.
2. Log on to the appliance operating system with the user name, **rsaadmin**, and the operating system password.
3. Update the antivirus definition files. Choose one of the following procedures:
   - If the Authentication Manager instance has access to the Internet, you can automatically download and apply the latest antivirus definition files. Type the following command:

     ```
     sudo /usr/bin/freshclam
     ```

   - If the Authentication Manager instance does not have access to the Internet, manually download the **main.cvd** and **daily.cvd** antivirus definition files from the ClamAV web site: **http://www.clamav.net/**.

     Copy the files into the **/var/lib/clamav/** directory on the instance.
4. To scan files and directories for viruses manually, type the following line:

   ```
   sudo clamscan -r / --exclude-dir=/proc --exclude-dir=/sys
   --exclude-dir=/opt/rsa/am/rsapgdata
   --follow-dir-symlinks=0 --follow-file-symlinks=0
   --log=/var/log/clamav.log
   ```

   To schedule automatic virus scans, create a **cron** job that runs the same command.
5. Check the scan results in **/var/log/clamav.log**.

RSA Authentication Manager Services

All RSA Authentication Manager services that are required for product functionality are started automatically. You can also manage these services manually.

RSA Authentication Manager Services That Start Automatically

The following table lists the Authentication Manager services that start automatically.

Service Name	Description	Details
console	RSA Console Server	Hosts the Security Console and the Self-Service Console.
biztier	RSA Runtime Server	
admin	RSA Administration Server with Operations Console	Hosts the Operations Console.
db	RSA Database Server	
primary_replication	RSA Replication (Primary)	Runs on the primary instance only.
replica_replication	RSA Replication (Replica)	Runs on the replica instance only.
radius	RSA RADIUS Server	
radiusoc	RSA RADIUS Server Operations Console	

For security purposes, the appliance does not start the SSH service automatically. Before you can log on to the appliance operating system using an SSH client, you must enable SSH in the Operations Console. For more information, see Log On to the Appliance Operating System with SSH on page 404.

Manage RSA Authentication Manager Services Manually

Use the following procedure to manage RSA Authentication Manager services manually. You can perform the following actions on a selected service or on all services at the same time:

- Stop
- Start
- Display current status
- Restart

Procedure

1. Use an SSH client (or the VMware vSphere client for a virtual appliance) to log on to the appliance with the User ID **rsaadmin** and the current operating system password. For instructions, see Log On to the Appliance Operating System with SSH on page 404.
2. Change the directory. Type:

   ```
   cd /opt/rsa/am/server
   ```

   and press ENTER.
3. Run a command. Type the following, and press ENTER:

   ```
   ./rsaserv stop|start|status|restart [service name]
   [nodep] [exclude service name]
   ```

   where:

   - *stop*, *start*, *status*, *restart*, *and nodep* are options for managing the RSA service. Use *nodep* if you do not want to start dependent services. Use *exclude* and the *service name* to exclude that service from the command.
   - *service name* is the name of the Authentication Manager service that you want to manage.

   Service names:

   all (All RSA services)
   console (RSA Console Server)
   biztier (RSA Runtime Server)
   admin (RSA Administration Server with Operations Console)
   db (RSA Database Server)
   primary_replication (RSA Replication Primary)
   replica_replication (RSA Replication Replica)
   radiusoc (RSA RADIUS Server Operations Console)
   radius (RSA RADIUS Server)

   Examples:

   To start all services, use the following command:

   ```
   ./rsaserv start all
   ```

   To restart the database server without restarting any dependent services, use the following command:

   ```
   ./rsaserv restart db nodep
   ```

   To stop all RSA services except for the RSA Administration services, use the following command:

   ```
   ./rsaserv stop all exclude admin
   ```

4. When you are done, type:

   ```
   exit
   ```

   and press ENTER.

Super Admin Restoration

The Super Admin role is a predefined administrative role and the only role with full administrative permission for the entire deployment. A Super Admin can:

- Delegate roles to all other administrators.
- Create the security domain hierarchy.

The Super Admin is created during deployment. Only a Super Admin can perform certain critical tasks. A deployment must have at least one Super Admin.

If a Super Admin is deleted, use the Super Admin Restoration utility, restore-admin, to create a new Super Admin. RSA recommends that you assign the Super Admin role to only the most trusted administrators.

You need to restore a Super Admin if any of the following conditions exist:

- The sole Super Admin has been deleted from the deployment.
- No users have been assigned the Super Admin role.
- The sole Super Admin has been locked out.

If a Super Admin has been locked out, recovery can occur in any of the following ways:

- Another Super Admin can manually unlock the Super Admin.
- If the lockout policy that applies to the Super Admin allows auto-unlock, you can wait for lockout to expire.
- If the previous methods fail, use the Super Admin Restoration utility. For instructions, see Restore the Super Admin on page 408.

Restore the Super Admin

Use this procedure to restore the Super Admin user to a deployment using the Super Admin Restoration utility, restore-admin.

The Super Admin Restoration utility is used to restore access to the deployment in an emergency. By default, the lifetime for the Super Admin account that you create with this utility is 24 hours. The password you specify when creating this Super Admin is not validated by the default password policy. Instead, the password is validated by the initial password policy that is applied during Quick Setup. This initial password policy requires between 8 and 32 characters, at least one alphabetic character, and at least one special character, excluding spaces, @, and ~. RSA recommends as a best practice that you create a password that conforms to the current default password policy when you use this utility.

Although it is possible to enter the Operations Console administrator credentials on the command line along with the other options, this creates a potential security vulnerability. RSA recommends that you enter the password only when the utility presents a prompt.

Before You Begin

- You must be familiar with the Linux operating system.
- Do not perform this procedure on a replica instance.
- You must enable SSH through the Operations Console (OC). This provides access to the Operating System (OS) shell command prompt.
- You must have OS login credentials (rsaadmin login ID and password). These credentials allow you to login to the OS and access the OS shell command prompt.
- You must have OC credentials. These are required to execute the restore-admin command.

Procedure

1. Use an SSH client (or the VMware vSphere client for a virtual appliance) to log on to the appliance with the User ID **rsaadmin** and the current operating system password. For instructions, see Log On to the Appliance Operating System with SSH on page 404.
2. Change directories to **/opt/rsa/am/utils**.
3. Type:

   ```
   ./rsautil restore-admin -u newadmin -p adminpassword
   ```

   where:

   - *newadmin* is the User ID for the new Super Admin.
   - *adminpassword* is the password for the new Super Admin. The password requires between 8 and 32 characters, at least one alphabetic character, and at least one special character, excluding spaces, @, and ~.

   and press ENTER.
4. When prompted for the Operations Console Administrator username, enter the Operations Console administrator User ID, and press ENTER.
5. When prompted, enter the Operations Console administrator password, and press ENTER.
6. When prompted with **Are you sure you want to continue? (Y/N)**, type **Y**, and press ENTER.

Next Steps

The Super Admin Restoration utility also resets the Security Console authentication policy to LDAP_Password/RSA Password. In order for this change to take effect, use the Operations Console to flush the cache. For instructions, see Flush the Cache on page 369.

RSA Authentication Manager Updates

RSA issues product updates periodically for RSA Authentication Manager in the form of patches and service packs. RSA recommends applying product updates as they become available to ensure that the deployment is secure and efficient. For each product update, RSA provides release notes that contain important information about applying the update. To avoid problems, you should read all of the information in the release notes before you apply the update.

To receive e-mail notifications of new product updates, log on to **RSA SecurCare Online** and subscribe to RSA SecurCare Notes & Security Advisories for Authentication Manager.

You download product updates from **RSA SecurCare Online**. Updates are provided in the form of an ISO image. RSA recommends that you do not burn the ISO image to a physical DVD or CD. Instead, save the ISO image in a directory that is accessible to the deployment.

You use the Operations Console to apply product updates on each primary and replica instance. After you download a product update, you specify the location of the ISO image. You can apply an individual update through your local browser, or you can scan for stored updates in an NFS share, a Windows shared folder, or a DVD/CD. After scanning, you can select an individual update to apply.

Note: Apply updates to embedded third-party products only as part of RSA-delivered updates. For example, RSA provides the required updates to the virtual appliance and hardware appliance operating system.

If the deployment includes a web tier, you must update the web tier when you update the version of Authentication Manager. Authentication Manager displays an update button in the Operations Console for each web tier that is not up-to-date. For instructions, see Update the Web-Tier on page 178.

View Software Version Information

Procedure

In to the Security Console, click **Software Version Information**.

Verify an IP Address or Hostname

Use the Operations Console to run operating system commands to verify an IP address or hostname.

Procedure

In to the Operations Console home page, click **Administration** > **Network** > **Network Tools**.

For more information, see the Operations Console Help topic, "Verify an IP Address or Hostname."

17 Administering Trusted Realms

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.

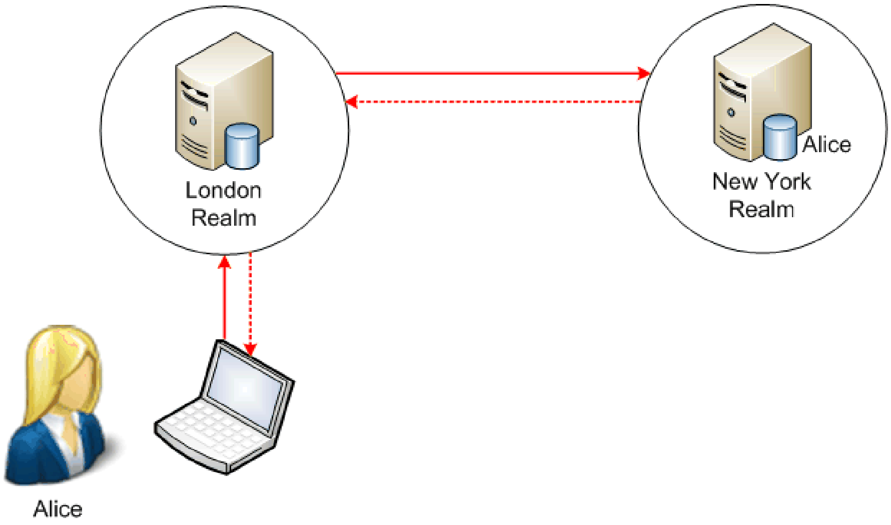
You create a trust relationship by performing the following tasks:

- 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.

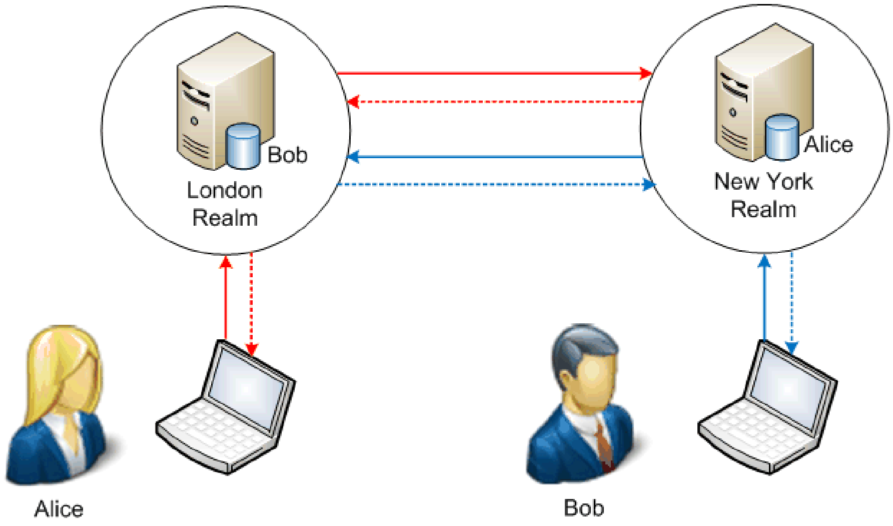
For example, if the trust relationship between London and New York is one way, either trusted London users can authenticate on New York or trusted New York users can authenticate on London. In a two-way trust, trusted users on each realm can authenticate on the other. For example, if the trust relationship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



Creating a Trust Relationship

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. You use the Security Console to create and manage trust relationships between these realms:

- Two Authentication Manager 8.0 or 8.1 realms
- An Authentication Manager 8.0 or 8.1 realm and an Authentication Manager 7.1 realm

Procedure

1. Add a trusted realm. For instructions, see Add a Trusted Realm on page 415.
2. Configure an agent for trusted realm authentication. For instructions, see Configure an Agent for Trusted Realm Authentication on page 416.
3. Add a trusted user. For instructions, see Add a Trusted User on page 419.
4. (Optional) Add a trusted user group. For instructions, see Add a Trusted User Group on page 420.
5. (Optional) Add trusted users to a trusted user group. For instructions, see Add Trusted Users to a Trusted User Group on page 420.

Add a Trusted Realm

You create a trust relationship by adding an external realm as a trusted realm. A trust relationship allows users to authenticate between these realms:

- Two RSA Authentication Manager 8.0 or 8.1 realms
- An Authentication Manager 8.0 or 8.1 realm and an Authentication Manager 7.1 realm

Before You Begin

- You and the administrator of the realm you are adding as a trusted realm need to perform this procedure at the same time.
- You and the administrator of the realm you are adding as a trusted realm need to be able to communicate while you perform this procedure.

Procedure

1. In the Security Console, click **Administration** > **Trusted Realms** > **Add New**.
2. Under **Generate Trust Package**, click **Generate & Download**.
3. After the trust package is generated, use a secure method to exchange your trust package with the trust package from the trusted realm administrator. Wait until you receive the trust package before you continue.
4. In the **Trust Package from Trusted Realm** field, enter the path to the trust package that you just received by browsing to the package file, and click **Open**.
5. Click **Next**.

6. Verify the trust package confirmation codes with the trusted realm administrator. Go to the next step only after verifying the confirmation codes.
7. Click **Confirm and Next**.
8. In the **Trusted Realm Name** field, enter a unique, user-friendly name that identifies the trusted realm, for example, London office.
9. For **Authentication Status**, select **Authenticate Trusted Users** if you want your realm to authenticate users from the trusted realm.
10. For **Trusted Realm Status**, select **Enable Trusted Realm**. When enabled, your realm can send authentication requests to the trusted realm.
11. For **Create Trusted Users in Security Domain**, select the security domain that will own users from the trusted realm.

    After your realm authenticates users from the trusted realm, the users must belong to a security domain in your realm. The security domain that you select must be configured to use the internal database as an identity source.
12. In the **Trusted User Name Identifier** field, enter a unique identifier that your realm can recognize for the trusted user, and click **Add**. The unique identifier could be the user's domain name or e-mail address, such as jsmith@company.com. The value must be unique among trusted realms.

    For example, suppose John Smith from Realm A is jsmith in his local realm. Your realm does not know the identity of jsmith. If you enter yourcompany.com in this field, John Smith will be identified within your realm as jsmith@yourcompany.com.
13. Click **Save**.
14. In the Security Console, click **Administration** > **Trusted Realms** > **Manage Existing**.
15. Test the network connection between the trusted realms. Click the name of the trusted realm, and from the context menu, select **Test Trusted Realm**.

Next Step

Before trusted realm authentication can take place, you must enable an agent to process authentication requests from trusted users. For more information, see Configure an Agent for Trusted Realm Authentication on page 416.

Configure an Agent for Trusted Realm Authentication

You must specify which authentication agents are available for trusted realm authentication.

On each agent in your realm, you specify one of the following:

- Not open to trusted users
- Open to all trusted users
- Open only to trusted users in trusted user groups

For a one-way trust, the trusted realm administrator enables the agents for authentication in the trusted realm. For a two-way trust, you and the trusted realm administrator enable the agents in both your realms.

Before You Begin

- Add a trusted realm. For instructions, see Add a Trusted Realm on page 415.
- Create a new agent configuration file that specifies 25 seconds for a response from the server.

  For instructions on creating a new agent configuration file, see the Security Console Help topic "Generate the Authentication Manager Configuration File."

Procedure

1. In the Security Console, click **Access** > **Authentication Agents** > **Manage Existing**.
2. Use the search fields to find the agent that you want to configure.
3. From the search results, click the authentication agent that you want to configure.
4. From the context menu, click **Edit**.
5. Do one of the following:
   - If you do not want trusted users to access this agent:
     a. Under Trusted Realm Settings, ensure that **Enable Trusted Realm Authentication** is not selected.

     b. Click **Save**.
   - If you want trusted users to access this agent:
     a. Under **Trusted Realm Settings**, select **Enable Trusted Realm Authentication**.

     b. For **Trusted User Authentication**, select one of the following:

     – **Open to all Trusted Users**. This option automatically designates users from a trusted realm as trusted users after successful authentication.

     – **Only Trusted Users in Trusted User Groups with access to the agent can authenticate**. These trusted users and trusted user groups are manually created by the administrator.

     c. Click **Save**.

Duplicate Agent Record for Access Control

You can control which users have access to an authentication agent in the trusted realm by adding a duplicate authentication record of the agent in the trusted realm. A duplicate authentication record allows you to restrict user access to members of a group. Only the users you assign to this group are able to access the agent in the trusted realm.

For example, suppose that you are the London administrator for a company that has a trusted relationship between two realms: New York and London. The New York realm has an unrestricted VPN agent called “VPN1.” You want to restrict which London users can access VPN1, so you create a duplicate agent record of this agent record, also called “VPN1,” in the London realm. This agent record contains the same data as the agent record in the New York realm, including IP address. You make VPN1 a restricted agent, and create a user group called “VPN users.” Only London members of VPN users have permission to access VPN1 in New York.

You assign the user “jsmith” to the VPN users group. When jsmith travels to New York and attempts to access VPN1 on the New York realm, the New York realm does not recognize the user jsmith, and forwards the following information to the London realm: user name, agent name, and passcode. The London realm recognizes the user name and agent name, and immediately checks to see if the agent is restricted. Because the agent is restricted, and jsmith is a member of VPN users, the authentication request is approved and the New York realm allows jsmith to authenticate.

If you create a duplicate agent record, it is important to know if the corresponding agent in the trusted realm has trusted user groups. If a trusted user group in the duplicate agent record does not contain the same users as the group on the agent on the trusted realm, users might not be able to authenticate. Note the following:

- In the above example, assume that VPN1 in the trusted realm has a trusted user group associated with it. If jsmith is not a member of the trusted user group, he cannot authenticate, even though he is a member of his realm’s corresponding user group.
- In the above example, assume that a second London user, “sbrown,” is a member of the trusted user group, but is not a member of his realm’s corresponding user group. Despite being a member of the trusted user group, sbrown cannot authenticate because his realm has not given him access to the agent.

Duplicate Agent Record for Resolving Aliases

If you use aliases for user groups, users might attempt to log on to an authentication agent in the trusted realm using their aliases. To ensure successful authentications in this case, add a duplicate record of the agent in the trusted realm with associated user groups and aliases to your realm.

For example, suppose that your realm has a restricted VPN agent, “VPN2.” Only members of the VPN2 user group can access VPN2. In that user group, users have aliases, a special user name they use just for VPN2. For example, the user “jdoe” has the alias “jdoeVPN,” which he uses when he logs on to VPN2.

If jdoe attempts to authenticate to the trusted realm’s VPN agent, “VPN1” using his alias, “jdoeVPN,” the trusted realm does not recognize jdoe and sends his user name and agent information back to jdoe’s realm. Jdoe’s realm does not recognize the agent “VPN1” or the user name “jdoeVPN.” Therefore, access is denied and the user cannot authenticate.

If jdoe’s realm has a duplicate agent record, also called “VPN1” and VPN1 has an associated user group where jdoe is a member and has “jdoeVPN” as his alias, the problem is solved. Now when “jdoeVPN” tries to access VPN1 in the trusted realm, the trusted realm forwards the user name and agent information back to jdoe’s realm. Jdoe’s realm recognizes the agent name and the alias. Now jdoe can authenticate successfully.

Add a Trusted User

Only trusted users can access the agents enabled for trusted realm authentication. An authentication agent can be configured to automatically designate all users from a trusted realm as trusted users. You can manually add trusted users if more restriction is necessary. When you manually add trusted users, only the users you add are trusted users.

Before You Begin

- Add a trusted realm. For instructions, see Add a Trusted Realm on page 415.
- Configure an agent for trusted realm authentication. For instructions, see Configure an Agent for Trusted Realm Authentication on page 416.

Procedure

1. In the Security Console, click **Administration** > **Trusted Realms** > **Trusted Users** > **Add New**.
2. In the **Trusted User ID** field, enter the user's User ID.
3. From the **Trusted Realm Name** drop-down menu, select the trusted realm where the user belongs.
4. From the **Security Domains** drop-down menu, select the security domain where the policies for this trusted user are managed.

   Only administrators whose administrative scope includes the security domain you select can manage the user.
5. In the **Default Shell** field, enter the shell that users employ to access a UNIX machine.
6. Click **Save**.

Allow Trusted Users to Authenticate Using RSA RADIUS

To allow trusted users to authenticate using RSA RADIUS, you define these trusted users on the trusted realm before they authenticate. You may also set up a special RADIUS profile for trusted users.

For more details about configuring RADIUS to handle trusted users, see Trusted User Assignment on page 307.

For more information on associating trusted users with RADIUS attributes, see Map a RADIUS User Attribute Definition to an Identity Source Attribute on page 313.

Add a Trusted User Group

A trusted user group restricts access to an agent that is enabled for trusted realm authentication. When you create a trusted user group and enable associated agents, only members of the trusted user group can access that authentication agent.

By adding a trusted user group, only users who have a business need to access the resources protected by the agent are allowed to authenticate. For example, by creating a trusted user group for human resource workers, you can limit access to personnel records to those in the group.

Before You Begin

- Add a trusted realm. For instructions, see Add a Trusted Realm on page 415.
- Configure an agent for trusted realm authentication. For instructions, see Configure an Agent for Trusted Realm Authentication on page 416.

Procedure

1. In the Security Console, click **Administration** > **Trusted Realms** > **Trusted User Groups** > **Add New**.
2. In the **Trusted User Group Name** field, enter a unique name for the trusted user group.

   The trusted user group name must not exceed 255 characters.
3. From the **Security Domain** drop-down menu, select the security domain select the security domain where the policies for this trusted user group are managed.

   Only administrators whose administrative scope includes the security domain you select can manage the trusted user group.
4. Click **Save**.

Add Trusted Users to a Trusted User Group

A trusted user group restricts access to an agent that is enabled for trusted realm authentication. When you create a trusted user group, only members of the trusted user group can access the agent that is enabled for trusted realm authentication.

You can add new trusted users to an existing trusted user group.

Procedure

1. In the Security Console, click **Administration** > **Trusted Realms** > **Trusted User Groups** > **Manage Existing**.
2. Use the search fields to find the trusted user group where you are adding users.
3. From the search results, click the trusted user group name.
4. From the context menu, click **Add More**.
5. Select the checkbox next to the trusted users that you want to add.
6. Click **Add to Trusted User Group**.

Creating a Trust Relationship with a Legacy Realm

You can create a trust relationship between an RSA Authentication Manager 8.0 or 8.1 realm and an RSA Authentication Manager 6.1 legacy realm by enabling cross-realm authentication.

Procedure

1. Enable cross-realm authentication on the Authentication Manager 6.1 deployment.

   For instructions, see the chapter "Realm Administration" in the *RSA Authentication Manager 6.1 Administrator's Guide*.

2. After you enable cross realm authentication, you must configure the ports that Authentication Manager 8.0 or 8.1 uses to authenticate to the trusted legacy realm.

   For instructions, see Configure Ports for Trusted Legacy Realm Authentication on page 421.

   Note: Trust relationships between RSA Authentication Manager 8.0 or 8.1 and RSA Authentication Manager 6.1 realms do not support authentications using RSA_RADIUS.

Configure Ports for Trusted Legacy Realm Authentication

When you enable cross realm authentication between an RSA Authentication Manager 6.1 legacy realm and Authentication Manager 8.0 or 8.1, you must configure a port range that Authentication Manager 8.1 uses for authentication. You configure this port range with the Security Console, which has the following defaults:

- 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 8.0 or 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.

Before You Begin

Enable cross-realm authentication on the Authentication Manager 6.1 deployment.

Procedure

1. In the Security Console, click **Setup** > **System Settings**. Under **Advanced Settings**, click **Ports for Legacy Cross (Trusted) Realms**.
2. On the Ports for Legacy Cross (Trusted) Realms page, for **Port Range**, accept the default settings, or enter new minimum and maximum port numbers. At least 10 ports are required.
3. Click **Save**.

Next Steps

Reboot the appliance to enable the port settings. For instructions, see Reboot the Appliance on page 366.

Trusted Relationship Repair

When you restore an RSA Authentication Manager 8.1 primary instance on a machine with a new hostname or perform a migration, and you had a trust relationship previously with another realm, the following trust relationships must be repaired:

- **Trusted Realm.** A trust relationship between two Authentication Manager 8.0 or 8.1 deployments or between an Authentication Manager 8.0 or 8.1 and an Authentication Manager 7.1 deployment. For instructions, see Repair a Trust Relationship with a Version 8.0 or 8.1 Realm on page 390 or Repair a Trust Relationship with a Version 7.1 Realm on page 392.

  For a trusted realm, the repair process ensures that the original trusted realm information, such as trusted users and groups, is preserved. The process is similar to adding a trusted realm. Both the administrator of the migrated or restored version 8.0 or 8.1 deployment, and the administrator of the version 8.0, 8.1, or 7.1 deployment participate in the repair process. However, only the administrator of the previously trusted realm imports a trust package. The administrator of the migrated or restored deployment provides a trust package to the administrator of the deployment where the trust will be repaired. This package is used to repair the trusted realm.

- **Cross Trust.** A legacy trust relationship between a version 8.0 or 8.1 and a version 6.1 deployment. For instructions, see Repairing a Trusted Legacy Realm on page 395.

  For a legacy trust relationship, the repair process requires updating the host name and IP address in the realm record on the Authentication Manager 6.1 deployment.

A Changing the Instance Network Settings

Primary or Replica Instance Network Settings Updates

In the Operations Console, you can update the network settings for an RSA Authentication Manager primary or replica instance. The IPv4 network settings created during Quick Setup are used for most purposes. In a replicated deployment, if you change the IPv4 hostname or IP address on the primary instance, you must use the Operations Console to update the replica instance with the new information. You can create IPv6 network settings to support IPv6-compliant agents.

Authentication Manager supports dual network interface card (NIC) configurations. All Authentication Manager services are available on both NICs. For example, you can use one Authentication Manager deployment to authenticate users from two networks by configuring the agents on each network to send authentication requests to different NICs.

Advanced administrators can log on to an instance and run commands that create IPv4 and IPv6 static routes. Static routes send data through a network on a fixed, predictable path. Both persistent and non-persistent static routes are supported.

If the primary or replica instance IPv4 network settings are incorrect and you cannot access the Operations Console, you can log on to the appliance operating system and change the settings. On a virtual appliance use the VMware vSphere Client. On a hardware appliance, use Secure Shell (SSH).

Note: Network setting recovery procedures require knowledge of an operating system-level Linux text editor, such as the vi editor.

If you cannot access the hardware appliance operating system to correct the network settings, you can perform a factory reset. A factory reset restores the hardware appliance to a pre-configured state. For more information, see Factory Reset on page 396.

For instructions on how to update the primary or replica instance network settings, see the following procedures:

- Change the Primary Instance IPv4 Network Settings on page 426
- Update the Primary Instance Hostname and IP Address on a Replica Instance on page 430
- Change the Replica Instance IPv4 Network Settings on page 430
- Create IPv6 Network Settings on a Primary or Replica Instance on page 455

Advanced administrative tasks require you to log on to the appliance operating system. For more information, see the following topics:

- Static Routes on page 434
- Recovery from Incorrect Network Settings on page 442

Change the Primary Instance IPv4 Network Settings

You can change the IPv4 network settings that were created during Quick Setup, such as the subnet mask, default gateway, hostname or IP address. There are several reasons why you might need to change the network settings. For example, you might need to change the IP address to resolve an IP address conflict with another resource, you might need to change the subnet mask when the network is reorganized, or you might need to change network settings when you move an appliance from one data center to another.

Before You Begin

- Users are unable to authenticate on this instance while you perform this procedure, and some administrative features are not available. Plan to perform this procedure at a time when the absence of authentication service is minimally disruptive.
- Changing the hostname for a single primary instance in a deployment with a web tier requires you to reinstall the web tier. In a replicated deployment, the web tier automatically obtains the updated hostname.
- You must be an Operations Console administrator.
- If you change the primary instance hostname or IP address in a replicated deployment, Super Admin credentials are required for the Next Steps.

Procedure

1. On the primary instance, log on to the Operations Console.
2. Click **Administration > Network > Appliance Network Settings**.
3. Under Global Settings, configure the following:
   - In the **Fully Qualified Domain Name** field, modify the fully qualified domain name (FQDN).
   - For **DNS Servers**, add, update or remove an IP address from the list of IP addresses for DNS servers.
     – To add an IP address, enter the IP address in the **DNS Server IP Address** field and click **Add**.
     – To update an IP address, select the IP address from the list, modify the IP address in the **DNS Server IP Address** field and click **Update**.

  - To remove an IP address, select the IP address form the list and click **Remove**.
  - To change the order in which the DNS servers are used, select an IP address and click the up or down arrow.

  You may enter multiple IP addresses, and specify the order. Authentication Manager submits DNS lookup queries to the DNS servers in the order listed.

- For **DNS Search Domains**, add, update or remove a domain from the list of DNS search domains.
  - To add a search domain, enter the name of the domain in the **DNS Search Domain** field and click **Add**.
  - To update a search domain, select the name of the domain from the list, modify the name in the **DNS Search Domain** field and click **Update**.
  - To remove a search domain, select the domain from the list and click **Remove**.
  - To change the order in which the domains are searched, select the domain and click the up or down arrow.

  You may enter multiple search domains, and specify the order. Authentication Manager uses the search domains in the order listed.

4. For each network interface card (NIC) that you want to use, configure the following:

   a. In the **IPv4 Address** field, modify the IP address.

   b. In the **IPv4 Subnet Mask** field, modify the subnet mask.

   c. In the **IPv4 Default Gateway** field, modify the IP address.

   To configure an additional NIC, select the **Enabled** checkbox under the name of the NIC, and configure the settings. For a virtual appliance, the Appliance Network Settings page displays an additional NIC only after you add the NIC on the virtual machine hosting the appliance.

   RSA recommends using a different subnet for each NIC. If two NICs share the same subnet and one NIC becomes unavailable, then Authentication Manager services will not be available on either NIC.

   Note: Configure IPv6 Settings only if your deployment contains authentication agents that use the IPv6 protocol. The IPv6 settings contain an additional field, **IPv6 Prefix**.

5. Click **Next**. The Operations Console displays a review page.
6. Review the changes you made, highlighted in bold and italic. Click **Apply Network Settings** to accept the changes, click **Back** to make additional changes, or click **Cancel**.

   To apply the changes, Authentication Manager restarts the system-level networking service. If you changed the hostname or IP address, Authentication Manager restarts additional services. After the services are running, the Operations Console and the Security Console are available at the new hostname and IP address.

Next Steps

Complete these tasks after changing your primary instance hostname or IP address. If you change both the hostname and the IP address, you must perform all of the tasks that apply to your deployment. Changes to other network settings, such as the subnet mask, do not require these additional tasks.

Task	Hostname Change Requirement	IP Address Change Requirement
Update the DNS server with the new hostname or IP address.	Yes	Yes
Verify that the hostname used to access the RSA Consoles (Operations Console, Security Console, and Self-Service Console) resolves to the new IP address.	No	Yes
In a replicated deployment, after updating your DNS server, you must log on to the replica instance Operations Console and update the primary instance hostname and IP address on the replica instance. A replica instance requires the primary instance hostname and IP address in order to communicate with the primary instance. For instructions, see Update the Primary Instance Hostname and IP Address on a Replica Instance on page 430.	Yes	Yes
If you installed an SSL certificate that is signed by a third-party certificate authority (CA), changing the hostname causes the deployment to revert to the SSL certificate signed by the RSA Authentication Manager CA that is enabled when the instance is deployed. To install a new SSL certificate, import a new SSL certificate that is signed by the third-party certificate authority and whose common name (CN) is the new hostname. See the Operations Console Help topic "Replacing the Console Certificate."	Yes	No
Configure authentication agents to communicate with the new IP address. Generate a new configuration file, **sdconf.rec**, and deploy it to all authentication agents. For instructions, see Generate the Authentication Manager Configuration File on page 65. If you want agents to communicate with the IP address of an additional NIC, you must configure the IP address of the additional NIC as an alternate IP address. For more information, see the Security Console Help topic "Add Alternate Agent IP Addresses for Servers."	No	Yes

Task	Hostname Change Requirement	IP Address Change Requirement
Repair any trusted realm relationships. For instructions, see Repair a Trust Relationship with a Version 8.0 or 8.1 Realm on page 390.	Yes	No
If you changed that hostname in a replicated deployment that includes a web tier, the web tier obtains the primary instance hostname from a replica instance. After you update the primary instance hostname on every replica instance, wait five minutes for the web tier to update. You can then make additional replica instance hostname changes as needed.	Required in a replicated deployment.	No
If you changed the hostname for a single primary instance and your deployment includes a web tier but no replica instances, you must reinstall the web tier. For instructions, see the chapter "Installing Web Tiers" in the *Setup and Configuration Guide*.	Required if there is only one Authentication Manager instance	No
Update any other external clients, such as RADIUS and SNMP, to use the new IP address. Changing the IP address for the primary instance also updates the RADIUS IP address. Reconfigure RADIUS clients so that they send requests to the new IP address.	No	Yes
Update any external clients, such as RADIUS clients and SNMP, to use the new hostname.	Yes	No
If your deployment includes a replica instance, check the replication status for the primary instance. Synchronize the replica instance if necessary. For instructions, see the Operations Console Help topic "Synchronize a Replica Instance."	Yes	Yes
Check the replication status for RADIUS. For instructions, see Initiate Replication to RADIUS Replica Servers on page 294.	Yes	Yes

Update the Primary Instance Hostname and IP Address on a Replica Instance

Replica instances use the primary instance IPv4 hostname and IP address to communicate with the primary instance. If you change the primary instance hostname or IP address, you must provide the new network settings to each replica instance in the deployment.

Before You Begin

You must be a Super Admin.

Procedure

1. On the replica instance, log on to the Operations Console.
2. Click **Administration** > **Network** > **Update Primary Hostname**.
3. If prompted, enter your Super Admin User ID and password.
4. In the **Primary Hostname** field, enter the primary instance hostname.
5. Click **Test Connection**. The system resolves the hostname, and updates the **Primary IP Address field**, if necessary.
6. Click **Save**.

Change the Replica Instance IPv4 Network Settings

You can change the replica instance IPv4 network settings, such as the subnet mask, default gateway, hostname or IP address. There are several reasons why you might need to change the network settings. For example, you might need to change the IP address to resolve an IP address conflict with another resource, you might need to change the subnet mask when the network is reorganized, or you might need to change network settings when you move an appliance from one data center to another.

Before You Begin

- Users cannot authenticate on this instance while you perform this procedure, and some administrative features are not available. Plan to perform this procedure at a time when the absence of authentication service is minimally disruptive.
- You must be a Super Admin.

Procedure

1. On the replica instance, log on to the Operations Console.
2. Click **Administration** > **Network** > **Appliance Network Settings**.

3. Under Global Settings, configure the following:
   - In the **Fully Qualified Domain Name** field, modify the fully qualified domain name (FQDN).
   - For **DNS Servers**, add, update or remove an IP address from the list of IP addresses for DNS servers.
     - To add an IP address, enter the IP address in the **DNS Server IP Address** field and click **Add**.
     - To update an IP address, select the IP address from the list, modify the IP address in the **DNS Server IP Address** field and click **Update**.
     - To remove an IP address, select the IP address form the list and click **Remove**.
     - To change the order in which the DNS servers are used, select an IP address and click the up or down arrow.

     You may enter multiple IP addresses, and specify the order. Authentication Manager submits DNS lookup queries to the DNS servers in the order listed.
   - For **DNS Search Domains**, add, update or remove a a domain from the list of DNS search domains.
     - To add a search domain, enter the name of the domain in the **DNS Search Domain** field and click **Add**.
     - To update a search domain, select the name of the domain from the list, modify the name in the **DNS Search Domain** field and click **Update**.
     - To remove a search domain, select the domain from the list and click **Remove**.
     - To change the order in which the domains are searched, select the domain and click the up or down arrow.

     You may enter multiple search domains, and specify the order. Authentication Manager uses the search domains in the order listed.
4. For each network interface card (NIC) that you want to use, configure the following:

   a. In the **IPv4 Address** field, modify the IP address.

   b. In the **IPv4 Subnet Mask** field, modify the subnet mask.

   c. In the **IPv4 Default Gateway** field, modify the IP address.

   To configure an additional NIC, select the **Enabled** checkbox under the name of the NIC, and configure the settings. For a virtual appliance, the Appliance Network Settings page displays an additional NIC only after you add the NIC on the virtual machine hosting the appliance.

   RSA recommends using a different subnet for each NIC. If two NICs share the same subnet and one NIC becomes unavailable, then Authentication Manager services will not be available on either NIC.

   Note: Configure IPv6 Settings only if your deployment contains authentication agents that use the IPv6 protocol.

5. Click **Next**. The Operations Console displays a review page.
6. Review the changes you made, highlighted in bold and italic. Click **Change Network Settings** to accept the changes, click **Back** to make additional changes, or click **Cancel**.
7. Select **Yes, change network settings**, and click **Change Network Settings.**

   To apply the changes, Authentication Manager restarts the system-level networking service. If you changed the hostname or IP address, Authentication Manager restarts additional services. After the services are running, the Operations Console and the Security Console are available at the new hostname and IP address.

Next Steps

Complete these tasks after changing your replica instance hostname or IP address. If you change both the hostname and the IP address, you must perform all of the tasks that apply to your deployment. Changes to other network settings, such as the subnet mask, do not require these additional tasks.

Task	Hostname Change Requirement	IP Address Change Requirement
Update the DNS server with the new hostname or IPv4 address.	Yes	Yes
Verify that the hostname used to access the Consoles (Operations Console, Security Console, and the Self-Service Console) resolves to the new IP address.	No	Yes
If you installed an SSL certificate that is signed by a third-party certificate authority (CA), changing the hostname causes the deployment to revert to the SSL certificate signed by the RSA Authentication Manager CA that is enabled when the instance is deployed. To install a new SSL certificate, import a new SSL certificate that is signed by the third-party certificate authority and whose common name (CN) is the new hostname. See the Operations Console Help topic "Replacing the Console Certificate."	Yes	No
Configure authentication agents to communicate with the new IP address. Generate a new configuration file, **sdconf.rec**, and deploy it to all authentication agents. For instructions, see Generate the Authentication Manager Configuration File on page 65. If you want agents to communicate with the IP address of an additional NIC, you must configure the IP address of the additional NIC as an alternate IP address. For more information, see the Security Console Help topic "Add Alternate Agent IP Addresses for Servers."	No	Yes

Task	Hostname Change Requirement	IP Address Change Requirement
Repair any trusted realm relationships. For instructions, see Repair a Trust Relationship with a Version 8.0 or 8.1 Realm on page 390.	Yes	No
Wait five minutes for the web tier to update. You can then make additional hostname changes as needed. In a replicated deployment, the web tier obtains the replica instance hostname from the primary instance. The waiting period allows the web tier to maintain communication with the Authentication Manager instances.	Yes	No
Update any other external clients, such as RADIUS and SNMP, to use the new IP address. Changing the IP address for the replica instance also updates the RADIUS IP address. Reconfigure RADIUS clients so that they send requests to the new IP address.	No	Yes
Update any external clients, such as RADIUS clients and SNMP, to use the new hostname.	Yes	No
Check the replication status for the replica instance, and synchronize the replica instance if necessary. For instructions, see the Operations Console topic "Synchronize a Replica Instance."	Yes	Yes
Check the replication status for RADIUS. For instructions, see Initiate Replication to RADIUS Replica Servers on page 294.	Yes	Yes

Static Routes

RSA Authentication Manager supports the creation of IPv4 and IPv6 static routes. Static routes send data through a network on a fixed, predictable path.

For example, you can create an IPv4 static route for all network traffic from an Authentication Manager instance to an Authentication Manager web tier. The default route to an internal router would be used for other network traffic from the instance. If the static route to the web tier becomes unavailable, the network traffic intended to take that route is not sent.

You can create persistent and non-persistent static routes:

- A persistent static route is not deleted if the Authentication Manager instance is rebooted or if the interface with which the static route is associated is unavailable.
- A non-persistent static route is deleted if the Authentication Manager instance is rebooted or if the interface with which the static route is associated is unavailable. A non-persistent static route might be used to test a network route, or as a temporary path if part of the network is being repaired or restored.

To add a static route, see the appropriate instructions for your network:

- Add a Persistent IPv4 Static Route on page 434
- Add a Persistent IPv6 Static Route on page 436
- Add a Non-Persistent IPv4 Static Route on page 437
- Add a Non-Persistent IPv6 Static Route on page 438

To delete a static route, see the appropriate instructions:

- Delete a Persistent IPv4 or IPv6 Static Route on page 439
- Delete a Non-Persistent IPv4 or IPv6 Static Route on page 440

Add a Persistent IPv4 Static Route

Use this procedure to add a persistent IPv4 static route.

Before You Begin

You must access the appliance operating system to add a static route. For instructions, see Troubleshooting and Advanced Administration Using the Appliance Operating System on page 403.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. To view the current routing table, type:

```
sudo ip -4 route show
```

3. To add a persistent IPv4 route entry to a network interface routing file, type:

   ```
   sudo bash -c "echo 'destination gateway subnet_mask eth0'
   >> /etc/sysconfig/network/ifroute-eth0"
   ```

   where:

   - *destination* specifies the IP address of the network or host for which you are adding a static route. Any network traffic to the destination IP address follows the route defined by the entry.
   - *gateway* specifies the IP address of the node that will route traffic to the destination network or host.
   - *subnet_mask* specifies the subnet mask associated with the destination IP address.
   - *eth0* specifies the network interface, for example, eth0 or eth1.

   For example, to add a persistent static route that sends all network traffic for any host in the 10.100.212.0 subnet (that uses the subnet mask 255.255.252.0) to the gateway 10.100.219.102, type:

   ```
   sudo bash -c "echo '10.100.212.0 10.100.219.102
   255.255.252.0 eth0' >>
   /etc/sysconfig/network/ifroute-eth0"
   ```

4. To add a persistent IPv4 route entry to the corresponding table. Type:

   ```
   sudo bash -c "echo 'destination gateway subnet_mask eth0
   table Teth0' >> /etc/sysconfig/network/ifroute-eth0 table
   Teth0"
   ```

   where:

   - *destination* specifies the IP address of the network or host for which you are adding a static route. Any network traffic to the destination IP address follows the route defined by the entry.
   - *gateway* specifies the IP address of the node that will route traffic to the destination network or host.
   - *subnet_mask* specifies the subnet mask associated with the destination IP address.
   - *eth0* specifies the network interface, for example, eth0 or eth1.
   - `Teth0` specifies the table in the network interface routing file, such as Teth0 for the interface eth0.

   For example, to add a persistent static route that sends all network traffic for any host in the 10.100.212.0 subnet (that uses the subnet mask 255.255.252.0) to the gateway 10.100.219.102, type:

   ```
   sudo bash -c "echo '10.100.212.0 10.100.219.102
   255.255.252.0 Teth0' >>
   /etc/sysconfig/network/ifroute-Teth0 table Teth0"
   ```

5. Restart the network services to apply the new static route. Type:

   ```
   sudo service network restart
   ```

   and press ENTER.

Add a Persistent IPv6 Static Route

Use this procedure to add a persistent IPv6 static route to support IPv6-compliant agents.

Before You Begin

You must access the appliance operating system to add a static route. For instructions, see Troubleshooting and Advanced Administration Using the Appliance Operating System on page 403.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. View the current routing table, type:

   ```
   sudo ip -6 route show
   ```

3. To add a persistent IPv6 route entry to a network interface routing file, type:

   ```
   sudo bash -c "echo 'destination gateway prefix_length -
   -' >> /etc/sysconfig/network/ifroute-eth0"
   ```

   where:

   - *destination* specifies the IP address of the network or host for which you are adding a static route. Any network traffic to the destination IP address follows the route defined by the entry.
   - *gateway* specifies the IP address of the node that will route traffic to the destination network or host.
   - *prefix_length* specifies the prefix length associated with the destination IP address.
   - *eth0* specifies the network interface, for example, eth0 or eth1.

   IPv6 special notation can be used. For example, to add a persistent static route that sends all network traffic for IPv6-compliant agents in the 2005::0/64 network to the gateway 2001::2, type:

   ```
   sudo bash -c "echo '2005::0 2001::2 64 - -' >>
   /etc/sysconfig/network/ifroute-eth0"
   ```

4. To add a persistent IPv6 route entry to the corresponding table, type:

   ```
   sudo bash -c "echo 'destination gateway prefix_length -
   -' >> /etc/sysconfig/network/ifroute-eth0 table Teth0"
   ```

   where:

   - *destination* specifies the IP address of the network or host for which you are adding a static route. Any network traffic to the destination IP address follows the route defined by the entry.
   - *gateway* specifies the IP address of the node that will route traffic to the destination network or host.
   - *prefix_length* specifies the prefix length associated with the destination IP address.

- *eth0* specifies the network interface, for example, eth0 or eth1.
- Teth0 specifies the table in the network interface routing file, such as Teth0 for the interface eth0.

IPv6 special notation can be used. For example, to add a persistent static route that sends all network traffic for IPv6-compliant agents in the 2005::0/64 network to the gateway 2001::2, type:

```
sudo bash -c "echo '2005::0 2001::2 64 - -' >>
/etc/sysconfig/network/ifroute-eth0 table Teth0"
```

5. Restart the network services to apply the new static route. Type:

```
sudo service network restart
```

and press ENTER.

Add a Non-Persistent IPv4 Static Route

Use this procedure to add a non-persistent IPv4 static route.

Before You Begin

You must access the appliance operating system to add a static route. For instructions, see Troubleshooting and Advanced Administration Using the Appliance Operating System on page 403.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. View the current routing table, type:

```
sudo ip -4 route show
```

3. To add a non-persistent IPv4 route to a network interface routing file, type:

```
sudo ip route add destination/nn via gateway dev eth0
```

where:

- *destination* specifies the IP address of the network or host for which you are adding a static route. Any network traffic to the destination IP address follows the route defined by the entry.
- */nn* is the prefix length notation used to specify the subnet mask associated with the destination IP address.
- *gateway* specifies the IP address of the node that will route traffic to the destination network or host.
- *eth0* specifies the network interface, for example, eth0 or eth1.

For example, to add a non-persistent static route that sends all network traffic for any host in the 10.100.212.0/22 network to the gateway 10.100.219.102, type:

```
sudo ip route add 10.100.212.0/22 via 10.100.219.102 dev
eth0
```

4. To add a non-persistent IPv4 route entry to the corresponding table, type:

   ```
   sudo ip route add destination/nn via gateway dev eth0
   table Teth0
   ```

   where:

   - `destination` specifies the IP address of the network or host for which you are adding a static route. Any network traffic to the destination IP address follows the route defined by the entry.
   - `/nn` is the prefix length notation used to specify the subnet mask associated with the destination IP address.
   - `gateway` specifies the IP address of the node that will route traffic to the destination network or host.
   - `eth0` specifies the network interface, for example, eth0 or eth1.
   - `Teth0` specifies the table in the network interface routing file, such as Teth0 for the interface eth0.

   For example, to add a non-persistent static route that sends all network traffic for any host in the 10.100.212.0/22 network to the gateway 10.100.219.102, type:

   ```
   sudo ip route add 10.100.212.0/22 via 10.100.219.102 dev
   eth0 table Teth0
   ```

5. Press ENTER. The non-persistent route takes effect immediately.

Add a Non-Persistent IPv6 Static Route

Use this procedure to add a non-persistent IPv6 static route to support IPv6-compliant agents.

Before You Begin

You must access the appliance operating system to add a static route. For instructions, see Troubleshooting and Advanced Administration Using the Appliance Operating System on page 403.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. View the current routing table, type:

   ```
   sudo ip -6 route show
   ```

3. To add a non-persistent IPv6 route to a network interface routing file, type:

   ```
   sudo ip -6 route add destination/nn via gateway dev eth0
   ```

   where:

   - `destination` specifies the IP address of the network or host for which you are adding a static route. Any network traffic to the destination IP address follows the route defined by the entry.
   - */nn* is the prefix length notation used to specify the subnet mask associated with the destination IP address.

- `gateway` specifies the IP address of the node that will route traffic to the destination network or host.
- `eth0` specifies the network interface, for example, eth0 or eth1.

IPv6 special notation can be used. For example, to add a non-persistent static route that sends all network traffic for IPv6-compliant agents in the 2005::0/64 network to the gateway 2001::2, type:

```
sudo ip -6 route add 2005::0/64 via 2001::2 dev eth0
```

4. To add a non-persistent IPv6 route entry to the corresponding table, type:

```
sudo ip -6 route add destination/nn via gateway dev eth0
table Teth0
```

where:

- *`destination`* specifies the IP address of the network or host for which you are adding a static route. Any network traffic to the destination IP address follows the route defined by the entry.
- */nn* is the prefix length notation used to specify the subnet mask associated with the destination IP address.
- *`gateway`* specifies the IP address of the node that will route traffic to the destination network or host.
- `eth0` specifies the network interface, for example, eth0 or eth1.
- `Teth0` specifies the table in the network interface routing file, such as Teth0 for the interface eth0.

IPv6 special notation can be used. For example, to add a non-persistent static route that sends all network traffic for IPv6-compliant agents in the 2005::0/64 network to the gateway 2001::2, type:

```
sudo ip -6 route add 2005::0/64 via 2001::2 dev eth0 table
Teth0
```

5. Press ENTER. The non-persistent route takes effect immediately.

Delete a Persistent IPv4 or IPv6 Static Route

Use this procedure to remove a persistent IPv4 or IPv6 static route. The following procedure uses the eth0 interface as an example. To remove a persistent route from the eth1 interface, replace eth0 with eth1 in the following procedure.

Before You Begin

You must access the appliance operating system to delete a static route. For instructions, see Troubleshooting and Advanced Administration Using the Appliance Operating System on page 403.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. Use vi editor to delete the persistent static route entry from the **ifroute-eth0** file.
3. Use vi editor to delete the persistent static route entry from the **Teth0** table.

4. Restart network services to apply the change. Type:

   ```
   sudo service network restart
   ```

   and press ENTER.

Delete a Non-Persistent IPv4 or IPv6 Static Route

Use this procedure to remove a non-persistent IPv4 or IPv6 static route.

Before You Begin

You must access the appliance operating system to delete a static route. For instructions, see Troubleshooting and Advanced Administration Using the Appliance Operating System on page 403.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. For a list of the available static routes, you can view the current routing tables.
   - For IPv4, do the following:
     - To show the main routing table, type:

       ```
       sudo ip -4 route show
       ```

     - To show the table in the network interface routing file, type:

       ```
       sudo ip -4 route show table Tetho
       ```

       where:

       `Teth0` specifies the table in the network interface routing file, such as Teth0 for the interface eth0.
   - For IPv6, do the following:
     - To show the main routing table, type:

       ```
       sudo ip -6 route show
       ```

     - To show the table in the network interface routing file, type:

       ```
       sudo ip -6 route show table Tetho
       ```

       where:

       `Teth0` specifies the table in the network interface routing file, such as Teth0 for the interface eth0.

3. Choose one of the following options:

   - To manually delete a non-persistent IPv4 static route, without restarting network services or rebooting the Authentication Manager instance, do the following:

     a. Delete the route from the interface. Type the following, and press ENTER:

     ```
     sudo ip route del destination/nn via gateway dev eth0
     ```

     where:

     –*destination* specifies the the IP address of the network or host for which you are deleting the static route.

     –*/nn* is the prefix length notation used to specify the subnet mask associated with the destination IP address.

     –*gateway* specifies the IP address of the node that will route traffic to the destination network or host.

     –*eth0* specifies the network interface, for example, eth0 or eth1.

     b. Delete the route from the interface table. Type the following, and press ENTER:

     ```
     sudo ip route del destination/nn via gateway dev eth0
     table Teth0
     ```

     where:

     –*destination* specifies the the IP address of the network or host for which you are deleting the static route.

     –*/nn* is the prefix length notation used to specify the subnet mask associated with the destination IP address.

     –*gateway* specifies the IP address of the node that will route traffic to the destination network or host.

     –*eth0* specifies the network interface, for example, eth0 or eth1.

     –*Teth0* specifies the table in the network interface routing file, such as Teth0 for the interface eth0.

   - To manually delete a non-persistent IPv6 static route, without restarting network services or rebooting the Authentication Manager instance, do the following:

     a. Delete the route from the interface. Type the following, and press ENTER:

     ```
     sudo ip -6 route del destination/nn via gateway dev
     eth0
     ```

     where:

     –*destination* specifies the IP address for the network or host for which you are deleting the static route.

     –*/nn* is the prefix length notation used to specify the subnet mask associated with the destination IP address.

–*gateway* specifies the IP address of the node that will route traffic to the destination network or host.

–*eth0* specifies the network interface, for example, eth0 or eth1.

b. Delete the route from the interface table. Type the following, and press ENTER:

```
sudo ip -6 route del destination/nn via gateway dev
eth0 table Teth0
```

where:

–*destination* specifies the IP address for the network or host for which you are deleting the static route.

–*/nn* is the prefix length notation used to specify the subnet mask associated with the destination IP address.

–*gateway* specifies the IP address of the node that will route traffic to the destination network or host.

–*eth0* specifies the network interface, for example, eth0 or eth1.

–*Teth0* specifies the table in the network interface routing file, such as Teth0 for the interface eth0.

- To automatically delete all non-persistent IPv4 and IPv6 static routes, you can restart the network services on the RSA Authentication Manager instance. Network services will not be available for several seconds. Type:

  ```
  sudo service network restart
  ```

  and press ENTER.

Recovery from Incorrect Network Settings

If the appliance network settings are incorrect, you can change them. Usually, you can use the Operations Console to correct these IPv4 settings:

- Fully qualified domain name (FQDN)
- Domain Name Service (DNS) Settings
- Valid, but incorrect Operations Console IP address

If you cannot access the Operations Console, log on to the appliance operating system and correct the settings. See the appropriate instructions for your appliance:

- Recover from an Incorrect IP Address Change on page 443
- Recover from an Incorrect Subnet Mask on page 444
- Recover from an Incorrect Gateway on page 445

Recover from an Incorrect IP Address Change

Use this procedure to recover from an incorrect IPv4 IP address change that blocks access to the Operations Console on the primary instance or a replica instance.

The following procedure uses the eth0 interface as an example. You can update the eth1 interface by replacing eth0 with eth1.

Before You Begin

This procedure assumes that you know how to use the vi editor.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password that was specified during Quick Setup.
2. Update the **hosts** file with the correct IP address:
   a. Use vi to open the **hosts** file at **/etc/hosts**.
   b. At **local address**, correct the IP address associated with the Fully-Qualified Domain Name (FQDN) of the virtual appliance.
   c. Save and close the **hosts** file.
3. Update the **ifcfg-eth0** file with the correct IP address:
   a. Use vi to open the **ifcfg-eth0** file at **/etc/sysconfig/network/ifcfg-eth0**.
   b. Correct the IP address by changing the IP address value for **IPADDR**.
   c. Save and close the **ifcfg-eth0** file.
4. If you are correcting the IP address for the primary interface, such as eth0, then you must update the **routes** file with the correct IP address. This step is not required for a secondary interface. Do the following:
   a. Use vi to open the **routes** file at **/etc/sysconfig/network/routes**.
   b. Correct the IP address value for **gateway IP**.
   c. Save and close the **routes** file.
5. Update the **ifroutes-eth0** file with the correct gateway IP address:
   a. Use vi to open the **ifroutes-eth0** file at **/etc/sysconfig/network/ifroutes-eth0**.
   b. Correct the IP address value for **gateway IP**.
   c. Save and close the **ifroutes-eth0** file.
6. Restart the network services. Type:

   ```
   sudo /etc/service network restart
   ```

   and press ENTER.

7. Restart RSA Authentication Manager services.
   a. Change the directory to **/opt/rsa/am/server**.
   b. Type:

      ```
      ./rsaserv restart all
      ```

      and press ENTER.

Next Steps

- If you changed the IP address of the primary instance in a replicated deployment, you must log on to the replica instance Operations Console and update the primary instance hostname and IP address on the replica instance. A replica instance requires the primary instance hostname and IP address in order to communicate with the primary instance.

  For instructions, see Update the Primary Instance Hostname and IP Address on a Replica Instance on page 430.
- Verify the changes by logging on to the Operations Console on the instance that you updated. Click **Deployment Configuration** > **Instances** > **Status Report**. Verify that the **Status** is normal.

  In a replicated deployment, check the replication status. Synchronize the replica instance if necessary. For instructions, see the Operations Console Help topic "Synchronize a Replica Instance."
- For instructions on what to do if your primary instance has a DNS Server, replica instances, trusted realms, web tiers, uses RADIUS, or have authentication agents, see Change the Primary Instance IPv4 Network Settings on page 426.
- For instructions on what to do if your replica instance has a DNS Server, web tiers, uses RADIUS, or has authentication agents, see Change the Replica Instance IPv4 Network Settings on page 430.

Recover from an Incorrect Subnet Mask

If you cannot use the Operations Console to change the appliance network settings, you might have to change the IPv4 subnet mask on the appliance.

The following procedure uses the eth0 interface as an example. You can update the eth1 interface by replacing eth0 with eth1.

Before You Begin

This procedure assumes that you know how to use the vi editor.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. Update the **ifcg-eth0** file with the correct subnet mask:
   a. Use vi to open the **ifcg-eth0** file at **/etc/sysconfig/network/ifcg-eth0**.
   b. Change the line **NETMASK=*subnet mask*** to the correct subnet mask.
   c. Save and close the **ifcg-eth0** file.

3. Restart the network services. Type:

   ```
   sudo /sbin/service network restart
   ```

   and press ENTER.

Recover from an Incorrect Gateway

If you cannot use the Operations Console to change the appliance network settings, you might have to change the IPv4 gateway on the appliance.

The following procedure uses the eth0 interface as an example. You can update the eth1 interface by replacing eth0 with eth1.

Before You Begin

This procedure assumes that you know how to use the vi editor.

Procedure

1. Log on to the appliance with the user name **rsaadmin** and the operating system password.
2. If you are correcting the gateway for the primary interface, such as eth0, then you must update the **routes** file with the correct gateway. This step is not required for a secondary interface. Do the following:
   a. Use vi to open the **routes** file at **/etc/sysconfig/network/routes**.
   b. Change the line **default *gateway-ip*** to the correct gateway.
   c. Save and close the **routes** file.
3. Update the **ifroutes-eth0** file with the correct gateway:
   a. Use vi to open the **ifroutes-eth0** file at **/etc/sysconfig/network/ifroutes-eth0**.
   b. Change the line **default *gateway-ip*** to the correct gateway.
   c. Save and close the **ifroutes-eth0** file.
4. Restart the network services. Type:

   ```
   sudo /sbin/service network restart
   ```

   and press ENTER.

B Managing RSA SecurID Tokens Using the Microsoft Management Console

Overview

The RSA Token Management snap-in provides a convenient way to manage RSA SecurID tokens for deployments that have an Active Directory identity source. The RSA Token Management snap-in extends the context menus, property pages, control bars, and toolbars in the Active Directory Users and Computers snap-in for the Microsoft Management Console (MMC). You can use the RSA Token Management snap-in to enable or disable a token, assign a token, or perform other token-related tasks without logging on to the Security Console.

Access the RSA Token Management Snap-in

The RSA Token Management snap-in is visible in the Microsoft Management Console (MMC) through a menu option, Manage SecurID Token(s).

Procedure

1. From Windows, click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
2. Open the Users folder to view all of the users and user groups in the Active Directory.
3. To launch RSA Token Management, right-click a user name and click **All Tasks** > **Manage SecurID Token(s)**.

   The RSA Token Management page is displayed.

Note: Press the F1 key to access MMC Help topics.

Token Management Using the RSA Token Management Snap-In

You can perform the following token management tasks using the RSA Token Management snap-in:

- **Assign and unassign tokens.** When you assign a token to a user, it is automatically enabled. When you unassign the same token, it becomes disabled. For more information see MMC Help Topic "Managing Tokens."
- **Disable and enable tokens.** You can manually enable or disable a token on the Assigned SecurID Tokens page. A disabled token cannot be used for authentication. For more information see MMC Help Topic "Managing Tokens."
- **Edit user authentication attributes.** View and edit a user's authentication attributes, such as assigning a fixed passcode, clearing incorrect passcodes, Windows password integration and logon aliases. For more information see MMC Help Topic "Edit Authentication Attributes."
- **Edit token properties.** View and edit token properties, such as the security domain, token serial number, token type and authentication attributes. For more information see MMC Help Topic "Edit Token Properties."
- **Replace tokens.** Replace lost, stolen, or damaged tokens. For more information see MMC Help Topic "Replace a Token."
- **Manage PINS.** Users may forget their PIN or their PINs maybe compromised. In these situations, you must clear the existing PIN, or force the user to create a new PIN. You can also allow users to authenticate without PIN using only the tokencode. For more information see the MMC Help Topics "Clear an RSA SecurID PIN" and "Require a User to Change a PIN."
- **Provide emergency access.** Users may require emergency access if their token is temporarily or permanently unavailable.For more information, see the MMC Help Topics "Generate an Online Emergency Access Code" and "Assign an Offline Emergency Access Tokencode."

Assign a Hardware Token Using the RSA Token Management Snap-in

Before a user can use a hardware token to authenticate, you must assign the token to the user. You can assign a maximum of three tokens to a single user. RSA recommends that you do not assign more than one hardware token to a user as this may increase the likelihood that users will report a lost or stolen token.

Procedure

1. On the RSA Token Management page, under the Assigned SecurID Tokens tab, click **Assign Token**.
2. In the Assign Token to User window, select a token from the list of available RSA SecurID tokens. You can also use the search options to find a specific token.
3. Click **Assign**.

   A dialog box indicates that the token has been successfully assigned to the user.
4. Click **OK** to close the Assign Token to User window.

Assigning a Software Token Using the RSA Token Management Snap-In

Before a user can use a software token to authenticate, you must first assign the token to the user, and then distribute the tokens. You can assign a maximum of three tokens to a single user.

Procedure

1. Assign an RSA SecurID Software Token Using the RSA Token Management Snap-In.
2. Distribute Software Tokens Using the RSA Token Management Snap-In.

Assign an RSA SecurID Software Token Using the RSA Token Management Snap-In

This is the first of a two-step procedure to assign a software token. This allows you to search for available tokens and then assign it to a user.

Procedure

1. On the RSA Token Management page, under the Assigned SecurID Tokens tab, click **Assign Token**.
2. In the Assign Token to User window, use the search parameters to search for available tokens.
3. Select the token you want to assign.
4. Click **Assign**. A dialog box opens showing you that the token has been successfully assigned to the user.
5. Click **OK** to close the Assign Token to User window.

Distribute Software Tokens Using the RSA Token Management Snap-In

This procedure allows you to configure the token properties for the assigned tokens and then distribute it.

Procedure

1. In the RSA Token Management page, under the Assigned SecurID Tokens tab, select the software token.
2. Click **Token Properties**.
3. In the Token Basics tab, click **Distribute Token** to configure the token profile and attributes.
4. In the Software Token Profile drop-down list, select a software token profile.

   Note: The distribution method can be either file-based (STDID) - STDID 3.0 or dynamic seed provisioning (CT-KIP). The distribution method is automatically populated, depending on the software token profile chosen.

5. In the Device Attributes section, provide values for the attributes, if needed.

6. Do one of the following:
   - If the distribution method is dynamic seed provisioning (CT-KIP), choose an option from the **CT-KIP Activation Code** drop-down list.
   - If the distribution method is file-based (STDID) – STDID 3.0, choose the appropriate option for **Password Protection** in the Token File Options section.
7. Click **Save and Distribute**.

C Deploying IPv4/IPv6 Authentication Agents

Overview

An IPv4/IPv6 authentication agent is a software application that securely passes user authentication requests to and from RSA Authentication Manager. IPv4/IPv6 agents use IPv4 or IPv6 addresses and the HTTP and TCP protocols rather than the UDP protocol.

Important: This release of Authentication Manager 8.1 includes a backward compatible software development kit (SDK). It does not include the IPv4/IPv6 agent.

The TCP agent protocol comprises of three core services:

- **Configuration Service**. Allows agents to retrieve and verify configuration data.
- **Message Key Service**. Allows agents to negotiate a key that can be used to encrypt subsequent authentications.
- **Authentication Service.** Processes authentication requests.

IPv4/IPv6 Agent Name

Unlike the UDP agents, the IPv4/IPv6 agent uses a logical name to identify agents. An agent name is not required to be a fully qualified host name and does not require an IP address. Agents running on different physical hosts can share a logical agent name. It is also possible to have multiple logically named agents on a single physical host.

Deploying an IPv4/IPv6 Authentication Agent

Before an authentication agent can communicate with RSA Authentication Manager, you must deploy the agent.

Before You Begin

- Determine whether the authentication agent is restricted or unrestricted. For more information see Authentication Agent Types on page 63.
- (Optional) Define IPv6 network settings on the primary and replica instances. IPv4/IPv6 authentication agents can use IPv4 or IPv6 addresses. If you are using IPv6 addresses, RSA strongly recommends configuring IPv6 network settings on more than one instance. Multiple instances provide deployment-level redundancy and failover authentication, if an instance becomes unresponsive.

  For instructions, see Create IPv6 Network Settings on a Primary or Replica Instance on page 455.

Procedure

1. Use the Security Console to generate a configuration file for the agent. This allows the agent to locate Authentication Manager servers. For instructions, see Generate the Authentication Manager Configuration File on page 65.
2. Use the Security Console to add a record for the new agent to the internal database. In this step, you can specify whether you are creating a restricted agent. The agent record identifies the agent to RSA Authentication Manager. This process is called registering the agent. For instructions, see Add an Authentication Agent on page 66. IPV4/IPv6 agents cannot register automatically. You must add them manually.

   Note: You can create a single logical agent to reference multiple physical agents. For example, you can create a logical agent called Finance Laptop that can be used for multiple physical agents. This reduces the overhead required to maintain agents.

3. Configure an IPv4/IPv6 Agent.

Configure an IPv4/IPv6 Agent

Configuring the IPv4/IPv6 agent is the second part of the two-step process to register the agent.

Before You Begin

- Generate the Authentication Manager Configuration File on page 65
- Add an Authentication Agent on page 66

Procedure

1. In the Security Console, click **Setup** > **System Settings**.
2. Under Authentication Settings, click **Agents**.

3. On the Agents page, click the link to configure IPv6 agents.

   The IPv4/ IPv6 Agents page is displayed.

4. In the Authentication Servers section, do the following:

   - Select **All Instances** to allow the IPv4/IPv6 agent to communicate with any primary or replica instance in the current deployment. The agent can select any instance for authentication requests, and any NIC configured for the selected instance.
   - Select **Specified Server Names or Addresses** to choose the fully qualified hostnames or IP addresses of specific instances, or a DNS name that resolves to a list of instances.

     In the **Hostname or IP Addresses** field, you can add or remove entries from the list of fully qualified hostnames and IP addresses. RSA strongly recommends entering more than one instance. Multiple instances provide redundancy and support failover authentication.

5. In the **Authentication Service Port** field, enter a port number between 1025 and 49151. The default port number is 5500.

   Important: If you change the port number, the agent cannot retrieve configuration data, until after a new configuration file, **sdconf.rec**, is updated on the agent. Configure your routers and firewalls to pass TCP traffic on the port.

6. In the **Connection Timeout** field, specify how long the agent waits while attempting to establish a connection to the server. The default value is 60 seconds.

7. In the **Read Timeout** field, specify how long the agent waits while attempting to retrieve data from a previously established connection. The default value is 60 seconds.

8. (Optional) In the **Import Certificate of the New Primary Server** field, click **Browse** to locate and import a new root certificate.

   Note: You are required to import a new root certificate only if you are migrating agents to a new deployment. This feature supports migrations from RSA Authentication Manager 8.0 to future versions of Authentication Manager.

9. Click **Update**.

Next Step

Load a New Node Secret (optional)

Load a New Node Secret

The node secret is a shared secret known only to the IPv4/IPv6 authentication agent and RSA Authentication Manager. Authentication agents use the node secret to encrypt authentication requests that they send to Authentication Manager. Authentication Manager uses the node secret to verify the identity of IPv4/IPv6 authentication agents. IPv4/IPv6 authentication agents do not require a node secret.

You can manually create a node secret in the Authentication Manager server and export it to the agent host. Once the node secret file is imported into the agent host machine, you must run the **agent_nsload** utility to extract the node secret file and store it appropriately. The node secret can be stored either in the default path or in a user-defined path.

The Node Secret Load utility, **agent_nsload**, is located in the RSA Authentication Manager 8.1 download kit.

Before You Begin

- On Windows 2008, Windows Vista, and Windows 7 or later, with the User Account Control feature enabled, the **agent_nsload** utility must be run from an elevated command prompt if the node secret is being stored at the default location, **drive:\%windir%\system32**.
- The **sdconf.rec** file must be present in the destination folder on the host machine.

Procedure

1. To extract the node secret to the default location, using the **agent_nsload** utility, type:
   - On UNIX:

     ```
     agent_nsload -f /default_dir/nodesecret.rec
     ```
   - On Windows:

     ```
     agent_nsload -f C:\default_path\ nodesecret.rec
     ```

   To extract the node secret to a user-defined location, using the **agent_nsload** utility, type:
   - On UNIX:

     ```
     agent_nsload -f /VAR_ACE/nodesecret.rec -d
     /VAR_ACE/new_dir/
     ```
   - On Windows:

     ```
     agent_nsload -f C:<windows path>\System32\
     nodesecret.rec -d C:\<windows path>\System32\new_dir\
     ```
2. When prompted, type the password and press **Enter**.

Resolving Common IPv4/ IPv6 Issues

The following table lists common IPv4/IPv6 agent issues, their possible causes, and the corresponding resolutions.

Problem	Possible Cause	Resolution
Bootstrap.xml not found.	The **sdconf.rec** file is incorrect, missing or is in an inaccessible location.	Generate the Authentication Manager Configuration File on page 65
Unable to retrieve configuration data	• The agent cannot connect to the server. • Agent created on server.	• Verify communication between the agent and server • Verify that the correct agent name exists on the server
Agent Credential Mismatch Error	The node secret is defined on the server and not on the agent, or vice versa.	Deploying an IPv4/IPv6 Authentication Agent on page 452
Crypto algorithm unsupported.	The unlimited strength cryptography policy is not installed (Agent SDK).	Install the unlimited strength cryptography policy. For more information see **http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html**
Unable to perform Diffie-Hellman (DH) Key agreement	The RSA cryptographic provider is not installed. (Agent SDK)	Alter security providers by replacing the com.sun providers with com.rsa equivalents.

Create IPv6 Network Settings on a Primary or Replica Instance

You can use the Operations Console on a primary or replica instance to create IPv6 network settings that support IPv6-compliant agents. Authentication Manager supports the TCP agent protocol. By default, Authentication Manager port 5500 supports IPv4- and IPv6-compliant agents. For all other services and ports, IPv4 is supported. Configuring IPv6 in the Operations Console does not enable its use for communications between the primary instance and replica instances.

Procedure

1. In the Operations Console, click **Administration > Network > Appliance Network Settings**.
2. Click **Edit Network Settings**.

3. Under **IPv6 Settings**, check **Enable for IPv6**.
4. In the **IPv6 Address** field, enter a valid IPv6 address, for example, 2001:0db8:85a3:0000:0000:8a2e:0370:7335.
5. In the **IPv6 Prefix** field, enter a prefix length, for example, 64.
6. Click **Next**.

   The Operations Console displays a review page.
7. Select **Yes, change the network settings**, and click **Change Network Settings**.

   Authentication Manager restarts services.

Next Step

Update the DNS server with the new IP address.

Enabling IPv6 in the VMware Infrastructure

You can enable the VMware infrastructure to process authentications requests sent from agents using an IPv6 address. For more information, see your VMWare documentation.

Glossary

Active Directory

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

Active Directory forest

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

administrative role

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

administrator

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

agent host

The machine on which an agent is installed.

appliance

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

approver

A Request Approver or an administrator with approver permissions.

assurance level

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

attribute

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

attribute mapping

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

audit information

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

audit log

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

authentication

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

authentication agent

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

authentication method

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

authentication protocol

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

authentication server

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

authenticator

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

authorization

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

backup

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

certificate

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

certificate DN

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

command line utility (CLU)

A utility that provides a command line user interface.

core attributes

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

Cryptographic Token-Key Initialization Protocol (CT-KIP)

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

custom attributes

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

data store

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

delegated administration

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

delivery address

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

deployment

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

demilitarized zone

The area of a network configured between two network firewalls.

device history

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

device registration

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

distribution file password

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

distributor

A Token Distributor or an administrator with distributor permissions.

DMZ

See demilitarized zone.

dynamic seed provisioning

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

e-mail notifications

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

e-mail templates

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

excluded words dictionary

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

fixed passcode

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

Global Catalog

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

Global Catalog identity source

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

identity attribute

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

identity confirmation method

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

identity source

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

instance

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

internal database

The Authentication Manager proprietary data source.

keystore

The facility for storing keys and certificates.

load balancer

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

lower-level security domain

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

minimum assurance level

See assurance level.

node secret

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

on-demand tokencode

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

on-demand tokencode service

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

Operations Console

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

permissions

Specifies which tasks an administrator is allowed to perform.

preferred instance

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

primary instance

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

promotion, for disaster recovery

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

promotion, for maintenance

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

provisioning

See token provisioning.

provisioning data

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

RADIUS

See Remote Authentication Dial-In User Service.

RBA

See risk-based authentication.

RBA integration script

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

realm

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

Remote Authentication Dial-In User Service (RADIUS)

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

replica instance

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

replica package

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

requests

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

Request Approver

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

risk-based authentication (RBA)

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

risk engine

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

round robin DNS

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

scope

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

Secure Sockets Layer (SSL)

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

Security Console

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

security domain

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

security questions

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

self-service

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

Self-Service Console

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

session

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

shipping address

An address used by distributors to distribute hardware tokens.

silent collection

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

SSL

See Secure Sockets Layer.

Super Admin

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

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

system event

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

System log

A persistable store for recording system events.

time-out

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

token distributor

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

token provisioning

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

top-level security domain

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

Trace log

A persistable store for trace information.

trusted realm

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

trust package

An XML file that contains configuration information about the deployment.

UDP

See User Datagram Protocol.

User Datagram Protocol (UDP)

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

User ID

A character string that the system uses to identify a user attempting to authenticate.

Typically a User ID is the user's first initial followed by the last name. For example, Jane Doe's User ID might be *jdoe*.

virtual host

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

virtual hostname

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

web tier

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

workflow

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

workflow participant

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

Index