RSA® Authentication Manager 8.1
Help Desk 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.

Copyright © 1994-2013 EMC Corporation. All Rights Reserved
December 2013

Contents

Preface

About This Guide

This guide describes the most common tasks that a Help Desk Administrator needs to manage RSA® Authentication Manager.

Your company determines which tasks a Help Desk Administrator is allowed to perform. Since each company is different, this guide may contain some tasks that you cannot perform.

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

This chapter introduces you to the components, features, and tasks in Authentication Manager that are important for helping customers solve day-to-day authentication problems.

For additional information about the features in this guide, see the *RSA Authentication Manager 8.1 Administrator’s Guide*.

Purpose of RSA SecurID and RSA Authentication Manager

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.

How Authentication Manager Protects Resources

Records of users, agents, tokens, and user’s PINs reside in Authentication Manager or in LDAP directories. During authentication, Authentication Manager compares these records to the information a user enters when logging on. If the records and tokencode or passcode match, the user gains access.

During an authentication, Authentication Manager and the agent software work in the following way:

1. A user logs on to access a protected resource.
2. The agent prompts the user to enter a User ID and an RSA SecurID passcode or tokencode.
3. The user reads the tokencode from the token and then enters his or her PIN plus the tokencode to create the passcode. (If a PIN is not required, the user enters the tokencode only.)

   The entered data is encrypted and the agent sends the data to Authentication Manager.
4. Authentication Manager receives the User ID and passcode or tokencode and looks for the user record in an identity source.

5. Authentication Manager calculates the correct value of the passcode by accessing the token record of the token assigned to the user. Using data contained in the token record, it generates the passcode to compare with that supplied by the user.
6. Authentication Manager evaluates the policies defined by the administrator.
7. If the passcode is correct and the policies allow access, Authentication Manager approves the authentication request. The user gains access to the protected device.

RSA SecurID Tokens Overview

RSA SecurID tokens offer two-factor authentication by generating a 6-digit or 8-digit tokencode at regular intervals. When the tokencode is combined with a personal identification number (PIN), the result is called a passcode. Users enter the passcode 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 and software tokens require similar administrative tasks. You can perform many token-related administrative tasks with the User Dashboard in the RSA Security Console.

On-Demand Authentication Overview

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.

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. 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 pre-enrolled security questions. Correct answers to questions can be established either during pre-enrollment 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.

Policies Overview

Policies are associated with security domains and control various aspects of your deployment.

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.

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

Password policy. Password policies define the users' password length, format, and frequency of change.

Lockout policy. 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.

Self-Service troubleshooting policy. The self-service troubleshooting feature allows Self-Service Console users to troubleshoot routine authentication problems if 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.

Risk-based authentication (RBA) policy. 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. The RBA message policy defines the message that users receive when they are challenged to configure their identity confirmation method.

Identity Sources

In Authentication Manager, user and group data are kept in data stores called identity sources. There are two types of identity sources:

- The Authentication Manager internal database. This database contains all application and policy data, and your company may also choose to store user and user group data in it.
- One or more external LDAP directories such as Oracle Directory Server (ODS) or Microsoft Active Directory. Authentication Manager access to external LDAP identity sources is read-only.

As a Help Desk Administrator, you need to perform tasks that require Authentication Manager to access identity sources. For example, these tasks include:

- Add a User to the Internal Database on page 29
- Delete a User on page 31
- Enable a User Account in the User Dashboard on page 32
- Disable a User Account in the User Dashboard on page 33
- Change a User's Password in the User Dashboard on page 35

RSA Self-Service

RSA 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 helping users when they forget their PINs, misplace their tokens, require emergency access, or require token resynchronization.
- **Provisioning**. Users can 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.

Certain tasks related to Self-Service still require administrative assistance. As a Help Desk Administrator, you may be asked to perform the following tasks:

- Clear a Cached Copy of Windows Credentials in the User Dashboard on page 77
- Managing Security Questions on page 36

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.

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 a supplied template. Each template allows you to choose the types of information being reported and which parameters to apply in order to refine that information. You can view activities for all administrators, or you can display detailed information on one administrator.

In addition, you can perform the following reporting tasks:

- View and download completed reports, view reports that are currently running or reports that are waiting in the report queue.You can view the report output in the Security Console, or download the report as a CSV, XML, or HTML file.
- Transfer reports to other security domains. When running a report, change the report ownership so that the administrative scope is narrowed or broadened.

Administrative Roles

Administrators manage all aspects of the Authentication Manager 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.

2 Confirming a User’s Identity

As a Help Desk Administrator, it is critical that you verify the end user’s identity before performing any Help Desk operations on their behalf. Recommended actions include:

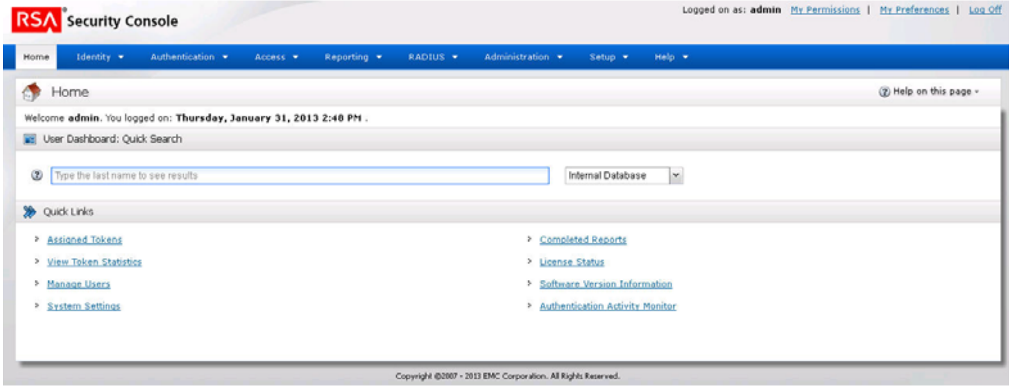
- When a user calls the Help Desk, only ask for the user’s User ID. You should never ask for token serial numbers, tokencodes, PINS, passwords, and so on.
- If you must initiate contact with a user, do not request any user information. Instead, tell users to call the Help Desk back at a well-known Help Desk telephone number to ensure that their original request is legitimate.
- Call the user back on a phone owned by the organization and on a number that is already stored in the system.
- Send the user an e-mail to a company e-mail address. If possible, use encrypted e-mail.
- Work with the employee’s manager to verify the user’s identity.
- If possible, meet the user in person to verify his or her identity.
- Use multiple open-ended questions from employee records (for example: Name one person in your group; What is your badge number?). Avoid yes/no questions.

3 Using the Security Console

Security Console

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

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



Welcome **admin**. You logged on: **Thursday, January 31, 2013 2:40 PM** .

Copyright ©2007 - 2013 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
- Assign and manage RSA SecurID tokens
- Enable and disable users for risk-based authentication or on-demand authentication

Log On to the Security Console

You must log on to the Security Console in order to complete administrative tasks.

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.

Before You Begin

Make sure you have the appropriate logon credentials.

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.

Online Help

The Security Console provides several ways to access online Help:

- Help On This Page
- Help Table of Contents
- iHelp

Help On This Page

Each page of the Security Console offers a list of Help topics relevant to that page on the Security Console.

To access Help on This Page, find the Help on This Page link on the right side of the page.

Help Table of Contents

The Help table of contents for the Security Console organizes help topics by Authentication Manager features and concepts. The Help table of contents displays on the left side of the Security Console window.

To access the table of contents, click on a Help on This Page link, or click **Help** > **All Help Topics**.

iHelp

The iHelp refers to the question mark icon that is located beside Security Console fields and options. When you place the cursor over the icon, you can see the text that describes the field. Use the iHelp when you need assistance as you complete tasks in the Security Console. The iHelp allows you to quickly access information about a field without using the Help system.

To access the iHelp, move your cursor over the iHelp icon that is located on the left of the field.

4 Managing Users

Users

If your deployment uses the internal database as an identity source, you can use the Security Console to manage all user data.

If your deployment uses an LDAP directory, the identity source is read-only. You can add users to an LDAP directory using a tool appropriate for the directory. After users are added, you can use the Security Console to perform certain administrative functions, such as enabling the user for risk-based authentication (RBA).

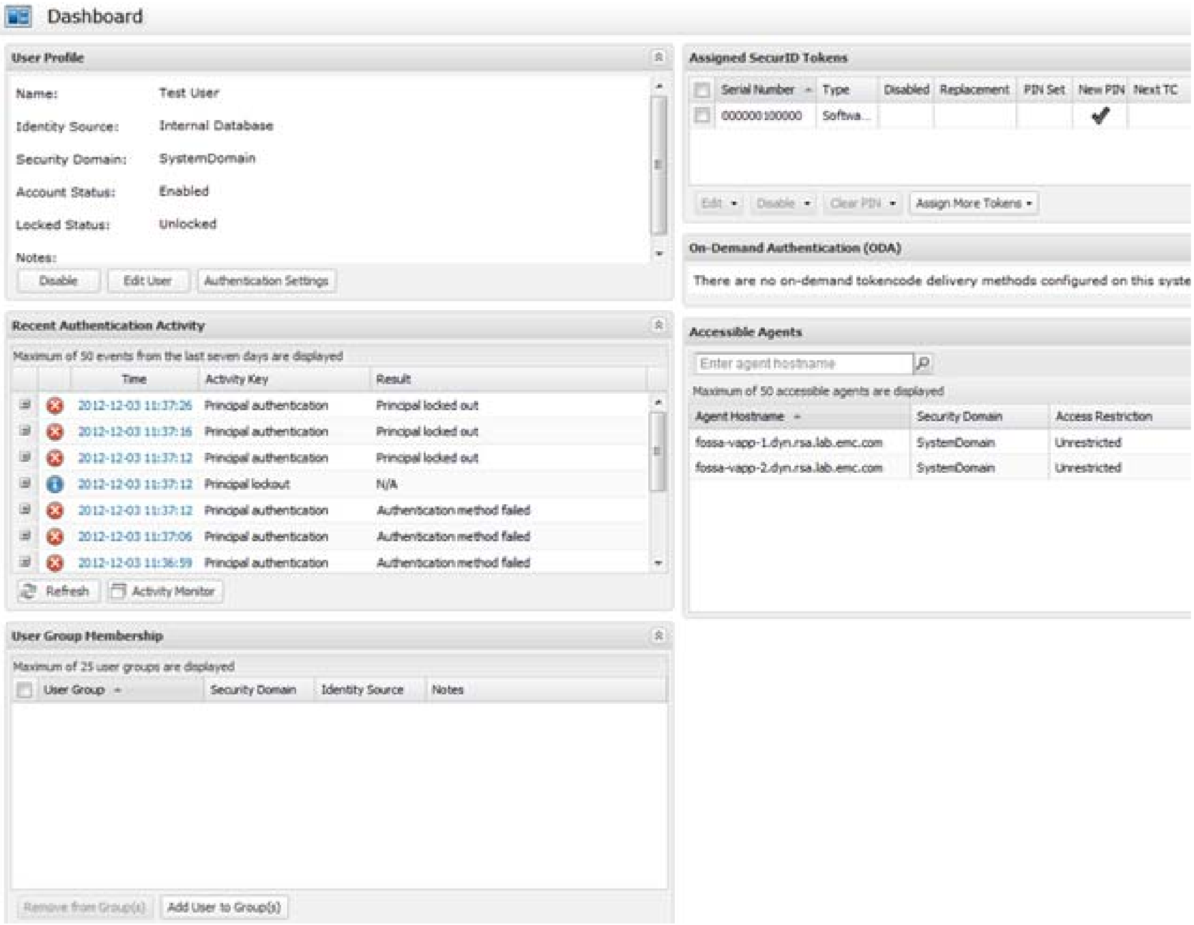
You can manage certain user account related activities on the User Dashboard page in the Security Console. For more information, see User Dashboard on page 24.

For more information on managing users, see the chapter “Administering Users” in the *Administrator’s Guide*.

User Dashboard

The User Dashboard provides a consolidated view of authentication data for a single user, allowing you to identify and troubleshoot issues.

You can view the User Dashboard using Quick Search on the Home page. Quick User Search can be customized to search by last name or User ID.You can search for users in one identity source or across all identity sources within your scope. For instructions, see Use Quick Search to View the User Dashboard for a User on page 27.



Dashboard

User Profile

Name:	Test User
Identity Source:	Internal Database
Security Domain:	SystemDomain
Account Status:	Enabled
Locked Status:	Unlocked
Notes:	

Recent Authentication Activity

Maximum of 50 events from the last seven days are displayed

	Time	Activity Key	Result
✖	2012-12-03 11:37:26	Principal authentication	Principal locked out
✖	2012-12-03 11:37:16	Principal authentication	Principal locked out
✖	2012-12-03 11:37:12	Principal authentication	Principal locked out
ℹ	2012-12-03 11:37:12	Principal lockout	N/A
✖	2012-12-03 11:37:12	Principal authentication	Authentication method failed
✖	2012-12-03 11:37:06	Principal authentication	Authentication method failed
✖	2012-12-03 11:36:59	Principal authentication	Authentication method failed

User Group Membership

Maximum of 25 user groups are displayed

□	User Group	Security Domain	Identity Source	Notes

Assigned SecurID Tokens

□	Serial Number	Type	Disabled	Replacement	PIN Set	New PIN	Next TC
□	000000100000	Softwa...				✓	

On-Demand Authentication (ODA)

There are no on-demand tokencode delivery methods configured on this syste

Accessible Agents

Maximum of 50 accessible agents are displayed

Agent Hostname	Security Domain	Access Restriction
fossa-vapp-1.dyn.rsa.lab.emc.com	SystemDomain	Unrestricted
fossa-vapp-2.dyn.rsa.lab.emc.com	SystemDomain	Unrestricted

User Dashboard Tasks

You can use the User Dashboard to perform these tasks for a particular use.

Note: Your ability to view or perform tasks in the User Dashboard depends on your license and administrative permissions.

Action	Description	Reference
Enable or disable account	Enable or disable a user from authenticating.	Enable a User Account in the User Dashboard Disable a User Account in the User Dashboard
Assign a user alias	A logon alias allows users to authenticate with their RSA SecurID token using User IDs other than their own.	Assign a User Alias in the User Dashboard
Unlock	Locked out users cannot authenticate until they are unlocked.	Unlock a User in the User Dashboard
Change a password	You can change passwords for users whose accounts are in the internal database. You might perform this task if the security of the old password has been compromised.	Change a User's Password in the User Dashboard
Clear security question answers and cached windows password	You might clear security question answers if the user forgot the answers, or if the security of the answers was compromised in some way. You can avoid a failed logon attempt by clearing the saved copy of the user's Windows password.	Clear Security Question Answers in the User Dashboard Clear a Cached Copy of Windows Credentials in the User Dashboard
Add to a user group and view user group memberships	You can add users from any identity source to one or more user groups in the internal database only.	Add a User to a User Group in the User Dashboard View User Group Memberships for a User in the User Dashboard
Manage authentication settings	You can create exceptions to authentication policies for individual users. These settings also allow you to troubleshoot user authentication issues.	Manage User Authentication Settings in the User Dashboard

Action	Description	Reference
Enable or disable on-demand authentication	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.	Enable On-Demand Authentication for a User in the User Dashboard Disable On-Demand Authentication for a User in the User Dashboard
Clear and set temporary on-demand authentication PIN	You might clear a user's 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.	Clear a User's On-Demand Authentication PIN in the User Dashboard
Require a password change at next logon	You can require users to change their passwords if the password is suspected of being compromised. If a user's identity source is the internal database, you can force the user to change the password the next time the user logs on.	Require a User to Change a Password using the User Dashboard
Assign hardware a token	Assign up to three tokens per user.	Assign a Hardware Token to a User in the User Dashboard
Assign and distribute a software token	Assign up to three tokens per user.	Assign and Distribute a Software Token to a User Using Dynamic Seed Provisioning in the User Dashboard Assign and Distribute a Software Token to a User Using File-Based Distribution in the User Dashboard
Clear a PIN	Once cleared, the user must enter a tokencode, and then create a new PIN.	Clear an RSA SecurID PIN in the User Dashboard

Action	Description	Reference
Generate emergency access tokencode	Generate an emergency access tokencode for a user whose existing token has been permanently lost or destroyed.	Provide an Offline Emergency Access Tokencode
Resynchronize tokens	Resynchronize a token when its tokencode does not match the tokencode generated by Authentication Manager. Mismatched tokencodes cause authentication to fail.	Resynchronize a Token in the User Dashboard
Replace a token	Replace a token that has been permanently lost, stolen, damaged or expired.	Replace a Token for a User in the User Dashboard
Enable or disable tokens	Only enabled tokens can be used for authentication. Tokens are automatically enabled when first assigned to a user. You might choose to disable a token if a user is out of the office for an extended period of time. Disabling a token does not remove it from the deployment.	Enable a Token in the User Dashboard Disable a Token in the User Dashboard
Unassign a token	When you unassign a token, the user can no longer use the token to authenticate and the token is disabled.	Unassign a Token from a User in the User Dashboard

Use Quick Search to View the User Dashboard for a User

You can view a user's authentication data in the User Dashboard by using Quick Search on the Security Console Home page to find the user. You can search one or more identity sources within your administrative scope. Quick User Search can be customized to search by last name or User ID. By default, all identity sources are searched.

Procedure

1. On to the Security Console Home page, use the **Quick Search** field to find the user that you want to manage.
2. (Optional) From the **Identity Source** drop-down list, select the user’s identity source.

Add a User with Options to the Internal Database

To add a new user “with options” means that when you add user records, you can configure additional options for the user. For example, when you finish adding the user information, you can assign a token, add the user to a user group or assign the user an administrative role.

Use this procedure to add users to the internal database. Authentication Manager has read-only access to external identity sources.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Add New With Options**.
2. Decide which options that you want to assign to the new user, and select the appropriate checkboxes.
3. Click **Next**.
4. In the **Administrative Control** section, from the **Security Domain** drop-down menu, select the security domain to which you want to assign the user.
5. Complete the **User Basics** section:
   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 must be unique within the identity source where you save the user, and not exceed 255 characters. Do not use multi-byte characters, such as

      東

      Note: If this account is for an administrator who requires access to the Security Console, the User ID must be unique in 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.
6. Complete the **Password** section:
   a. In the **Password** field, enter a password for the user. Password requirements are determined by the password policy assigned to the user's security domain. This is the user's identity source password, which may be different from alternative passwords provided by applications.
   b. In the **Confirm Password** field, reenter the password.

c. To force the user to change the password during the next logon, select **Force Password Change**.

7. Complete the **Account Information** section:

   a. From the **Account Starts** drop-down lists, select the date and time when the user account becomes active. The time zone is determined by local system time.

   b. (Optional) Use **Account Expires** options to modify account expiration settings. To set an expiration date for this user, select **Expires on**, and select the date and time when the user account will expire. (The time zone is determined by local system time.) To remove account expiration, select **Does not expire**.

   c. To disable the new account, select **Account is disabled**.

8. In the Attributes section, in the **Mobile Number** field, enter a mobile phone number for the user.

9. Click **Save & Next**.

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.

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**.

Edit a User in the User Dashboard

Use the Security Console to edit a user that is stored in the internal database.

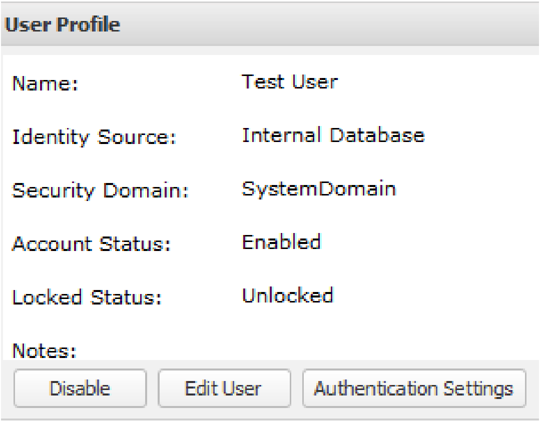
If a user is stored in an external LDAP directory identity source, you can manage only a limited number of items in the user's account.

Before You Begin

Your administrative permissions determine whether you can specify attributes for a user. You can only enter values for attributes that your role permits you to edit, even if the attribute is required.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user you want to edit.
4. Under **User Profile**, click **Edit User**.



User Profile

Name: Test User

Identity Source: Internal Database

Security Domain: SystemDomain

Account Status: Enabled

Locked Status: Unlocked

Notes:

5. Edit the user and click **Save**.

Delete a User

You can use the Security Console to delete users who are stored in the internal database as their identity source. After you delete the user, you cannot manage the user with RSA Authentication Manager. For example, you can no longer enable the user for authentication.

If the user that you delete is enabled for risk-based authentication (RBA), the system deletes the user device history and updates the feature license so that the seat is available to another user.

You can delete users who use an LDAP directory as their identity source only by using 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 delete. Some fields are case sensitive.
3. Select the users that you want to delete, and click **Delete**.
4. Click **OK**.

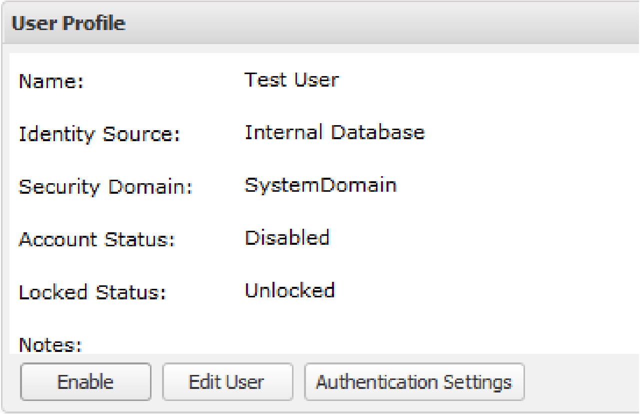
Enable a User Account in the User Dashboard

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

To enable users who are in an external 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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user you want to enable.
4. Under **User Profile**, click **Enable**.



User Profile

Name: Test User

Identity Source: Internal Database

Security Domain: SystemDomain

Account Status: Disabled

Locked Status: Unlocked

Notes:

5. When prompted, click **Enable User** to confirm.

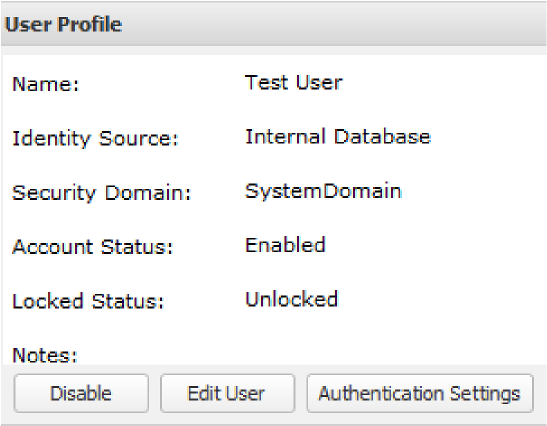
Disable a User Account in the User Dashboard

When you disable a user, you prevent the user from authenticating and accessing protected resources. Disabling a user does not delete the user from the deployment.

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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user you want to disable.
4. Under **User Profile**, click **Disable**.



User Profile

Name: Test User

Identity Source: Internal Database

Security Domain: SystemDomain

Account Status: Enabled

Locked Status: Unlocked

Notes:

5. When prompted, click **Disable User** to confirm.

Locked User Accounts

When a user account is locked, the user cannot authenticate and access protected resources. A user account can be locked in two ways:

- **Lockout policy**. This policy locks a user account if authentication fails a specified number of times using the primary authentication method. Lockout policies apply to the total number of logon attempts a user makes regardless of the type of credential used for each attempt.
- **Token policies**. Token policies determine RSA SecurID PIN lifetime and format, and fixed passcode lifetime and format. They are assigned to security domains and apply to all tokens assigned to users managed by a given security domain. If a user puts the wrong tokencode in a specified number of times, they will be locked out.

Unlock a User in the User Dashboard

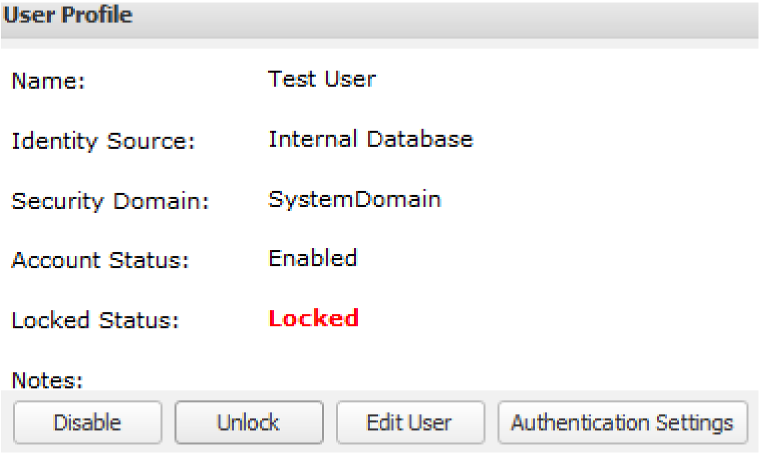
Locked out users cannot authenticate until they are unlocked.

The lockout policy specifies the number of failed authentication attempts allowed before the system locks the account. The user might be locked out after a series of incorrect tokencodes or next tokencodes.

If the lockout policy is configured to unlock a user after a certain period of time, the user will be unlocked when the time expires. The user will show as **Locked** on the Users page and in the User Dashboard. The user will show as “True” (locked) in the **Locked Out** field in reports until the next successful authentication.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user you want to unlock.
4. Under **User Profile**, click **Unlock**.



User Profile

Name: Test User

Identity Source: Internal Database

Security Domain: SystemDomain

Account Status: Enabled

Locked Status: Locked

Notes:

5. When prompted, click **Unlock User** to confirm.

Assign a User Alias in the User Dashboard

A logon alias allows users to authenticate with their RSA SecurID token using User IDs other than their own.

Before You Begin

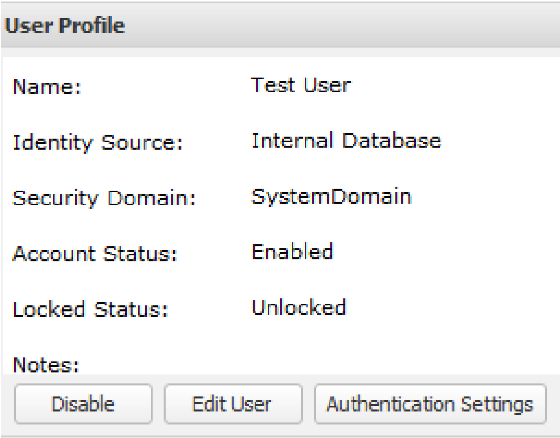
Before you assign a user alias, your Super Admin should have done the following:

- Included a restricted or unrestricted agent in your deployment.

- 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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user to which you want to assign an alias.
4. Under **User Profile**, click **Authentication Settings**.



User Profile

Name: Test User

Identity Source: Internal Database

Security Domain: SystemDomain

Account Status: Enabled

Locked Status: Unlocked

Notes:

5. Under **Authentication Settings**, select whether you want to allow users to use their own User IDs or an alias.
6. Select the user group to which you want to assign the alias.
7. In the **User ID** field, enter the User ID that you want to assign to the alias.
8. In the **Shell** field, enter the shell that you want assigned to the alias.
9. If your deployment uses RADIUS, from the **RADIUS Profile** drop-down menu, select the RADIUS profile to assign to the alias.
10. Click **Add**.
11. Click **Save**.

Change a User's Password in the User Dashboard

You can change passwords for users whose accounts are in the internal database. You might perform this task if the security of the old password has been compromised.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.

3. Select the user whose password you need to change.
4. Under **User Profile**, click **Edit User**.
5. In the **Password** section, enter the new password in the **Password** field.
6. Enter the new password again in the **Confirm Password** field.
7. Click **Save**.

Require a User to Change a Password using the User Dashboard

If a user's identity source is the internal database, you can force the user to change his or her password the next time the user logs on.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose password needs to be changed.
4. Under **User Profile**, click **Edit User**.
5. In the **Password** section, select **Require user to change password at next logon**.
6. Click **Save**.

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 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**.

Clear Security Question Answers in the User Dashboard

You can clear the answers for a particular user’s security questions. For example, you might do this if the user forgot the answers, or if the security of the answers was compromised in some way. After answers are cleared, the user must provide new answers in order to use security questions for self-service troubleshooting.

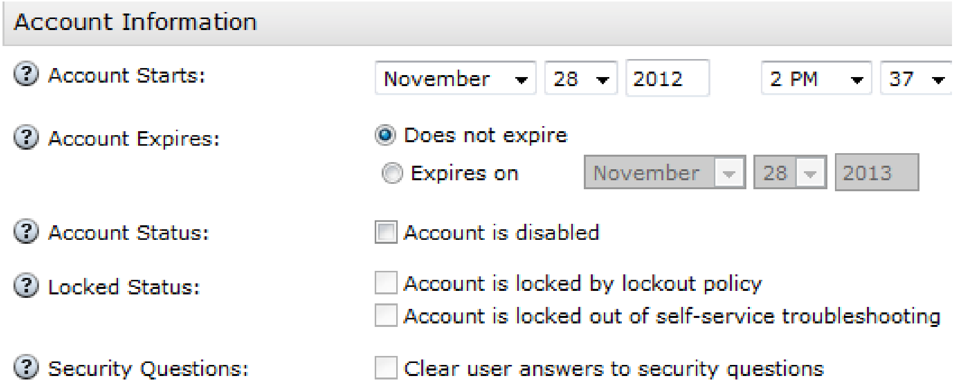
Before You Begin

Make sure that the user configured security questions with answers.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user you want to edit.
4. Under **User Profile**, click **Edit User.**

5. Under **Account Information**, select the checkbox for **Clear user answers to security questions**.



Account Information

Account Starts: November 28 2012 2 PM 37

Account Expires: ● Does not expire
○ Expires on November 28 2013

Account Status: □ Account is disabled

Locked Status: □ Account is locked by lockout policy
□ Account is locked out of self-service troubleshooting

Security Questions: □ Clear user answers to security questions

6. Click **Save**.

Manage User Authentication Settings in the User Dashboard

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

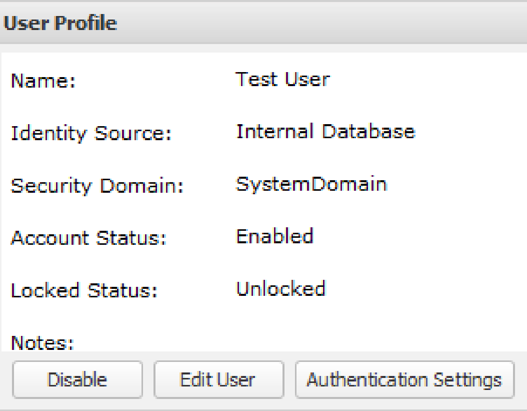
Before You Begin

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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose authentication settings you want to manage.

4. Under **User Profile**, click **Authentication Settings**.



User Profile

Name: Test User

Identity Source: Internal Database

Security Domain: SystemDomain

Account Status: Enabled

Locked Status: Unlocked

Notes:

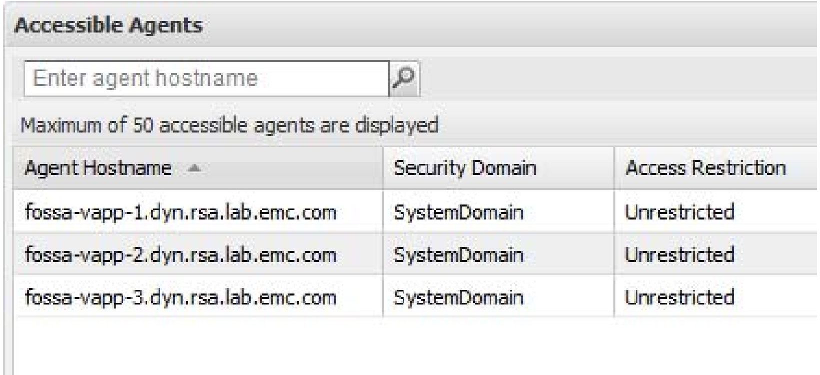
5. Edit the user’s authentication settings.
6. Click **Save**.

View Accessible Agents in the User Dashboard

You can view up to 50 restricted and unrestricted agents the selected user can access. For restricted agents, the user can authenticate within the designated access times. You can search these agents by hostname.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose recent authentication you want to view.
4. Under **Accessible Agents,** the agents accessible to the user are listed.



Accessible Agents

Maximum of 50 accessible agents are displayed

Agent Hostname ▲	Security Domain	Access Restriction
fossa-vapp-1.dyn.rsa.lab.emc.com	SystemDomain	Unrestricted
fossa-vapp-2.dyn.rsa.lab.emc.com	SystemDomain	Unrestricted
fossa-vapp-3.dyn.rsa.lab.emc.com	SystemDomain	Unrestricted

5. (Optional) Search for an agent by hostname.

5 Managing User Groups

User Groups

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. Grouping users makes it easy to manage access to protected resources. Users can be grouped according to your organizational needs.

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**.

Edit User Groups

You can edit user groups for users whose accounts are in the internal database. Editing a user group allows you to change information such as the user group's name and security domain.

Before You Begin

If a user group resides in an external LDAP identity source, you can edit the following fields only:

- Security Domain
- Notes

Procedure

1. In the Security Console, click **Identity** > **User Groups** > **Manage Existing**.
2. Select the user group that you want to edit, and click **Edit**.
3. Make the necessary changes to the user group.

4. Click **Save**.

   If you have not saved your edits, you can click **Reset** to reset the user group to be as it was before you began editing.

View User Group Members

You can view users who are organized into user groups based on criteria such as geographic location or job title.

Procedure

1. In the Security Console, click **Identity** > **User Groups** > **Manage Existing**.
2. Click the user group, and select **Member Users**.
3. Use the search fields to search for all users.

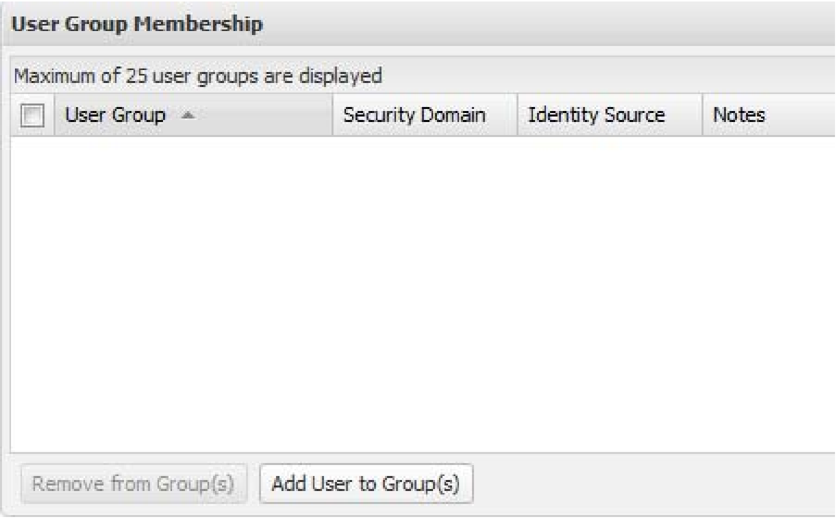
Add a User to a User Group in the User Dashboard

You can add users from any identity source to one or more user groups in the internal database. To add users to a group in an external LDAP identity source you must use a tool appropriate for the directory.

You can organize users into user groups based on criteria such as geographic location or job title. You can also restrict which agents the user members can use to authenticate and the times that they can authenticate through the agent.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user you want to add to a user group.
4. Under **User Group Membership**, click **Add User to Group(s)**.



User Group Membership

Maximum of 25 user groups are displayed

□	User Group ▲	Security Domain	Identity Source	Notes

5. When prompted, search for a user group.
6. Select the user group or groups to which you want to add the user.
7. Click **Add to Group(s)**.

View User Group Memberships for a User in the User Dashboard

Use the Security Console to view the user groups in which a user has membership. The Security Console cannot display a user's primary Active Directory group, such as Domain Users. The group appears empty even though it has members.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose user group memberships you want to view.
4. Under **User Group Membership**, the user group memberships for the user are listed.

6 Managing RSA SecurID Tokens

RSA SecurID Tokens Overview

RSA SecurID tokens offer two-factor authentication by generating a 6-digit or 8-digit tokencode at regular intervals. When the tokencode is combined with a personal identification number (PIN), the result is called a passcode. Users enter the passcode 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 and software tokens require similar administrative tasks. You can perform many token-related administrative tasks with the User Dashboard in the Security Console.

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 and Distribute a Software Token to a User Using File-Based Distribution in the User Dashboard on page 51.
- Assign and Distribute a Software Token to a User Using Dynamic Seed Provisioning in the User Dashboard on page 57.
- Assign a Hardware Token to a User in the User Dashboard on page 46.

Assign a Hardware Token to a User in the User Dashboard

Before a user can use a hardware token to authenticate, you must assign the token to the user. You can assign up to 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.

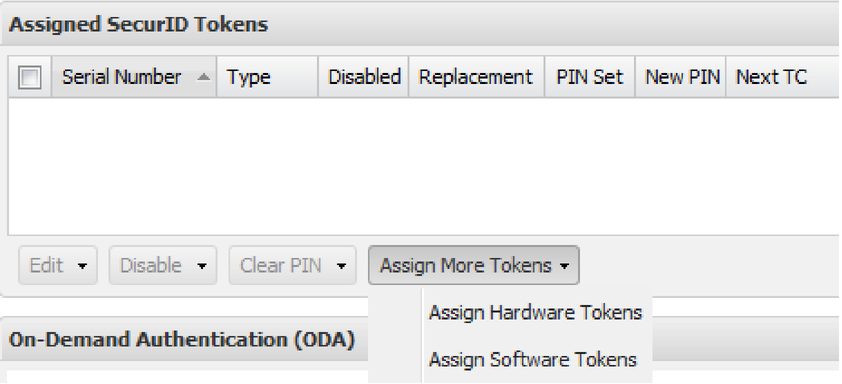
Before You Begin

Import a token record file. For instructions, see Import a Token Record File on page 45.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user to whom you want to assign a hardware token.

4. Under **Assigned SecurID Tokens**, click **Assign More Tokens** > **Assign Hardware Tokens**.



5. Select a token from the list or search for a token in the search bar.
6. Click **Assign Token(s)**.

Next Steps

Distribute a Hardware Token on page 48

Assign Hardware Tokens to Multiple Users

Before users can use hardware tokens to authenticate, you must assign the tokens to the users. You can assign up to three tokens to a single user.

Before You Begin

See Import a Token Record File on page 45.

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, select the checkboxes next to the users to whom you want to assign tokens.
4. From the Action menu, click **Assign SecurID Tokens**.
5. Click **Go**.
6. From the list of available RSA SecurID tokens, select the checkbox next to the hardware tokens that you want to assign.

   Note: The number of selected tokens must equal the number of selected users.

7. Click **Assign.**

Next Steps

Distribute a Hardware Token on page 48

Distribute a Hardware Token

Before a user can use a hardware token to authenticate, you must distribute the token to the user.

Before You Begin

Assign a hardware token to a user.

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.

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.

Assign Software Tokens to Multiple Users

Before users can use software tokens to authenticate, you must assign the tokens to the users, and then deliver the token to the users.

Procedure

1. In the Security Console, click **Identity** > **Users** > **Manage Existing**.
2. Use the search fields to find the user to whom you want to assign tokens.
3. From the search results, select the checkboxes next to the users to whom you want to assign tokens.
4. From the Action menu, click **Assign SecurID Tokens**.

5. Click **Go**.
6. From the list of available RSA SecurID tokens on the Assign to Users page, select the checkbox next to the software tokens that you want to assign to the users. Remember which tokens you assign so you can deliver them later.

   Note: The number of selected tokens must equal the number of selected users.

7. Click **Assign**.

Next Steps

Deliver the tokens using one of the following methods:

- For file-based provisioning, save a software token to a file and electronically deliver it to the user's device. For instructions, see Distribute Multiple Software Tokens Using Dynamic Seed Provisioning (CT-KIP) on page 58.
- For the CT-KIP protocol, use dynamic seed provisioning to deploy a software token on a user's device. For instructions, see Assign and Distribute a Software Token to a User Using Dynamic Seed Provisioning in the User Dashboard on page 57.

Assign and Distribute a Software Token to a User Using File-Based Distribution in the User Dashboard

Before a user can use a software token to authenticate, you must assign the token to the user. You can assign up to three tokens to a single user.

Software token files provisioned using file-based distribution have the.SDTID extension. The data in the token file includes the seed used by the SecurID algorithm, and other metadata such as expiration date, serial number, and number of digits in the tokencode.

Before You Begin

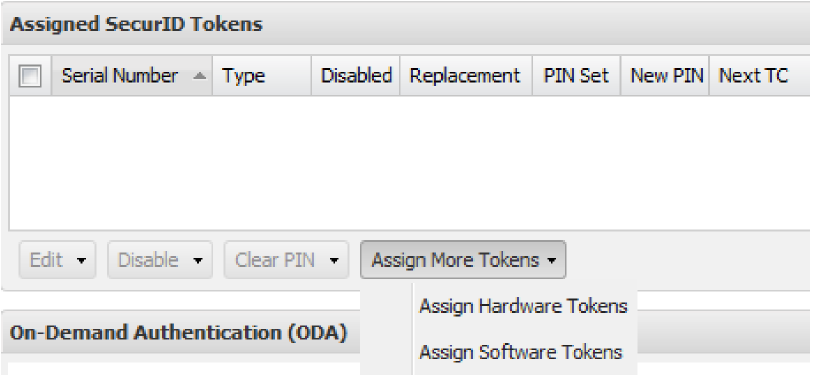
Confirm the following:

- Software tokens have been imported.
- Software token profiles have been added.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user to whom you want to assign a token.

4. Under **Assigned SecurID Tokens**, click **Assign More Tokens** > **Assign Software Tokens**.



5. Select a token from the list or search for a token in the search bar.
6. Click **Assign Token(s)**.
7. From the **Select Token Profile** drop-down list, select a software token profile with file-based provisioning as the delivery method.
8. In the **Device Serial Number** field, leave the default selection or enter the appropriate device information.
9. (Optional) In the **Nickname** field, enter a user-friendly nickname for the software token, if supported.
10. 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.
    - **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.
11. If you select **Password or Combination**, choose a password, and enter it in the **Password** and **Confirm Password** fields.
12. Click **Save and Distribute**.
13. Click **Download Now.**

Next Step

Save a software token to a file and electronically deliver it to the user's device.

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.
- Your Super Admin must add a software token profile.
- Assign tokens to users.

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 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. Only a Super Admin can add software token profiles.

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.

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. Only a Super Admin can add software token profiles.

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.

Assign and Distribute a Software Token to a User Using Dynamic Seed Provisioning in the User Dashboard

Before a user can use a software token to authenticate, you must assign and distribute the token to the user. You can assign up to three tokens to a single user.

Authentication Manager provides dynamic seed provisioning, which uses the Cryptographic Token Key Initialization Protocol (CT-KIP) to generate token data without the need for a token file. After you complete the provisioning steps, Authentication Manager displays the URL link of the CT-KIP server and the token activation code. You need these two pieces of information in order to deliver the token to a device as a URL.

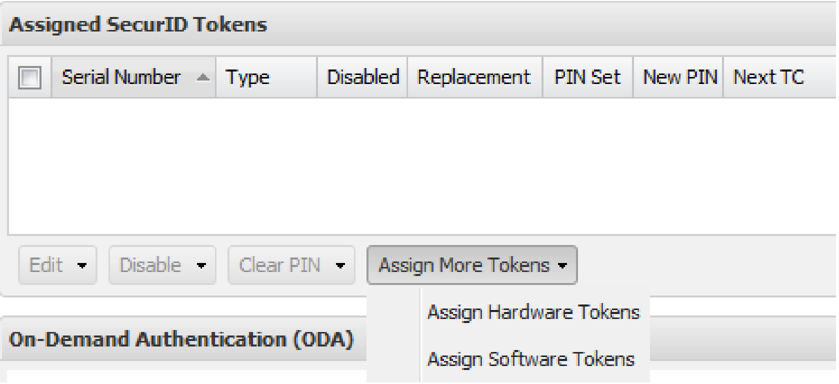
Before You Begin

Confirm the following:

- Software tokens have been imported.
- Software token profiles have been added.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user to whom you want to assign a token.
4. Under **Assigned SecurID Tokens**, click **Assign More Tokens** > **Assign Software Tokens**.



5. Select a token from the list or search for a token in the search bar.
6. Click **Assign Token(s)**.
7. From the **Select Token Profile** drop-down list, select a software token profile with dynamic seed provisioning as the delivery method.
8. In the **Device Serial Number** field, leave the default selection or enter the appropriate device information.

9. From the CT-KIP Activation Code drop-down list, select an activation code for the software token.
10. Click **Save and Distribute**.
11. Click **Done**.

Next Step

Use dynamic seed provisioning to deploy a software token on a user's device.

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.
- Your Super Admin must add a software token profile.
- Assign tokens to users.
- 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.

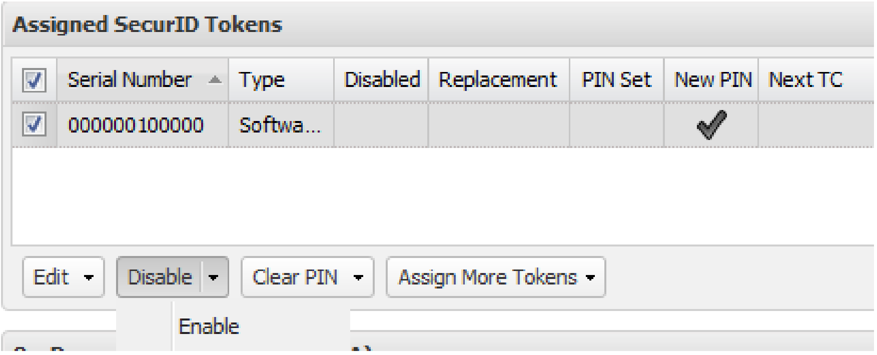
    For more information, see the software token *Administrator's Guide* for your platform.

Enable a Token in the User Dashboard

Before a user can use an assigned token to authenticate, you must enable the token.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose token you want to enable.
4. Under **Assigned SecurID Tokens**, click the token you want to enable.
5. Click the arrow next to **Disable** and then click **Enable**.



Assigned SecurID Tokens

☑	Serial Number	Type	Disabled	Replacement	PIN Set	New PIN	Next TC
☑	000000100000	Softwa...				✓	

6. When prompted, click **Enable Token(s)**.

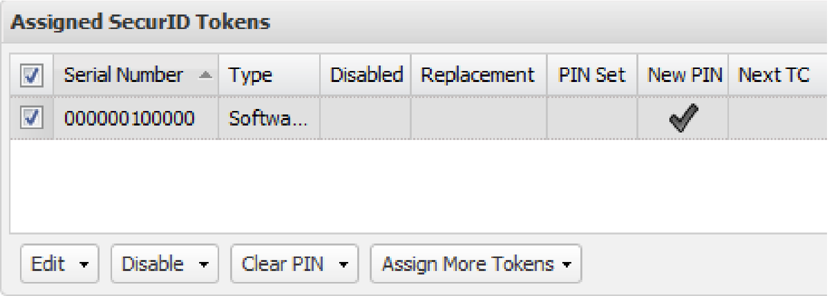
Disable a Token in the User Dashboard

When you disable a token, the assigned user can no longer use the token to authenticate. You might choose to disable a token if a user is out of the office for an extended period of time.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose token you want to disable.
4. Under **Assigned SecurID Tokens**, click the token you want to disable.

5. Click **Disable**.



Assigned SecurID Tokens

☑	Serial Number	Type	Disabled	Replacement	PIN Set	New PIN	Next TC
☑	000000100000	Softwa...				✓	

6. When prompted, click **Disable Token(s)**.

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.

View a Token

You can view all tokens that have been imported to security domains included in the scope of your administrative role. You can view both assigned and unassigned tokens.

Procedure

1. In the Security Console, click **Authentication** > **SecurID Tokens** > **Manage Existing**.

2. Click the **Assigned** and **Unassigned** tabs to alternately view assigned and unassigned tokens respectively.
3. Use the search fields to find the token that you want to view.
4. From the context menu, select **View**.

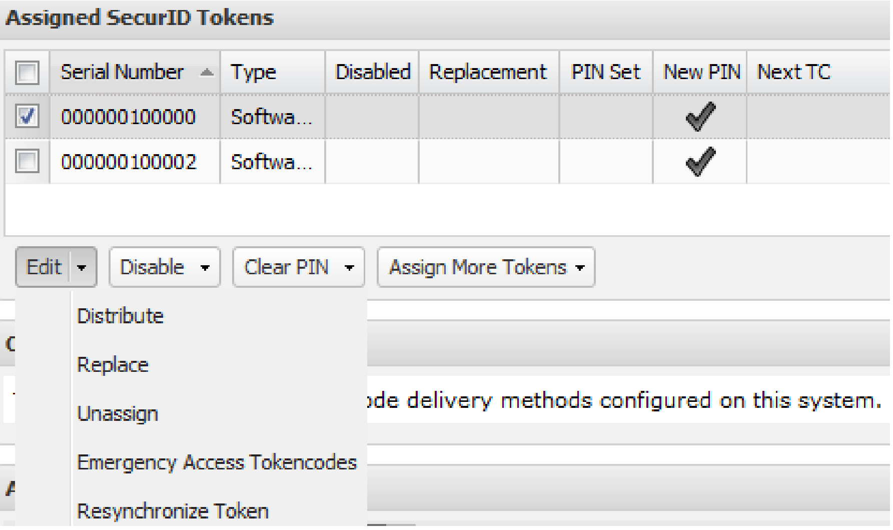
Replace a Token for a User in the User Dashboard

Occasionally, you must assign a new token to a user. For example, you must assign a new token to a user whose existing token has been permanently lost or destroyed. A user also needs a new token if his or her current token has expired.

Replaced tokens are either unassigned or deleted from the deployment, depending on your configuration.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose token you want to replace.
4. Under **Assigned SecurID Tokens**, click the token you want to replace.
5. Click the arrow next to the **Edit** button and select **Replace**.



Assigned SecurID Tokens

☐	Serial Number	Type	Disabled	Replacement	PIN Set	New PIN	Next TC
☑	000000100000	Softwa...				✓	
☐	000000100002	Softwa...				✓	

ode delivery methods configured on this system.

6. Select a token from the list or search for a token in the search bar.
7. Click **Replace Token**.

Resynchronize a Token in the User Dashboard

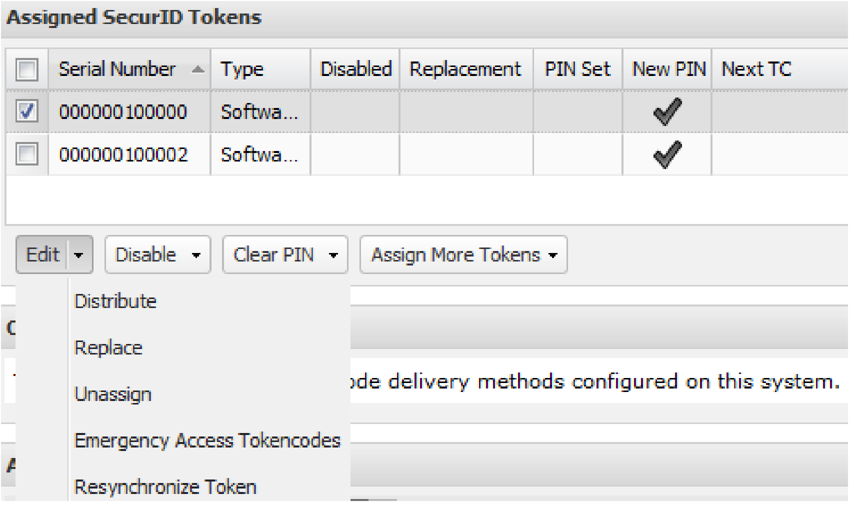
A token must be resynchronized when the tokencode displayed on the token does not match the tokencode generated by Authentication Manager. When the tokencodes do not match, authentication attempts fail. Depending on your configuration, users can resynchronize tokens with the Self-Service Console.

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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose token you want to resynchronize.
4. Under **Assigned SecurID Tokens**, click the token you want to resynchronize.
5. Click the arrow next to the **Edit** button and select **Resynchronize Token**.



Assigned SecurID Tokens

□	Serial Number	Type	Disabled	Replacement	PIN Set	New PIN	Next TC
☑	000000100000	Softwa...				✓	
□	000000100002	Softwa...				✓	

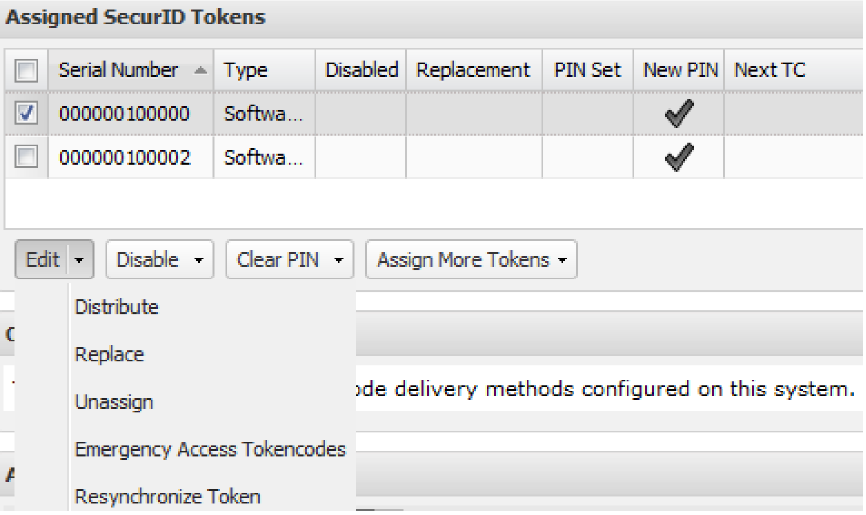
6. Type the current tokencode.
7. Type the next tokencode.
8. Click **Resynchronize**.

Unassign a Token from a User in the User Dashboard

When you unassign a token, the user can no longer use the token to authenticate and the token is disabled. If you reassign the token to another user, it is automatically re-enabled.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose token you want to unassign.
4. Under **Assigned SecurID Tokens**, click the token you want to unassign.
5. Click the arrow next to the **Edit** button and click **Unassign.**



Assigned SecurID Tokens

☐	Serial Number	Type	Disabled	Replacement	PIN Set	New PIN	Next TC
☑	000000100000	Softwa...				✓	
☐	000000100002	Softwa...				✓	

6. When prompted, click **Unassign Token**.

7 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 web-based 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.

Enable On-Demand Authentication for a User in the User Dashboard

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. You can use ODA to protect web-based resources, such as an SSL-VPN, thin client, or web portal.

Enable ODA for users so that they can receive on-demand tokencodes.

Before You Begin

On-demand tokencode delivery must be configured for your deployment.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user for whom ODA must be enabled.
4. Under **On-Demand Authentication (ODA)**, click **Manage**.
5. For **Enable User**, select **Enable user for on-demand authentication**.
6. (Optional) Set an expiration date for the on-demand tokencode.
7. Enter the user’s mobile phone number.
8. Use the **Associated PIN** options to specify how the user's initial PIN is created. Create an initial PIN if necessary.
9. Click **Save**.

Enable Users to Set Initial On-Demand Authentication PINs in the User Dashboard

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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user for whom ODA must be enabled.
4. Under **On-Demand Authentication (ODA)**, click **Manage**.
5. For **Enable User**, select **Enable user for on-demand authentication**.
6. Select **Require user to set the PIN through the RSA Self-Service Console**.
7. Click **Save**.

Clear a User's On-Demand Authentication PIN in the User Dashboard

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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user you whose ODA PIN you need to clear.
4. Under **On-Demand Authentication (ODA)**, click **Manage**.
5. In **Associated PIN**, select **Clear existing PIN and set temporary PIN for the user**.
6. Enter a new PIN.
7. Click **Save**.

Disable On-Demand Authentication for a User in the User Dashboard

Disable on-demand authentication (ODA) for a user when you no longer want to allow the user to request on-demand tokencodes. You can do this, for example, when users who needed temporary access no longer need it.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user for whom ODA must be disabled.
4. Under **On-Demand Authentication (ODA)**, click **Manage**.
5. For **Enable User**, deselect **Enable user for on-demand authentication**.
6. Click **Save**.

8 Emergency Access

This chapter provides information on two kinds of emergency access, online emergency access and offline authentication.

Online Emergency Access

You can provide emergency access for users with misplaced, lost, stolen, or damaged tokens through the use of an online emergency access tokencode. There are two types of online emergency access tokencodes:

- Temporary fixed tokencode. Used with the user's PIN. You can configure the expiration date.
- One-time tokencode set. A set of tokencodes. Each tokencode can be used only once, and is used with the user's PIN.

An online emergency access tokencode provides two-factor authentication. This tokencode is an 8-character alphanumeric code generated by Authentication Manager. Similar to the tokencode that is used under non-emergency circumstances, the online emergency access tokencode is combined with the user's PIN to create a passcode.

The format of the online emergency access tokencode is determined by the token policy of the security domain to which it belongs.

If the user has an expired token, you need to replace the token, and then provide temporary access. An online emergency access tokencode cannot be assigned to an expired token.

Assign a Temporary Fixed Tokencode

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**.

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**.

Offline Authentication

Offline authentication provides emergency access for RSA SecurID for Windows users who require emergency access while authenticating offline. Temporary emergency access can be provided for users:

- With a misplaced, lost, or stolen token. See Provide an Offline Emergency Access Tokencode on page 72. Users authenticate with their PIN and emergency tokencode.
- Who have forgotten their PIN. See Provide an Offline Emergency Passcode in the User Dashboard on page 72.

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 in the User Dashboard

Users who forgot their PIN may need 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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user you want to whom you want to provide a temporary fixed passcode.
4. Under **User Profile**, click **Authentication Settings**.
5. In **Fixed Passcode**, select **Allow authentication with a fixed passcode**.
6. In the **Fixed Passcode** and **Confirm Fixed Passcode** fields, enter a new passcode.
7. Click **Save**.

9 Managing RSA SecurID PINs

RSA SecurID PINs

A personal identification number (PIN) is a numeric password used to authenticate a user.

Users may be required to create PINs containing both letters and numbers and to change their PINs at regular intervals. A lost or stolen PIN puts protected resources at risk. For this reason, you should instruct users to report compromised PINs as soon as possible.

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 in the User Dashboard on page 75.

Users can also use the Self-Service Console to reset their PINs.

Clear an RSA SecurID PIN in the User Dashboard

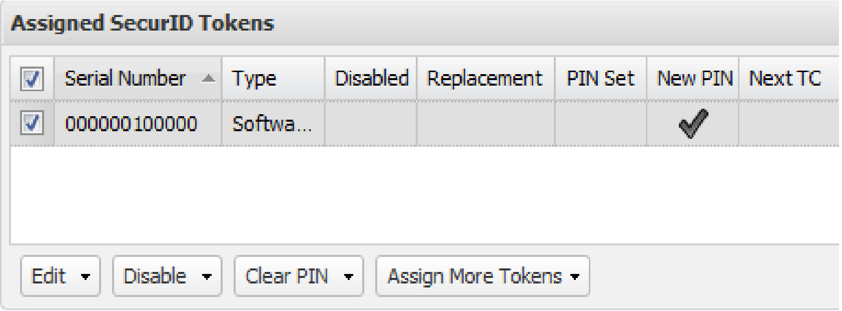
When a user forgets a SecurID PIN, you can clear the PIN so that the user can create a new one. When you clear a user's PIN, the user can create a new PIN the next time the user authenticates.

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, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose PIN needs to be cleared.
4. Under **Assigned SecurID Tokens**, click the token with the PIN that needs to be cleared.

5. Click **Clear PIN**.



Assigned SecurID Tokens

☑	Serial Number	Type	Disabled	Replacement	PIN Set	New PIN	Next TC
☑	000000100000	Softwa...				✓	

6. When prompted, click **Clear PIN(s)**.

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. page 132

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.

10 RSA Self-Service

RSA Self-Service

RSA 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 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.

Certain tasks related to Self-Service still require administrative assistance. As a Help Desk Administrator, you may be asked to perform the following tasks:

- Clear a Cached Copy of Windows Credentials in the User Dashboard on page 77
- Managing Security Questions on page 36

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.

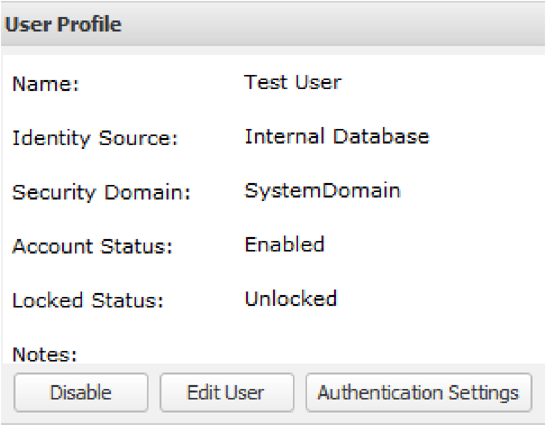
Clear a Cached Copy of Windows Credentials in the User Dashboard

If Windows password integration is enabled in the offline authentication policy, users can authenticate with only a Windows user name and an RSA SecurID passcode. This feature causes RSA Authentication Manager to save users’ Windows passwords, which become invalid if the Windows password has been changed. You can avoid a failed logon attempt by clearing the saved copy of the user's Windows password.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose cached passwords you want to clear.

4. Under **User Profile**, click **Authentication Settings**.



User Profile

Name:	Test User
Identity Source:	Internal Database
Security Domain:	SystemDomain
Account Status:	Enabled
Locked Status:	Unlocked
Notes:	

5. Select the **Clear cached copy of selected user's Windows credential** checkbox to clear a cached version of the user's Windows password.

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.

Self-Service Request Management

Self-Service automatically sends e-mail to notify you about user requests that you need to review. The types of requests are:

- Self-Service accounts for new users. A new user is not in a directory server. Users must enter user information for an account.
- Changes in user group membership
- New or additional SecurID tokens
- Replace an expired or about to expire SecurID token
- Replace a broken or permanently lost SecurID token
- On-demand authentication

Approve and Reject User Requests

Self-Service automatically sends e-mail to Request Approvers about user requests. Each approval step requires a unique Request Approver. After you approve a request, Self-Service sends e-mail to the next participant (either a Request Approver or Token Distributor) in the workflow. If you are the last participant in the workflow, Self-Service sends users an e-mail informing them their request has been accepted or rejected.

Procedure

1. In the Security Console, click **Administration** > **Provisioning**.
2. Click the **Pending** tab to see all open user requests. If no requests appear, click **Search** to refresh the screen.
3. Click the request you want to work with.
4. Complete any missing information, and make any necessary changes to the request.
5. Under **Action Required**, select an option:
   - **Defer Action** - Saves the request without taking any action.
   - **Approve request -** Approves the request. When approved, the user receives e-mail indicating that the request has been approved.
   - **Reject request -** Rejects the request. When rejected, the user receives e-mail indicating that the request has been rejected.

6. (Optional) Add comments to the request. Your comments appear in the e-mail sent to the user when you take action on a request.
7. (Optional) Notes. Add any notes that you want to keep about this request. These notes are not sent to the user.
8. Click **Go**.

Search for User Requests

You can search for pending or closed provisioning requests by security domain and identity source. For example, you might want to know how many requests need approval.

Search results are only returned for the type of user requests for which you search. For example, if you search for requests that require approval, you must run a new search to view requests that require distribution or select "All" from the **Status** drop-down menu to see all types of requests.

Procedure

1. In the Security Console, click **Administration** > **Provisioning**.
2. Decide if the request you want to search for is pending or closed, and click the appropriate tab.
3. On the **Search** panel, from the **Security Domain** drop-down list, select the security domain you want to search.
4. From the **Identity Source** drop-down list, select the identity source of the user whose request you want to find.
5. From the **Status** drop-down menu, select the type of request you want.
6. Use the **Where** field to select the search criteria. For example, enter “User Last name,” “starts with” and “S” to search for requests made by the users with last names that start with S.
7. Click **Search**.

View User Requests

You can view pending and closed provisioning requests in the Security Console. For example, you can view a request to learn its status.

Procedure

1. In the Security Console, click **Administration** > **Provisioning**.
2. Click the **Pending** tab to see all open requests, and the **Closed** tab to see all closed requests.
3. Use the search fields to find the request you want to view.
4. Click the request you want to view.

Complete User Requests

Self-Service automatically sends e-mail to Request Approvers about user requests that need to approval. After the request is approved, Self-Service sends an e-mail notification to the next participant in the workflow. Each approval step requires a unique Request Approver. To complete a request, a Request Approver may have to give final approval to the request, or distribute a token to a user.

Procedure

1. In the Security Console, click **Administration** > **Provisioning**.
2. Click the **Pending** tab to see all open user requests. If no requests display, click **Search** to refresh the screen.
3. Click the user request with which you want to work.
4. Complete any missing information, and make any necessary changes to the request.
5. Under **Action Required**, do one of the following.
   - Select **Defer Action** and click **Submit**.
     The Provisioning page displays.
   - Select **Approve Request** and do one of the following.
     - If you have distribution steps, click Submit & Continue.

       The Properties page displays, where you continue this procedure with step 6.
     - If you have no distribution steps, click Submit.

       The Provisioning page displays.
   - Select **Reject Request** and click **Submit**.
     The Provisioning page displays.
6. On the Properties page, under **Action Required**, select **Complete action item by indicating how to assign and distribute token** and do one of the following:
   - For hardware tokens:
     - Under **Assignment Method,** select the method you want to use to assign the token:

       Notify third-party or user to assign token - If you use a third-party distribution company to distribute tokens, decide how to notify the company or users to assign tokens.
       Assign SecurID token serial number myself - If you assign the token yourself, type the hardware token serial number in this field.
     - Under **Distribution Method**, select the method you want to use to deliver the token to the user:

       Notify third-party to deliver or **Deliver the token myself**
   - For software tokens, select **Mark action item as completed** to close the request.

7. (Optional) Under **Comment to User**, enter any comments that you want sent to the user in an e-mail.
8. Click **Submit**.

Cancel User Requests

Occasionally, it may be necessary to cancel a user request. When this happens, Self-Service generates an e-mail that contains comments from the workflow participant who canceled the request and sends it to the user.

Procedure

1. In the Security Console, click **Administration** > **Provisioning**, and then click the **Pending** tab to see all open user requests. If no requests appear, click **Search** to refresh the screen.
2. Click the checkbox of the request you want to cancel.
3. From the Action menu, select **Cancel Request**.
4. Click **Go**.
5. Under **Comment to User**, enter the reason why you canceled the request.
6. Click **Cancel Requests**.

11 Managing Reports

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 a supplied template. Each template allows you to choose the types of information being reported and which parameters to apply in order to refine that information. You can view activities for all administrators, or you can display detailed information on one administrator.

In addition, you can perform the following reporting tasks:

- View and download completed reports, view reports that are currently running or reports that are waiting in the report queue.You can view the report output in the Security Console, or download the report as a CSV, XML, or HTML file.
- Transfer reports to other security domains. When running a report, change the report ownership so that the administrative scope is narrowed or broadened.

Run a Report Job

To generate output from a report that you have created, you must run the report. After you run the report, you can view the report output in a browser, or save the report as a CSV, XML, or HTML file.

When you run the report, make sure that you download it to your local machine, and view it using the associated applications.

You may only run reports that fall within the scope of your administrative role. If an error indicates that you have insufficient privileges, review your permissions carefully. The report fails if it needs to access data that you are not permitted to view. For example, the All Users report requires permission to view all of the security domains in the deployment because it accesses the security domains to which the reported users belong.

Procedure

1. In the Security Console, click **Reporting** > **Reports** > **Manage Existing**.
2. Click the report that you want to run, and click **Run Report Job Now**.

3. Enter any input parameters required by the report.
4. Click **Run Report**.
5. Click the **Completed** tab to view the report output.

View a Report Template

You can view a list of all saved report templates. After the list displays, you may edit or run the reports in the list.

Procedure

1. In the Security Console, click **Reporting** > **Reports** > **Manage Existing**.
2. Use the search fields to find the report that you want to view.
3. Click the report, and click **View**.

View An In Progress Report Job

You can only view reports that are included in your administrative scope.

Procedure

In the Security Console, click **Reporting** > **Report Output** > **In Progress**.

You can cancel the report job from this tab.

View A Completed Report

Perform this procedure to view the output of a completed report saved in the system.

Procedure

1. In the Security Console, click **Reporting** > **Report Output** > **Completed Reports.**
2. Under the **Completed** tab, click the report job that you want to view, and select how to display it. You can save the report output as a CSV, XML, or HTML file. You can also choose to send the output directly to a web browser for display. The figure below shows an example of a output that is viewed in a web browser.

Be sure to delete reports when they are no longer needed.

Edit a Report

You can edit a report to change information that is included in the report or to change the information that must be entered when a report is run.

Only the administrator who created the report can change the **Run As** option.

Procedure

1. In the Security Console, click **Reporting** > **Reports** > **Manage Existing**.
2. Select the report that you want to edit, and click **Edit**.
3. Make any necessary changes to the report.
4. Click **Save**.

   If you have not saved your edits, you can click **Reset** to reset the report to be as it was before you began editing.

12 Monitoring User Activity in Real-Time

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 four Activity Monitors; Authentication Activity, System Activity, and Administration Activity open in a separate browser window and displays a different type of information, while Authentication Activity Monitor in the User Dashboard opens in the User Dashboard.

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.
Authentication Activity Monitor in the User Dashboard	• Log entries for authentication activity over the past seven days for one user, maximum of 50 records • 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.

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.

View Recent Authentication Activity in the User Dashboard

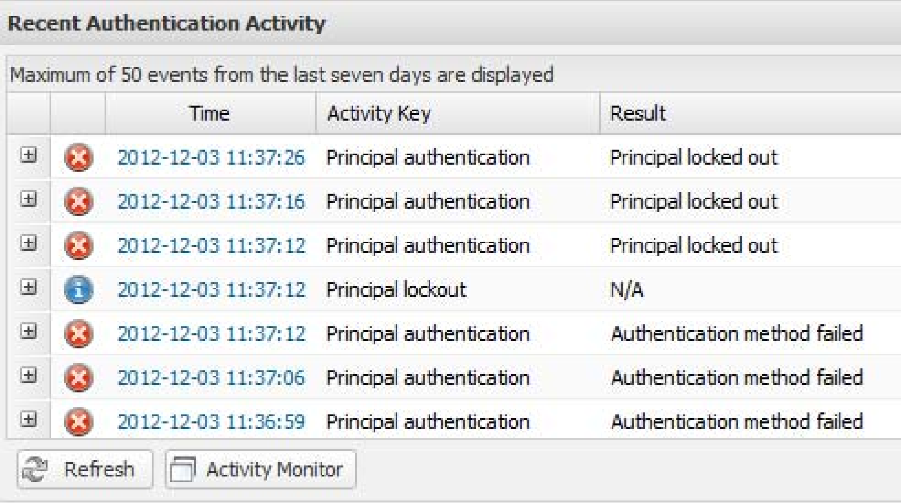
You can view a user's authentication activity through the User Dashboard in real time. You can customize the information displayed. A maximum of 50 records can be shown.

Procedure

1. In the Security Console, go to the Home page.
2. Use **Quick Search** to find the user.
3. Select the user whose recent authentication you want to view.

4. Under **Recent Authentication Activity**, the user’s recent authentication activities are listed.

   This is an example of a user’s activities for the past seven days. It covers the time of each activity, a description of each activity, and the result of the activity.



Recent Authentication Activity

Maximum of 50 events from the last seven days are displayed

		Time	Activity Key	Result
⊞	✖	2012-12-03 11:37:26	Principal authentication	Principal locked out
⊞	✖	2012-12-03 11:37:16	Principal authentication	Principal locked out
⊞	✖	2012-12-03 11:37:12	Principal authentication	Principal locked out
⊞	ℹ	2012-12-03 11:37:12	Principal lockout	N/A
⊞	✖	2012-12-03 11:37:12	Principal authentication	Authentication method failed
⊞	✖	2012-12-03 11:37:06	Principal authentication	Authentication method failed
⊞	✖	2012-12-03 11:36:59	Principal authentication	Authentication method failed

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