

RSA[®] Authentication Manager 8.2 Security Configuration Guide



Contact Information

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

Trademarks

RSA, 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 Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

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

Distribution

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

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

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

Contents

Preface	5
About This Guide.....	5
RSA Authentication Manager 8.2 Documentation	5
Support and Service	7
Before You Call Customer Support.....	7
Chapter 1: Security Configuration	9
Security Configuration.....	9
Access Control Settings	9
User Authentication.....	9
User Authorization.....	9
Component Access Control	10
System Administrator Accounts	10
Authentication Manager Administrator Accounts.....	10
Appliance Operating System Account.....	11
Super Admin Restoration.....	12
Change an Operations Console Administrator's Password.....	12
Password Policies.....	13
Configuring Administrative Role Scope and Permissions.....	13
Token Protection.....	15
Tokencode Tokens (No PIN Required)	15
Token File Protection.....	16
Token Serial Number Masking in Log Messages.....	16
Hardware Token Distribution	17
Software Token Distribution	17
Dynamic Seed Provisioning for Software Token Delivery	17
On-Demand Authentication Tokencode Delivery	18
Lost Tokens.....	18
Software Development Kit.....	19
Monitoring & Auditing	19
Policies and Roles.....	19
Monitoring Authentication Manager	19
Log Messages	20
Log Types	20
Logging Levels	20
Real-Time Log Monitoring.....	21
Appliance Logs	21
Best Practices for Custom Reports.....	22
Communication Security.....	22
Port Usage.....	22
SMTP Encryption	22
Data Security.....	23

Chapter 2: Secure Deployment and Usage	25
Secure Appliance Deployment.....	25
Web Tier Deployment.....	26
Network Infrastructure Hardening	26
Firewalls.....	27
Protecting Sensitive Files.....	28
External Identity Sources	28
Agents	29
Suggested Security Practices for a VMware Virtual Environment.....	29
Suggested Security Practices for a Hyper-V Virtual Environment.....	30
System Hardening	31
BIOS Hardening	32
Command Line Privileges	32
NFS Server and Windows Share Security	33
RSA Authentication Manager Services That Start Automatically	34
Chapter 3: Secure Maintenance	35
RSA Authentication Manager Updates.....	35
Operating System Access.....	36
Run Clam Antivirus Software.....	37
Protecting Backups	38
Chapter 4: Physical Security Controls	39
Protecting the Authentication Manager Environment	39
Physical Security Controls.....	39
Remote Access to Server Environments.....	40
Chapter 5: Supporting End Users	41
Procedures and Training	41
Preventing Social Engineering Attacks.....	41
Confirming a User’s Identity	42
PIN Management	42
Advice for Users	44
Emergency Access and Static Tokencodes.....	45

Preface

About This Guide

This guide is intended to help identify configuration options and best practices designed to help ensure correct operation of RSA® Authentication Manager 8.2, and to offer maintenance recommendations. However, it is up to you to ensure the products are properly monitored and maintained and to develop appropriate corporate policies regarding administrator access and auditing.

When deploying software tokens, use this guide in conjunction with your software token documentation and the *RSA SecurID Software Token Best Practices Guide*.

In addition to the recommendations in this guide, RSA strongly recommends that you follow industry best practices for hardening the network infrastructure, such as applying the latest Authentication Manager product updates, segmenting your network, and monitoring your network for intrusions.

RSA Authentication Manager 8.2 Documentation

RSA Authentication Manager 8.2 includes the following documentation.

Title	Purpose
Configuration	
<i>Planning Guide</i>	Describes the high-level architecture of Authentication Manager and how it integrates with your network.
<i>Hardware Appliance Getting Started</i>	Describes how to deploy a hardware appliance and perform the Authentication Manager Quick Setup process.
<i>Virtual Appliance Getting Started</i>	Describes how to deploy a virtual appliance and perform the Authentication Manager Quick Setup process.
<i>Setup and Configuration Guide</i>	Describes how to set up and configure Authentication Manager, and how to upgrade from version 8.1 Service Pack 1 to version 8.2.
<i>Security Configuration Guide</i>	Describes the security configuration settings available in RSA Authentication Manager. It also describes secure deployment and usage settings, secure maintenance, and physical security controls.

Title	Purpose
Administration	
<i>Administrator's Guide</i>	Provides an overview of Authentication Manager and its features. Describes how to configure the system and perform a wide range of administration tasks, including managing users and security policies.
<i>Developer's Guide</i>	Provides information about developing custom programs using the RSA Authentication Manager application programming interfaces (APIs). Includes an overview of the Authentication Manager APIs and the related Javadoc.
<hr/> <p>Note: The software development kit (SDK) is located in the RSA Authentication Manager SDK directory of the RSA Authentication Manager 8.2 Extras ZIP file. The Extras ZIP file is located on Download Central at https://download.rsasecurity.com.</p> <hr/>	
<i>Help Desk Administrator's Guide</i>	Provides instructions for the most common tasks that a Help Desk Administrator performs.
<i>RSA RADIUS Reference Guide</i>	Describes the usage and settings for the initialization files, dictionary files, and configuration files used by RSA RADIUS.
<i>SNMP Reference Guide</i>	Describes how to configure Simple Network Management Protocol (SNMP) to monitor an instance of Authentication Manager on a hardware appliance or a virtual appliance.
<i>Troubleshooting Guide</i>	Describes the most common error messages in RSA Authentication Manager and provides the appropriate actions to troubleshoot each event.
<i>AMBA Custom Application Guide</i>	Describes how the RSA Authentication Manager Bulk Administration (AMBA) command-line utility simplifies the bulk administration of users, tokens, agents, and so on. Requires a standalone AMBA license or an Enterprise license.
Online Help	
<i>Security Console Help</i>	Describes day-to-day administration tasks performed in the Security Console.
<i>Operations Console Help</i>	Describes configuration and setup tasks performed in the Operations Console.

Title	Purpose
<i>Self-Service Console Help</i>	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 .
<i>RSA Token Management Snap-In for the Microsoft Management Console Help</i>	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.

Support and Service

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

The RSA Ready Partner Program website at www.rsaready.com provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with 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 you 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

Security Configuration

Security Configuration

This chapter provides an overview of the settings available in RSA Authentication Manager to ensure a secure operation of the product. Security settings consist of:

- [Access Control Settings](#). Limit access by end user or by external product components
- [Monitoring & Auditing](#). Settings related to the logging of events
- [Communication Security](#). Security for Authentication Manager network communications
- [Data Security](#). Helps ensure protection of the data handled by Authentication Manager.

Access Control Settings

Access control settings consist of:

- [User Authentication](#)
- [User Authorization](#)
- [Component Access Control](#)

User Authentication

The following user authentication settings control the process of verifying a user's identity when the user attempts to access Authentication Manager:

Default Accounts. For a list of the default appliance accounts, see [System Administrator Accounts](#) on page 10.

Authentication Configuration. The Super Admin account controls the initial administrative access to the Security Console. The Super Admin user creates additional administrator accounts and designates the allowable authentication methods for those accounts.

User Authorization

Authenticated administrators configure all permissions through the Security Console. For more information on permissions, see the chapter "Preparing RSA Authentication Manager for Administration" in the *Administrator's Guide*.

You can deploy a custom logon banner that displays before administrators or users access Authentication Manager. The logon banner is often used for legal reasons, for example, to warn users that only authorized personnel have permission to access the system. For more information, see the chapter “Administering RSA Authentication Manager” in the *Administrator’s Guide*.

Component Access Control

These component access control settings define control over access to the product by external and internal systems or components:

Component Authentication. Administrators cannot configure authentication between the components of RSA Authentication Manager.

Component Authorization. With the exception of enabling replica instances or a web tier, administrators cannot configure authorization of or restrict access to components of Authentication Manager. Authorization and access restrictions are set to default methods that cannot be changed.

System Administrator Accounts

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

- [Authentication Manager Administrator Accounts](#)
- [Appliance Operating System Account](#)

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

Authentication Manager Administrator Accounts

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

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

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

User IDs for a Super Admin and a non-administrative user are validated in the same way. A valid User ID must be a unique identifier that uses 1 to 255 ASCII characters.

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

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

Appliance Operating System Account

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

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

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

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

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

For more information, see the Operations Console Help topics “Enable Secure Shell on the Appliance” and “Change the Operating System Account Password.”

Super Admin Restoration

Your deployment must have at least one Super Admin. Only a Super Admin can perform certain critical tasks:

- Delegate roles to all other administrators.
- Create the security domain hierarchy.

RSA recommends that you assign the Super Admin role to only the most trusted administrators.

You need to restore a Super Admin if any of the following conditions exist:

- The sole Super Admin has been deleted from the deployment.
- No users have been assigned the Super Admin role.
- The sole Super Admin has been locked out.

If a Super Admin has been locked out, recovery can occur in any of the following ways:

- Another Super Admin can manually unlock the Super Admin.
- If the lockout policy that applies to the Super Admin allows auto-unlock, you can wait for lockout to expire.
- If the previous methods fail, use the Super Admin Restoration utility, `restore-admin`, to create a new Super Admin. For instructions, see “Restore the Super Admin” in the chapter “Advanced Administration” in the *Administrator’s Guide*.

Change an Operations Console Administrator's Password

Before You Begin

You must be a Super Admin.

Procedure

1. In the Security Console, click **Administration > Manage OC Administrators**.
2. Next to the Operations Console administrator whose password you wish to modify, click **Change Password**.
3. In the **Create New Password** field, enter the Operations Console administrator’s new password.

The password must be between 8 and 32 characters, contain at least 1 alphabetic character, at least 1 special character, and may only contain characters in the basic ASCII character set, excluding space, @, and ~. The password may not match the corresponding user ID.

4. In the **Confirm New Password** field, reenter the new password.

5. Click **Save**.

Note: It can take from fifteen to thirty minutes for changes to an Operations Console administrator's account to replicate to a replica instance.

Password Policies

To enforce strong passwords, which will help secure sessions, RSA strongly recommends that you configure all password policies to meet the following minimum requirements:

- Minimum Password Length: 15 Characters
- Alpha Characters Required: 2 Characters
- Numeric Characters Required: 1 Character
- Special Characters Required: 1 Character
Users cannot use the following characters: space / ; : ,
- Uppercase Characters Required: 1 Character
- Lowercase Characters Required: 1 Characters
- Password Change Interval: 90 Days
- Previous Passwords Disallowed: 20 Passwords
- Maximum Failed Login Attempts: 3 Attempts

Configuring Administrative Role Scope and Permissions

The pre-defined administrative roles configured as part of Authentication Manager setup have scope over the top-level security domain by default. As a result, it is possible for administrators who are assigned one of these pre-defined roles to modify the account of a Super Admin, because the initial Super Admin account resides in the top-level security domain as well. This is because the top-level security domain is the only security domain in the system when Authentication Manager is initially set up.

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

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

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

- Make sure that the scope of the administrator does not include the following:
 - A security domain that contains the user account or token of a higher-privileged administrator.
 - The security domain that contains the administrator’s own token so that the administrator cannot modify his own token or other credentials to provide additional privileges to his account.
 - The administrator’s own security domain so that the administrator cannot modify his own account.
- Create separate security domains to enforce your intended administrative scopes. For example, create one for Super Admins, one for other administrators and one for users with no administrative role. Reduce the scope of the lower-privileged administrators to the security domains of users with no administrative role. Configure Authentication Manager according the following model:
 - Create a distinct security domain for Super Admins.
 - Place all other administrators, including those who have permission to edit users or authentication credentials, in lower-level domains.
 - Place all other users in another security domain.
 - Assign the appropriate role and scope to administrators. Make the lower-privileged administrator’s scope include only the security domain over which the administrator has authority. For example, make sure that the Help Desk administrator has scope only for the security domain of end users, and not for his own security domain or the security domain of the Super Admin. For instructions, see the Security Console Help topic, “Change the Scope of an Administrative Role.”

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

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

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

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

Token Protection

Importing new tokens and distributing tokens to users are sensitive operations and if not done properly could expose an organization to security risks. The following sections contain recommendations designed to minimize risk during these sensitive operations.

Important: RSA strongly 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.

Tokencode Tokens (No PIN Required)

If you use RSA SecurID tokens that do not require a PIN (also known as Tokencode tokens), you should ensure that a second authentication factor, such as a Windows password, is required to authenticate to protected systems.

Important: If the deployment does not have a second factor and one cannot be implemented, RSA strongly recommends switching your RSA SecurID tokens to require a PIN. If you cannot switch all tokens to require a PIN, RSA strongly recommends regularly auditing agents on systems that do not require a second authentication factor for token users without a PIN.

Implement help desk procedures that ensure that administrators:

- Allow a user to authenticate with a Tokencode token only when the user requires access to systems that enforce an additional authentication factor.

- Allow a user to authenticate with a Tokencode token only when a second authentication factor is required on every resource the user may access.
- Flag groups that contain users with Tokencode tokens to ensure that these groups are enabled only on agents that protect resources that require a second authentication factor.

RSA strongly recommends that the audit trails of the following administrative activities be carefully monitored:

- Agent creation
- Group creation and assignment
- Group membership changes
- Token assignment
- Tokencode token enablement

Token File Protection

RSA Manufacturing or certified partners deliver token files for import into your deployments. These files enable the use of strong authentication, and they contain sensitive information about tokens. RSA strongly recommends the following best practices:

- Limit access to these files to individuals responsible for importing tokens into RSA Authentication Manager.
- Store encrypted backup copies of token XML files in a secure location with no network connectivity.
- Files used for the import operation should be permanently deleted from the file system after the import operation is complete. If you use multiple systems as temporary storage locations, immediately delete the token files from the temporary locations as soon as you import the files.
- Secure any media used to deliver token information to you.

Token Serial Number Masking in Log Messages

RSA strongly recommends that you implement token serial number masking to enhance protection of token serial numbers.

Token serial number masking is designed to allow you to mask part of the token serial number in log data that is sent over the network. This capability helps ensure that any log data sent in the clear over a non-secured network follows RSA Authentication Manager best practices. You can configure how many token serial number digits to display in the log message. Masked digits display as the 'x' character. The masked digits are always at the beginning of the serial number, while the exposed digits are always at the end. For example, if you configure token serial number masking to include 4 digits, the number displays as xxxxxxxx7056.

For instructions, see the Security Console Help topic "Mask Token Serial Numbers in Logs."

Hardware Token Distribution

Take the following steps to protect hardware tokens during distribution:

- Distribute hardware tokens in a disabled state.
- Before enabling a token, Help Desk administrators should confirm the user's identity. For example, ask the user one or more questions to which only he or she knows the answer.
- Do not record the user's serial number outside the Authentication Manager server.

See [Preventing Social Engineering Attacks](#) on page 41.

Software Token Distribution

RSA strongly recommends that you take the following steps to protect software tokens during distribution:

- When generating the token files for distribution, protect the files with a password, which encrypts the file. Use passwords that conform to best practices. For more information, see [Password Policies](#) on page 13.
- Use the RSA Security Console to bind software tokens to device IDs when issuing software tokens. This limits the installation of tokens to only those machines that match the binding information. See the chapter “Deploying and Administering RSA SecurID Tokens” in the *Administrator's Guide*.
- RSA recommends that you use dynamic seed provisioning to distribute software tokens. For more information, see [Dynamic Seed Provisioning for Software Token Delivery](#).

Dynamic Seed Provisioning for Software Token Delivery

Dynamic seed provisioning is a client-server protocol that enables secure, rapid setup of software tokens. A feature of RSA Authentication Manager 8.2, dynamic seed provisioning uses the industry-standard Cryptographic Token Key Initialization Protocol (CT-KIP).

Dynamic seed provisioning eliminates the need for a token distribution file. Instead, the software token application running on the device (the client) and Authentication Manager (the server) use a four-pass CT-KIP protocol to exchange information that is used to dynamically generate a unique seed on the client and the server. In this way, the CT-KIP protocol protects against potential interception of the seed.

After you complete the software token provisioning steps, 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.

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 user with a QR Code that encapsulates the CT-KIP URL and activation code. Scanning the QR Code in the Self-Service Console imports and activates the token.
- 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.

For more information, see the chapter “Deploying and Administering RSA SecurID Tokens” in the *Administrator’s Guide*.

On-Demand Authentication Tokencode Delivery

On-demand authentication (ODA) delivers a one-time tokencode to a user’s mobile phone or e-mail account. ODA is easy to deploy because it does not require extra hardware, such as physical tokens. Employees already have and use mobile phones and e-mail accounts.

To increase security when you enable on-demand authentication (ODA) tokencodes for a user, follow these guidelines:

- Help Desk administrators should confirm the user’s identity. For example, ask the user one or more questions to which only he or she knows the answer.
- Ensure that ODA tokencodes expire within a short period of time. Configure as short a period of time as your organization needs. RSA strongly recommends that this be no more than 15 minutes.
- Users should be trained to use ODA tokencodes immediately when they receive them.

Lost Tokens

A lost token can be an RSA SecurID hardware authenticator or a software token on a user’s mobile phone. When a user reports a lost token, RSA strongly recommends that Help Desk Administrators perform the following steps:

- Confirm the user’s identity. For example, ask the user one or more questions to which only he or she knows the answer.
- Ask the user when they lost the token.
- Disable the token.
- Make note of the date and audit your logs for authentication attempts with the lost token until the token is recovered.
- Follow your organization’s security policy to address any suspicious authentication attempts.

Software Development Kit

When using the Software Development Kit, RSA strongly recommends that you:

- Obfuscate the command client password whenever possible.
- Never accept passwords on the command line.
- Protect any secrets you manage.

Monitoring & Auditing

As with any critical infrastructure component, you should constantly monitor your system and perform periodic and random audits (configuration, permissions, and so on).

Policies and Roles

At a minimum, you should periodically review that the following settings match company policy and functional needs:

- Configuration settings
- Policies
- Administrative roles and associated permissions
- Which administrators are assigned to which roles
- Agent host enabled lists

Note: Verify that unauthorized users are not enabled through membership in a nested group.

Monitoring Authentication Manager

RSA strongly recommends the following:

- Run network intrusion detection systems and host intrusion detection systems in your environment.
- Run Simple Network Management Protocol (SNMP). SNMP can monitor the state of Authentication Manager and perhaps indicate possible attacks. For information on using SNMP, see the chapter “Logging and Reporting” in the *Administrator's Guide*.
- Monitor which ports are open. For information about port usage, see the *Planning Guide*.

- Audit and analyze system and application logs periodically. You can use a security information and event management (SIEM) solution, such as RSA enVision, to help you with this task.
- Retain log data in compliance with your security policies and local laws. For information about methods of monitoring the Authentication Manager, see the chapter “Logging and Reporting” in the *Administrator's Guide*.

Log Messages

RSA Authentication Manager generates log messages for all events. These messages are stored in log and database files according to the origin of the message. You can use these log files to monitor deployment activity and produce a record of events such as user logon requests or administrative operations.

Most log settings are instance-based, unless you choose to replicate logging configuration changes. The exception is log rotation settings, which are configured in the Operations Console on each instance.

The system does not log most successful read actions.

Log Types

Authentication Manager maintains the following types of logs:

- **Administrative Audit.** Log messages that record administrative actions, such as adding and editing users. This category does not include system level failures of administrative actions. Those messages are captured in the system log.
- **Runtime Audit.** Log messages that record any runtime activity, such as authentication and authorization of users.
- **System.** System level messages, such as “Server started” and “Connection Manager lost db connection.” This category includes system level failures of administrative actions.

Logging Levels

For each type of log, you can use the Security Console to configure the level of detail written to the log files. For example, you might choose to record only fatal errors in the Administrative Audit log, while recording all messages in the System log.

If you change the logging levels and want to return to the default values, select the values listed in the following table.

Log	Default Setting
Administrative Audit Log	Success
Runtime Audit Log	Success
System Log	Warning

Real-Time Log Monitoring

RSA Authentication Manager provides these options to monitor your deployment in real time:

- Activity Monitors
- Support for a remote Syslog host
- Simple Network Management Protocol (SNMP)
- Critical system event notifications

For information on these features, see the chapter “Logging and Reporting” in the *Administrator’s Guide*.

You can also view a user’s authentication activity through the User Dashboard page in the Security Console. For more information, see the Security Console Help topic “User Dashboard.”

Appliance Logs

The appliance maintains operating system logs that track items such as syslog entries, appliance SNMP messages, and Network Time Protocol (NTP) server updates. You can use these logs to monitor the appliance and maintain an audit trail of appliance SNMP and time synchronization operations.

Note: These logs do not duplicate the messages contained in the RSA Authentication Manager logs. For more information, see the Security Console Help topic “Log Archives.”

Authentication Manager maintains the following appliance logs in the **var/log** directory:

messages. Contains syslog messages about the underlying operating system, such as disks, the BIOS, and memory usage and performance.

net-snmpd.log. Used for appliance SNMP log messages.

ntp. Changes to the date and time settings. For example, adding a new NTP server or synchronizing the date and time.

These logs are not included in the backup file, so you must manually back up the log files. Follow your organization's backup and archival policies to determine how often you must back up the log files.

To simplify log data management, the appliance uses a log rotation policy that creates multiple files for the appliance log files. You can specify the log rotation policy for the appliance logs.

For more information on logging, see the Operations Console Help topics “Log Rotation Policy for the Appliance Logs” and “Configure Appliance Log Settings.”

Best Practices for Custom Reports

RSA recommends the following best practices for custom reports:

- For custom reports that directly access the Authentication Manager internal database, make sure that any passwords are obfuscated and rotated on a regular basis.
- Disable the report's service account after the report is run.
- Make sure the report service account only has read-only access to the database.
- Secure output from custom reports in a secure location with no network connectivity. If you need to transfer it over the network, first encrypt the output.
- Restrict access to the custom reports and their outputs.

Communication Security

Secure communication between RSA Authentication Manager components or between Authentication Manager and external systems is enabled by default. You cannot configure the security mechanisms used.

An administrator can replace the existing secure sockets (SSL) certificate that secures communication between your browser and the Security Console, Operations Console, and Self-Service Console. An administrator can replace the default RSA virtual host certificate used by the web tier. There is no ability to alter the SSL security parameters. For more information, see the chapter “Administering RSA Authentication Manager” in the *Administrator's Guide* and the Operations Console Help topic “Web Tier Deployments.”

Port Usage

For a list of the ports that must be accessible to enable authentication, administration, replication, and other services on the network, see the chapter “Planning RSA Authentication Manager Network Integration,” in the *Planning Guide*.

SMTP Encryption

RSA Authentication Manager does not encrypt e-mail. For example, if you are distributing software tokens using dynamic seed provisioning (CT-KIP), you must provide users with the URL link to the CT-KIP server and a unique, one-time token activation code. To more securely provide Authentication Manager data to users, you can do the following:

- Provide the user with a QR Code that encapsulates the CT-KIP URL and activation code. Scanning the QR Code in the Self-Service Console imports and activates the token.
- 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 applicable, configure the Self-Service Console to provide the information to users. Self-Service is a web-based system that enables users to manage their profiles and authenticators. For more information, see the chapter “RSA Self-Service” in the *Administrator's Guide*.

Data Security

Data in the internal database is secure by default. Administrators cannot change the settings for securing data.

Data Encryption. Sensitive data stored in the internal database is encrypted. You cannot configure the encryption method or disable encryption.

Data Integrity. All security-related data in Authentication Manager has data integrity built-in. This detects if security-related data has been tampered with or moved between records. Compromised data causes decryption failure runtime errors in the Authentication Manager log files. You cannot configure or disable data integrity checking.

Data Erasure. You cannot configure secure erasure of data.

You can overwrite deleted appliance log files to make them more difficult to recover later. For more information, see the Operations Console Help topic “Log Rotation Policy for the Appliance Logs.”

2

Secure Deployment and Usage

Secure Appliance Deployment

After you deploy RSA Authentication Manager 8.2 on a hardware appliance or a virtual appliance, the operating system console screen displays a Quick Setup Access Code along with a Quick Setup URL. The Quick Setup Access Code is only available until Quick Setup is complete.

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

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

RSA recommends the following guidelines when deploying an appliance:

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

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

Alternately, you can deploy the hardware appliance and run Quick Setup in a protected test environment and later change the network settings, such as the hostname and IP address, to attach the appliance to your production environment. For more information, see the Operations Console Help topic "Primary or Replica Instance Network Settings Updates."

- Deploy a virtual appliance on an isolated network until Quick Setup is complete. Use VMware or Hyper-V to maintain full control over the appliance. Restrict network access to the appliance, and only allow authorized individuals to access the virtual appliance.
- If you access an appliance to run Quick Setup, and you discover that the appliance has already been configured or you receive error messages because Quick Setup is in progress, then do the following:
 - a. Contact other administrators in your organization to ensure that a malicious user is not trying to take control of the appliance.
 - b. If you believe that the appliance has been compromised, remove the primary or replica instance from your deployment. For instructions, see the chapter "System Maintenance and Disaster Recovery" in the *Administrator's Guide*.

- c. Do one of the following:
 - For a hardware appliance, shut down the appliance and remove the machine from service.
 - For a virtual appliance, suspend the appliance, and quarantine the machine for further investigation.
- d. Contact your IT department or RSA immediately.

Web Tier Deployment

For an additional layer of security, you can deploy RSA Authentication Manager on a web tier to protect your private network. A web tier is a secure platform for installing and deploying the Self-Service Console, dynamic seed provisioning (CT-KIP), and the risk-based authentication (RBA) service.

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

RSA recommends that you do the following:

- Limit network port activity on the web tier. For a list of the ports that must be accessible, see the chapter “Planning RSA Authentication Manager Network Integration,” in the *Planning Guide*.
- Configure an external firewall on your web-tier server.
- Shut down any unnecessary operating system services on the web-tier server. Authentication Manager requires networking services, but other operating system services are not needed. Follow the system hardening guidelines that are provided by Microsoft or Red Hat for your operating system.

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

Network Infrastructure Hardening

To help ensure the highest level of security and reduce the risk of intrusion or malicious system or data access, RSA strongly recommends that you follow industry best practices for hardening the network infrastructure, including, without limitation:

- Run anti-virus and anti-malware tools with the most current definition files.
- Do not directly connect Authentication Manager servers to the Internet or place them in a Demilitarized Zone (DMZ). Instead, use a web tier to receive and manage inbound Internet traffic before it enters the private network. For more information on the Authentication Manager deployment types, see the *Planning Guide*.

- Prevent unauthorized users from changing the time on any local Network Time Protocol (NTP) servers that are accessed by Authentication Manager. Authentication Manager requires accurate date and time settings for replication and authentication. If the token clock and the Authentication Manager system clock do not match, the generated tokencodes will not match, and authentication attempts can fail.
- Examine your self-service policies and consider hardening self-service access and functionality. For example, you can require users who must reset their PINs to contact the Help Desk.
- For a VMware virtual appliance, you can do the following:
 - Follow VMware standard best practices and the information provided by the VMware Security and Compliance Community on the VMware website. VMware provides VMware *vSphere Security Hardening Guides* for different versions of the vSphere.
 - Use VMware open-source tools to verify that your deployment meets the standards described in the applicable *vSphere Security Hardening Guide* for your version of vSphere.
 - Use VMware Configuration Manager (VCM) to generate and send reports to RSA Archer Governance, Risk, and Compliance (GRC). RSA Archer can analyze your configuration and provide information on how to comply with best practices.
- For a Hyper-V virtual appliance, follow the Hyper-V hardening, virtual machine management recommendations, and standard best practices provided by the Microsoft Solution Accelerator *Hyper-V Security Guide*, the Microsoft *Security Guide for Hyper-V in Windows Server 2012*, and *Configuring Security in System Center 2012 - Virtual Machine Manager*. Microsoft provides these documents on the Microsoft Technet website.

Firewalls

RSA strongly recommends that you use firewalls designed to remove unnecessary network access to RSA Authentication Manager, and follow network security best practices. RSA recommends that you deploy the instance in a subnet that also has an external hardware firewall to segregate it from the rest of the network.

The Authentication Manager instance has an internal firewall that limits traffic to specific ports. The internal firewall restricts inbound traffic to the hosts and services that provide product functionality. Outbound traffic is not restricted.

For information about port usage, see the chapter “Planning RSA Authentication Manager Network Integration” in the *Planning Guide*. Allow only inbound and outbound traffic on the documented ports to reach Authentication Manager.

Protecting Sensitive Files

The Authentication Manager Quick Setup generates keys and passwords used to access internal services such as the internal database. These credentials are stored in a secure vault in Authentication Manager, protected both by a system-specific key for unattended startup as well as the Operations Console administrator credentials for interactive operations. The Operations Console administrator credentials are created during Quick Setup.

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

When you plan a failover and disaster recovery strategy, you can export the system keys and passwords to an encrypted, password-protected file as part of a backup of all of the system passwords. When recovering from a disaster, you can import the file back into the deployment. RSA strongly recommends storing the exported file in a safe and secure manner.

Consider keeping an encrypted copy of the following data offline in a secure physical location, such as a locked safe, in accordance with your disaster recovery and business continuity policies:

- Authentication Manager license files
- Backup data
- Authentication Manager passwords
- Archived log files and report data

To help protect online data, such as current log files and configuration files, RSA strongly recommends that you restrict access to the files and configure file permissions so that only trusted administrators are allowed to access them.

External Identity Sources

External identity sources hold sensitive data that Authentication Manager frequently accesses. RSA strongly recommends that you take the following steps designed to increase the security of this flow of information:

- Use SSL/TLS to communicate with all external identity sources, for example, LDAP or Active Directory.
- Change the password for the service accounts that connect to Active Directory and LDAP regularly.

Agents

Agent hosts are often more exposed to external threats than Authentication Manager. RSA strongly recommends that you observe the following precautions designed to help protect agent hosts:

- Update the operating system and hosted applications that are protected by agents with the latest security patches.
- Limit physical access to the devices that host agents.
- Limit remote access to privileged accounts on devices that host agents.
- Do not configure agents as open to all users. RSA strongly recommends restricting access to agents to specific users and groups.
- Ensure that the location where agents are installed is protected by strong access control lists (ACL).
- Run anti-virus and anti-malware software.
- Run host-based intrusion detection systems.
- If logging is enabled, write logs to a secure location.
- Do not modify the permissions and ownerships for any agent file. Do not allow unauthorized users to access the agent files.
- When you integrate an agent into a custom application, make sure you follow industry standard best practices to develop a secure custom application.

For more information, see the *RSA Authentication Agents Security Best Practices Guide* at <https://community.rsa.com/docs/DOC-42644>.

Suggested Security Practices for a VMware Virtual Environment

If you are using VMware virtual appliances, RSA recommends that you follow the standard VMware best practices for securely deploying and administering the virtual environment:

- Review the VMware security guidelines and documentation that is available in the VMware Security and Compliance Community on the VMware website.
- Follow the applicable *VMware vSphere Security Hardening Guide* for your version of vSphere to protect access to items such as the following:
 - Datastores. For example, limit access to virtual drives and virtual machine snapshot storage.
 - Network switches. For example, verify that switches are not in promiscuous mode.
 - Management consoles and interfaces.
 - Administrative user names and passwords.

- Use the VMware tools for hardening analysis to verify that the virtual environment complies with the standards of the applicable *VMware vSphere Security Hardening Guide* for your version of vSphere. These tools are available on the VMware website.
- You can create separate application and management networks, as described in the VMware security and best practices documentation. Administrators use the higher security management network to manage the virtual appliances. RSA Authentication Manager and agent hosts use the application network.
- If VMware vCenter is deployed, use vCenter to manage access. For more information, see your VMware documentation.
- Implement strong role-based access control. For example, you can create virtual infrastructure (VI) administrators and security administrators. VI administrators manage the entire virtual infrastructure. Security administrators are responsible for Authentication Manager administrative and security tasks.

During Authentication Manager deployment, a VI administrator deploys the virtual appliance and provides the Quick Setup URL to a security administrator. The security administrator runs Quick Setup, which allows the security administrator to create a Super Admin, an Operations Console administrator, and the operating system password.
- For enhanced security, especially in an enterprise environment, you can create a shared administrative role. The VI administrator and the security administrator each know half of the shared password.

You should continue to use role-based controls across the entire infrastructure, but major changes must be performed by the shared administrative role. For example, you might require the shared account to delete a virtual machine, change memory settings, or change the network settings for a switch that is part of the virtual infrastructure.

The shared role requires the VI and security administrators to discuss and agree on important decisions. These discussions help to prevent the configuration problems that are a major issue in virtual environments.

Suggested Security Practices for a Hyper-V Virtual Environment

If you are using Hyper-V virtual appliances, RSA recommends that you follow the standard Hyper-V best practices for securely deploying and administering the virtual environment:

- Review the Hyper-V security guidelines and documentation that is available on the Microsoft Technet website. This material includes:
 - The Microsoft Solution Accelerator *Hyper-V Security Guide*
 - The Microsoft *Security Guide for Hyper-V in Windows Server 2012*, including Chapter 5, “Best Practices Checklist”
 - *Configuring Security in System Center 2012 - Virtual Machine Manager*

- Follow the Microsoft security recommendations to protect access to items such as the following:
 - Datastores. For example, limit access to virtual drives, virtual machine libraries, and any location where you store Hyper-V checkpoints.
 - Network switches. For example, verify that switches are not in promiscuous mode.
 - Management consoles and interfaces.
 - Administrative user names and passwords.
- You can create separate application and management networks on different virtual local area networks (VLANs). Administrators use the higher security management network to manage the virtual appliances. RSA Authentication Manager and agent hosts use the application network.
- If the Hyper-V System Center Virtual Machine Manager (VMM) is deployed, use the VMM Console to manage access. For more information, see *Configuring Security in System Center 2012 - Virtual Machine Manager* on the Microsoft Technet website.
- Implement strong role-based access control. For example, you can create virtual infrastructure (VI) administrators and security administrators. VI administrators manage the entire virtual infrastructure. Security administrators are responsible for Authentication Manager administrative and security tasks.

During Authentication Manager deployment, a VI administrator deploys the virtual appliance and provides the Quick Setup URL to a security administrator. The security administrator runs Quick Setup, which allows the security administrator to create a Super Admin, an Operations Console administrator, and the operating system password.

System Hardening

RSA Authentication Manager was developed using industry-standard best practices for security and the EMC Product Security Policy and Security Development Lifecycle. The lifecycle is a repeatable and measurable process that enables RSA to optimally apply security controls during the product development lifecycle.

The RSA Authentication Manager appliance is intended to be a closed system for a single purpose: running the RSA Authentication Manager services. While there are other tools and services available in the operating system, the appliance is not a general-purpose system, and administrators should not attempt to use or configure additional features. Such unsupported changes may reduce the security of the appliance, creating security vulnerabilities in your installation.

When working with the appliance, administrators must be aware of the security implications, including but not limited to the following:

- System access is limited by design. Adding additional operating system users or modifying user privileges or group membership could allow unauthorized access.
- Files and applications should be protected. File permissions should not be modified. Be aware of any copies of protected files that are created, protect transferred files with strong passwords, and remove any temporary files.
- The appliance includes only the operating system components required to support RSA Authentication Manager. Due to the nature of operating system component packages and dependencies, some unused modules are included on the system. These features should not be used or enabled.
- Files and applications should not be transferred to the appliance. Various vulnerabilities could be introduced with untrusted data and applications.
- The appliance should not be connected to any file servers or networks that are not completely secure.

The appliance security assumes that the system is deployed as described in this guide, in a secure network and physical environment accessible only by trusted administrators. Most of the normal management of the appliance is expected to be performed from the Operations Console. Only a limited amount of work will require access to the operating system for infrequent maintenance tasks, such as when running documented command line utilities or when working with RSA Customer Support.

BIOS Hardening

As part of hardening the appliance image, RSA preconfigures the hardware appliance with a password. The default BIOS password is rsabios.

To protect access to the BIOS, RSA recommends that you change the preconfigured BIOS password to a strong password of your choice. Refer to your hardware owner's manual for information on changing and maintaining the system password.

Be sure to remember and secure the new BIOS password. Entrust knowledge of the BIOS password only to a limited number of personnel who require the password to access the hardware appliance BIOS.

Command Line Privileges

The following commands are used to diagnose issues or maintain the appliance. For auditing and authorization purposes, you must use a specific administrator account to execute these commands.

The following table describes the commands and the user account which is allowed to run each command.

Command	Allowed User	Description
Operating system commands (for example: scp, sftp)	The rsaadmin operating system account.	For a description of an operating system command, run the command with the help option. For example: scp --help.
RSA Authentication Manager command line utilities (CLUs)	The rsaadmin operating system account and Authentication Manager account assigned the administrative role	Utility that you access from the command line.

Note: The CLU prompts you to enter the required credentials, for example, an Operations Console Administrator or a Super Admin user name and password.

NFS Server and Windows Share Security

You can use a Network File System (NFS) or Windows share for:

Backup and restore operations. By default, when you create a backup, the appliance encrypts the data and saves the backup file to the local hard disk. However, you can configure the appliance to save backup files to an NFS or Windows share, and then restore a backup from the same location, if necessary.

Storing and applying appliance updates. You can copy appliance updates to an NFS or Windows share and then apply the updates to the appliance.

RSA Authentication Manager backup files are encrypted, but Authentication Manager update files are not encrypted. RSA recommends that you protect your NFS or Windows share and the network path. If you use an NFS or Windows share, do the following:

- Secure the NFS or Windows share directories to protect data and prevent file tampering and disclosure. For example, for a Windows share, configure a username and password.
- Secure the network path between the NFS or Windows share and the appliance. The update files are not encrypted when traversing the network.

RSA Authentication Manager Services That Start Automatically

RSA Authentication Manager does not install services that are not used. Authentication Manager only runs necessary services. The following table lists the Authentication Manager services that start automatically.

Service Name	Description	Details
console	RSA Console Server	Hosts the Security Console and the Self-Service Console
biztier	RSA Runtime Server	
admin	RSA Administration Server with Operations Console	Hosts the Operations Console
db	RSA Database Server	
primary_replication	RSA Replication (Primary)	Runs on the primary instance only.
replica_replication	RSA Replication (Replica)	Runs on the replica instance only.
radius	RSA RADIUS Server	
radiusoc	RSA RADIUS Server Operations Console	

You can manage Authentication Manager services manually. You can perform the following actions on a selected service or on all services at the same time:

- Stop
- Start
- Display current status
- Restart

For security purposes, the appliance does not start the Secure Shell (SSH) service automatically. Before you can log on to the appliance operating system using an SSH client, you must enable SSH in the Operations Console.

For information on how to enable SSH and how to manually manage Authentication Manager services, see the chapter “Advanced Administration” in the *Administrator’s Guide*.

3

Secure Maintenance

RSA Authentication Manager Updates

RSA issues product updates periodically for RSA Authentication Manager in the form of patches and service packs. RSA recommends applying product updates as they become available to ensure that the deployment is secure and efficient. For each product update, RSA provides release notes that contain important information about applying the update. To avoid problems, you should read all of the information in the release notes before you apply the update.

You download product updates from RSA Link at <https://community.rsa.com/community/products/securoid>. Updates are provided in the form of an ISO image. RSA recommends that you do not burn the ISO image to a physical DVD or CD. Instead, save the ISO image in a directory that is accessible to the deployment.

You use the Operations Console to apply product updates on each primary and replica instance. After you download a product update, you specify the location of the ISO image. You can apply an individual update through your local browser, or you can scan for stored updates in an NFS share, a Windows shared folder, or a DVD/CD. After scanning, you can select an individual update to apply.

Note: Apply updates to embedded third-party products only as part of RSA-delivered updates. For example, RSA provides the required updates to the virtual appliance and hardware appliance operating system.

If the deployment includes a web tier, you must update the web tier when you update the version of Authentication Manager. Authentication Manager displays an update button in the Operations Console for each web tier that is not up-to-date.

Operating System Access

Although you use the Operations Console and the Security Console to administer RSA Authentication Manager, there may be times when you need to access the appliance operating system to perform the following advanced administration tasks:

- Stop and start Authentication Manager services.
- Troubleshoot complex appliance problems that cannot be resolved through the Operations Console.
- Run Authentication Manager command line utilities (CLUs).

You can access the appliance operating system with a Secure Shell (SSH) client, a software application that uses SSH to connect with a remote computer. The client is installed on a local computer that has a network connection to the appliance. Before you can access the appliance operating system through an SSH client, you must enable SSH on the appliance.

You can also access the operating system on a virtual appliance with the VMware vSphere Client, the Hyper-V System Center Virtual Machine Manager (VMM) Console, or the Hyper-V Manager.

You can define session lifetime settings for logging on to the appliance operating system. Session lifetime is an important security feature because it prevents administrators from keeping sessions open indefinitely, leaving them vulnerable to unauthorized access. The session lifetime settings apply when you access a virtual appliance or hardware appliance operating system with an SSH client or when you access a virtual appliance operating system with the VMware vSphere Client, the Hyper-V VMM Console, or the Hyper-V Manager. For instructions, see the Operations Console Help topic “Edit Session Lifetime Settings for Operating System Access.”

An operating system account password is required to access the operating system directly or through SSH.

Run Clam Antivirus Software

Each RSA Authentication Manager instance includes Clam Antivirus (ClamAV) software. ClamAV is an open-source software toolkit that is intended to reduce the risk of intrusion or malicious system or data access. Apply software updates to ClamAV only as part of RSA-delivered updates. You are responsible for updating antivirus definition files and running ClamAV in order to scan any Authentication Manager instance for known malware.

Before You Begin

- This procedure assumes a knowledge of Linux commands.
- For the operating system account User ID **rsaadmin**, obtain the operating system password.
- To access the operating system with a secure shell (SSH) client, you must enable SSH. You can also access the operating system on a virtual appliance in the VMware vSphere client, the Hyper-V System Center Virtual Machine Manager Console, or the Hyper-V Manager.

Procedure

1. Log on to the appliance with the User ID **rsaadmin** and the current operating system password:
 - On a hardware appliance, log on to the appliance using an SSH client.
 - On a virtual appliance, log on to the appliance using an SSH client, the VMware vSphere client, the Hyper-V System Center Virtual Machine Manager Console, or the Hyper-V Manager.
2. Update the antivirus definition files. Choose one of the following procedures:
 - If the Authentication Manager instance has access to the Internet, you can automatically download and apply the latest antivirus definition files. Type the following command:

```
sudo /usr/bin/freshclam
```
 - If the Authentication Manager instance does not have access to the Internet, manually download the **main.cvd** and **daily.cvd** antivirus definition files from the ClamAV web site: <http://www.clamav.net/>. Copy the files into the **/var/lib/clamav/** directory on the instance.
3. To scan files and directories for viruses manually, type the following line:

```
sudo clamscan -r / --exclude-dir=/proc --exclude-dir=/sys  
--exclude-dir=/opt/rsa/am/rsapgdata  
--follow-dir-symlinks=0 --follow-file-symlinks=0  
--log=/var/log/clamav.log
```

To schedule automatic virus scans, create a **cron** job that runs the same command.
4. Check the scan results in **/var/log/clamav.log**.

Protecting Backups

You can use the Operations Console to create a backup of the deployment data using one of the following methods:

- **Back Up Now.** A manual, one-time backup of the deployment.
- **Schedule Backups.** Regular backups of the deployment according to a schedule that you specify.

RSA recommends that you maintain a current backup. If a successful backup has not been created during the past seven days and Critical System Notifications are configured, the deployment sends a notification.

The deployment encrypts backups because backups contain sensitive information. During the backup process, you must specify a password that is used for encryption. During the restore process, you provide this password so that the backup can be decrypted and checked for integrity. Be sure to record the password in a safe location, as dictated by your organization's policies, so that it will be available when you need to restore the deployment.

You can save your backup on the appliance or at a remote location. RSA recommends saving a current backup in a remote location so that you can restore your deployment to recover from a disaster. RSA recommends periodically testing your backups on a spare, non-production system, to ensure that you will be able to restore if a disaster occurs.

For instructions, see the Operations Console Help topics “Create a Backup using Backup Now” and “Create a Backup Using Schedule Backups.”

4

Physical Security Controls

Protecting the Authentication Manager Environment

It is very important to protect all physical, local and remote access to the Authentication Manager environment, including the Authentication Manager server and agent hosts. It is important to restrict all access methods to the bare minimum required to maintain Authentication Manager.

Note: RSA strongly recommends that your Authentication Manager test environments not be exact copies of your full production environment. If they are, you should take the same precautions to protect the test environment as you do your production environment.

Physical Security Controls

Physical security controls protect resources against unauthorized physical access and physical tampering. Authentication Manager is designed to be a critical infrastructure component so it is important that physical access be restricted to authorized personnel only. Restricting physical access is an important security measure, even in a virtual environment with shared resources. After installation, authorized users only need limited access to Authentication Manager, and either the hardware appliance or the physical machine hosting the virtual appliance.

RSA recommends using the following physical security controls:

- Place the hardware appliance or the physical machine hosting the virtual appliance in a locked cabinet. As with any other hardware device in your network, allow only authorized users to physically access the hardware appliance or the host system.
- In a virtual environment, protect the physical machine hosting the virtual appliance. Protect the hosts where virtual disks, virtual memory, and any VMware snapshots or Hyper-V checkpoints are stored.
- Place physical locks on all external interfaces.
- Place tamper evident stickers on each server chassis and other hardware.
- Employ strong access control and intrusion detection mechanisms where the product cabling, switches, servers, and storage hardware reside.
- If you use a DVD/CD or USB flash drive to apply updates to the primary or replica instance, you must securely manage the removable media. You want to prevent unauthorized personnel from copying files onto the media that might harm the instance at the next use.

- Secure the server room such that it's only accessible by authorized personnel and audit that access. For example, use room locks that allow traceability and auditing.
- Minimize the number of people who have physical access to devices hosting Authentication Manager server, agents, and instances of the software development kit (SDK).
- After Quick Setup is complete, allow only authorized users to have direct physical access to the hardware appliance. A user with the rsaadmin operating system account password can log on to the appliance by attaching a keyboard and a monitor or by accessing a remote management module port.

Remote Access to Server Environments

RSA recommends limiting remote access as follows:

- Remote access to server system components should be limited. For example, restrict access to the operating system on a virtual appliance through the OS Console in the VMware vSphere Client, the Hyper-V System Center Virtual Machine Manager Console, or the Hyper-V Manager.
- RSA Authentication Manager supports Secure Shell (SSH) as a remote management capability. By default, SSH is disabled. Only enable SSH when it is absolutely required for maintenance. Disable SSH immediately when maintenance is complete.

For instructions on using SSH, see the Operations Console Help topic “Enable Secure Shell on the Appliance.”

- Remote access to any host or system connected to or managed by Authentication Manager, such as hosts with agents installed, should be limited as indicated above. In addition, disable remote access methods for the operating system, for example telnet or ftp, that communicate over unsecured channels.

5

Supporting End Users

Procedures and Training

It is important to have well-defined policies around help desk procedures for RSA Authentication Manager. Help Desk administrators must understand the importance of PIN strength and the sensitivity of data such as the user's login name and token serial number. Creating an environment where an end user is frequently asked for this kind of sensitive data increases the opportunity for social engineering attacks. Train end users to provide, and Help Desk administrators to request, the least amount of information needed in each situation.

For information on the most common tasks that a Help Desk Administrator needs to manage Authentication Manager, see the *Help Desk Administrator's Guide*.

Preventing Social Engineering Attacks

Fraudsters frequently use social engineering attacks to trick unsuspecting employees or individuals into divulging sensitive data that can be used to gain access to protected systems. Use the following guidelines to reduce the likelihood of a successful social engineering attack:

- Help Desk administrators should only ask for a user's User ID over the phone when he or she calls the help desk. Help Desk administrators should never ask for token serial numbers, tokencodes, PINs, passwords, and so on.

Note: When resynchronizing tokens, users should enter tokencodes in the administrative interface under the supervision of the logged-on administrator. If the user cannot enter tokencodes in this way, make sure that the user adheres to the other recommendations in this section and that administrators adhere to the recommendations in [Confirming a User's Identity](#) on page 42 when it is necessary to resynchronize a token.

- The Help Desk telephone number should be well-known to all users.
- Help Desk administrators should authenticate the user's identity before performing any administrative action on a user's token or PIN. For example, ask the user one or more questions to which only he or she knows the answer. For more information, see [Confirming a User's Identity](#) on page 42.

- If Help Desk administrators need to initiate contact with a user, they should not request any user information. Instead, users should be instructed to call back the Help Desk at a well-known Help Desk telephone number to ensure that the original request is legitimate.
- To confirm that all PIN changes are requested by authorized users, you should have a policy in place to notify users when their PINs have been changed. For example, send an e-mail notification to the user's corporate e-mail address, or leave a voicemail message. Users that suspect a change was made by an unauthorized person should contact the Help Desk.

Confirming a User's Identity

It is critical that Help Desk Administrators verify the end user's identity before performing any Help Desk operations on the user's behalf. Recommended actions include:

- Call the end user back on a phone owned by the organization and on a number that is already stored in the system.

Important: Be wary of using mobile phones for identity confirmation, even if they are owned by the company, as mobile phone numbers are often stored in locations that are vulnerable to tampering or social engineering.

- 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.
- Verify the identity in person.
- 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.

PIN Management

RSA strongly recommends the following to help protect RSA SecurID PINs:

- For software tokens:
 - When software tokens are issued as PINPad-style tokens (the Authentication Type is set to PINPad-style in the software token profile), the software token PIN should be equal in length to the tokencode, and all numeric.
 - When software tokens are issued as fob-style tokens (the Authentication Type is set to Fob-style in the software token profile), the software token PIN should be alphanumeric and eight digits in length. To require alphanumeric PINs, an administrator must configure the token policy in the Security Console.

- Your corporate token policy should require the use of 6-character to 8-character PINs. Do not use 4-character numeric PINs. RSA recommends that your PINs require alphanumeric characters (a-z, A-Z, 0-9) when the token type supports them. You must configure Authentication Manager to allow these characters.
- Configure Authentication Manager to lock out a user after three failed authentication attempts. Require manual intervention to unlock users who repeatedly fail authentication.
For information about configuring the number of failed attempts, see the Security Console Help topic “Add a Lockout Policy.”
- To roll out a new Authentication Manager token policy for PINs, set the maximum PIN lifetime to a period that is short enough so that all users will be forced into New PIN mode but long enough where users will not be forced to change their PIN multiple times. If your user population is segmented by security domains, it is recommended that you stagger the policy change by security domain to avoid overwhelming your Help Desk.
Be sure to notify the affected users in advance that they should authenticate and change their PIN as soon as possible. To verify all users have changed their PINs, run a report detailing user authentication activity for that period of time.
After the Authentication Manager token policy rollout is complete and you have verified that all users have changed their PINs in accordance with the new policy, the Authentication Manager token policy for PIN lifetimes should be restored to adhere to your corporate security policy. If you have changed your Authentication Manager token policy settings and users are not being prompted for a new PIN, please contact RSA Customer Support for information on how to force the new PIN mode.

Note: It is important to strike the right balance between security best practices and user convenience. If system-generated alphanumeric 8-digit PINs are too complex, find the strongest token policy for PINs that best suits your user community.

For information about changing to stronger PINs, see the Security Console Help topic “Edit a Token Policy.”

- You should notify users before you update the policy. If you have a large number of users who do not meet the new policy, you may experience an increase in Help Desk calls.
- You can increase the complexity of user PINs by requiring system-generated PINs. However, you may be reducing security as people may write down complex PINs, or call the Help Desk more frequently to have their PINs cleared.
Increased phone calls to the Help Desk to clear PINs increases the possibility of a social engineering attack from unauthorized individuals posing as users. For more information, see [Confirming a User’s Identity](#) on page 42.
- Instruct all users to never tell anyone their PINs. Administrators should never ask for or know the user’s PIN.
- Configure policies that restrict the re-use of PINs.
- Configure the use of the dictionary to prevent the use of simple PINs.

- Configure Authentication Manager to require users to change their PINs at regular intervals. These intervals should be no more than 60 days. If you use 4-digit numeric PINs, the intervals should be no more than every 30 days. For software tokens, the PIN should be equal in length to the tokencode, and all numeric. For information about requiring periodic PIN changes for users, see the Security Console Help topic “Edit a Token Policy.”

Note that more frequent PIN changes may also result in an increase in Help Desk calls.

- RSA strongly recommends that you do not use system-generated PINs in conjunction with the RADIUS PAP protocol.
- You can gradually phase in a requirement for users to change their PINs. Changing a token policy assigned to a security domain changes the policy for all users in the domain. It is not possible to change a policy for a subset of users in a security domain. However, it is possible to effectively change a policy on a subset of users by moving those users to a new security domain with the changed policy. For instructions, see the Security Console Help topics “Edit a Token Policy” and “Move Users Between Security Domains.”

If a token policy is assigned to more than one security domain and you want to change the policy for only one of the security domains, duplicate the existing policy. You can make the necessary changes to the duplicate policy and assign the policy to the security domain you want to change. For instructions, see the Security Console Help topics “Duplicate a Token Policy” and “Assign a Token Policy to a Security Domain.”

Advice for Users

Note: Consider regular training to communicate this guidance to users.

RSA strongly recommends that you instruct users to do the following:

- Never give the token serial number, PIN, tokencode, token, passcode or passwords to anyone.
- To help avoid phishing attacks, do not enter tokencodes into links that you clicked in e-mail. Instead, type in the URL of the reputable site to which you want to authenticate.
- Inform users of what information requests to expect from Help Desk administrators.
- Always log out of applications when you’re done with them.
- Always lock your desktop when you step away.
- Regularly close your browser and clear your cache of data.
- Immediately report lost or stolen tokens.

Emergency Access and Static Tokencodes

Use the Security Console to generate emergency access tokencodes. For instructions, see the chapter “Administering Users” in the *Administrator’s Guide*.

RSA strongly recommends that you do the following:

- Confirm the user’s identity before assigning the user an emergency access tokencode. For example, ask the user a question to which only he or she knows the answer.
- Discontinue the use of static passwords.
- Ensure that emergency access tokencodes expire within a short period of time. RSA strongly recommends that emergency access tokencodes expire within a day. Emergency access tokencodes are not a permanent solution to lost tokens.
- Use on-demand tokencodes for emergency access when possible.
- Verify that the user’s phone number has not changed.

Glossary

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 email address or the mobile phone number where the on-demand token codes 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 email 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).

email 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, email notifications also contain information about how to download and activate tokens. Request Approvers and Token Distributors receive email notifications about requests that require their action. See email templates.

email templates

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

TCP

See Transmission Control Protocol.

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.

Transmission Control Protocol (TCP)

A protocol that allows programs on networked computers and major Internet applications to communicate with one another by sending reliable, ordered, and error-checked units of information.

trusted realm

A trusted realm is a realm that has a trust relationship with another realm. RSA Authentication Manager can add an RSA Via Access deployment as a trusted realm and send RSA Via TokenCodes directly to RSA Via Access. An RSA Authentication Manager deployment can also trust another RSA Authentication Manager deployment. Users on an Authentication Manager trusted realm have permission to authenticate to another Authentication Manager realm and access the resources on that realm. Two or more Authentication Manager realms can have a trust relationship that can be either one-way or two-way.

trust package

An XML file that contains configuration information about the deployment.

UDP

See User Datagram Protocol.

User Datagram Protocol (UDP)

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

User ID

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

virtual host

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

virtual hostname

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

web tier

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

workflow

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

workflow participant

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

Index

A

- access control, 9, 10
- Administrative Audit log
 - definition, 20
- administrators
 - diagnose product issues, 32
 - required to execute commands, 32
 - system administrator accounts, 10
 - virtual environment, 30, 31
- agent hosts, 29
- antivirus software
 - using, 37
- appliance
 - logs, 21
- applying updates, 33
- audit logs
 - Security Console, 20
- audit trail
 - types of logs, 20
- audit trails
 - monitoring, 16
- auditing
 - Authentication Manager, 19, 20, 21
- authentication, 9
- authentication failure
 - system time changed, 27

B

- backups
 - protecting, 33, 38

C

- certificates
 - SSL, 22
 - web tier, 22
- Clam Antivirus
 - using, 37
- CLUs. *See* command line utilities.
- command line privileges, 32
- command line utilities, 33, 36
- communication
 - secure, 22
- component access control, 10
- confirming user identity, 42
- CT-KIP. *See* dynamic seed provisioning
- custom reports, 22

D

- deleted Super Admin, 12
- delivering
 - on-demand tokencodes, 18
- demilitarized zone
 - deploying servers, 26
- deployment
 - product updates, 35
 - using a subnet, 27
 - using antivirus software, 37
- diagnose issues, 32
- disaster recovery
 - planning, 28
- distributing
 - hardware tokens, 17
 - software tokens, 17
 - tokens, 15
- DMZ. *See* demilitarized zone.
- dynamic seed provisioning, 17

E

- emergency access tokencodes, 45
- encryption
 - backups, 38
 - data, 23
 - files, 28
 - Simple Mail Transfer Protocol, 22

F

- failover strategy
 - planning, 28

H

- hardware tokens
 - distribution, 17
 - lost, 18
 - token policy, 43
- help desk procedures, 41
 - Tokencode tokens, 15

I

- identity sources
 - external, 28
- importing
 - tokens, 15

K

keystores, 28

L

license

 ID, 7

 serial number, 7

locked out Super Admin, 12

log messages

 token serial number masking, 16

log types, 20

logging

 Authentication Manager, 19, 20, 21

M

maintenance, 35

masking

 token serial numbers, 16

monitor system

 types of logs, 20

monitoring

 Authentication Manager, 19, 20, 21

N

network file system, 33

network infrastructure hardening, 26

Network Time Protocol (NTP) server, 27

NTP server. *See* Network Time Protocol server.

O

on-demand authentication tokencodes

 delivery, 18

operating system

 access, 36

 account, 11

 commands, 33

 logs, 21

Operations Console

 administrator permissions, 11

 protect credentials, 28

P

passwords

 lost, 11–12

 strong, 13

PINless tokens. *See* Tokencode tokens.

PINs

 protecting, 42

policies, 19

 passwords, 13

ports

 usage, 19

product updates, 35

protecting

 tokens, 15

R

RADIUS PAP protocol, 44

real-time log monitoring, 21

reports

 custom, 22

restore

 from a backup, 33

restore Super Admin, 12

resynchronizing tokens, 41

roles, 19

Runtime Audit log

 definition, 20

S

SDK. *See* Software Development Kit

secure

 communication, 22

Secure Shell

 for accessing the appliance, 11, 34, 36

 session lifetime settings, 36

 to access the appliance, 37

secure sockets certificates, 22

security, 28

security administrators, 30, 31

Security Console

 access, 9

 audit logs, 20

services

 manage manually, 34, 36

 Secure Shell, 34, 36

 start automatically, 34

session lifetime settings

 Secure Shell, 36

Simple Mail Transfer Protocol

 encryption, 22

SMTP. *See* Simple Mail Transfer Protocol

social engineering

 preventing, 41

Software Development Kit, 19

software tokens

 distribution, 17

 PINs, 42

 token policy, 43

- SSH. *See* Secure Shell.
- storing updates, 33
- subnet
 - deploying appliance, 27
- Super Admin, 9
 - permissions, 10
 - restoration, 12
- system administrator accounts, 10
- system hardening, 26
 - Hyper-V best practices, 27
 - software development lifecycle (SDL), 31
 - tools, 30
 - VMware best practices, 27, 29, 30
- System log
 - definition, 20

T

- token files
 - protection, 16
- token serial numbers
 - masking in log messages, 16
- Tokencode tokens, 15
- tokens, 15
 - distributing, 15, 17
 - distribution, 17
 - emergency access, 45
 - lost, 18
 - PINs, 43
 - static tokencodes, 45
 - token policy, 43
 - Tokencode tokens, 15

- Trace log
 - definition, 20
- training
 - help desk administrators, 41
 - users, 41, 44

U

- User IDs
 - valid characters, 11
- users
 - confirming identity, 42

V

- valid characters
 - for User IDs, 11
- version
 - viewing, 7
- virtual appliance
 - logs, 21
- virtual environment, 29, 30
- virtual infrastructure (VI)
 - administrators, 30, 31

W

- web tier
 - certificates, 22
 - definition, 26
- Windows share, 33