RSA SecurID Appliance 3.0
System Hardening Guide

Revision 1

The Security Division of EMC

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers**:** **www.rsa.com**

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.rsa.com/legal/trademarks_list.pdf**.

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 in the **thirdpartylicenses.pdf** file.

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.

January 2011
Revised: July 2011

Revision History

Revision Number	Date	Revision
1	July 2011	• Updated the names of user interface elements in the procedure in the Enable SSH section of Chapter 1. • Added the Using ClamAVAntivirus Software with the RSA SecurID Appliance section to Chapter 2.

Contents

Revision History 3

Preface 7

About This Guide 7

RSA SecurID Appliance Documentation 7

Related Documentation 8

RSA Authentication Manager Documentation 8

RSA RADIUS Documentation 8

Getting Support and Service 9

Before You Call Customer Support 9

Chapter 1: Appliance Components Hardened by RSA 11

Overview 11

System Module Versions 11

RSA Authentication Manager Services 12

RSA Authentication Manager Services Started by Default 12

RSA Authentication Manager Services Not Started by Default 13

Ports and Firewall Settings 14

Overview of Port Traffic 14

Port Usage on the Appliance 15

User Accounts and Passwords 16

Linux Service Account 16

Linux Root Account 16

Linux User Account 17

Runtime Command Privileges 17

Chapter 2: Post-Deployment Hardening Recommendations 19

Change the Default SNMP Community String 19

Password Protection 20

Administrative Role Assignment 20

Network File System Server Security 21

Appliance System Event Audits 22

RSA Authentication Manager Logs 22

Appliance-Only Logs 23

Removable Media Used on the Appliance 23

Appliance Access Restriction 23

Using ClamAV Antivirus Software with the RSA SecurID Appliance 24

Install ClamAV 0.97 on the SecurID Appliance 24

Configure ClamAV 0.97 on the SecurID Appliance 24

Scan the SecurID Appliance with ClamAV 0.97 25

Index 27

Preface

About This Guide

This guide describes how RSA hardens (increases the security of) RSA SecurID Appliance 3.0 before shipping it. It also describes additional steps that you can take after deployment to further secure the Appliance.

This guide is intended for administrators and other trusted personnel. Do not make this guide available to the general user population.

Note: For the most up-to-date recommendations on security best practices, see the *RSA Authentication Manager 7.1Security Best Practices Guide* and the *RSA SecurID Software Token Security Best Practices Guide*.

RSA SecurID Appliance Documentation

For more information about RSA SecurID Appliance, see the following documentation. You can access this documentation on RSA SecurCare Online at **https://knowledge.rsasecurity.com** and on the RSA SecurID Appliance 3.0 Documentation CD.

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

Getting Started. Provides information to help you with the RSA SecurID Appliance Quick Setup process.

Owner's Guide. Provides information on planning, implementing, and administering the RSA SecurID Appliance.

Migration Guide. Provides information on planning and implementing a migration to RSA SecurID Appliance 3.0. You can migrate from RSA SecurID Appliance 2.0 or later and from RSA Authentication Manager 6.1 or later. You cannot migrate from RSA Authentication Manager 7.0 or 7.1.

SNMP Reference Guide. Provides information about the available SNMP traps and gets for the RSA SecurID Appliance hardware.

Rack and Bezel Installation Guide. Describes how to install the Appliance in a rack and how to attach the bezel. This guide is available on the RSA Appliance Rack and Bezel Installation Guide CD that ships in the Appliance package.

RSA Operations Console Help. Describes RSA SecurID Appliance and Authentication Manager configuration and setup tasks performed in the RSA Operations Console.

Related Documentation

For more information about RSA Authentication Manager, RSA RADIUS, security best practices, see the following documentation. You can access this documentation on RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

RSA Authentication Manager Documentation

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

Getting Started. Lists what the kit includes (all media, diskettes, licenses, and documentation), specifies the location of documentation on the DVD or download kit, and lists RSA Customer Support web sites.

Planning Guide. Provides a general understanding of RSA Authentication Manager, its high-level architecture, its features, and deployment information and suggestions.

Installation and Configuration Guide. Describes detailed procedures on how to install and configure RSA Authentication Manager.

Administrator's Guide. Provides information about how to administer users and security policy in RSA Authentication Manager.

Migration Guide. Provides information for users moving from RSA Authentication Manager 6.1 to RSA Authentication Manager 7.1, including changes to terminology and architecture, planning information, and installation procedures.

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

Performance and Scalability Guide. Provides information to help you tune your deployment for optimal performance.

RSA Security Console Help. Describes day-to-day administration tasks performed in the RSA Security Console. To view Help, click the **Help** tab in the Security Console.

RSA Operations Console Help. Describes configuration and setup tasks performed in the RSA Operations Console. To log on to the Operations Console, see "Logging On to the RSA Operations Console" in the *Administrator's Guide*.

RSA Self-Service Console Frequently Asked Questions. Provides answers to frequently asked questions about the RSA Self-Service Console, RSA SecurID two-factor authentication, and RSA SecurID tokens. To view the FAQ, on the **Help** tab in the Self-Service Console, click **Frequently Asked Questions**.

Note: To access the *Developer's Guide* or the *Performance and Scalability Guide*, go to **https://knowledge.rsasecurity.com**. You must have a service agreement to use this site.

RSA RADIUS Documentation

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

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**www.rsa.com/rsasecured**

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

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

Before You Call Customer Support

Before you call Customer Support, please have the following available:

- ❑ Access to the RSA SecurID Appliance.
- ❑ Your RSA License ID. You can find this number on your license distribution media, or in the RSA Security Console by clicking **Setup** > **Licenses** > **Manage Existing**, and then clicking **View Installed Licenses**.

The RSA SecurID Appliance software information. You can find this information in the RSA Operations Console by clicking **Maintenance** > **Manage Updates** > **Apply Updates**.

1 Appliance Components Hardened by RSA

- Overview
- System Module Versions
- RSA Authentication Manager Services
- Ports and Firewall Settings
- User Accounts and Passwords
- Runtime Command Privileges

Overview

RSA SecurID Appliance 3.0 was developed using industry-standard best practices for security, as outlined in the EMC Security Development Lifecycle (SDL). The lifecycle is a repeatable and measurable process that enables RSA to optimally apply security controls during the product development lifecycle.

Following this process, RSA hardened the Appliance by restricting the components described in the following sections.

System Module Versions

The following table shows the current versions of system modules that are included in RSA SecurID Appliance 3.0. The Appliance contains only those modules that are required for the Appliance operating system or the RSA Authentication Manager software.

System Module	Description	Version
System Kernel version	Linux kernel	2.6.24.7-3
Open SSH version	Open SSH server daemon and client	4.9p-1-1-1
Open SSL version	Open SSL toolkit	0.9.7f-13-1
NFS version	NFS utilities, client and daemon	1.0.7-17-1
NetSNMP version	SNMP protocol tools and libraries	5.2.1.2-7-1

Do not update these modules on your own. If it is necessary to update one of these modules, RSA will create an update and notify you of its availability. For more information, see the chapter “Updating the Appliance” in the *Owner’s Guide*.

RSA Authentication Manager Services

The Appliance disables all Authentication Manager services, unless they are required for product functionality. The following sections list the Authentication Manager services that are started or not started by default:

- "RSA Authentication Manager Services Started by Default"
- "RSA Authentication Manager Services Not Started by Default"

RSA Authentication Manager Services Started by Default

The Appliance starts the services in the following table by default.

Service	Description
manager	RSA Authentication Manager
proxy	RSA Authentication Manager proxy server administration channel
admin	RSA Security Console
dblistener	RSA Authentication Manager database listener
db	RSA Authentication Manager internal database
dbconsole	RSA Authentication Manager database console
all	All of the Appliance services
nodemanager	RSA Authentication Manager node manager
oc	RSA Operations Console
managed	All of the Appliance services with the exception of the RSA RADIUS services (radius and radiusoc)
radius	RSA RADIUS
radiusoc	RSA RADIUS server functionality in the Operations Console

RSA Authentication Manager Services Not Started by Default

For security purposes, the Appliance does not automatically start the following services:

- **SSH**. You need to start SSH to log on to the Appliance operating system to complete certain advanced administrative tasks or to run command line utilities (CLUs).
- **SNMP**. You need to start SNMP if you want to use SNMP to monitor the Appliance.

Enable SSH

You must enable SSH on at least one Network Interface Card (NIC). This can be the primary NIC (used by Authentication Manager), the secondary NIC (used for administration), or both.

To enable SSH on a NIC:

1. In the Operations Console, click **Administration > Networking > Configure Connectivity using SSH**.
2. In the SSH Settings section of the Configure SSH and Operating System Connectivity page, do the following:
   - **SSH**—Select **Enable SSH**.
   - **Bind SSH to Selected NICs**—Select one or more **Available** NICs, and use the arrow buttons to move the NICs to the **Selected** box on the right.
3. Click **Save**.

For more information, see the chapter “Advanced Administration” in the *Owner’s Guide*.

Enable SNMP

To configure Appliance SNMP:

1. In the Operations Console, click **Administration** > **SNMP** > **Configure Appliance SNMP**.
2. Select **Network Management** to enable the Appliance SNMP agent.
3. Click **Save**.

For more information, see the chapter “Appliance Logging and SNMP” in the *Owner’s Guide*.

Ports and Firewall Settings

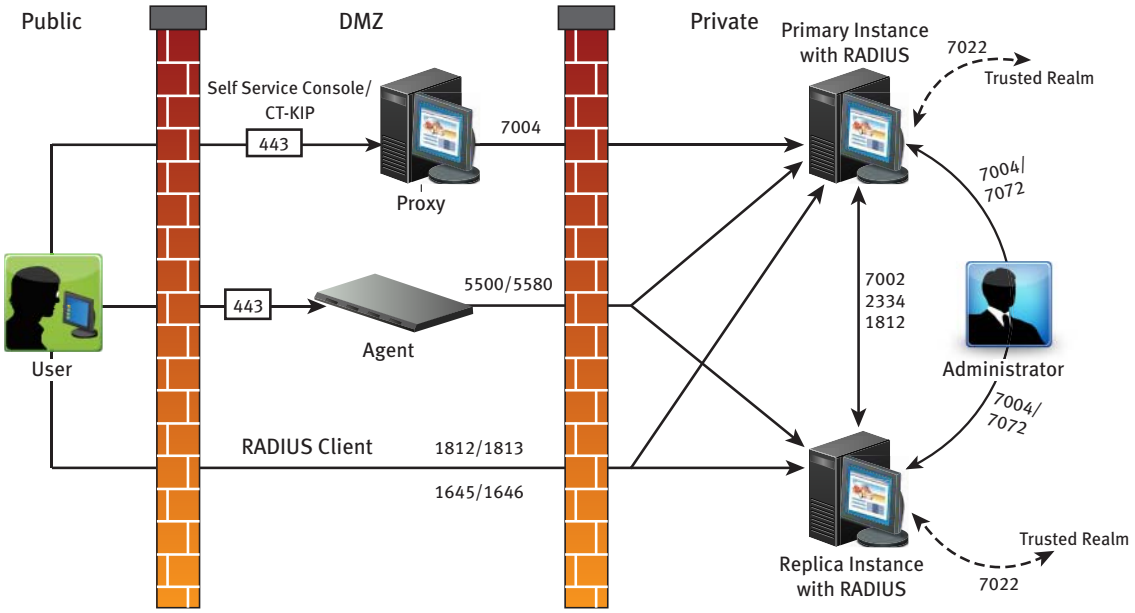
The Appliance preconfigures the iptables firewall to ensure that all unused ports are closed. The following table lists the ports opened in the firewall. The port numbers listed in the following table enable authentication, administration, replication, and other services on the network.

RSA Authentication Manager has a firewall that restricts inbound traffic to the hosts and services that provide product functionality. RSA recommends that you deploy the Appliance in a subnet that also has an external firewall to segregate it from the rest of the network.

Depending on your deployment, you may need to configure network resources, such as firewalls and proxy servers, to allow communication between the Appliance and other network-based hosts and services. This section includes an overview of port traffic with figures that show common network deployments and a list of all ports on the Appliance.

Overview of Port Traffic

The following figure represents an Authentication Manager deployment with primary and replica instances, and local RADIUS. An external firewall protects the primary and replica instances, and another firewall protects the DMZ.



Port Usage on the Appliance

The following table lists additional port considerations specific to Appliance deployments. (Outbound traffic is not restricted.) For an environment with external firewalls or proxy servers, you must ensure that they allow communication between the Appliance and all other hosts and services that provide Authentication Manager functionality. These hosts and services, which are listed in the Source column, include Authentication Manager instances, load balancers, and browsers.

For a complete list of the Authentication Manager ports, see "Port Usage" in the *RSA Authentication Manager 7.1 Planning Guide*.

Ports 80 and 443 (TCP) are open only during Quick Setup. These ports are reopened temporarily only if you perform a factory reset

Port Number and Protocol	Function	Description	Direction
22/TCP	SSH	Used to access the Appliance operating system, if SSH is enabled. The operating system password is required. This port is closed by default.	Inbound
123/UDP	NTP	Used to synchronize the clock of your Authentication Manager installation with a reliable external time server.	Inbound
161/UDP	Appliance SNMP agent	Used by the Appliance SNMP agent to listen for requests and send responses to the NMS. The Appliance SNMP agent is used for Appliance-specific monitoring, such as traps to monitor fan failure and temperature sensors. By default, the Appliance sends traps to port 162 on the machine that receives the traps.	Inbound
199/TCP 199/UDP	Appliance operating system	Internal listening port for the appliance. This port should be blocked on the firewall.	Block
	Appliance operating system	Used as a listening port by the Appliance operating system.	Inbound
1161/UDP	SNMP agent	Used by the Authentication Manager SNMP agent to listen for requests and send responses to the NMS. This allows the NMS to monitor Authentication Manager. This can be configured in the Operations Console.	Inbound

1162/UDP	SNMP agent	Used to send Authentication Manager traps to the NMS using the Simple Network Management Protocol (SNMP). This allows the NMS to monitor Authentication Manager. This can be configured in the Operations Console.	Inbound

User Accounts and Passwords

To control access to the Appliance operating system, the Appliance contains the following user accounts:

- "Linux Service Account"
- "Linux Root Account"
- "Linux User Account"

Note: For more information about Authentication Manager user accounts and passwords, see the chapter "Advanced Administration" in the *Owner's Guide*.

Linux Service Account

You use the Linux service account emcsrv for logging on to the Appliance operating system (through SSH). In the product documentation, this account is also called the operating system account.

During Quick Setup, you specify the password for the emcsrv user account. Thus each physical Appliance has its own password for its emcsrv user account. You can change the emcsrv password in the Operations Console. For more information, see the chapter "Advanced Administration" in the *Owner's Guide*.

The Appliance grants sudo privileges to the emcsrv user account. You use the sudo privilege to change to the root or rsaadmin user accounts to run command line utilities (CLUs) or other configuration files. The emcsrv user account times out after 30 minutes of inactivity.

Linux Root Account

You use the Linux user account root to run certain Authentication Manager commands or to copy files onto the Appliance (if instructed to do so) and then change their locations and permissions.

In RSA SecurID Appliance 3.0, the password for the root user account is locked. This means that you cannot log on as root directly or use the **su** command to become the root user.

To use the root user account, you first must log on with the emcsrv account and then use sudo to change to the root account. For example, on the emcsrv command shell, type:

```
sudo su -
```

You do not need to enter the root password.

Linux User Account

You use the Linux user account rsaadmin to run Authentication Manager CLUs or to stop or start Authentication Manager processes. The rsaadmin account is the owner of the RSA Authentication Manager 7.1 application and its files. This account does not have the sudo privilege.

You cannot log on to the Appliance with the rsaadmin account. You first must log on with the emcsrv account and then use sudo to change to the rsaadmin account. For example, on the emcsrv command shell, type:

```
sudo su - rsaadmin
```

You do not need to enter the password for the rsaadmin user account.

Runtime Command Privileges

You can use certain commands to diagnose issues or maintain the Appliance. To execute these commands, you must have certain privileges for security purposes.

The following table describes the commands and required privileges.

Command	Privilege	Description
scp	Common user	Secure remote file copy.
sftp	Common user	Secure remote file transfer.
Authentication Manager CLUs	rsaadmin user account and Authentication Manager administrative role **Note:** The required Authentication Manager administrative role varies per CLU. For example, to run some CLUs you must be a Super Admin. For another CLU, you can be a Token Administrator.	Authentication Manager utility that you access from the command line.

Command	Privilege	Description
sudo	Linux service account (emcsrv)	Changes the privileges of user accounts. The Appliance records all sudo use in the product logs. Only the emcsrv user has sudo privileges. If using the sudo privilege, the emcsrv user must enter the corresponding password every five minutes.

2 Post-Deployment Hardening Recommendations

RSA strongly recommends that you perform the following post-deployment system hardening tasks:

- Change the Default SNMP Community String
- Password Protection
- Administrative Role Assignment
- Network File System Server Security
- Appliance System Event Audits
- Removable Media Used on the Appliance
- Appliance Access Restriction
- Using ClamAV Antivirus Software with the RSA SecurID Appliance

Change the Default SNMP Community String

After you complete the initial deployment of RSA SecurID Appliance, consider changing the default SNMP community string for both the RSA Authentication Manager SNMP and Appliance SNMP. The SNMP server needs the community string (or password) to query the SNMP agents.

By default, this password is “public” for both Authentication Manager SNMP and Appliance SNMP. Consider changing the default string to a more secure password.

To change the default SNMP community string for Authentication Manager SNMP:

1. In the RSA Security Console, click **Setup** > **Instances**.
2. Click on the server instance for which you want to configure network management.
3. From the Context menu, click **Network Management (SNMP)**.
4. In the **SNMP Community String** field, enter a new string.
5. Click **Save**.

To change the default SNMP community string for Appliance SNMP:

1. In the RSA Operations Console, click **Administration > SNMP > Configure Appliance SNMP**.
2. In the **SNMP Community String** field, enter a new string.
3. Click **Save**.

Password Protection

You should protect the following passwords that you create during Quick Setup because they provide access to the Appliance:

- **Password for User ID emcsrv**: The Linux service account emcsrv (or the operating system account) is the account that you use to log on to the physical Appliance. You might log on to the Appliance to perform system maintenance or troubleshooting tasks, such as running command line utilities (CLUs).

  The User ID is always emcsrv. You create the initial password during Quick Setup.

- **Password for Authentication Manager Super Admin**: The Authentication Manager Super Admin can perform all tasks within Authentication Manager. You use the Super Admin account to access the Security Console and the Operations Console.

  You create the initial Super Admin account (both User ID and password) during Quick Setup on the Appliance primary. The Super Admin password that you create during Quick Setup is also used as the initial master password.

- **Master password**: The master password is required to perform certain administrative tasks in the Operations Console, such as generating replica package files, and for some of the Authentication Manager CLUs.

  On an Appliance primary, the initial master password is the initial Super Admin password that you create during Quick Setup. On an Appliance replica, the master password is the existing Super Admin password that you enter during Quick Setup.

If you record these passwords, be sure to put the record in a secure location.

You can change these passwords. For more information, see the chapter "Advanced Administration" in the *Owner's Guide*.

Administrative Role Assignment

After you complete the initial Appliance deployment, create administrators with only the necessary privileges for their job functions. During Quick Setup, you create the initial Super Admin account. However, because of the vast scope and permissions of the Super Admin role, you do not want all administrators using this account.

To create new administrators, add users to Authentication Manager and then assign them administrative roles with the appropriate permissions. After you assign an administrative role to a user, the user becomes an administrator.

By default, Authentication Manager provides the following administrative roles:

- **Super Admin**. The only role with full administrative permission in all realms and security domains in your deployment. Use it to create other administrators, and to create your realm and security domain hierarchy.

  You must be a Super Admin to complete some tasks in the Operations Console, such as generating a replica package file.

- **Realm Administrator**. This role grants complete administrative responsibility for managing all aspects of the realm. This role is limited in scope to the realm in which it is created and it does not include Super Admin permissions. The Realm Administrator can delegate some of the responsibilities of this role.
- **Security Domain Administrator**. This role grants permission to manage all aspects of a branch of the security domain hierarchy. This administrator has all permissions within that branch except the ability to manage top-level objects, such as policies and attribute definitions. By default, this role's scope includes the entire realm.
- **User Administrator**. This role grants administrative responsibility to manage users, assign tokens to users, and access to selected authentication agents. This administrator cannot delegate the responsibilities of this role.
- **Token Administrator**. This role grants complete administrative responsibility to import and manage tokens, and to assign tokens to users. This administrator cannot delegate the responsibilities of this role.
- **Privileged Help Desk Administrator**. This role grants administrative responsibility to resolve user access issues through password reset, and unlocking or enabling accounts. It also grants permission to provide online and offline emergency access help. This administrator cannot delegate the responsibilities of this role.
- **Help Desk Administrator**. This role grants administrative responsibility to resolve user access issues through password reset, and unlocking or enabling accounts. This administrator cannot delegate the responsibilities of this role.
- **Agent Administrator**. This role grants administrative responsibility to manage authentication agents and grants access to selected authentication agents. This administrator cannot delegate the responsibilities of this role.
- **Request Approver**. This role grants administrative responsibility to view and approve requests. This administrator can delegate the responsibilities of this role.
- **Token Distributor**. This role grants administrative responsibility to view requests and distribute requests. Distributors also determine how to assign and deliver tokens to users. This administrator can delegate the responsibilities of this role.

You can also create custom roles, if necessary. For more information, see the chapter "Preparing RSA Authentication Manager for Administration" in the *RSA Authentication Manager 7.1 Administrator's Guide*.

Network File System Server Security

If you use a Network File System (NFS) server for backup and restore operations or for updating the Appliance, be sure that you have secured the NFS server and the network on which it resides.

By default, when you create a backup file, the Appliance saves an unencrypted file to the local hard disk. However, you can configure the Appliance to save backup files to an NFS server.

If you do this, secure the NFS server to protect data and prevent file tampering. Then consider encrypting the backup file with a third-party application. Also, secure the network path between the NFS server and the Appliance because the backup file is not encrypted when traversing the network.

You can restore an Appliance from a backup file stored on an NFS server. You can also apply an update to the Appliance from a file stored on an NFS server. In both of these situations, secure the NFS server to protect data and prevent file tampering. You also want to secure the network path from the NFS server and the Appliance because the backup and updates files are not encrypted when traversing the network.

Appliance System Event Audits

You should routinely monitor the Authentication Manager and Appliance-only logs to confirm that Appliance events are authorized.

RSA Authentication Manager Logs

Authentication Manager maintains logs of all system events:

- **Trace**. Captures log messages that you can use to debug your system.
- **Administrative Audit**. Captures log messages that record any administrative action, such as adding and editing users.
- **Runtime Audit**. Captures log messages that record any runtime activity, such as authentication and authorization of users.
- **System**. Captures log messages that record system-level messages, such as "Authentication Manager Server started," and "Connection Manager lost db connection."

View Authentication Manager Logs

You can use the Authentication Manager logs to monitor the system and maintain an audit trail of all logon requests and operations performed using the Security Console.

To view Authentication Manager logs:

1. In the Security Console, click **Reporting** > **Real-time Activity Monitors**, and select one of the available Activity Monitors.
2. Enter the criteria of the log messages that you want the Activity Monitor to display. Leave these fields blank to view all activity.
3. Click **Start Monitor**.
4. When a message appears that you want to view, click **Pause Monitor**.
5. Click the date and time of the message that you want to view.

For more information about Authentication Manager logs, see the chapter "Logging and Reporting" in the *RSA Authentication Manager 7.1 Administrator's Guide*.

Appliance-Only Logs

The Appliance maintains logs of events specific to the Appliance:

- **Appliance log**. Contains messages for features that are only available in the Appliance version of Authentication Manager, such as SNMP hardware monitoring, update and rollback of the Appliance, and backup and restore of the Appliance.
- **Operating system logs**. Contains messages about the underlying Appliance operating system, such as disks, the BIOS, and memory usage and performance.

View Appliance-Only Logs

You can use the Appliance-only logs to monitor the Appliance and maintain an audit trail of operations performed using the Operations Console and the Appliance operating system.

To view Appliance-only logs:

1. In the Operations Console, click **Administration** > **Log Management** > **Download Log Files**.
2. Click the **Appliance Logs** or **Operating System Logs** tab.
3. Click the log file that you want to download.
4. From the Context menu, click **Download**.

For more information about Appliance-only logs, see the chapter "Appliance Logging and SNMP" in the *Owner's Guide*.

Removable Media Used on the Appliance

If you use a DVD, CD, or USB flash drive to apply updates to the Appliance, securely manage the removable media. You want to prevent unauthorized personnel from copying files onto the media that might harm the Appliance at the next use.

Appliance Access Restriction

As with any other hardware device in your network, allow only authorized users to physically access the Appliance. After Quick Setup, authorized users only need limited access to the physical Appliance.

For example, you might need to access the Appliance if you are applying an update from a DVD. In this situation, you need to put the DVD in the Appliance DVD/CD drive. Also, you might need to access the Appliance if you need to restore the Appliance to its system defaults (factory reset). In this situation, you need to restart the physical Appliance.

Using ClamAV Antivirus Software with the RSA SecurID Appliance

RSA has certified the ClamAV 0.97 anti-virus tool to work with the RSA SecurID Appliance 3.0.

Install ClamAV 0.97 on the SecurID Appliance

To install ClamAV 0.97 on the SecurID Appliance, complete the following tasks:

1. Enable SSH on the Appliance. Use a secure shell (SSH) client to install and run ClamAV 0.97 on the Appliance. Make sure that SSH is enabled in the RSA Operations Console. For more information, see "Enable SSH" on page 13.
2. Download the ClamAV archived files from the internet to your local machine.
3. Transfer the ClamAV archived files from your local machine to a location on the Appliance.
4. Extract the ClamAV archived files.
5. Load and install the ClamAV files on the Appliance.
6. Download the latest virus definitions.

After completing these tasks, you can use ClamAV 0.97 to scan your Appliance.

Configure ClamAV 0.97 on the SecurID Appliance

In order for ClamAVAntivirus software to work effectively with SecurID, you must configure this tool to exclude all of the files in the following Authentication Manager directories.

Path	Extensions to exclude
***RSA_AM_HOME*/db/oradata**	***.ctl** ***.dbf** ***.log** ***.dat**
***RSA_AM_HOME*/db/dbs**	***.ora**
***RSA_AM_HOME*/db/admin...**	***.log** ***.trc**
***RSA_AM_HOME*/backup**	***.arc**

Scan the SecurID Appliance with ClamAV 0.97

After you install ClamAV 0.97 on the Appliance, you can scan the Appliance for virus infections.

To scan the SecurID Appliance with ClamAV 0.97:

1. Open an SSH connection to your Appliance. For more information, see "Enable SSH" on page 13.
2. Log on as **emcsrv** using the operating system password.
3. Switch user to **root**. Type:

   ```
   sudo su -
   ```

   and press ENTER.
4. When prompted, enter the emcsrv password, and press ENTER.
5. Change directories to the ClamAV 0.97 installation directory, **../clamav-0.97/**.
6. Run ClamAV 0.97, excluding the necessary files. Type:

```
clamscan -r /
--exclude-dir=/usr/local/RSASecurity/RSAAuthenticationManager/db/oradata/
--exclude-dir=/usr/local/RSASecurity/RSAAuthenticationManager/db/dbs
--exclude-dir=/usr/local/RSASecurity/RSAAuthenticationManager/db/admin
--exclude-dir=/usr/local/RSASecurity/RSAAuthenticationManager/db/backup |
tee /tmp/clamav.log
```

   and press ENTER.

For more information, see the *Clam AntiVirus 0.96 User Manual*.

Index

A

Appliance SNMP
  agent, 9
Authentication Manager
  documentation set, 4

C

communication
  port usage, 9
Customer Support, 5

D

documentation set
  RSA Authentication Manager, 4
  RSA RADIUS, 4
  RSA SecurID Appliance, 3

F

firewall, required open ports, 9

L

license
  determining ID of, 5

O

operating system
  port, 9

P

ports, 9

R

RADIUS, 12

S

SecurID Appliance documentation set, 3
services
  defined, 9
  protocols used, 9
SSH
  port, 9
Support, Customer, 5

V

version, viewing, 5