RSA Authentication Manager 7.1
Planning Guide

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 and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**. EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.

License agreement

This software and the associated documentation are proprietary and confidential to RSA, 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 RSA.

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.html** files.

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

Limit distribution of this document to trusted personnel.

RSA notice

The RC5™ Block Encryption Algorithm With Data-Dependent Rotations is protected by U.S. Patent #5,724,428 and #5,835,600.

First printing: April 2008

The Security Division of EMC

Contents

The Security Division of EMC

Preface

About This Guide

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

RSA Authentication Manager Documentation

For more information about RSA Authentication Manager, see the following 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.

Related 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

Make sure you have access to the computer running the RSA Authentication Manager software.

Please have the following information available when you call:

- ❑ 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 Authentication Manager software version number. You can find this in the RSA Security Console by clicking **Help > About RSA Security Console > See Software Version Information**.
- ❑ The names and versions of the third-party software products that support the Authentication Manager feature on which you are requesting support (operating system, data store, web server, and browser).
- ❑ The make and model of the machine on which the problem occurs.

The Security Division of EMC

1 Overview of RSA SecurID Authentication

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

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

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

Product or Application	Description
VPN access	RSA SecurID provides security when used in combination with a VPN.
Remote dial-in	RSA SecurID operates with remote dial-in servers, such as RADIUS.
Web access	RSA SecurID protects access to web pages.
Wireless networking	Authentication Manager includes an 802.1-compliant RADIUS server.
Secure access to Microsoft Windows	Authentication Manager can be used to control access to Microsoft Windows environments both online and offline.
Network hardware devices	Authentication Manager can be used to control desktop access to devices enabled for SecurID, such as routers, firewalls, and switches.

Authenticating Users

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

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

The Authentication Manager authentication process is an interaction of three distinct products:

- RSA SecurID tokens
- RSA Authentication Agents
- RSA Authentication Manager

RSA SecurID Tokens

An RSA SecurID token is a hardware device or software-based security token that generates and displays a random number that enables users to securely access protected resources. The random number is called a tokencode.

In addition to the tokencode, RSA SecurID typically requires a PIN, either created by the user or generated by Authentication Manager. Requiring both the tokencode and the PIN is known as two-factor authentication: something you have (the token) and something you know (the PIN). In Authentication Manager, the tokencode and the PIN combined are called a passcode. When users try to access a protected resource, they enter the passcode at the logon prompt. (To protect against the use of stolen passcodes, Authentication Manager checks that a passcode has not been used in any previous authentication attempt.) RSA SecurID also supports tokens that do not require a PIN. The user can authenticate with the current tokencode only.

Before a user can authenticate with a token, the token must be recognized by Authentication Manager. RSA, or your vendor, ships a token seed file that you must import into the data store. Seeds listed in this file are assigned to tokens for generating the tokencode when an authentication request is received from an Authentication Manager agent.

RSA Authentication Agents

An agent is a software application installed on a machine, such as a domain server, web server, or personal computer, that enables authentication communication with Authentication Manager on the network server. The authentication agent requires any user logging on to provide the correct RSA SecurID passcode in addition to any other required logon information, such as User ID and network password.

There are two types of agents in Authentication Manager:

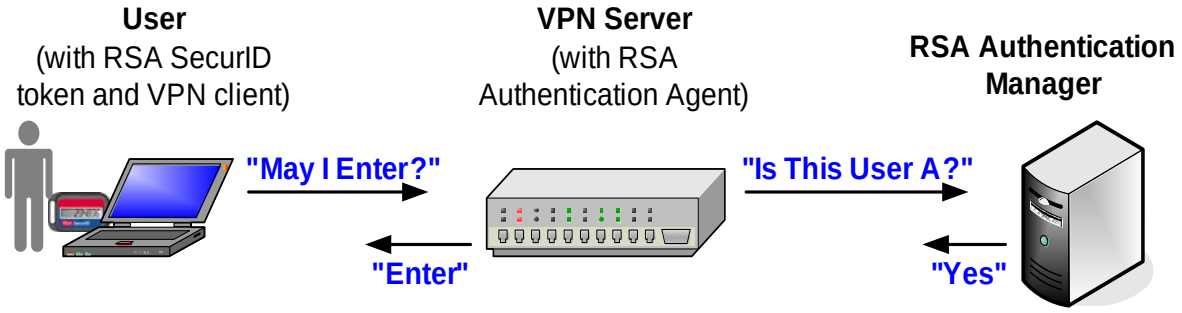
Unrestricted. Unrestricted agents can be accessed by all registered users in the same realm as the agent. Registered users are users who are known to the agent. If there are multiple identity sources associated with the realm, users in all identity sources can access the unrestricted agent. An identity source is a data store containing user and user group data.

Restricted. Restricted agents can be accessed only by users belonging to the user group associated with the restricted agent. Resources protected by restricted agents are considered to be more secure. Rather than allowing access to any user in the identity source, only a subset of users are allowed access.

RSA Authentication Manager

Records of users, agents, tokens, and user's PINs reside somewhere in your network. Portions of these records may reside in Authentication Manager or in LDAP directories. During authentication, Authentication Manager compares these records to the information it receives when a user attempts to access the network. If the records and tokencode or passcode match, the user is granted access.

Authentication Manager verifies the supplied passcodes, user records, agents, tokens, user's PINs, and policies. It responds to the request sent by the authentication agent, as shown in the following figure of authentication through a VPN server.



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

1. A user initiates an authentication request by logging on to a system.
2. The agent prompts the user to enter a User ID and an RSA SecurID passcode or tokencode.
3. The user reads the tokencode from the token and then enters his or her PIN plus the tokencode to create the passcode. (In systems where a PIN is not required, the user enters the tokencode only.)

4. The agent software sends the entered data to Authentication Manager.

   The packets containing the data are encrypted using a shared key called a node secret, which is known only to Authentication Manager and the agent. The node secret itself is encrypted on the agent and in the database.

5. Authentication Manager receives the User ID and passcode or tokencode and looks for the user record in an identity source.
6. Authentication Manager calculates the correct value of the passcode by accessing the token record of the token assigned to the user. Using data contained in the token record, it generates the passcode and time to compare with that supplied by the user.
7. Authentication Manager evaluates the policies defined by the administrator.
8. If the passcode is correct and the policies allow access, Authentication Manager approves the authentication request. The user is allowed access to the protected device.

2 System Requirements

Hardware and Operating System Requirements

Make sure that your system meets these minimum requirements for supported platform and system components. The requirements listed in this section serve only as guidelines. Hardware requirements vary depending on a number of factors, including authentication rates, number of users, frequency of reporting, and log retention. For more information, see the *Performance and Scalability Guide*.

The values listed for RSA RADIUS disk space and memory are in addition to those for Authentication Manager when RADIUS is installed on the same machine with Authentication Manager. When RADIUS is installed on a standalone machine, the values listed for Authentication Manager are sufficient.

Note: You must install all of your Authentication Manager and RADIUS software on the same system types. For example, do not configure Authentication Manager on Solaris and then configure RADIUS on Windows.

For CPU speed, memory, and disk speed, RSA recommends that the database server be significantly more powerful than every other machine in your Authentication Manager deployment.

RSA recommends that you deploy Authentication Manager on machines to which only authorized users have access. For example, avoid deploying Authentication Manager on machines that host other applications to which non-administrative users have access.

Important: Be sure that your UNIX and Windows servers are known by their fully qualified domain names. If you are installing the Authentication Manager database on a separate machine, configure your DNS server to resolve by both fully qualified name and short name.

Windows System Requirements

Operating System	Microsoft Windows Server 2003 Enterprise R2 SP2 (32-bit) Microsoft Windows Server 2003 Enterprise SP2 (32-bit) Microsoft Windows Server 2003 Enterprise R2 SP2 (64-bit) Microsoft Windows Server 2003 Enterprise SP2 (64-bit) **Note:** RADIUS is not supported on 64-bit Windows and Linux systems.
Hardware	Intel Xeon 2.8 GHz or equivalent (32-bit) Intel Xeon 2.8 GHz or equivalent (64-bit)
Disk Space	**RSA Authentication Manager:** 60 GB free space recommended **Important:** Do not allow all disk space to become consumed. At that point, Authentication Manager may stop operating and be difficult to restore. **RSA RADIUS:** Add 125 MB of free space
Memory Requirements	**RSA Authentication Manager:** 2 GB **RSA RADIUS:** Add 512 MB
Page File	2 GB

Linux System Requirements

Operating System	Red Hat Enterprise Linux 4.0-1 ES (32-bit) Red Hat Enterprise Linux 4.0-1 ES (64-bit) Red Hat Enterprise Linux 4.0-1 AS (32-bit) Red Hat Enterprise Linux 4.0-1 AS (64-bit) **Note:** RADIUS is not supported on 64-bit Windows and Linux systems.
Hardware	Intel Xeon 2.8 GHz or equivalent (32-bit) Intel EM64T 2.8 GHz or AMD Operon 1.8 GHz, or equivalent (64-bit)
Disk Space	**RSA Authentication Manager:** 60 GB free space recommended **Important:** Do not allow all disk space to become consumed. At that point, Authentication Manager may stop operating and be difficult to restore. **RSA RADIUS:** Add 470 MB of free space
Memory Requirements	**RSA Authentication Manager:** 2 GB **RSA RADIUS:** Add 512 MB
Swap Space	2 GB
Kernel Version	2.6.9-22.EL and later
Kernel Parameters	Maximum shared memory must be at least 256 MB

Packages (RPM) 32-bit	The following packages must be installed: binutils-2.15.92.0.2-12 bog1-0.1.18-4 compat-db-4.1.25-9 compat-libstdc++-296.2.9.6-132.7.2 compat-open1dap coreutils 5.2.1-31.2 or later control-center-2.8.0-12 cyrus-sasl-gssapi-2.1.19-5 cyrus-sasl-ntlm-2.1.19-5 cyrus-sasl-sql-2.1.19-5 fribidi-0.10.4-6 gcc-3.4.3-22.1 gcc-c++-3.4.3-22.1 gnome-libs-1.4.1.2.90-44.1 glibc-common-2.3.4-2.19 glibc-2.3.2-95.20 gsl-1.5-2 gtkspell-2.0.7-2 kdelibs initscripts 7.93.20 or later libstdc++-3.4.3-22.1 libaio-0.3.105-2.i386 libavc1394-0.4.1-4 libdbi-0.6.5-10 make-3.80-5 libstdc++-devel-3.4.3-22.1 pdksh-5.2.14-30 setarch-1.6-1 sysstat-5.0.5-1 xscreensaver-4.18-5 **Note:** To check your RPM versions on Linux, use the command, rpm -q *package name*.
Packages (RPM) 64-bit	Install the following packages: Compatibility Arch Development Support Compatibility Arch Support **Note:** Make sure that all components in each package are selected.

Solaris System Requirements

Operating System	Solaris 10 (64-bit)
Hardware	UltraSPARC 1.5 GHz, or equivalent For improved performance, use Sun 6 or 8 core UltraSPARC T1 servers. **Note:** On Sun UltraSPARC systems, Authentication Manager start-up and migration processes can take considerable time. For example, restarting Authentication Manager can take 15 minutes or more. Migration of a large database can take 12 hours or more. In general, Sun UltraSPARC systems with faster processors will yield better start-up and migration performance.
Disk Space	**RSA Authentication Manager**: 60 GB free space recommended 20 GB free space minimum **RSA RADIUS:** Add 650 MB of free space
Memory Requirements	**RSA Authentication Manager:** 4 GB **RSA RADIUS:** Add 512 MB
Swap Space	4 GB
Packages	SUNWarc SUNWbtool SUNWhea SUNWlibm SUNWlibms SUNWsprot SUNWtoo SUNWi1of SUNWi1cs SUNWi15cs SUNWxwfnt

Supported Browsers

This section describes the browsers supported for the RSA Security Console for your platform.

On Windows

- Internet Explorer 6.0 with SP2 for Windows XP
- Internet Explorer 7.0 for Windows XP and Windows Vista
- Firefox 2.0

On Linux

- Firefox 2.0

On Solaris

- Firefox 2.0
- Mozilla 1.07

Note: On all browsers, JavaScript must be enabled. Microsoft Internet Explorer may require configuration depending on its security level setting. See the Microsoft Internet Explorer Help for more information.

Port Usage

The following port numbers must be available to enable authentication, administration, replication, and other services on the network. RSA recommends that you reserve these ports for Authentication Manager, and make sure that no other applications or services are configured to use them.

Port Number	Protocol	Service	Description
1161	UDP	SNMP agent	Used to communicate with a Network Management Server using the Simple Network Management Protocol.
1162	UDP	SNMP agent	Used to communicate with a Network Management Server using the Simple Network Management Protocol.
1645	UDP	RADIUS authentication (legacy port)	Used for authentication requests from RADIUS clients.

Port Number	Protocol	Service	Description
1812	UDP	RADIUS authentication (standard port)	Used for RADIUS authentication and accounting.
1646	UDP	RADIUS accounting (legacy port)	Used for requests for accounting data.
1813	TCP	RADIUS (standard port)	Used for RADIUS administration and replication.
2334	TCP	RSA Authentication Manager database listener	Used to replicate data between instances.
5500	UDP	Agent authentication	Used for communication with authentication agents. This service receives authentication requests from agents and sends replies.
5550	TCP	Agent auto-registration	Used for communication with authentication agents that are attempting to register with Authentication Manager.
5556	TCP	RSA Authentication Manager node manager	Used to monitor and manage various services.
5580	TCP	Offline authentication service	Used to receive requests for additional offline authentication data, and send the offline data to agents. Also used to update server lists on agents.
7002	TCP	RSA Authentication Manager	Used for SSL-encrypted administration connections.
		RSA Authentication Manager Microsoft Management Console snap-in	Used for SSL-encrypted connections.

Port Number	Protocol	Service	Description
7004	TCP	RSA Authentication Manager proxy server	Used for load balancing of administration in an instance with multiple server nodes. This port is used for SSL connections.
		RSA Self-Service Console proxy server/SSL	Used for communication from users to Authentication Manager for requests and maintenance tasks. This port is used for SSL connections.
		RSA Authentication Manager Microsoft Management Console snap-in proxy server	Used for load balancing of administration in an instance with multiple server nodes. This port is used for SSL connections.
7006	TCP	RSA Authentication Manager cluster administration channel	Internal use only.
7008	TCP	RSA Authentication Manager cluster administration server	Internal use only.
7012	TCP	RSA Authentication Manager administration channel	Internal use only.
7014	TCP	RSA Authentication Manager proxy server administration channel	Internal use only.
7022	TCP	Network access point	Used for mutually authenticated SSL-encrypted trusted realm connections.
7071	TCP	RSA Operations Console	Used for non-SSL connection.
7072	TCP	RSA Operations Console	Used for SSL connections.

Supported Data Stores

You can store data in:

- The internal database
- One or more LDAP directories (called an identity source within Authentication Manager)

If you use the Authentication Manager internal database only, it contains all user, user group, policy, and token data. If you integrate Authentication Manager with external identity sources, only user and user group data reside in the external identity source. Policy and token data are stored in the Authentication Manager internal database.

Internal Database

Authentication Manager is installed with an internal database. The internal database contains all application and policy data, and you may choose to store user and user group data in it.

Identity Sources

Authentication Manager supports the use of an external LDAP directory for user and user group data.

Supported LDAP directories are:

- Sun Java System Directory Server 5.2, SP 3
- Microsoft Active Directory 2003, SP 2

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

Sun Java System Directory Server can be located on the same machine as Authentication Manager or on a different machine. When the Sun Java System Directory Server is not on the same machine, a network connection between the two machines is required. Active Directory must be located on a different machine.

Authentication Manager LDAP integration does not modify your existing LDAP schema, but rather creates a map to your data that Authentication Manager uses.

RSA requires SSL for Active Directory connections to avoid exposing sensitive data passing over the connection. For example, if bind authentications are performed over a non-SSL connection, the password is sent over the wire in the clear. The use of SSL-LDAP requires that the appropriate certificate is accessible by Authentication Manager.

System Requirements Summary

Know the following when planning system requirements.

- Machines hosting Authentication Manager and RADIUS must be on the same platform.
- Which machines must meet minimum Authentication Manager requirements.
- Which server node must be the most powerful.
- Which browsers are supported.
- Which ports are required for Authentication Manager.
- Which third-party directory servers are supported, if you plan to use them.
- When SSL-LDAP certificates are required.

3 The Deployment Process

Each section in this chapter summarizes the concepts and considerations around a specific decision point for planning an RSA Authentication Manager 7.1 deployment. For complete details about a particular topic, a cross-reference to the corresponding chapter is provided at the end of the section.

Important Terms and Concepts

The following terms and concepts are unique to Authentication Manager. It is important that you understand them before you read the remainder of this document.

Agent. A software application installed on a device, such as a domain server, web server, or desktop computer, which enables authentication communication with Authentication Manager on the network server.

An agent protects the device on which it is installed. When a user attempts to log on, the agent passes the user's logon credentials to Authentication Manager. Based on the pass or fail information that the agent receives from Authentication Manager, it either allows or prevents the user from accessing the device.

Deployment. The arrangement of Authentication Manager instances into appropriate locations in a network to perform authentication.

Instance. A single Authentication Manager database server, or an Authentication Manager database server and one or more server nodes, acting as a single cohesive processing unit.

Primary instance. Where authentication and all administrative actions occur. You update administrative information on the primary instance. The first instance you install is the primary instance for your deployment. All other instances are replica instances.

Realm. A hierarchy of organizational units, called security domains, for administrative purposes. A realm includes all the objects that your administrators need to manage in Authentication Manager, including users, user groups, identity sources, tokens, policies, and more.

Replica instance. A copy of your primary instance. You can view, but not update, administrative data on a replica instance. Administrative updates are propagated to the replica instances from the primary instance.

Security domain. An organizational container that defines an area of administrative management within a realm, for example, business units, departments, or partners. They establish ownership and namespaces for objects (users, roles, permissions, and so on) within the system. Security domains are hierarchical.

Server node. An installation of Authentication Manager on a single server host.

RSA Authentication Manager Network Integration

Before you begin planning your Authentication Manager deployment, review your existing network topology. Gather and review charts, diagrams, and lists that describe how your current network is designed. Your current topology impacts how you plan the organization, configuration, and administration of Authentication Manager.

Authentication Manager integrates with VPNs, RADIUS, TACACS, OWA, Web pages, FTP, CITRIX servers, and Windows desktops. When you install Authentication Manager, you can acquire certain VPN and RADIUS servers that contain agents. For more information, go to **http://www.rsa.com/rsasecured/**. After reviewing your current network topology, determine which devices you want to integrate with Authentication Manager, and plan to acquire any new ones.

Authentication Manager includes an internal database that can store all of the data required to administer and run the system. If you have an existing directory server, you can integrate it with Authentication Manager.

An Authentication Manager deployment consists of one primary instance and up to 15 replica instances. Each instance has one server node that contains the internal database and each instance can support up to 4 server nodes. RSA recommends that you install at least one replica instance for failover and disaster recovery.

You can locate the Authentication Manager internal database on a standalone server, or you can add server nodes to your primary instance and replica instances for performance. Plan the number of instances that you require, the location of the Authentication Manager internal database, and you can add the number of server nodes you want for your deployment.

The organizational hierarchy of your RSA Authentication Manager deployment is made up of realms and security domains. A realm contains users, user groups, administrative roles, tokens, and policies. A default realm is automatically created when you install Authentication Manager and you can add realms as needed.

Security domains represent areas of administrative responsibility. All Authentication Manager objects are managed by a security domain. Security domains allow you to organize and manage your users, enforce system policies, and limit the scope of administrator's control by limiting the security domains to which they have access. Scope is the security domain or security domains in which an administrative role applies. An administrative role is a collection of permissions and the scope within which those permissions apply.

See Chapter 4, "Planning RSA Authentication Manager Network Integration."

Optimal System Performance

It is likely during daily operation that your users will log on to the network at specific times, requiring Authentication Manager to authenticate large numbers of users in a relatively short time frame. Determine the times each day that the highest rates of authentication occur.

Authentication Manager provides load balancing through contact lists, which contain a list of all the server nodes where the authentication agent can direct authentication requests.

See Chapter 5, "Planning Optimal System Performance."

Failover and Disaster Recovery

RSA recommends that you perform backups on a regular and frequent basis. Formulate a backup policy, a recovery plan, and store a copy of the backup at an off-site location. Know the common reasons why an instance might stop responding and know how to promote a replica instance to a primary instance, if a primary instance stops responding.

Note: When using third-party backup software, exclude RSA directories unless you stop Authentication Manager first.

See Chapter 6, "Planning for Failover and Disaster Recovery."

Installation and Upgrading

An Authentication Manager installation consists of one or more installation types. Depending on the requirements of your deployment, you need to install one or more of the following:

- A primary instance
- One or more replica instances
- One or more server nodes
- RADIUS
- A standalone database server
- Software Developer's Kit and documentation
- Upgrade

The installation process often requires coordination among the people who have permissions to access and administer the various components in your network, such as access through proxy servers and firewalls. Develop a plan to coordinate the necessary people along with a timetable for implementation.

If your deployment uses an external directory server, you can integrate it with Authentication Manager. Choose whether you want Authentication Manager to have read-only access or read/write access to directory servers.

Authentication Manager 7.1 includes command line utilities for upgrading from version 7.0. You can upgrade your existing Authentication Manager 7.0 machine, or install version 7.1 on a different machine. With either of these options, you can install your database on a separate machine. If you are upgrading from Authentication Manager 7.0 to version 7.1, see the *Installation and Configuration Guide*. If you are upgrading from Authentication Manager 6.1 to version 7.1, see the *Migration Guide*.

RSA recommends that you conduct a pilot test of Authentication Manager in advance of your live deployment. Test authentication, system connections, disaster recovery, administrative tasks, and reports.

See Chapter 7, "Planning for Installation and Upgrading."

Administration

The Authentication Manager administrative model is built on the concepts of roles, permissions, and scope. Authentication Manager includes a set of predefined administrative roles and it enables you to create custom roles.

You can perform administrative changes for Authentication Manager and RADIUS only on the primary instance, which replicates these changes to all of the replica instances in the deployment. If you have Active Directory and plan to install the Authentication Manager Microsoft Management Console (MMC) snap-in, plan to deploy the MMC snap-in on the machines where the Active Directory administrators have permission to perform Active Directory administration tasks.

By default, all users are managed in the top-level security domain. After you create your security domain hierarchy and link your identity source to your realm, you can transfer users to other security domains in your hierarchy.

Develop a plan to train your users and administrators. If you have any tasks that are unique and specific to your business, remember to add them to your list of training topics.

See Chapter 8, "Planning for Administration."

Planning Policies

RSA Authentication Manager provides authentication services that allow you to verify the identity of each user attempting to access computers and network resources. This does not replace the need to implement and use the product properly nor can it offer protection against an intruder who has both a user's PIN and RSA SecurID token. Plan to create policies to protect against:

- Random guessing of passcodes
- Compromised PINs
- Stolen passcodes
- Easily guessed PINs
- Automated logon attempts

Policies control various aspects of a user's interaction with Authentication Manager such as RSA SecurID PIN lifetime and format, fixed passcode lifetime and format, password length, lockout policies, format, and frequency of change. You enforce system policies by assigning policies to security domains. You can use the default policy, or create a custom policy, for each policy type, for each security domain.

Password Policies

Password policies for Administrator's access to the RSA Security Console define the password length, format, and frequency of change, and are assigned on a per security domain basis.

Token and PIN Policies

You can configure the following requirements and restrictions:

- Require system generated PINs
- Require periodic PIN changes
- Restrict the use of old PINs
- Limit PIN lengths
- Use an excluded words dictionary
- Set PIN character requirements

Lockout Policies

Lockout policies are assigned to a security domain to define how many failed logon attempts users can make before Authentication Manager locks their account.

Offline Authentication

Offline authentication extends RSA SecurID for Windows authentication to users when they work away from the office, or when network conditions make the connection temporarily unavailable. Specify an offline authentication policy and apply it to Authentication Manager security domains.

See Chapter 9, "Planning Policies." on page 93.

RSA SecurID Token Deployment

The complexity of your deployment, the size of your user population, and the ease of distribution are important factors in deciding which type of token to deploy. Determine which types of tokens best meet the needs of your users and your deployment. These are the RSA SecurID token types:

- Hardware

  A physical device, usually a key fob or USB token, that displays a tokencode. Users receive tokens at a central location or in the mail.

- Software

  A software token record is issued from the RSA Security Console and distributed to the user in file format for installation on devices such as a client workstation, web browser, RSA smart card, PDA, or mobile devices.

See Chapter 10, "Planning RSA SecurID Token Deployment"

Self-Service and Provisioning

RSA Credential Manager allows users to request tokens, perform token maintenance tasks, and troubleshoot tokens. Credential Manager consists of self-service and provisioning.

If you plan to deploy self-service, you need to:

- Decide on the user authentication method to use for the RSA Self-Service Console
- Decide how to customize user profiles
- Decide which security domains to make available to users
- Decide which identity sources to make available to users
- Decide which authentication method to make available to users for self-service troubleshooting

If you plan to deploy provisioning, you need to:

- Determine the roles you need to create
- Define the workflows for each type of user request
- Decide which user group membership to make available to users
- Decide which tokens to make available to users
- Decide whether users can request the on-demand tokencode service
- Decide how to customize e-mail notifications for your company's needs

See Chapter 11, "Planning Self-Service and Provisioning."

RSA RADIUS Integration

RADIUS is a client/server based access-control protocol that verifies and authenticates users based on the commonly used challenge/response method. While RADIUS has a prominent place among Internet service providers and network service providers, it can benefit any environment where central authentication, regulated authorization, and detailed user accounting is needed. RSA RADIUS is an optional feature of RSA Authentication Manager 7.1. There are many RADIUS server vendors who provide SecurID-ready machines. For more information, go to **http://www.rsa.com/rsasecured/**.

If you want to install RADIUS on your Authentication Manager machine, you should do so when you install Authentication Manager. If you want to install RADIUS on your Authentication Manager machine at a later date, you must uninstall Authentication Manager and reinstall it. RSA recommends that your RSA RADIUS deployment follows the same deployment model you choose for Authentication Manager. Each deployment of Authentication Manager (a primary instance and one or more replica instances) should have a similar deployment of RADIUS (a primary instance and one or more replica instances).

RADIUS supports a single realm. For an environment with multiple Authentication Manager realms, plan a separate RADIUS deployment (one primary instance and one or more replica instances) for each realm. RADIUS supports all users in the realm, regardless of where they are in the security domain hierarchy in the realm.

Other planning decisions include:

- Installation and administration requires a user account that must exist on the machine where RADIUS is installed. Create this account before installing RADIUS.
- RSA recommends placing RADIUS equipment in a locked location accessible to a minimum number of trusted personnel.
- RADIUS is subject to the same peak authentication periods as Authentication Manager. The main consideration is to have enough RADIUS servers to handle the peak load.

See Chapter 12, "Planning for RSA RADIUS Integration."

Planning for Administration and Maintenance

Administrators require knowledge of how RADIUS operates to effectively manage and maintain RADIUS. Some training may be needed, especially for new administrators.

See "Planning for Administration" on page 142.

Accounting and Logging

RSA RADIUS has very flexible accounting capabilities that let you capture as many or as few usage statistics as needed for billing or monitoring purposes. Audit logs capture administrator actions including authentications and any changes made using the Security Console or Operations Console. RADIUS configuration files allow administrators to control these functions. For more details, see the *Administrator's Guide*.

Planning for Failover and Disaster Recovery

Key issues to consider:

- RADIUS is not included in an Authentication Manager backup.
- Prepare a recovery plan, and conduct regular RSA RADIUS backups to ensure against loss. Store a copy of the backup at an off-site location.
- Know how to detect an RSA RADIUS server that has stopped responding. Understand why it has stopped responding and how this affects administration and performance.
- Understand how to remove a stopped instance from the system and how to promote a replica instance to primary instance, if necessary.

See "Planning for Failover and Disaster Recovery" on page 140.

Emergency Access

Plan how you want users to authenticate when they lose, misplace, or damage their tokens. Authentication Manager provides these emergency access methods for SecurID for Windows deployments.

For online users:

- Temporary fixed tokencode. For users whose computers are online with the network. They can access their protected computers without a tokencode (for example, when they have lost their tokens).
- One-time tokencode. For users whose computers are online with the network. They can access their protected computers with a tokencode that allows one access.
- On-demand tokencode. For users with digital mobile devices and home e-mail accounts. If enabled, they can receive one-time tokencodes as text messages.

For offline users:

- Offline emergency access tokencode. For users whose computers are not connected to the network. They can access their protected computers without a tokencode (for example, when they have lost their tokens).
- Offline emergency access passcode. For users whose computers are not connected to the network. They can access their protected computers without a PIN (for example, when they have forgotten their PINs).

See Chapter 13, "Planning for Emergency Access."

Logging and Reporting

Audit information about all significant aspects of any administrative or runtime action performed by an administrator or user in a single deployment is recorded in the internal database. The system also provides a decentralized tracing log capability, per component, to help you resolve issues at the local level. Consider the following logging and reporting options:

- Standard reports

  There are report templates, that you can customize.
- Event logging

  The system automatically logs all authentication and administrative events and stores them in a database.
- Activity monitor

  This tool enables you to view authentication and administration activity in real-time.
- Log signing

  Enables you to sign by log type. For example, Admin, System, Runtime. You must decide to enable this upon installation. Log signing is typically used on Admin and Runtime logs. Use the command line utility **verify_archive_log** to confirm that signed logs have not been altered. For example, for compliance purposes.

  Note: You cannot enable or disable log signing after installation.

Each replica instance automatically sends its log files to the database in the primary instance. In this way, all of your Authentication Manager logs are consolidated into one database.

If your company utilizes a Network Management System (NMS), consider enabling the SNMP agent for your Authentication Manager instances and using the NMS to monitor critical events and overall system health.

The information that you can query for a report is controlled by your administrative scope. If you plan to delegate running reports to other administrators, be sure that you trust them to view all of the information that they can see in such reports. Consider designing delegated reports in a way that limits the information appropriately to the viewer. Select only your most trusted administrators to run reports.

You can run reports manually at any time, or you can schedule them to run automatically at predetermined times.

RSA RADIUS includes two types of logging:

- Accounting, which logs user activity. For example, user logons.
- RADIUS, which logs events in RADIUS. For example, the number of authentications.

See Chapter 14, "Logging and Reporting."

The Security Division of EMC

4 Planning RSA Authentication Manager Network Integration

Reviewing Your Existing Network Topology

Before you plan to integrate RSA Authentication Manager, review your existing network topology. The information will help you determine how Authentication Manager affects your network. As you review this information, consider where you might want to add or upgrade any hardware in your network. The following table describes the types of information to review.

Information to Review	Description
Diagrams of your network topology	Diagrams of the physical location of all servers, other hardware, wireless access points, internal resources, firewalls, portals, and users' machines
Lists of applications	Lists of applications in use for authentication, where they are, and who uses them
Authentication process flow charts	Flow charts depicting the existing authentication process, if any
Organizational hierarchy charts	Charts of the logical organization of users, groups, security domains, departments, business units, and other such entities
Policies and permissions	Descriptions of the network policies and permissions for all of your users and administrators
Checklists	Checklists of tasks from past implementations

How RSA Authentication Manager 7.1 Protects Your Network

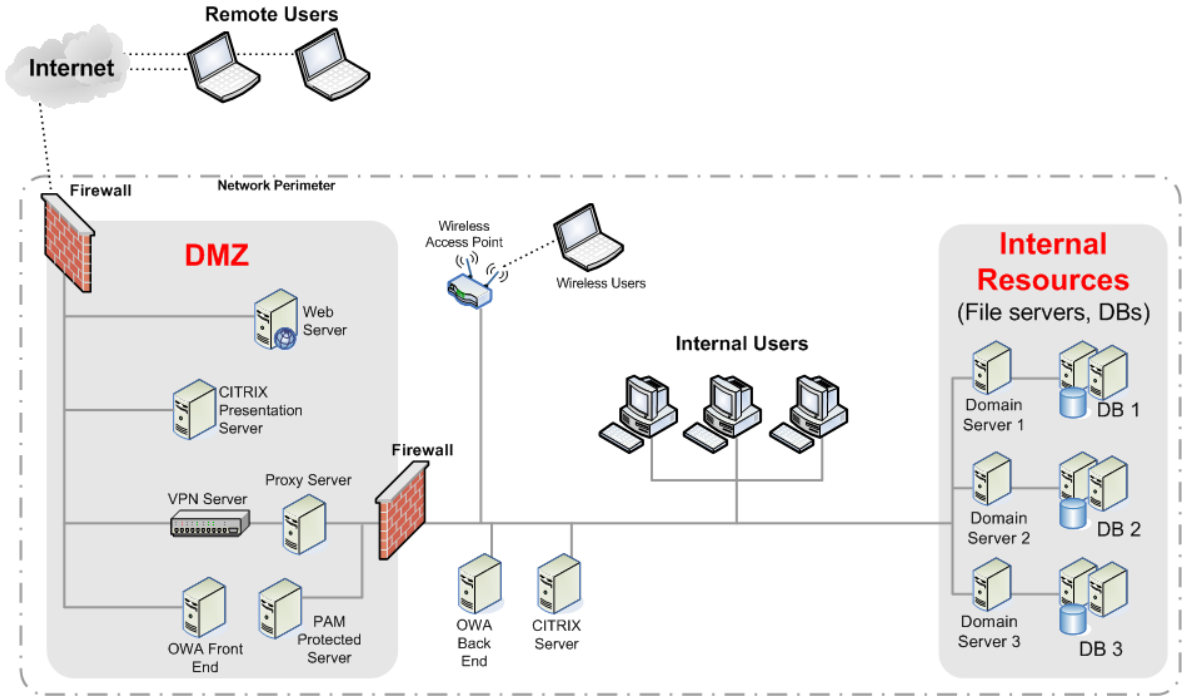
Authentication Manager protects a wide variety of resources, regardless of the method used to access those resources. The following table lists a number of resources used to provide protection.

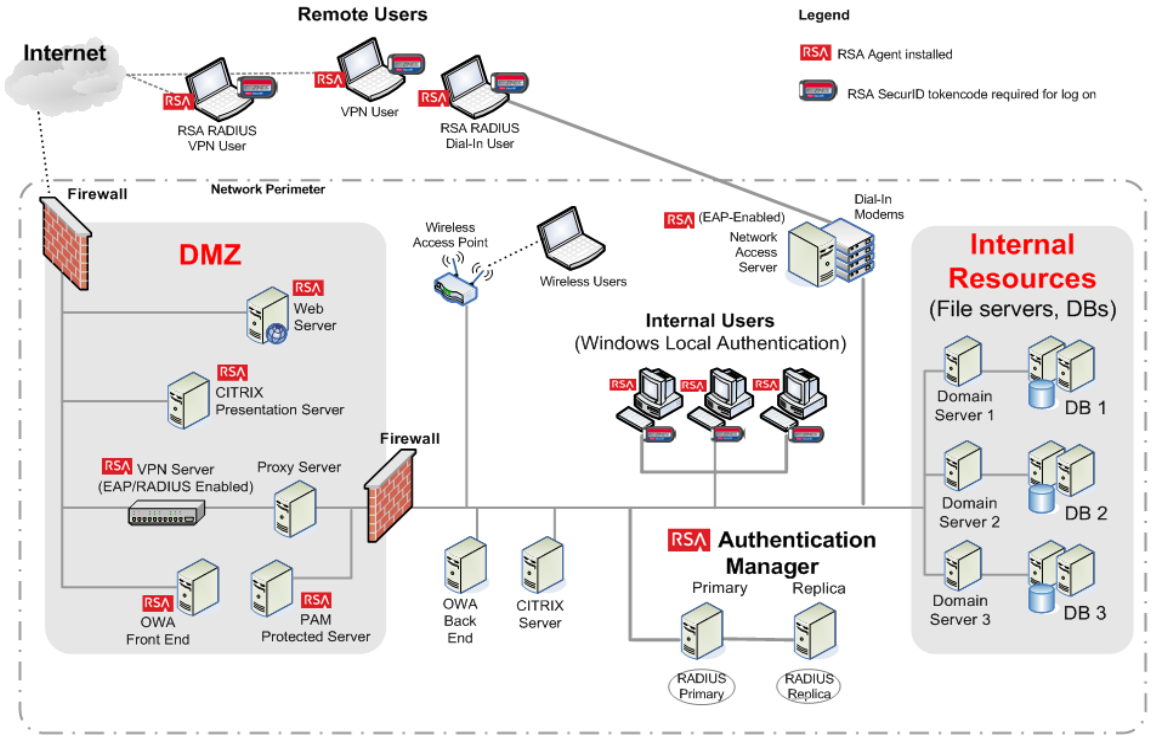
Resources	Protection
RSA Authentication Manager Servers	By default, administrative access to the RSA Security Console is protected by RSA SecurID. Access is configurable, and you can require one or more of the following instead of, or in addition to, SecurID: • RSA Security Console password • LDAP password • Security questions • SMS The Security Console is browser-based and all connections through it are encrypted by a Secure Sockets Layer (SSL). Direct access to the machine itself is not protected until you install an authentication agent on the machine and configure the agent to require authentication at log on.
Virtual Private Network (VPN) Server	Authentication Manager protects connections through Virtual Private Networks, when used in conjunction with third-party VPN servers. (You can obtain VPN servers that contain an embedded RSA Authentication Agent.) For more information about supported VPN servers, go to **http://www.rsa.com/rsasecured/**.
Remote Authentication Dial-In User Service (RADIUS) server	Authentication Manager includes RSA RADIUS. A RADIUS server configured to handle RSA SecurID authentications forwards such requests to Authentication Manager, which processes the request and returns the result (either allowing or denying access) to the RADIUS server. If you already use RADIUS servers to authenticate users accessing your resources, Authentication Manager can accommodate them. You can also obtain RADIUS servers that contain an embedded RSA Authentication Agent.
Terminal Access Controller Access Control System (TACACS)	RSA provides an authentication agent that specifically supports the TACACS protocol for UNIX.
Outlook Web Access (OWA)	Authentication Manager protects users access to Microsoft Outlook e-mail accounts through the web interface (OWA) using the RSA Authentication Agent 5.3 for Web for Internet Information Services installed on a Microsoft Exchange server. Go to **http://www.rsa.com/node.asp?id=2807**.

Resources	Protection
Web pages	Authentication Manager protects user access to individual web pages or entire web sites using the RSA Authentication Agent for Web on a variety of web server platforms, including Microsoft IIS, Apache, and Sun Java Web Server. Go to **http://www.rsa.com/node.asp?id=2573**.
File Transfer Protocol (FTP) and other UNIX-based products	Authentication Manager protects access to UNIX and LINUX systems when using system entry services such as login, dtlogin, passwd, rlogin, telnet, ftp and su. It also protects OpenSSH through the agent for UNIX or Linux, which implements the Pluggable Authentication Module (PAM) protocol. To download the agent, go to **http://www.rsa.com/node.asp?id=1177**.
CITRIX server	Authentication Manager protects access to applications running on CITRIX. For more information, including implementation guides and solution briefs, go to **http://www.rsa.com/rsasecured/**.
Windows desktops	Authentication Manager protects access to users' local Windows desktops.

There are more than 800 partner applications. For more information go to **http://www.rsa.com/rsasecured/**.

The following figures show a sample network before and after Authentication Manager integration.





RSA Authentication Manager 7.1 Topology

Authentication Manager provides authentication services that allow you to verify the identity of each user attempting to access computer and network resources. An Authentication Manager deployment can consist of 1 or as many as 16 instances (1 primary instance and 15 replica instances), depending on license type. See "License Types and Options" on page 65.

A deployment is the arrangement of Authentication Manager instances into appropriate locations in a network to perform authentication. For examples of deployments, see Appendix B, "Sample Deployment Scenarios."

Each instance includes one server node (the database server) that contains the internal database, and you can add additional server nodes to increase authentication performance. A server node is an installation of Authentication Manager on a single server host. The additional server nodes cannot operate alone because they do not contain the internal database. You must connect the additional server nodes to the database server. Server nodes must be on the same subnet as the database server to which they are connected. For examples of instances and server nodes, see Appendix A, "Terms and Concepts."

In the Authentication Manager model:

- The primary instance is where all administration takes place. It can also service authentication requests like any other network instance.

  The first instance you install is the primary instance for your deployment. All other instances in the deployment are replica instances. For examples of primary and replica instances, see Appendix A, "Terms and Concepts."

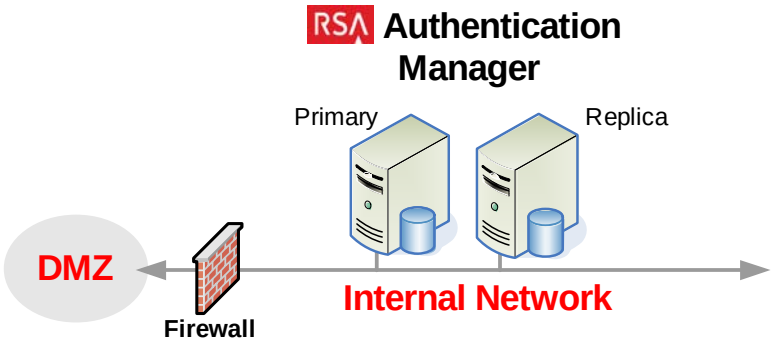
- The replica instance handles authentication activity, depending on the system load and agent load balancing. It also provides failover protection and enables you to recover administration capabilities and Authentication Manager data in the event that the primary instance stops responding.

  A replica instance is a copy of your primary instance. You can view, but not update, administrative data on a replica instance.

A single instance of Authentication Manager can handle administration and authentication of users in a deployment with a small user population. However, RSA recommends that you install at least two instances (one primary instance and one replica instance) for the following reasons:

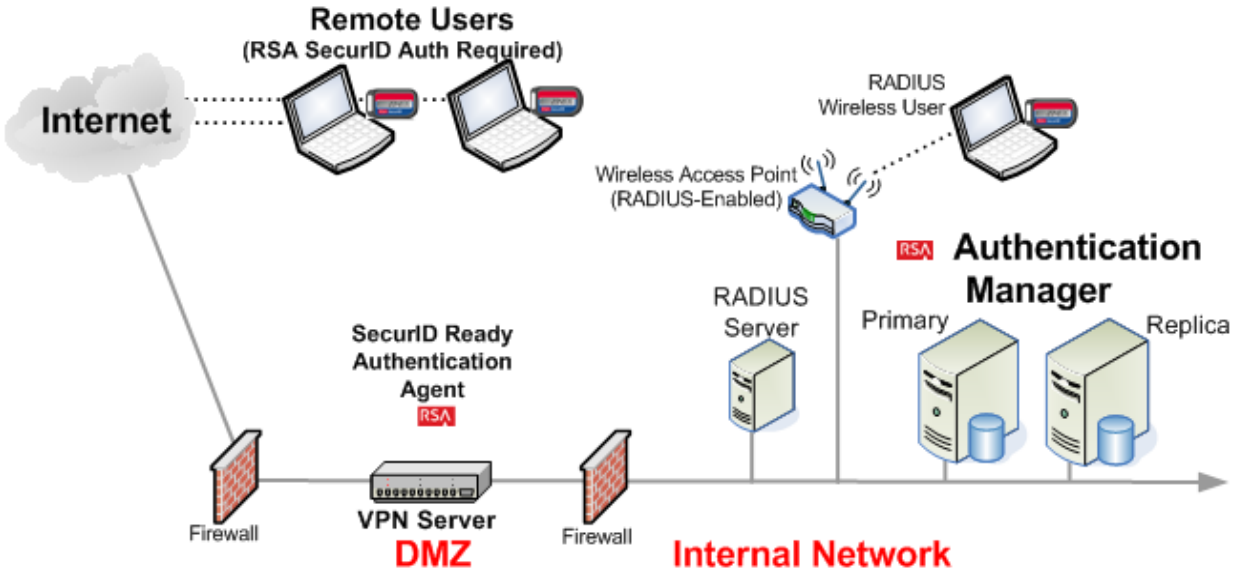
- To provide failover to safeguard data in the internal database
- To provide continuous authentication in the event that an instance stops responding
- To provide a method of recovering administrative capabilities in the event that the primary instance stops responding

The following figure shows the minimum recommended Authentication Manager installation.



In an cluster deployment that has multiple server nodes, only one server node contains the database. This server node is known as the database server. (The database server can be on a separate machine from your primary instances or replica instances.) All server nodes authenticate users. On a primary instance with multiple server nodes, all server nodes provide administrative access to the database through the Security Console.

The following figure shows RSA SecurID components supporting secure and remote wireless access.



Realms

A realm is an independent organizational unit that contains all objects in your deployment. This includes users and user groups, administrative roles, tokens, and policies for passwords, lockout, and tokens.

When you install Authentication Manager, a default realm is automatically created. You can build your entire organizational hierarchy within this one realm, or you can create additional realms. You must have an Enterprise Server license to add realms.

- Each realm has its own set of users, user groups, tokens, authentication agents, and so on.
- You cannot transfer objects, such as users, user groups, or tokens, between realms.
- Agents are active in a single realm. You cannot add an agent to multiple realms.

Users and user groups managed by a realm are stored in identity sources. Such identity sources are either:

- An external Directory Server
- The Authentication Manager internal database

Each realm may be associated with multiple identity sources, but each identity source may only be associated with a single realm.

You can create as many realms as your organization needs. Organizations typically need few realms, and many use the default realm only.

You might choose to add an additional realm if your organization has separate subsidiaries where agents accessed and administrative control is entirely separate. Users, user groups, tokens, and other objects in each realm remain separate.

Administrators can manage only the realm in which their user record is stored. They cannot manage multiple realms. Super Admins are the only exception to this because Super Admins can manage all realms in the deployment.

If your organizational needs require you to move users, user groups, tokens, and other objects between organizational units—departments within your company, for example—create a security domain hierarchy, rather than multiple realms. Multiple security domains allow you more flexibility to reorganize your deployment than multiple realms.

Use the Security Console to create and manage realms. In a deployment with multiple realms, the Super Admin is prompted at logon to select which realm to log on to. To switch between realms, the Super Admin must log off, and then log on to the other realm. All other administrators log on to the realm in which their user record is stored.

Security Domains

Security domains are containers that represent areas of administrative responsibility, typically business units, departments, partners, and so on. Security domains establish ownership and namespaces for objects (users, roles, permissions, and so on) within the system. All Authentication Manager objects are managed by a security domain. Security domains allow you to:

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

When a new realm is created—either automatically when you install Authentication Manager, or by an administrator—a top-level security domain is automatically created in the realm. The top-level security domain is assigned the same name as the realm.

Note: You cannot edit the name of the top-level security domain.

By default, all users are managed in the top-level security domain. You can transfer users from the top-level security domain to other security domains within the realm.

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

Know the following about security domains:

- Security domains are organized in a hierarchy within a realm. Create as many security domains as your organization requires.
- Security domains are often created to mirror the departmental structure or the geographic locations of an organization.

You also use security domains to enforce system policies. Policies control various aspects of a user's interaction with Authentication Manager, such as RSA SecurID PIN lifetime and format, fixed passcode lifetime and format, and password length, format, and frequency of change.

The following policies are assigned to security domains:

- Password policies
- Token policies
- Lockout policies
- Offline authentication policies

You can use the default policy, or create a custom policy, for each policy type, for each security domain. When you create a new security domain, the default policy is automatically assigned. You can optionally assign a custom policy to the new security domain. If you assign the default policy to a security domain, whatever policy designated as the default is automatically assigned to the security domain. When a new policy is designated as the default, the new default is automatically assigned to the security domain.

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

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

Trust Relationships

It is possible that you have more than one deployment of Authentication Manager. For example, your company acquires another company with its own Authentication Manager deployment.

Authentication Manager deployments function independently of one another. Each deployment has separate and different components such as identity sources, realms, and security domains. By default, users in a deployment can only authenticate to resources within that deployment. In some business cases, you might want to allow users to authenticate across deployments and access resources in another realm protected by Authentication Manager. To do this, you can create a trust relationship between the realms in your deployments. For more information, see the chapter “Administering Trusted Realms” in the *Administrator’s Guide*.

Trust relationships are created between two realms in separate deployments. When you create a trusted realm relationship, users in one realm can authenticate through an agent in a second realm (trusted realm) and access the resources protected by that realm’s deployment of Authentication Manager. When the user attempts to authenticate in the trusted realm, the trusted realm forwards the authentication request to the realm that contains the user’s record. The realm with the user’s record processes the authentication request and the user can access the trusted realm’s protected resources.

For example, assume you have an Authentication Manager deployment in London, and a second deployment in New York. You can create a trusted realm relationship between these two realms. When that relationship is established, users in the London realm can access the New York authentication agents. New York is the trusted realm. The New York realm forwards the authentication request, with the appropriate user and agent information, to the London realm, which then authenticates the user. The user can then access New York’s protected resources.

Using the previous example, assume a user “jdoe” travels to New York for business. The user needs to access the company network, so he attempts to access the VPN. In New York, the VPN server is protected by an authentication agent. When jdoe attempts to access the agent using his credentials (user name and passcode), the agent does not immediately recognize the user. Because the agent has been enabled for trusted realm authentication, it looks for the user in other realms. Finding jdoe in the London realm, the New York realm forwards the user credentials and the agent information to the London realm. The London realm verifies the user credentials and tells New York to authenticate the user. The authentication is successful.

Users who can authenticate through realms other than their own are called trusted users. Trusted users are users who can access resources in one realm, but whose identity is managed in a different realm. Only trusted users can authenticate through a trusted realm, so trusted user records are created in the trusted realm upon authentication. Note that a trusted user record is not the same as a user. The trusted user record points to a user. In the example above, the London user jdoe is a trusted user in the New York realm. The New York realm maintains a trusted user record for jdoe.

You can group trusted users into trusted user groups. Similar to user groups, you can use trusted user groups to restrict access to an authentication agent. Only members of the trusted user group can access the agent. In addition, trusted users and trusted user groups can only access authentication agents that have been enabled and configured for trusted realm authentication.

There are three types of trust relationships you can establish with RSA Authentication Manager 7.1:

- One-way between two RSA Authentication Manager 7.1 realms
- Two-way between two RSA Authentication Manager 7.1 realms
- Two-way between an RSA Authentication Manager 5.2 or 6.1 realm and an RSA Authentication Manager 7.1 realm

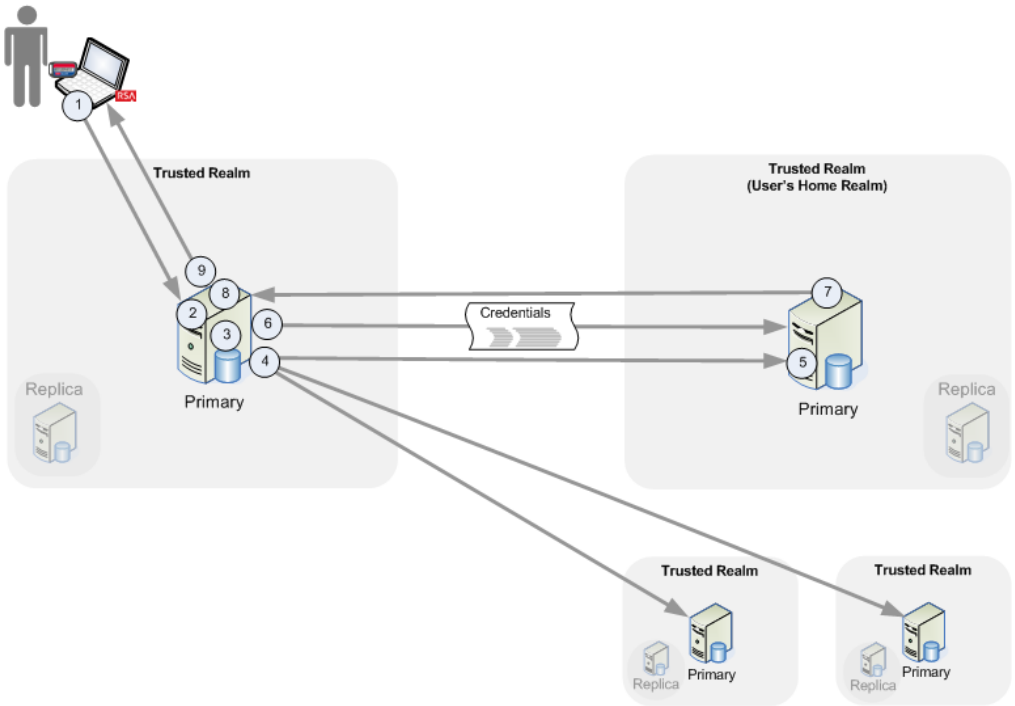
Note: If you have multiple Authentication Manager 7.1 realms on a single machine, you can establish a trust relationship with only one of them from a 5.2 or 6.1 realm.

The following process describes how a trusted user gains access to a realm that has a trust relationship with the realm that stores the user’s record. This example assumes that the agent host is enabled for trusted access and is configured “open” to all trusted users. When the agent is not “open”, you must create the remote user’s record manually.

1. A user attempts authentication to a realm that does not host the user’s record by providing credentials to an agent in that realm.
2. The realm that does not host the user’s record cannot find the user in its database.
3. The server in the realm that does not host the user’s record confirms that its agent is open to trusted users, and that “Enable cross realm authentication” is selected.
4. The server in the realm that does not host the user’s record broadcasts a user discovery message to all trusted realms.

5. The server in the realm that hosts the user's record processes the discovery request and indicates to the realm that does not host the user's record that the user belongs to this realm.
6. The server in the realm that does not host the user's record sends credentials to the server in the realm that hosts the user's record.
7. The server in the realm that hosts the user's record sends the "Access OK" message to the server in the realm that does not host the user's record. The server in the realm that does not host the user's record checks the credentials against its records.
8. The server in the realm that does not host the user's record stores the information about which realm contains the user's record.
9. The "Access OK" message is returned to the agent, and the user gains access to the realm that does not host the user's record.

The following figure illustrates the preceding process.



On subsequent authentication attempts for the same user, steps 3 - 5 and 8 are skipped. The realm that did not host the user's record before the authentication, uses the information it stored in step 8 to determine where to send the credentials in step 6.

Deciding Where to Store User Data

When planning how to store Authentication Manager data for access, you need to decide which data store to use as the location for user and user group data. The data store that stores user and user group data is known as an identity source. An identity source represents the physical source of the data of the users and user groups that you manage through the Security Console. An identity source can be one of the following:

- An external directory, such as Sun Java System Directory Server or Microsoft Active Directory.
- The Authentication Manager internal database.

If your data resides in a heterogeneous, multi-directory server environment, Authentication Manager allows you to specify any or all of the identity sources listed. For example, you can use both a Microsoft Active Directory Server and a Sun Java System Directory Server as identity sources. This functionality accommodates environments that have evolved over time, due to acquisitions, upgrades, or architectural changes. For example, when you first install Authentication Manager, you can specify the internal database as the single identity source, but accommodate a growing user population when an external directory server is introduced into your system.

When choosing whether to use the internal database or the external directory server, consider your current network configuration and needs.

If you have a large population of users and one or more existing external directory servers, you can specify the external directories, or subtrees within them, as identity sources. If you have a small number of users and have not set up an external directory server, you may find that the internal database provided with Authentication Manager meets your needs.

RSA recommends that you give each Authentication Manager user a unique name because duplicate names in identity sources can cause Authentication Manager agents to deny authentication. For example, you have two identity sources and you do not require fully qualified, unique names for log on. One identity source contains bob@divsion1 and the other contains bob@division2. The authentication agent discovers two identities named “bob” and denies authentication. Some other possible solutions include the following:

- Use aliases
- Require logging on with fully qualified names
- Use flat name space

Using the Internal Database as Your Data Store

If your deployment uses the internal database as the only identity source, all data is stored in the internal database and there is no need to specify a directory server as an identity source.

Using a Directory Server as Your Data Store

You can access the user and user group data in the directory server through the Security Console in read-only mode or read/write mode, depending on how you configure permissions on the directory server, and how you configure the identity source when you associate it with Authentication Manager. The decision to enable read/write access to the directory server depends upon the existing policies of your company, the division of responsibilities in your organization, and whether you use the token provisioning feature of Credential Manager. See Chapter 11, "Planning Self-Service and Provisioning," "Establishing a Secure Communications Path" on page 72, and "Implications of Read/Write or Read-Only Access" on page 117.

Know the following about using directory servers:

- You can change the read-only or read/write decision after installation.
- You cannot move users among identity sources.
- You cannot place a user from one identity source into a group from another identity source.

The user and user group data in the directory server is referenced by default when you specify a directory server as an identity source. You can view and, if write-access is enabled, manage additional data residing in your directory server by mapping the additional data in the directory server to extension fields in the internal database that are accessible through the Security Console. See "Attribute Mapping" on page 72.

Different administrators, with different security levels, may manage Authentication Manager and the directory server. If the directory server is the authoritative source for user information, disabling a user through directory server administration affects the ability of the user to authenticate. Consider these things:

- Do you want directory server administrators to have the ability to disable a user's ability to authenticate?
- Do you want Authentication Manager administrators to have the ability to edit directory server data?

Note: Active Directory requires SSL for administering users.

Planning Physical Security

Plan to protect the physical assets in your deployment from unauthorized users and potential damage from the elements.

Equipment

Ensure the physical security of the equipment running Authentication Manager by following any existing corporate guidelines your company has already instituted. RSA recommends locating the equipment in a locked location accessible to a minimum number of trusted personnel.

Connections and Ports

Minimize the number and types of connections that can be made to the Authentication Manager machine. Block access through ports that are not necessary to the functionality of Authentication Manager.

Passwords and Key Material

The Authentication Manager installer 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 a master password for interactive operations. The master password is created during installation. For more information, see the chapter "Preparing for Installation" in the *Installation and Configuration Guide*.

It is imperative that you secure the master password, as it protects all of the system passwords required to run Authentication Manager.

As part of failover and disaster recovery planning, the master password can be exported as part of a backup of all of the system passwords, and exported to an encrypted, password-protected file. When recovering from a disaster, the file can be imported back into the system. RSA strongly recommends storing the exported file in a safe and secure manner.

System Integration Summary

Know the following when planning system integration:

- How your existing network topology is organized.
- Which resources to protect with Authentication Manager.
- What your Authentication Manager license allows.
- Which equipment to acquire with the Authentication Manager agent embedded, if any.
- Which RSA partner applications you need, if any.
- How to organize realms, security domains, and hierarchies.
- How trust relationships between deployments work, if needed.
- Where to store your user data.
- How read-only or read/write settings affect operations on your directory servers, if any.
- How to ensure the physical security of equipment, connections and ports, and passwords and key material.

The Security Division of EMC

5 Planning Optimal System Performance

In a deployment with multiple server nodes, performance and scalability are affected by the hardware on which the database server and server nodes are installed. The database server handles authentication requests from the server nodes, as well as administration connections through the server nodes. The primary instance database server has the additional burden of handling all replication to and from the replica instances.

Database Replication

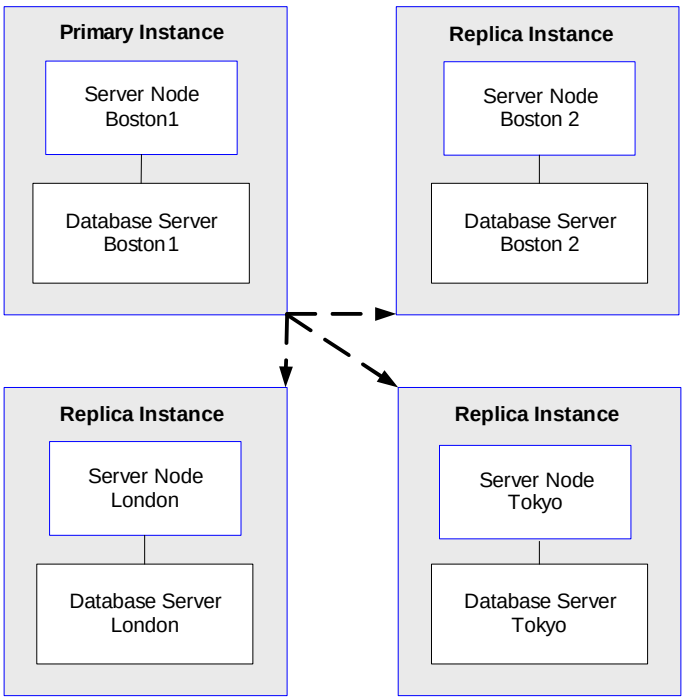
You can install a replica instance of RSA Authentication Manager as a means of minimizing data loss and loss of administration capability in the event of a hardware disaster. Replicated instances allow authentication and administration to continue while the primary instance is offline. Although certain functions may be disabled or performance may decrease, the product's core functions continue to operate.

The following sections describe how the primary and replica instances interact.

Administrative Updates

You must perform all administrative changes, such as adding or deleting users, at the primary instance. The primary instance propagates the administrative changes to all replica instances, as shown in the following figure.

Administrative Updates Data Flow



All changes that occur on a primary instance are replicated to each replica instance in the deployment. All changes that occur on a replica instance are replicated to the primary instance, which then replicates the changes to all other replica instances in the deployment.

Log data on a replica instance is not replicated in the same way as changes resulting from authentication. Log data is sent only to the primary instance, or to a designated centralized log. It is not replicated to all instances in your system.

Important: The user and user group data that resides in your directory server is not replicated by Authentication Manager. In a replicated directory server environment, it is your responsibility to properly configure the directory server to replicate changes.

Runtime Updates

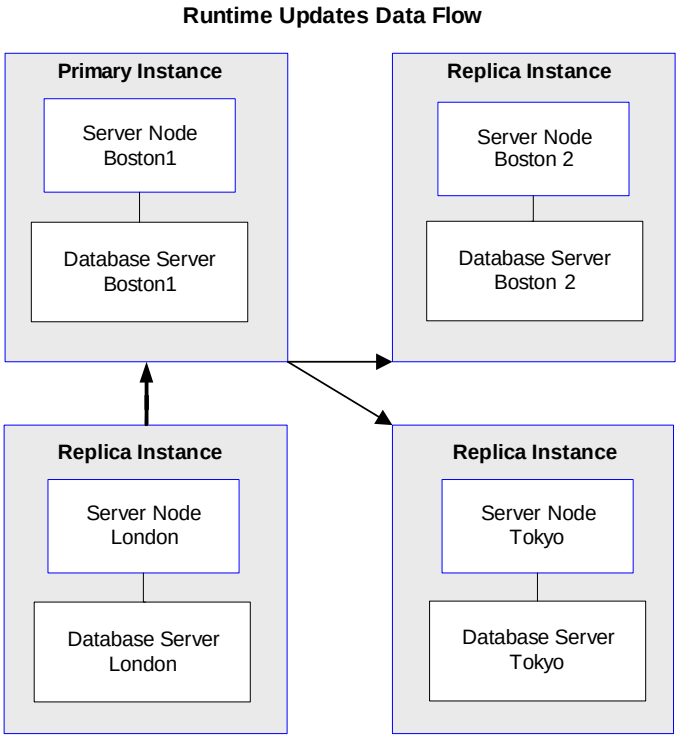
Runtime changes, such as those resulting from user authentication, can be initiated at any primary or replica instance. If the runtime change occurs at a replica instance, the change is first propagated to the primary instance. The primary instance then propagates the change to all other replica instances.

The following table lists the runtime changes that can occur on a replica instance.

Object	Change That Is Replicated
User	• Any change to the user's fixed passcode or PIN. • The user's last logon.
Agent	• The creation of an agent through agent auto-registration. • Assignment of an agent to a contact list. See "Using Contact Lists for Load Balancing" on page 55. • Updating a node secret.
Token	Any changes that occur as a result of the following activities: • Authentication. • Token replacement, including disabling, unassigning and deleting an existing token, and assigning and enabling a replacement token. The exact changes that occur depend upon how you configure Authentication Manager to handle token replacement. For more information, see "Replacing Tokens" in the *Administrator's Guide*. • Emergency passcode processing. • The distribution of offline authentication data to agents. • Seed initialization of software tokens.

The following figure shows:

1. Runtime authentication changes occur at the replica instance in London.
2. London updates the primary instance in Boston.
3. Boston updates the other replicas.



Notes:

- You can see the changes at any instance after the changes have been propagated.
- If a replica instance contains more recent changes than those received from the primary instance, the replica instance can reject the less timely data.
- If Authentication Manager does not load the database after the data has been changed, you see obsolete data at the replica instance. For example, if the primary instance is down.

Planning for Peak Authentication Periods

It is likely during daily operation that your users will log on to the network at specific times, requiring Authentication Manager to authenticate large numbers of users in a relatively short time frame. Such peak authentication times might occur when employees arrive at work and after they return from lunch. If you have multiple geographic sites, peak authentication periods may occur throughout the day. Determine the times each day that the highest rates of authentication occur.

For example, your primary instance is in Boston and you have employees in London. The five-hour time difference means that peak authentication periods may occur during the following Boston time periods:

- 3:00 a.m. - 4:00 a.m. when London employees arrive to work
- 7:00 a.m. - 8:00 a.m. when London employees return from lunch
- 8:00 a.m. - 9:00 a.m. when Boston employees arrive to work
- 1:00 p.m. - 2:00 p.m. when Boston employees return from lunch

The use of a replica instance in London and the contact list feature of Authentication Manager help to alleviate some of the burden of the peak authentication period. RSA recommends that you monitor the CPU performance of Authentication Manager during these peak periods in order to gauge the effect on your system.

Using Contact Lists for Load Balancing

Authentication Manager provides load balancing through contact lists, which contain a list of all the server nodes where the authentication agent can direct authentication requests. After an agent's initial contact, Authentication Manager provides the agent with the contact list.

Important: Do not use any third-party load balancing products. Authentication agents perform their own load balancing and server discovery. The authentication agent protocol is not compatible with third-party UDP load balancing products.

Agents receive notification from Authentication Manager of any changes to the contact list. Periodically, the agent reviews all the server nodes listed in the contact list to determine where to send authentication requests. The agent uses metrics such as response performance to determine where to send requests. Note that agents do not remove servers from contact lists, they only add them to the list.

There are two types of contact lists:

Automatic contact lists. These lists are automatically maintained by Authentication Manager and automatically add new server nodes. An automatic contact list is assigned to each instance in your deployment. The list contains the IP addresses of each server node in the instance the contact list is assigned to, and the IP address of one server node from each other instance in your deployment, up to a limit of 11. Agents are sent automatic contact lists by default.

Note: By default, servers are not removed from the automatic contact list. For a revised list of additions and removals, delete the **sdstatus.12** file.

Manual contact lists. These lists are maintained by administrators. They must be manually updated to reflect the most recent list of server nodes. Manual lists can contain the IP address of any server node in the deployment, up to a limit of 11 server nodes.

For almost all organizations, automatic contact lists are sufficient. However, you may choose to create a manual contact list if you have a specific way that you want to route authentication requests. For instructions on adding manual contact lists, see the Security Console Help topic, "Add a Manual Contact List."

Load Balancing RSA RADIUS Servers

Load balancing is maintained by the RADIUS client devices in that each contains an address table for all RADIUS servers. These RADIUS-enabled devices choose servers from that table and distribute the authentication workload evenly across available servers.

The following optimizations can help speed up authentication for your users:

- If your deployment has multiple geographic locations, consider installing at least one Authentication Manager replica and one RSA RADIUS replica in each geographic location so that authentication traffic need not travel over a wide-area network.
- Make sure there is an appropriate number of RADIUS replica servers to handle peak loads.

System Performance Summary

Know the following when planning system performance:

- Why to gauge the effect of peak authentication periods on your system.
- Where to install replica instances or server nodes to best handle peak authentication periods.
- When to use automatic or manual contact lists.
- Why you should co-locate RSA RADIUS servers with Authentication Manager servers.
- Why you should install Authentication Manager servers in each geographic location, if you have multiple locations.
- How to load balance RSA RADIUS servers by properly configuring the RADIUS server address table in RADIUS client devices.

6 Planning for Failover and Disaster Recovery

Planning for failover and disaster recovery is part of deployment planning because the location of equipment and the administrator's ability to react quickly are important factors in the event of an emergency.

Understanding Why an Instance Might Stop Responding

An instance might stop responding for any of the following reasons:

Power outage. In this case, you know that the instance can be restarted when power is restored. You probably do not need to take further action. When the primary instance is restarted, RSA Authentication Manager synchronizes the databases.

Hardware malfunction. Estimate the level of effort required to replace the hardware component. Take into account the fact that you might have to reinstall Authentication Manager for all server nodes in the instance.

Database corruption. If runtime or console error messages indicate that the database is corrupted, you can assume that all databases in the deployment are also corrupted. You must restore the primary instance database from a previous backup using the Manage Backups utility.

Inoperable database. A database is inoperable if it runs out of disk space, or if its configuration prevents Authentication Manager from accessing it. If the surviving replica instance appears to function normally, you need to promote the replica instance to a primary instance. For more information, see the chapter "Disaster Recovery" in the *Administrator's Guide*.

Network malfunction. When Wide Area Network (WAN) connectivity is lost between a replica instance and a primary instance, the disconnected replica instance can neither send nor receive database updates. Transactions sent to the replica instance quickly queue up, consuming valuable disk space. Consider removing the replica instance from the system. After removal, agents stop routing transactions to the disconnected server node. You can add another replica instance to improve performance.

Understanding What Happens when a Primary Instance, Replica Instance, Server Node, or RADIUS Server Stops Responding

When you plan your deployment, consider the following information about the possible effects of an emergency situation.

Primary Instance Stops Responding

When a primary instance database server stops responding, the following events occur:

- You cannot administer the system.

  You can read administrative data through a replica instance, but you cannot modify this data until a new primary instance is configured (a replica instance is promoted) or the original one is restarted.
- Authentication performance slows down.

  All server nodes that connect to the database that stopped functioning do not process runtime or administrative requests.
- Help Desk Administrators are blocked.
- Users who are permanently locked out cannot be restored.
- The database on the stopped server may be temporarily unavailable.
- Data accumulates at replica instances, waiting to update the primary instance.

  In extreme situations, disk space might fill up.
- All database updates that occurred on any replica instances after the primary instance stopped, and any updates that occurred at the primary instance but were not yet propagated to all replica instances before the stoppage, are lost.

Replica Instance Stops Responding

When a replica instance stops responding, the following events occur:

- Administrative capabilities continue as usual, because they are performed at the primary instance.
- Authentication performance slows down.

  This decline might continue even after the stopped instance is repaired and brought back online, while the database is being synchronized with other instances.
- You lose the copy of the database that resides on the stopped database server.
- Data flowing to this instance is queued in the primary instance database server, potentially filling up disk space. The consumption of disk space depends on how many transactions the replica handles per hour or day. After you restart the replica instance, the queued data updates it.

Server Node Stops Responding

When a server node that does not host a database server stops responding, the instance where the server node resides continues to function with the following consequences:

- Authentication throughput performance declines for the entire instance, especially during peak authentication periods.
- Uncommitted, partial transactions being processed at the time of stoppage are lost.

RADIUS Server Stops Responding

When a RADIUS server stops responding, the following events occur:

- You may lose changes that occurred since the most recent replication, depending on the frequency of replication.
- You may lose customized configuration files, initialization files, and dictionary files.

Planning Recovery from the Loss of a Primary Instance, Replica Instance, Server Node, or RADIUS Server

When you plan your deployment, consider the following guidelines for recovering from an emergency. For more information, see the chapter “Disaster Recovery” in the *Administrator’s Guide*.

Primary Instance Recovery

Follow these guidelines to ensure quick recovery if the primary instance stops responding.

- Locate a replica instance at the same geographic site as the primary instance. The same personnel who administer the primary instance need access to this local replica instance in case of emergency. Access is through the Operations Console.
- Train your staff to learn recovery procedures and make sure they have the necessary privileges to promote a replica instance if the primary instance stops responding. If your staff is familiar with these steps before a real emergency occurs, they can anticipate what needs to be done and act quickly.
- Confirm that a surviving replica has enough disk space to handle transactions that will queue while the primary is unavailable.
- If you are deploying software tokens using remote token key generation, unused token key generation URLs and service addresses that you have distributed to users become invalid when a primary instance stops responding. If your proxy server supports failover mode, you can configure it to pass CT-KIP data to the new primary instance. This allows users to use the original token key generation URLs and service addresses and saves administrators from the task of sending new URLs to users.

Replica Instance Recovery

If a stopped replica instance cannot be recovered, remove it from the system and install a new replica instance as soon as possible to ensure failover and scalability. For more information, see the chapter "Installing a Replica Instance" in the *Installation and Configuration Guide.*

Important: RSA Authentication Agents route authentication requests to specific replica instances based on information defined in an automatic contact list, manual contact list, or the **sdconf.rec** file. For more information on contact lists and the **sdconf.rec** file, see "Creating and Installing the RSA Authentication Manager Configuration File" and "Specifying Where Agents Send Authentication Requests" in the *Administrator's Guide*.

Server Node Recovery

If a server node is down for an extended period of time, consider removing the server node from the deployment and replacing it.

RADIUS Server Recovery

In the event an RSA RADIUS server stops responding, or is taken offline for some reason, you can replace that server by promoting a RADIUS replica server to a RADIUS primary server.

If the server is a replica server, you can install another server and force replication to that new server. Any configuration changes made since the most recent replication must be manually restored on the new server. Any customizations to initialization files, configuration files or dictionary files must also be manually restored.

If the server is a primary server, you must first promote a replica to become the primary server. Then you can install another server as a replica server and force replication to that new server. Any configuration changes made since the most recent replication must be manually restored on the new server. Any customizations to initialization files, configuration files or dictionary files must also be manually restored. Plan for this possibility by configuring more than one replica server. For more information, see the chapter "Managing RSA RADIUS" in the *Administrator's Guide*.

Planning Regular Database Backups

Different organizations have different needs and requirements, but RSA recommends frequent backups to minimize data loss. Decide how often you need to create backups and where to store backup data. Consider these issues:

- How critical is the data?
- What regulations does your industry require you to follow?
- How much data can you afford to lose in the event of an emergency?

- Run backups during off-peak periods because the backup operation can affect general system performance. (The database can still service requests while you perform the backup.)
- An Authentication Manager backup does not include RADIUS, which must be backed up separately.
- Plan to store one backup copy at an off-site location.

Note: You can automate database backups by writing a script that calls the Manage Backups utility. Make sure the script sends the data either to a disk that is separate from the actual database, or to tape. These measures prevent a single point of failure for the database and backup. For more information, see the chapter "Disaster Recovery" in the *Administrator's Guide.*

Failover and Disaster Recovery Summary

Know the following when planning failover and disaster recovery:

- How to identify common disaster situations.
- How to monitor the status of each instance and detect any stoppages.
- What happens when a primary instance, replica instance, server node, or RADIUS server stops responding.
- How replication works so you can make appropriate decisions if an instance stops responding.
- How to recover a primary instance, replica instance, or server node that stopped responding.
- How to promote a replica instance to a primary instance.
- How to use the Manage Backups utility to back up the primary instance database. server.
- What is included in an Authentication Manager backup and what is not included (RADIUS).
- How to write a script to automate backups.
- What disaster recovery training your staff needs.

7 Planning for Installation and Upgrading

Installation Personnel

Primary instances, replica instances, and server nodes are core components of RSA Authentication Manager. They contain sensitive data and administrative information. RSA recommends that only your most trusted personnel perform your Authentication Manager installations.

The installation process often requires coordination among the people who have permissions to access and administer the various components in your network. For example, an administrator in your home office may need to work with an administrator in a remote office to open ports for Authentication Manager. Use the following table to help you coordinate access to the components of your network for installation.

Component	Component Administrator	Administrator Who Needs Access
Operating system		
Firewall portals		
Virtual Private Network (VPN) server		
Wireless router		
Protected resources		
Desktop machines		
Primary instance, replica instances, and server nodes		
Web server		
Proxy server		

Component	Component Administrator	Administrator Who Needs Access
Authentication agents		
Outlook Web Access (OWA) server		
Citrix Presentation server		
Internet Authentication Server (IAS)		
Remote Authentication Dial-In User Service (RADIUS)		
Domain controllers		
Server protected by Pluggable Authentication Module (PAM)		
RSA Authentication Manager internal database		
Active Directory identity source		
Sun Java System Directory Server identity source		

Installation Considerations

Develop a plan for the physical location and installation of primary instances, replica instances, server nodes, and RADIUS servers.

Consider the following factors in your installation plan:

- Machine Requirements
- License Types and Options
- Necessary Level of Security
- Timetable for Installation
- Access Through Firewalls

Machine Requirements

There are minimum requirements for the machines used for Authentication Manager. Consider whether the minimum requirements are sufficient for your authentication and administrative activity. If not, you may need to include more powerful machines in your plan. For more information on system requirements, see Chapter 2, "System Requirements." All machines in your deployment must run the same operating system.

License Types and Options

Each Authentication Manager installation has one or more software licenses associated with it. The license represents permission to use the Authentication Manager software. Your installation personnel need to understand how the license type impacts the installation of Authentication Manager. Review these license types and options with your installers:

Base Server. Allows up to two instances of Authentication Manager.

Enterprise Server. Allows up to 15 instances of Authentication Manager.

Each license type has a limit on the number of instances of Authentication Manager that can be installed and whether or not multiple realms are allowed. User limits are determined on an individual basis, based on the customer's usage requirements.

For example, a customer with 10,000 employees may purchase a license for 11,000 users to accommodate current employees and to allow for future hiring.

The following table shows the attributes for each license type..

License Feature	Base Server	Enterprise Server
Number of users	Specified by customer at time of purchase	Specified by customer at time of purchase
Number of instances	2[1]	15
Allows multiple realms?	No	Yes
Allows clusters?	No	Yes
RSA Credential Manager self-service	Yes	Yes
RSA Credential Manager provisioning	No	Yes
On-demand tokencode service	Optional	Optional
RADIUS	Yes	Yes
Business Continuity	Optional	Optional
Allows offline authentication?	Yes	Yes

[1]Licenses with a two instance limit allow a third instance for disaster recovery situations.

Necessary Level of Security

Plan the level of security you require for assets and users. You might require different levels of authentication from some users than from others. For example, you may require laptop users to authenticate for access to their computers. This prevents unauthorized use of the laptop. You may not require on-site users to authenticate to their desktop machines.

Consider the following factors:

- The degree of authentication required for each asset that you want to protect
- The degree of authentication required for each type of user
- The number of security domains you require
- Which assets to place in which security domains

Timetable for Installation

To perform the installation with minimal disruption to your employees and customers, develop a timetable and consider the following:

- The number of replica instances and server nodes to install
- The total amount of time that it will take for the installation
- Your system's peak and off-peak usage times
- Your business hours
- The possible effect on your offices in other time zones
- The hours specified in your support plan when RSA support is available

Access Through Firewalls

Plan which ports to open for Authentication Manager communications.

RSA recommends that you install all Authentication Manager servers behind a firewall. To enable authentication through firewalls and accommodate Network Address Translation (NAT), the RSA Security Console allows you to configure alias IP addresses for your Authentication Manager instances and alternate IP addresses for your authentication agents. You can assign four distinct IP addresses (the original IP address and up to three aliases) to each Authentication Manager instance. You can assign an unlimited number of alternate IP addresses (one primary IP address) to your agents.

Your installers need to know the agent's primary and alternate IP addresses and the Authentication Manager primary IP address and aliases for each instance. If your deployment includes multiple locations, your installers also need to know the ports used for Authentication Manager communications and processes (such as replication). You may need to open some new ports in your firewall, or clear some existing ports for your deployment. For more information on ports, see "Port Usage" on page 22.

Installation Types

RSA recommends you install one primary instance and at least one replica instance. Depending on your business needs, you may also install additional server nodes, a standalone Authentication Manager database, or RSA RADIUS.

At installation time, you must select an installation type. The installer creates differently configured combinations of Authentication Manager components on your system depending on which type of installation you choose.

The following sections describe the installation types.

Primary Instance

Select a machine for your primary instance. There is only one primary instance per deployment. (All other instances are replicas.) You must install the primary instance before you can install replica instances or server nodes because certain information is required from the primary instance. For more information, see the chapter "Installing an RSA Authentication Manager Primary Instance" in the *Installation and Configuration Guide.*

The machine on which the primary instance is installed must meet minimum requirements. For more information on system requirements, see Chapter 2, "System Requirements." If your deployment requires higher specifications, plan to acquire and prepare a machine accordingly.

Note: Your consolidated log file is located on your primary instance. Administrators who have permission to read the log file will need access to this machine.

Replica Instance

Plan the number, requirements, and locations of your replica instances. Plan where to locate them to provide for failover, disaster recovery, and local authentication for geographically dispersed offices.

If you have the Base Server license, you can install one replica instance. If you have the Enterprise Server license, you can install up to 15 replica instances.

Note: At a minimum, you must have an Enterprise Server license to install more than one replica instance.

Adding a replica to your system means that you need to plan for additional hardware because the replica instance must be installed on a machine other than the primary instance. RSA recommends that you install at least one replica instance for failover and disaster recovery.

The machine on which the replica instance is installed must meet minimum requirements. For more information on system requirements, see Chapter 2, "System Requirements." If your deployment requires higher specifications, plan to acquire and prepare a machine accordingly.

Server Node

To further enhance authentication performance, you can add up to four server nodes per instance. Consider whether you need to add server nodes to some, or all, authenticating servers to increase authentication performance.

Note: At minimum, you must have the Enterprise Server license to add server nodes.

Server nodes must be installed on the same platform as the primary instance or replica instance. For example, if the primary instance is installed on Linux, your server nodes must be installed on Linux. The host for the server node must be in the same subnet as its primary instance or replica instance database server.

You must first install your primary instance and any replica instances to which you want to add a server node. You will need this data when you install the server node. For more information, see "Installing a Server Node" in the *Installation and Configuration Guide*.

RADIUS Only

RSA RADIUS can reside on a primary instance, a replica instance, or on a separate machine. The installation program provides several alternatives:

- You can install RADIUS on a 32-bit Authentication Manager primary instance or replica instances at the same time you install Authentication Manager.

  You cannot install RADIUS on a 64-bit Authentication Manager server.
- You can install RADIUS primary instances or replica instances on machines separate from Authentication Manager after you have installed Authentication Manager. You must install Authentication Manager before installing RADIUS because you must provide certain information from Authentication Manager during the RADIUS installation procedure.
- Organizations may have a mixed configuration wherein RSA RADIUS is installed on the Authentication Manager primary and replica instances and some additional RADIUS replicas are installed on separate machines. Your performance requirements can determine the best configuration for your organization.

For more information about RADUIS, see Chapter 12, "Planning for RSA RADIUS Integration."

Standalone RSA Authentication Manager Database

You have the option to install the Authentication Manager database for either a primary instance or replica instance on a separate machine. For more information, see "Preparing to Install the Database on a Separate Machine" in the *Installation and Configuration Guide.*

If you want to install the Authentication Manager database on a standalone machine, plan to perform this installation before installing the primary instance. Certain information is required from the standalone database before you can install the primary instance.

Documentation

The installer provides an option to install only Authentication Manager documentation.

Upgrading from RSA Authentication Manager 7.0

For more information, see the chapter "Upgrading from RSA Authentication Manager 7.0" in the *Installation and Configuration Guide*.

Note: If you are upgrading from RSA Authentication Manager 6.1 to version 7.1, see the *Migration Guide*.

Planning LDAP Directory Server Integration

If your deployment includes using an external LDAP directory server and you want to use it as an identity source for Authentication Manager, plan to integrate it with Authentication Manager. For more information, see the chapter "Integrating an LDAP Directory" in the *Installation and Configuration Guide*.

The relationship of the Authentication Manager internal database to an external one is that users, user groups, and custom attribute data are stored in the external identity source. All other data, including agent and token data, is stored in the internal database.

Authentication Manager enables you to integrate LDAP identity sources without modifying the LDAP schema. Administrators use the RSA Security Console to create the identity source record and map Authentication Manager attributes to the LDAP attributes.

All information that is specific to Authentication Manager, such as Authentication Manager security policies and user-token associations, resides only in the internal database. Linkages between Authentication Manager information and LDAP user records are also maintained in the internal database.

Consider the following factors before you integrate your external identity source with Authentication Manager:

- Supported external identity sources
- Selecting read-only or read/write
- Handling security considerations
- Performing the integration
- Mapping custom attributes
- Physical co-location of replicated LDAP directory instances with Authentication Manager instances

Specifying Read-Only or Read/Write

Authentication Manager supports either read-only or read/write operations on directory servers. You must select either read-only or read/write when you integrate Authentication Manager with your identity source.

Read-Only

- You cannot make changes to the data in your directory server through the Security Console.
- You must make changes to the data in your directory server through the directory server's native user interface.

Read/Write

- You can manage users and make changes to the data in your directory server through the Security Console and your directory server's native user interface.
- You must use SSL for write functionality.

If you are using either self-service or provisioning, there are further implications of read-only or read/write. For more information, see Chapter 11, "Planning Self-Service and Provisioning."

Microsoft Active Directory

RSA recommends that you seek people who are extremely knowledgeable about Active Directory, your network topology, and your business requirements for using Authentication Manager to plan your Active Directory integration.

Plan to configure an identity source for each domain in the forest that contains users who are required to authenticate with RSA SecurID. Optionally, you may use the Global Catalog feature of Active Directory by configuring an identity source that maps to the Global Catalog. In such configurations, Authentication Manager can access the Global Catalog and perform faster user searches at runtime.

In Authentication Manager terminology, using the Active Directory Global Catalog entails configuring two types of identity sources:

Runtime identity source. An identity source configured for runtime operations only, to find and authenticate users, and to resolve group membership within the forest. You can map a domain controller or Global Catalog as a runtime identity source.

Administrative identity source. An identity source used for administrative operations such as adding users and user groups. This identity source maps to a domain controller.

If you choose not to configure Authentication Manager to use the Global Catalog, you save the effort required to configure the identity source for the Global Catalog at the expense of runtime performance. In this scenario, when authenticating a user, Authentication Manager searches each Active Directory domain to find the user.

When the Global Catalog is not used, only one type of identity source is configured for each domain in the Active Directory forest. In other words, Authentication Manager uses the administrative identity source for both administrative and runtime operations.

When integrating Authentication Manager with Active Directory, you have the option to establish a Secure Sockets Layer (SSL) connection. To establish an SSL connection to Authentication Manager, import the required Active Directory server's certificate. Do this for each Active Directory server to which you want an SSL connection.

Active Directory has a default password policy that is stricter than the Authentication Manager policy. This can cause errors when adding and updating users. To prevent this, you must either relax the Active Directory requirements or make the Authentication Manager requirements stricter. The directory server must have read/write access to change password requirements through Authentication Manager.

Global Catalogs

You can use Global Catalogs with Authentication Manager as runtime identity sources, but there is no requirement to do so.

If you want to use the Global Catalogs to increase performance, you can add them as runtime identity sources. The runtime identity source is used to find and authenticate users and to resolve group membership within the forest. Authentication Manager does not use Global Catalogs for administrative operations. Administrative actions (for example, adding users) are performed against the administrative identity sources only.

If you want to use the Global Catalog, map a runtime identity source to the domain controller which hosts the Global Catalog. Each identity source can be mapped to up to two directory servers, one for production and one for failover. Your runtime identity source can be mapped to two Global Catalogs on two domain controllers in your Active Directory forests.

If you want to use the Global Catalog, and your deployment uses restricted authentication agents and user groups, you must meet the following requirements:

- Active Directory groups given access to restricted Authentication Manager agents must be Windows universal groups.
- Your Active Directory domains must be configured to operate at the Windows 2003 functional level.
- Only the Windows administrator can change the group type in Active Directory.

  If the Active Directory is read/write in Authentication Manager, you can use the Security Console to change the group type.

For more information see the appendix "Integrating Active Directory Forests" in the *Administrator's Guide*.

Sun Java System Directory Server

When integrating Authentication Manager with Sun Java System Directory Server, you have the option to communicate over a Secure Sockets Layer (SSL).

If you want to communicate over SSL, plan to import a certificate of authority from Authentication Manager and enable it on your Sun Java System Directory Server. Plan to do this on each Sun Java System Directory Server for which you want an SSL connection to Authentication Manager.

Consider what information and personnel you need to integrate Sun Java System Directory Server. Plan how you want to configure user groups and users. The following process applies to each Sun Java System Directory Server that you integrate.

1. Add the Sun Java System Directory Server to Authentication Manager.
2. Select directory settings.
3. Map attributes.

Establishing a Secure Communications Path

RSA recommends that you encrypt data in transit between Authentication Manager and your identity source. Authentication Manager connects to the LDAP directory server by way of a Secure Sockets Layer (SSL). This protects the data in transit. An SSL certificate is required for Active Directory. It is optional for Sun Java System Directory Server.

To establish SSL, you import a certificate from your directory server and register it in Authentication Manager. Plan to do this with each LDAP directory server for which you want an SSL connection to Authentication Manager.

For Active Directory there are additional important considerations for password policies and group membership support. For more information, see "Overview of LDAP Directory Integration" in the *Installation and Configuration Guide*.

Directory Server Integration Process

RSA recommends that you select a technician with a background in LDAP and knowledge of your directory server deployment to perform your integration. Some of the tasks require using the Operations Console, and others are performed through the Security Console.

Depending on your configuration and directory server type, there may also be important tasks to prepare the directory for integration. For more information, see "Overview of LDAP Directory Integration" in the *Installation and Configuration Guide*.

The integration process is as follows:

- Prepare for integration
- Add the identity source through the Operations Console
- Link the identity source to a realm
- Verify the identity source
- Optional. Map custom fields to your identity source

Attribute Mapping

All required external attributes are mapped when you create your identity sources. If you plan to map any additional attributes in your directory server to Authentication Manager, do this through the Security Console. For more information, see "Mapping Attributes to Active Directory" in the *Administrator's Guide*.

Conducting a Pilot Test

RSA recommends that you conduct a pilot test of Authentication Manager to test:

- Devices in the network
- System connections
- Disaster recovery
- Administrative tasks
- Reports

Consider the following when you plan your pilot test:

- The scope of the test
- How much hardware you will need
- How much disk space is required
- Your time frame for staging and performing the test
- The types of disaster recovery to test
- The number and types of authentication to test

Note: You may need to change the IP address and hostname when you move a machine from the test environment into the production environment.

Installation and Upgrading Summary

Know the following when planning your installation or upgrade:

- What system requirements you need to meet.
- What your license specifies.
- How to coordinate administrators to provide the required access during installation.
- What level of security you require for your users and your resources.
- Your timetable for installation.
- Which ports must be open and available for Authentication Manager.
- Which installation types to perform, and at which locations.
- How to integrate directory servers, if any.
- How to conduct a pilot test.
- Which version of Authentication Manager you plan to upgrade.
- Which upgrade type you require.
- Which administrators of instances in other geographic locations need to know your upgrading plan.

8 Planning for Administration

RSA Authentication Manager Administration

In RSA Authentication Manager, administration and authentication activities result in changes to the internal database. Administrative changes can be performed only on the the primary instance, which replicates these changes to all of the replica instances in the deployment. Authentication changes can occur on both the primary and replica instances. Each replica instance replicates its authentication changes to the primary instance, which then replicates those changes to all other replica instances in the deployment.

For example, an administrator assigns a token to a user. The database on the primary instance now contains new information about the user and the token, resulting from the administrative action of assigning the token to the user. The primary instance replicates this new information to the replica instances. When the user attempts to authenticate to a replica instance, the replica instance changes the user record to indicate that the user authenticated, and sends that new information to the primary instance. The primary instance then replicates the change to the other replicas.

Microsoft Management Console (MMC) Administration

The information in this section applies only to Authentication Manager customers who use Active Directory for their identity source. The Authentication Manager MMC snap-in is an option that enables you to use the Microsoft Management Console (MMC) to perform many of your token-related tasks in Active Directory. This eliminates the need for Active Directory administrators to log on to the RSA Security Console whenever they need to enable or disable a token, assign a token, and so on. It also enables you to delegate limited responsibility to specific administrators for token-related tasks.

The MMC snap-in enables administrators to perform the following tasks:

- Assign and unassign tokens to users
- Enable, disable, and edit users' tokens
- Edit user authentication attributes
- Edit token properties
- Manage PINs
- Replace tokens
- Generate and download seed files
- Provide emergency access

The pages in the Authentication Manager MMC snap-in are designed to match the corresponding pages in the RSA Security Console. This provides consistency for administrators who want to use both tools for token-related tasks.

If you have Active Directory and plan to install the Authentication Manager snap-in, plan to deploy the MMC snap-in on the machines where the Active Directory administrator has permission to perform Active Directory administration tasks. There are two possible deployment scenarios:

- Install the MMC snap-in on the machine that serves as the domain controller.
- Install the MMC snap-in on the Active Directory user's machine to manage Active Directory remotely.

Note: Remote administration mode is not available on Windows x64. From a Windows x64 machine, use Remote Desktop or the Windows Management Instrumentation Command-line (WMIC) to access the domain controller where MMC is installed.

RSA RADIUS Administration

Routine RSA RADIUS administration takes place through the Security Console. When you edit RADIUS settings, the Security Console makes the changes on the RADIUS server. You must replicate the RADIUS database to the RADIUS replica servers. You can force the RADIUS primary server to replicate the RADIUS database to one or all RADIUS replica servers. For example, if you just promoted a replica to a primary server, and you need to replicate this change to all RADIUS replica servers.

To manage machine-specific parameters, a Super Admin must use the Operations Console. Machine-specific operations include modifying configuration files, initialization files, and dictionary files; setting or changing the IP address; stopping and starting the RADIUS server; and promoting a RADIUS replica server to a primary server.

Authentication Manager provides a default RADIUS Administrator role that allows access to functions in the Security Console.

Only a Super Admin can access the Operations Console after providing the Super Admin password for the user account under which the RADIUS server is running.

Planning Administrative Roles, Permissions, and Scope

Administrators manage all aspects of your Authentication Manager deployment, such as users, tokens, and security domains. The Authentication Manager administrative model is built on the concepts of roles, permissions, and scope. When you assign an administrative role to a user, the user becomes an administrator and can log on to the Security Console, Operations Console, and optional Microsoft Management Console to administer Authentication Manager.

Authentication Manager includes a set of predefined administrative roles and it enables you to create custom roles. You can create as many types of administrators, and as many of each type, as your deployment requires. See "Adding Administrators" on page 80.

These three elements define administrators.

Element	Description
Role	Governs which aspects of the system an administrator can manage. For example, user accounts. A role is a collection of one scope and one or more permissions.
Permission	Governs the actions an administrator can perform. For example, assign tokens to users.
Scope	Governs the boundaries of an administrator's authority. Scope is limited by the security domain and the identity source.

Administrative Roles

You can assign administrative roles to any user in your identity source. When you do so, you give the user permission to perform the administrative actions specified by the role within the specified scope. You may assign more than one administrative role to an administrator.

When assigning roles to administrators, be sure to assign roles that grant only enough permission to accomplish their tasks. Avoid granting administrative roles that are overly broad.

For example, Help Desk Administrators need sufficient security permissions to view and change certain user, user group, token, and user account data. Depending on your deployment, they might need access to multiple security domains. Plan to configure the Help Desk Administrator role with enough permission to perform the job, but not so much as to permit access to other areas or data not vital to their responsibilities.

Authentication Manager provides a set of predefined roles that you can assign to users, allowing them to manage specific aspects of your deployment. You can assign these predefined roles in their default form, or you can modify them by editing the permissions assigned to the roles.

For example, you do not want Help Desk Administrators to be able to view authentication agents. Edit that role through the Security Console and remove that permission.

An administrative role has two components:

- A collection of permissions based on a job function profile. See the following section "Permissions."
- The scope in which the permissions apply. See "Scope" on page 79.

Remember that an administrator can have two roles that have some, or all of the same permissions, but with a different scope.

Permissions

The permissions you assign to an administrative role govern the actions that may be taken by an administrator assigned to the role. Be sure to assign enough permissions so that administrators can manage all the objects, such as users, user groups, and attributes, necessary to accomplish their assigned tasks, but not so many as to let them manage objects not vital to their responsibilities.

For example, an administrator's only task is assigning tokens to users. You assign the following permissions to the role:

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

The optional permissions in the previous example give the administrative role slightly expanded capabilities that complement the stated task of assigning tokens to users. Notice that this role does not include permission to add and delete users, resynchronize tokens, or manage emergency offline authentication. These permissions are not related to the stated task of assigning tokens to users.

When you assign permissions to a role, keep in mind that an administrator in that role might need to associate two objects in the deployment. The administrator must have the appropriate permissions and scope for both objects at both ends of the association. For example:

- To assign tokens to users, an administrator must be able to view tokens, assign tokens, and view users.
- To move users between security domains, an administrator must be able to view security domains and users.
- To assign administrative roles to users, an administrator must be able to view roles, assign roles, and view users.

Scope

The scope of an administrative role controls where an administrator may perform specified administrative tasks. Scope consists of two parts:

- The portion of the security domain hierarchy that the administrative role can manage
- The identity sources the administrative role can manage

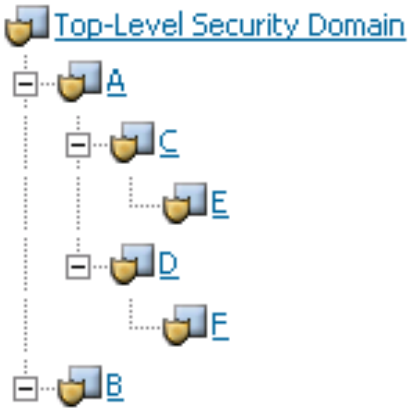
Be sure to assign a scope broad enough so that the administrator can access all the necessary security domains and identity sources. Avoid assigning a scope so unnecessarily broad as to grant access to security domains and identity sources where the administrator has no responsibilities.

For example, a Help Desk Administrator can edit the user record of any other administrator within his scope. This means that a Help Desk Administrator can change the password of a higher-level administrator and gain the administrative privileges of the higher-level administrator. To avoid such situations, assign the higher-level administrator to a security domain that is not within the scope of the Help Desk Administrator.

When you plan the scope of your administrative roles, consider:

- An administrative role manages only within the security domain where the role definition was saved. This includes all of the lower-level security domains in the same security domain.
- You can limit the scope of an administrative role for those security domains that are at or below the level of the security domain that owns the role. An administrative role can only manage down the security domain hierarchy, never up.
- An administrative role that manages a top-level security domain always manages the lower-level security domains beneath it.

For example, consider the following hierarchy:



- You can scope an administrative role saved in the top-level security domain to manage any one or more security domains in the realm. For example, it can manage only security domain F or every security domain in the realm.
- An administrative role saved in security domain A can be defined to manage security domains: A, C, and E, or A, D, and F.
- An administrative role saved in security domain C manages security domains C and E or E only.
- An administrative role saved in security domain E can be defined to manage only security domain E.
- An administrator whose own LDAP record resides in security domain E can manage users in security domain A, C, D, and F if the administrator's role was saved at or above security domain A and includes C, D, and F.

Adding Administrators

Authentication Manager allows you to create different types of administrators with different privileges and areas of administrative responsibility. You can create as many administrators, and types of administrators, as your organization needs.

For example, you divide your organizational hierarchy into three security domains called HR, R&D, and Finance. You create the following custom administrators.

Custom Administrator	Privileges
Token and User Administrators	Performs all token-related duties—for example, assigning tokens or resetting PINs—and can administer users and tokens in all security domains. In a multisite organization, it is likely that there would be Token and User Administrators at each site, whose area of responsibility is limited to the security domain for their respective site.
General Report Administrator	Runs all reports in all security domains except the Finance security domain.
Finance Report Administrator	Runs and views reports in the Finance security domain only. Because of the sensitive nature of the Finance department's duties, only this custom administrator can run Authentication Manager reports on activity in the Finance security domain.

Adding an administrator is a two-step process. You must:

- Create an administrative role. For more information, see "Creating Administrative Roles" in the *Administrator's Guide*.
- Assign the administrative role to a user. For more information, see "Assigning Administrative Roles" in the *Administrator's Guide*.

Predefined Administrative Roles

Authentication Manager provides you with a set of predefined roles that you can assign to users, allowing them to manage specific aspects of your deployment. You can assign predefined roles in their default form, or you can edit the permissions assigned to the roles through the Security Console. The following sections describe the default administrative roles.

Super Admin

This role is created when you install Authentication Manager, and it grants complete administrative responsibility for Authentication Manager. The Super Admin role is the only role with full administrative permission in all realms and security domains in your deployment. You can use it to create other administrators and to create your realm and security domain hierarchy.

You can assign the Super Admin role to as many administrators as you want, but RSA recommends you only assign it to the most trusted administrators because the Super Admin role has a broad scope and a wide array of permissions. You assign the Super Admin role in the same way that you assign all other administrative roles.

RSA recommends that you assign the Super Admin role to at least two administrators. This ensures that you still have someone with full administrative control in situations where a Super Admin leaves for vacation or some other extended absence.

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

No one can modify the Super Admin role, including the administrators assigned the Super Admin role. It is possible, though not recommended by RSA, to delete the Super Admin role. If you accidentally delete this role, you can restore it.

The Super Admin can delegate some of the responsibilities of this role.

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.

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

- All realm permissions
- Replica instances
- Disaster recovery
- Agent deployment
- Identity sources
- Import tokens
- Lower-level security domains
- User groups
- User assignments
- User attribute categories and specific user attributes
- Users that match a condition
- Trusted users and user groups
- RADIUS servers, clients, user and agent profiles, and realm settings
- Self-service troubleshooting policies
- Configuration of security questions
- Reports
- Log maintenance

Security Domain Administrator

This role grants complete administrative responsibility to manage all aspects of a branch of the security domain tree. This administrator has all permissions within that branch except to manage top-level objects such as policies and attribute definitions. By default, this role's scope includes the entire realm. If you want to limit this role's scope to a lower-level security domain in the realm, edit this role, or duplicate this role and then edit the scope of the duplicate role. This role has the same permissions as the Realm Administrators and Super Admins, but is limited to the security domain in which it is created. The Security Domain Administrator can delegate some of the responsibilities of this role.

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

- Security domains
- Administrative roles
- Permissions
- User groups
- Trusted users and user groups
- User attribute categories and specific user attributes
- Users that match a condition
- Identity sources
- RADIUS servers, clients, user and agent profiles, and realm settings
- Reports
- Tokens
- User accounts
- Agents and server nodes

User Administrator

This role grants administrative responsibility to manage users, assign tokens to users, and access selected authentication agents. This administrator cannot delegate any of the responsibilities of this role.

The default permissions for this role limit management to the following.

Users	Add, delete, edit, view
User groups	View user group, assign user group membership
Reports	Add, delete, edit, view, run, schedule

Tokens	View token, reset SecurID PINs, enable and disable SecurID tokens, resynchronize tokens, assign tokens to users, replace tokens, issue software tokens, manage online and offline emergency access tokencodes
User accounts	Manage fixed passcode, manage logon aliases, edit default shell, manage incorrect passcode count, clear cached Windows credential, manage offline emergency access passcode
Agents	View, grant user groups access to restricted authentication agents

Token Administrator

This administrative role grants complete administrative responsibility to import and manage tokens, and to assign tokens to users. This administrator cannot delegate any of the responsibilities of this role.

The default permissions for this role limit management to the following.

Users	View
Reports	Add, delete, edit, view report definition, run, schedule
Tokens	Import, delete, edit, view token, reset SecurID PINS, resynchronize tokens, manage online and offline emergency access tokencodes, assign tokens to users, replace tokens, issue software tokens, export tokens, manage incorrect passcode count

Token Distributor

This role grants administrative responsibility to manage provisioning requests. Token Distributors also determine how to assign and deliver tokens to users. This administrator can delegate the responsibilities of this role.

The default permissions for this role limit management to the following:

Requests - view, distribute

Request Approver

This role grants administrative responsibility to approve, update, and reject provisioning requests, including new user accounts, user group membership, token requests, and the on-demand tokencode service. This administrator can delegate the responsibilities of this role.

The default permissions for this role limit management to the following:

Requests - view, approve

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 view and provide online and offline emergency access help. This administrator cannot delegate any of the responsibilities of this role.

The default permissions for this role limit management to the following.

Users	View, reset passwords, enable and disable accounts, terminate active sessions
User groups	View user groups
Reports	Run, schedule
Tokens	View token, reset SecurID PINs, resynchronize tokens, manage online and offline emergency access tokencodes
User accounts	Manage fixed passcode, manage logon aliases, edit default shell, manage incorrect passcode count, clear cached Windows credential, manage online and offline emergency access passcode
Agents	View

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 any of the responsibilities of this role.

The default permissions for this role limit management to the following.

Users	View, reset passwords, enable and disable accounts, terminate active sessions
User groups	View user groups
Tokens	View token, reset SecurID PINs, resynchronize tokens, enable and disable SecurID tokens
User accounts	Manage logon aliases, edit default shell, manage incorrect passcode count, clear cached Windows credential
Agents	View

Agent Administrator

This role grants administrative responsibility to manage authentication agents and grants access to selected authentication agents. This administrator cannot delegate any of the responsibilities of this role.

The default permissions for this role limit management to the following.User and User

Users	View
User groups	View user groups, assign user group membership
Reports	Add, delete, edit, view report definition, run, schedule
Agents	Add, delete, edit, view, manage node secret, grant user groups access to agents

Group Administration

Once you create your security domain hierarchy and link your identity source with your realm, all users appear by default in the top-level security domain. To help you organize and manage your system, you may want to create user groups and possibly transfer users to one of the other security domains in your hierarchy.

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

For example, if you have a top-level security domain named FocalView Software Company, and lower-level security domains named Boston, New York, and San Jose, you would likely move users located in each of those locations to their respective security domains.

Note: Each user can exist in one security domain only.

Users

Organizing users in security domains helps you find users and assign them tokens or add them to user groups. See the following section, "User Groups." For example, you can search for all users in the Boston security domain and then assign a token to each member.

This allows you greater control because you can limit users and administrators by department, geographic location, or in any other way that you choose.

User Groups

A user group is a collection of users, other user groups, or both. Members of the user group must belong to the same identity source.

User groups have the following characteristics:

- They can be made up of one or more users or user groups.
- They can occur across security domains. This means that users in security domain A and users in security domain B can both be members of the same user group and thus access the same protected resources.

- A user or user group can be a member of more than one user group.

You can create user groups in one of two ways:

- Use the User Groups option in the Identity menu in the Security Console.
- For external data sources such as Active Directory, create the groups using the directory's user interface.

After you create user groups and add users, you can give the users access to restricted agents. Restricted agents can be accessed only by users belonging to the user group associated with the restricted agent. (Unrestricted agents can be accessed by all registered users in the same realm as the agent. If there are multiple identity sources associated with the realm, users in all identity sources can access the unrestricted agent.)

If you plan to use restricted access, and your identity source is a Global Catalog, all of the Active Directory groups must be of the "universal" type for replication. Groups of the "global" type are not replicated in the Global Catalog.

Time Restricted Access

You can control access by restricting the hours when specified groups can authenticate. For example, you specify that users in the Debt Collection Group may access the Accounts Receivable database only between the hours of 8:00 a.m. and 8:00 p.m to allow for overnight reconciliation of customer payment records.

Note: Time restricted access is based on Coordinated Universal Time (UTC), not local time.

Restricted access is through restricted agents, and applies to user groups. You cannot specify restricted access for individual users or agent hosts. The hours are specified by the administrator, and they apply to all users contained in the specified user group. Users who are members of multiple user groups will be able to authenticate if they are a member of any user group that has access during the specified hours of access. The server enforces the hours at runtime.

Know the following about time restricted access:

- When an authentication is attempted through a restricted agent, the server seeks all user groups that are both enabled on the restricted agent and contain the authenticating user. If the user is found in a user group that is allowed access at that time, the authentication succeeds. The authentication will not succeed if the user is not contained in an allowed user group, or if the user group is not allowed access at the time of the authentication attempt.
- You cannot restrict access by time on an unrestricted agent because unrestricted agents do not have user groups associated with them.
- Time restrictions are based on increments of an hour. For example, you cannot set the restricted times to minutes.
- Time restricted access does not apply to administrators authenticating to the Security Console.

- In order to edit restricted access hours for a user group, an administrator must log on and have the necessary administrative role to add, remove, or modify a user group.
- You can only add, edit, and remove access time restrictions by user group.

If you want to use time restricted access, plan:

- Which resources require restricted access
- Which user groups can access the restricted resources
- Which users belong to the restricted access user groups
- The range of restricted hours for each restricted resource

Administrator and User Training

Develop a plan to train your users and administrators. If you have any tasks that are unique and specific to your business, remember to add them to your list of training topics.

Help Desk Administrator training should include awareness of the tactics of unauthorized individuals who try to enter your system by way of your Help Desk. Plan to provide strategies to your Help Desk Administrators for dealing with such attempts.

User Training

The following list contains topics for the tasks most commonly performed by users:

- Two-factor authentication
- Using RSA SecurID tokens
- Requesting on-demand tokencodes
- Online and offline authentication

The following list contains topics for tasks most commonly performed by self-service and provisioning users:

- Self-service:
  - Troubleshooting tokens
  - Changing token passwords and PINs
  - Resynchronizing tokens
  - Resetting token PINs
  - Using self-service troubleshooting policies
  - Putting tokens into emergency access mode if a token is lost, broken, or temporarily unavailable
  - Activating tokens
  - Testing authentication

- Provisioning:
  - Requesting enrollment
  - Requesting new or additional hardware or software tokens
  - Requesting the on-demand tokencode service
  - Requesting replacement tokens for tokens that are about to expire
  - Requesting replacement tokens for temporarily lost tokens
  - Requesting replacement tokens for permanently lost or broken tokens
  - Requesting a change in user group membership

Administrator Training

The following list contains topics for the tasks most commonly performed by Help Desk Administrators:

- Viewing users
- Viewing user and token data
- Assigning and unassigning tokens
- Enabling and disabling user accounts
- Enabling, re-enabling, disabling, and editing user tokens
- Editing user authentication attributes
- Editing token properties
- Synchronizing tokens
- Viewing and resetting RSA SecurID PINs
- Viewing and resetting passwords
- Replacing tokens
- Managing logon aliases
- Editing the default shell for user accounts
- Generating and downloading seed files
- Managing an incorrect passcode count
- Clearing a cached Windows credential
- Providing emergency access
- Terminating active sessions
- Viewing agents
- Viewing user groups
- Approving token requests
- Distributing tokens

Request Approvers and Token Distributors

The following list contains topics for the tasks most commonly performed by Request Approvers and Token Distributors:

- Request Approvers:
  - Viewing requests for enrollment, tokens, on-demand tokencode service, or user group membership
  - Approving or rejecting requests for enrollment, tokens, on-demand tokencodes, or user group membership
  - Deferring action on enrollment requests with incorrect security domains, identity sources, and user groups
  - Correcting enrollment requests
  - Updating requests for enrollment, tokens, on-demand tokencodes, or user group membership
- Token Distributors:
  - Viewing requests for tokens that require distribution
  - Assigning tokens to users
  - Delivering tokens to users
  - Creating distribution reports
  - Closing requests

Administration Summary

Know the following when planning administration:

- Where to make administrative changes, and how changes are propagated.
- How to use the Microsoft Management Console for administration of Active Directory.
- How to administer RADIUS, if you plan to use RADIUS.
- How to plan roles, permissions, and scope.
- Which predefined administrative roles meet your needs.
- How to customize roles, if needed.
- How to add administrators, if needed.
- How to assign administrative roles to users.
- How to administer users and user groups.
- How to assign roles permissions, and scope to administrators and users.
- How to transfer users from the top-level security domain to lower-level security domains, if necessary.
- How to create restricted groups, if necessary.
- How to apply time restricted access to groups, if necessary.
- What training your administrators and users need.

9 Planning Policies

Planning Password, Token, Lockout, and Offline Authentication Policies

Policies control various aspects of a user's interaction with RSA Authentication Manager, such as RSA SecurID PIN lifetime and format, fixed passcode lifetime and format, and password length, format, and frequency of change. Default policies are created in the top-level security domain and are assigned to each security domain within the realm. You can create custom policies for each security domain, or assign them the default policies.

Each security domain has policies assigned to it that dictate the following:

- Password. See "Planning Password Requirements and Restrictions" on page 94.
- Token. See "Planning Token PIN Requirements and Restrictions" on page 95.
- Lockout. See "Determining When to Lock Out Users After Failed Authentications" on page 98.
- Offline Authentication. See "Planning Offline Authentication" on page 99.

When you create a new security domain, the default policy is automatically assigned. You can optionally assign a custom policy to the new security domain. If you designate a new default policy, the new default policy is automatically assigned to the security domain.

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

Planning Password Requirements and Restrictions

In Authentication Manager, passwords are only used as the default method for administrators logging on to the RSA Security Console. No agent will acknowledge a password authentication other than to the Security Console. Consider this purpose when you determine which requirements and restrictions you want to use for your password policies in Authentication Manager.

Password policies define users' password length, format, and frequency of change, and are assigned on a per security domain basis. One password policy is always designated as the default policy, and assigned to each new security domain that is created. You can use the default password policy or apply a custom policy to each security domain.

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

Password policies are put in place to overcome the shortcomings of static passwords by not allowing users to create easily-guessed passwords like birthdays, or the names of pets, children, or favorite fictional characters. The use of an excluded words dictionary can also help to overcome typical password choices.

Authentication Manager allows you to configure the following password requirements and restrictions:

- Use of system-generated passwords
- Periodic password changes
- Reuse of old passwords
- Password lengths
- Excluded words dictionary
- Password character requirements

  You can require the following types of characters:

  - Alphabetic characters
  - Uppercase characters
  - Lowercase characters
  - Numeric characters
  - Non-alphanumeric characters

The requirements and restrictions for passwords are similar to the requirements and restrictions for PINs. See the following section, "Planning Token PIN Requirements and Restrictions."

Planning Token PIN Requirements and Restrictions

A PIN is the second factor of RSA SecurID two-factor authentication, and as such, the policies you apply to the creation and use of PINs are an integral part of securing your systems.

To protect against a stolen PIN, Authentication Manager employs token policies, which you can configure to prompt users for a second tokencode after a series of failed logon attempts. In this case, Authentication Manager is effectively requiring the user to prove that the token is in his or her possession. For example, if an unauthorized user with a stolen PIN eventually succeeds in guessing a valid tokencode, he is denied access when he does not correctly enter the next tokencode generated by the token.

One of the most common security issues regarding PINs (and passwords) is employees writing them down on a piece of paper and leaving it in a convenient location. Even when employees are discouraged from such behavior, the problem of forgetting long, complex, system-generated PINs creates an additional administrative burden on your Help Desk. When setting token policies in regards to PINs, the goal is to create a situation that balances security and ease of use.

For example, longer PINs are more difficult to remember, but more secure. Shorter PINs are easier to remember, but also easier to guess. If you set your policy to use shorter PINs to ensure that employees remember them and do not write them down, you can offset this by requiring alphanumeric PINs that must be changed more frequently.

The longer a PIN is valid, the greater the risk that it will be compromised. A short maximum lifetime may increase security. However, it may also be counterproductive in that remembering a new PIN, especially a system-generated PIN, is difficult and may increase the number of employees who write down their PINs. This negates the effectiveness of the strict policy.

When allowing users to create their own PINs, you run the risk that they may select easily guessed PINs, such as birthdays, or the names of pets or children. You can set your policy to exclude certain words, and to require alphanumeric characters.

Instruct your users to protect the secrecy of their PINs and the physical security of their tokens.

Instruct your administrators to respond immediately to disable compromised PINs and missing tokens.

Creating Secure PINs

Authentication Manager allows you to configure the PIN requirements and restrictions described in the following table.

PIN Requirement	Description
Require the use of system-generated PINs	Enabling this feature ensures that users' PINs are random and therefore less likely to be guessed by an unauthorized person attempting to access your network.
Require periodic PIN changes	Enabling this option allows you to set minimum and maximum PIN lifetimes. The minimum PIN lifetime is the minimum amount of time that a password can exist before the user can change it. The maximum password lifetime is the maximum amount of time a user can keep a password before being required to change it. Setting a minimum PIN lifetime prevents users from circumventing any restrictions on the reuse of old PINs that you may have set. For example, if users are restricted from reusing their five most recent PINs, the minimum PIN lifetime prevents them from immediately changing their PIN six times so they can reuse a particular PIN. Setting a maximum PIN lifetime prevents users from indefinitely keeping the same PIN, which increases the likelihood that it might be guessed by an unauthorized person trying to access your network. **Note:** Be sure to balance security of the system and ease of use for the members of your organization. An overly strict maximum lifetime, such as one that requires a PIN change every seven days, may be counterproductive in that remembering a new PIN every seven days is difficult and may increase the number of employees who write down their PINs. This negates the effectiveness of the strict policy.
Restrict the reuse of old PINs	Setting a restriction on the reuse of old PINs prevents users from reusing the same two or three PINs over and over, which decreases the likelihood that an unauthorized person may guess a PIN.

PIN Requirement	Description
Limit PIN lengths	Setting minimum and maximum PIN lengths prevents users from creating PINs that are too short and easily guessed by an unauthorized person attempting to access your network, or that are too long and difficult for the authorized users to remember. **Note:** Be sure to balance security of the system and ease of use for the members of your organization. Required PIN lengths that are too long may be counterproductive in that remembering a long PIN is difficult and may increase the number of employees who write down their PINs. This negates the effectiveness of the strict policy. Long PINs that users cannot remember can also lead to more users locked out of your network, and therefore more calls to the Help Desk for assistance.
Use an excluded words dictionary	The excluded words dictionary prevents users from using common, and therefore, easily guessed words as PINs. The excluded words dictionary is a record of words that users cannot use as PINs, including several thousand commonly used words that are likely to be included as part of any dictionary attacks on the system. For example, you can prevent PINs such as “1111” or “1234” with the excluded words dictionary.
Set PIN character requirements	Requiring and allowing specific characters in PINs can make guessing the PIN more difficult. You can require alphabetic or numeric characters. **Note:** The PIN character requirements do not apply to software tokens and PINPads. Software tokens and PINPads require numeric PINs.

You can place greater restrictions on users associated with a particular security domain by defining multiple PIN policies. By defining additional policies, you can require some employees to adhere to more strict standards when selecting and using PINs.

For example, your company has three security domains:

- Research and Development (R&D)
- Human Resources (HR)
- Finance

The administrator determines that the default policy is adequate for protecting the R&D and HR security domains, but given new government compliance regulations, the administrator wants to define a more strict policy for the Finance security domain. As a result, users in the Finance security domain require longer PINs and more frequent PIN changes.

Determining PIN Creation Methods

Authentication Manager provides two methods of PIN creation:

System-generated PINs. Created by Authentication Manager based on the PIN policies you set.

User-generated PINs. Allows users to select their own PINs, within the restrictions of the PIN policies you set.

Note: Regardless of the method you select, PINs are assigned to users during their first authentication attempt.

Determining When to Lock Out Users After Failed Authentications

To protect against the random guessing of passcodes, Authentication Manager employs lockout policies, which allow you to configure a specific number of allowed incorrect authentication attempts. When this number is exceeded, the user is locked out. This prevents users from entering passcode after passcode in an attempt to guess a correct passcode (either a stolen PIN, with guessed tokencodes, or guessed PINs with correct tokencodes read from a stolen token). You can specify one or more lockout policies.

Administrators can define a lockout policy for each security domain. The lockout policy assigned to a security domain dictates the lockout requirements for all the users assigned to that security domain.

Lockout policies specify:

- The maximum number of failed authentication attempts a user can make within a given period of time.
- Whether an administrator must re-enable users, or users are automatically re-enabled after a given period of time.

One lockout policy is always designated as the default policy, which is assigned to each new security domain unless another policy is explicitly assigned to a security domain. Lockout policies assigned to top-level security domains are not inherited by lower-level domains.

You can set lockout policies in the following ways:

- Never lock the user's account, regardless of the number of incorrect authentication attempts made by the user.
- Lock the user's account after a certain number of consecutive failed authentication attempts.
- Unlock the user's account automatically after a specific period of time, or require the administrator to manually unlock the user's account.
- Allow self-service users to unlock their own accounts.

Planning Offline Authentication

Offline authentication extends RSA SecurID authentication to users when the connection to Authentication Manager is not available. For example, when users work away from the office, or when network conditions make the connection temporarily unavailable. You enable, disable, and configure offline authentication through Authentication Manager by specifying an offline authentication policy and applying that policy to Authentication Manager security domains.

When offline authentication is enabled, Authentication Manager downloads a configurable number of "offline days" of tokencode data to user's machines. This data is used when users attempt to authenticate offline.

You enable local authentication and Windows password integration through the Security Console, as part of an offline authentication policy. Only users assigned to security domains with an offline authentication policy that allows offline authentication and Windows password integration can use these features.

When you install Authentication Manager, a default offline authentication policy is automatically created. You can use this policy, or create a custom offline authentication policy and designate it as the default.

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

Integrating User's Windows Passwords with RSA SecurID

Windows password integration integrates RSA SecurID into the Windows password logon process. Users provide their Windows logon passwords only during their initial online authentication. Passwords are then stored with the users' authentication data in the internal database and, for offline authentication, in the offline data.

During subsequent authentications, users enter only their user names and SecurID passcodes. The authentication agent gets the Windows password from the Authentication Manager and passes it to the Windows logon system.

Setting Minimum Online Passcode Lengths

This setting adjusts the cryptographic strength of your offline authentication policy. RSA recommends that the minimum online passcode length setting be at least twelve characters long. If your RSA SecurID tokens display six characters, for example, require your users to specify PINs that are at least six characters.

To download offline data, the user's passcode (PIN + tokencode) length must be 8 to 16 characters.

Handling Offline Authentication with Devices that Do Not Meet Security Recommendations

RSA does not recommend offline authentication for the following authenticators:

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

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

Offline Emergency Codes

Users can use offline emergency tokencodes or offline emergency passcodes to authenticate when their computers are disconnected from the network.

Offline emergency tokencodes. Used when users have misplaced their tokens.

Offline emergency passcodes. Used when users have forgotten their PIN and need a full passcode.

Important: Because emergency passcodes enable authentication without a PIN, RSA recommends that you use emergency tokencodes instead. Users still must enter their PIN followed by the emergency tokencode to gain entry to their computers. Provide emergency passcodes only in situations where users have forgotten their PINs. In such cases, make sure you properly identify the users before providing them with emergency passcodes.

You enable offline emergency codes through the Security Console as part of a token policy. Only users assigned to security domains with an offline authentication policy that allows offline emergency tokencodes or passcodes can use this feature.

Policies Summary

Know the following when planning policies:

- How many distinct policies you need and how to define default and custom policies.
- Which policies you want for top-level security domains and which ones you want for lower-level security domains.
- How PINs are created.
- How and when to lock a user account for unsuccessful authentication attempts.
- How and when to unlock a user account.
- Determine password policies and restrictions.
- How administrators manage emergency access situations.
- How to establish character restrictions for PINs, passwords, and emergency access tokencodes.
- What training users and administrators need on policies.

10 Planning RSA SecurID Token Deployment

Overview of RSA SecurID Token Types

RSA SecurID tokens generate and display tokencodes. The tokencode must be combined with the user's PIN to create a passcode, which enables authentication.

RSA SecurID token types include:

Hardware token. A device manufactured by RSA that displays tokencodes. Hardware tokens are either time-based (a tokencode is always displayed and changes automatically every 60 seconds), or event-based (a tokencode displays whenever the user presses a button). Standard tokens, PINPads, key fobs, and USB tokens are time-based tokens. The RSA SecurID Display Card is an event-based token.

Software token. A software-based security token installed with an associated RSA SecurID application to a Windows desktop or laptop, web browser, an RSA Smart Card, a personal digital assistant (PDA), or a mobile device. The installed token displays tokencodes.

Hardware Token Types

RSA provides the following hardware tokens.

Standard token. A time-based, credit-card-size hardware device. It displays a unique code generated by the RSA SecurID or AES industry-standard algorithm in combination with the unique seed contained in the token and an internal clock.

PINPad. A time-based, credit-card-size hardware device. It differs from the standard token in that the user enters the PIN directly into the card on a 10-digit numeric keypad. The generated passcode displayed is a hash-encrypted combination of the PIN and the current tokencode.

Key fob. A time-based hardware device that connects to a key ring and fits into a user's pocket or small carrying case. It operates identically to the standard token.

RSA SecurID 700. A time-based, smaller key fob model that connects to a key ring. It operates identically to the standard token.

RSA SecurID SID800 USB token. A time-based, multifunction device that combines the features of the traditional RSA SecurID hardware token with a smart chip. In addition to generating passcodes, it is capable of storing multiple X.509 digital certificates that enable authentication, digital signature, and file encryption applications.

For use as a smart card, the device can store several User ID and password combinations for logon to password-enabled applications. When connected, the device becomes an RSA SecurID authenticator that enables applications to programmatically access tokencodes, eliminating the need for users to type their code. When disconnected, the SID800 operates like a standard.

RSA SecurID Display Card. An event-based, credit-card-size hardware device. It differs from standard and PINPad tokens in that it generates tokencodes whenever the user presses a button on the card.

Software Token Types

A software token is a software-based security token that a user can install to an RSA SecurID application on a desktop or laptop PC, a personal digital assistant, a mobile device, or an RSA Smart Card. The token seed record is generated in the RSA Security Console and then imported to the installed software token application. The Security Console provides a centralized administration interface for issuing RSA SecurID software tokens to the supported device types.

RSA SecurID software tokens are available for the following platforms:

- Windows Computers
- Windows Mobile Devices
- Palm Handhelds
- BlackBerry Handhelds
- Symbian OS and UIQ
- Java ME Devices
- RSA SecurID Toolbar

  RSA SecurID Toolbar is a browser plug-in that users install into a Mozilla Firefox or Microsoft Internet Explorer browser. Users must install a token to use the toolbar. To access resources protected by Authentication Manager, users must enter an 8-digit code displayed in their toolbar in addition to the credentials that they normally provide (user name and password) to enter a secure site.

Note: The Security Console provides a centralized administration interface for issuing RSA SecurID software tokens to the supported device types. You can add information to software tokens, such as device serial number or token nickname, using the token attributes fields.

The following table describes the issues that you need to consider before implementing software tokens.

Consideration	Description
Enabling copy protection	The Enable Copy Protection option ensures that the software token cannot be copied or moved from the directory in which it is installed on a user's computer or other device. RSA strongly recommends that you use copy protection.
Binding a software token to a device	When you issue the token, you can include the serial number of the device in the token file. If the serial number in the token file does not match the serial number of the device, the token cannot be installed. Binding a software token to a device increases administrative control over the use of software tokens.

Consideration	Description
Issuing software token files	You can issue software tokens in token files (sdtid files). You can issue multiple software tokens per file (best used for situations in which an administrator is installing the tokens), or issue separate files for each token (best used when users are installing tokens on their own PCs or devices).
Using passwords to protect software token files	You can specify a password that protects the issued software token. The type of password protection depends on which method of issuing tokens you select. • If you select a single file for all issued software tokens, you can protect the file with a password of your choice. • If you select separate files for each issued software token, you can specify a single password of your choice, specify the User ID of the user to whom you issue the token, or a combination of the two for each file.
Using remote token-key generation to deploy software tokens	Remote token-key generation enables Authentication Manager and the device that hosts the software token, such as a web browser, to simultaneously and securely generate the same token seed on a device and Authentication Manager. This allows you to put a token seed on a user's device without actually sending the token seed through e-mail or putting it on electronic media. This greatly decreases the chances that the token seed will be intercepted by an unauthorized person. **Note:** If you install RSA Authentication Manager inside a secure DMZ, you may decide only to allow traffic through a proxy server. If the primary instance stops responding, token key generation URLs and service addresses that you have distributed to users, but that users have not yet used, become invalid. If your proxy server supports failover mode, you can configure it to pass CT-KIP data to the new primary instance. For more information, see the chapter "Protecting Network Resources with RSA SecurID" in the *Administrator's Guide*.

Determining Which Types of Tokens to Deploy

The most important factors in deciding which type of tokens to deploy are, the complexity of your deployment, the size of your user population, and the ease of distribution. Determine which types of tokens best meet the needs of your users and your deployment.

For example, your organization has a remote sales force whose members must authenticate with an RSA SecurID token when they log on to their laptop computers. You might choose to distribute hardware tokens to these users.

You might choose to distribute software tokens to users who have a Blackberry or other portable devices that they use for work. With a software token installed directly on a PDA or mobile device, these employees do not need to carry a separate hardware token.

Deploying Tokens to Users

The types of token you use, ease of administration, and security are factors in determining the method of token distribution that you use.

Note: Instead of deploying tokens, you can allow users to request tokens and automate token deployment with the token provisioning feature of RSA Credential Manager. For more information, see Chapter 11, "Planning Self-Service and Provisioning."

Hardware Tokens

The methods of delivering hardware tokens are:

- **Users receive tokens at a central location.**

  This is the most secure method, although it may not be feasible for all users. The advantage of this distribution method is the assurance that the hardware tokens are delivered to the right users and that they work when users receive them. To accommodate this delivery method, plan to have trained administrative personnel at each office site where tokens are distributed.

- **Users receive tokens in the mail.**

  Mailing hardware tokens through interoffice mail, post, or overnight express, for example, may be more feasible for your organization. However, this usually involves more preparation to ensure success. You will need to develop a process for generating mailing labels, mailing the hardware tokens, and verifying that users receive their tokens. The most secure recommendation is to set tokens to disabled before you mail them. Send any information about enabling tokens separately from the actual tokens or make it accessible only from a secure location.

Use secure methods such as the following to distribute hardware tokens to users:

- Distribute tokens that are assigned but disabled.
- Enable a token only after you are satisfied that it is in the possession of the assigned user and that the user is ready to log on for the first time using this token.
- If you must distribute enabled tokens to assigned users, do so through secure channels (such as having them delivered in person by trusted staff members).

You may need to use a combination of these delivery methods, depending on your organization's size and number of locations.

Software Tokens

RSA SecurID software tokens must be installed with an associated RSA SecurID application. The application must be distributed to users and installed on desktops and handheld devices.

You can assign the task of installing the application and the seed record to your IT personnel. A variety of methods are available for deploying software tokens, depending on the device to which the token is deployed. For deployment information, see the documentation provided with the software token application.

Delivering Tokencodes by Way of Mobile Devices and E-mail Accounts

In addition to receiving tokencodes on hardware and software tokens, users can receive tokencodes by way of their digital cellular phones or personal e-mail accounts. The Authentication Manager on-demand tokencode service delivers tokencodes by way of Short Message Service (SMS) for cellular phones or Simple Mail Transfer Protocol (SMTP) for e-mail accounts. Tokencodes delivered by way of SMS or SMTP are called on-demand tokencodes.

If you plan to enable users to request and receive on-demand tokencodes, you need to first set up and configure the service in Authentication Manager. If you plan to use SMS, you must establish a relationship with an SMS provider. The default provider is Clickatell. For more information, go to **http://www.clickatell.com/rsa/securid.php**. Many mobile service providers offer SMS transmission to mobile devices. Contact RSA Professional Services for information about using other providers.

As with the tokencode generated by a hardware or software token, on-demand tokencodes are used with a PIN to achieve two-factor authentication. The difference is that on-demand tokencodes are user-initiated. Authentication Manager only sends a tokencode to the user when it receives a user request by way of RSA Credential Manager. On-demand tokencodes can only be used once, and they expire after the lifetime that you configure.

For example, a user who is enabled for on-demand authentication can request a tokencode so that he or she can access the resources protected by Authentication Manager. Authentication Manager receives the request and sends a tokencode to the user's e-mail address or mobile device. The user can then use that tokencode to authenticate.

On-demand tokencode service is typically used when:

- Users prefer this method to using hardware or software tokens.
- A user loses his or her hardware token or device containing a software token.
- You use the Business Continuity option to temporarily increase your number of RSA SecurID users. For more information, see "Business Continuity Option" on page 147.

Know the following about delivering tokencodes by way of mobile devices and e-mail accounts:

- On-demand tokencode service can use telephone numbers or e-mail addresses stored in either the Authentication Manager internal database or an LDAP directory.
- Both delivery methods may be enabled simultaneously in your system, but you can select only one method per user.
- Authentication Manager provides a configurable integration with Clickatell.
- A custom on-demand tokencode service transmission integration can be implemented by RSA Professional Services if you choose other SMS vendors.
- Authentication Manager provides an SMTP plug-in gateway.
- On-demand tokencode service is specific to the deployment where it is enabled. It cannot be used for communications among trusted realms.

Informing Users About the Planned Rollout

Deploying Authentication Manager changes the way users log on to their systems and to the network. It is imperative that you train users and administrators in the use and care of their tokens.

Consider the following:

- When and how will you inform users about the planned rollout of RSA SecurID tokens?
- How will you communicate authentication instructions to users?

Give users advance notice of the scheduled changeover. By doing so, you give them a chance to ask questions and clear up any confusion before you implement the new procedures.

You may want to inform users through one of the following methods:

- E-mail
- Company/IT/MIS newsletter
- Intranet

Informing Hardware Token Users

RSA recommends that you provide documentation with each hardware token. If you plan on mailing hardware tokens to your users, consider including a small card with instructions for locating a more detailed procedure or a telephone number to call to enable the device. If you plan to distribute hardware tokens directly to users, consider giving them complete procedures as part of the package. Alternatively, you can include the instructions with the initial notification to users of the planned rollout, or include a URL where they can download the instructions.

Informing Software Token Users

Documentation for software tokens is provided with the software application. Inform the individuals responsible for deploying the application that they need to read the documentation.

Consider the following options.

Option	Description
RSA documentation	RSA software token products provide an administrator's guide, as well as user documentation (typically a Help document, a Quick Start document, or both). If you are deploying the RSA SecurID SID800 Authenticator, see the *RSA Security Center Help* and *RSA Authentication Client User's Quick Reference*, both of which are provided with RSA Authentication Client. These documents contain user instructions.
Your own documentation	Document procedures for performing certain functions, including enabling the token, setting an initial PIN, resetting a PIN, and acquiring help with authentication problems. You may want to include screenshots of different processes.
RSA SecurID tour	An online, interactive tour that you can view at **http://www.rsa.com/node.asp?id=1159**. The tour explains the concept of two-factor authentication, the different types of RSA SecurID authenticators, and the procedures associated with two-factor authentication.

Token Deployment Summary

Know the following when planning token deployment:

- Which types of tokens you want to use in your deployment.
- How to distribute hardware tokens.
- How to distribute software tokens.
- How and when to use one-time tokencode delivery by mobile device or e-mail. (Special license required.)
- How and when to use Credential Manager token provisioning. (Enterprise Server license required.)
- How and when to inform users about the rollout of RSA SecurID tokens.

11 Planning Self-Service and Provisioning

Overview of RSA Credential Manager

RSA Credential Manager is a web-based workflow system that automates the token deployment process and provides user self-service options.

Provisioning streamlines the token deployment process if you are rolling out a large-scale token deployment. It also reduces administrative services and the time typically associated with deploying tokens.

Self-service allows you to reduce the time that the Help Desk spends servicing deployed tokens—when users forget their PINs, misplace their tokens, and require emergency access, or resynchronization. Users perform token maintenance tasks and troubleshoot tokens using the RSA Self-Service Console without involving administrators.

Licensing Options

The Base Server license includes self-service. The Enterprise Server license includes self-service and provisioning.

Note: If you want provisioning, and have a Base Server license, you must upgrade to the Enterprise Server license.

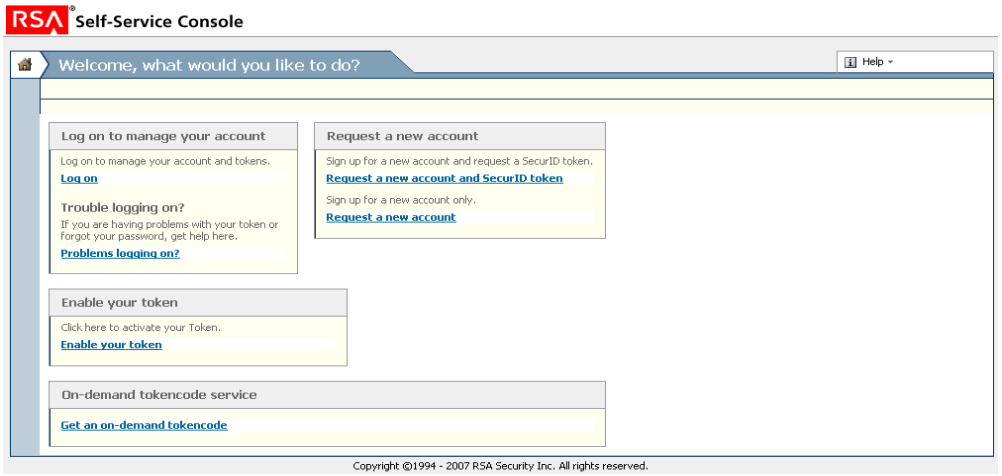
RSA Self-Service Console

The Self-Service Console is a browser-based interface where users can request tokens, troubleshoot tokens, and perform token maintenance tasks. You can customize the header text of the landing page of the Self-Service Console using the RSA Security Console. For more information, see the Security Console Help topic "Customize the RSA Self-Service Console Landing Page."

You can customize the Self-Service Console Help (RSA Self-Service Console Frequently Asked Questions) to reflect how your company uses self-service and provisioning. For more information, see "Customizing Help for the RSA Self-Service Console" in the *Administrator's Guide*.

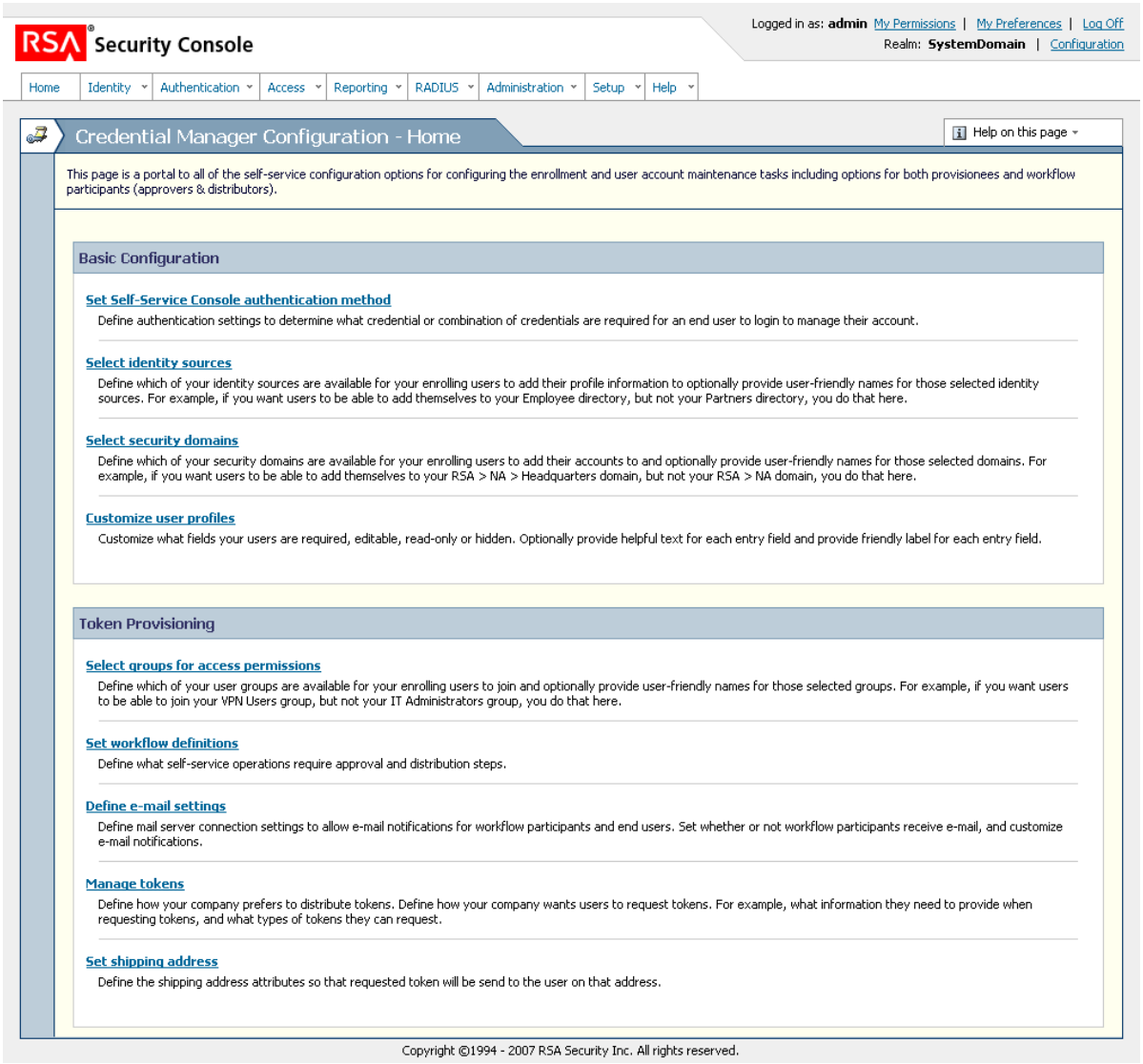
Note: The tasks that users can perform from the Self-Service Console depend on the type of access to identity sources and the license installed. For more information, see "Implications of Read/Write or Read-Only Access" on page 117.

The following figure shows the landing page of the Self-Service Console.



RSA Security Console

Super Admins use the Security Console to configure Credential Manager. The following figure shows the Credential Manager Configuration - Home page. For more information, see the Security Console Help topic “Configure Credential Manager.”



RSA Credential Manager Deployment Decisions

This section describes the benefits of deploying self-service and provisioning.

The tasks that users can perform are dependent on the license you install and whether you decide to make your identity source read/write or read-only. Self-service is available with all licenses. Provisioning is available with the Enterprise Server license.

Note: If you want provisioning, and have a Base Server license, you must upgrade to the Enterprise Server license.

Deploying Self-Service

When deciding whether to deploy self-service, consider the following:

- Does the Help Desk receive a large number of calls from users for token maintenance, troubleshooting tokens, and emergency access?
- Do you need to reduce the number of calls to the Help Desk?
- Do you need to reduce the cost of maintaining the Help Desk?

With self-service, users can use the Self-Service Console to:

- Enroll. When users enroll in self-service, they become users without administrative privileges.
- Test tokens, resynchronize tokens, change token PINS, and report problems with tokens. This eliminates a call to the Help Desk.
- Update user profiles. User profiles contain user name, user ID, e-mail address, and password.
- Change passwords for the Self-Service Console. They can do this only if the identity source is read/write.
- Troubleshoot tokens and get emergency access for lost, broken, or temporarily unavailable tokens.

Deploying Provisioning

When deciding about whether to deploy provisioning, consider the following:

- Do you have a large number of tokens to deploy or continual token deployment requirements?
- Do you need to reduce token deployment costs?

With provisioning, users can use the Self-Service Console to:

- Request enrollment. Users need approval to enroll in provisioning. When users get approval and enroll, they become users without administrative privileges.
- Request new or additional tokens.
- Enable a token.
- Request the on-demand tokencode service.
- Request on-demand tokencodes.
- Request replacement tokens if tokens are lost, broken, temporarily unavailable, or about to expire.
- Request user group membership for access to protected resources.

Implications of Read/Write or Read-Only Access

If you configure Authentication Manager to have read-only access to identity sources, some Credential Manager tasks are unavailable. If you configure Authentication Manager to have read/write access to identity sources, all Credential Manager tasks are available.

The following table shows the tasks that users can perform with the Base Server and Enterprise Server licenses, and whether these tasks are available if the identity source is set to read/write or read-only access.

Note: If a directory server is read-only, user information must exist in the directory server or in the Authentication Manager internal database for users to perform tasks using the Self-Service Console.

User Task	Identity Source (Base Server License)		Identity Source (Enterprise Server License)	
	Read/Write	Read-Only	Read/Write	Read-Only
Enrollment Tasks				
Request an account	✓	✓	✓	✓
Request an account, a token, or the on-demand tokencode service			✓	✓
Select identity source	✓	✓	✓	✓
Select security domain	✓	✓	✓	✓
Create user profile	✓		✓	

User Task	Identity Source (Base Server License)		Identity Source (Enterprise Server License)	
	Read/Write	Read-Only	Read/Write	Read-Only
Create password	✓		✓	
Answer security questions	✓	✓	✓	✓
Select user group membership			✓	
Troubleshoot problems using the self-service troubleshooting authentication method	✓	✓	✓	✓
Log On to the Self-Service Console				
Log on to the Self-Service Console	✓	✓	✓	✓
Token Management Tasks				
Request a token or the on-demand tokencode service			✓	✓
Enable a token			✓	✓
Change token PIN	✓	✓	✓	✓
Test a token	✓	✓	✓	✓
Report a problem with a token	✓	✓	✓	✓
Request a replacement token			✓	✓
Management Tasks				
Update profile	✓		✓	
Change password	✓		✓	
Request additional user group membership			✓	

Planning the RSA Credential Manager User Experience

To plan the Credential Manager user experience, consider how users will log on to the Self-Service Console, enroll in Credential Manager, and troubleshoot issues.

User Logon

You need to decide how users log on to the Self-Service Console. The following table lists the primary logon methods.

Primary Logon Method	Description
RSA password	The RSA password is the default method for protecting the Self-Service Console. The RSA password is optional for the internal database.
LDAP password	If you use a directory server as your identity source, you may also want to enable LDAP passwords as an authentication method. This allows users whose user records are saved in the identity source to access the Self-Service Console.
SecurID token	For additional security, you can configure Credential Manager to require users to present a credential more secure than a password, such as a passcode, before they access the Self-Service Console. A passcode consists of a PIN and tokencode. For more information, see the "RSA Self-Service Frequently Asked Questions."

User Enrollment

When users enroll in Credential Manager, they must:

- Enter or review information in a user profile
- Select a security domain
- Select an identity source

Entering Information in the User Profile

Credential Manager uses the information in user profiles to allow users to log on to the Self-Service Console and to send e-mail notifications to users.

Note: Users must enroll in Credential Manager to log on to the Self-Service Console or perform tasks such as requesting tokens.

There are several different enrollment paths for Credential Manager users that affect how users enter information into a user profile. The enrollment paths are:

New users. If a user is not in Authentication Manager and not in a directory server, the user enters all the required information in the user profile.

Users not in Authentication Manager, but in a read/write directory server. The directory server enters information in the user profile from the directory server, and the user can edit the information.

Users not in Authentication Manager, but in a read-only directory server. The directory server enters information in the user profile from the directory server, and the user cannot edit any information.

You can use the default user profile provided for users, or customize the user profile for each identity source that you make available to users. When deciding whether to customize user profiles, consider the following:

- Does your company have different names for some of the fields in the default user profile, for example, “User name” instead of “User ID”?
- Do you need to add descriptive text to instruct users about the information to enter for any of the fields?
- Do you need to add custom attributes, for example, a home address for users?
- Do you need to change fields in the user profile to require read/write, read-only, or hidden depending on the identity source that you use?

Note: If you use an identity source for enrollment, and it is read/write, you can make user profile fields read/write or read-only. If an identity source is read-only, all user profile fields are read-only.

Select Security Domains

Users must select a security domain when enrolling in Credential Manager. You need to plan which security domains to make available to the users. Consider the following when planning which security domains to make available:

- Make security domains available if you want users in those security domains to use self-service and provisioning. For example, if a security domain gets a large number of Help Desk calls from users, or deploys a large number of tokens, make that security domain available.
- Make all security domains available, if users can easily identify the correct ones. For example, if your company has security domains for locations or for departments, users can identify the correct security domain.
- Do not select security domains that are not appropriate for users. For example, if users in a security domain are not intended for self-service or provisioning, do not make that security domain available.

To make sure that users select the correct security domains, you can customize the names and descriptive text of all available security domains that appear on the Self-Service Console. For example, if you configure security domains for each department in your company, you can label each security domain with the department name and add instructions for users to pick their departments.

Select Identity Sources

Users must select an identity source when enrolling in Credential Manager. You need to plan which identity sources to make available to the users. Consider the following when planning which identity sources to make available:

- Make all identity sources available if users can easily identify which ones to select. For example, if your company has an identity source for company employees and another identity source for partners, users can easily identify the correct identity source.
- Do not select identity sources that are not appropriate for users.

To make sure that users select the correct identity sources, you can customize the names and descriptive text of all available identity sources that appear on the Self-Service Console. For example, if identity sources are set up for different locations in your company, you can label the identity sources with the locations and add instructions for users to pick their locations.

User Self-Service Troubleshooting

Self-service troubleshooting policies provide authentication that allows users to troubleshoot problems from the Self-Service Console.

Users can troubleshoot problems with tokens or with the Self-Service Console by clicking **Problems Logging on?** on the Self-Service Console. Users can perform the following troubleshooting tasks after authenticating with a self-service troubleshooting authentication method or after logging on to the Self-Service Console:

- Reset their password
- Reset their PIN
- Resynchronize their token
- Request a new token (if they lost the old one)
- Request an emergency access tokencode

The type of troubleshooting that users can do depends on the type of authentication method that you plan. The following table describes the authentication methods available for self-service troubleshooting and what users can troubleshoot with each method.

Self-Service Troubleshooting Authentication Method	Description	What Users Can Troubleshoot
Security questions	Users must answer security questions when they enroll.	Users can troubleshoot tokens and passwords from the Self-Service Console.
Passwords	Users must enter the password that is associated with their identity source (either directory server or the internal database).	Users can troubleshoot tokens only from the Self-Service Console. If users do not have a password, or forget their passwords, they must call the Help Desk for assistance. **Note:** Passwords are less secure than two-factor authentication.
None	Use if company policy does not allow users to store personal information (security questions and answers) in the system.	Users cannot perform self-service troubleshooting tasks, and this may result in additional calls to the Help Desk for assistance.

Number of Incorrect Self-Service Troubleshooting Authentication Attempts

You can configure an unlimited number of incorrect self-service troubleshooting authentication attempts, or you can allow a specified number of failed attempts within a specified number of days, hours, or minutes.

Note: The number of attempts applies only to self-service troubleshooting authentication attempts. All other authentication attempts are governed by the lockout policies associated with the security domain that manages the authenticating user.

For more information, see the Security Console Help topic “Self-Service Troubleshooting Policies.”

You can require that administrators must unlock accounts after users have exceeded the limit of incorrect attempts, or you can allow the system to automatically unlock accounts after a specified number of days, hours, or minutes.

For instructions, see the Security Console Help topic “Add Self-Service Troubleshooting Policies.”

Planning Provisioning

For provisioning, consider:

- How user requests are routed through provisioning systems
- What user groups to make available to users
- Which RSA SecurID token types to make available to users
- How to distribute hardware tokens
- What information you want to include in automated e-mail notifications to users
- What kinds of emergency access to make available to users

Workflows

A workflow defines the number of steps or work items for each type of user provisioning request. Provisioning uses workflows to automate token deployment. Users can request enrollment in provisioning, new or additional tokens, the on-demand tokencode service, replacement tokens, or changes in user group membership.

Workflow Definitions

A workflow definition consists of a combination of the following steps or work items for each type of request:

- One or two approval steps
- One distribution step for token requests
- Optionally, add one distribution step for software token requests

You can plan definitions for each type of request using the available steps or work items.

You need to consider the following when you plan definitions:

- How many approvals does each type of request require? For example, do you want a manager and an administrator to approve each request for enrollment for new employees.
- Do hardware token requests require a distribution step?
- Do software token requests require a distribution step?

Provisioning Roles

There are two predefined roles for provisioning:

Request Approver. Views user requests and approves, defers, or rejects user requests.

Token Distributor. Views user requests and determines how to deliver tokens to users. The Token Distributor also records how tokens are delivered to users and closes token requests.

You can use the predefined roles or customize your own roles. For more information, see “Predefined Administrative Roles” on page 81.

Consider the following when you plan provisioning roles:

- How many approvers do you need for the number of user requests you expect?
- Do you need approvers for each security domain?
- How many distributors do you need?
- Do you need distributors for each location?

Scope for Approvers

Scope for approvers is the same as scope for an Authentication Manager administrator. For example, when approving tokens, approvers can approve requests for tokens only if there are unassigned tokens available in their scope.

The exceptions are:

- Approvers can only approve requests for group membership if the user and the group is in their scope. Be sure to define approvers with scope over both users and user groups so that approvers can approve requests for group membership.

  For example, suppose an approver’s only responsibility is to assign users in the identity source “Developers” to groups in the security domain “Boston.” Users can request membership in any group that is in the same identity source to which they belong. If a user requests membership in a group in the security domain “Newton,” which is in their identity source, and the approver does not have scope over the “Newton” security domain, the approver cannot approve the request.
- If you set default groups for Credential Manager enrollment, any approver with scope for a user can approve the user request for enrollment in the default group, regardless of the approver’s scope over the group. For example, if a user requests membership in a default group in the “Newton” security domain, and the approver does not have scope for “Newton,” the approver can approver that request because the request is for a default group.
- If you set up default groups from multiple identity sources and there is more than one identity source, users can only belong to default groups from the identity source in which they are registered.

Select User Groups

User group membership allows provisioning users access to protected resources. See "User Groups" on page 86.

When you select user groups for Credential Manager, consider the following:

- Users can request membership in any groups that are in the same identity source to which they belong.
- If you set up more than one identity source, and set a default group from multiple identity sources, users can only belong to the default group in the identity source to which they belong.
- Which user groups provide users with the access to resources that they need?
- Are there any user groups that you do not want users to access?
- Is there a user group that you want all users to access?

Select Tokens

You need to decide which type of tokens you want to allow users to request.

The following table lists the available token types.

Tokens	Description
Hardware tokens	Handheld devices, such as a key fob, that display tokencodes that change at regular intervals. See "Hardware Token Types" on page 103.
Software tokens	Software-based tokens that reside on a user's computer, PDAs, or mobile devices. Once installed, the software token generates tokencodes that are displayed on the device screen. See "Software Token Types" on page 105.

On-Demand Tokencode Service

In addition to receiving tokencodes on hardware and software tokens, users can receive on-demand tokencodes delivered to mobile devices or e-mail addresses using the Short Message Service (SMS) or Simple Mail Transfer Protocol (SMTP). For more information about on-demand tokencodes, see "Delivering Tokencodes by Way of Mobile Devices and E-mail Accounts" on page 108.

Important: RSA SecurID hardware tokens offer the highest level of security. Other methods of tokencode delivery, such as software tokens and on-demand tokencodes, are easier to use but do not provide the same level of security as a hardware token. RSA recommends using hardware tokens.

You can set up Credential Manager to allow users to request the on-demand tokencode service themselves, instead of having users call the Help Desk for this service. After the on-demand tokencode service is approved, users request on-demand tokencodes from the on-demand tokencode site.

Choosing a Default

Optionally, you can choose a default token type or the on-demand tokencode service for user requests.

Replacement Tokens for Expiring Tokens

If a token is about to expire, users can get replacement tokens through the Self-Service Console. You can decide how many days to allow users to request replacement tokens before the expiration date of a token.

Customizing Token Graphics

Users view token graphics when they request new or additional tokens from the Self-Service Console. You can replace the default token graphics that ship with Credential Manager with your company's custom token graphics. For more information, see "Customizing Token Graphics" in the *Administrator's Guide*.

Token Distribution

You must decide how to distribute tokens to the user. This varies depending on the token type.

On-Demand Tokencode Distribution

Users gets on-demand tokencodes from the on-demand tokencode site. On-demand tokencodes are not distributed.

Hardware Token Distribution

For hardware tokens, ease of administration and security are factors in determining the method of hardware token distribution that you use. For more information, see "Hardware Tokens" on page 107.

Authentication Manager provides report templates you can use to create customized reports for hardware distribution. The distribution report template lists details about requests, tokens, shipping addresses, and information about users who made the requests. Token Distributors can use the information in the distribution report to distribute hardware tokens or send the distribution reports to third-party distribution companies. You can optionally customize distribution reports for token requests.

You also need to plan how to collect shipping addresses for token requests from users. You can collect shipping addresses in one of the following ways:

- If you use a directory server to store user information, you can map an attribute from the directory server for the shipping address, or create a custom attribute for the shipping address in the directory server. For more information, see "Attribute Mapping" on page 72.
- If you do not use a directory server for user information, users can enter their shipping address every time they request tokens.

Methods for Issuing Software Tokens

You can use Credential Manager to automatically deliver software tokens by e-mail to users when user requests are approved. You do not need to plan a distribution method for this type of token. However, there is a risk that an unauthorized person can intercept the token file and use the software token.

You can require users to supply passwords for token files to protect software tokens. For tokens with PINs, the password for token files is optional. For tokens without PINs, which have one-factor authentication, the password is required.

You can select from the following methods for issuing software tokens:

ZIP file format. Credential Manager packs up the token record into a single .sdtid file, adds the .sdtid file to a .zip archive, and e-mails it to the user.

SDTID file format. The software token record is written to an .sdtid file, and Credential Manager e-mails it to the user.

E-mail Notifications

Credential Manager sends e-mail notifications automatically to users about requests for enrollment, tokens, the on-demand tokencode service, and user group membership. Also, Credential Manager sends e-mail notifications automatically to workflow participants (approvers and distributors.)

Plan for E-mail Servers

You need to know the following information for e-mail servers:

Hostname. Decide which e-mail server to use to send e-mail notifications.

SMTP port. Determine which SMTP port to use. Simple Mail Transfer Protocol (SMTP) is the standard for e-mail transmissions across the Internet.

E-mail address. The address from which Credential Manager sends e-mail notifications.

Logon. Find out if your e-mail server requires a User ID and password.

For more information, see the Security Console Help topic “Configure the SMTP Mail Service.”

Customize E-mail Notifications

You can change the content of e-mail notifications by customizing the Credential Manager e-mail notifications. Consider the following:

- Do you need to send information about requests that is unique to your company?
- Do you have information that is appropriate only for certain situations? You can use conditional statements in your e-mail templates to include information, if certain conditions are met.

For more information, see the appendix “Customizing RSA Credential Manager” in the *Administrator’s Guide*.

Enabling or Disabling E-mail Notifications

The default setting for e-mail notifications is to send e-mail notifications to workflow participants (approvers and distributors). If workflow participants do not want to receive e-mail notifications about requests, you can disable this setting. Workflow participants who decide not to receive e-mail notifications can view all requests by clicking the **Pending Request** tab on the Provisioning Requests page of the Security Console.

Note: Credential Manager sends e-mail notifications automatically to users about their requests for enrollment, tokens, the on-demand tokencode service, and user group membership. You cannot disable e-mail notifications to users.

You can also enable e-mail notifications to Super Admins and workflow participants in the parent security domain. When you nest security domains to create an administrative hierarchy, the top-level security domain is the parent security domain. If you enable e-mail to workflow participants in the parent security domain, all approvers and distributors in security domains above the security domain where a request originates receive e-mail notifications.

Decide who you want e-mail notifications sent to:

- All workflow participants
- Super Admins
- Participants in the parent security domain

Emergency Access

If tokens are temporarily unavailable or permanently lost or broken, users may require emergency access to the resources protected by Authentication Manager. Users can get emergency access using the Self-Service Console. For more information, see "For Online Users" on page 146.

You need to consider the following when planning emergency access:

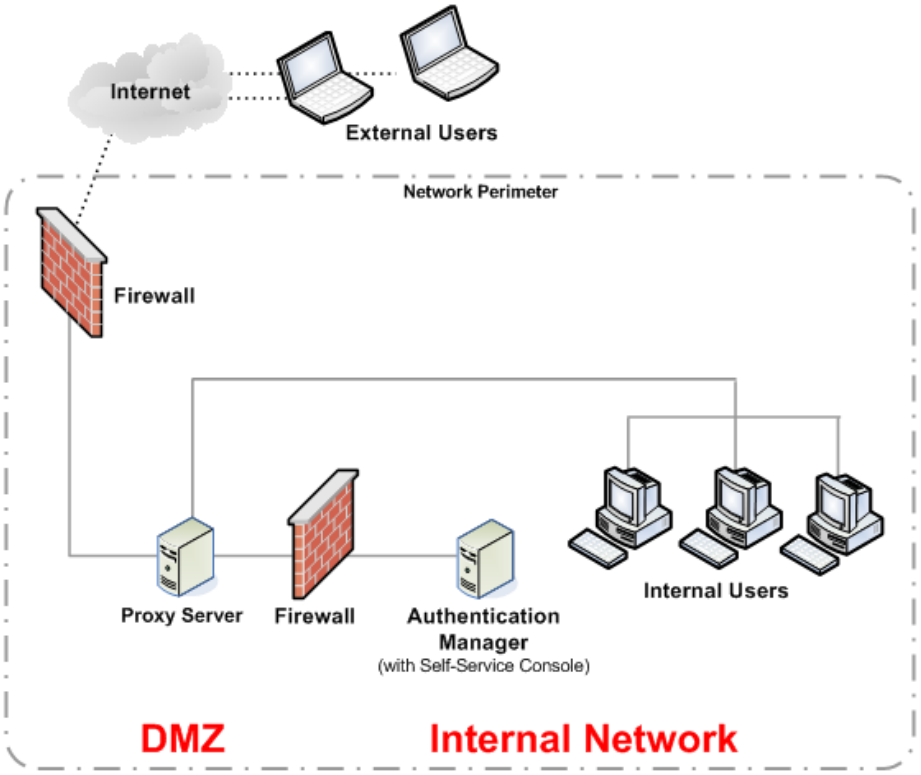
- Whether to allow users to get emergency access.
- The type of emergency access tokencodes available: temporary fixed tokencodes, one-time tokencodes, or on-demand tokencodes.
- The lifetime of emergency access tokencodes.
- The number of one-time tokencodes to issue in a set. One-time tokencodes are issued in sets. The number of tokencodes in the set is determined by your business rules.
- What happens if temporarily unavailable tokens becomes available:
  - Deny authentication with tokens.
  - Allow authentication with tokens and disable emergency access.
  - Allow authentication with tokens after the emergency access lifetime expires, and then disable emergency access.

RSA Self-Service Console Security and Disaster Recovery

Because the RSA Self-Service Console is installed on the same machine as Authentication Manager, RSA recommends that you set up a proxy server in your network DMZ to protect Authentication Manager and accept requests.

Note: If you set up a proxy server in your network DMZ to protect Authentication Manager, you must customize the e-mail notifications to replace the URL for the authentication server with information for the proxy server. For more information, see "Customizing E-mail Notifications for Proxy Servers" in the *Administrator's Guide*.

The following figure shows a basic network setup with Self-Service Console traffic directed through a proxy server.



Disaster Recovery for Users

In the case of failover, the administrator must immediately change the IP address that is associated with the Self-Service Console alias URL to that of the new primary instance. This allows users to use the same Self-Service Console URL when a primary instance is removed from a deployment and a replica is promoted. If this change is not made, the proxy server continues to try to access the original primary server, causing downtime for users.

If you do not set up an alias for the proxy server, you need to consider how you want to notify users if the primary instance goes down and the replica instance is promoted to the primary instance. The RSA Self-Service Console uses the same port as Authentication Manager. The URL for the Self-Service Console is: https://machinename:7004/console-selfservice.

If the primary instance is down, users cannot create any requests from the RSA Self-Service Console or do any other tasks until the replica has been promoted to the primary. You need to plan how you want to notify users about the new address (URL) for the RSA Self-Service Console when a replica is promoted to the primary because of the machine name change. For more information about disaster recovery, see Chapter 6, "Planning for Failover and Disaster Recovery."

Training for RSA Credential Manager Administrators and Users

Develop a plan to train your users and administrators. If you have any tasks that are unique and specific to your business, remember to add them to your list of training topics. For information about training administrators and users, see "Administrator and User Training" on page 88.

RSA Credential Manager Summary

Know the following when planning self-service and provisioning:

- Whether to deploy self-service or provisioning.
- How to notify users about self-service and provisioning.
- Implications of read/write or read-only identity sources on self-service and provisioning tasks.
- How to plan the user experience.
- Which primary logon method for the Self-Service Console to use.
- Which security domains to make available for user enrollment.
- How to customize user profiles for user enrollment.
- What authentication method to use for self-service troubleshooting.
- How and when to lock a user account for self-service troubleshooting.
- How and when to unlock a user account for self-service troubleshooting.

- How to set up a proxy server to protect Authentication Manager when allowing users access with the Self-Service Console.

In addition, you need to understand the following when planning provisioning:

- Whether to deploy provisioning.
- How to customize workflows for requests.
- Which predefined administrative roles meet your needs.
- Which user groups to make available.
- Which tokens to make available.
- How to distribute hardware tokens.
- How to use distribution reports.
- How to distribute software tokens.
- Which e-mail server port to use.
- Which e-mail address to use to send e-mail notifications.
- Which participants to send e-mail notifications.
- How to customize e-mail templates, if necessary.
- Whether to allow Self-Service Console users to request emergency access.
- What method to make available for emergency access.
- How to set the lifetime for lost or broken tokens or for temporarily unavailable tokens.
- What to do if a missing token is recovered.
- What training approvers and distributors need for requests.

The Security Division of EMC

12 Planning for RSA RADIUS Integration

Note: If you are migrating from RSA Authentication Manager 6.1 to version 7.1, refer to the *Migration Guide* for planning and installation information.

Authentication Manager may be used without RSA RADIUS to directly authenticate users attempting to access network resources. Adding RADIUS gives administrators more precise control over network access sessions, as well as more stable and more secure wireless connections. RADIUS adds these capabilities:

- RADIUS profiles monitor attributes provided with authentication requests to ensure the request meets established requirements before handling the request. Once a request is authenticated by Authentication Manager, RADIUS profiles can return attributes to network access devices that control user sessions.
- 802.1x and EAP-POTP protocols strengthen wireless access point connections. These protocols:
  - Securely pass user identity and authentication data so it is not accessible to eavesdroppers.
  - Help provide a per-user session key to protect session data from eavesdroppers.
  - Provide session resumption, which lets users roam across wireless access points. If a session is lost due to a weak or lost signal, the session is resumed without having to reauthenticate.

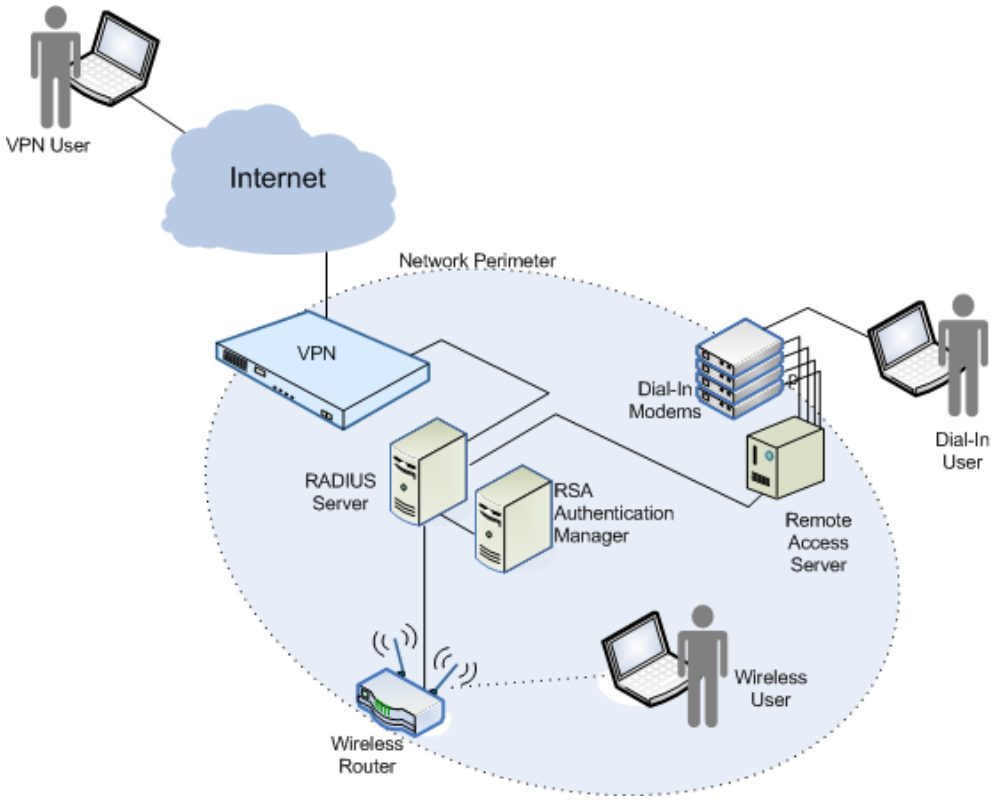
- Accounting capabilities let administrators closely track usage statistics for billing or auditing purposes.
- Administration is integrated within the RSA Security Console so administrators need to learn only one interface. Routine administration is centralized so there is no need to log on to separate RADIUS servers for most day-to-day operations. The RSA Operations Console is provided for settings that must be made on individual machines.

If you already have a RADIUS system (not RSA RADIUS), you may continue to use that system although administration requires use of that system's separate proprietary administration interface. You must configure your RADIUS system to direct RSA SecurID authentication requests to Authentication Manager. Refer to your RADIUS administration documentation for instructions on configuring the RADIUS system to communicate with Authentication Manager.

If you decide to replace a third-party RADIUS system with RSA RADIUS, special procedures are needed to move existing configuration data from the third-party RADIUS to RSA RADIUS. Contact RSA Professional Services for assistance.

Overview of an RSA RADIUS Operation

The following figure shows a simplified example of an RSA RADIUS server, positioned between users and network access devices (RADIUS clients) at the network perimeter, and Authentication Manager.



RADIUS users who want to access network resources send an access request to RADIUS. RADIUS establishes a secure connection with the user, and requests the User ID and authentication data, such as a passcode from an RSA SecurID token.

The RADIUS server forwards the authentication data to the Authentication Manager for validation. Depending on the result, the RADIUS server returns an access accept or access reject message to the RADIUS client that grants or denies access. The RADIUS server may provide additional attributes to the RADIUS client that can limit a user's session length, allowed IP addresses, or other parameters.

The figure is actually a bit more complicated as firewalls typically separate the VPN server from the RADIUS server and the Internet. Also, a single RADIUS server is shown but RADIUS replica servers are configured along with a primary server for load balancing and failover. Additional RADIUS client devices may also be configured, such as a number of wireless access points in strategic locations throughout a site.

RSA RADIUS System Requirements

The system requirements for RADIUS and Authentication Manager are the same. You can install RADIUS on the same machine as Authentication Manager. For more information, see Chapter 2, "System Requirements."

You can also install RADIUS on a separate machine. If you do this, both Authentication Manager and RADIUS must be on the same platform. For example, do not install Authentication Manager on Solaris and then install RADIUS on Windows.

The values listed for RSA RADIUS disk space and memory are in addition to those for Authentication Manager when RADIUS is installed on the same machine with Authentication Manager. When RADIUS is installed on a standalone machine, the values listed for Authentication Manager are sufficient.

Note: RADIUS is not supported on 64-bit Windows or Linux operating systems. Solaris Sparc64 is supported.

Disk Space Requirements

Note: Hard disk space requirements for running RADIUS depend on your system's product configuration.

Windows	Linux	Solaris
RADIUS server software requires adding approximately 125 megabytes of local disk space.	RADIUS server software requires adding 512 megabytes of local disk space.	RADIUS server software requires approximately 650 megabytes of local disk space.

Memory Requirements

Add 512 MB of memory to the RADIUS server software host.

Operating System Requirements

- Red Hat Enterprise Linux 4.0-1 ES (32-bit)
- Solaris 10 (64-bit)
- Microsoft Windows Server 2003 Enterprise R2 SP2 (32-bit)
- Microsoft Windows Server 2003 Enterprise SP2 (32-bit)

Supported Browsers

RSA RADIUS browser-based administration is integrated within the RSA Security Console. The supported browsers are the same as Authentication Manager. For more information, see Chapter 2, "System Requirements."

Ports

RSA RADIUS uses the following legacy and standard ports.

Port Number	Protocol	Service	Description
1645	UDP	RADIUS Authentication (legacy port)	RSA RADIUS listens on this port for authentication requests from RADIUS clients.
1812	UDP	RADIUS Authentication (standard port)	RSA RADIUS listens on this port for authentication requests from RADIUS clients.
1646	UDP	RADIUS Accounting (legacy port)	RSA RADIUS listens on this port for requests for accounting data.
1813	TCP	RADIUS Accounting (standard port)	RSA RADIUS listens on this port for requests for accounting data.

License Types

Your installation personnel need to understand how the license type impacts the installation of RSA RADIUS. See "License Types and Options" on page 65.

Planning Your Deployment

Your Authentication Manager license specifies the number of RSA RADIUS servers you can deploy. Where you deploy these systems depends on your organization's network topology.

Physical Deployment

The physical deployment of RSA RADIUS mirrors the physical deployment of Authentication Manager. That is, if your Authentication Manager deployment consists of one primary instance and one or more replica instances, your RADIUS deployment must have one primary server and one or more replica servers. This deployment is suitable for use in a single realm.

If your organization has multiple realms (see "Realms" on page 43), each realm has its own deployment of Authentication Manager. Each realm must have a complete RADIUS deployment consisting of one RADIUS primary server and one or more RADIUS replica servers. For example, if your organization has three realms, each realm needs one Authentication Manager primary instance and one or more replica instances, and one RADIUS primary server and one or more replica servers.

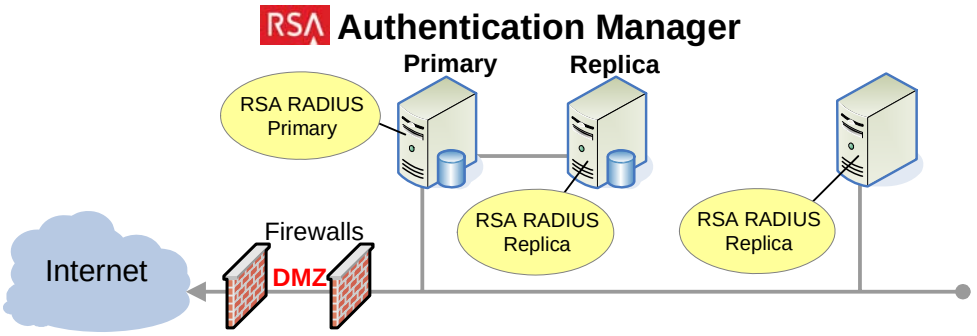
The following figure shows a possible deployment for an organization with a single realm. The realm has an Authentication Manager primary instance and one replica instance, and one RADIUS primary server and two replica servers. The additional RADIUS replica server can help in load balancing or in failover situations.

The figure also shows the RADIUS primary server installed on the same machine with the Authentication Manager primary instance and the RADIUS replica server installed on the same machine with the Authentication Manager replica instance. This is the recommended installation for these reasons:

- Latency between RADIUS and Authentication Manager is minimized as there is no network between these systems to form a bottleneck, possibly speeding up authentication traffic.
- This approach autoconfigures RADIUS to operate with Authentication Manager because the RADIUS primary server acquires the necessary communication parameters directly from Authentication Manager. If the RADIUS primary server is installed on a separate machine, additional steps are needed to provide these communication parameters. For more information, see the chapter "Installing RSA RADIUS on a Separate Machine," in the *Installation and Configuration Guid*e.

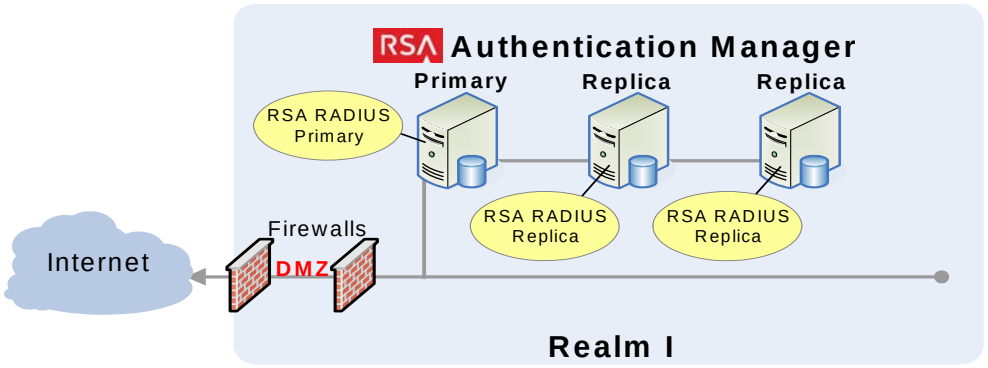
  RADIUS replica servers always acquire their communication parameters from the primary server by referencing a "replica package file" during the replica installation.
- Up to 15 RADIUS replica servers can be installed.

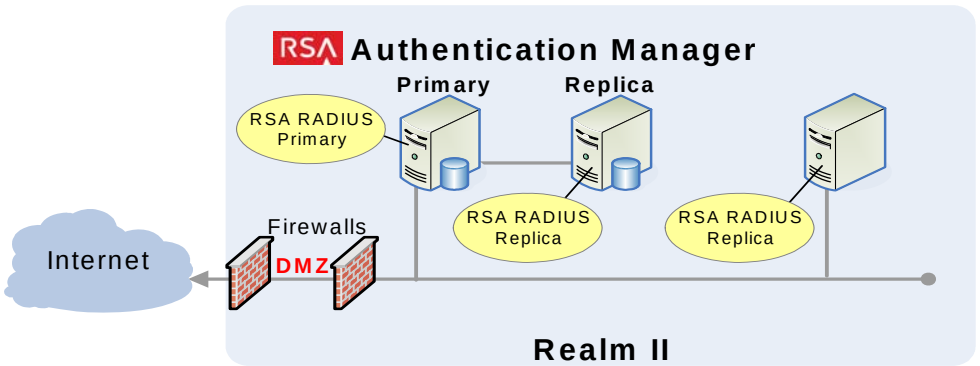
Over time you may promote RADIUS replica servers to primary servers to handle failover or system maintenance conditions. This means the strict correlation of the RSA RADIUS primary and replica servers and the Authentication Manager primary instances and replica instances shown in this figure is not necessarily preserved.



Realm Deployment Example

The following figure shows a possible deployment for multiple realms. Each realm has an Authentication Manager primary instance and at least one replica instance, and one RSA RADIUS primary and two replica servers. The Enterprise Server license (required for multirealm deployments) allows up to 15 RADIUS replica servers.



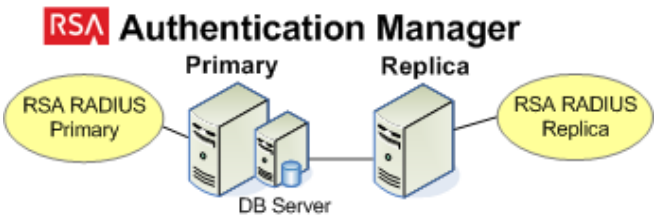


System Performance Guidelines

RSA RADIUS is a database transaction-based application that is closely bound to disk performance. Authentication Manager caches more data than RADIUS and relies more heavily on memory operations for performance. The number of RADIUS servers needed to support a given number of users depends how RADIUS is deployed within the overall deployment configuration of Authentication Manager.

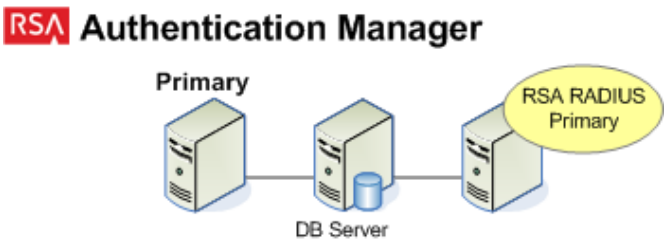
1. Two replicated, integrated servers (provides a low-end, realistic number):

   Authentication Manager + Authentication Manager internal database + RADIUS (x2 - one primary server, one replica server)



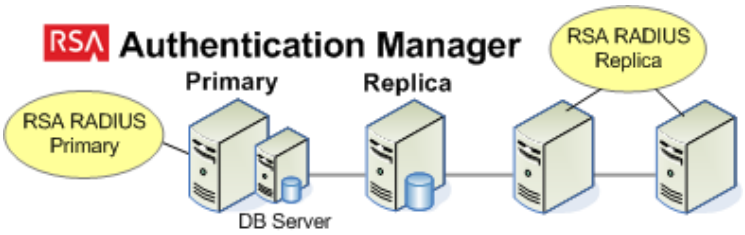
2. Three non-replicated standalone servers (should provide the best number, but it is not realistic):

   Authentication Manager (primary instance), Authentication Manager internal database (primary instance), RADIUS (primary server)



3. Five replicated servers. Three standalone, two integrated (should provide good numbers with the most realistic configuration):

   Authentication Manager (primary instance), Authentication Manager internal database (primary instance), RADIUS (primary server), Authentication Manager + Authentication Manager internal database + RADIUS (x2 - replica servers)



The number of machines that is right for your organization depends on your expected peak RADIUS authentication load, balanced by what you determine is an acceptable authentication time for users (the number of seconds between the access request and the response to a user).

If your system configuration seems appropriate, but the authentication response time at peak authentication times needs further improvement, consider adding another replica, or contact RSA Professional Services for further guidance.

If your deployment has multiple geographic locations, consider installing at least one Authentication Manager replica instance and one RADIUS replica server in each geographic location so that authentication traffic can be handled locally. If authentication traffic must always traverse a wide-area network, inherent latencies can slow down authentications.

Load balancing is maintained by the RADIUS client devices that each contain an address table for all RADIUS servers. These RADIUS-enabled devices choose servers from that table in a manner to distribute the workload evenly across available servers.

Planning for Failover and Disaster Recovery

You can protect yourself from system disasters by installing replica servers that can be promoted to primary servers if a primary server stops responding or is taken offline for some reason.

For many situations, the redundancy of RADIUS configuration information on RADIUS replica servers satisfies backup needs. If one server is lost, a replica can be promoted to a primary. This results in losing only those changes made since the most recent replication. Consider the number of replica servers needed to minimize data loss if a server fails or is taken offline. This approach does not back up customized configuration files, initialization files, or dictionary files.

To support disaster recovery, perform full system backups and store that backup data in an off-site location. To recover from a disaster, restore the data from the off-site location. For more information, see the chapter “Managing RSA RADIUS” in the *Administrator’s Guide*.

If you operate in multiple geographic locations, be sure each location has at least one Authentication Manager instance and one or more RADIUS servers so authentication can be handled locally in each location.

Schedule regular full system backups that include your RADIUS configuration data as well as customized initialization files, dictionary files, and configuration files. You can restore this data from an off-site location in a disaster recovery situation.

If RADIUS authentications stop working, use the event logs and perform test authentications to isolate and recover from the problem.

Installation and Configuration Overview

Installation of RSA RADIUS is controlled in part by the installation program. When you start the installer, it scans the machine for existing Authentication Manager and RADIUS products and displays installation choices based on what it finds on the machine. For installation procedures, see the chapter "Installing an RSA Authentication Manager Primary Instance" in the *Installation and Configuration Guide*.

You can install RADIUS along with Authentication Manager by selecting "Enable RSA RADIUS" from the installation choices. If you do not want to install RADIUS, simply do not select it as an optional feature during the Authentication Manager installation process.

You can install RADIUS on a separate machine by selecting "Install RSA RADIUS" from the installation choices.

If you want to install RADIUS on your Authentication Manager machine, RSA recommends doing so when you first install Authentication Manager. If you want to install RADIUS on your Authentication Manager machine at a later date, you must:

- Back up the Authentication Manager primary instance
- Uninstall Authentication Manager
- Reinstall Authentication Manager with the RADIUS option
- Restore the primary instance from the backup

RSA recommends installing RADIUS on the same machine with Authentication Manager. For example, install your RADIUS primary server on your Authentication Manager primary instance, and install your RADIUS replica servers on your Authentication Manager replica instances. This minimizes latency between these systems and autoconfigures RADIUS to communicate properly with Authentication Manager.

When you know authentication is working between RADIUS and Authentication Manager, you can perform an end-to-end test authentication. This involves an actual user authenticating with an RSA SecurID token. For many deployments, the RADIUS default settings suffice, but you may need to configure the RADIUS client devices (VPN server, network access server, or wireless access points) with the IP address of the RADIUS server being tested. You may need to perform some configuration of RADIUS for customized or specialized environments.

Planning for Administration

Administrators need to know how to access RADIUS for administration and what actions they can perform. Users need no special knowledge of RADIUS.

Administration Interfaces

RSA RADIUS administration is integrated with Authentication Manager in that it uses the RSA Security Console for routine operations. Persons having the same access as Authentication Manager administrators can manage RADIUS. No additional authentication is needed to access the RADIUS administration pages.

Authentication Manager also has an RSA Operations Console for use in managing system-specific settings like starting and stopping servers, promoting a RADIUS replica server to a primary server, and editing RADIUS initialization and dictionary files. Any customizations made to these files must be repeated on other RADIUS servers. Administrators accessing this interface need a local account on each RADIUS server.

User and Administrator Training

No special training is needed for users beyond using their RSA SecurID tokens. Token usage is covered in the training for users using RSA Authentication Manager. See "Administrator and User Training" on page 88.

Administrators need to understand how RADIUS profiles help RADIUS client devices enforce network access controls. This knowledge is needed to properly create and manage profiles. For more information, see the chapter "Managing RSA RADIUS" in the *Administrator's Guide*.

Administration Activities

If you are installing RSA RADIUS for the first time (not replacing a third-party RADIUS system or migrating from an earlier version of RSA RADIUS), plan to spend some time setting up profiles relevant for your environment and associating users, user aliases, agents, and perhaps trusted users (if you are using trusted realms) with profiles. You may also assign RADIUS user attributes to your users.

Once profile and user associations are complete, administrators only need to maintain them, adding or removing user associations as people come and go in the organization.

If you acquire specially customized RADIUS clients (network access devices such as VPN servers or wireless access points), administrators may need to add or modify RADIUS initialization, dictionary, or configuration files so RADIUS can interoperate properly with the new device. See your RADIUS client documentation and the *RADIUS Reference Guide* for details.

Conducting a Pilot Test

You can conduct a pilot test of RSA RADIUS to test the RADIUS installation and perform a test authentication in advance of your live deployment.

Other advantages include safely testing:

- Devices
- System connections
- Disaster recovery
- Administrative tasks

Consider the following when you plan your pilot test:

- The scope of the test
- How much hardware you will need
- How much disk space is required
- Your time frame for staging and performing the test
- The types of disaster recovery to test
- The number and types of authentication to test

Migrating from RSA RADIUS Server 6.1

If you are migrating from RSA RADIUS Server 6.1 to version 7.1, refer to the *Migration Guide*.

RSA RADIUS Summary

Know the following when planning RSA RADIUS:

- How and where to install RSA RADIUS in each security domain where it will be used.
- How to configure RSA RADIUS to accept authentication requests from any other RADIUS client device, if necessary.
- How to secure RSA RADIUS equipment, physically and logically.
- How to create a user account on the machine where RSA RADIUS is installed.
- How many RSA RADIUS servers to install to handle your peak load.
- How to plan for failover and disaster recovery.
- When to perform database backups and where to store them.
- Which personnel (administrators, installers) need RADIUS training.
- How to conduct a pilot test.

13 Planning for Emergency Access

Emergency Access

Determine how you want online and offline users to authenticate when they do not have their assigned tokens in their possession.

Users occasionally lose, misplace, or damage their tokens. While a damaged token is an inconvenience for the user, a lost or stolen token compromises the security of the system because it can end up in the hands of an unauthorized individual who may attempt to authenticate.

Regardless of the exact circumstances, users still need to authenticate, even without a token. In these situations, authentication is still possible with the use of online and offline emergency access tokencodes and passcodes. Similar to a tokencode generated by an RSA SecurID token, the emergency access tokencode is generated by Authentication Manager and assigned to the user. Offline users who do not have their PIN can receive an emergency passcode, if their machines are enabled in advance.

While emergency access tokencodes and passcodes provide a quick and convenient way to deal with a typical problem, they do open the system up to additional risks. Emergency access tokencodes and passcodes are fixed, therefore not as secure as the dynamic ones generated by a token. To alleviate any security concerns, Authentication Manager allows you to set restrictions on how the system handles emergency access tokencodes on a user by user basis. There is no system-wide policy governing the behavior of emergency access tokencodes. The administrator handling a particular situation determines the appropriate behavior for that situation. For more information, see the chapter "Configuring Authentication Policies" in the *Administrator's Guide*.

Another method of emergency access is the Business Continuity option, which enables you to temporarily increase your number of RSA SecurID users. For more information, see "Business Continuity Option" on page 147.

For information about emergency access for self-service users, see "Emergency Access" on page 128.

The following tables describe the emergency access methods and lists where to find more information.

For Online Users

Method	Description	Characteristics	More Information
Temporary fixed tokencode	Users whose computers are online with the network can access their protected computers without a tokencode (for example, when they have lost their tokens).	• Must be combined with the user's RSA SecurID PIN. • Created automatically by Authentication Manager. • Valid until the user's lost token status is changed.	See the chapter "Administering Users" in the *Administrator's Guide*.
One-time tokencode	Users whose computers are online with the network can access their protected computers with a tokencode that allows one access. One-time tokencodes are issued in sets. The number of tokencodes in the set is determined by your business rules.	• Must be combined with the user's RSA SecurID PIN. • System generated by an Authentication Manager administrator. • Each tokencode in the set is valid one time.	See the chapter "Administering Users" in the *Administrator's Guide*.
On-demand tokencode	Users with digital mobile devices and home e-mail accounts can receive one-time tokencodes as text messages.	• Must be combined with the PIN for the user's authenticator. • User's digital mobile devices and e-mail accounts must be enabled to receive on-demand tokencodes.	See the chapter "Protecting Network Resources with RSA SecurID" in the *Administrator's Guide*.

For Offline Users

Method	Description	Characteristics	More Information
Offline emergency access tokencode	Users whose computers are not connected to the network can access their protected computers without a tokencode (for example, when they have lost their tokens).	• Must be combined with the user's RSA SecurID PIN. • System generated by an Authentication Manager administrator. • Valid until a successful online authentication is performed.	See the chapter "Administering Users" in the *Administrator's Guide*.
Offline emergency access passcode	Users whose computers are not connected to the network can access their protected computers without a PIN (for example, when they have forgotten their PINs).	• Used in place of a PIN and a tokencode. • Valid for one authentication only.	See the chapter "Administering Users" in the *Administrator's Guide*.

Business Continuity Option

If you have a situation where you need your employees who are not RSA SecurID users to access your network, the Business Continuity option enables you to temporarily add them to your Authentication Manager license. For example, you may want to temporarily add RSA SecurID users when:

- Water damage in a building requires all your employees to temporarily work from home.
- A hurricane is approaching the coast, your offices have been evacuated, and all your staff must work from home.
- A major influenza outbreak has made it mandatory that your employees stay home.

In all of these situations the number of remote access users goes up dramatically but only for a short duration. The Business Continuity option enables on-demand authentication for a short period of time for a large number of users. Enabled users can receive one-time tokencodes by way of their mobile devices or home e-mail addresses. This provides continuity for your business operations.

RSA recommends that for users created with the temporary license, you enable them to receive on-demand tokencodes so that you do not have to assign tokens to them. However, if you want, you can assign them RSA SecurID tokens.

Emergency Access Summary

Know the following when planning emergency access:

- How online users can authenticate without their assigned tokens.
- How offline users can authenticate without their assigned tokens.
- What to do if a missing token is recovered.
- How to set restrictions for how the system handles emergency access tokencodes.

14 Logging and Reporting

Logging and Reporting in RSA Authentication Manager

Consider which logging and reporting options you want to use. Audit information about all significant aspects of any administrative or runtime action performed by an administrator or user in a single deployment is recorded in the internal database. The system also provides a decentralized tracing log capability, per component, to help you resolve issues at the local level.

Review the following Authentication Manager tools and consider how you want to manage logging and reporting.

Tool	Description
Standard reports	There are a number of report templates, which you can modify and save through the RSA Security Console. You can send saved reports to other administrators for use in their security domains.
Event logging	The system automatically logs all authentication and administrative events and stores them in a database. You can encrypt the information that is stored in the log entries, as well as the logging information that is transferred between each component and the internal database.
Activity monitor	This tool enables you to view authentication and administration activity in real-time. It is especially useful for resolving user's issues because you can watch their activity, as they attempt to use the system.
Log signing	Log signing enables you to sign by log type, for example, Admin, System, Runtime. You must decide to enable this upon installation. Log signing is typically used on Admin and Runtime logs. Use the Verify Archive Log utility to confirm that signed logs have not been altered, for example, for compliance purposes. **Note:** You cannot enable or disable log signing after installation.

Permission to view logs is controlled by the security domain. Administrators can view only the log messages for the security domains within their administrative scope.

Permission to run reports is controlled by administrative roles.

Logging in RSA RADIUS

Audit information about all significant aspects of any administrative or runtime action performed by an administrator or user in a single deployment is recorded in the internal database. For more information see the previous section, "Logging and Reporting in RSA Authentication Manager."

All authentication attempts and responses using RADIUS are recorded in the RADIUS accounting logs. Configuration files let you choose exactly which accounting statistics or events you want to capture.

Permission to view logs in the internal database is controlled by the security domain. Administrators can view only the log messages for the security domains within their administrative scope. Permission to run reports is controlled by administrative roles.

An administrator who can access the Security Console RADIUS functions can view authentication statistics.

Planning Log Maintenance

Consider how you want to manage your log files. Authentication Manager automatically logs all authentication and administration events.

There are four types of log files generated by the system.

Log	Description
Audit information	Includes the date and type of action performed, which are used to validate a certain state of the data. Authentication and authorization policies are based on the state of the data.
System information	Provides information about the environment, internal processes, state, or events in the system. For example, activation or deactivation, connection refresh, or reclaim events.
Runtime information	Includes any runtime activity, such as authentication and authorization of users.
Trace information	Used for resolving user issues in a production deployment, where code debugging is not possible. Trace logs usually capture enough information to help you follow the thread of execution with appropriate contextual data.

All audit log messages are sent to the Authentication Manager internal database for storage. You cannot filter audit log messages. You can only filter trace log messages that appear to the users at the time of the event. Use your log monitor to filter the following trace log attributes:

- Admin User ID
- Security domain
- Affected User ID
- Authenticator serial number
- User group
- Authentication agent hostname
- Authentication Manager instance

Planning for audit log maintenance includes selecting a rotation scheme to help you manage the size of the file that contains all of the administrative, system, and runtime messages. Authentication Manager provides these file rotation schemes:

- Never rotate log file
- By file size
- On schedule

Plan to specify a maximum file size, the number of files to back up, and polling frequency.

Log Archiving

Archiving is the process by which log records are converted to flat files, removed from the database, copied onto external media, and moved to a long-term storage location. Without archiving, logs grow until they consume all available disk space. A large site with many authentications per hour fills up quickly, while a smaller site might fill disk space more slowly. Use the Security Console for log archiving.

Important: Once all disk space is consumed, Authentication Manager may stop operating and be difficult to restore. You must devise policies and procedures to ensure that logs are archived from the database and moved to external media on a regular basis. You can use the Security Console to create log files and set up recurring archive jobs.

Consider these questions:

- How often do you need to archive log files? Consider your company's particular audit trail requirements and the amount of disk space available for logs in the database.
- How often will you purge logs from the archive? Consider how much disk space is available in the archive, and how often you expect to access the archived logs.
- What is the maximum length of time you want to capture in each log file? This decision affects the size of each file and the total number of log files. The number of files equals the total time stored in archive files divided by the maximum file size, rounded up to the nearest integer number of files.

  For example, if the offline storage time is 180 days and the default log size is 30 days, six logs are created over time.

  Consider these things:

  – How often to archive data?
  – Available disk space
  – The volume of data being archived
  – How you will access the logs if you need them

You can choose to use fewer (larger) log files, or more (smaller) log files.

You can also export logs to third-party systems.

Log Consolidation

The system provides a mechanism to consolidate all Authentication Manager log files in your realm. Consider how you want to manage your files.

Each replica instance automatically sends its log files to the database in the primary instance. In this way, all of your Authentication Manager logs are consolidated into one database. Note that this service does not include any operating system log files originating in the replica instances because those are not automatically sent to the primary instance. They remain on the replica instance. You may want to configure your Network Management Server to retrieve such information.

If you want any of your Authentication Manager log files sent to your system log, you can configure the primary instance to send messages to the Windows Event Log or Linux Syslog. For instructions, see the Security Console Help topic "Configure Logging."

If the physical location of the log files is a concern in your deployment plan, perhaps because a key administrator is in a certain location, consider where you locate your primary instance because that is also where your consolidated log file is located.

SNMP Trapping

If your company utilizes a Network Management System (NMS), consider enabling the SNMP agent for your Authentication Manager instances and using the NMS to monitor critical events and overall system health. For instructions on enabling network monitoring, see the Security Console Help topic “Configure for SNMP Trapping.”

Report Scheduling

The information that you can query for a report is controlled by your administrative scope. The scope of the data collected in a report is governed by either of the following:

- Administrative permissions of the administrator executing the report
- Administrative permission of the Run-As identity in the report definition

If you plan to delegate running reports to other administrators, be sure that you trust them to view all of the information that they can see in such reports. Consider designing delegated reports in a way that limits the kinds of information that others can view, and select only your most trusted administrators to run them.

Available Reports

Authentication Manager includes a variety of report templates, which you can customize from the Security Console to meet your requirements. Note that there are several new reports in RSA Authentication Manager 7.1. As you plan your deployment, consider which reports you need. For more information, see the chapter “Logging and Reporting” in the *Administrator’s Guide*.

Scheduling Reports

You can run reports manually at any time, or you can schedule them to run automatically at predetermined times. This enables you to meet any requirements for recurring reports, while enabling you to run reports in response to unplanned requests. Both tasks are accomplished through the Reporting tab in the Security Console.

Logging and Reporting Summary

Know the following when planning logging and reporting:

- What reporting or logging options are available.
- How to create custom reports from the Authentication Manager report templates.
- How to assign permission to view logs to appropriate administrators.
- How to perform log file management and maintenance.
- How to enable SNMP trapping, if you use a Network Management System.
- How to schedule reports.

15 Completing the Deployment Checklist

Use the following checklist to specify installation, configuration, and administration information for your deployment. If you need more information about items on this list, refer to the appropriate chapter in this guide. RSA recommends that you complete this checklist and distribute it to the appropriate personnel for your deployment. Save a copy of the completed checklist in a secure location for future reference.

Note: Some of the information that you enter in this checklist may be sensitive. Consult your company's policies before entering sensitive information, such as a password, in this checklist.

Pre-Installation

Element	Description	Your Plan
License or option type	• Base Server • Enterprise Server • Business Continuity option • Credential Manager Provisioning option	
Platform	• Microsoft Windows Server 2003 Enterprise R2 SP (32-bit) • Microsoft Windows Server 2003 Enterprise SP2 (32-bit) • Microsoft Windows Server 2003 Enterprise R2 SP2 (64-bit) • Microsoft Windows Server 2003 Enterprise SP2 (64-bit) • Red Hat Enterprise Linux 4.0-1 ES (32-bit) • Red Hat Enterprise Linux 4.0-1 ES (64-bit) • Solaris 10 (64-bit) **Note:** RADIUS is not supported on 64-bit Windows and Linux systems.	

Element	Description	Your Plan
Master password		
Super Admin user name	Authentication Manager Super Admin user name	
Super Admin password	Authentication Manager Super Admin password	

Installation

Element	Description	Your Plan
Primary instance	Physical location	
	Name and IP address of the database server	
	Name and IP address of any server nodes	
Replica instance	Number of instances	
	Physical location(s)	
	Name and IP address of the database server	
	Name and IP address of any server nodes	

Identity Source Configuration

Element	Description	Your Plan
Identity source	Number and type For example: • RSA Authentication Manager internal database – Same machine as primary – Standalone machine • Active Directory • Sun Java System Directory Server Select the identity sources to make available for self-service and provisioning	
LDAP	User defined unique identity source name	
	URL of the LDAP identity source	
	URL of the failover identity source (optional)	
	LDAP server user name	
	LDAP server password	
	Read/write access or read-only access	

Administrative Configuration

Element	Description	Your Plan
Realm	Number	
	Names	
Security domain	Top-level name **Note:** The top-level security domain in a realm has the same name as the realm. This name cannot be changed.	
	Lower-level names	
Tokens	Number and type For example: • RSA SecurID token • RSA Smart Card • RSA SecurID Software Toolbar Token • RSA USB token	
	Contact person for obtaining token seed records	
Policies	Number of custom policies	
	Names of security domains requiring custom policies	

Element	Description	Your Plan
	Method of PIN creation For example: • System-generated • User-generated	
	Length of PINs (4-8 characters)	
	Character restrictions on PINs	
	Number of failed authentication attempts allowed before user lockout	
	Method of unlocking locked user. For example: • Automatic • Manual	
	Password lifetime	
	Maximum and minimum password length	
	Number of restricted old passwords	
	Excluded words dictionary	
	Character restrictions on password	
	Lifetime of Emergency Access Tokencodes	
	Behavior of Emergency Access Tokencode when token is recovered For example: • Deny authentication with the token • Allow authentication with the token and disable the Emergency Access Tokencode • Allow authentication with the token only after the Emergency Access Tokencode expires	

Administrative Configuration for Self-Service and Provisioning

Element	Description	Your Plan
Logon Method	• RSA password • LDAP password • SecurID token	
User Enrollment	• Select identity sources. • Select security domains. • Customize user profiles. • Customize the RSA Self-Service Console Home page.	
Self-Service Troubleshooting	Authentication methods: • Security questions • Passwords • None Number of self-service authentication attempts: • Allow an unlimited number of failed self-service troubleshooting authentication attempts. • Allow a specified number of failed attempts within a specified number of days, hours, or minutes. Method of unlocking locked user for self-service troubleshooting: • Unlock accounts after users have exceeded the number of failed attempts specified. • Allow the system to automatically unlock accounts after a specified number of days, hours, or minutes.	
Proxy Server for self-service requests	Set up proxy server in your network's DMZ to protect Authentication Manager.	

Element	Description	Your Plan
Additional Administrative Configuration for Provisioning		
Workflows	For each type of request, set: • One or two approval steps • One distribution step for hardware token requests • Optionally, add one distribution step for software token requests	
Roles for Requests	• Create approvers • Create distributors	
User Group Membership	Select user group membership to make protected resources available for requests. For example: • HR • Finance	
Tokens	Select tokens to make available for provisioning requests. For example: • RSA SecurID token • RSA Smart Card • RSA SecurID Software Toolbar Token • RSA USB token Optionally, select a default token. Decide when to allow requests for replacement tokens. Optionally, make the on-demand tokencode service available. Optionally, make the on-demand tokencode service the default.	

Element	Description	Your Plan
Hardware token distribution	Plan distribution reports for tokens. Optionally, customize distribution reports. Plan how to collect shipping addresses from users. • Map an attribute in an directory server for the shipping address. • Create a custom attribute in an directory server. • Allow users to enter shipping addresses.	
Software token distribution	Protect token files. Decide the file format: • ZIP format • SDTID format	
E-mail notifications	Set up an e-mail server: • Determine which SMTP port to use. • Decide the e-mail address from which Credential Manager sends e-mail notifications. • Determine if the e-mail server requires User ID and password. Optionally, customize e-mail templates. Select e-mail notification recipients. • All workflow participants • Super Admins • Workflow participants in the parent security domain	

Element	Description	Your Plan
Emergency access	Allow users to get emergency access. Set method to authenticate: • Temporary fixed tokencode (TFT). • One-time tokencode (OTT). • Decide the number of one-time tokencodes to issue in a set. • On-demand tokencode. Set the lifetime of emergency access tokencodes. • For lost or broken tokens • For temporarily unavailable tokens Method if a missing token is recovered. • Deny authentication with tokens. • Allow authentication with tokens and disable emergency access. • Allow authentication with tokens after the emergency access lifetime expires, and then disable emergency access.	

Post-Installation

Element	Description	Your Plan
Resources to protect	For example: • File servers • Databases • Identity sources	
Agents	Number	
	Physical location of agents	
	Name and IP address of agents	

A Terms and Concepts

Selected Terms and Concepts

The following terms and concepts are unique to Authentication Manager. They are presented here because they require more explanation than is possible in a Glossary definition, or are too long to insert inline in the body text of this document.

Deployment

A deployment is the arrangement of Authentication Manager instances into appropriate locations in a network to perform authentication.

Realm

A realm is a hierarchy of organizational units, called security domains, for administrative purposes. A realm includes all the objects that your administrators need to manage in Authentication Manager, including users, user groups, identity sources, tokens, policies, and more.

Security Domain

In Authentication Manager, a security domain is an organizational container that defines an area of administrative management within a realm. Security domains can be organized in terms of business units, for example, departments or partners. They establish ownership and namespaces for objects (users, roles, permissions, and so on) within the system. Security domains are hierarchical.

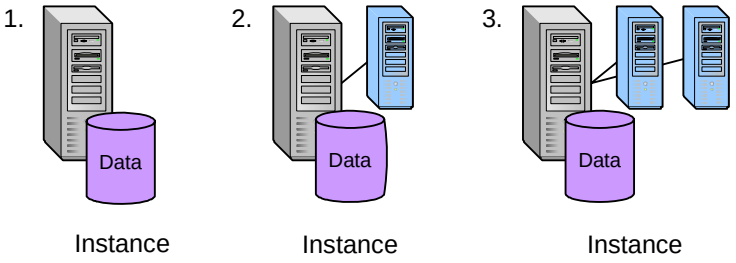
The following figure shows the concepts of realm and security domain.

Instance

An instance is one physical installation of Authentication Manager acting as a single cohesive processing unit. An instance can contain the database server (which is considered a server node) alone, or it can contain the database server with additional server nodes. The following figure shows these sample instances:

1. Database server
2. Database server with one additional server node

3. Database server with multiple additional server nodes



Server Node

A server node is an installation of Authentication Manager on a single server host. Each instance has one server node that contains the internal database. You can add additional server nodes to an instance to increase authentication performance. The additional server nodes cannot operate alone because they do not contain the internal database. You must connect the additional server nodes to the database server.

In the preceding figure, the data icon represents the database server. The small central processing unit icon represents an additional server node.

In deployments that use LDAP directories, the database server is connected directly to the LDAP directory server.

Primary Instance

The primary instance is where authentication and all administrative actions occur. You must designate one instance as the primary instance for your deployment. All other instances in the deployment are replica instances.

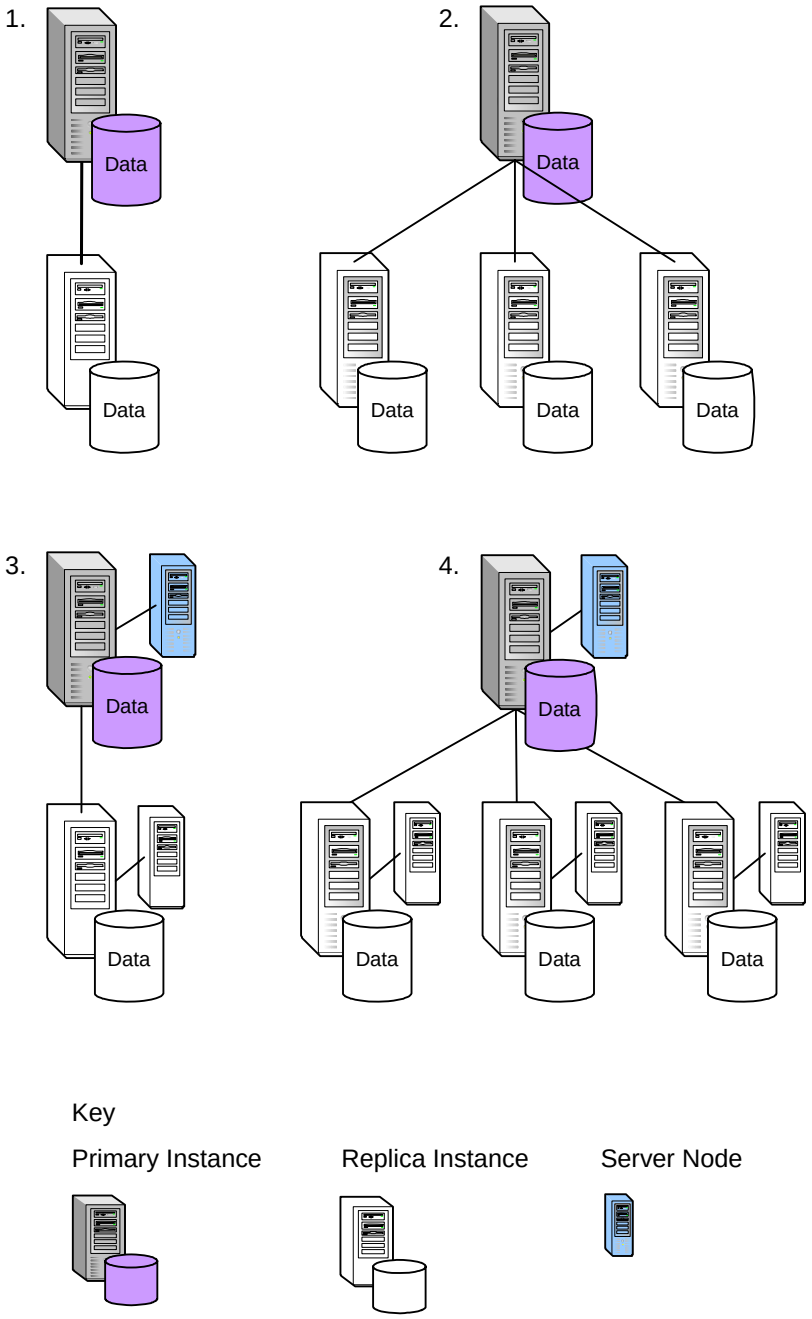
Replica Instance

The replica instance is a copy of your primary instance. You can view, but not update, administrative data on a replica instance.

The following figure shows these sample deployments containing primary and replica instances:

1. A single server node primary instance with a single server node replica instance
2. A single server node primary instance with multiple single server node replica instances
3. A multiple server node primary instance with a multiple server node replica instance

4. A multiple server node primary instance with multiple replica instances with multiple server nodes



Agent

An agent is a software application installed on a device, such as a domain server, web server, or desktop computer, which enables authentication communication with Authentication Manager on the network server.

An agent protects the device on which it is installed. When a user attempts to log on, the agent passes the user's logon credentials to Authentication Manager. Based on the pass or fail information that the agent receives from Authentication Manager, it either allows or prevents the user from accessing the device.

B Sample Deployment Scenarios

Overview

This appendix describes sample deployment scenarios for RSA Authentication Manager 7.1. These are fictitious representative companies to show you examples of Authentication Manager deployments.

Acronyms Used in this Document

IAS. Microsoft Internet Authentication Service provides centralized user authentication and authorization, centralized auditing, and accounting.

OWA. Outlook Web Access is a webmail service of Microsoft Exchange Server, used to access e-mail, calendars, contacts, tasks, and other mailbox contents.

PAM. Pluggable authentication modules are used to integrate multiple authentication schemes into an application programming interface API. This allows developers to write authentication programs independently of the underlying authentication scheme.

RADIUS. Remote Authentication Dial-In User Service is an authentication, authorization, and accounting protocol for network access.

VPN. A Virtual Private Network is a private communications network used to communicate over a public network.

DMZ. The Demilitarized Zone is the part of a network between an organization's internal and external networks. The DMZ typically contains resources accessible to users outside the organization's network, such as proxy servers.

RSA Authentication Manager 7.1 Licensing Options

There are two essential license types defined: Base Server and Enterprise Server. The following table compares the features of the license types..

License Feature	Base Server	Enterprise Server
Number of users	Specified by customer at time of purchase	Specified by customer at time of purchase
Number of instances	2[1]	15
Allows multiple realms?	No	Yes

License Feature	Base Server	Enterprise Server
Allows clusters?	No	Yes
RSA Credential Manager self-service	Yes	Yes
RSA Credential Manager provisioning	No	Yes
On-demand tokencode service	Optional	Optional
RADIUS	Yes	Yes
Business Continuity	Optional	Optional
Allows offline authentication?	Yes	Yes

[1]Licenses with a two instance limit allow a third instance for disaster recovery situations.

Summary of Scenario Elements

The following table lists the common elements in the four scenarios and the specifics of those common elements.

Element	Scenario 1	Scenario 2	Scenario 3	Scenario 3
License type	Base Server	Enterprise Server	Enterprise Server	Enterprise Server
Number of users	50	2,500	15,000	50,000
Primary instances	1 database server	1 database server and 1 additional server node	1 database server and 1 additional server node	3 database servers and 2 additional server nodes
Replica instances	1 database server	1 database server and 1 additional server node	3 database servers and 3 additional server nodes	6 database servers and 6 additional server nodes
Realms (top-level security domains)	1	1	1	3
Lower-level security domains	None	3 (Finance, HR, R&D)	3 (Boston, New York, San Jose)	9 (New York – Finance, Sales, HR; London – Finance, Sales, HR; Tokyo – Sales, HR, Engineering)

Element	Scenario 1	Scenario 2	Scenario 3	Scenario 3
Geographic locations	1	1	3 (Boston, New York, San Jose)	3 (New York, London, Tokyo)
Number of administrators	2	4	6	12
Number of IT support staff	0	20	50	150
Authentication Manager software platforms	Windows 2003 SP2	Windows 2003 R2 SP2	Windows 2003 SP2	Windows 2003 SP2 RedHat Linux 4.0 Solaris 10
Identity source (user and user group data)	Authentication Manager internal database (read/write access)	Microsoft Active Directory (read/write access)	Sun Java System Directory Server (read-only access) Microsoft Active Directory (read-only access)	Sun Java System Directory Server (read-only access) Microsoft Active Directory (read-only access)
Authentication method for internal users	Password	RSA SecurID for Windows Local Authentication Client	RSA SecurID for Windows Local Authentication Client	RSA SecurID for Windows Local Authentication Client
Authentication method for external users	RSA SecurID	RSA SecurID	RSA SecurID	RSA SecurID
Policies	Default	Default Custom	Default Custom	Default Custom
RSA Credential Manager components	Self-Service	Self-service Token provisioning	Self-service Token provisioning	Self-service Token provisioning

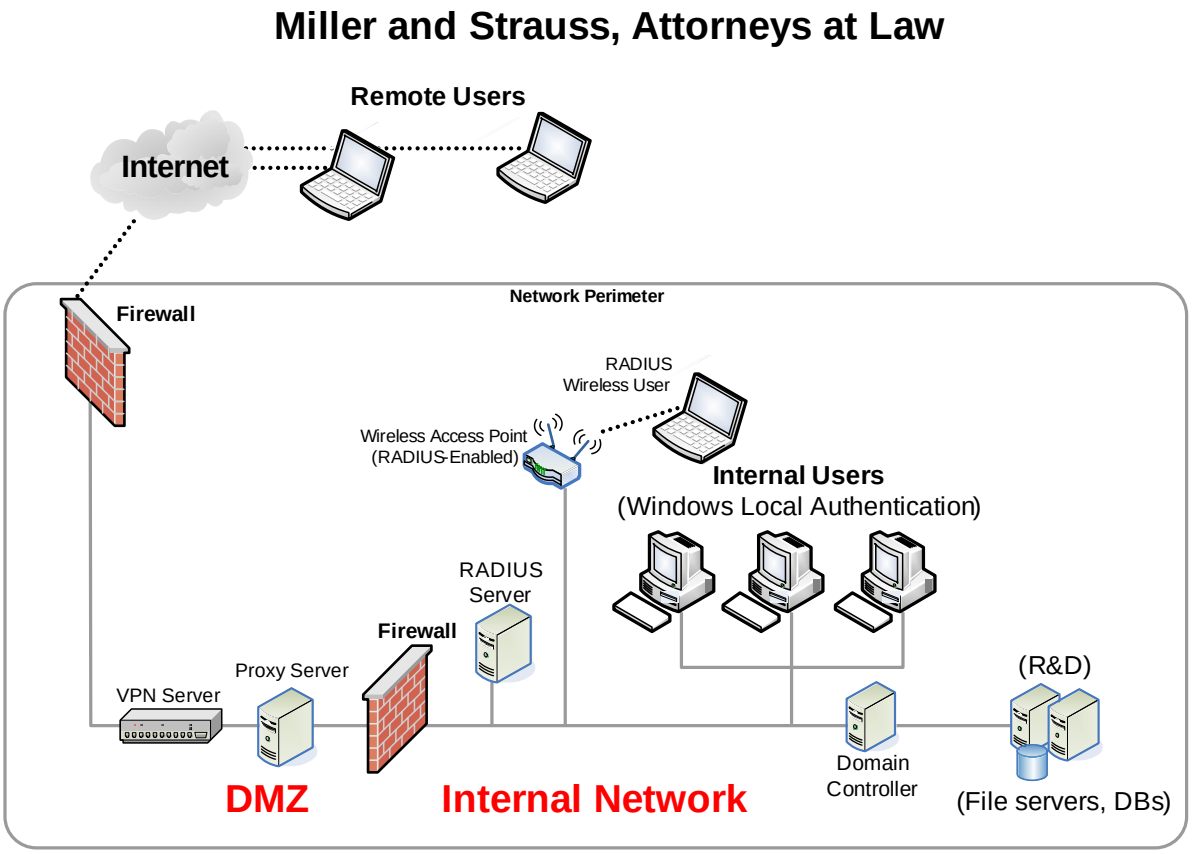
Scenario 1: Secure Remote and Wireless Access for a Small, Single Site Business

Miller and Strauss, Attorneys at Law (a single office location with 50 employees)

Miller and Strauss, Attorneys at Law, is a small private law firm with 50 employees. As a private company, they have no specific Sarbanes-Oxley compliance requirements. However, for legal liability reasons, they need to maintain records of all business and network transactions.

The firm has a small, Windows-based network managed by two full-time IT administrators. The network includes a Windows domain controller inside the corporate firewall, which contains a variety of file and print servers, and a client database. It also includes a wireless router connected to a RADIUS server. In the DMZ, the network includes a VPN server and a proxy server. The firm currently uses password authentication for all network access, inside the corporate firewall, for wireless access, and remotely through a VPN.

The following figure shows the initial network topology for a small, single-site organization.



Business Needs

Miller and Strauss' needs are:

Secure remote and wireless access. For partners, associates, and certain other employees, enable secure remote and wireless access to sensitive and confidential client files.

Auditing and non-repudiation. For legal and compliance reasons, the firm also needs an audit trail and non-repudiation by persons accessing these files (meaning whoever accesses these files cannot claim that it was someone else).

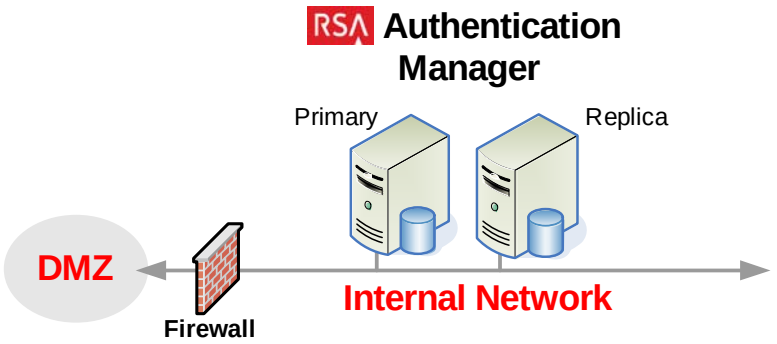
How RSA Products Are Deployed to Satisfy Business Needs

Physical Deployment

Miller and Strauss purchased RSA Authentication Manager 7.1 with a Base Server license. They installed the Authentication Manager primary instance (for authentication) and one replica instance (for failover) behind the corporate firewall.

The firm uses the Authentication Manager internal database as the sole identity source. Administrators manually assigned and distributed RSA SecurID tokens to all 50 employees of the firm.

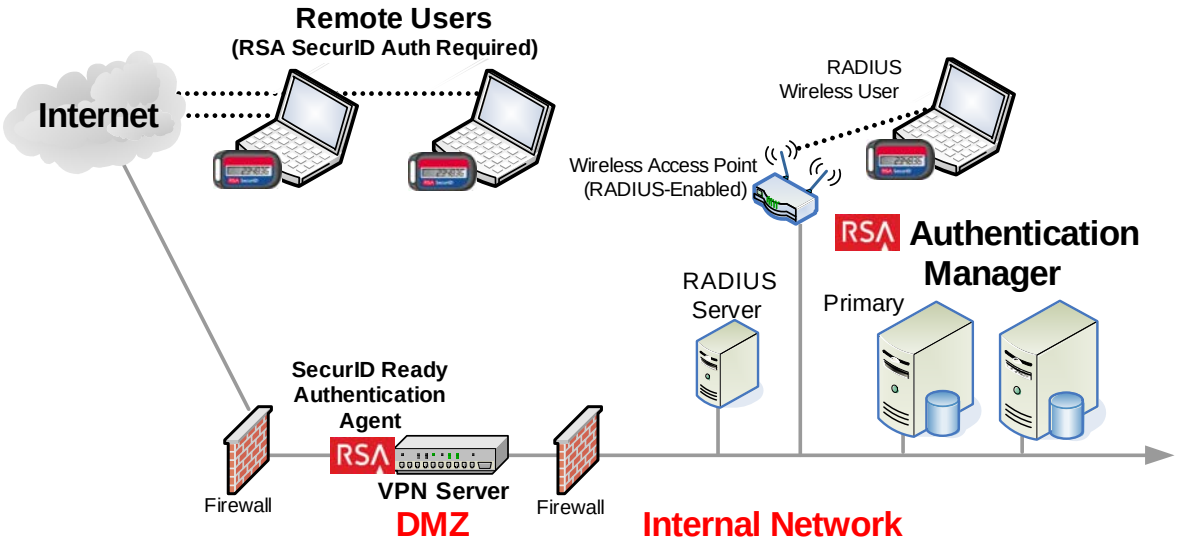
The following figure shows the components of RSA Authentication Manager for Miller & Strauss.



Secure Remote and Wireless Access

For secure remote access, the firm used their existing VPN server, which is certified with RSA SecurID and includes a built-in 5.x custom agent. Remote access is now protected by two-factor authentication. Users who log on through the VPN, or who use wireless or dial-in access, must enter a SecurID passcode before they are allowed to access the firm's network.

The following figure shows the RSA Authentication Manager components supporting secure remote and wireless access for a small, single-site organization.



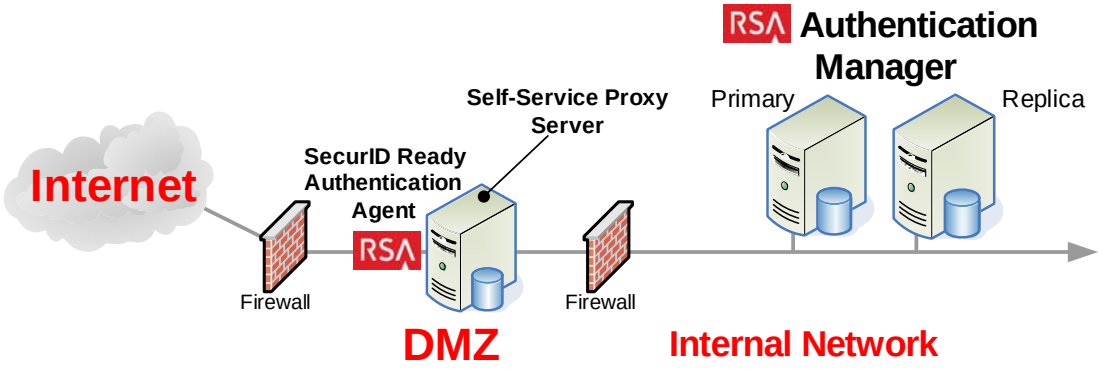
Auditing and Non-Repudiation

The firm's auditing and non-repudiation requirements are met by the robust logging and reporting capabilities of Authentication Manager. The Runtime Audit log, which records all user authentications, allows the firm to know who authenticated and when. The Administrative Audit log captures all administrative activity and makes it available for review by the firm. With these reporting capabilities, administrators and managers can print reports of system activity from the Authentication Manager log files.

Self-Service Features

To lighten their administrative load, Miller and Strauss use RSA Credential Manager (a component of Authentication Manager) to enable users to troubleshoot problems with their assigned tokens. To enable self-service capabilities for remote users, the company installed a proxy server in the DMZ to field self-service requests and proxy to the Credential Manager server on the Authentication Manager primary instance inside the corporate firewall. All self-service features are available because the firm uses the Authentication Manager internal database as their identity source.

The following figure shows the RSA components supporting Self-service features for a small, single-site organization.



Logical Deployment

Miller and Strauss chose a simplified logical deployment, accepting many of the default configurations of Authentication Manager. The firm decided to use only a single realm, and assigned all users, administrative roles, authentication agents, tokens, and reports to the default top-level security domain. The relatively small user population and small number of administrators did not require a security domain hierarchy.

The firm also decided to use the default system policies (password, lockout, token, offline authentication). All Miller and Strauss users have the same usage requirements, so it was not necessary to create custom policies.

Two administrators perform all the Authentication Manager administrative chores. Both are assigned the Super Admin role.

Scenario 2: Secure Internal, Remote and Wireless Access for a Medium, Single-Site Business

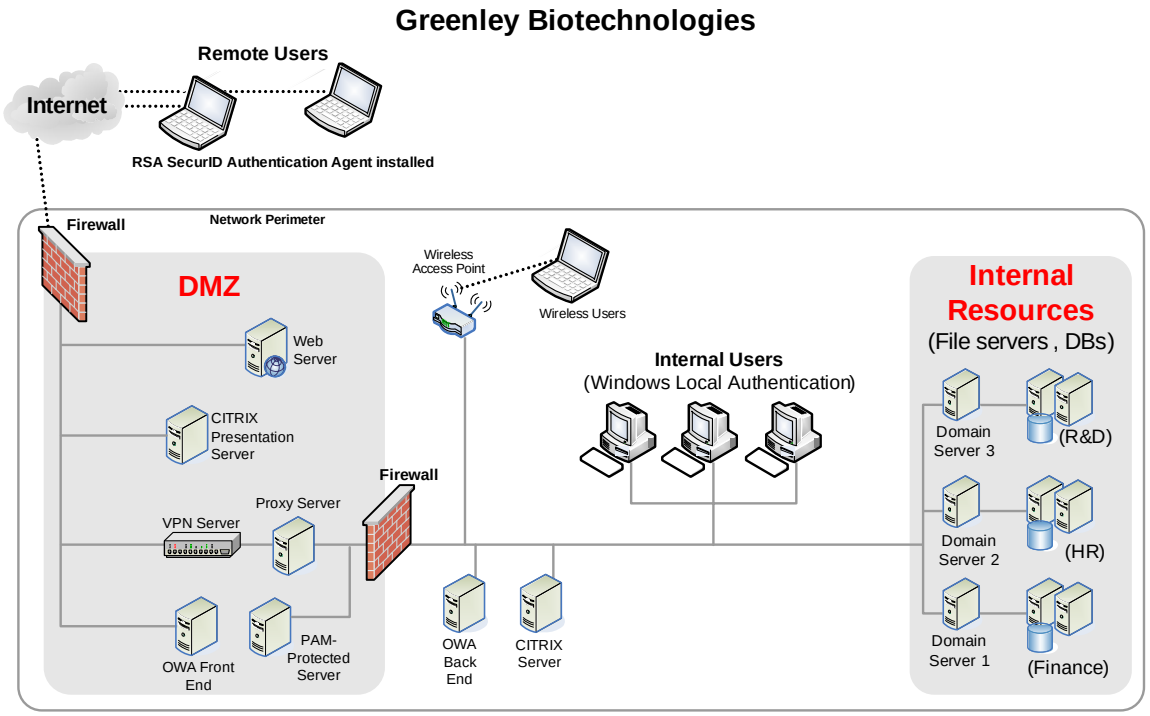
Greenley Biotechnologies (2,500 Employees)

Greenley Biotechnologies is a publicly traded, medium-sized company with 2,500 employees in one location. Because the company is publicly traded, it must meet all Sarbanes-Oxley requirements and maintain detailed records of all business and network transactions.

Greenley Biotechnologies uses the Windows operating system. They employ an IT staff of 24, including four system administrators who oversee general administrative tasks and operate the Help Desk. All employee data is maintained in Active Directory. Employees have local and remote access to the network.

The Greenley Biotechnologies network includes three Windows domain controllers inside the corporate firewall, which contain a variety of file and print servers. The network also includes a wireless access point with WPA encryption. In the DMZ, the network includes a VPN server, proxy server, CITRIX presentation server, web server, PAM-protected server, and an OWA front end.

The following figure shows the initial network topology for a medium-size single-site organization



Business Needs

Greenley Biotechnologies' needs are:

Secure remote access. Enable secure remote, wireless, and dial-in access to e-mail, applications, and confidential proprietary files, intellectual property, and research materials for management, researchers, and certain other employees.

Secure internal access. Enable secure on-site access to sensitive confidential proprietary files, intellectual property, and research materials for management, researchers, and certain other employees.

Auditing and non-repudiation. To assist with Sarbanes-Oxley requirements, the company also needs an audit trail and non-repudiation by persons accessing these files.

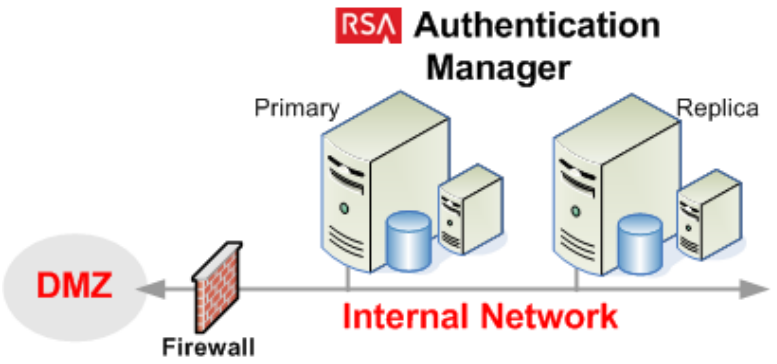
How RSA Products Are Deployed to Satisfy Business Needs

Physical Deployment

Greenley Biotechnologies purchased RSA Authentication Manager 7.1 with an Enterprise Server license. They installed the Authentication Manager primary instance (for authentication) and one replica instance (for failover) on the network behind the corporate firewall. For increased performance, the primary instance and the replica instance are both two-node clusters.

The company uses Active Directory as its identity source, and has granted Authentication Manager read/write access to it. The Authentication Manager administrators assigned and distributed RSA SecurID tokens to all 2,500 employees.

The following figure shows the RSA Authentication Manager components for a medium-size, single-site organization.

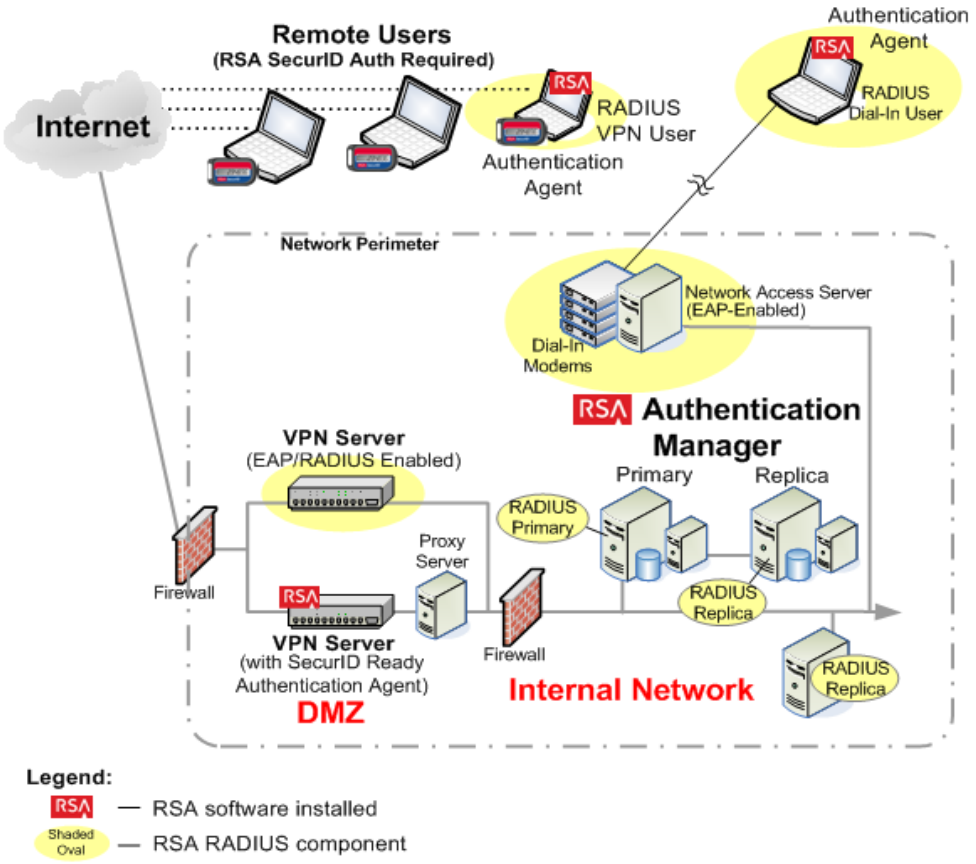


Secure Remote Access

To satisfy the need for secure remote access, the company used their existing VPN server, which is certified with RSA SecurID and includes a built-in 5.x custom agent. Remote access is now protected by two-factor authentication. Users who log on through the VPN, must enter a passcode before they are allowed to access the company's network.

To support users whose resource consumption must be closely tracked, the company deployed an EAP-POTP/RADIUS-enabled VPN server (for broadband and DSL users) and corresponding network access server and modems for dial-in users. Like other remote users, these remote RADIUS users have RSA SecurID for Windows on their machines, and must enter a SecurID passcode from their SecurID token before they are allowed to access the company's network.

The following figure shows the RSA components supporting secure remote access for a medium-size, single-site organization.



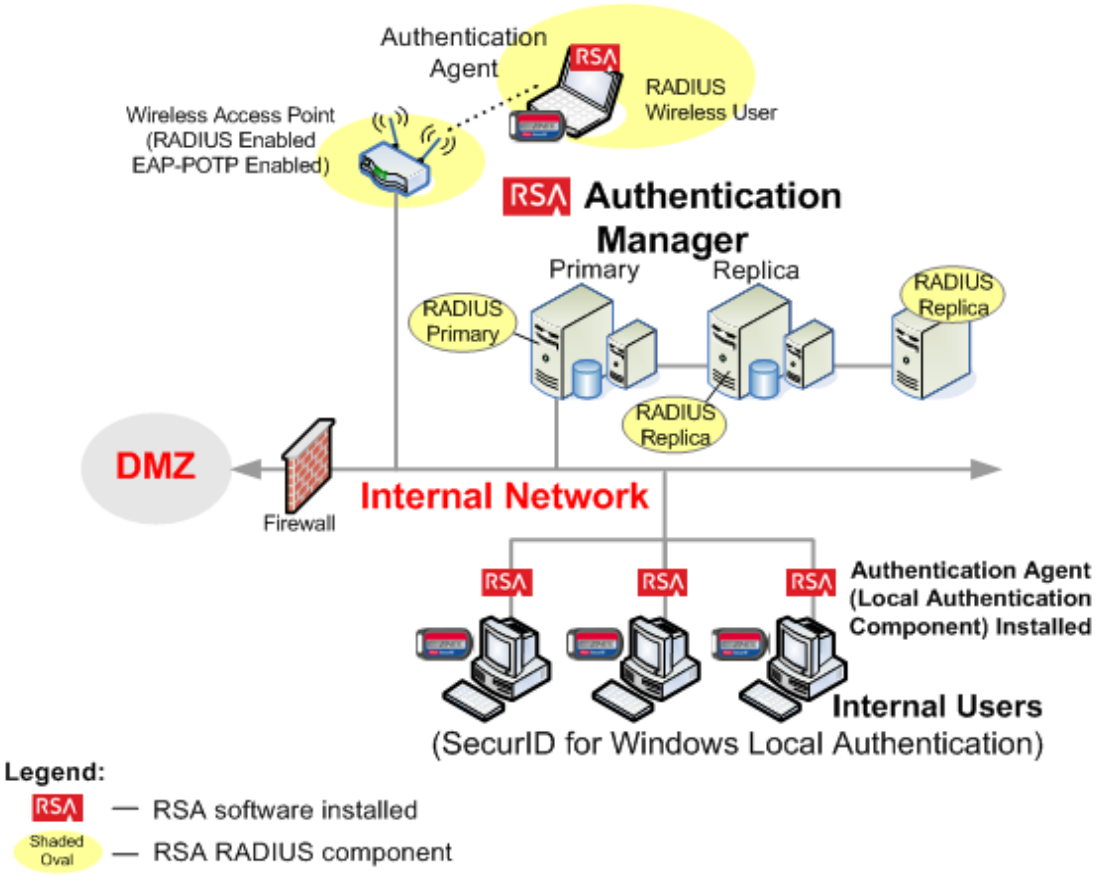
Secure Internal Access

To secure internal access to the corporate network with two-factor authentication, Greenley Biotechnologies deployed the RSA SecurID for Windows Local Authentication Client (LAC) on all internal desktop and laptop machines. All internal users must enter a SecurID passcode before they can access their desktop machine.

To strengthen internal wireless access and better track the consumption of network resources by certain remote users, the company deployed RSA RADIUS along with the Authentication Manager primary and replica instances and one standalone RADIUS replica server for additional failover protection.

To secure internal wireless access, the company deployed EAP-POTP/RADIUS-enabled wireless access points on their internal network and RSA SecurID for Windows on all wireless-enabled laptops. Just like internal wired users, wireless users must enter a passcode from their SecurID tokens before they can access their laptop.

The following figure shows the RSA Authentication Manager components supporting secure internal access for a medium-size, single-site organization.



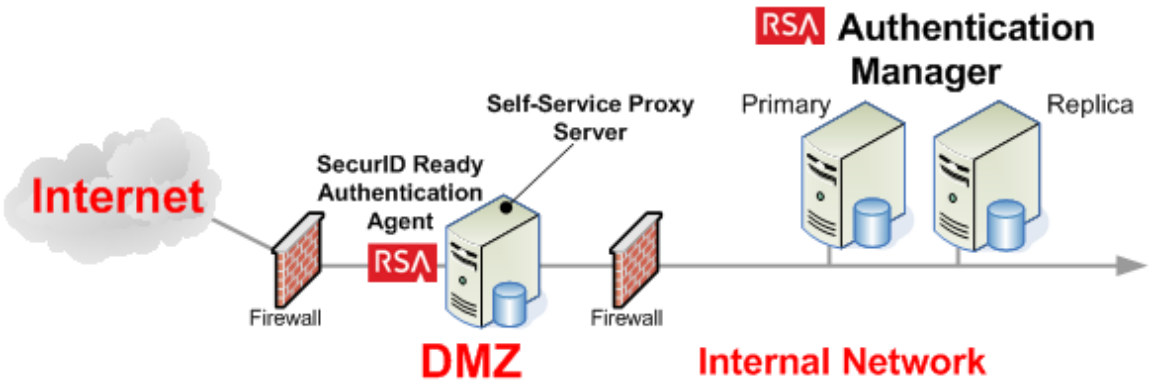
Auditing and Non-Repudiation

The company's auditing and non-repudiation requirements are met by the robust logging and reporting capabilities of Authentication Manager. The Runtime Audit log, which records all user authentications, lets the company know who authenticated and when. The Administrative Audit log captures all administrative activity and makes it available for review by the company. With these reporting capabilities, administrators and managers can print reports of system activity from Authentication Manager log files.

Self-Service and Provisioning Features

To lighten the administrative load, Greenley Biotechnologies uses RSA Credential Manager (a component of Authentication Manager) to allow users to troubleshoot problems with their assigned tokens and to request new tokens. To enable self-service capabilities for remote users, the company installed a proxy server in the DMZ to field self-service requests and proxy to the Credential Manager server on the Authentication Manager primary instance inside the corporate firewall. All self-service and provisioning features are available because the company has granted Authentication Manager read/write access to the Active Directory identity source.

The following figure shows the RSA Authentication Manager components supporting Self-Service features for a medium-size, single-site organization.



Logical Deployment

Greenley Biotechnologies uses a single realm. Lower-level security domains were created for Finance, HR, and R&D. Users who are members of these departments are contained in the lower-level security domains. Multiple security domains allow administrators' scope to be limited by, in this case, department.

The Finance department uses a combination of default and custom policies. Because of the sensitive nature of the department's work, the password policies are stricter and require more frequent password changes. The lockout and token policies are also less forgiving than the default policy used by other departments. Likewise, they use a custom restricted access time policy that limits when they can access the network. Default policies (password, lockout, token, offline authentication) are used in the top-level, HR and R&D security domains.

Reports specific to a department are contained in the lower-level security domains. Reports of a more general nature are contained in the top-level security domain. Agents, administrative roles, and tokens are contained in the top-level security domain.

Four administrators perform Authentication Manager administrative chores. Two of these administrators are Super Admins and two are Privileged Help Desk Administrators. The Privileged Help Desk Administrator is a predefined role. In this case, the role has been modified to include the following permissions:

- Move users and user groups between security domains
- View security domains
- Approve Credential Manager requests

IT managers are assigned the Request Approver and Token Distributor roles to handle Credential Manager requests.

One Privileged Help Desk Administrator is assigned to each security domain. In this case, the scope of the Privileged Help Desk Administrator role includes all security domains. Twenty additional members of the IT staff are assigned the Help Desk Administrator role. They spend 10% of their time on general administrative tasks and staff a 9 a.m. to 5 p.m. Help Desk.

Scenario 3: Secure Internal, Remote, and Wireless Access for a Large, Multisite, Single-Realm Enterprise

FocalView Software Corporation (15,000 Employees)

FocalView Software Corporation is a publicly traded, large enterprise company with 15,000 employees in three different locations (Boston, New York, and San Jose). Because the company is publicly traded, it must meet all Sarbanes-Oxley requirements and maintain detailed records of all business and network transactions.

FocalView Software operates a multiple platform network with Windows clients and Linux and Solaris servers on the back end. They employ an IT staff of 56, including six system administrators, who oversee general administrative tasks and operate the Help Desk. Boston and New York employee data is maintained in a read-only Active Directory forest, with a domain for each of the locations. Employee data for the San Jose location, a recent acquisition, is maintained in a Sun Java Directory Server that is also read-only. Employees at the various sites have local and remote access to the network.

The FocalView Software network includes a Windows domain controller inside the corporate firewall, which contains a variety of file and print servers. It also includes wireless access points with WPA encryption. In the DMZ, the network includes a VPN server, proxy server, CITRIX presentation server, web server, PAM-protected server, and an OWA front end. This network configuration is present at each of the three locations.

Business Needs

FocalView Software Corporation's needs are:

Secure remote access. Enable secure remote, wireless, and dial-in access to e-mail, applications, and confidential proprietary files, intellectual property, and research materials for management, researchers, and certain other employees.

Secure internal access. Enable secure on-site access for users at all three company sites to sensitive confidential proprietary files, intellectual property, and research materials for management, developers, and certain other employees.

Auditing and non-repudiation. For legal and compliance reasons, they also need an audit trail and non-repudiation by persons accessing these files (meaning whoever accesses these files cannot claim that it was someone else).

How RSA Products Are Deployed to Satisfy Business Needs

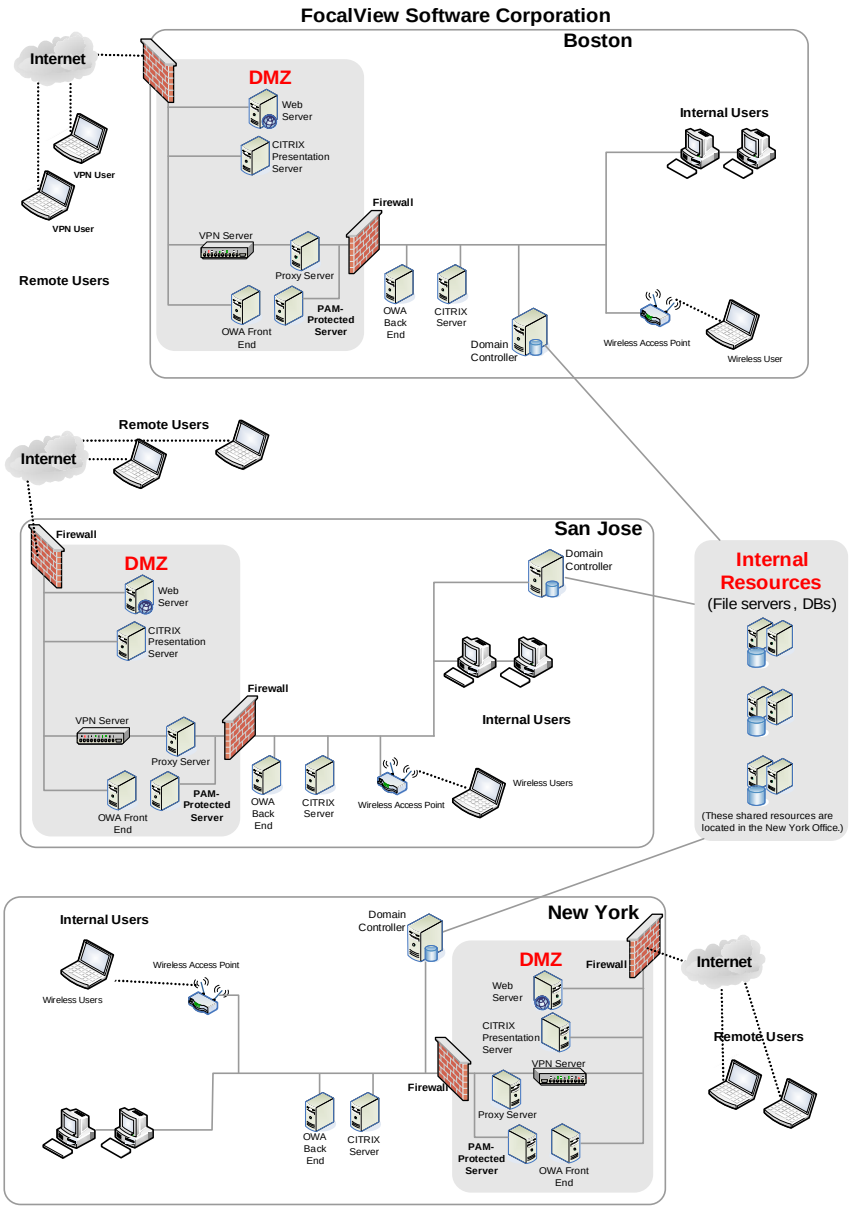
Physical Deployment

FocalView Software Corporation purchased RSA Authentication Manager 7.1 with an Enterprise Server license. They installed instances of Authentication Manager in the following locations:

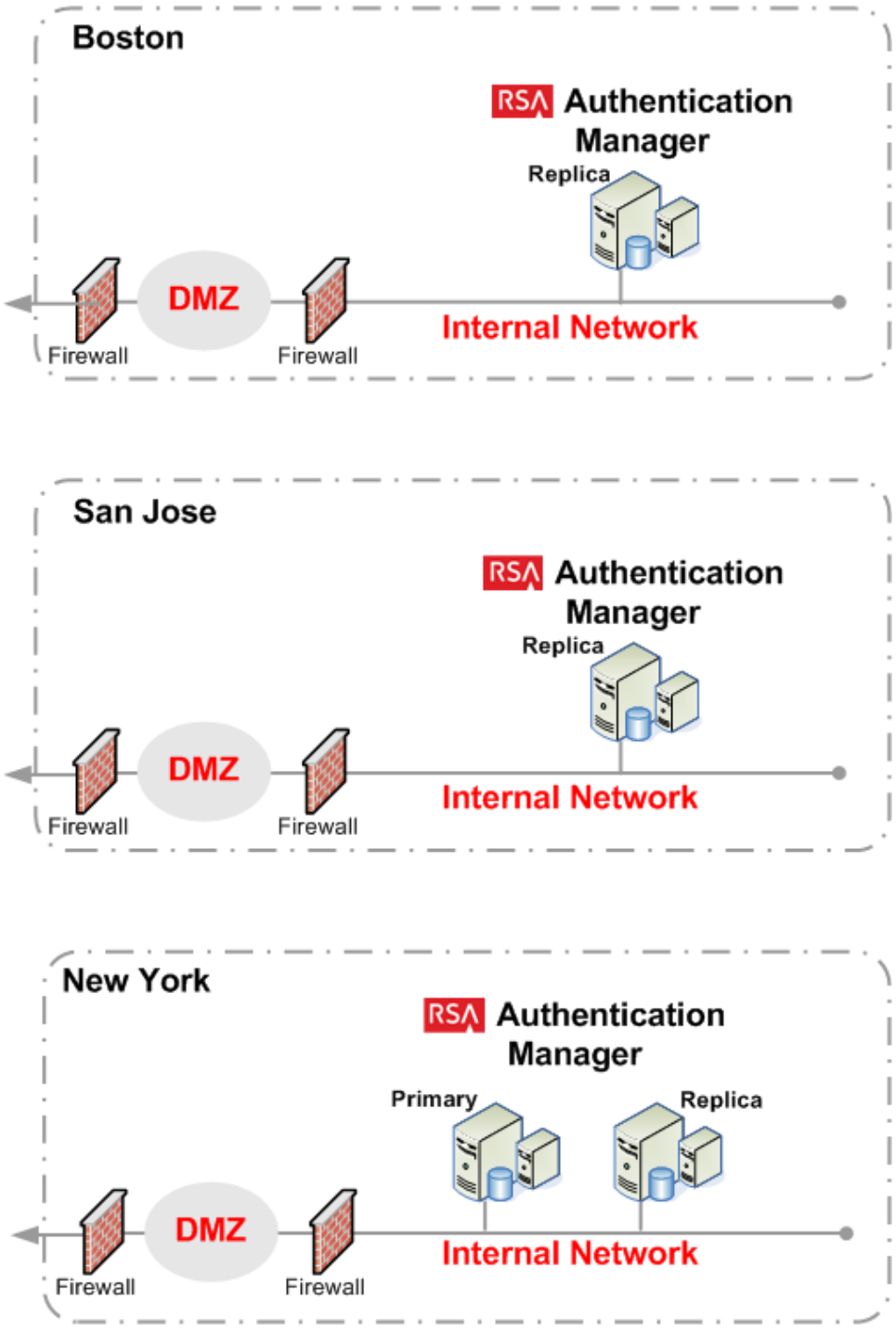
- One primary instance (for authentication), and one replica instance (for failover) in the server room of the corporate offices in Boston. For increased performance, the primary instance and the replica instance are both two-node clusters.
- One replica instance in the server room of the San Jose office. For increased performance, the replica instance is a two-node cluster.
- One replica instance in the server room of the New York office. For increased performance, the replica instance is a two-node cluster.

The company uses Active Directory and Sun Java System Directory Server as its identity sources, and has granted Authentication Manager read-only access to them. Authentication Manager administrators assigned and distributed RSA SecurID tokens to all 15,000 employees. They keep an additional supply of 2,000 tokens for new users and to replace lost or damaged tokens.

The following figure shows the initial network topology for a large, single-realm, multisite organization



The following figure shows the RSA Authentication Manager components for a large, single-realm, multisite organization.



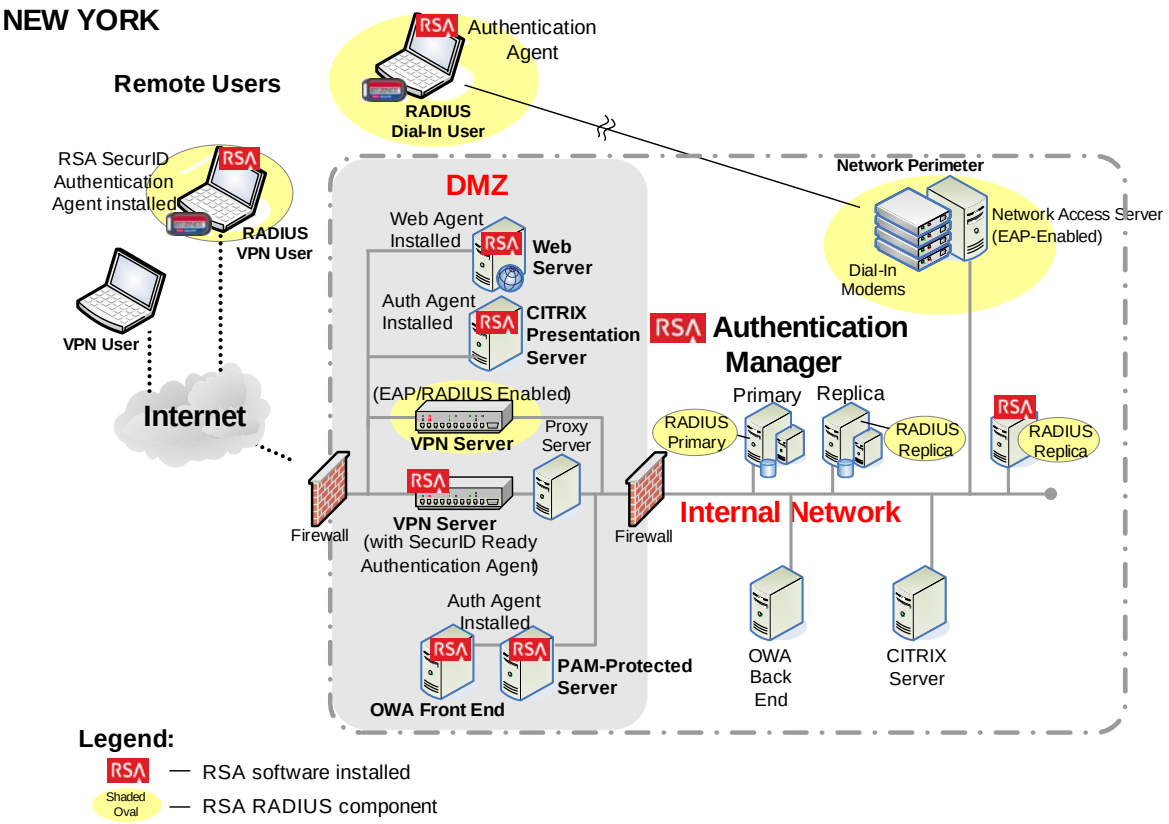
Secure Remote Access

For secure remote access, the company performed the following actions:

- They used their existing VPN server, which is certified with RSA SecurID and includes a built-in 5.x custom agent. Remote access is now protected by two-factor authentication. Users who log on through the VPN, or who use wireless or dial-in access, must enter a passcode from their SecurID token before they are allowed to access the firm's network.
- They installed RSA Authentication Agents on their web server, Citrix Presentation Server, and Outlook Web Access (OWA) Server in the DMZ. All users accessing information through these servers must enter a SecurID passcode.
- To support users whose resource consumption must be closely tracked, the company deployed an EAP-POTP/RADIUS-enabled VPN server (for broadband and DSL users) and corresponding network access server and modems for dial-in users. Like other remote users, these remote RADIUS users have the RSA SecurID for Windows Local Authentication Client (LAC) on their machines, and must enter a SecurID passcode before they are allowed to access the network.

The following figure shows only the New York location. Other locations are similar except that only replica instances of RSA Authentication Manager and RSA RADIUS replica servers are deployed in the Boston and San Jose offices.

The following figure shows the RSA Authentication Manager components supporting secure remote access for a large, single-realm, multisite organization.



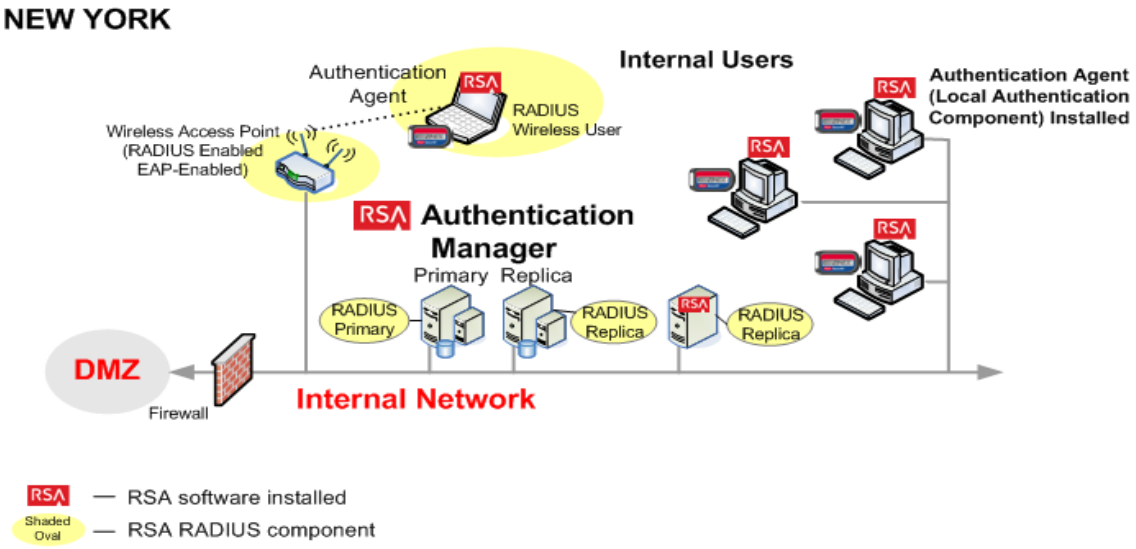
Secure Internal Access

For secure internal access, the company performed the following actions:

- To secure internal access to the corporate network with two-factor authentication, FocalView Software Corporation deployed the RSA SecurID for Windows Local Authentication Client (LAC) on all internal desktop and laptop machines. All internal users must enter a passcode from their SecurID token before they can access their desktop machine.
- To strengthen internal wireless access and better track the consumption of network resources by certain remote users, the company deployed RSA RADIUS along with the Authentication Manager primary and replica instances and one standalone RADIUS replica server for additional failover protection.
- To secure internal wireless access, the company deployed EAP-POTP/RADIUS-enabled wireless access points on their internal network and the RSA SecurID for Windows Local Authentication Client (LAC) on all wireless-enabled laptops. Just like internal wired users, wireless users must enter a passcode from their SecurID token before they can access their laptop.

The figure shows only the New York location. Other locations are similar except that only replica instances of Authentication Manager and RADIUS replica servers are deployed in the Boston and San Jose offices

The following figure shows the RSA components supporting secure internal access for a large, single-realm, multisite organization.



Auditing and Non-Repudiation

The company's auditing and non-repudiation requirements are met by the robust logging and reporting capabilities of Authentication Manager. The Runtime Audit log, which records all user authentications, lets the company know who authenticated and when. The Administrative Audit log captures all administrative activity and makes it available for review by the company. With these reporting capabilities, administrators and managers can print reports of system activity from Authentication Manager log files.

Self-Service and Provisioning Features

To lighten the administrative load, FocalView Software Corporation uses the RSA Credential Manager component of Authentication Manager to allow users to troubleshoot problems with their assigned tokens and to request new tokens. To enable self-service capabilities for remote users, the company installed a proxy server in the DMZ to field self-service requests and proxy to the Credential Manager server on the Authentication Manager primary instance inside the corporate firewall. FocalView Software Corporation can only use a subset of self-service and provisioning features because they have only granted Authentication Manager read-only access to their identity sources.

Logical Deployment

FocalView Software Corporation uses a single realm with three lower-level security domains for each of the company's geographic locations.

The company has organized its administrative hierarchy in the following way:

- Users are contained in the lower-level security domain that corresponds to their physical location. Multiple security domains allow administrators' scope to be limited by, in this case, by geographic location.
- Reports specific to a geographic site are contained in the lower-level security domains. Reports of a more general nature are contained in the top-level security domain.
- Tokens assigned to users at a site are contained in the security domain specific to the site. In addition, each security domain includes some unassigned tokens to facilitate assignment and delivery to its new users.
- Agents located in a specific geographic site are contained in the security domain specific to the site. This allows Privileged Help Desk Administrators assigned to the location to manage the agent records, and, if necessary, access the physical machines.

Default policies (password, lockout, token, offline authentication) are used for the top-level security domain, and the Boston and New York security domains. The San Jose security domain uses custom password, lockout and token policies. The San Jose location has recently been acquired, and their administrators prefer stricter password policies that require more frequent password changes, as well as lockout and token policies that are less forgiving than the default policy used by other locations.

Six administrators perform Authentication Manager administrative chores. Four of these administrators are Super Admins. Two are assigned the System Administrator role and have all administrative permissions, except those assigned only to the Super Admin.

An additional IT staff of 50 spend 10% of their time on general administrative tasks and the other 90% staffing a 9 a.m. to 8 p.m. IT Help Desk. There are:

- 20 Boston Privileged Help Desk Administrators
- 15 New York Privileged Help Desk Administrators
- 15 San Jose Privileged Help Desk Administrators

These administrators all have the permissions of the Privileged Help Desk Administrators, plus the following custom privileges:

- Move users and groups between security domains
- View security domains
- Approve Credential Manager requests

Each is located in the location indicated in the title of their role. Their scope is limited to the security domain where they are located and the identity source where their respective users are stored.

IT managers are assigned the Request Approver and Token Distributor roles to handle Credential Manager requests.

Scenario 4: Secure Internal, External, and Guest Access for a Large Enterprise (Multiple International Locations, Multiple Deployments Using Trusted Realm Authentication)

International Gadget Corporation (50,000 Employees)

International Gadget Corporation (IGC) is a publicly traded, large enterprise company with 50,000 employees, headquartered in New York, with divisions also in London and Tokyo. Because the company is publicly traded, it must meet all Sarbanes-Oxley requirements and maintain detailed records of all business and network transactions.

IGC is a multi-platform shop with a variety of Windows, Linux and Solaris systems on their corporate network. They employ an IT staff of 162 who oversee general administrative tasks and operate the Help Desk. Employee data is maintained in an Active Directory forest, with a domain for each of the locations. London employee data is also maintained in a Sun Java Directory Server. Employees have local and remote access to the network.

IGC maintains a wide-area network (WAN) that links together its three international sites. Each site maintains a local-area network that includes Windows domain controllers inside the corporate firewall, each maintaining a variety of file and print servers. In the DMZ, each LAN also includes wireless access points with WPA encryption, a VPN server, a proxy server, CITRIX presentation server, web server, PAM-protected sever and an OWA front end.

Business Needs

IGC's needs are:

Secure remote access. Enable secure remote and dial-in access to e-mail, applications, and confidential proprietary files, intellectual property, and research materials for management, researchers, and certain other employees.

Secure access for employees visiting from other corporate offices. Enable secure on-site access to confidential proprietary files, intellectual property, and research materials when a user from one location is visiting another location.

Secure internal access. Enable secure on-site wired and wireless access for users at all three company sites to confidential proprietary files, intellectual property, and research materials for management, researchers, and certain other employees.

Auditing and non-repudiation. For legal and compliance reasons, IGC also needs an audit trail and non-repudiation by persons accessing these files.

How RSA Products Are Deployed to Satisfy Business Needs

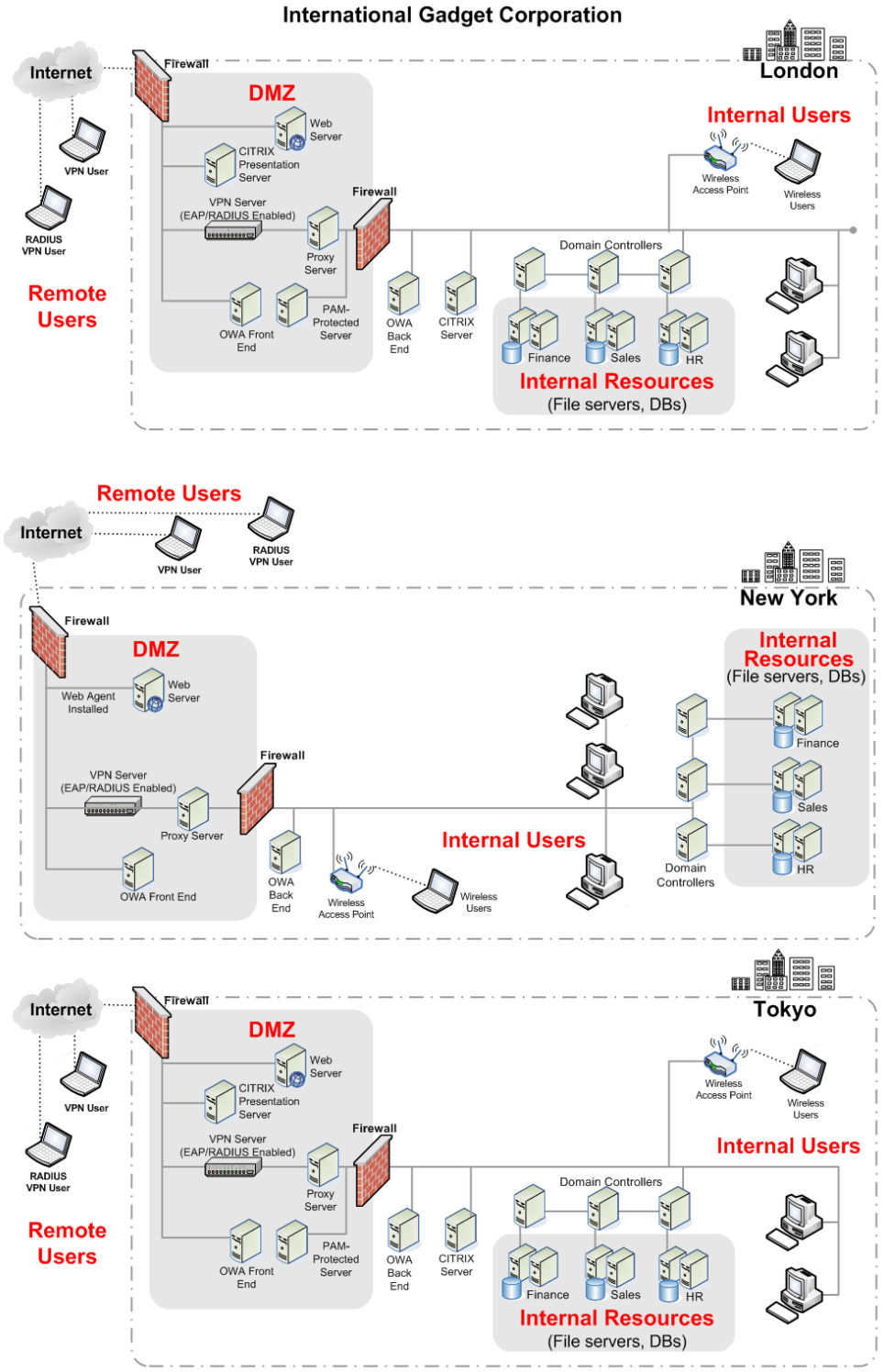
Physical Deployment

IGC purchased RSA Authentication Manager 7.1 with an Enterprise Server license. To minimize the amount of authentication traffic on the corporate WAN, they configured three separate deployments, one in each geographic location where the company has a major facility. Each deployment has a separate license, its own supply of RSA SecurID tokens, and identity sources. The deployments are configured in the following way:

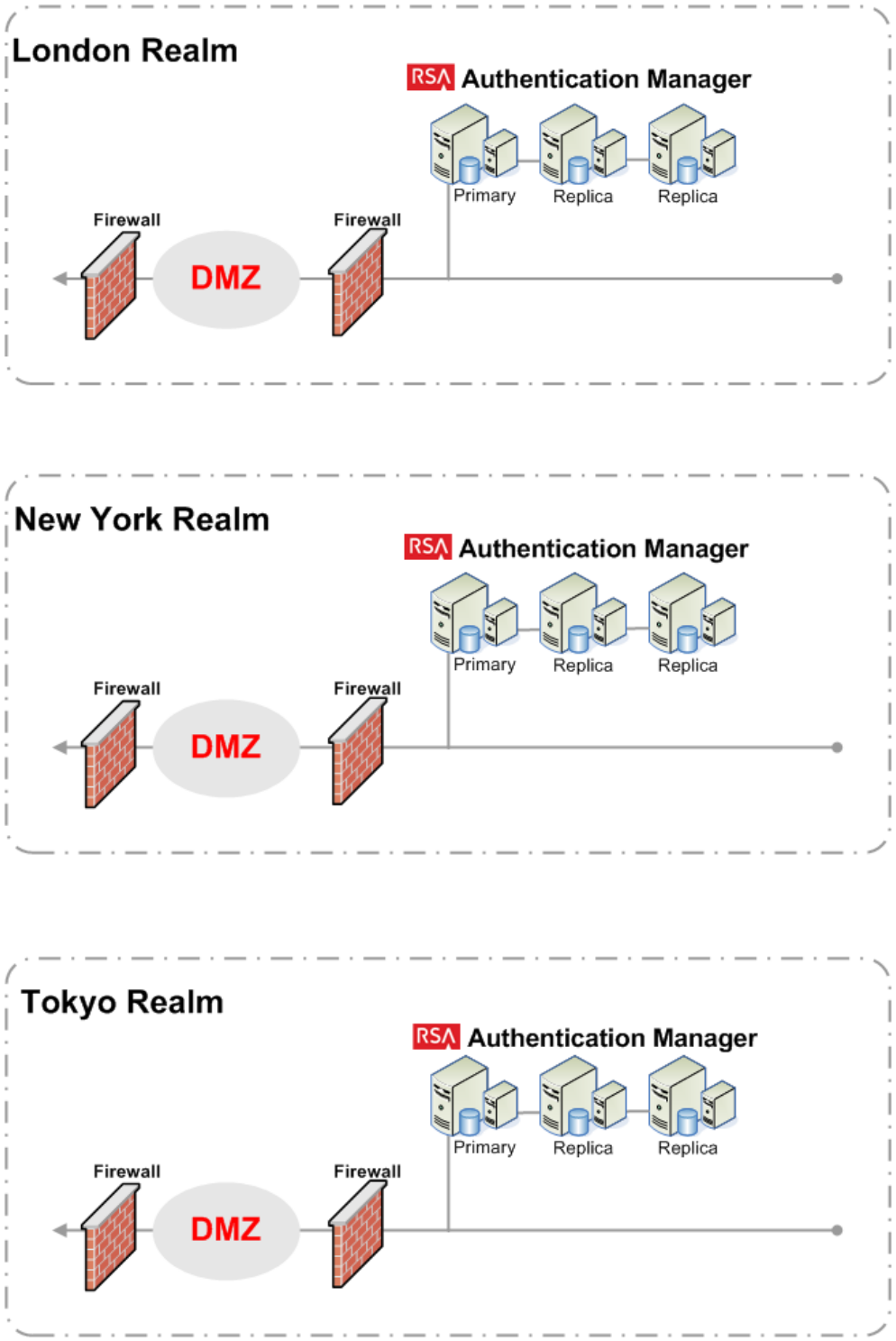
- London: One primary instance (for authentication), and two replica instances (for failover) inside the corporate firewall. For increased performance, the primary instance and the replica instances are both two-node clusters.
- New York: One primary instance (for authentication), and two replica instances (for failover) inside the corporate firewall. For increased performance, the primary instance and the replica instances are both two-node clusters.
- Tokyo: One primary instance (for authentication), and two replica instances (for failover) inside the corporate firewall. For increased performance, the primary instance and the replica instances are both two-node clusters.

The company uses Active Directory and Sun Java System Directory Server as its identity sources, and has granted Authentication Manager read-only access to them. Authentication Manager administrators assigned and distributed RSA SecurID tokens to all 50,000 employees. They keep an additional supply of 3,000 tokens for new users and to replace lost or damaged tokens.

The following figure shows the network topology for a large, multirealm, multisite organization.



The following figure shows the RSA Authentication Manager components for a large, multirealm, multisite organization.



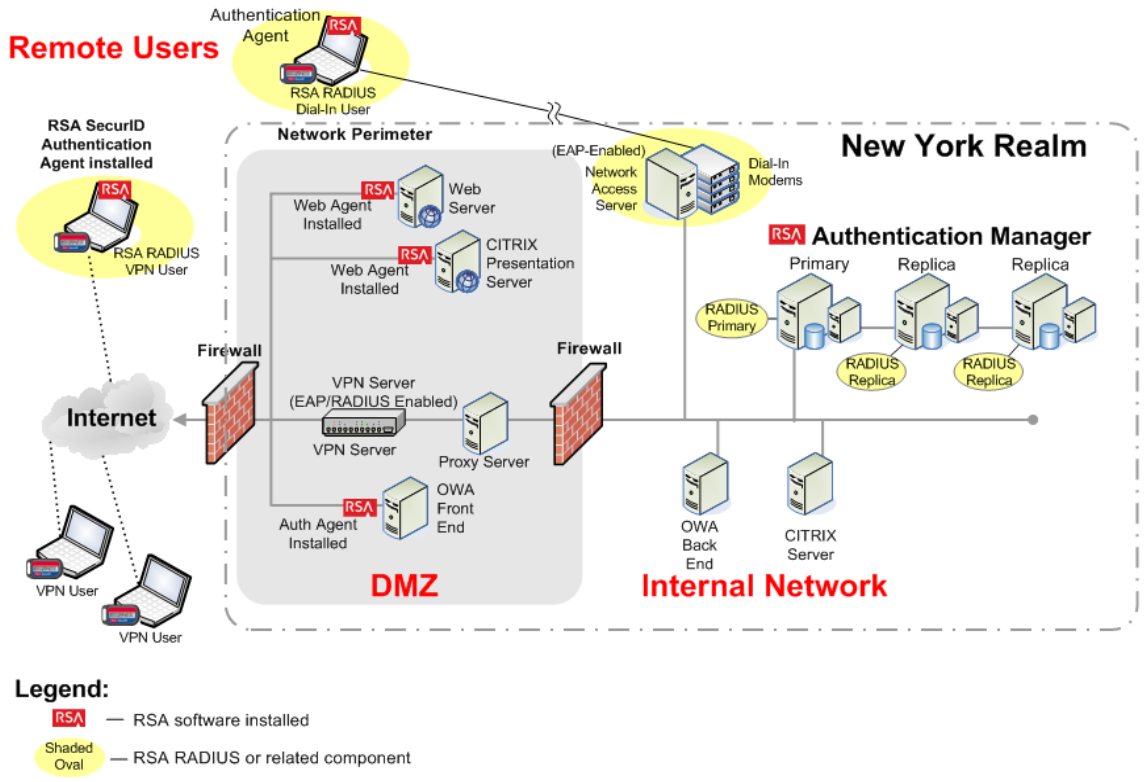
Secure Remote Access

For secure remote access, the company performed the following actions for each deployment:

- They used their existing VPN server, which is certified with RSA SecurID and includes a built-in 5.x custom agent. Remote access is now protected by two-factor authentication. Users who log in through the VPN, or who use wireless or dial-in access, must enter a SecurID passcode before they are allowed to access to firm's network.
- They installed RSA Authentication Agents on their web server, Citrix Presentation Server, and Outlook Web Access (OWA) Server in the DMZ. All users accessing these servers must enter a SecurID passcode.
- To support users whose resource consumption must be closely tracked, the company deployed an EAP-POTP/RADIUS-enabled VPN server (for broadband and DSL users) and corresponding network access server and modems for dial-in users. RADIUS users now use a VPN client to enter a SecurID passcode before they are allowed to access the network.

The figure shows only the New York realm. Other locations are similar.

The following figure shows the RSA Authentication Manager components supporting secure remote access for a large, multirealm, multisite organization.

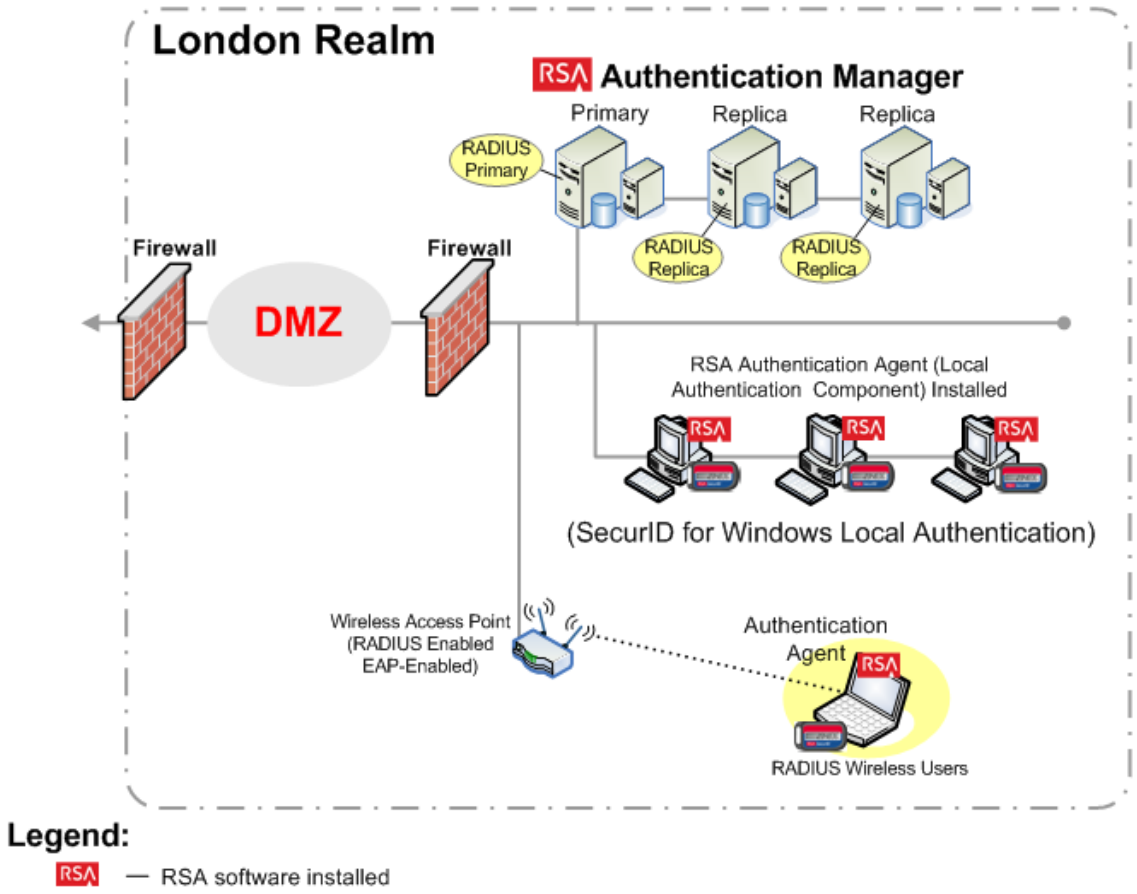


Secure Internal Access

For secure internal access, the company performed the following actions:

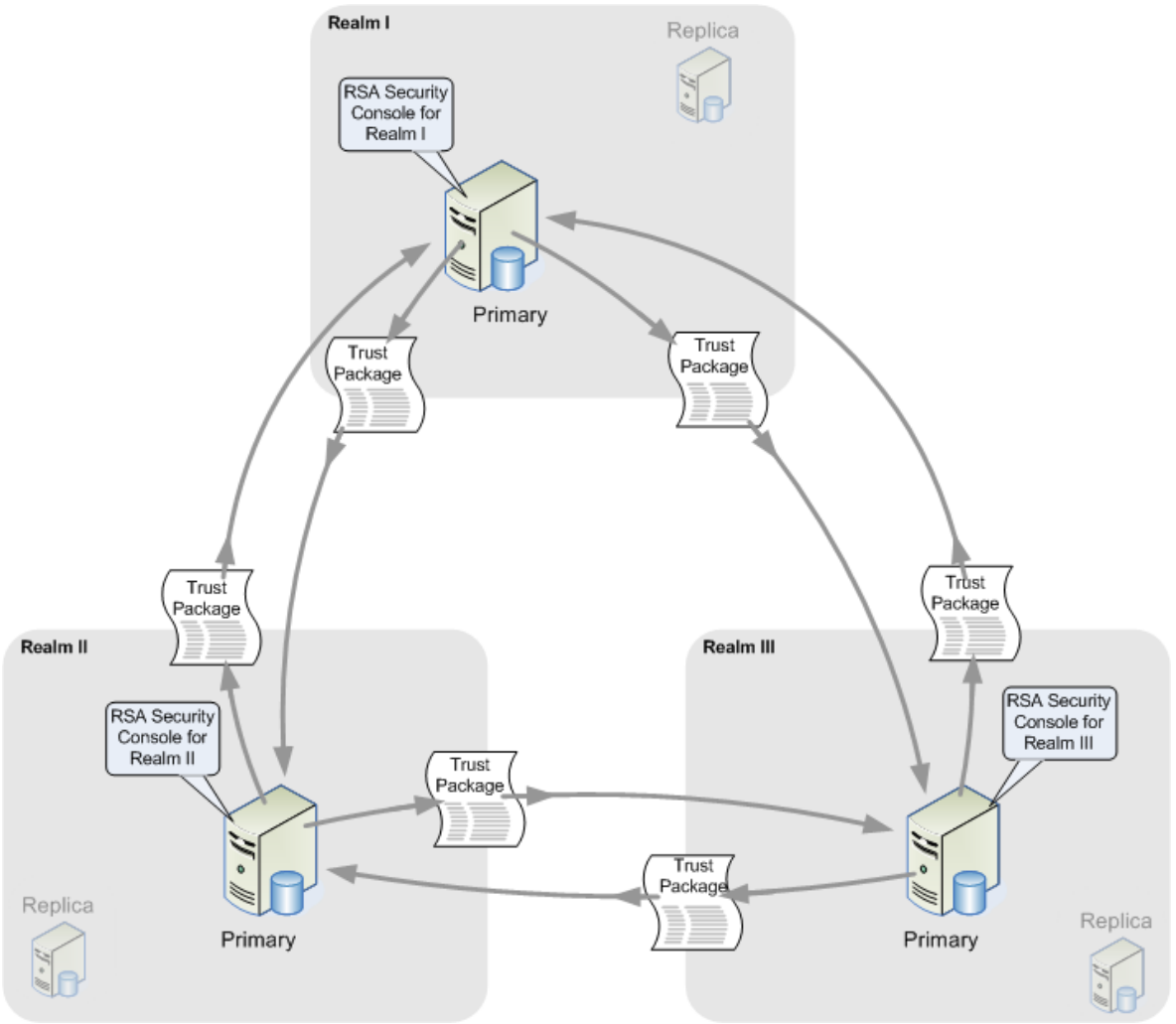
- To secure internal wired and wireless access to the corporate network with two-factor authentication, IGC deployed the RSA SecurID for Windows Local Authentication Client (LAC) on all internal desktop machines and laptops (wired and wireless). All internal users must enter a SecurID passcode before they can access their desktop machine.
- To ease RADIUS administration, the company deployed RSA RADIUS so that routine management operations can be conducted from within the Authentication Manager administration interface. The company deployed RADIUS along with the Authentication Manager primary and replica instances and one standalone RADIUS replica server for additional failover protection.
- To strengthen internal wireless access and better track the consumption of network resources by certain remote users, the company deployed RADIUS along with the Authentication Manager primary and replica instances and one standalone RADIUS replica server for additional failover protection.
- To secure internal wireless access, the company deployed EAP-POTP/RADIUS-enabled wireless access points on their internal network and the RSA SecurID for Windows Remote Authentication Client (RAC) on all wireless-enabled laptops. Just like internal wired users, wireless users must enter a passcode from their SecurID token before they can access their laptop.

The following figure shows the RSA Authentication Manager components supporting secure internal access for a large, multirealm, multisite organization. It shows only the London realm. Other locations are the same.



Secure access for employees visiting from other corporate offices

To allow visiting employees network access, the company uses the Authentication Manager trusted realm feature. The trusted realm feature allows the company to create a “trust relationship” between its three deployments, so that users from one deployment may be authenticated through agents in another deployment. For example, employees visiting the New York office may authenticate on the New York network.



Auditing and Non-Repudiation

The company’s auditing and non-repudiation requirements are met by the robust logging and reporting capabilities of Authentication Manager. The Runtime Audit log, which records all user authentications, lets the company know who authenticated and when. The Administrative Audit log captures all administrative activity and makes it available for review by the company. With these reporting capabilities, administrators and managers can print reports of system activity from Authentication Manager log files.

Self-Service and Provisioning Features

To lighten the administrative load, IGC uses RSA Credential Manager to allow users to troubleshoot problems with their assigned tokens and to request new tokens. Credential Manager is deployed as part of the Authentication Manager deployment at each location. To enable self-service capabilities for remote users, the company installed a proxy server in the DMZ to field self-service requests and proxy to the Credential Manager server on the Authentication Manager primary instance inside the corporate firewall. The company can only use a subset of self-service and provisioning features because they have only granted Authentication Manager read-only access to their identity sources.

Logical Deployment

IGC has three separate deployments, one in each geographic location where the company has a major facility. Each deployment is organized the same way. Each deployment uses a single realm. Lower-level security domains are used in each deployment for the departments at each geographic location as follows:

- The New York deployment has Finance, Sales, and HR security domains.
- The London deployment has Finance, Sales, and HR security domains.
- The Tokyo deployment has Sales, HR, and Engineering security domains.

A mix of custom and default policies (password, lockout, token, offline authentication) are used for the top-level security domain in each realm.

The company has organized its administrative hierarchy as follows:

- Users are stored in the security domain that corresponds to their department and geographic location. Administrators have created a “trust relationship” between the three deployments within International Gadget Corporation. This allows users from each location to authenticate when visiting other locations.
- Reports specific to a department are contained in the lower-level security domains. Reports of a more general nature are contained in the top-level security domain.
- Tokens assigned to users at a site are contained in the security domain specific to the site. In addition, each security domain includes some unassigned tokens to facilitate assignment and delivery to its new users.
- Agents located in a specific geographic site are contained in the realm specific to the site. This allows administrators at each location to manage agent records, and, if necessary, access the physical machine.

Twelve administrators are available to perform Authentication Manager administrative chores. Eight are Super Admins. Four are assigned the System Administrator role and have all administrative permissions, except those assigned to the Super Admin only.

An additional IT staff of 150 spend 10% of their time on general administrative tasks and staff a 9 a.m. to 8 p.m. Help Desk. There are:

- 50 New York Privileged Help Desk Administrators
- 50 London Privileged Help Desk Administrators
- 50 Tokyo Privileged Help Desk Administrators

They have all permissions of the Privileged Help Desk Administrators, plus the following custom privileges:

- Move users and user groups between security domains
- View security domains
- Approve Credential Manager requests

Each is located in the geographic location indicated by their role title. Their scope is limited to only the realm where they are located and the identity source where their respective users are stored.

IT managers are assigned the Request Approver and Token Distributor roles to handle Credential Manager requests.

Glossary

Term	Definition
Active Directory	The directory service that is included with Microsoft Windows Server 2003 and Microsoft Windows 2000 Server.
Active Directory forest	A federation of identity servers for Windows Server environments. All identity servers share a common schema, configuration, and Global Catalog.
AD	See Active Directory.
adjudicator	A component that defends Authentication Manager against replay attacks in which an intruder attempts to reuse an old passcode or acquires the current passcode for a token and sets the system clock back to use the captured passcode.
administrative command	A command other than a system-generated command.
administrative role	A collection of permissions and the scope within which those permissions apply.
administrator	Any user with one or more administrative roles that grants administrative permission to manage administrative resources.
Advanced Encryption Standard (AES)	The current cryptographic standard, adopted by the National Institute of Standards and Technology (NIST) in November, 2001. AES replaces Data Encryption Standard (DES) because it is considered to be more secure.
AES	See Advanced Encryption Standard.
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.
agent auto-registration utility	A utility included in the RSA Authentication Agent software that enables you to automatically register new authentication agents in the internal database, and updates the IP addresses for existing agents.
agent host	The machine on which an agent is installed.

Term	Definition
Agent Protocol Server	The Authentication Manager component that manages the ACE protocol packet traffic to and from agents. The inbound request packets are routed to the appropriate message handler. The response packets are sent to the originating agent.
approver	A Request Approver or an administrator with approver permissions.
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 a given realm. 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 authority	The central entry point for authentication services.
authentication broker	A component that handles the authentication process and issuance of authentication tickets.
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 policy	A collection of rules that specify the authentication requirements. An authentication policy may be associated with one or more resources.
authentication protocol	The convention used to transfer credentials of a user during authentication. For example, HTTP-BASIC/DIGEST, NTLM, Kerberos, and SPNEGO.

Term	Definition
Authentication Server	An Authentication Manager component made up of services that handle authentication requests, database operations, and connections to the RSA 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.
authorization data	Information defined by the provisioning server, which is necessary to complete the provisioning of a CT-KIP-enabled token. Authorization data includes the appropriate serial number and places the new token credentials in the Authentication Manager internal database.
auto-registration	A setting which, if enabled, permits unregistered users to become registered upon a successful authentication to a system-managed resource. If auto-registration is disabled, only an administrative action can register users. Also see registered user and unregistered user.
Base Server license	Authentication Manager license that allows one primary instance and one replica instance. (Multiple replica instances and server nodes are not allowed.) Includes RSA Credential Manager self-service. Credential Manager provisioning can be added.
Business Continuity option	Authentication Manager option that allows you to temporarily increase the number of users allows into your system and the number of users allowed to use on-demand authentication.
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.
chained authentication	The process of creating a strong form of authentication by combining two weaker forms. For example, the user is required to use a PIN and a tokencode.
client time-out	The amount of time (in seconds) that the user’s desktop can be inactive before reauthentication is required.
CLU	See command line utility.

Term	Definition
cluster	An instance consisting of a database server and one or more server nodes.
command line utility (CLU)	A utility that provides a command line user interface.
connection pool	A named group of identical connections to a data store.
contact list	A list of server nodes provided by the Authentication Manager to the agent, to which the agent can direct authentication requests.
context-based authentication	An authentication sequence in which the system presents the user with only the authentication options that are appropriate for the User ID entered. The options are based on policy requirements and the authenticators that the user owns.
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.
Credential Manager Provisioning	An option that automates the token deployment process and provides user self-service options.
cryptographic algorithm	A mathematical function that uses plain text as the input and produces cipher text as the output and vice-versa. It is used for encryption and decryption.
CT-KIP	Cryptographic Token-Key Initialization Protocol.
CT-KIP-capable token	A token that is capable of storing the authorization data and seed generated as a result of CT-KIP operations between a CT-KIP 1.0 client and an Authentication Manager CT-KIP server.
CT-KIP client	A program that implements the CT-KIP client-side protocol and interacts with a CT-KIP server for the secure initialization of CT-KIP-capable tokens.
CT-KIP server	A software component of Authentication Manager that implements the CT-KIP server-side protocol and interacts with a CT-KIP client application for the secure initialization of CT-KIP-capable tokens.
CT-KIP toolkit	An implementation of the CT-KIP client-server protocol. It provides the API for creating CT-KIP server or client applications.

Term	Definition
customer name	The name of the enterprise to which the license is issued.
data encryption standard (DES)	The cryptographic standard prior to November 2001, when the National Institute of Standards and Technology (NIST) adopted the Advanced Encryption Standard (AES).
data store	A data source such as a relational database (Oracle or DB2) or directory server (Sun Java System Directory Server or Microsoft Active Directory). Each type of data source manages and accesses data differently.
data transfer object	Simple object used to pass data between tiers. It does not contain business logic.
database server	The server where the database is installed.
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.
denial of service	The process of making a system or application unavailable. For example, the result of barraging a server with requests that consume all the available system resources, or of passing malformed input data that can cause the system to stop responding.
delivery address	The e-mail address or the cell phone number where the on-demand tokencodes will be delivered.
deployment	The arrangement of Authentication Manager instances into appropriate locations in a network to perform authentication.
DES	See data encryption standard.
distribution file	A shared secret between a hardware or software authenticator and an authentication server. The authenticator, sometimes called a token, and the server work together in a time synchronous, or time dependent mode to provide a one-time passcode that the token holder enters at logon.
distribution file password	A password used to protect the distribution file when the distribution file is sent by e-mail to the user.
distributor	A Token Distributor or an administrator with distributor permissions.
DTO	See data transfer object.

Term	Definition
dump	An RSA ACE/Server format used to back up, restore, and merge database information. A dump file is a binary data file that contains all database tables and columns in table-dependency order.
EAP	See extensible authentication protocol.
EAP-POTP	An RSA-proposed IETF (Internet Engineering Task Force) standard that defines the method for one-time password (RSA SecurID) authentication. It provides capabilities, such as end-to-end protection of one-time passwords and support for token exception cases (New PIN, Next Tokencode, and others).
EAP-POTP client	Client that supports the EAP-POTP method.
e-mail notifications	Contain status information about requests for user enrollment, tokens, and user group membership are sent to users who initiated the request. For token requests, e-mail notifications also contain information about how to download and activate tokens. Request Approvers and Token Distributors receive e-mail notifications about requests that require their action. See e-mail templates.
e-mail templates	Templates that administrators can use to customize e-mail notifications about user requests for user enrollment, tokens, user group membership, or the on-demand tokencode service. See e-mail notifications.
emergency access	The process for enabling a token for a user whose token is not available or is not functioning. Used in connection with offline authentication access.
emergency access passcode	A complete authentication code that, if enabled, can be used by a user to perform an offline authentication without an authenticator or PIN.
emergency access tokencode	A partial authentication code that, if enabled, can be used by a user to perform an offline authentication without an authenticator. The user is required to provide his or her PIN.
Enterprise Server license	Authentication Manager license that allows a primary instance, multiple replica instances, and multiple server nodes.
Evaluation license	Authorizes an evaluation copy of the product at a customer site.
event-based token	A hardware token that displays a tokencode whenever the user presses the button on the token.

Term	Definition
excluded words dictionary	A dictionary containing a record of words that users cannot use as passwords. It includes several thousand commonly used words that are likely to be included as part of any dictionary attacks on the system, for example, “password.” The excluded words dictionary prevents users from using common, and therefore, easily guessed words as passwords.
extensible authentication protocol (EAP)	An authentication framework that supports multiple authentication methods.
failover mode	The state in which the connection pool management service has to use the secondary connection pools for serving the connection requests, because the primary connection pools are not available due to the failed primary data servers.
four-pass CT-KIP	The exchange of two protocol data units (PDUs) between the client and server.
Global Catalog	A read-only, replicated repository of a subset of the attributes of all entries in an Active Directory forest.
graded authentication	A mechanism for noting the relative strengths of authentication methods (either individually or as combinations). For example, an RSA SecurID token is stronger than a user name and password. Equivalently ranked methods may be used interchangeably.
group membership	See user group.
hardware token	A physical device, such as an RSA SecurID standard card, key fob, or PINPad that displays a tokencode.
high-water mark	The highest numbered interval used by a user to authenticate.
identity attribute definition	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 the LDAP or RDBMS.
Identity Management Services	The set of shared components, toolkits, and services used to build RSA products, for example, Authentication Manager.
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 Sun Java System Directory Server or Microsoft Active Directory.

Term	Definition
IMS	See Identity Management Services.
initial time-out	The wait time, in seconds, before the initial remote access prompt appears. (The term is used in relation to remote RSA SecurID authentication.)
instance	One single database server, or a database server and one or more server nodes, acting as a single cohesive processing unit. An instance does not have to be a cluster, but a cluster is an instance.
instance ID	This ID identifies a single logical installation of a product or component. For example, in a non-clustered environment, it identifies the database server. In a clustered environment, it identifies the database server and the entire cluster of server nodes. Likewise for web agents, a single agent may have a unique instance ID or an entire server cluster may share a single instance ID.
instance name	The name assigned to an instance. It is either the hostname where a single server node is installed or the cluster name where the clustered instance is installed.
interval	A value used to represent a specific time-based PRN code being generated by an authenticator.
internal database	The Authentication Manager proprietary data source.
J2EE	See Java 2 Enterprise Edition.
Java 2 Enterprise Edition	A framework for building enterprise applications using Java technology.
Java Cryptographic Architecture (JCA)	The set of APIs provided by the Java 2 platform that establishes the architecture and encapsulates limited cryptographic functionality from various cryptographic providers.
Java Cryptographic Extensions (JCE)	The set of APIs provided by the Java 2 platform that encapsulates additional cryptographic functionality from various cryptographic providers.
Java keystore (JKS)	The Java 2 platform implementation of a keystore provided by Sun Microsystems.
Java Management Extensions (JMX)	The set of APIs provided by the Java 2 platform that enables building distributed, web-based, dynamic, and modular solutions for managing and monitoring devices, applications, and service-driven networks.

Term	Definition
Java Messaging Service (JMS)	A standard Java interface for interacting with message queues and topics.
Java Server Pages (JSP)	A commonly used technology for dynamic web content.
JCA	See Java Cryptographic Architecture.
JCE	See Java Cryptographic Extensions.
JKS	See Java keystore.
JMS	See Java Messaging Service.
JMX	See Java Management Extensions.
JSP	See Java Server Pages.
keystore	The Java 2 platform facility for storing keys and certificates.
Key Management services	The management of the generation, use, storage, security, exchange, and replacement of cryptographic keys.
Key Management encryption key	The key used for encryption or decryption operations of keys managed by Key Management services.
license	A verifiable piece of information that represents permission from RSA to use Authentication Manager, its features, or both. A license is a component of the License Management Service.
license category	A way of grouping different types of licenses. The license categories for Authentication Manager are Base Server, Enterprise Server, and Evaluation.
license creation date	The date when the license file is created.
license deployment	Specifies either a server or floating license.
license file	An XML file containing license data that is common across all IMS-based products. The categories of data are: client, product, and feature. A license file is a component of LMS.
license file version	The version of the license schema to which the generated license conforms.
license ID	An internal identifier associated with the license. RSA Manufacturing assigns the license ID.
License Management Service (LMS)	A service responsible for managing and validating product licenses.

Term	Definition
license.rec	A license record file containing the database key needed to extract critical information from the dump file.
LMS	See License Management Service.
local authentication client component	An RSA Authentication Agent component that requires users to enter valid RSA SecurID passcodes to access their Microsoft Windows desktops.
locked license	A license limited to a specific server instance. See server license.
lockout policy	A set of conditions specifying when an account will be locked and whether the account must be unlocked by an administrator or will unlock on its own after a designated amount of time. Lockout policies are applied to security domains. Each realm has a default lockout policy.
log archival	Creates a backup copy of the log for noncurrent, permanent storage.
logging service	A component responsible for recording system, audit, and trace events.
lower-level security domain	In a security domain hierarchy, a security domain that is nested within another security domain.
Management Information Base (MIB)	A type of virtual database used to manage the devices (switches and routers, for example) in a communication network. For example, SNMP uses MIB to specify the data in a device subsystem.
MD5	An algorithm that produces a 128-bit message digest.
member user	A user who is a member of a member user group.
member user group	A user group that is a member of another user group. For example, an organization might define a Sales Managers user group within a North America user group. All member user groups must belong to the same identity source as the parent group, with one exception: any user group from any identity source can be assigned to a parent group that is stored in the internal database.
MIB	See Management Information Base.
Microsoft Management Console (MMC)	A user interface through which system administrators can configure and monitor the system.
MMC	See Microsoft Management Console.

Term	Definition
namespace	A set of names. A namespace defines a scope for a collection of names.
Network Management System (NMS)	Software used to manage and administer a network. The NMS uses SNMP to monitor networked devices and is responsible for polling and receiving SNMP traps from agents in the network.
NMS	See Network Management System.
NMS administrator	The person monitoring the network (through the NMS) for significant events. Also known as a network administrator.
node secret	A long-lived symmetric key that the agent uses to encrypt the data in the authentication request. Authentication Manager generates the authentication request when a user makes a successful authentication attempt. The node secret is known only to the Authentication Manager and the agent.
offline emergency tokencode	Provides emergency access for RSA SecurID for Windows users who require emergency access while authenticating offline. Use this option if the user has a temporarily misplaced, lost, or stolen token. The Offline Emergency Access Tokencode is used with the user's PIN.
offline emergency passcode	Provides emergency access for RSA SecurID for Windows users who require emergency access while authenticating offline. Use this option if the user has forgotten his or her PIN. The Offline Emergency Passcode is used in place of the user's PIN and tokencode.
object	Describes the following: security domains, identity sources, attributes, users, user groups, administrative roles, and policies.
offset	A value used to represent the amount of time an authenticator's internal clock has drifted over time.
on-demand tokencode	Tokencodes delivered by SMS or SMTP. They 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 only be used once, and you configure the lifetime of an on-demand tokencode. See on-demand tokencode service.

Term	Definition
on-demand tokencode service	A service that allows users to request on-demand tokencodes delivered by text message or e-mail, instead of tokens. You configure the on-demand tokencode service for requests using the Security Console. Users must be enabled to receive on-demand tokencodes before they can request them.
one-time tokencode set	Used for online emergency access. A set of tokencodes, each of which can be used only once, and is used with the user's PIN to create a passocde. The administrator can specify how many tokencodes are in the set.
PAM	See Pluggable Authentication Modules.
passcode	A code entered by a user to authenticate. The passcode is a combination of a PIN and a tokencode.
password-based encryption	The process of obscuring information so that it is unreadable without knowledge of the password.
password policy	A set of specifications that define what constitutes a valid password and the conditions under which the password expires. Password policies are applied to security domains.
PDU	See Protocol Data Unit.
permissions	Specifies which tasks an administrator is allowed to perform.
Pluggable Authentication Modules (PAM)	Mechanisms that allow the integration of new authentication methods into an API, independent of the existing API authentication scheme.
primary connection pool	Refers to the connection pools containing the connections to the primary instance database server.
primary instance	The machine with the installation of Authentication Manager at which authentication and all administrative actions occur.
private key	In asymmetric key cryptography, the cryptographic key that corresponds to the public key. The private key is usually protected by some external mechanism (for example, smart card, password encrypted, and so on).
PRN	See pseudorandom number.
Protocol Data Unit	A packet of data exchanged between two application programs across a network.
provisioning	See token provisioning.

Term	Definition
provisioning data	The provisioning server-defined data. This is a container of information necessary to complete the provisioning of a token device. Its format is not specified by CT-KIP because it is outside the realm of CT-KIP, but it is necessary for provisioning.
pseudorandom number (PRN)	A random number or sequence of numbers derived from a single seed value.
public key	In asymmetric key cryptography, the cryptographic key that corresponds with the private key. The public key is usually encapsulated within a certificate.
RADIUS	See Remote Authentication Dial-In User Service.
realm	An entire security domain hierarchy consisting of a top-level security domain and all of its lower-level security domains. A realm includes all of the objects managed within the security domain hierarchy (users, tokens, and password policies, for example). Each realm manages users and user groups in one or more identity sources.
regular time-out	The number of seconds before remote access prompts time out. The term is used in relation to remote RSA SecurID authentication.
Remote Authentication Dial-In User Service (RADIUS)	A UDP-based protocol for administering and securing remote access to a network.
remote EAP (extensible authentication protocol)	A remote authentication feature that requires users to submit RSA SecurID passcodes in order to open remote connections to the network. EAP has a graphical user interface and enhanced security and is supported in both Point-to-Point Protocol (PPP) authentication environments and non-PPP authentication environments, including Point-to-Point Tunneling Protocol (PPTP) VPN connections, 802.1x wired, and 802.11 wireless connections, and other specialized network media.
remote post-dial	Refers to the dial-in Point-to-Point Protocol (PPP) authentication support. With a post-dial terminal-based connection, when remote users dial in, a terminal-like character interface presents a simple user name and passcode prompt. If the right passcode is entered, the PPP connection is established. If the wrong passcode is entered, the dial-up connection is severed.

Term	Definition
replica instance	The machine with the installation of Authentication Manager at which authentication occurs and at which an administrator can view the administrative data. No administrative actions are performed on the replica instance. All administrative actions are performed on the primary instance.
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.
RSA Credential Manager	A component of Authentication Manager that allows users to request, maintain, and troubleshoot tokens.
RSA EAP	The RSA Security implementation of the EAP 15 authentication protocol that facilitates RSA SecurID authentication to networks in PPP, PPTP (VPN), and 802.1x (wireless or port access) environments.
RSA 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.
RSA Protected OTP	The RSA implementation of the EAP 32 authentication protocol that facilitates RSA SecurID authentication to networks in PPP, PPTP (VPN), and 802.1x (wireless or port access) environments.
RSA Security Console	An administrative user interface through which the user performs most of the day-to-day administrative activities.
RSA Self-Service Console	A user interface through which the user requests, maintains, and troubleshoots tokens.
runtime	Describes automated processing behavior—behavior that occurs without direct administrator interaction.
runtime command	A logon or logoff command.
runtime identity source	The runtime representation of the identity source. Runtime identity sources are used during runtime operations, such as authentication and group membership resolution instead of the corresponding administrative source, which is used for all other operations. This is an integral part of Active Directory forest support, which uses the Global Catalog during runtime operations.

Term	Definition
scope	In a realm, the security domain or domains within which a role's permissions apply.
secondary connection pool	The connection pools containing the connections to the secondary data stores.
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 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. The answers to security questions are case sensitive.
self-service	Allows users to perform maintenance tasks and troubleshoot tokens themselves, instead of calling the Help Desk. See also Token Provisioning.
Self-Service Console	See RSA Self-Service Console.
self-service requests	See requests.
self-service troubleshooting policy	Provides an emergency form of authentication that allows users to log on to the RSA Self-Service Console to perform troubleshooting tasks.
server node	An installation of Authentication Manager on a single server host. Each instance has one server node that contains the internal database. You can add additional server nodes to an instance, if your license allows. The additional server nodes cannot operate alone because they do not contain the internal database.
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.

Term	Definition
session policy	A set of specifications designating the restrictions on overall session lifetime and multiple session handling. Session policies are applied to an instance.
SHA1	A secure hash algorithm function that produces a 160-bit hash result.
shipping address	An address used by distributors to distribute hardware tokens.
Short Message Service (SMS)	A mechanism of delivery of short messages over mobile networks. It is often called text messaging. In Authentication Manager, it is a means of sending tokencodes to a cell phone. Tokencodes delivered by SMS are called on-demand tokencodes.
Simple Mail Transfer Protocol (SMTP)	A TCP/IP protocol used in sending and receiving e-mail. In Authentication Manager, it is a means of sending tokencodes to e-mail accounts. Tokencodes delivered by SMTP are called on-demand tokencodes.
Simple Network Management Protocol (SNMP)	A protocol for exchanging information about networked devices and processes. SNMP uses MIBs to specify the management data, and then uses the User Datagram Protocol (UDP) to pass the data between SNMP management stations and the SNMP agents.
single sign-on (SSO)	The process of requiring only a single user authentication event in order to access multiple applications and resources.
SMS	See Short Message Service.
SMTP	See Simple Mail Transfer Protocol.
snap-in	A software program designed to function as a modular component of another software application. For example, the MMC has a variety of snap-ins that offer different functionality (for example, Device Manager).
SNMP	See Simple Network Management Protocol.
SNMP agent	Software module that performs the network management functions requested by network management stations.
SNMP trap	An asynchronous event that is generated by the agent to tell the NMS that a significant event has occurred. SNMP traps are designed to capture errors and reveal their locations.
SSL	See Secure Sockets Layer.
SSO	See single sign-on.

Term	Definition
Super Admin	An administrator who has all permissions within the system. A Super Admin: • Can create and delete realms • Can link identity sources to realms • Has full permissions within any realm • Can assign administrative roles within any realm
symmetric key	A key that allows the same key value for the encryption and decryption of data.
system event	System-generated information related to nonfunctional system events such as server startup and shutdown, failover events, replication events, and so on.
system log	Persistable store for recording system events.
TACACS+	See Terminal Access Controller Access Control System+.
temporary fixed tokencode	Used for online emergency access. This temporary tokencode is used in conjunction with the user's PIN to create a passcode. The user can use this tokencode more than once. The administrator can configure the expiration date and other Temporary Fixed Tokencode attributes.
Terminal Access Controller Access Control System+ (TACACS+)	A remote authentication protocol that is used to communicate with an authentication server. Allows a remote access server to communicate with an authentication server to determine if a user has access to the network.
time-based token	A hardware token that always displays a tokencode and the tokencode changes automatically every 60 seconds.
token	A hardware device or software program that generates a pseudorandom number that is used in authentication procedures to verify a user's identity.
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.
tokencode	The random number displayed on the front of a user's RSA SecurID token. Tokencodes change at a specified time interval, typically every 60 seconds.

Term	Definition
top-level security domain	The top-level security domain is the first security domain in the security domain hierarchy (realm). The top-level security domain is unique in that it links to the identity source or sources and manages password, locking, and authentication policy for the entire realm.
trace log	Persistable store for trace information.
trusted realm	A trusted realm is a realm that meets these criteria: • It is located in a different deployment than your realm. • It has exchanged configuration settings with your realm. The settings are in an XML file called a trust package.
trust package	An XML file that contains configuration information about the realm.
two-factor authentication	An authentication protocol requiring two different ways of establishing and proving identity, for example, something you have (such as an authenticator) and something you know (such as a PIN).
two-pass CT-KIP	The exchange of one protocol data unit (PDU) between the client and server.
UDP	See User Datagram Protocol.
user	An account managed by the system that is usually a person, but may be a computer or a web service.
User Datagram Protocol (UDP)	A protocol that allows programs on networked computers to communicate with one another by sending short messages called datagrams.
user group	A collection of users, other user groups, or both. Members of the user group must belong to the same identity source. User group membership determines access permission in some applications.
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*.

Term	Definition
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

B

C

D

E

F

G

H

I

J

K

L

M

N

P

R

S

T

U

V

W

Z