RSA Authentication Manager 7.1
Basic Exercises

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

License agreement

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the **thirdpartylicenses.pdf** file.

Note on encryption technologies

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

Distribution

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.

April 2009
Revised: August 2009

The Security Division of EMC

Contents

Preface

About This Guide

This guide provides exercises to familiarize administrators with basic installation and administrative tasks for RSA Authentication Manager 7.1. These exercises are intended to be used with the User Trial kit.

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** > **Status > 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 Before You Begin

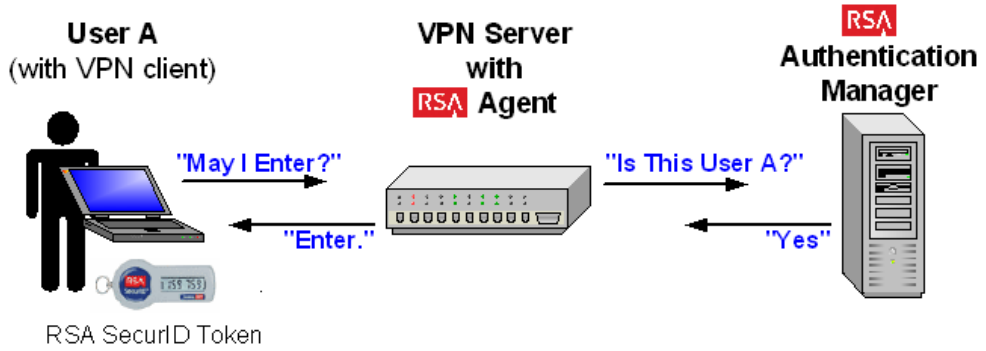
This chapter provides a brief overview of how RSA Authentication Manager works. It also provides a description of the exercises included in this guide and a list of setup tasks that you must perform before you begin the exercises.

About RSA Authentication Manager

An RSA Authentication Manager deployment has three basic components:

- An instance of RSA Authentication Manager
- An authentication agent installed on the network resource, such as a VPN or web server, that is to be protected
- RSA SecurID tokens

When a user attempts to access a protected resource, the agent transmits the user's user name and credentials to Authentication Manager for verification.



An Authentication Manager deployment may have other components, such as replica instances. You can also integrate it with other network resources, such as an LDAP directory or an external RADIUS server.

About The Exercises

The exercises in this guide give you a hands-on experience with the following:

1. Installing Authentication Manager on a Windows 2003 server
2. Administering Authentication Manager by creating security domains, users, administrators, and policies
3. Installing and configuring an authentication agent on an IIS web server
4. Administering tokens
5. As a user, accessing a web site using a token
6. Monitoring the system and generating reports of system events

These exercises provide suggested inputs for the various fields. You may use the suggested inputs, or use inputs specific to your organization.

Before You Start the Exercises

For a hands-on experience with these exercises, you need:

- Access to a server registered with DNS on which to install RSA Authentication Manager 7.1. It must meet these requirements:
  - OS: Microsoft Windows Server 2003 Enterprise with SP2 (32-bit or 64-bit)
  - CPU: Intel Xeon 2.8 GHz or equivalent
  - Disk space: 60 GB (for RADIUS, add 125 MB)
  - Memory: 2 GB (for RADIUS, add 512 MB)
  - Page file: 2 GB
  - These ports available for external communication:

TCP Ports			UDP Ports
5550	7002	7008	1161
5580	7004	7012	1162
2334	7006	7014	5500

- Access to the same or another server running Microsoft Internet Information Services 6.0 (IIS) on which to install the authentication agent.
- A PC to serve as the administrative workstation, with Internet Explorer 6.0 SP2, Internet Explorer 7.0, or Firefox 2.0 installed and JavaScript enabled. For instructions, see the browser Help.

- The RSA Authentication Manager 7.1 User Trial kit, which includes:
  - The RSA Authentication Manager 7.1 DVD
  - An RSA Authentication Manager license CD (copy the license file, server key, and certificate files onto the Windows server in a temporary directory)
  - RSA token record files (copy onto the administrative workstation in a temporary directory)
  - RSA SecurID hardware tokens
- RSA Authentication Agent 5.3 for Web for Internet Information Services.

  Go to **http://www.rsa.com/node.aspx?id=2807**, and download this agent to a temporary directory on the IIS server.

The Security Division of EMC

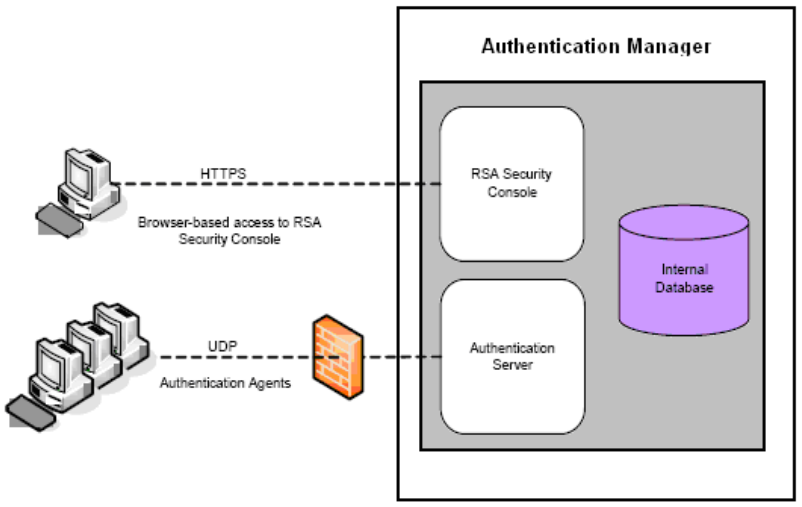
2 Installing RSA Authentication Manager

This chapter describes the procedure for installing RSA Authentication Manager 7.1 on a Windows 2003 Enterprise server.

RSA Authentication Manager Components

RSA Authentication Manager consists of a number of components and back-end services. The ones mentioned in these exercises are:

- **Authentication server.** Processes the agent authentication requests.
- **Internal database.** Stores user and policy data.
- **RSA Security Console.** A web-based interface for performing most administrative tasks.
- **RSA RADIUS server (optional, 32-bit systems only).** Provides centralized authentication, authorization, and accounting services.



Performing the Installation

You install Authentication Manager using the graphical user interface (GUI) installer. For these exercises, install RSA Authentication Manager using the following inputs.

1. Insert the RSA Authentication Manager 7.1 for Windows DVD into the server drive.

   The setup program runs automatically.

2. When the RSA Authentication Manager 7.1 page is displayed, click **Install Now**.

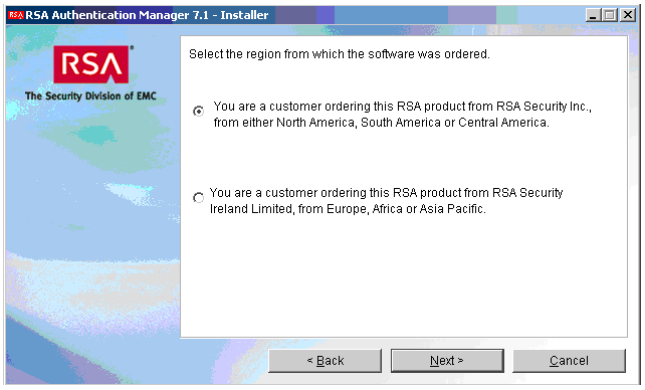
The Installation Wizard is displayed.

3. Click **Next**.

The Software Origin page is displayed.

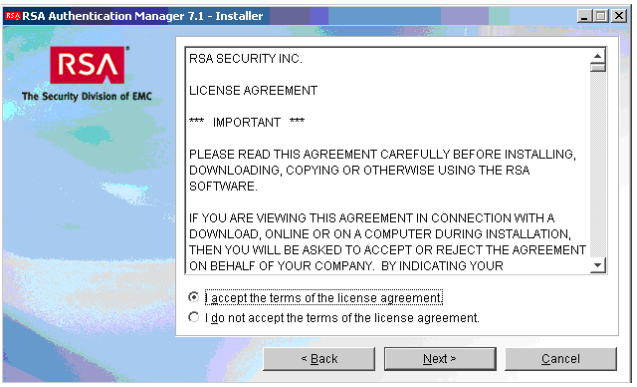
Note: The page names given in this exercise are descriptive only.

4. Select your region, and click **Next**.



The License Agreement page is displayed.

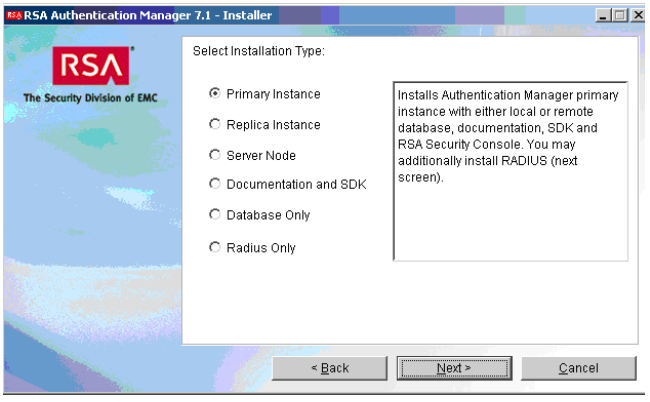
5. Accept the terms of the license agreement, and click **Next**.



The Installation Type page is displayed.

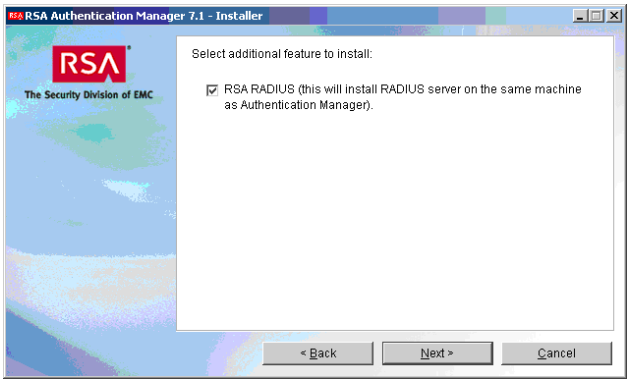
6. Select the type of installation you are doing. Because this is your first installation, select **Primary Instance**.

7. Click **Next**.



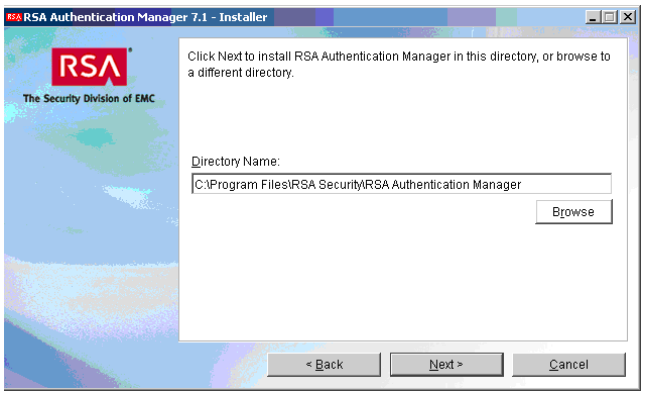
The Select Additional Features page is displayed

8. Accept the default (RSA RADIUS), and click **Next**.



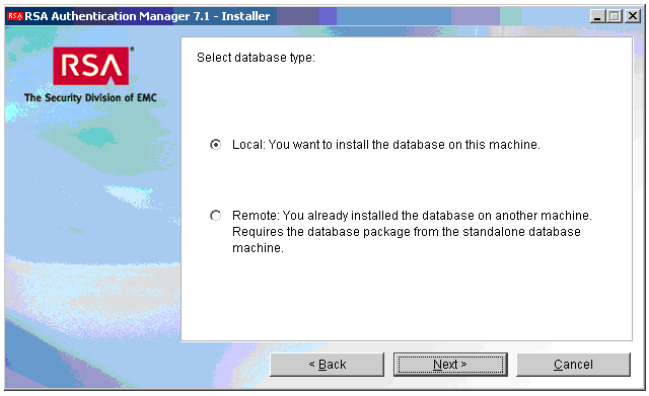
The Target Directory page is displayed.

9. Accept the default, and click **Next**.



The Select Database Type page is displayed.

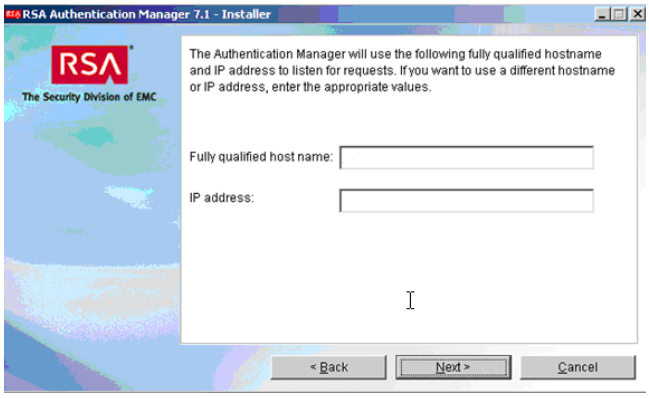
10. Accept the default (Local), and click **Next**.



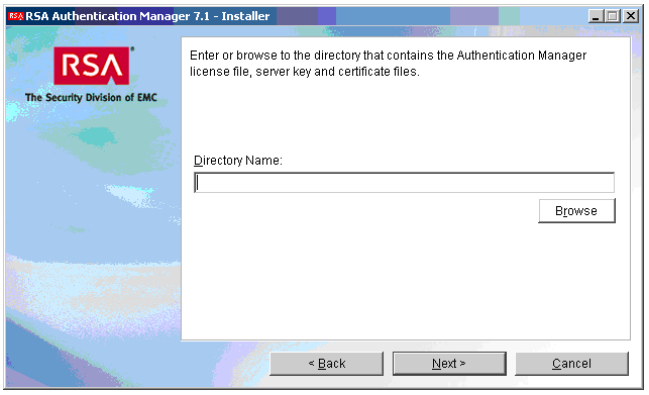
The Hostname page is displayed.

The fields auto-populate with the fully qualified hostname and IP address of the server on which you are installing Authentication Manager.

11. Verify or correct the information, and click **Next**.



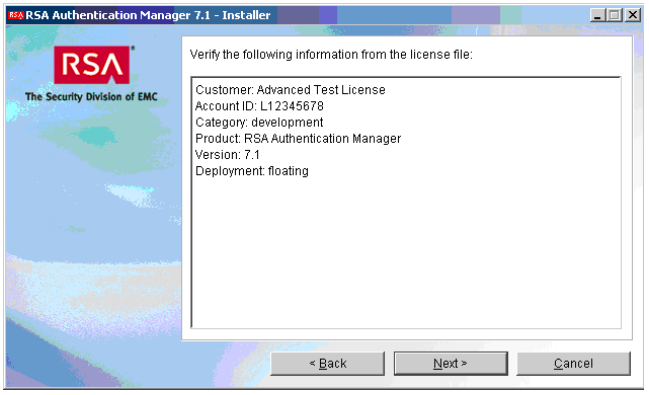
The License Location page is displayed.



12. Enter the pathname of the directory where you stored the Authentication Manager license file, server key, and certificate files, or click **Browse** to locate the directory.

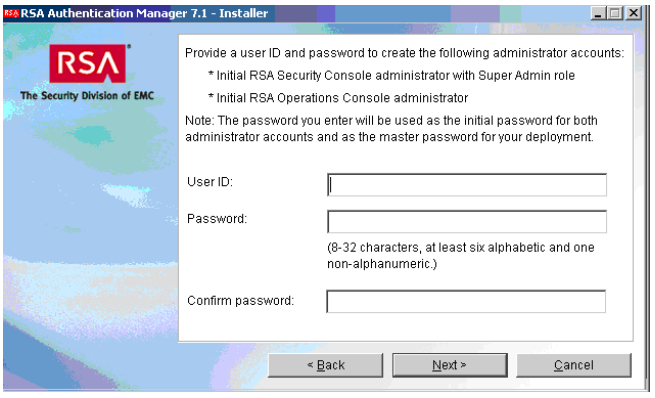
13. Click **Next**.

The license file contents for your license are displayed.



14. Verify that the contents are correct, and click **Next**.

The User ID and Password page is displayed.

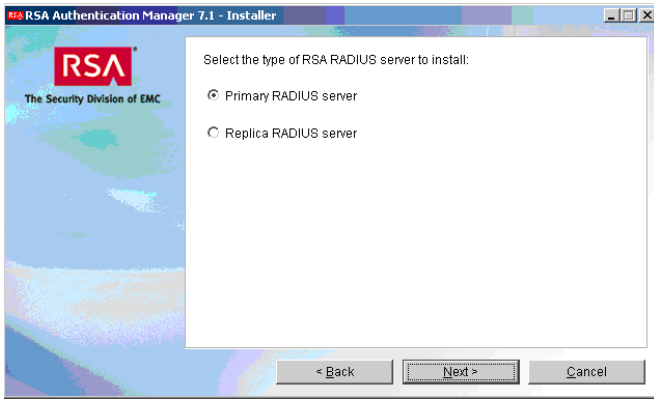


This page requests a user name and password for the initial RSA Security Console administrator. An administrator with the Super Admin role can perform all tasks within Authentication Manager.

15. Enter a User ID and password, re-enter the password, and click **Next**.

The RADIUS Server Type page is displayed.

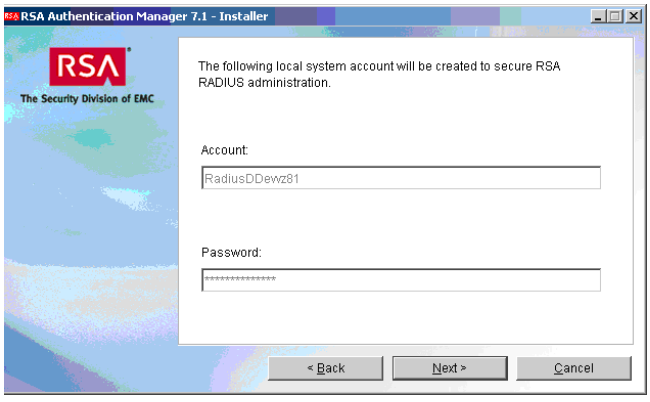
16. Because this is your first installation, select **Primary RADIUS Server**, and click **Next**.



The Create RADIUS Account page is displayed.

This page requests an account name and password for the local RADIUS system administrator. This account is created at the Windows level.

17. Accept the defaults, and click **Next**.

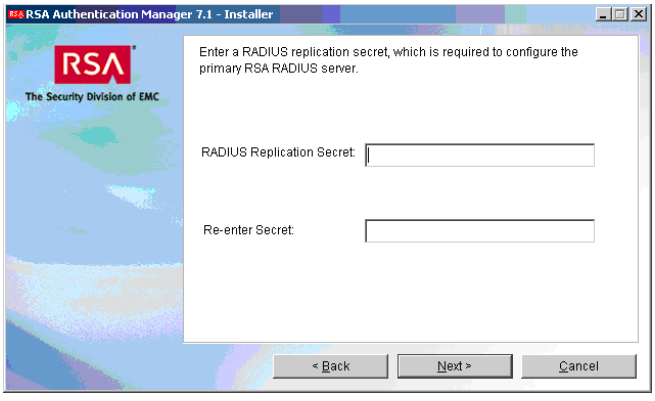


Note: When you complete the installation, you can set the RADIUS password not to expire. From Windows, click **Start > All Programs > Administrative Tools > Computer Management > Local Users and Groups > Users**. Right-click **Radius User > Properties**, and select **Password never expires**.

The RADIUS Replication Secret page is displayed.

The secret enables multiple instances of RADIUS to recognize one another.

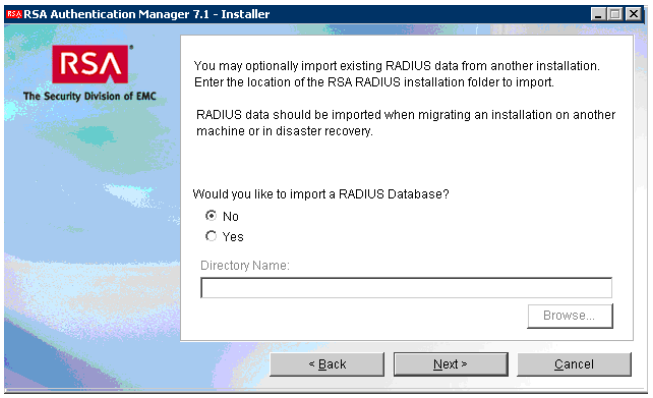
18. Enter and re-enter a secret, and click **Next**.
    (You can choose any value for the replication secret. There are no rules for the length or character type. However, you cannot use spaces.)



The Import RADIUS Data page is displayed.

You have the option of importing data from an existing installation of RADIUS.

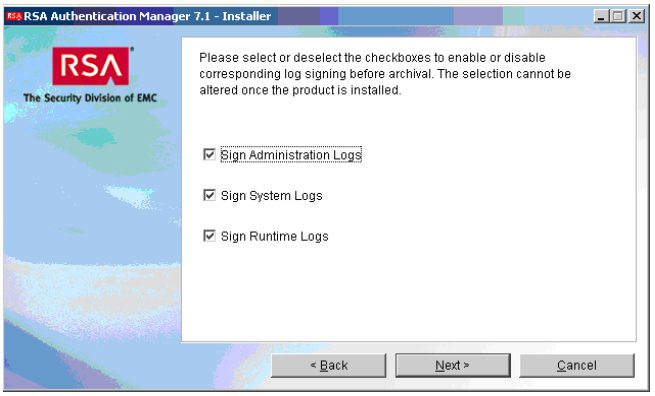
19. Select **No**, and click **Next**.



The Log Signing page is displayed.

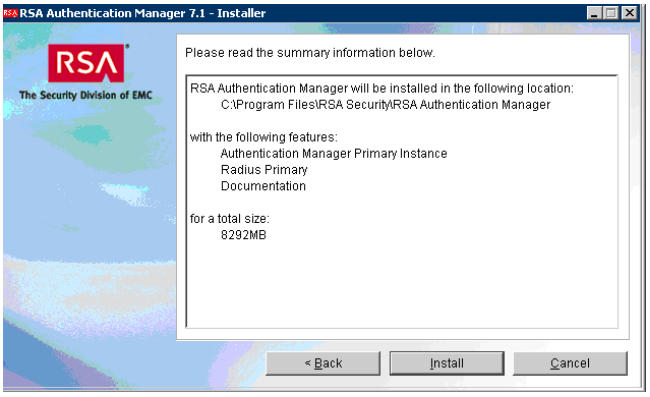
Log signing helps you detect tampering with log files.

20. Select or clear the log file categories, and click **Next**.

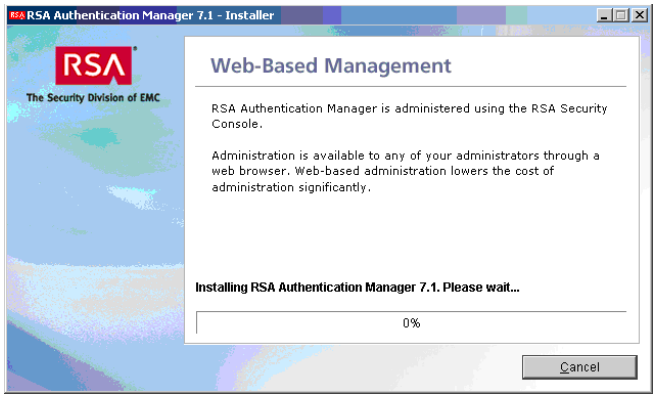


The Summary Information page is displayed.

21. Verify your selections for this installation, and click **Install**.



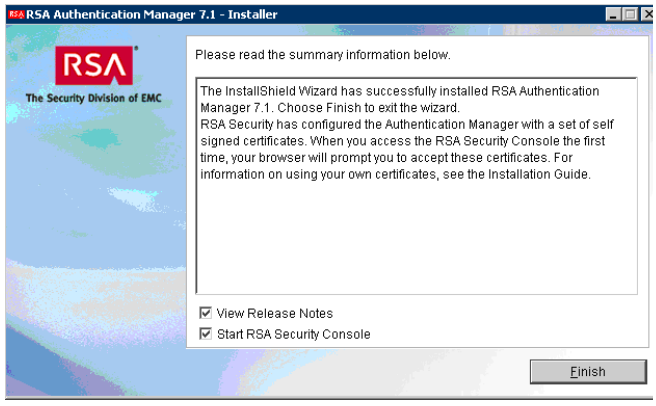
The Installation Progress page is displayed.



The Installation Completed page is displayed.

The installation script starts the Authentication Manager services and gives you the option of opening the *Release Notes* and the RSA Security Console in your browser.

22. Accept the defaults, and click **Finish**.



3 Administering RSA Authentication Manager

This chapter describes the following tasks for administering RSA Authentication Manager:

- Configure administrative policies
- Add security domains
- Add users and user groups
- Assign administrative roles

You perform all these tasks from the RSA Security Console.

Logging On to the RSA Security Console

If the RSA Security Console is not already open, perform the following procedure.

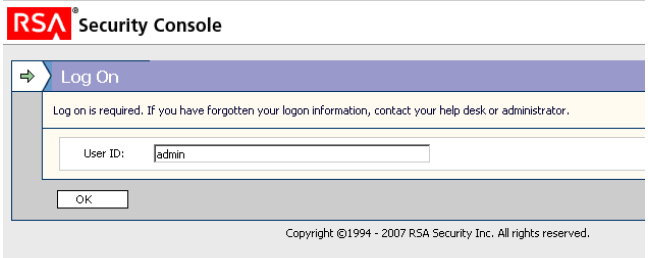
1. Open the RSA Security Console from the administrative workstation. Do one of the following:
   - Click **Start > Programs > RSA Security > RSA Security Console**
   - Go to **https://*server_name*:7004/console-ims**

   Use the fully qualified name (as registered with DNS) of the server on which Authentication Manager is installed.

The Security Alert page is displayed. (The content of this page is browser-dependent.)

2. Click **Yes**.

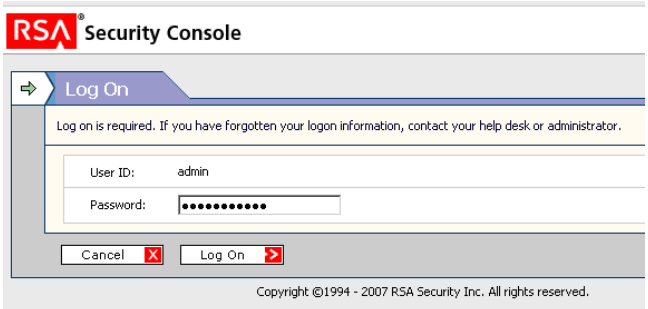
The User ID page is displayed.



3. Enter the User ID you supplied at installation for the RSA Security Console administrator, and click **OK**.

   In this example, the User ID is **admin**.

The Password page is displayed.



4. Enter the password you supplied at installation for the RSA Security Console administrator, and click **Log On**.

The RSA Security Console Home page is displayed.

Most administrative operations begin with clicking one of the tabs across the top of the page. The tabs repeat on most RSA Security Console pages.

Configuring Administrative Policies

The following administrative policies are included with RSA Authentication Manager:

- Password Policy
- Lockout Policy
- Self-Service Troubleshooting Policy
- Authentication Grade
- Token Policy
- Offline Authentication Policy

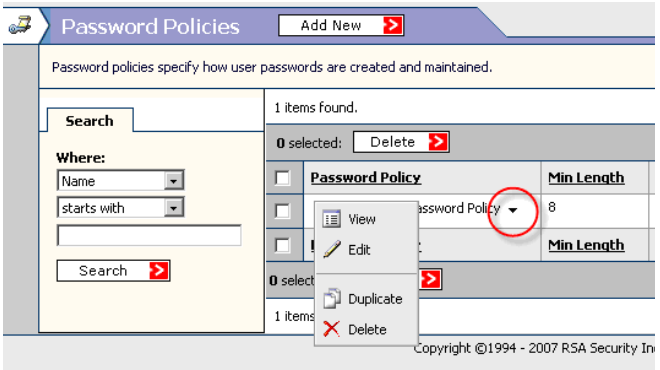
You can use these policies as defined, or modify them to create custom policies.

When a policy is set as the default, it applies to all security domains in the system that are not explicitly set to a different variant of that policy.

The following exercise creates a new password policy based on an existing policy and makes the new policy the default.

1. Click **Authentication > Policies > Password Policies > Manage Existing**.

2. On the Password Policies page, select Initial RSA Password Policy, and from the drop-down list, select **Duplicate**.



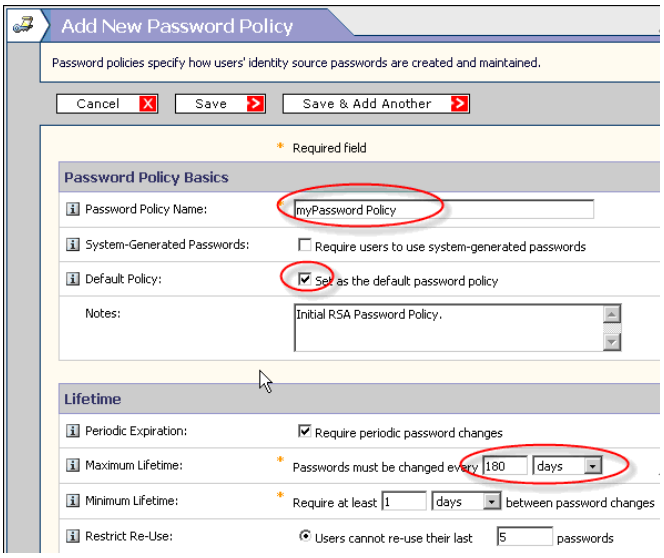
3. On the Add New Password Policy page, specify the new policy attributes.

   For this exercise, modify these fields:

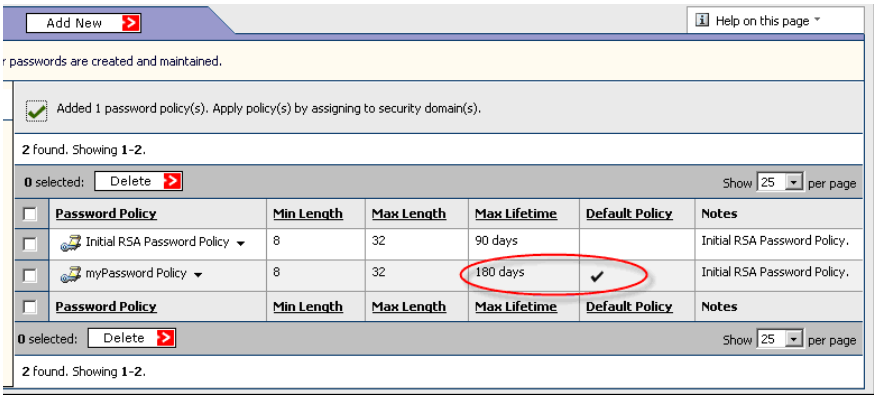
   In the **Password Policy Basics** section:
   - Password Policy Name: **my PasswordPolicy**
   - Default Policy: Select **Set as the default password policy**

   In the **Lifetime** section:
   - Maximum Lifetime: **180 days**

4. At the bottom of the page, click **Save**.



The new password policy is created and enabled as the default.



Adding Security Domains

When you install Authentication Manager, a top-level security domain is automatically created. By default, all users and tokens are managed in the top-level security domain. You may want to divide your users into geographic areas or define areas of administrative responsibility. To do this, you create security domains, each with specified administrators, users, and policies.

You create security domains from the RSA Security Console.

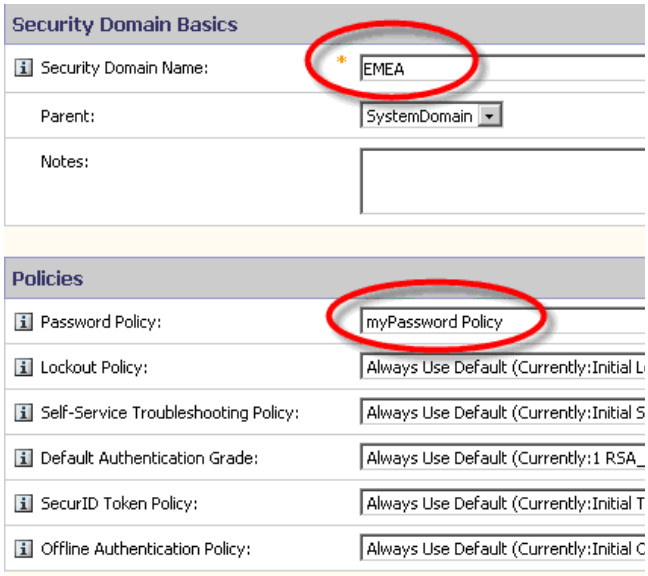
The following exercise creates two new security domains that reflect an organization's geographic areas, EMEA (Europe, Middle East, and Africa) and AsiaPac (Asia Pacific).

1. Click **Administration > Security Domains > Add New**.

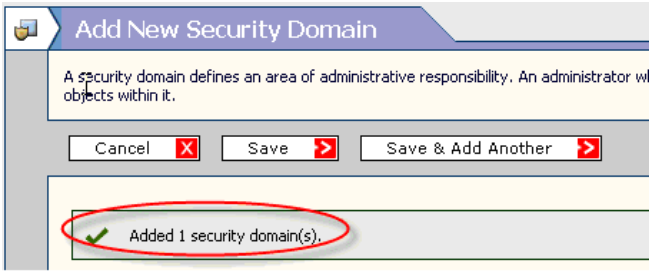
2. On the Add New Security Domain page, specify the attributes you want.

   For this exercise, modify these fields:
   - Security Domain Name: **EMEA**
   - Password Policy: **myPasswordPolicy**

3. At the bottom of the page, click **Save and Add Another**.



When the Add New Security Domain page refreshes, the EMEA security domain has been added.

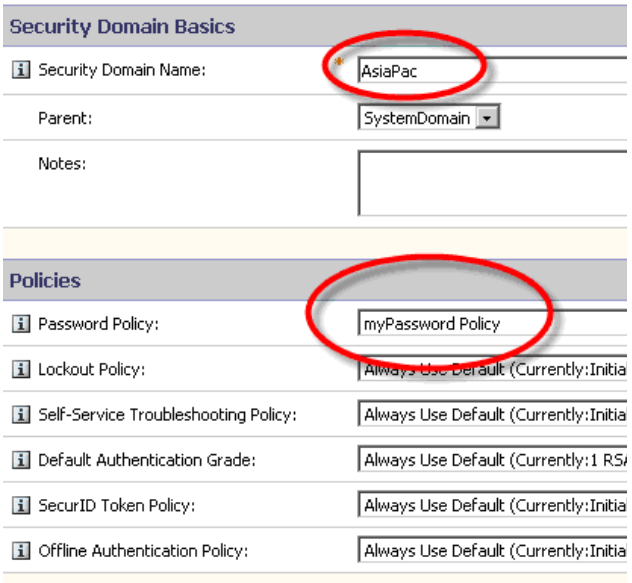


4. Specify the attributes for another new security domain.

   For this exercise, specify:
   - Security Domain Name: **AsiaPac**
   - Parent: **SystemDomain**

   Because you have more than one security domain, you must specify the parent of the new security domain.

   Note: The new security domain is assigned the default Password Policy (unless you specify otherwise). It does not inherit the policies of the parent security domain.



5. Click **Save**.

You have now created two security domains under the top-level security domain, SystemDomain.

Adding Users and User Groups

After you add users to your RSA Authentication Manager deployment, you can:

- Delete users
- Edit user information
- Assign users to a security domain
- Add users to user groups
- Disable and re-enable users
- Lock and unlock users

In a more complex deployment, you can link to users in an external identity source, such as an LDAP directory.

You perform these tasks from the RSA Security Console.

The following exercise adds a user and stores his information in the Authentication Manager internal database. It then shows how to view and edit the user's attributes.

1. Click **Identity > Users > Add New**.

2. On the Add New User page, specify the user attributes.

   For this exercise, modify these fields:

   In the **Administrative Control** section:
   – Identity Source: **Internal Database**
   – Security domain: **SystemDomain**

   In the **User Basics** section: Enter the user's name, User ID, and Email.

   In the **Password** section:
   – Password: Enter a password
   – Force Password Change: Make sure the checkbox is not selected.

3. Click **Save**.

4. To view the attributes of the new user, click **Identity > Users > Manage Existing**, and search for the user name.

	User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
	jsmith	smith, john			SystemDomain	Internal Database

5. To edit the user attributes, select the User ID, and from the drop-down list, select **Edit**.

You can create user groups if you want to manage collections of users. For instance, you can create groups for Open Web Application (OWA) users and VPN users and then restrict the web server and the VPN server to the appropriate group.

The following exercise creates groups for OWA and VPN users, and then shows how to view and edit their attributes.

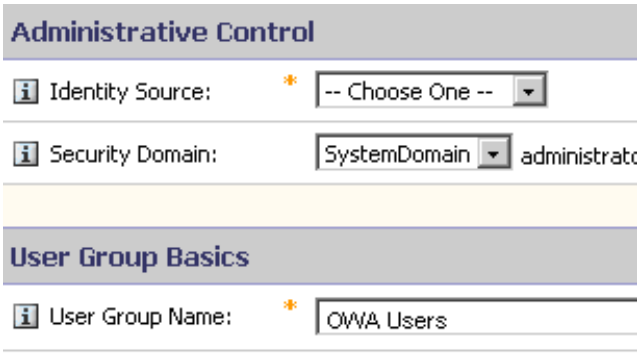
1. Click **Identity > User Groups > Add New**.

2. On the Add New User Group page, specify the group attributes.

   For this exercise, modify these fields:

   In the **Administrative Control** section:
   – Identity Source: **Internal Database**
   – Security Domain: **SystemDomain**

   In the **User Group Basics** section:
   – User Group Name: **OWA Users**

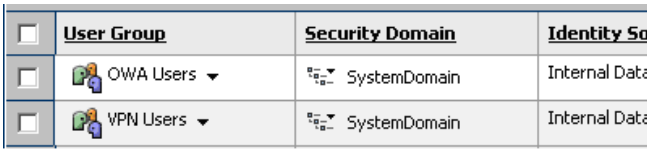


3. Click **Save and Add Another**.

4. Repeat the procedure to create a group named VPN Users.

5. To view the attributes of the new user groups, click **Identity > User Groups > Manage Existing**.

6. To edit the user group attributes, select the user group name, and from the drop-down list, select **Edit**.

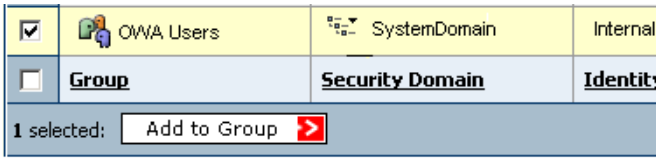


Once you have created a user group, you can add users to it. A user can be in any number of user groups, and user groups can be included within other user groups.

The following exercise shows you how to add user jsmith to the user group, OWA Users.

1. Click **Identity > Users > Manage Existing**.
2. On the Users page, use the search fields to find user jsmith.
3. Select the checkbox next to user jsmith.
4. At the bottom of the Users page, from the drop-down list, select **Add to User Groups**, and click **Go**.

5. On the Add User Group Membership page, select the **OWA Users**, and click **Add to Group**.



Adding and Assigning Administrative Roles

You can assign any user to one or more administrative roles. Assigning a user to an administrative role gives the user the permissions associated with that role.

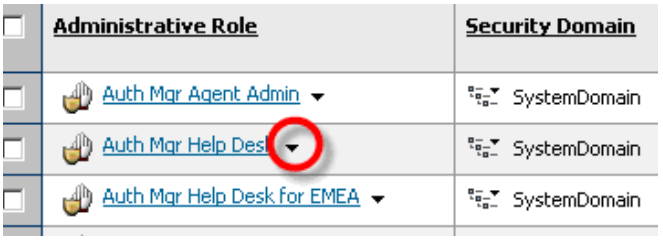
Authentication Manager includes some predefined administrative roles. You can use a role as defined, edit the permissions to modify the role, or create a new role.

You perform these tasks from the RSA Security Console.

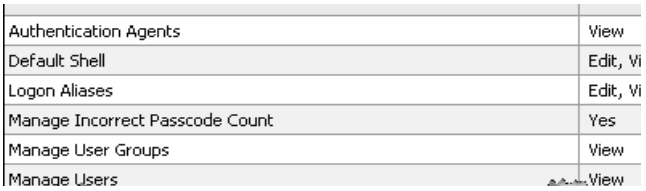
The following exercise views the details of an administrative role.

1. Click **Administration > Administrative Roles > Manage Existing**.

2. On the Administrative Roles page, from the drop-down list next to any role name, select **View**.



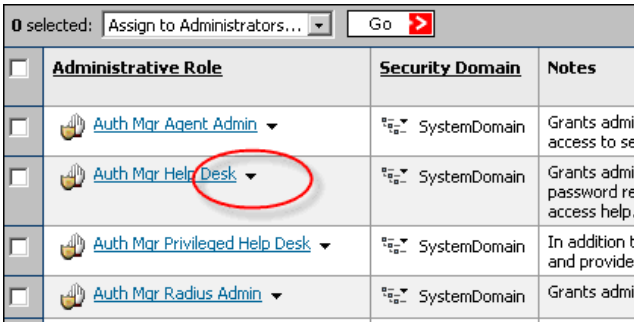
A list showing the tasks and the permissions for each task is displayed.



The following exercise creates a new Help Desk Administrator role with permissions limited to the EMEA security domain, and then assigns user jsmith that role.

1. Click **Administration > Administrative Roles > Manage Existing**.

2. Select **Auth Mgr Help Desk**, and from the drop-down list, select **Duplicate**.



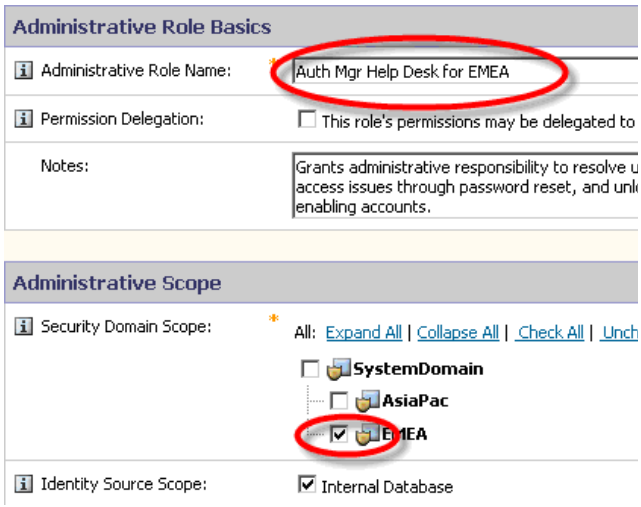
3. On the Add New Administrative Role page, specify the attributes of the new role.

   For this exercise, modify these fields:

   In the **Administrative Role Basics** section:
   – Administrative Role Name: **Auth Mgr Help Desk for EMEA**

   In the **Administrative Scope** section, under Security Domain Scope:
   – Clear **SystemDomain**
   – Select **EMEA**

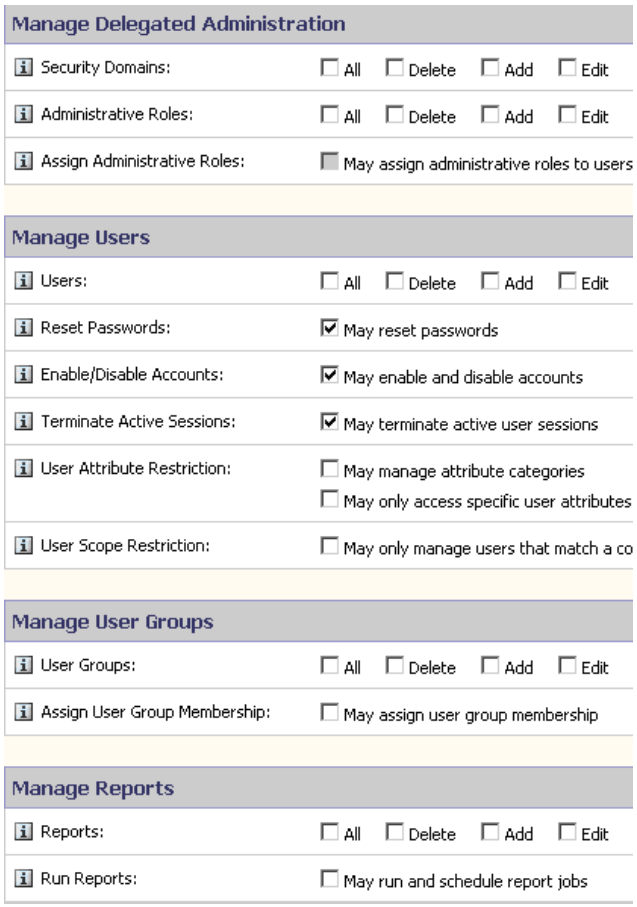
4. Click **Next**.



A series of pages follow, showing all the permissions, by category, and their settings for the administrative role you are adding.

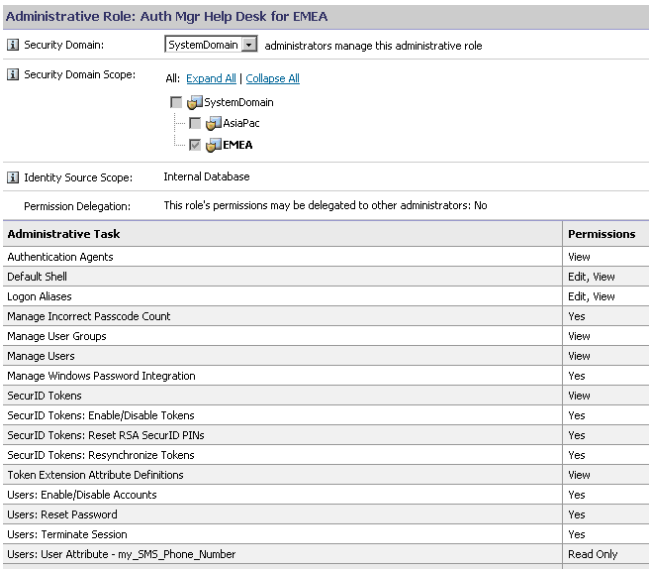
You can edit the permissions for the new administrative role by selecting or clearing the checkboxes. (This exercise makes no changes.)

5. Click **Next** after reviewing each page.



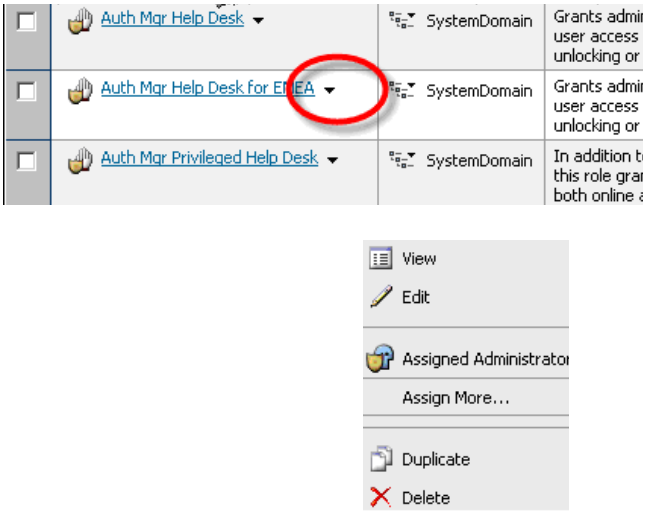
The next page lists the permissions you selected for the administrative role you are creating.

6. Click **Save** to create the new administrative role.



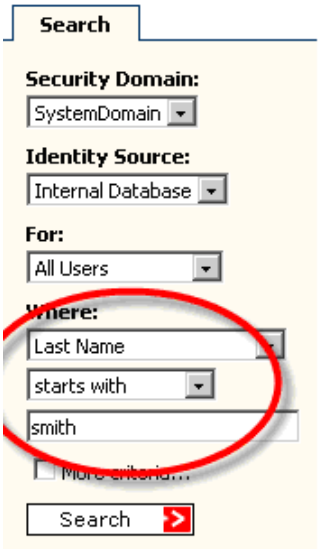
7. Click **Administration > Administrative Roles > Manage Existing**.

8. Select **Auth Mgr Help Desk for EMEA**, and from the drop-down list, select **Assign More**.

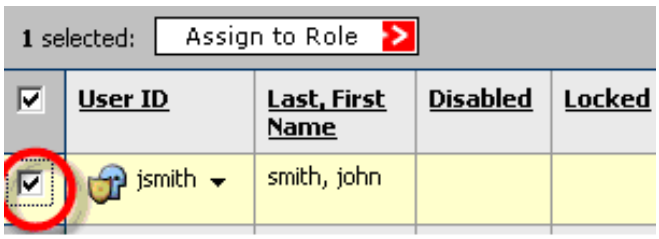


A search window is displayed.

9. Search for **smith**.



10. When user name **jsmith** is displayed, select the checkbox next to **jsmith**, and click **Assign to Role**.



User jsmith is now a Help Desk Administrator for EMEA. Although jsmith is a user in the SystemDomain security domain, he has administrator privileges only in the EMEA security domain.

4 Administering Authentication Agents

An authentication agent protects a network resource, such as a web server or VPN server, by granting access only to users who are verified by RSA Authentication Manager.

To establish this protection, you need to:

- Register the agent with Authentication Manager
- Install the agent on the host resource
- Enable the agent to communicate with Authentication Manager
- Configure the agent to use RSA SecurID authentication

The exercises in this chapter use the authentication agent for Microsoft Internet Information Services (IIS), which you downloaded in preparation for these exercises. If you want to do the exercises with a different agent, you can download the appropriate authentication agent from the RSA web site.

You perform these exercises on the RSA Security Console and on the server where IIS is installed.

Registering an Agent

The first step in establishing protection for a network resource is to create an agent record in Authentication Manager for the IIS agent. This process is called registering the agent. The agent record identifies the agent to the Authentication Manager. You also generate a file, **SDCONF.REC**, that enables the agent to communicate with Authentication Manager.

The following exercise registers the RSA Authentication Agent 5.3 for Web for Internet Information Services with Authentication Manager.

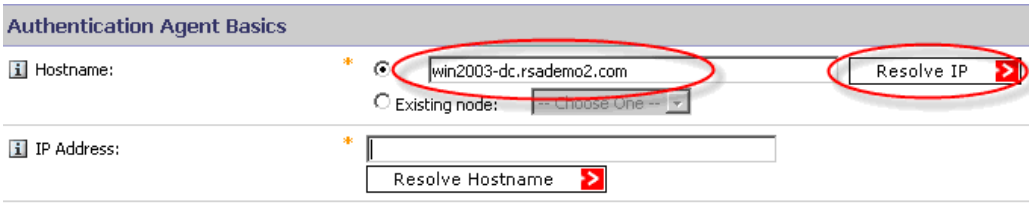
1. Click **Access > Authentication Agents > Add New**.

2. On the Add New Authentication Agent page, specify the agent host and its attributes.

   For this exercise, modify these fields:

   In the **Authentication Agent Basics** section:

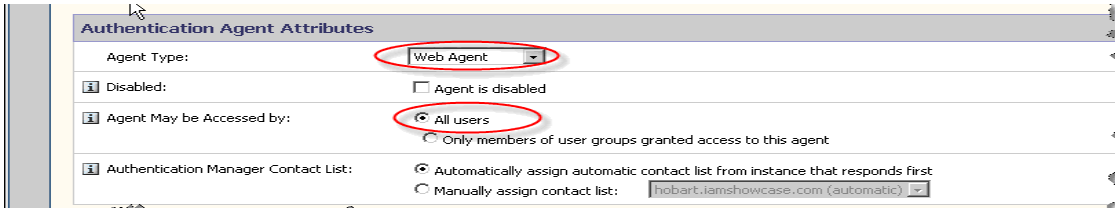
   – Hostname: Enter the hostname of the IIS server
   – Click **Resolve IP**



Note: If your are entering input specific to your organization, make sure you enter your server hostname as registered with DNS. Otherwise, Authentication Manager cannot resolve the IP address.

   In the **Authentication Agent Attributes** section:

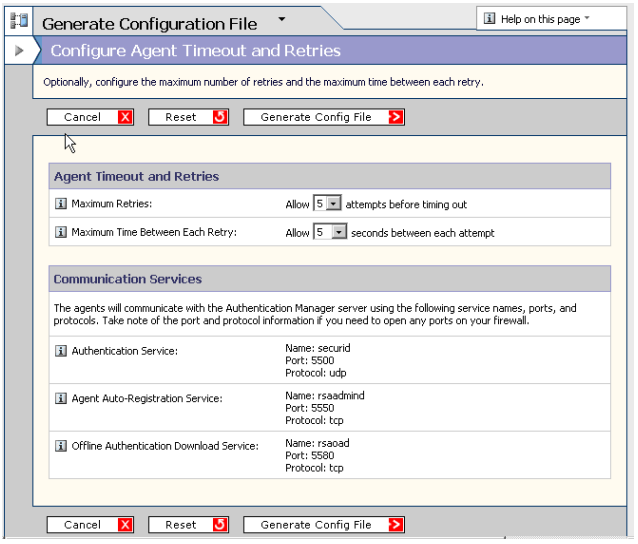
   – Agent Type: Select **Web Agent**
   – Agent May be Accessed by: Select **All Users**



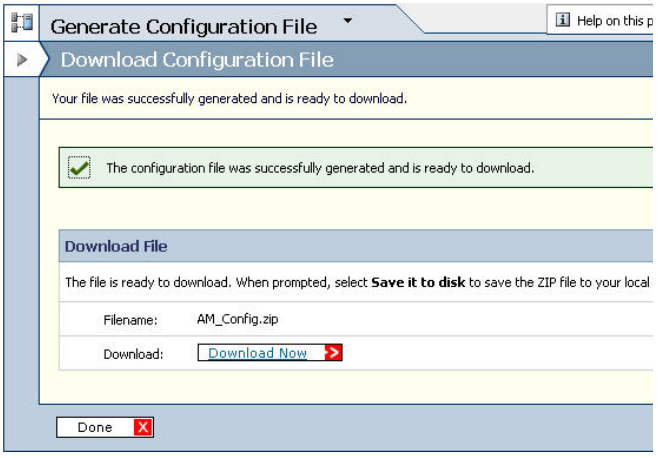
3. Click **Save**.

4. Click **Access > Authentication Agents > Generate Configuration File**.

5. On the Generate Configuration File page, click **Generate Config File**.



6. When the file is generated, click **Download Now**, and save the **AM_Config.zip** file to a temporary directory on the administrative workstation.

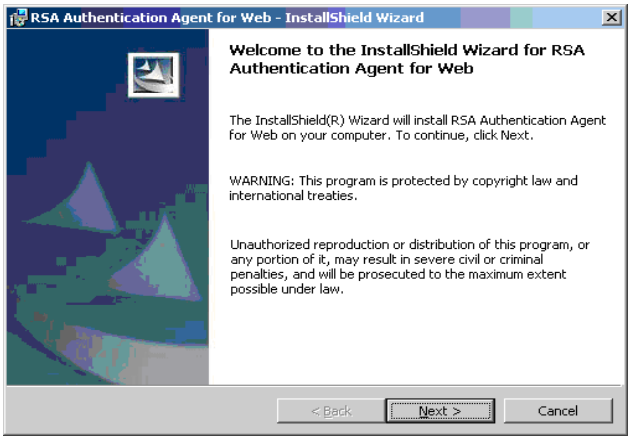


Installing an Agent

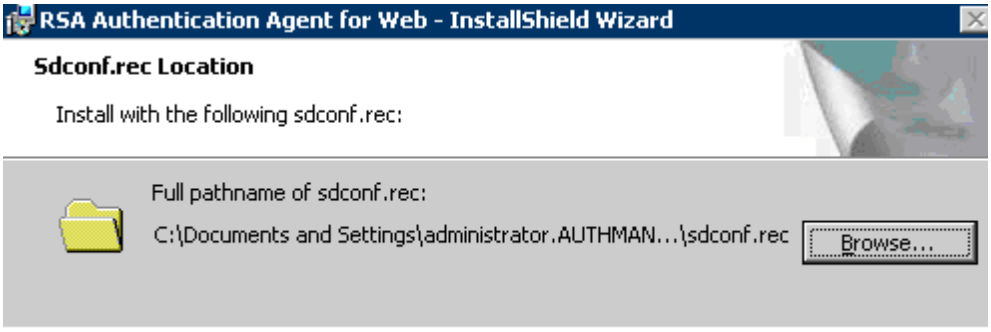
After you register the agent, you must install the agent on the resource to be protected.

The following exercise installs RSA Authentication Agent 5.3 for Web for Internet Information Services on the IIS server.

1. Log on to the IIS server as an administrator.
2. Copy the **AM_Config.zip** file from the Authentication Manager server to a temporary directory on the IIS server.
3. Extract the **SDCONF.REC** file from **AM_Config.zip**.
4. From the **c:*temp*\RSA_WebAgent_53_for_MS_IIS** directory, run **setup.exe** to start the agent installation wizard.
5. On the screens that follow, click **Next** to accept the place of purchase and the license agreement.

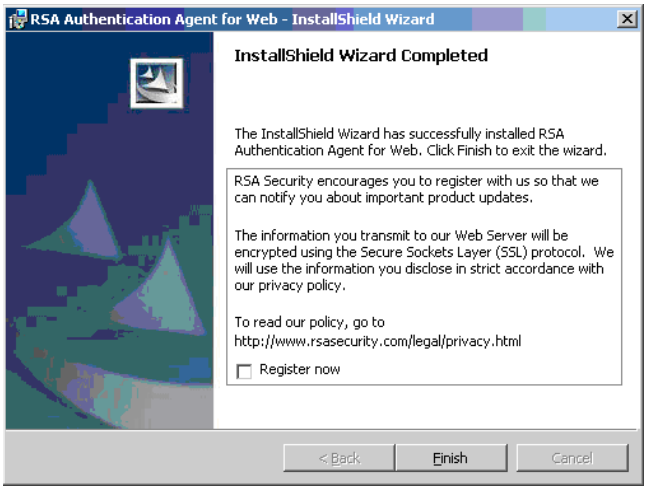


6. Click **Browse** to locate the **SDCONF.REC** file.



7. Click **Next**.
8. On the screens that follow, click **Next** to accept the destination folder, and click **Install** to begin the installation.

9. When the installation is complete, click **Finish** to exit the installation wizard.

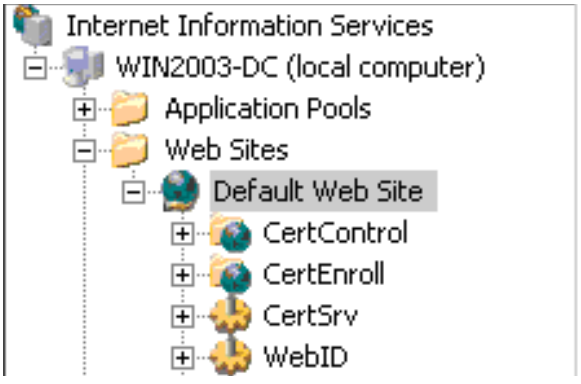


Enabling an Agent for IIS

Once the agent is installed, you must configure the agent host to use Authentication Manager to protect the server or particular web pages. When RSA SecurID authentication is enabled and the resources are configured to use it, a user must present a valid passcode to gain access.

The following exercise enables RSA SecurID authentication on an IIS server and configures a web page on the server to use RSA SecurID to authenticate users trying to gain access.

1. On the IIS server, click **Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand the directory tree to view the Web Sites directory.
3. Select the **Default Web Site** folder.
4. Right-click, and select **Properties**.

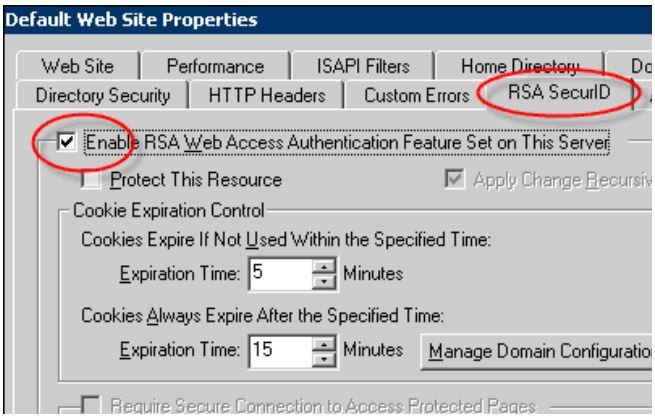


5. On the Default Web Site Properties page, click the **RSA SecurID** tab.

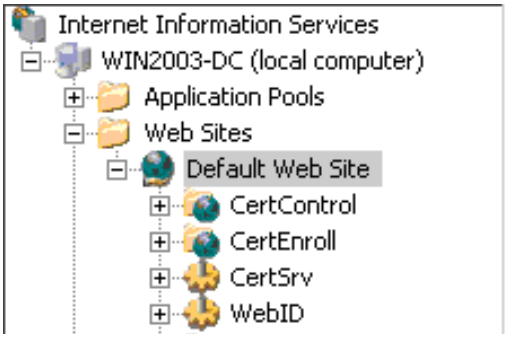
6. Select **Enable RSA Web Access Authentication Feature Set on This Server**.

7. Click **Apply**.

8. Click **OK**.



9. On the IIS Manager page in the **Default Web Site** folder, select a web site you want to protect.



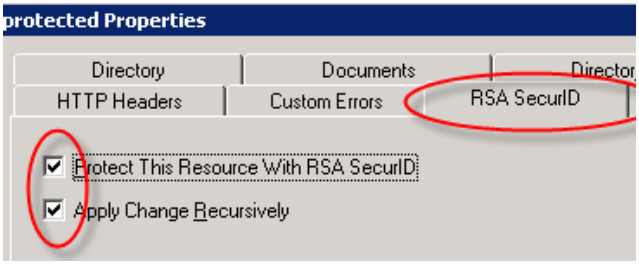
10. If the web site you want to protect is a file (rather than a folder), right-click the filename.

    If the web site you want to protect is a folder, expand the folder, select the **protected** subfolder, right-click, and select **Properties**.

11. On the Protected Properties page, select **Protect This Resource With RSA SecurID** and **Apply Change Recursively**.

12. Click **Apply**.

13. Click **OK**.



14. Click **File > Exit** to close the Microsoft IIS Manager.

5 Administering Tokens

RSA SecurID tokens are hardware or software entities that generate a semi-random number, called a tokencode, which changes periodically.

When trying to access a protected resource, the user enters a SecurID PIN and the tokencode from his or her token. This is called two-factor authentication: something you know (the PIN) and something you have (the token). The combined PIN and tokencode are called a passcode.

RSA Authentication Manager verifies that a user seeking access has entered a valid passcode.

To administer tokens, you need to:

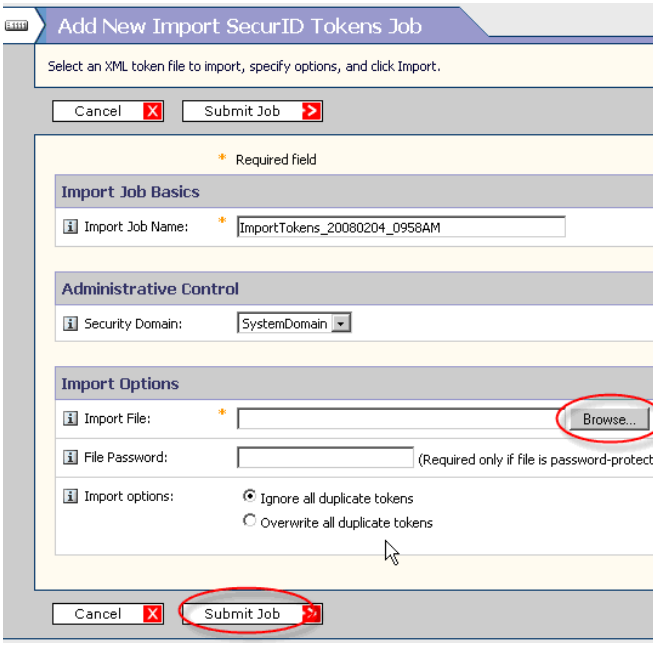
- Import token records
- Assign tokens to users
- Instruct users on using the tokens

You administer tokens from the RSA Security Console.

Importing Tokens

The following exercise imports token records into Authentication Manager. It refers to the token record files you copied onto the administrative workstation in preparation for these exercises.

1. Click **Authentication > SecurID Tokens > Import Tokens Job > Add New**.
2. Select the security domain where you want to import the token records. This exercise imports the token records into the top-level security domain (the default).
3. **Browse** to locate the token records on the administrative workstation.
4. Click **Submit Job**.



The Import SecurID Token Jobs page is displayed, which shows that the job is in progress.

5. Click the **Completed** tab to see if the tokens have been imported.

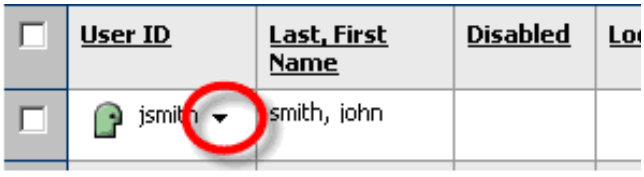
Assigning Tokens

After importing tokens, you can assign them to users.

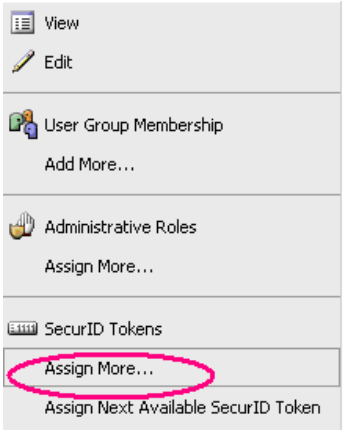
The following exercise assigns a hardware token to user jsmith.

1. To view all users, click **Identity > Users > Manage Existing**.

2. On the Manage Existing Users page, **Search** for user jsmith.

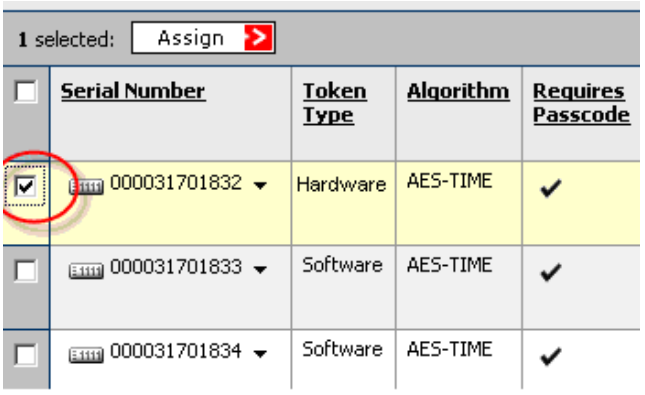


3. Select the user name, and from the drop-down list in the SecurID Tokens section, click **Assign More**.



On the Assign SecurID Tokens page, select an available token serial number, and click **Assign**.

Note: Select the appropriate type of token, hardware or software.



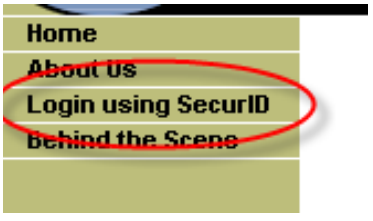
Using Tokens

Once you assign the tokens to users, you must instruct the users how to access a network resource protected by RSA SecurID authentication.

The following exercise shows how to access a web site on the IIS server (or other server) that you previously configured to use RSA SecurID authentication. For this exercise, you are user jsmith.

1. Direct your browser to a protected page on the IIS server.

2. Click **Login using SecurID**.



3. On the Log In page, enter the user name **jsmith**, and the number that is currently showing (tokencode) on the token you assigned to that user.

Authentication Manager recognizes that the user is logging on for the first time, and prompts the user to establish a PIN.

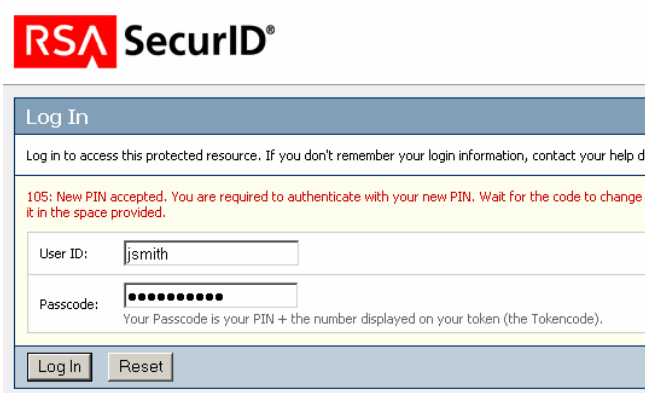
4. Enter and re-enter a PIN.

5. Click **OK**.

6. On the Log In page, enter the passcode.

   The passcode is your PIN followed by the tokencode that your token currently displays.

7. Click **Log In**.



You are now logged on to the protected web site.

6 Reporting and Monitoring

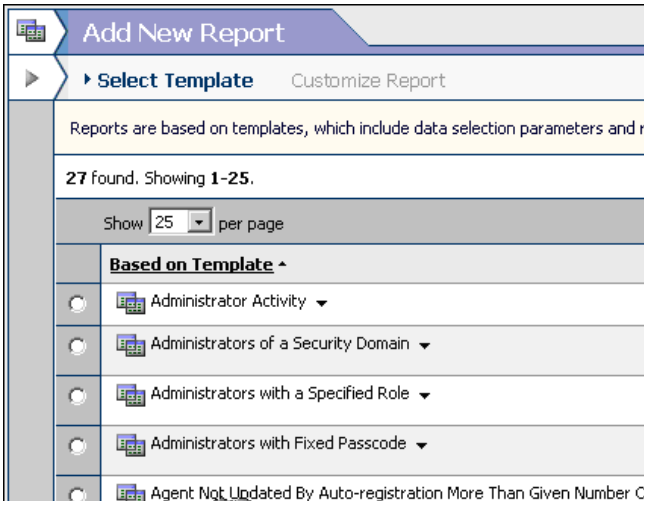
Authentication Manager keeps records of logon attempts and other system events. You can generate batch reports of these events or monitor them in real time.

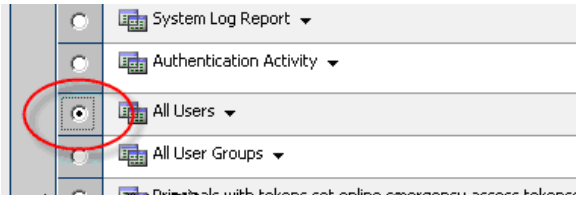
You perform these tasks from the RSA Security Console.

Generating Reports

The following exercise shows how to create, run, and view a report named My Users. This report is based on the predefined report template, All Users.

1. Click **Reporting > Reports > Add New**.
2. On the Add New Report page, in the **Based On Template** section, select **All Users**.
3. Click **Next**.

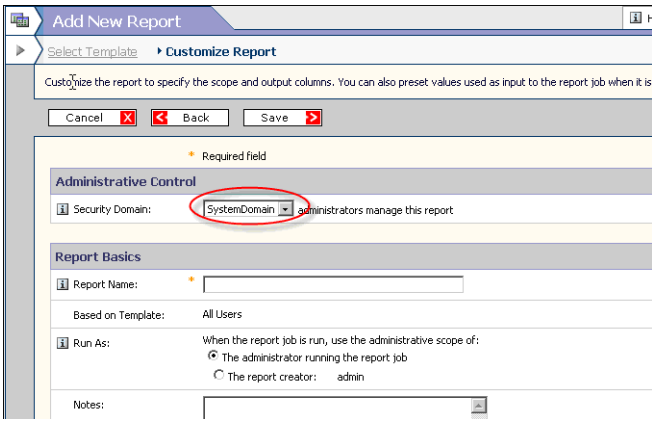




4. On the Add New Report page, specify the report name and parameters.

   For this exercise, modify these fields:
   - Report Name this report **My Users**.
   - Accept the defaults for the other parameters.

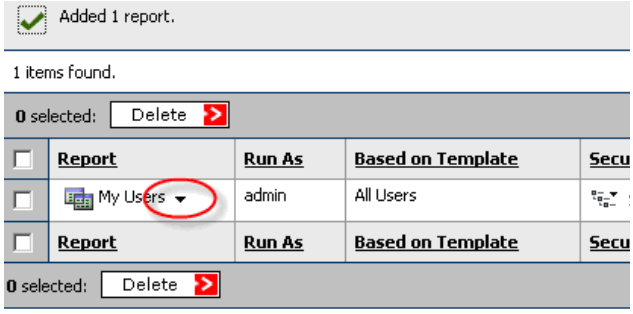
5. Click **Save**.



6. Click **Reporting > Reports > Manage Existing**.

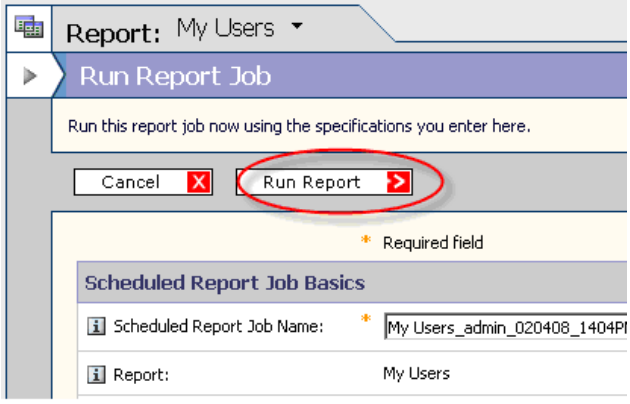
7. On the Reports page, select **My Users**, and from the drop-down list, select **Run Report Job Now**.

   The server generates a job request for your report.



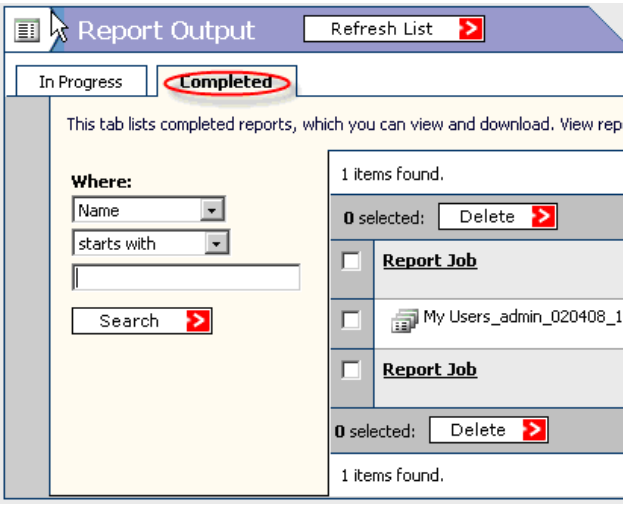
8. On the Run Report Job page for the **My Users** report, click **Run Report**.

   A Report Output page is displayed showing that the job status is **In Progress**.



9. On the Report Output page, click the **Completed** tab to see whether the job is complete.

   The Report Output page reports that this job has completed.



10. From the drop-down list beside the report name **My Users**, select the report output format.

    You can view the report on the Authentication Manager server. or download the report to your administrative workstation.

Monitoring System Events

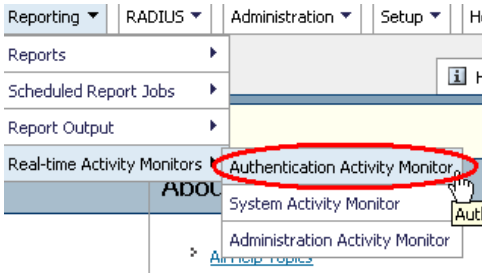
Authentication Manager provides the following real-time activity monitors:

- **Authentication Activity Monitor.** Displays authentication-specific events, such as authentication requests and restricted agent access checks.
- **System Activity Monitor.** Displays system events, such as the replication of data.
- **Administrator Activity Monitor.** Displays administrator activities, such as creating and updating users.

An Activity Monitor opens in a new browser window. You can launch Activity Monitors from the RSA Security Console and leave them running.

The following exercise launches the Authentication Activity Monitor.

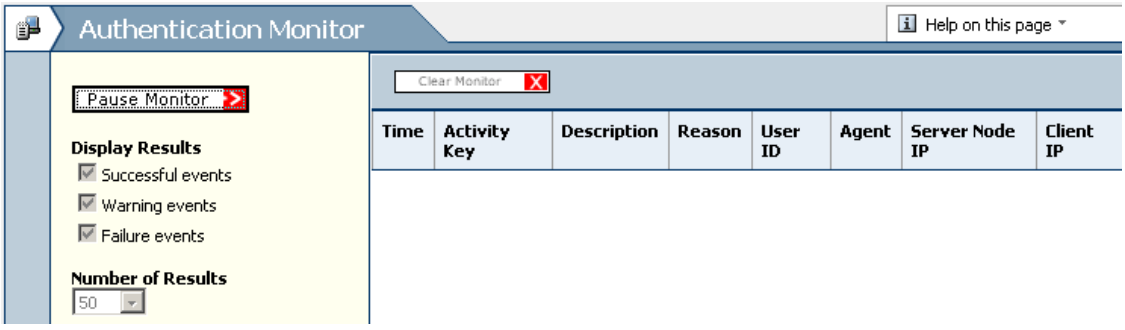
1. Click **Reporting > Real-Time Activity Monitors > Authentication Activity Monitor**.



2. On the Authentication Monitor page:
   – Select the events you want to display.
   – Select the number of results to display.

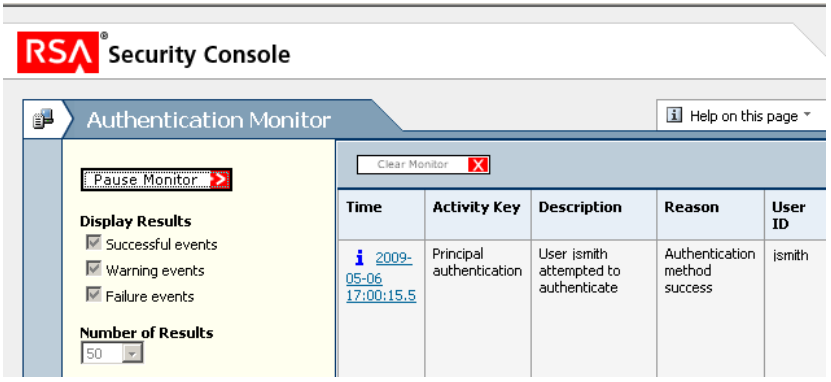
3. Click **Start Monitor**.

The monitor starts in a separate browser window, and runs until you close it.



4. To see the Authentication Monitor in action, you can repeat the procedure of logging on to a protected web site as jsmith. See "Using Tokens" on page 39.

   The Authentication Monitor immediately reports authentication activity on behalf of user jsmith.



At any time, you can generate a report of the authentication activities, using the Reporting facility. See "Generating Reports" on page 41.

The Security Division of EMC

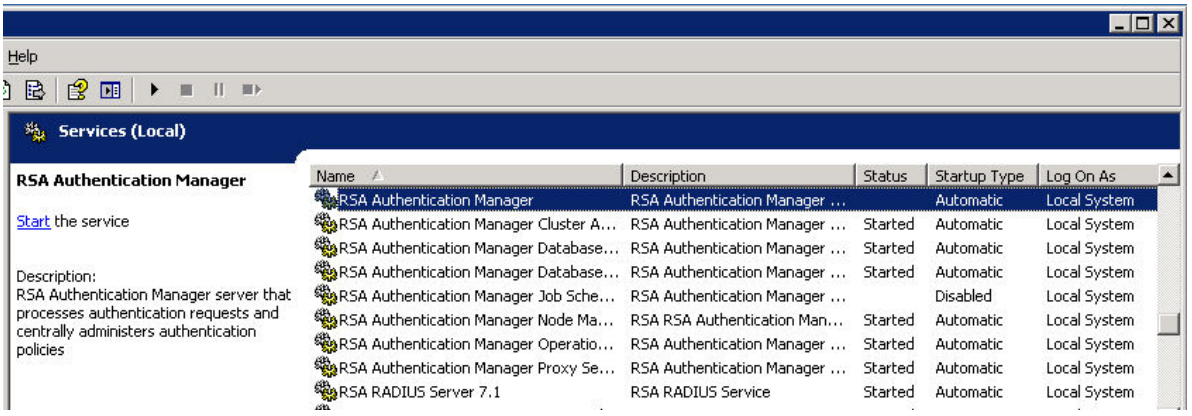
A Starting RSA Authentication Manager Manually

RSA Authentication Manager is set to start automatically after installation and whenever the server reboots.

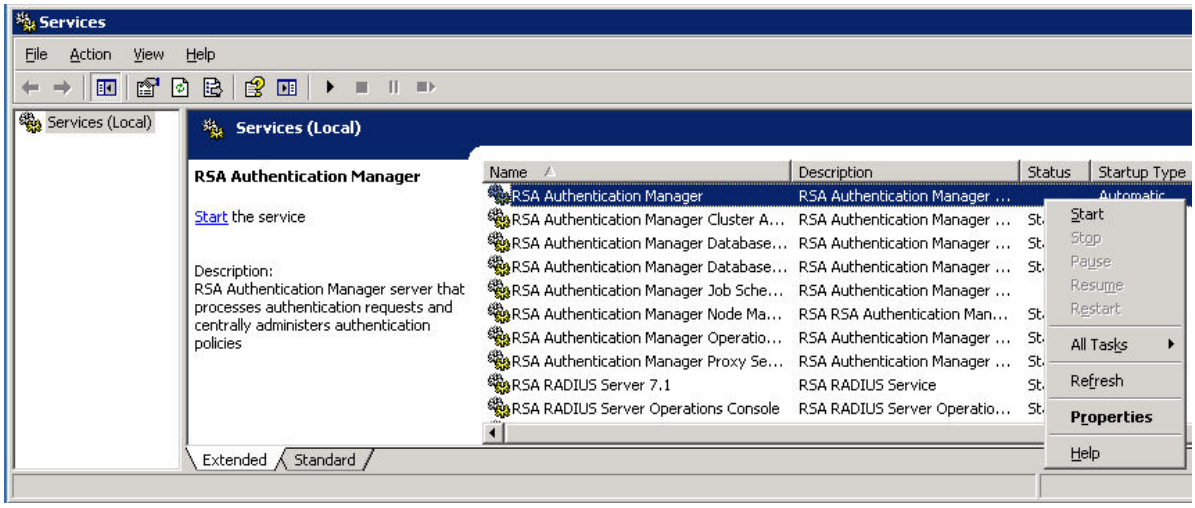
If you try to access the RSA Security Console and do not succeed, check to see whether Authentication Manager and its back-end services are started. If not, you can start them manually.

1. On the server where Authentication Manager is installed, click **Start > All Programs > Administrative Tools > Services**.

   Scroll down to the set of services that begin with "RSA." The start-up status of RSA Authentication Manager is blank in the following example.

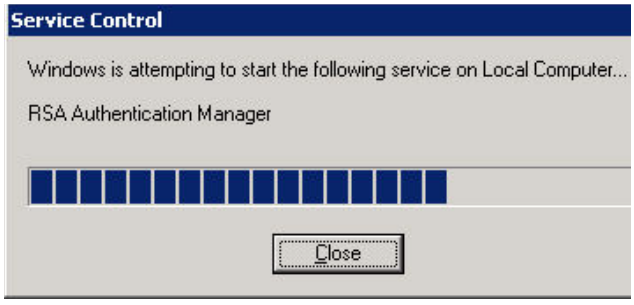


2. If the RSA Authentication Manager service is not **Started** or **Starting**, right-click **RSA Authentication Manager**, and select **Start**.

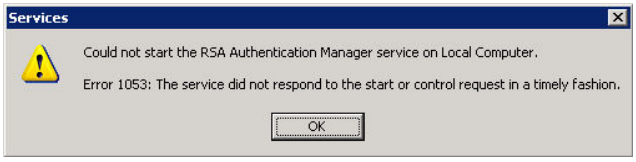


As Authentication Manager starts up, a progress window is displayed. Startup might take several minutes.

When the Authentication Manager service starts, it starts all the related RSA services.



You may see this error message. The message indicates that the Windows GUI timed out waiting for the startup process to complete.



3. Click **OK**.

Upon completion, the Authentication Manager status, and the status of its related services, are shown as **Started**.