

RSA Authentication Agent 7.2 for Microsoft Windows Installation and Administration Guide



Contact Information

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

Trademarks

RSA, the RSA Logo, SecurID and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.rsa.com/legal/trademarks_list.pdf.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-party licenses

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

Note on encryption technologies

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

Distribution

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

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

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

Contents

Preface	7
About This Guide.....	7
RSA Authentication Agent for Microsoft Windows Documentation.....	7
Related Documentation.....	7
Support and Service.....	8
Before You Call Customer Support.....	8
Chapter 1: Product Overview	9
RSA Authentication Agent for Microsoft Windows.....	9
Key Features.....	10
Challenge Users for RSA SecurID Passcodes.....	10
RSA SecurID Authentication without an Authentication Manager Connection.....	10
Integration of Windows Passwords in the RSA SecurID Logon Process.....	11
Automatic Password Synchronization.....	11
Access to Protected Desktops in Emergency Situations.....	11
Central Management of Authentication Settings.....	12
Automatic Update of IP Addresses.....	13
Access to Protected Computers Using a PIN or Password.....	13
Multidomain Group Support.....	14
Fast User Switching.....	14
Options to Customize RSA Authentication Agent.....	15
Supported Authenticators.....	17
RSA Control Center.....	18
RSA Control Center Icons.....	20
Chapter 2: Preparing for Installation	21
System Requirements.....	21
Required Ports.....	21
Supported Operating Systems.....	22
Supported Third-Party Remote Access Products.....	22
Supported RSA Authentication Manager Products.....	23
Supported Third-Party Credential Providers.....	23
Remote Access Support.....	24
Preparations to Install Authentication Agent.....	25
Set Up RSA Authentication Manager.....	26
Create Groups of Users to Challenge with RSA SecurID.....	27
Choose Emergency Access Methods.....	28
Prepare Users for RSA SecurID Authentication.....	30
Chapter 3: Installing RSA Authentication Agent	31
Installation Methods.....	32
Single Installations.....	32
Large-Scale Deployments.....	33

Import Authentication Manager Files	33
Installation Considerations	34
Install the Product on a Single Computer	36
Install the Product on Multiple Computers	38
Create an Installation Package	38
Provide Account Control Privileges to User Computers	41
Deploy the Installation Package to Multiple Computers	42
Test the Installation	43
Review the Server Settings	43
Test Authentication	44
Install a Language Pack	46
Use the Node Secret Load Utility	47
Modify an Installation	48
Modify the Installation for a Single Computer	48
Modify the Installation for Multiple Computers	49
Repair an Installation	50
Upgrade to RSA Authentication Agent 7.2	51
Uninstall the Product	51
Uninstall the Product from a Single Computer	52
Uninstall the Product from Multiple Computers	52
Uninstall the Language Pack	53
Chapter 4: Managing Authentication Agents	55
Offline Authentication	55
Password Changes and Offline Authentication	56
Clock Changes and Offline Authentication	56
Manage Offline Days	57
Refresh Offline Days	57
Check the Supply of Offline Days	59
Clear Offline Data	60
Emergency Access	60
Emergency Access Options	61
Reserve Passwords	61
Set Up Offline Authentication	62
Users Who Work Locally and Remotely	62
Different Remote Users Who Share a Computer	63
Users Who Only Work Remotely	64
Automatic Registration Process	64
Prevent Automated Registration During Specified Events	65
Automated Registration and the Node Secret	66
Automated Registration and Offline Authentication	67
Maintain the Primary IP Address of the Authentication Agent Host	67
Multidomain Group Support	68
Automatic Password Synchronization	70

Chapter 5: Troubleshooting	71
Offline Authentication and the Auto-Registration Utility	71
Authentication Issues	72
RSA SecurID 800 Driver Might Not Install Automatically	72
Authentication Fails After Changing the ‘Send Domain and Username Option’	72
Test Authentication Succeeds, but Actual Authentication Fails.....	72
Node Verification Fails.....	72
Correct a Node Verification Failure	73
Enable Tracing	74
Diagnose Authentication Issues	74
Verify the Accuracy of the Computer Clock	74
Verify the System Configuration (sdconf.rec) File	74
Replace the System Configuration (sdconf.rec) File	75
Error and Event Viewer Log Messages	76
Appendix A: Configuring Automatic Load Balancing	81
Automatic Load Balancing	81
Dynamic Load Balancing	81
Manual Load Balancing.....	81
Manage an sdopts.rec File.....	82
Create an sdopts.rec File.....	82
Exclude an Authentication Manager Server During Dynamic Load Balancing.....	85
Configure Manual Load Balancing.....	85
Specify Alias IP Addresses for Use or Exclusion.....	86
Specify an Overriding IP Address	87
Glossary	89
Index	93

Preface

About This Guide

This guide describes how to install and configure RSA Authentication Agent 7.2 for Microsoft Windows. It is intended for administrators and other trusted personnel. Do not make this guide available to the general user population.

RSA Authentication Agent for Microsoft Windows Documentation

For more information about RSA Authentication Agent 7.2, see the following documentation and Help:

Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues. The latest version of the *Release Notes* is available on RSA SecurCare Online at <https://knowledge.rsasecurity.com>.

Group Policy Object Template Guide. Describes how to use Group Policy Object templates to configure RSA Authentication Agent 7.2 for Microsoft Windows. For example, you can use a policy template to define how users authenticate, define challenge groups, and set the logon field label.

RSA Authentication Agent Help. Describes user and administration tasks performed in the RSA Control Center. (The Control Center is the user interface for Authentication Agent.) For example, it contains procedures for users to refresh offline days or check their logon options. For administrators, it includes procedures to test authentication, enable a reserve password, override an IP address, enable tracing, challenge users, clear a node secret or offline data, and review server information.

Related Documentation

For more information about products related to RSA Authentication Agent 7.2, see the following:

RSA Authentication Manager documentation set. See the full documentation set for RSA Authentication Manager (6.1 or 7.1). To access a documentation set, go to <http://knowledge.rsasecurity.com>.

RSA Secured Partner Solutions directory. RSA has worked with a number of manufacturers to qualify software that works with RSA products. Qualified third-party products include virtual private network (VPN) and remote access servers (RAS), routers, web servers, and many more. To access the directory, including implementation guides and other information, go to <http://www.rsasecured.com>.

Support and Service

RSA SecurCare Online	https://knowledge.rsasecurity.com
Customer Support Information	www.emc.com/support/rsa/index.htm
RSA Solution Gallery	https://gallery.emc.com/community/marketplace/rsa?view=overview

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

The RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The directory includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Before You Call Customer Support

Make sure that you have direct access to the computer running the RSA Authentication Agent 7.2 for Microsoft Windows software.

Please have the following information available when you call:

- Your RSA Customer/License ID. RSA Authentication Agent 7.2 is free to customers. Use the RSA Authentication Manager software version number as your Customer/License ID. To find this number, do one of the following:

For Authentication Manager 7.1, click **Help > About RSA Security Console > See Software Version Information** from the RSA Security Console.

For RSA Authentication Manager 6.x, click **Help > About**.

- The make and model of the machine where the problem occurs.
- The name and version of the operating system where the problem occurs.

1

Product Overview

- [RSA Authentication Agent for Microsoft Windows](#)
- [Key Features](#)
- [Supported Authenticators](#)
- [RSA Control Center](#)

RSA Authentication Agent for Microsoft Windows

RSA® Authentication Agent for Microsoft Windows works with RSA Authentication Manager to allow users to perform two-factor authentication when accessing Windows computers. Two-factor authentication requires something you know (for example, an RSA SecurID® PIN) and something you have (for example, a tokencode generated by an RSA SecurID authenticator).

If you require a user to log on through Authentication Agent, the user may need to enter a passcode to access the computer. A passcode is an RSA SecurID PIN followed by a tokencode.

The first time users authenticate using a SecurID passcode, they are prompted to automatically generate or manually create their SecurID PINs. To enter the tokencode portion of the passcode, they can look at the numbers that appear on the front of their SecurID authenticators and manually enter them next to their PINs (if using a handheld authenticator). Or, if they use USB SecurID authenticators and they insert them into their USB ports, Authentication Agent automatically accesses the tokencodes from the authenticators after they enter their PINs.

To ensure they use a One-Time Passcode (OTP) for each authentication, the tokencode changes to a unique set of numbers approximately every minute. This helps prevent an unauthorized user from guessing a passcode—even if that person knows the PIN.

Note: Depending on the Authentication Manager settings, SecurID users can also log on by entering just their tokencodes.

When a user enters a passcode, Authentication Agent sends the passcode to Authentication Manager for validation. If the passcode is correct, the user gains access to the desktop. For information on requirements, see Chapter 2, “[Preparing for Installation.](#)” For installation information, see Chapter 3, “[Installing RSA Authentication Agent.](#)”

Key Features

The following sections summarize the key features of RSA Authentication Agent for Microsoft Windows. They include information about:

- Users to challenge for a passcode
- Offline authentication
- Integration of Windows password
- Exempt administrator account
- Automatic synchronization of passwords
- Central management of Authentication Agent policies using the Group Policy Object (GPO) templates
- Automatic update of IP addresses
- Access to protected computers using a PIN or password
- Multidomain group support
- Fast user switching

Challenge Users for RSA SecurID Passcodes

You can configure RSA Authentication Agent for Microsoft Windows to challenge all users or only specific groups of users for a SecurID passcode (PIN and tokencode). You select the user groups to challenge from a list that you already defined through the Microsoft Computer Management interface or in Active Directory. If necessary, create new groups before using Authentication Agent. For more information about creating challenge groups, see [“Create Groups of Users to Challenge with RSA SecurID”](#) on page 27.

You can also configure challenge settings for an individual computer from the RSA Control Center user interface. For more information, see the RSA Control Center Help topic Challenge Users. Note that if the computer is joined to a domain, settings configured by Group Policy override settings from the RSA Control Center.

RSA SecurID Authentication without an Authentication Manager Connection

You can configure RSA Authentication Agent for Microsoft Windows to extend SecurID authentication to users when the connection to RSA Authentication Manager is not available (for example, when users work away from the office, or when network conditions make the connection temporarily unavailable). For more information, see Chapter 4, [“Managing Authentication Agents.”](#)

Integration of Windows Passwords in the RSA SecurID Logon Process

You can configure RSA Authentication Agent for Microsoft Windows so that the Windows password is integrated into the SecurID logon process. When you configure Authentication Agent in this way, users provide their Windows passwords only during their initial online authentication. At this time, the passwords are stored with users' authentication data in the RSA Authentication Manager database and, for offline authentication, in the offline data. During subsequent authentications, users enter only their user names and SecurID passcodes until the password is changed in the Active Directory. Authentication Agent gets the Windows password from Authentication Manager and passes it to the RSA Authentication Agent Credential Provider. The RSA Authentication Agent functions as a logon interface for end users.

Important: If users have more than one domain and user name, your Authentication Manager administrator must add the different accounts in Authentication Manager. If the additional accounts do not exist in Authentication Manager, users cannot log on using SecurID authentication. For more information, see the *Group Policy Object Template Guide*.

You can enable Windows password integration system-wide, on an individual Agent basis, or by groups. For example, to enable Authentication Agent, you create an Agent record in the RSA Authentication Manager database. You can enable Windows password integration for all of the Authentication Agent computers in the database or select certain computers. For more information about RSA Authentication Manager, see the *RSA Authentication Manager Administrator's Guide* (6.1 or 7.1).

Note: The Windows password integration feature also requires that the offline authentication feature be enabled on both the Agent and the server. If you are using Windows password integration, do not disable offline authentication.

Automatic Password Synchronization

When Microsoft Windows passwords are changed by users who have Authentication Agent installed on their computers, passwords are automatically synchronized in corresponding accounts in the RSA Authentication Manager database. For more information, see "[Automatic Password Synchronization](#)" on page 70.

Access to Protected Desktops in Emergency Situations

The exempt administrator account is an emergency access method that enables you to authenticate to a protected desktop by using your administrator account with only a Windows password instead of an RSA SecurID passcode.

When you install RSA Authentication Agent for Microsoft Windows, the installation wizard prompts you to select a challenge option. If you select **Challenge all users except administrators**, Authentication Agent challenges all users who log on to the computer for SecurID credentials (PIN and tokencode), but it does not challenge any users who belong to the administrator group.

If you decide not to exempt the users in the administrator group during installation or when you first use the configuration wizard to create an installation package, you can set that option later. For example, you can reconfigure your settings using the Authentication Agent configuration wizard to create another installation package and deploy it. Or, you could make changes by changing the policy in the Group Policy Object template. For more information, see the *Group Policy Object Template Guide*. For a list of other emergency access methods, see “[Choose Emergency Access Methods](#)” on page 28.

Central Management of Authentication Settings

To manage RSA Authentication Agent for Microsoft Windows, you can use Group Policy Object templates to make changes to the Authentication Agent policies and apply those policies to the appropriate computers. You load the templates into the Microsoft Group Policy Management Console (GPMC) tool on your domain controller and specify policies within the templates. The policies are automatically downloaded by client computers within the domain.

Note: For computers you intend to protect with Authentication Agent that are not part of your domain or subject to Group Policy, you must install the templates on those computers and specify the template settings with the Local Group Policy Editor. See the *Group Policy Object Template Guide* for more information.

Before users start using Authentication Agent, you can define particular settings to tailor the product to your needs. RSA Authentication Agent comes with the following Group Policy Object (GPO) templates:

- **RSA_Authentication_Agent.adm**
- **RSA_Authentication_Agent_Password_Synchronization.adm**
- **RSA_SecurID_Expiration_Warning.adm**
- **RSACredProviderFilter_Microsoft.adm**
- **RSACredProviderFilter_SecurID.adm**
- **RSACredProviderFilter_SmartCard.adm**
- **RSACredProviderFilter_ThirdParty.adm**
- **RSADesktop_VerifyRSAComponents.adm**

If you want to restrict logon options for Authentication Agent users on Windows Vista or later Windows operating systems, you must install and configure one or more of the Credential Provider Filter policy templates. A Credential Provider filter allows you to hide the logon tile presented by a Credential Provider.

You can use the following filters:

GPO Template Filename	Description
RSACredProviderFilter_Microsoft	Filters the Microsoft Credential Provider.
RSACredProviderFilter_SmartCard	Filters the RSA Smart Card Credential Provider.
RSACredProviderFilter_ThirdParty	Filters all third-party Credential Providers.
RSACredProviderFilter_SecurID	Filters the RSA SecurID Credential Provider.

For more information about third-party options, see [“Supported Third-Party Credential Providers”](#) on page 23. For more information about how to use the templates, see the *Group Policy Object Template Guide*.

Automatic Update of IP Addresses

The IP address of an Authentication Agent client computer allows Authentication Manager to identify the computer during authentication. If you install the Auto-Registration utility when you install Authentication Agent, the utility automatically adds the agent to the Authentication Manager database the first time you log on to the computer using RSA SecurID authentication.

Authentication Agent also launches the Auto-Registration utility:

- If the IP address of Authentication Agent client computer changes
- When you use the RSA Control Center to clear the node secret on the Authentication Agent client computer

For more information, see Chapter 4, [“Managing Authentication Agents.”](#)

Access to Protected Computers Using a PIN or Password

You can configure RSA Authentication Agent to allow users to unlock their protected computers using only their RSA SecurID PINs or Windows passwords. Users can use only their PINs or passwords after they successfully authenticate with a passcode within the time configured for this feature.

As an administrator, you can select the option you want to use (PIN or password), enable and disable this feature, set a time-out period for the feature, and set the number of times users can enter incorrect PINs or passwords before they are prompted for passcodes. You configure this option using the Group Policy Object templates after installation. For more information, see the *Group Policy Object Template Guide*.

Note: For users to unlock the computer with just a SecurID PIN, the Authentication Manager administrator must have enabled the offline authentication feature for them and you must have left offline authentication running as a service on the Agent. If you disable the offline authentication service through the Local Authentication Settings template, users cannot use offline authentication or unlock their computers with just a SecurID PIN. For more information on settings, see the *RSA Authentication Agent 7.2 Group Policy Object Template Guide*.

Multidomain Group Support

When you select a Windows group as an RSA Authentication Agent challenge group using the GPO templates, all users in the group are challenged by RSA SecurID. Authentication Agent supports the group setup available in Microsoft Active Directory. However, Authentication Agent cannot determine group membership if a user is in a different forest than the one you selected. For more information about setting up challenge groups, see the *Group Policy Object Template Guide*.

There are many different combinations of Windows groups: universal, global, and domain local. Windows also allows groups to be nested within other groups. It is important to understand the possible combinations of groups so that when you challenge or exclude a group from an RSA SecurID challenge, you get the results that you expect.

For more information, see the example in [“Multidomain Group Support”](#) on page 68.

Fast User Switching

RSA Authentication Agent allows multiple users with different privileges to log on to the same computer protected by RSA SecurID. For example, if you use a computer with Authentication Agent in a hospital setting and that computer gets shared by several doctors, nurses, and administrators, those users would need to switch the current user out (not off) to log on with their accounts to access the desktop for their needs. When done, the previous user can log on by unlocking their account. This restores the desktop to what they last had open on their session.

With fast user switching, it is not necessary for the first user to log off for the second user to log on.

Note: Fast user switching is also not available during Remote Desktop Protocol (RDP) sessions.

Options to Customize RSA Authentication Agent

Once you install Authentication Agent, users can see the RSA Authentication Agent Credential Provider. You can customize the RSA Authentication Agent in the following ways:

Specify whether logon prompts request passwords or passcodes. If you require users to log on with an RSA SecurID passcode (PIN and tokencode), you may want the logon prompt to display “Passcode” instead of “Password.”

Note: This setting was available in the user interface on previous versions of RSA Authentication Agent. It is now configured exclusively with the Group Policy Object Templates. For more information on setting this policy see the “Local Authentication Settings Template” in the *Group Policy Object Templates Guide*.

Set the unlock option to allow access with an RSA SecurID PIN or a Windows password. If a user needs to log on with a passcode (PIN and tokencode), you can configure Authentication Agent to allow the user to unlock the computer by entering the SecurID PIN without the tokencode or their Windows password. You can also set a time when Authentication Agent no longer allows access without the full passcode. For example, if the user locks the computer and wants to unlock it within an hour, the user can enter a SecurID PIN or Windows password. Once that hour passes, the user must enter the full passcode (PIN and tokencode) to unlock the computer.

Note: This ability to log on with just a SecurID PIN was available in the user interface on previous versions of RSA Authentication Agent. It is now configured exclusively with the Group Policy Object Templates and includes the ability to unlock the desktop with a Windows password. For more information, see the “Local Authentication Settings Template” in the *Group Policy Object Templates Guide*.

Notify users of the number of days left before an RSA authenticator expires. Users can check the number of days left before their authenticator expires by looking at the RSA Control Center icon in the notification area of the Windows taskbar. For more information, see the “Warning Message for Expiring Authenticators Template” in the *Group Policy Object Templates Guide*.

Hide or show different RSA Credential Providers for Windows Vista, Windows 7, Windows 8, Windows Server 2008 (SP2 or R2), or Windows Server 2012. The RSA Authentication Agent Credential Provider functions as a logon interface for end users. For example, Windows Vista or later Windows operating systems come with the Microsoft Credential Provider. A user sees this as a tile with an image and a user name under the tile. The user can click the tile to open the logon prompt and log on to the computer with a Windows password.

After you install Authentication Agent, users can see the RSA Authentication Agent Credential Provider. This Credential Provider appears as an RSA SecurID tile with an image and the appropriate user name under it.

If you want to switch the logon option available to users, you can filter the credential providers by selecting different policy settings through the Group Policy Object Template. For example, you can select an option to hide the Microsoft Password Credential Provider or the Microsoft Picture Password Credential Provider, only show the RSA Authentication Agent Credential Provider, or show all the available Credential Providers.

Note: This setting was available in the user interface on previous versions of RSA Authentication Agent. It is now configured exclusively with the Group Policy Object Templates. For more information about policy templates, see the section “RSA Credential Provider Templates” in the *Group Policy Object Templates Guide*.

Install the language pack to see the product in a language other than English.

When you install the standard Authentication Agent application, the following components automatically appear in English:

- Authentication Agent logon prompts
- User interface (RSA Control Center)
- Help
- Documentation

If you use a Japanese operating system and you install the Japanese language pack for Authentication Agent, you see these components in Japanese. (If you install the Japanese language pack on a computer that uses an English operating system, you continue to see the product in English.) If you want to use the product in a language other than English or Japanese, contact your RSA representative. For more information, see [“Install a Language Pack”](#) on page 46.

Supported Authenticators

RSA Authentication Agent for Microsoft Windows supports the following types of authenticators:

- RSA SecurID key fobs
- RSA SecurID standard cards
- RSA SecurID PINPads
- RSA SecurID software tokens
- RSA SecurID 800 Authenticator
- RSA on-demand tokencode

Note: You cannot use software authenticators that reside on the computer to log on to protected Windows desktops. However, once you log on to the desktop using a different type of authenticator, you can use software authenticators to log on to the network. You can use Authentication Agent with a software authenticator installed on a portable device, for example, a Blackberry. For more information on software authenticators, see the RSA documentation that comes with your software authenticator.

The RSA SecurID 800 Authenticator (SecurID 800) can function as a SecurID authenticator and smart card. To use it as a SecurID token, you can read the tokencode off the front and manually enter it when prompted. Or, if you installed the Connected Authentication feature with Authentication Agent, you can connect it to the USB port for the Agent to automatically access the tokencode for you.

The SecurID 800 looks like this:



For smart card use, the SecurID 800 has a smart card with an embedded smart chip and reader built into it. (The smart chip is a microprocessor that can store and process data.) To use the SecurID 800 as a smart card, you need to install RSA Authentication Client 3.5.4 and connect the authenticator to the USB port. For more information on RSA Authentication Client, see the documentation that came with the product.

Note: If you have RSA Authentication Agent installed and you install RSA Authentication Client, the user interface (also called the RSA Control Center) to manage the SecurID or smart card portion of your authenticator changes. You see more or fewer options, depending on what you have installed. For more information, see [“RSA Control Center”](#) on page 18.

RSA Control Center

When you install RSA Authentication Agent, you also install a user interface called the RSA Control Center. The RSA Control Center allows users and administrators to use options to manage some aspects of their SecurID settings. The Control Center contains options that allow users to check the supply of offline days and refresh offline days when needed.

Some configuration settings that were available in the RSA Authentication Agent 6.1, 6.4, and 7.0 user interfaces are now available exclusively in the Group Policy Object templates. Settings include whether to unlock computers with a SecurID PIN or Windows password instead of a passcode, filter credential providers, and specify whether the local logon prompt displays passcode or password. For more information, see the *Group Policy Object Templates Guide*.

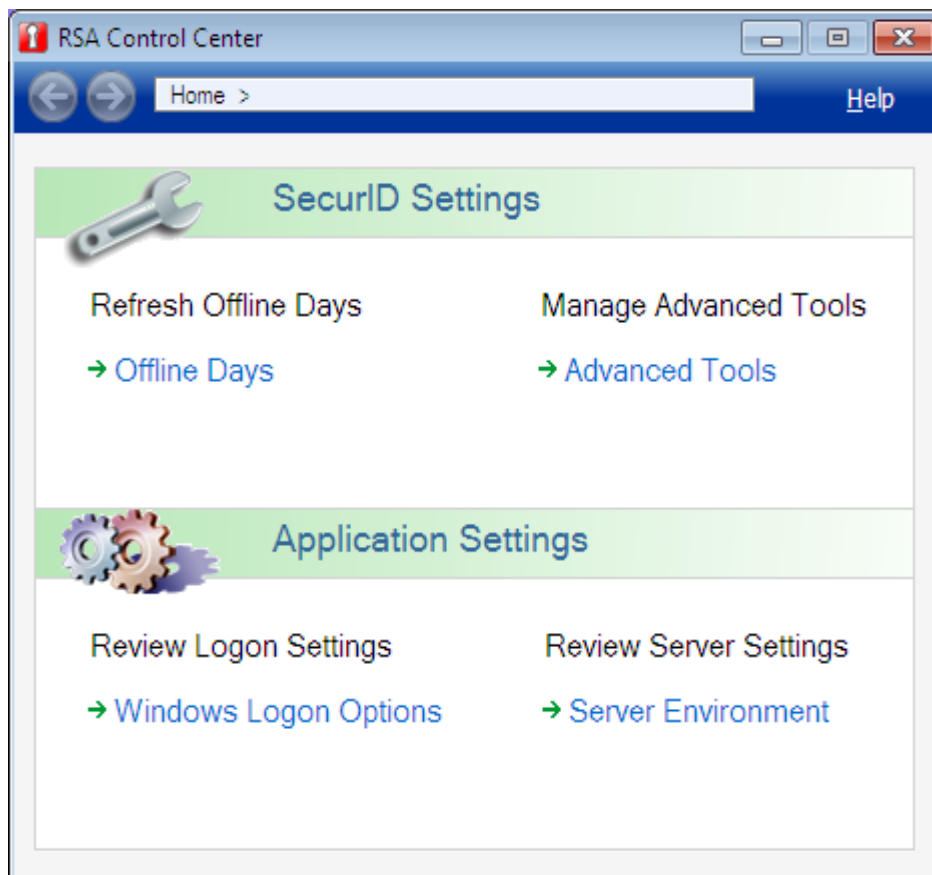
As an administrator, you can perform the following tasks from the RSA Control Center:

- Test authentication.
- View the RSA Authentication Manager server environment.
- Enable, test, or clear the reserve password. A reserve password allows users to log on to a computer if offline authentication is not running or the computer cannot connect to RSA Authentication Manager. You can also set the reserve password using the GPO templates. For more information, see the *Group Policy Object Template Guide*.
- Enable an IP address override to prevent any communication failures if Authentication Agent runs on a host that has multiple network interface cards and therefore multiple IP addresses.
- Clear the node secret if it is corrupt or does not match the node secret in the Authentication Manager database.
- Enable tracing to generate log files for troubleshooting.
- Specify which users to challenge, and set how users are challenged when their group membership cannot be determined on that specific computer. You can also specify challenge settings with Group Policy. Note that Group Policy settings override settings configured in the RSA Control Center. For more information, see the *Group Policy Object Template Guide*.
- Clear offline data if you disable offline authentication or you change the number of offline days that RSA Authentication Manager generates and downloads or if you want to reassign a protected computer to a different user.

To open the RSA Control Center, do one of the following:

- Click **Start > Programs** (or **All Programs**) > **RSA > RSA Control Center**.
- Double-click the Control Center icon in the notification area.

The following figure shows the Home page of the RSA Control Center.







Note: If you install RSA Authentication Client to use your SecurID 800 authenticator as a smart card, the RSA Control Center that is installed with Authentication Agent expands to show options to manage your smart card PIN. You continue to see the Authentication Agent SecurID options as well. If you remove RSA Authentication Client (or Authentication Agent), the options related to that product clear from the Control Center. For more information, see the RSA Authentication Client (Smart Card) Help or the RSA Authentication Agent (SecurID) Help that is installed with the Control Center.

For a description of the notification area and the RSA Control Center icons, see [“RSA Control Center Icons.”](#)

RSA Control Center Icons

When you install RSA Authentication Agent, the RSA Control Center icon appears in the notification area of the Windows taskbar. You can use this icon to open the RSA Control Center and view this icon for additional information about RSA Authentication Agent.

The following table describes the RSA Control Center icon.

Icons	Description
	<p>Opens the RSA Control Center. You can double-click the icon or right-click the icon and select an option to open the Control Center. To remove the icon from the system tray, right-click the icon and select the option to close it. Without the icon, you need to use the program group (for example, Start > All Programs > RSA > RSA Control Center) to open the Control Center.</p>
	<p>Warns that the number of offline days has dropped below a specified number by displaying a yellow exclamation point in the lower-right corner. Also displays the number of days left before an authenticator in the USB port expires.</p> <p>Use the Offline Days option from the Home page of the Control Center to check or refresh your days. For more information on offline days, see Chapter 4, “Managing Authentication Agents” or the RSA Authentication Agent (SecurID) Help. For more information on setting the expiration of an authenticator, see the Group Policy Object Guide.</p>
	<p>Indicates that the application recognizes an authenticator connected to the USB port by displaying a blue cross in the upper-right corner of the icon.</p> <hr/> <p>Note: Users can insert multiple authenticators into different USB ports and select the one they want to use. For more information, see the RSA Control Center (SecurID) Help.</p> <hr/>
	<p>Indicates that Authentication Agent is in the process of accessing data on the authenticator.</p> <hr/> <p>Note: A user should not remove an authenticator until Authentication Agent finishes processing data.</p> <hr/>

2

Preparing for Installation

- [System Requirements](#)
- [Remote Access Support](#)
- [Preparations to Install Authentication Agent](#)

System Requirements

RSA Authentication Agent for Microsoft Windows has the following system requirements:

- 1 GHz (x86) processor
- 1 GB of RAM
- 35 MB of free disk space
- TCP/IP networking
- Microsoft .NET Framework 4 Client Profile or later

Required Ports

The following table lists the ports that must be available for use by Authentication Agent.

Port	Description
5500/udp	RSA Authentication Manager uses this port to listen. Authentication Agent connects to this port during authentication.
5580/tcp	Authentication Agent clients connect to this port to perform offline data downloads.
5550/tcp	Used by Authentication Agent Auto-Registration utility. You can install the Auto-Registration utility when you install Authentication Agent or create an MSI package. This utility automatically records the Agent host IP address in the Authentication Manager database the first time users start their computers with the Agent installed on them.
389/tcp	Used by Authentication Agent to verify whether the user is a member of a challenge group in Microsoft Active Directory.

Supported Operating Systems

RSA Authentication Agent for Microsoft Windows is supported on the following operating systems:

- Windows Vista SP2, 32-bit and 64-bit, Business and Enterprise editions
- Windows 7 SP1, 32-bit and 64-bit, Enterprise and Professional editions
- Windows 8, 32-bit and 64-bit, Enterprise and Professional editions
- Windows Server 2008 SP2, 32-bit and 64-bit, Standard, Enterprise, Data Center, and Web Server editions
- Microsoft Windows Server 2008 R2 SP1, 64-bit, Standard, Enterprise, Data Center, and Web Server editions
- Windows Server 2012 SP2, Standard or Data Center editions (Server Core or Server with Graphical User Interface [GUI] mode)

For instructions on how to upgrade to RSA Authentication Agent for Microsoft Windows after you upgrade client computers to a different operating system, see [“Upgrade to RSA Authentication Agent 7.2”](#) on page 51.

Supported Third-Party Remote Access Products

The following table lists details on third-party remote access products supported by Authentication Agent.

Type of Product	Product Name
Remote access	<ul style="list-style-type: none"> • Desktop Connection <ul style="list-style-type: none"> – Version 6.1 (or later) for Windows Vista SP1, Windows 7, Windows 8, Windows Server 2008 SP1, or Windows Server 2012 • Citrix Independent Computing Architecture (ICA) Client/Receiver to connect to Citrix XenApp 6.5—Program Neighborhood, Citrix Program Neighborhood Agent, or Citrix Web Client: <ul style="list-style-type: none"> – Version 10.2 for Windows Vista SP1 users only

Supported RSA Authentication Manager Products

RSA Authentication Agent for Microsoft Windows functions as a client product that works with the authentication servers:

- RSA Authentication Manager 7.1 with SP3 hotfix 6 or later
- RSA Authentication Manager 6.1 with Patch 2

You must install SP3 hotfix 6 (or later) if you use RSA Authentication Manager 7.1 or Patch 2 if you use RSA Authentication Manager 6.1. For installation instructions, go to RSA SecurCare Online at <https://knowledge.rsasecurity.com>.

Before you enable RSA SecurID authentication, you must understand the RSA Authentication Manager system and its features. For more information, see the *RSA Authentication Manager Administrator's Guide* (6.1 or 7.1) or contact your Authentication Manager administrator.

Supported Third-Party Credential Providers

Users with Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 operating systems use a Credential Provider (logon tile).

Refer to one of the following sections depending on the operating system you use.

Using a Third-Party Credential Provider

If you install RSA Authentication Agent on Windows Vista, Windows 7, or Windows Server 2008 operating systems and leave the **RSACredProviderFilter_ThirdParty.adm** Group Policy Object template with the default setting, users cannot access the logon tile for the third-party credential provider. You must enable the third-party policy setting to allow users to access the third-party credential provider. For more information on templates, the *Group Policy Object Template Guide*.

Remote Access Support

If users need to use their local computers to log on to remote computers, they can use the appropriate application and logon accounts to connect to the remote computers. Once users connect to the remote computers, they can access applications, files, and network resources as if they were sitting in front of that computer.

RSA Authentication Agent supports these applications to connect to a remote computer:

- Microsoft Remote Desktop Connection
- Citrix ICA Client/Receiver (Citrix Program Neighborhood, Citrix Program Neighborhood Agent, or Citrix Web Client)

Users can open one of these applications from their local computers to log on to supported remote computers that have Authentication Agent installed on them. The supported operating systems of the remote computers are: Windows Vista, Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 running Terminal Services.

Microsoft Remote Desktop Connection allows a user to gain full access to a remote computer through a Local Area Network (LAN) or an Internet connection. If the local Windows computer has Microsoft Remote Desktop Connection, users can connect to remote computers using the RSA protected logon (if their Remote Desktop account and permissions allow it). The computers must have Authentication Agent installed on them.

Citrix Independent Computer Architecture (ICA) Client (Program Neighborhood, Program Neighborhood Agent, or Web Client) allows a user to connect to a remote Citrix XenApp computer to access published applications and desktops. Citrix users can also access remote computers that have Authentication Agent installed, and they can log on using RSA authenticators.

Remote Desktop Connection 6.1 or later includes Windows Network Level Authentication (NLA). If this feature is enabled when a user attempts to connect to a remote computer, the user is prompted to authenticate before establishing a connection. If the computer uses NLA with an RSA Authentication Agent Credential Provider configured on the remote computer, the user sees two prompts to authenticate before the user can access the remote desktop.

One prompt opens from the local computer and the other opens from the remote computer. This is not caused by the RSA Authentication Agent application. It is how Microsoft implements Network Level Authentication when you use a third-party credential provider. Once the user enters the account information and successfully authenticates through each prompt, the user can access the remote computer. Network Level Authentication is enabled by default for Windows Vista or later Windows operating systems.

For more information on using Network Level Authentication, see the [Microsoft](#) web site.

Preparations to Install Authentication Agent

This section describes tasks you must perform before installing and configuring RSA Authentication Agent for Microsoft Windows.

Task	Reference
Set up RSA Authentication Manager	“Set Up RSA Authentication Manager” on page 26
Create Groups of Users to Challenge with RSA SecurID	“Create Groups of Users to Challenge with RSA SecurID” on page 27
Choose Emergency Access Methods	“Choose Emergency Access Methods” on page 28
Prepare Users for RSA SecurID Authentication	“Prepare Users for RSA SecurID Authentication” on page 30

Set Up RSA Authentication Manager

Before you install and configure Authentication Agent, you or your RSA Authentication Manager administrator must complete these tasks:

- If you have not already done so, install either RSA Authentication Manager 7.1 with SP3 hotfix 6 (or later) or RSA Authentication Manager 6.1 with Patch 2 (or a later hotfix rollup). For instructions, see the *RSA Authentication Manager 7.1 Installation and Configuration Guide* or *RSA Authentication Manager 6.1 Installation Guide* (for Windows or UNIX).

- Make a copy of the system configuration (**sdconf.rec**) file from RSA Authentication Manager and give a copy to the administrator installing RSA Authentication Agent for Microsoft Windows (or tell the administrator how to locate it on the network). The Authentication Agent administrator must import this file when using the configuration wizard to create the installation package or while performing a local installation.

Users may experience problems logging on with a SecurID passcode after restarting the computer (or after resuming from Sleep or Hibernate mode) if you install the Auto-Registration utility with the agent and it attempts to contact an RSA Authentication Manager replica server instead of an Authentication Manager primary server.

In this environment, the Agent attempts to use offline authentication. If the user runs out of offline days, the SecurID authentication process fails. To ensure that SecurID authentication does not fail after a restart, you must use a copy of the **sdconf.rec** file from an Authentication Manager server that allows automatic registration and performs authentication. (The authentication service must be running on that server.)

If the Authentication Agent administrator plans to install the Auto-Registration utility to automatically register users' computers in the Authentication Manager database the first time users start their computers with Authentication Agent, make a copy of the **server.cer** file from RSA Authentication Manager in addition to the **sdconf.rec** file. Send it to the administrator installing RSA Authentication Agent for Microsoft Windows. The administrator can import it when creating an installation package or while performing a local installation.

For more information on the files you need to import, see Chapter 3, "[Installing RSA Authentication Agent](#)." For more information on the Auto-Registration utility, see Chapter 4, "[Managing Authentication Agents](#)."

- Verify that RSA Authentication Manager is installed and running on a server.

- Register the RSA Authentication Agent for Microsoft Windows host as an agent of RSA Authentication Manager. For more information, see the *RSA Authentication Manager Administrator's Guide* (6.1 or 7.1). You do not need to manually register user computers if you install the Auto-Registration utility when you install Authentication Agent. For more information, see Chapter 3, "[Installing RSA Authentication Agent](#)" and Chapter 4, "[Managing Authentication Agents](#)."

Note: If you install Authentication Agent on a multihomed server and not an agent with the Auto-Registration utility, provide an IP address override for Authentication Agent. (A multihomed server is a computer that has multiple IP addresses to connected networks. This helps a session survive if a network failure occurs.) For more information about setting an IP address override, see the RSA Authentication Agent (SecurID) Help.

Register SecurID users in the RSA Authentication Manager database and distribute SecurID authenticators to those users. For more information on manually registering users, see the *RSA Authentication Manager Administrator's Guide* (6.1 or 7.1).

Create Groups of Users to Challenge with RSA SecurID

You control access to resources protected by RSA Authentication Agent for Microsoft Windows by specifying which users to challenge for RSA SecurID passcodes. You can configure Authentication Agent to challenge:

- No users
- All users
- A group of users
- All users except a certain group of users

Authentication Agent uses Windows groups to control access to resources. These groups can be default Windows groups or groups that you create using the Windows Computer Management interface or Active Directory. If you want to use groups other than the Windows default groups, you need to create them before you configure Authentication Agent. For detailed instructions on creating groups, see your Microsoft Windows documentation.

You can apply challenge settings to individual computers with the RSA Control Center. For instructions and additional information, see the RSA Control Center Help topic Challenge Users. If you use the configuration wizard to configure an installation package as described in Chapter 3, "[Installing RSA Authentication Agent](#)," you can only select an option to challenge all users except those in the local administrator group. If you use the Group Policy Object templates, you can use the options listed in this section. For more information, see the *Group Policy Object Template Guide*.

Choose Emergency Access Methods

RSA Authentication Agent for Microsoft Windows includes options that allow users and administrators to access protected desktops when they lose their authenticators, forget their PINs, or run out of offline days. Before you install and configure Authentication Agent, decide on the emergency access methods you want to use. The following tables describe the emergency access methods and list where to find more information.

For Offline Users

Emergency Access Method	Description	Characteristics	Reference
Offline emergency tokencode	Users can access their protected computers without a tokencode (for example, when they have lost their authenticators)	<ul style="list-style-type: none"> • Must be combined with the user's RSA SecurID PIN • Changes the next time the user authenticates online • Expires after a specified amount of time 	See " Emergency Access " on page 60.
Offline emergency passcode	Users can access their protected computers without an RSA SecurID PIN or tokencode (for example, when they have forgotten their PINs, or when their PINs have been compromised)	<ul style="list-style-type: none"> • No RSA SecurID PIN required • Changes the next time the user authenticates online • Expires after a specified amount of time 	See " Emergency Access " on page 60.

For Online Users

Emergency Access Method	Description	Characteristics	Reference
One-time passwords	Users can access their protected computers without a tokencode (for example, when they have lost their authenticators)	<ul style="list-style-type: none"> • Must be combined with the user's RSA SecurID PIN • Generated by the RSA Authentication Manager • Valid for one authentication 	See the <i>RSA Authentication Manager Administrator's Guide</i> (6.1 or 7.1).

For Online Users

Emergency Access Method	Description	Characteristics	Reference
Fixed passwords	Users can access their protected computers without a tokencode (for example, when they have lost their authenticators)	<ul style="list-style-type: none"> • Must be combined with the user's RSA SecurID PIN • Created by an RSA Authentication Manager administrator • Valid until the user's lost authenticator status is changed 	See the <i>RSA Authentication Manager Administrator's Guide</i> (6.1 or 7.1).
On-demand tokencode	Users with digital mobile devices and home e-mail accounts can receive one-time tokencodes as text messages.	<ul style="list-style-type: none"> • Must be combined with the PIN for the user's authenticator. • User's mobile devices and e-mail accounts must be enabled to receive on-demand tokencodes. 	See the <i>RSA Authentication Manager 7.1 Administrator's Guide</i> .

For Administrators

Emergency Access Method	Description	Characteristics	Reference
Reserve password	The reserve password allows the administrator or user to bypass the passcode requirement. Administrators (or a user who obtained the reserve password from an administrator) can log on to the user's computer with the user's account (or any valid user name for the computer) and the reserve password.	<ul style="list-style-type: none"> • Set by an administrator on each agent after installation through the RSA Control Center or the Local Authentication Settings Group Policy Template • Never expires 	See the RSA Authentication Agent (SecurID) Help (in the RSA Control Center) or the <i>Group Policy Object Template Guide</i> .

For Administrators

Emergency Access Method	Description	Characteristics	Reference
Exempt administrator account	Administrators can authenticate to protected computers as themselves with only a password	<ul style="list-style-type: none"> • Set during Agent installation through the MSI file, configuration wizard, or the Local Authentication Settings Group Policy Template • Member of the administrator group on each agent • Protected by simple Windows password security 	See “ Access to Protected Desktops in Emergency Situations ” on page 11 or the <i>Group Policy Object Template Guide</i> .

Prepare Users for RSA SecurID Authentication

Before you deploy RSA Authentication Agent for Microsoft Windows, prepare your RSA SecurID users as follows:

- Register users who will be challenged for passcodes as RSA SecurID users in the RSA Authentication Manager database and activate their authenticators. For more information on registering users, see the *RSA Authentication Manager Administrator’s Guide* (6.1 or 7.1).

Important: The Windows user names for RSA SecurID users must be registered in the RSA Authentication Manager database. These user names cannot contain spaces and must not exceed forty-eight characters.

- Give assigned and enabled tokens to users who will be challenged for passcodes.
- Provide authentication instructions to users. For more information, see the documentation that comes with your authenticator.

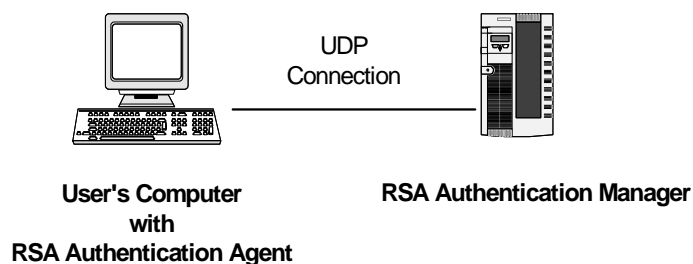
3

Installing RSA Authentication Agent

- [Installation Methods](#)
- [Installation Considerations](#)
- [Upgrade to RSA Authentication Agent 7.2](#)
- [Install the Product on a Single Computer](#)
- [Test the Installation](#)
- [Install a Language Pack](#)
- [Install a Language Pack](#)
- [Use the Node Secret Load Utility](#)
- [Modify an Installation](#)
- [Repair an Installation](#)
- [Uninstall the Product](#)

RSA Authentication Agent must communicate with RSA Authentication Manager for RSA SecurID authentication to occur. Before you install RSA Authentication Agent 7.2 for Microsoft Windows, make sure RSA Authentication Manager 7.1 SP3 hotfix 6 (or later) or Authentication Manager 6.1 with Patch 2 is installed on the appropriate server.

For information on installing Authentication Manager, see the *RSA Authentication Manager 7.1 Installation and Configuration Guide* or the *RSA Authentication Manager 6.1 Installation Guide* (for Windows or UNIX). The following figure shows the user datagram protocol (UDP) connection from the user's computer to the Authentication Manager server:



To upgrade from an earlier version of RSA Authentication Agent, see [“Upgrade to RSA Authentication Agent 7.2”](#) on page 51.

Note: After you install Authentication Agent, you can configure RSA Authentication Manager to extend the RSA SecurID logon process to users when their computers are not connected to Authentication Manager through the network. For more information, see [“Offline Authentication”](#) on page 55.

Installation Methods

Use one of the following methods to install Authentication Agent:

- To install Authentication Agent on a single computer, run the MSI file (**RSA Authentication Agent.msi**) on the local computer.
- For a large-scale deployment, use the configuration wizard (**ConfigWizard.exe**) to create a custom MSI installation package and deploy it to the appropriate users.

Important: If you installed Windows Server 2012 in Server Core mode (without a user interface or GUI), you need to install Authentication Agent from the command line. For example, you can run the configuration wizard (**ConfigWizard.exe**) to create an Authentication Agent installation package and install it by entering: `msiexec /qn /i "RSA Authentication Agent.msi"` at the command line. (Your installation package may use another msi name.) Once you install the product, you can access the Authentication Agent user interface (RSA Control Center) and use the options as needed. You can also switch between "Server Core" and "Server with GUI" mode after installing Authentication Agent and use it the same way. For more information on creating a custom installation package and using the command line, see ["Install the Product on Multiple Computers"](#) on page 38.

If you install Authentication Agent on the Windows Server where you plan to manage your RSA Group Policy Object templates, you do not need to manually install the templates. Authentication Agent automatically installs them in the Local Security Policy. For more information, see the *RSA Authentication Agent 7.2 Group Policy Object Template Guide*.

Single Installations

You may want to install the Authentication Agent on a single computer to run an authentication test before deploying an installation package to a larger group. Or, you may only need to install the product on one or two computers.

During the installation process, you choose a **Typical** or **Custom** installation. If you choose a **Typical** installation, you import the system configuration file (**sdconf.rec**). If you choose a **Custom** installation, you can select an option to install the Auto-Registration utility and the RSA SecurID Connected Authenticator feature.

The Auto-Registration utility automatically registers users' computers in the Authentication Manager database the first time users start their computers with Authentication Agent installed. If you select the Auto-Registration utility, you must import the server certificate file (**server.cer**). If you want users to authenticate with a SecurID 800 authenticator connected to the USB port, you must also select the RSA SecurID Connected Authenticator feature.

Large-Scale Deployments

To customize the Authentication Agent logon settings and install the product on many computers, use the **ConfigWizard.exe** file located in the Configuration Wizard folder that came in the zipped folder of the product. During the process, you import the system configuration file (**sdconf.rec**) and, if necessary, the server certificate file (**server.cer**). You obtain the **sdconf.rec** and the **server.cer** files from your RSA Authentication Manager administrator.

After you create an installation package using the configuration wizard, you can deploy it using Microsoft Systems Management Server (SMS), the command line, or a logon script.

Note: You can run the configuration wizard (**ConfigWizard.exe**) to create an Authentication Agent installation package on any of the supported Windows operating systems.

For more information on the Authentication Manager files, see the next section. For more information on installing Authentication Agent on a single computer, see [“Install the Product on a Single Computer”](#) on page 36. For more information on using the configuration wizard, see [“Install the Product on Multiple Computers”](#) on page 38.

Important: If you want to use Authentication Agent in a language other than English, install the language pack after you install the product. For more information on installing a language, see [“Install a Language Pack”](#) on page 46.

Import Authentication Manager Files

During the single installation process or when you use the configuration wizard to customize an installation package, you must import the system configuration file (**sdconf.rec**) for Authentication Agent to communicate with Authentication Manager. To install the Auto-Registration utility, you must also import the server certificate file (**server.cer**).

For RSA Authentication Manager 7.1, the Authentication Manager administrator can generate a **sdconf.rec** file and download a **server.cer** file to the Agent from the **Access** menu options of the RSA Security Console (**Authentication Agents > Generate Configuration File** for the **sdconf.rec** file and **Authentication Agents > Download Server Certificate File** for the **server.cer** file). The **sdconf.rec** file creates a snapshot of the server information available at the time the file was generated. For more information, see the *RSA Authentication Manager 7.1 Administrator's Guide* or your Authentication Manager administrator.

For RSA Authentication Manager 6.1 and later, the **sdconf.rec** and the **server.cer** files are located in the **ACEDATA** directory on the Authentication Manager host computer. You must request one or both of these files from your Authentication Manager administrator before you begin installing Authentication Agent.

For more information about installing these files, see [“Install the Product on a Single Computer”](#) on page 36 or [“Install the Product on Multiple Computers”](#) on page 38.

Installation Considerations

Before you install RSA Authentication Agent, review the following information:

- If you upgrade from RSA Authentication Agent 6.x or 7.0, you must map the old settings to the new policies in the RSA Authentication Agent Group Policy Object templates. For more information, see the *Group Policy Object Template Guide*.
- Authentication Agent is available as a .zip file that you must download from www.rsa.com.
- Installing RSA Authentication Agent on a computer with RSA EAP Client 6.1.3 removes RSA EAP Client 6.1.3 from the computer.
- You must use an administrator account or have administrator privileges to install the software. If you plan to deploy an installation package, you must also set the policies to control privileges to user desktops. For more information, see “[Provide Account Control Privileges to User Computers](#)” on page 41.
- If you install Authentication Agent on computers that are not joined to a domain, you must manually define the Group Policy settings on each computer. For more information, see the *Group Policy Object Template Guide*.
- If you plan to install Authentication Agent on a single computer, copy the system configuration file (**sdconf.rec**) and the server certificate file (**server.cer**) from RSA Authentication Manager to the computer where you plan to install Authentication Agent. (You only need the **server.cer** file if you plan to install the Auto-Registration utility.) Browse to these files when you run the **RSA Authentication Agent.msi**. For more information, see “[Import Authentication Manager Files](#)” on page 33.
- To use the configuration wizard (**ConfigWizard.exe**), get the system configuration file (**sdconf.rec**) and the server certificate file (**server.cer**) from the RSA Authentication Manager administrator so you can import them into your configuration package. (You only need the **server.cer** file if you plan to install the Auto-Registration utility.) Users do not need to browse to these two files when you deploy the installation package because they are in the installation package. For more information, see “[Import Authentication Manager Files](#)” on page 33.

Note: You must request one or both of these files from your Authentication Manager administrator before you install Authentication Agent.

- Users may experience problems logging on with a SecurID passcode after restarting the computer (or after resuming from Sleep or Hibernate mode) if you install the Auto-Registration utility with the Agent and it attempts to contact an RSA Authentication Manager replica server instead of an Authentication Manager primary server. In this environment, the Agent attempts to use offline authentication.

Important: If the user runs out of offline days, the SecurID authentication process fails. To ensure that SecurID authentication does not fail when the user attempts to log on after running out of offline days, you must use a copy of the **sdconf.rec** file from an Authentication Manager server that allows automatic registration and performs authentication. (The authentication service must be running on that server.) If you only use a primary server to perform database management, do not use the **sdconf.rec** file from that primary server. Instead, use a **sdconf.rec** file from a replica server. For more information on the Auto-Registration utility, see [“Automatic Registration Process”](#) on page 64.

- If you want to use a more secure way of establishing a node secret between Authentication Manager and the Agent computer, you can use the Node Secret Load utility that comes with Authentication Agent. This utility allows you copy the node secret from Authentication Manager and load it to the appropriate Authentication Agent computer before users start using SecurID authentication. That way, you do not have to wait until after the first authentication to establish the node secret. For more information, see [“Use the Node Secret Load Utility”](#) on page 47.

Install the Product on a Single Computer

To install RSA Authentication Agent on one or a few computers, follow the steps in this section. To install Authentication Agent on many computers, see “[Install the Product on Multiple Computers](#)” on page 38.

Note: If you installed Windows Server 2012 in Server Core mode, you do not use a user interface (GUI). You need to install Authentication Agent from the command line. For more information, see “[Install the Product on Multiple Computers](#)” on page 38.

Before you Begin

Review the following items before you install the product:

- Authentication Agent is available as a .zip file that you must download from www.emc.com/domains/rsa/index.htm.
- Authentication Agent requires the trusted root certificate *thawte Primary Root CA*. This certificate is automatically provisioned on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2, provided the machine has Internet access. On machines that do not have Internet access, you must use the appropriate Microsoft root update mechanism to install the certificate in the Trusted Root CA store of the machine account. For instructions, see [Microsoft Knowledge Base Article 931125](#).
- Contact your Authentication Manager administrator before you begin installing Authentication Agent to obtain the **sdconf.rec** file and the **server.cer** file (If you plan to install the Auto-Registration utility.). Copy both files onto the local computer or get the directory location of the files from the Authentication Manager administrator. For more information, see “[Import Authentication Manager Files](#)” on page 33.

To install Authentication Agent on a single computer:

1. Log on to the computer as an administrator (or install with administrator privileges).
2. Double-click **RSA Authentication Agent.msi** to start the installation wizard.
3. Click **Next** to advance through the Welcome dialog boxes.
4. Read the License Agreement or click **Print** to print it. When ready, select **I accept the terms in the license agreement** and click **Next**.
5. Do one of the following:
 - To install only RSA Authentication Agent without the Auto-Registration utility or the RSA SecurID Connected Authenticator, select **Typical**, and then click **Next**.
 - To install RSA Authentication Agent and additional features such as the Auto-Registration utility and the RSA SecurID Connected Authenticator features, select **Custom**. Click **Next** to open the Custom Setup dialog box:

- Select the drop-down arrow next to **Auto-Registration Utility**. Select the option you want from the drop-down list.
 - Select the drop-down arrow next to **Connected Authenticator**. Select the option you want from the drop-down list.
6. Leave the default directory for the installation folder or click **Change** to browse to another location. Click **Next**.
 7. Click **Browse** to browse to and open the system configuration file (**sdconf.rec**). Click **Next**. (You must obtain the file or the location of this file from your RSA Authentication Manager administrator.)
 8. Leave the default location for the offline data folder or click **Change** to browse to another location. Click **Next**.
 9. If you selected the Auto-Registration utility, click **Browse** to locate and open the server certificate file (**server.cer**), and then click **Next**. You must obtain the file or the location of this file from your RSA Authentication Manager administrator.
 10. If you want all users that are not administrators to log on to the desktop with SecurID Authentication, select **Challenge all users except administrators**. Local administrators can log on using their Windows method (password or smart card). Click **Next**.
 11. Click **Install**. Authentication Agent installs on the local computer. For Windows Vista or later operating systems, Windows prompts you to allow account control privileges if you set up account control privileges. Click **Allow**.
 12. Click **Finish**.

Next Steps

- To use a secure method of establishing a node secret between the Authentication Agent computer and the Authentication Manager server, use the Node Secret Load utility that comes with the RSA Authentication Agent 7.2 for Microsoft Windows kit. Use this utility before users begin authenticating with RSA SecurID passcodes. For more information, see [“Use the Node Secret Load Utility”](#) on page 47.
- To test the installation on a local computer, see [“Test the Installation”](#) on page 43.
- To view the product in another language instead of English, you can install a language pack after you install the standard product. For more information, see [“Install a Language Pack”](#) on page 46.
- For computers you intend to protect with Authentication Agent that are not part of your domain or subject to Group Policy, you must configure the template settings with the Local Group Policy Editor. See the Group Policy Object Template Guide for more information.

Install the Product on Multiple Computers

To install RSA Authentication Agent for Microsoft Windows on multiple computers at one time, do the following:

1. Review or customize the Authentication Agent options through the Authentication Agent configuration wizard to create an installation package (MSI file).
2. Provide the appropriate account control privileges to users' computers to allow the installation.
3. Deploy the installation package. For example, you can use Microsoft Systems Management Server (SMS) or another third-party product, such as Tivoli. Or, you can use the command line.
4. Deploy the language pack if users need to view the product in a language other than English, and they use the operating system in another language.

The following sections describe how to perform these tasks in the order shown.

Create an Installation Package

The configuration wizard, **ConfigWizard.exe**, allows you to quickly configure the Authentication Agent settings so you can deploy a custom installation package to multiple computers.

Before you Begin

- Decide if you need to create more than one installation package. For example, you can set up a package for users of 32- or 64-bit operating systems, and you can set up a package for users of 32- or 64-bit operating systems to use RSA SecurID 800 authenticators.
- Authentication Agent is available as a .zip file that you must download from www.rsa.com. Before installation, you must download the .zip file and extract either the **RSA Authentication Agent.zip** or **RSA Authentication Agent x64.zip** file depending on whether you are creating a 32-bit or 64-bit installation package.
- Authentication Agent requires the trusted root certificate *thawte Primary Root CA*. This certificate is automatically provisioned on Windows 8, Windows 7, Windows Vista, and Windows Server 2008 or later, provided the machine has Internet access. On machines that do not have Internet access, you must use the appropriate Microsoft root update mechanism to install the certificate in the Trusted Root CA store of the machine account. For instructions, see [Microsoft Knowledge Base Article 931125](#).
- Contact your Authentication Manager administrator before you begin installing Authentication Agent to obtain the **sdconf.rec** file and the **server.cer** file if you plan to install the Auto-Registration utility. Copy both files onto the local computer or get the directory location of the files from the Authentication Manager administrator. For more information about getting these files, see [“Import Authentication Manager Files”](#) on page 33.

To create a custom RSA Authentication Agent installation package using the configuration wizard:

1. To start the RSA Authentication Agent Installation Creation Wizard, open the Configuration Wizard folder and double-click **ConfigWizard.exe**.
2. Click **Browse** to locate the **RSA Authentication Agent.msi** or **RSA Authentication Agent x64.msi** file. Click **Next**.
3. Click **Browse** to import the system configuration (**sdconf.rec**) file that identifies the Authentication Manager server you want to use. You must obtain the system configuration file from your Authentication Manager administrator. Click **Next**.
4. Select **Enable Auto-Registration** to automatically register users' computers in the RSA Authentication Manager database the first time they start their computers with Authentication Agent installed.
5. If you enable automatic registration, leave the default location to the server certificate file (**server.cer**) or click **Browse** to locate it, and click **Next**. You must obtain the server certificate file from your Authentication Manager administrator.
6. If you want to allow users to log on with an RSA SecurID 800 authenticator connected to the USB port for the Agent to automatically access the tokencode, select **Enable RSA SecurID Connected Authenticator**. Otherwise, leave the default of not selected. Click **Next**.
7. If you want to challenge all users for an RSA SecurID passcode to log on to the computer except users who belong to the administrator group on the computer, select **Enable challenge with the exclusion of the administrator group**. Otherwise, leave the default of not selected. Click **Next**.

Important: Only select this option if all the appropriate users have their RSA SecurID authenticators and know how to log on with a passcode. If they do not, they can still log on to their computers if they do not belong to a challenge group or if they can access the Microsoft Password Provider Credential Provider option. For more information on setting logon options, see the *Group Policy Object Template Guide*.

8. Review your selections. For example, you can use the scroll bar to check the following:
 - Path of the system configuration file (**sdconf.rec**)
 - Auto-Registration utility state (enabled or disabled) and the path of the server certificate file (**server.cer**)
 - Connected authenticator state to use an RSA SecurID 800 authenticator in a USB port for the Agent to automatically access the tokencode (enabled or disabled)
 - Authentication challenge state (enabled or disabled)
9. To change any settings, click the back arrow (<-) and make any necessary changes. Click **Finish** when done.
10. Enter a name for the installation package file.
Make sure you give the file a unique name to help you distinguish it from other installation packages that you might create.
11. If necessary, browse to the location where you want to save the installation package file. Click **Save** when done.
12. Click **OK** to save the settings and close the wizard.

Next Steps

- To install a language pack to convert the Authentication Agent interface and documentation into a language other than English, see [“Install a Language Pack”](#) on page 46.
- To use a more secure method of establishing a node secret between the Authentication Agent computer and the Authentication Manager server, use the Node Secret Load utility that comes with the RSA Authentication Agent 7.2 for Microsoft Windows kit. Use this utility before users begin authenticating with RSA SecurID passcodes. For more information, see [“Use the Node Secret Load Utility”](#) on page 47.
- To modify settings of the installation after you deploy it, you can repeat the steps in this section to create another package and deploy it. New settings override the previous settings. (For more information, see [“Modify an Installation”](#) on page 48.) Or, you can define settings using the Group Policy Object templates, depending on the number of computers that need modifications. You can also set some settings on a local computer through the Control Center. See the RSA Authentication Agent (SecurID) Help for details.

The following settings that were in the previous versions of the Configuration Wizard are now policies configured by the GPO Templates. For more information about the following settings, see the *Group Policy Object Template Guide*:

- Set the Logon Prompt to use a Passcode or a Password
- Set the RSA SecurID PIN to allow users to unlock computers with a PIN instead of a full passcode
- Set the Credential Provider and third-party filtering

Provide Account Control Privileges to User Computers

Administrators can install Authentication Agent to all computers in a domain. Users who are members of the Administrators group can install Authentication Agent on their own computers. If you want Authentication Agent installed on the computers of users, you must set the appropriate policies to ensure that it can install on all the appropriate computers. For example, Authentication Agent requires access to Windows registry keys. Users do not have privileges to view or change the registry, so you must deploy the software as a managed application.

A managed application uses elevated privileges to install the application and make the required changes to registry keys. This ensures that users can install the software on their computers.

To provide privileges to user computers:

Use the following tools to control privileges:

- Microsoft Management Console (MMC) 3.0
- Use Group Policy to control MMC usage
For more information on using Group Policy, see [Using Group Policy to Control MMC 3.0 Usage](#) on the Microsoft web site.

Note: Having elevated privileges on the computer allows the installation of RSA Authentication Agent for Microsoft Windows, and it does allow a user with elevated privileges to remove it. Standard users can use the **Repair** option to repair the installation, if necessary.

Deploy the Installation Package to Multiple Computers

Once you create an installation package as described in “[Create an Installation Package](#)” on page 38 and set the account privileges to the necessary groups, you can deploy Authentication Agent. If you want to test the installation on a local computer after you deploy it, see “[Test the Installation](#)” on page 43.

Important: If you previously deployed RSA Authentication Agent and you later deploy another RSA Authentication Agent installation package, any changes you made through the configuration wizard override the previous settings. Before you deploy an MSI file, make sure all the settings include the options you want.

To deploy the installation package on multiple computers:

Use one of the following methods:

- Microsoft Systems Management Server (SMS) or another third-party product, such as Tivoli
- Command line installation
- Silent installation from the msixec command line

Note: Ensure that RSA Authentication Manager is installed before deploying Authentication Agent. For information on installing Authentication Manager, see the *RSA Authentication Manager 7.1 Installation and Configuration Guide* or the *RSA Authentication Manager 6.1 Installation Guide* (for Windows or UNIX).

Choose SMS deployment only if you are familiar with SMS operations, such as adding distribution points and programs and creating advertisements. For more information on SMS, go to the [Microsoft Systems Management Server web site](#).

Silent Installation

To perform a silent installation from the msixec command line, use the /qn option. When the installation is complete, the installer restarts the computer whenever necessary without displaying any prompt or warning to the user.

Note: You can only perform a silent installation on MSI files you created with the configuration wizard.

To install from the msiexec command line:

1. Right-click the command prompt icon from the **Start** menu and click **Run as administrator** to open the command prompt.
2. Navigate to the directory that contains the **RSA Authentication Agent.msi** package file (or a renamed Authentication Agent MSI file). Otherwise, you must provide the full pathname to the package file on the command line.
3. Type a command similar to the following, depending on the name of your MSI package:

```
msiexec /qn /i "RSA Authentication Agent.msi"
```

To log any errors, add the **/lv** (log verbose) option at the end of the command. The product completes the installation and the system restarts automatically.

Test the Installation

Before you deploy the product in your organization, you should test it on a local computer. Perform the tasks in the following table to test the installation.

Task	Reference
View the status of the server environment.	“Review the Server Settings” on page 43
Test authentication.	“Test Authentication” on page 44

If successful, you can deploy the product to multiple users as described in [“Deploy the Installation Package to Multiple Computers”](#) on page 42.

Review the Server Settings

Review the server settings by displaying information about RSA Authentication Manager in the RSA Control Center to verify whether the server environment is set up correctly. For more information on the server settings, see the RSA Authentication Agent (SecurID) Help.

To review the server settings:

1. Log on to a computer with Authentication Agent with an administrator account or run as an administrator.
2. Click **Start > Programs** (or **All Programs**) > **RSA > RSA Control Center** to open the RSA Control Center.
3. Under **Application Settings**, click **Server Environment**.
4. Review the RSA Authentication Manager limits, static information, and dynamic information.
5. (Optional) Click the **Server name** drop-down to view information about other servers.

Test Authentication

It is important to test authentication because, in addition to verifying the server environment, it creates a node secret for Authentication Agent and stores it in the RSA Authentication Manager database.

Important: If you want to use a more secure method of establishing a node secret between the Authentication Agent computer and the Authentication Manager server, use the Node Secret Load utility that comes with the RSA Authentication Agent 7.2 for Microsoft Windows kit. By creating the node secret before users authenticate, you use encrypted authentication immediately instead of after the first use. For more information, see [“Use the Node Secret Load Utility”](#) on page 47.

Node Secret

The node secret is a symmetric encryption key that RSA Authentication Manager and RSA Authentication Agent use to encrypt and decrypt packets of data as they travel across the network. The first time a user successfully authenticates or tests authentication from an Agent host, RSA Authentication Manager creates a node secret for that Agent host and stores it in the RSA Authentication Manager database. A copy of the node secret is encrypted and sent to the Authentication Agent. The node secret is stored on the agent.

If the node secret on the Authentication Agent host is corrupted or does not match the node secret in the RSA Authentication Manager database, encrypted communications between the Authentication Agent and Authentication Manager cannot work. If this happens, Authentication Manager logs a node verification failure message in the RSA Authentication Manager Activity monitor. For more information on testing authentication or clearing the node secret, see the RSA Authentication Help. For more information on how Authentication Manager manages logs node verification failures, see the *RSA Authentication Manager Administrator’s Guide* (6.1 or 7.1).

To test authentication with a SecurID authenticator:

1. Log on to a computer with Authentication Agent using an administrator account (or run as an administrator).
2. Click **Start > Programs (or All Programs) > RSA > RSA Control Center** to open the RSA Control Center.
3. Under **SecurID Settings**, click **Advanced Tools**.
4. Click **Test Authentication**.
5. In the **Choose authenticator** field, do one of the following:
 - If you have a handheld authenticator (an authenticator not inserted into a USB port), leave the default of **Handheld token** in the field.
 - If you have an RSA SecurID 800 authenticator inserted into the USB port, leave the default serial number or name of the authenticator in the field.
 - If you have multiple RSA SecurID 800 authenticators inserted into USB ports, leave the current authenticator serial number or name in the field or select another one from the drop-down list.

6. In the **User name** field, leave the current user name or change it to another one.
 7. In the **Passcode** or **SecurID PIN** field, do one of the following:
 - If you use a handheld authenticator without a set SecurID PIN, enter the tokencode shown on the front of the authenticator. Click **OK**. The Set New RSA SecurID PIN dialog box opens. Continue to step 8.
 - If you use an RSA SecurID 800 authenticator without a set SecurID PIN, leave the field empty. Click **OK**. The Set New RSA SecurID PIN dialog box opens. Continue to step 8.
 - If you use a handheld authenticator that has a set SecurID PIN, enter the passcode (PIN followed by the tokencode shown on the front of the authenticator). Click **OK**. Skip to step 10, if necessary.
 - If you use an RSA SecurID 800 authenticator that has a set SecurID PIN, enter the PIN. Click **OK**. (Authentication Agent automatically accesses the tokencode from the authenticator for you.) Skip to step 10, if necessary.
 8. If you need to generate or create a SecurID PIN, do one of the following:
 - To receive a system-generated PIN, select **Generate my SecurID PIN for me**. Click **OK**. The system prompts you to memorize your PIN. Click **Yes** to memorize it within 10 seconds. Do not write it down. Click **OK**.
 - To create your PIN, select **Create my own SecurID PIN**. In the **SecurID PIN** field, enter a PIN. Enter it again in the **Confirm SecurID PIN** field. Click **OK**.
-
- Note:** The options available depend on your Authentication Manager settings. You may have only one option available.
-
9. If you just received a system-generated PIN or created a PIN, do one of the following:
 - If you use a handheld authenticator, wait until your token changes, then enter your PIN and tokencode in the **Passcode** field. Click **OK**.
 - If you use a USB token, you see a message to wait while Authentication Agent accesses the next tokencode. You do not need to enter a PIN.
 10. If you see a prompt to enter the next tokencode to confirm your possession of the token and synchronize it with Authentication Manager, do one of the following:
 - If you use a handheld authenticator, wait for your tokencode to change. Enter the tokencode in the **Next tokencode** field and click **OK**.
 - If you use a USB authenticator, you see a message to wait while Authentication Agent accesses the next tokencode. You do not need to enter a PIN.

Once you successfully authenticate, you see a success message. If you cannot authenticate, you may need to check your Authentication Manager settings. See the *RSA Authentication Manager Administrator's Guide* (6.1 or 7.1).

Install a Language Pack

If you installed RSA Authentication Agent for Microsoft Windows and you do not want to view it in English, you can install a language pack file to view it in another language. To request another language, contact your local RSA sales representative.

Important: The desktop must use an operating system in a language other than English or the product remains in English. If you attempt to install the MSI language pack before you install Authentication Agent, you see a message that the system cannot install the language. You must install RSA Authentication Agent before you install the language pack.

To install a language pack on a single computer:

1. Log on with elevated privileges (an administrator account) and double-click the appropriate MSI file.
2. Double-click the **RSA Authentication Agent <name of language> Language.msi** file.
3. Restart your computer when prompted to complete the installation.

To install a language pack on multiple computers:

1. Verify that all the appropriate computers have RSA Authentication Agent for Microsoft Windows installed.
2. Deploy the **RSA Authentication Agent <name of language> Language.msi** file using your preferred method. If you use the command line, enter the filename of the language pack. To log any errors, use the **/v** (log verbose) option. For example, type the following to silently install a language pack:

```
msiexec /qn /i "RSA Authentication Agent <name of language>
Language.msi"
```

The system automatically restarts users' computers to complete the installation.

If you want to see Authentication Agent in English again, remove the language pack. If you remove Authentication Agent and leave the language, users can no longer access their computer through Authentication Agent. For details on removing a language pack, see ["Uninstall the Language Pack"](#) on page 53.

Use the Node Secret Load Utility

Each Authentication Agent computer has a unique node secret associated with it. The node secret allows the RSA Authentication Agent computer and RSA Authentication Manager server to use encrypted communication during the SecurID authentication process. To ensure a secure transaction the first time a user attempts to authenticate with a SecurID passcode, Authentication Agent and Authentication Manager automatically communicate using a hashed value of the unique node secret and store it on the Agent computer. From then on, each authentication interaction uses the node secret to encrypt the communication between the two systems.

If you want to use a more secure method of establishing a node secret between the Authentication Agent computer and the Authentication Manager server, use the Node Secret Load utility (**agent_nsload.exe**) that comes with the RSA Authentication Agent kit. You can use this utility to copy the node secret from Authentication Manager and load it on to the Authentication Agent computer before users start authenticating with SecurID passcodes.

To use the Node Secret Load utility:

1. Locate the node secret file for the Agent host on the appropriate RSA Authentication Manager server.

Note: The Authentication Manager administrator creates a unique node secret on Authentication Manager. For more information, see the RSA Authentication Manager Help.

2. Copy the node secret file and the **agent_nsload.exe** utility to the <<Program Files>>\RSA Shared\Auth API directory on the Agent computer.
3. Open a command prompt and move to the <<Program Files>>\Common Files>>\RSA Shared\Auth API directory. Enter:

```
agent_nsload -f <path> -d “..\AuthData”
```

where <path> is the directory location and name of the node secret file. You will be prompted to enter the password with which your node secret file was encrypted. The Node Secret Load utility loads the new node secret file into the Agent computer.

4. Repeat this procedure for each computer that needs the extra encryption protection during the first SecurID authentication.

Modify an Installation

If you need to modify the settings of RSA Authentication Agent for Microsoft Windows, the method you use depends on the number of computers that need modification. For one computer, you can make modifications using the `msiexec` command line or from the Control Panel. For multiple computers, you must use the command line. See the next two sections according to your needs.

Note: You must have administrator privileges to modify the installation package, and you must open the command prompt as an administrator to run the `msiexec` commands.

Modify the Installation for a Single Computer

To modify the installation for a single computer, you can:

- Reconfigure the MSI package
- Use the Control Panel to access the **Change** option

You can run the `msiexec` commands on a single computer and multiple computers.

To modify the installation for a single computer with the MSI package:

1. Double-click the **ConfigWizard.exe** file and browse to the **RSA Authentication Agent.msi** package you used for the original installation.
2. Make the changes you need, and save the package with the same name you originally used.
3. Open a command prompt with administrator privileges.
4. Use a case-sensitive command similar to the following example to reinstall the program.

```
msiexec /qn /i "RSA Authentication Agent.msi" REINSTALL=ALL  
REINSTALLMODE=vomus
```

Note: For more information on command-line installation modifications, including removing or adding a feature, see [“Modify the Installation for Multiple Computers”](#) on page 49.

To modify the installation for a single computer through the Control Panel:

1. For Windows Vista, Windows 7, or Windows 8, click **Start > Control Panel**. Click **Programs**. Then click the **Programs and Features** icon. Click **RSA Authentication Agent**. Click **Change** to open the wizard. Click **Next** to open the Program Maintenance dialog box. Leave **Modify** selected, or select it, if needed. Click **Next**.
2. Click the **Agent Host Auto-Registration Utility** drop-down box. Select **Install this feature on the local hard drive**, **Install this feature and all subfeatures on the local hard drive**, or **Do not install this feature**.

3. Click the **Connected Authenticator** drop-down box, and select **Install this feature on the local hard drive, Install this feature and all subfeatures on the local hard drive, or Do not install this feature.**
4. Click **Next**.
5. Clear or select the **Challenge all users except administrators** option. If you select this option, users will need to log on using SecurID authentication. Local administrators will not need to log on using SecurID authentication. Click **Next**.
6. Click **Install**.
7. Click **Finish** to restart the computer when prompted.

Modify the Installation for Multiple Computers

The following procedures describe how to modify configuration settings and features of Authentication Agent installations from a command prompt. You can also use these procedures on a single computer.

Modify an existing installation

Modify configuration settings with the Configuration Wizard, and redeploy the package with this command:

```
msiexec /qn /i "RSA Authentication Agent.msi" REINSTALLMODE=vomus  
REINSTALL=ALL
```

For more information on the Configuration Wizard, see [“Create an Installation Package”](#) on page 38.

Add a feature to an existing installation

To add a feature to an existing installation, you must use the Configuration Wizard to create another MSI package and run an msiexec command as an administrator to deploy the package. For example, if you did not enable the Auto-Registration utility the first time you deployed Authentication Agent, you can enable it by creating another MSI package. For more information on the Configuration Wizard, see [“Create an Installation Package”](#) on page 38. After you create the new MSI package with Auto-Registration enabled and the **server.cer** file imported, deploy the package with this command:

```
msiexec /qn /i "RSA Authentication Agent.msi" ADDLOCAL=ALL  
REINSTALLMODE=vomus REINSTALL=LAC
```

Remove a feature from an existing installation

You can remove a feature from an installation without creating another MSI package. However, you must use a different msiexec command to remove the feature. Use the commands below to remove Auto Registration, Connected Authenticator, or both. You must open a command prompt as an administrator to run these commands.

To remove Auto Registration:

```
msiexec /qn /i "RSA Authentication Agent.msi" REINSTALLMODE=vomus  
REMOVE=AutoReg_x86 or 64
```

To remove Connected Authenticator:

```
msiexec /qn /i "RSA Authentication Agent.msi" REINSTALLMODE=vomus
```

REMOVE=SID_C_x86 or 64

To remove Auto Registration and Connected Authenticator:

```
msiexec /qn /i "RSA Authentication Agent.msi" REINSTALLMODE=vomus  
REMOVE=AutoReg_x86 or 64,SID_C_x86 or 64
```

Repair an Installation

Repairing an installation replaces missing files in a damaged installation.

Note: To repair an installation, you must log on as an administrator to the computer that has Authentication Agent installed, but you do not need to elevate your Microsoft Windows user privileges.

To repair an installation on a single computer:

- For Windows Vista, Windows 7, or Windows 8, click **Start > Control Panel**. Click **Programs**. Then click the **Programs and Features** icon. Click **RSA Authentication Agent**. A **Repair** button appears on the menu bar. Click **Repair**.

Note: If you double-click the MSI file to repair the installation, select **Repair** and click **Next**. Then click **Install** to repair the installation. Click **Finish** when done.

Upgrade to RSA Authentication Agent 7.2

To upgrade from a previous version of RSA Authentication Agent to RSA Authentication Agent 7.2, perform the following tasks:

1. If you have Authentication Agent 7.0 or earlier installed, make a note of the settings in your current version of Authentication Agent. Authentication Agent now uses Group Policy Object (GPO) templates to configure policy settings for Authentication Agent. You will need to map your old settings to the new GPO policy settings after you install RSA Authentication Agent. (Authentication Agent 7.1.x or later retains your policy settings when you upgrade to a later version.)
2. If you have RSA Authentication Agent 5.x or earlier installed, remove it as described in the documentation that came with it.
3. Install RSA Authentication Agent as described in [“Install the Product on a Single Computer”](#) on page 36 or [“Install the Product on Multiple Computers”](#) on page 38.
4. Map the settings you noted from your previous version of RSA Authentication Agent to the new GPO templates. For more information, see the *Group Policy Object Template Guide*.

Uninstall the Product

If you need to remove RSA Authentication Agent, the method you use depends on the number of computers you need to remove it from. If you only need to remove Authentication Agent from one computer, you can use the method for a single computer. If you need to remove it from many computers, you use the method described for multiple computers.

Important: You may need to disable a local security setting to successfully remove the Authentication Agent from some computers. For example, you can install Authentication Agent if the local security policy has the **User Account Control: Only elevate executables that are signed and validated** setting enabled, but Windows may not allow you to remove the application.

To remove the application if Windows does not allow you to remove it:

1. Click **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Open the **Local Security Policy** folder.
3. Then open the **Security Options** folder. Scroll down to the **User Account Control: Only elevate executables that are signed and validated** setting.
4. If enabled, right-click the setting and click **Properties**.
5. From the **Local Security Settings** tab, select **Disabled**, and then click **OK**. You can now remove the application from the computer.

Uninstall the Product from a Single Computer

This section describes how to uninstall Authentication Agent from one computer. If you need to remove the product from many computers, see [“Uninstall the Product from Multiple Computers”](#) on page 52.

To uninstall the product from a single computer:

1. Click **Start > Control Panel > Programs and Features**.
2. Click **RSA Authentication Agent for Microsoft Windows**. An **Uninstall** button appears on the menu toolbar.
3. Click **Uninstall**.
4. Do one of the following (if prompted):
 - If logged on as an administrator, click **Allow** to elevate your privileges.
 - If logged on as a user, enter an administrator user name and password to elevate your privileges and allow the uninstall process to continue.
5. Restart the computer if prompted. If you cancel the uninstall process at any time, the application reverts back to its previous state.

Note: If you installed a language pack and want to remove it, see [“Uninstall the Language Pack”](#) on page 53.

Uninstall the Product from Multiple Computers

To remove Authentication Agent from multiple users' computers, use an `msiexec` command. To log any removal errors, use the `/lv` (log verbose) option. Put the log file, for example `uninstall.log`, in a known location such as `%USERPROFILE%`.

You can enter a command similar to the following with the `/x` (`REMOVE=ALL`) option (and the `/qn` option for silent mode) and the fully qualified pathname to remove Authentication Agent from multiple users' computers without user interaction:

```
msiexec /qn /x "RSA Authentication Agent.msi" /lv uninstall.log
```

Note: The `/lv` (log verbose) option in the command logs any errors. Execute the command to multiple computers using Microsoft Systems Management Server (SMS) or another third-party product. If you installed a language pack and want to remove it, see [“Uninstall the Language Pack”](#) on page 53.

Uninstall the Language Pack

If you installed a language pack to view Authentication Agent in another language, you can remove it to view the product in English.

Note: You can remove Authentication Agent or the language pack in any order. However, if you remove the Agent and leave the language pack installed, users can no longer log on through Authentication Agent. If you remove the language pack and leave Authentication Agent, users see Authentication Agent in English.

To remove the language pack from a single computer:

1. Click **Start > Control Panel > Programs and Features**.
2. Click **RSA Authentication Agent for Windows - <name of language> Language**. An **Uninstall** button appears on the menu toolbar.
3. Click **Uninstall**.
4. Do one of the following (if prompted):
 - If logged on as an administrator, click **Allow** to elevate your privileges.
 - If logged on as a user, enter an administrator user name and password to elevate your privileges and allow the uninstall process to continue.
5. Restart the computer if prompted.

To silently remove the language pack from multiple computers, enter the following command:

```
msiexec /qn /x "RSA Authentication Agent <name of language> Language.msi"
```

Note: Deploy the command to multiple computers using Microsoft Systems Management Server (SMS) or another third-party product.

4

Managing Authentication Agents

- [Offline Authentication](#)
- [Manage Offline Days](#)
- [Emergency Access](#)
- [Set Up Offline Authentication](#)
- [Automatic Registration Process](#)
- [Prevent Automated Registration During Specified Events](#)
- [Automated Registration and the Node Secret](#)
- [Automated Registration and Offline Authentication](#)
- [Maintain the Primary IP Address of the Authentication Agent Host](#)
- [Multidomain Group Support](#)
- [Automatic Password Synchronization](#)

Offline Authentication

Offline authentication extends RSA SecurID authentication to users when the connection to RSA Authentication Manager is not available, for example, when users work away from the office. You can enable and disable offline authentication and set the number of offline days users receive for individual Authentication Agents, groups of users, or system-wide through the RSA Authentication Manager. For more information, see the *RSA Authentication Manager Administrator's Guide* (6.1 or 7.1).

If offline authentication is enabled, Authentication Manager generates offline data (also called offline days) and downloads it to the Authentication Agent host when Authentication Agent connects to the host. Authentication Agent hosts begin receiving offline data during their second connected authentication to Authentication Manager. For example, if you perform the authentication test as described in "[Test Authentication](#)" on page 44, and then authenticate, Authentication Manager generates and downloads the offline data. This allows the Agent user to authenticate offline.

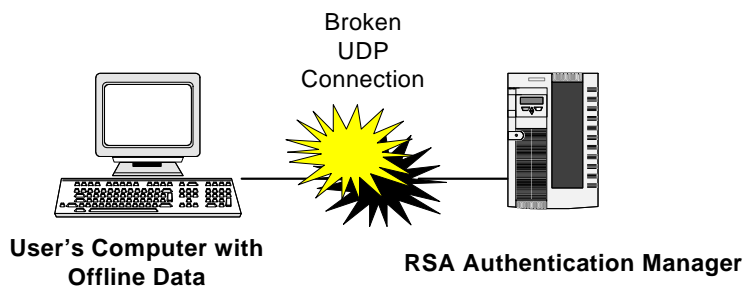
By default, offline data is stored in the following location:

- **C:\ProgramData\RSA\RSA Authentication Agent\Local\dayfiles** for Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.

You can specify the location during installation. If you specify a location, offline data is stored in *specified_path\RSA\RSA Authentication Agent\Local\dayfiles*.

When a user authenticates offline, Authentication Agent verifies the user's authentication information against the offline data stored on the user's computer. If the user's authentication information is correct, the user gains access to the protected computer.

The following graphic shows a scenario where a user's computer, not connected to the RSA Authentication Manager, can use offline data to access a protected computer.



Password Changes and Offline Authentication

Users who change their passwords while offline can still authenticate even though the new password does not match the one in their offline day files. In this scenario, the system prompts users for their new passwords after they enter their SecurID passcodes. Authentication Manager cannot capture or store the new password in the offline day files while the user works offline. Once the user works online, Authentication Manager can automatically synchronize the passwords and update the users' offline day files.

Clock Changes and Offline Authentication

Offline authentication monitors clock changes and maintains a system clock offset between the PC clock and the offline data. Users who change their PC clocks while offline instead of adjusting time zones cannot authenticate. For example, if you usually work in the United States and you take a trip to Japan, you cannot change your clock on your computer to the time in Japan and authenticate offline. Your offline day files continue to use the time set for the time zone. If the times do not match the correct time zone, you cannot authenticate. Change the time zone on your computer instead of the clock. You can then use your offline day files to authenticate when offline. You must use administrator privileges to change the time zone on a computer.

Manage Offline Days

This section describes how to refresh offline days under various circumstances and check the supply of offline days.

Before anyone can use offline days, the RSA Authentication Manager administrator sets the following in Authentication Manager:

- Authentication Agents allowed to use offline authentication
- Number of offline days issued
- Number that triggers the low supply warning.

For more information on the Authentication Manager settings, see the *RSA Authentication Manager Administrator's Guide* (6.1 or 7.1).

Refresh Offline Days

Offline days are automatically refreshed when the user performs any of the following:

- Authenticates directly to the network.
- Establishes a connection online after authentication offline.

Even if the user's supply of offline days is full, offline days are automatically updated when:

- The user changes the Windows password while authenticated online.
- An administrator issues a new policy to the Authentication Agent on the user's computer allowing emergency codes while the user is online. For information about emergency codes, see "[Emergency Access](#)" on page 60.

Offline days are not automatically refreshed if the authentication session has expired (the user remains online for 24 hours or more). In this situation, the user has to refresh offline days manually. Additionally, unlocking a computer with only an RSA SecurID PIN does not initiate an automatic refresh.

You can also configure how many days of offline data a user is allowed to download. This is the number of days' worth of token codes that are downloaded to the user's machine. This is configured in the RSA Security Console on the RSA Authentication Manager server as part of an offline authentication policy.

The following sections describe refresh scenarios.

Refresh When a Network Connection Exists

Authentication Agent recognizes that a network connection exists and attempts to download offline days.



Refresh When No Network Connection Exists

When the user logs on without a connection to the network, Authentication Agent attempts to automatically download offline days, but recognizes that no network connection exists. It displays an alert on the RSA Control Center icon to notify the user that the offline day supply is low. The user can click on the message in the notification area to open the RSA Control Center and refresh the days manually.

Note: If the RSA Control Center icon does not appear in the notification area of the Windows taskbar (for Windows 7), click the arrow to Show hidden icons, click Customize, find **RSA Control Center Notification Icon** in the Notification Area Icons dialog box, and then select **Show icon and notifications** from the drop-down list.

To refresh the offline days without a network connection, the user can:

1. Click the RSA Control Center icon. The RSA Control Center opens the Offline Days dialog box.
2. Connect to the network, and then click **Refresh** to manually refresh offline days. Authentication Agent does one of the following:

Description	Icon
If the connection to the network is successful, the system automatically downloads offline days and the RSA Control Center icon returns to normal.	
If the connection to the network fails, the system informs the user that a problem occurred and prompts the user to try again later. The RSA Control Center icon remains in the alert state and continues to display the “low on offline days” notification message each time the user logs on.	



3. Click **OK**.

Refresh When the Authentication Session Expired

If Authentication Agent attempts to automatically download offline days, but recognizes that the authentication session has expired, Authentication Agent sets the RSA Security Center icon to alert state to indicate that the supply of offline days is low. (For example, this can occur when the user has been logged on to the network for more than 24 hours.)



To refresh the offline days after an authentication session expired, the user can:

1. Click the notification message from the RSA Control Center icon. The RSA Control Center opens the Offline Days dialog box.
2. Click **Refresh**. Authentication Agent prompts the user for a passcode.
3. Enter the passcode. Authentication Agent does one of the following:

Description	Notification Icon
Downloads offline days and sets the RSA Control Center icon to normal.	
Informs the user that a problem occurred and to try again later. The RSA Control Center icon remains in the alert state.	

Check the Supply of Offline Days

Users can check their supply of offline days by looking at the icon in the notification area. The state of the icon tells the general status of the supply. The following table describes the icons that indicate the supply of offline days.

Notification Icons	Description
	Indicates the supply of offline days has not dropped below a specified number.
	An caution icon appears on the keyhole to warn that the number of offline days has dropped below a specified number. For more information, see the RSA Authentication Agent (SecurID) Help.

Clear Offline Data

Clearing offline data removes it from the agent. Without offline data, the user cannot access the protected resource without connecting through the network.

You need to clear offline data under the following circumstances:

- You changed the offline settings on the RSA Authentication Manager (for example, you disabled offline authentication for an Agent, or you changed the number of offline days the Authentication Manager generates and downloads).
- You change the authenticator properties for a user (for example, clear the user's PIN or synchronize the user's authenticator).
- You want to reassign a protected computer to a different user.
- You disable the user's authenticator.
- You set a token's status to lost in RSA Authentication Manager.

After you remove offline data from an agent, the next time that computer successfully authenticates to the RSA Authentication Manager, the Authentication Manager generates new offline data and downloads it to the agent. For instructions on clearing offline data, see the RSA Authentication Agent (SecurID) Help.

Emergency Access

Offline users can substitute offline emergency codes for passcodes by calling their SecurID Authentication Manager Help Desk administrator. The Help Desk administrator provides users with the offline emergency codes they need to use. For example, if offline users:

Forget their PINs or run out of offline days, they can authenticate with an offline emergency passcode. Users enter the offline emergency passcode instead of an RSA SecurID passcode.

Lose their tokens or cannot log on or unlock the computer because of too many failed authentication attempts, they can authenticate with an offline emergency tokencode. Users combine the offline emergency tokencode with their RSA SecurID PINs to authenticate.

The first time a user attempts to authenticate with a token after performing an offline authentication with an offline emergency tokencode, Authentication Manager places the user's authenticator into "lost authenticator temporary password" mode (if allowed).

The temporary password is the same as the offline emergency tokencode. It may have an expiration date set by the Help Desk administrator. Before the password expires, the user must contact the Authentication Manager Help Desk administrator to replace the lost authenticator with a new one or return the lost authenticator to a "not lost" status. For more information on how Authentication Manager manages emergency codes, see the *RSA Authentication Manager Administrator's Guide* (6.1 or 7.1).

Emergency Access Options

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

Reserve Passwords

The reserve password feature is an emergency access method that enables you, the administrator, to authenticate to a user's protected computer as that user without entering an RSA SecurID passcode under the following circumstances:

- The offline authentication service is not running on the local computer
- The computer cannot connect to RSA Authentication Manager
- No offline day files are available to allow offline authentication

To set up a reserve password, you use one of the following Authentication Agent options:

- Local Authentication Settings Group Policy Object (GPO) template
- RSA Control Center

If you select **All Users** as the challenge option, and the network connection fails, no one, including an administrator, can access the desktop on the protected computer. For this reason, RSA strongly recommends setting a reserve password or using another emergency access method for administrators. (For information on other emergency access methods, see [“Choose Emergency Access Methods”](#) on page 28.)

Only the Authentication Agent administrator knows the reserve password. If a user needs to log on to the computer that requires a reserve password, the user needs to contact the appropriate administrator for assistance.

Important: The reserve password is less secure than other emergency access methods. For example, it does not require a SecurID PIN and it remains valid unless an administrator changes it. With a one-time password, a user must include the SecurID PIN and the user can only use it once.

If the reserve password feature is enabled, and the Windows system is unable to communicate with the RSA Authentication Manager at the time of authentication, instead of displaying a message that the Authentication Manager is unreachable, the system prompts you to enter a reserve password. Users also need to enter a Windows password.

For information on setting the reserve password option through the Local Authentication Settings GPO template, see the *Group Policy Object Guide*. For information on setting the reserve password through the RSA Control Center, see the RSA Authentication Agent (SecurID) Help.

Set Up Offline Authentication

To accommodate different work environments, you can set up different ways to deploy offline authentication to users who work remotely.

Users Who Work Locally and Remotely

If you want to set up offline authentication for users who work both in the office and remotely, you can deploy offline authentication to these users by requiring them to perform an initial online authentication at the office before taking their computers offline.

To set up offline authentication before remote users leave the office:

1. Connect the user's computer to the network.
2. Add the user's computer to the domain (optional).
3. Instruct the user to perform a connected authentication to the RSA Authentication Manager. (If necessary, you can perform the authentication test described in "[Test Authentication](#)" on page 44.)
4. If the user's authenticator is in New PIN mode, instruct the user to authenticate a second time, using the new RSA SecurID PIN. If the authentication is successful, the RSA Authentication Manager downloads offline data to the user's computer.

5. Verify that offline data has been downloaded to the user's computer. To do this, use Windows Explorer to verify that the offline data is stored in the user's computer. For information about where offline data is stored, see "[Offline Authentication](#)" on page 55. The directories where offline data is stored are hidden directories. To see the offline data files, you must configure Windows Explorer to view hidden files.

Different Remote Users Who Share a Computer

If you want to set up offline authentication for several different users who share the same computer for working remotely, you can instruct users to download their offline data remotely instead of requiring each user to perform a connected authentication and download offline authentication data in the office.

To configure a shared computer for offline authentication:

1. Create a challenge group that includes the names of everyone who will share the computer. If you need to create new Windows groups, see the appropriate Microsoft documentation.
2. Set a reserve password for the computer.
For more information, see the RSA Control Center (SecurID) Help.
3. Specify the challenge for the group you created using the GPO template. For more information, see the *Group Policy Object Template Guide*.
4. Instruct the remote user to contact the administrator for the reserve password and then to log on to the computer. When a user attempts to access the computer while it is offline, the user is prompted first for the reserve password, and then for the Windows password.
5. Instruct the user to connect to the network remotely.
6. Instruct the user to lock the computer, and then unlock it by providing an RSA SecurID passcode when prompted. This downloads offline data to the user's computer. From this point forward, the user must provide RSA SecurID passcodes to authenticate locally.
7. Repeat steps 5 and 6 for each user account sharing the computer.

Users Who Only Work Remotely

You may want to deploy Authentication Agent and offline authentication to remote users who cannot come into the office to install Authentication Agent and perform an initial online authentication. Because users are added to the offline authentication challenge list only after downloading their initial set of offline days, remote users can access their desktops using their Windows passwords, and then open a remote connection to download offline days. Once a user downloads an initial set of offline days, that user is challenged for RSA SecurID passcodes on all subsequent authentications to the desktop.

To deploy offline authentication to remote users who cannot visit the office:

1. Instruct the user to install RSA Authentication Agent 7.2 using the MSI file. For information, see [“Install the Product on a Single Computer”](#) on page 36.
2. Instruct the user to log on to the desktop using a Windows password, and then connect remotely to the network.
3. Instruct the user to lock the computer, and then unlock it by providing an RSA SecurID passcode when prompted. This downloads offline data to the user’s computer.

Important: Remote users can refresh their offline data remotely, but must do so before the last offline day expires. Otherwise, they must perform a connected authentication to download more offline days. Users can continue to refresh their supplies of offline days this way until their RSA SecurID authenticators expire.

Automatic Registration Process

Every computer that hosts RSA Authentication Agent must have a corresponding Agent host record in the RSA Authentication Manager database. If the Agent Host Auto-Registration Utility (**sdadmreg.exe**) is installed on a new Authentication Agent host computer, the utility registers the computer in the Authentication Manager database and eliminates the need for an administrator to manually create the Agent host record.

The IP address of an Authentication Agent client computer enables the Authentication Manager to identify the computer during authentication. If the Auto-Registration utility is installed on an Authentication Agent client computer, the utility automatically records the Agent host IP address to the Authentication Manager database the first time you start the computer.

Additionally, Authentication Agent launches the utility under the following circumstances:

- If the IP address of the Authentication Agent client computer changes
- During RSA SecurID authentication to the local desktop
- When you use the RSA Control Center to clear the node secret on the Authentication Agent client computer

When the utility is launched, it determines whether the IP address of the Authentication Agent client computer has changed. If the IP address has changed, the utility updates it in the Authentication Manager database. If the IP address has not changed, the utility shuts down.

The Auto-Registration utility is useful for systems that use the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses, and environments that use wireless and Virtual Private Network (VPN) connections to access the corporate network. The utility also permits a registered Authentication Agent to update its own information with changes from the Authentication Manager **sdconf.rec** configuration file.

The Auto-Registration utility also assists in managing the node secret. For more information, see [“Automated Registration and the Node Secret”](#) on page 66.

To use the utility, you install it during the installation process as described in Chapter 3, [“Installing RSA Authentication Agent.”](#)

In addition, an RSA Authentication Manager administrator must configure Authentication Manager to allow automatic registration. For more information, see the RSA Authentication Manager Help.

Note: When you use the Auto-Registration utility to register a new Authentication Agent in the Authentication Manager database, the new Authentication Agent is registered with the offline authentication and password integration system settings specified in the Authentication Manager database.

You can configure the Auto-Registration utility to exempt events that, by default, trigger the utility to run. For more information, see [“Prevent Automated Registration During Specified Events”](#) on page 65.

Prevent Automated Registration During Specified Events

To reduce network traffic and maximize performance, you can configure the Auto-Registration utility to exempt events that, by default, trigger the utility to run. For example, you can specify that changes to the IP addresses of devices such as VMWare hosts or wireless routers do not trigger the utility to run. To specify exemptions, create the ExcludeAdaptor string in the Windows registry. Changes to the IP address of devices named in the ExcludeAdaptor string value list do not cause the Auto-Registration utility to run.

To configure the Auto-Registration utility to exempt an event:

1. On the Authentication Agent client computer, log on with an Administrator account.
2. Open the Registry Editor. For example, click **Start**. Then enter **regedit** in the **Start Search** prompt and click **regedit** from the **Programs** list.
3. In the Registry Editor, click **HKLM\ SOFTWARE\RSA\RSA Authentication Agent\AgentAutoRegistration**.
4. In the right pane of the Registry Editor window, right-click, and then click **New > String Value**.
5. For the new value name, enter **ExcludeAdapters**.
6. In the right pane of the Registry Editor window, right-click **ExcludeAdapters**, and click **Modify**.
7. For the value name, enter information to identify each of the devices you want the Auto-Registration utility to exclude from monitoring. Use semicolons to separate the identifiers for each device. For example, if you enter **VPN;VMWARE**, the **ExcludeAdapter** value exempts all devices whose names include **VPN** and all devices whose names include **VMWARE**.

Important: The **ExcludeAdapter** value is case sensitive.

Automated Registration and the Node Secret

The node secret is required for communication between Authentication Agent and Authentication Manager. For successful communication, the node secret generated by Authentication Manager must be installed on the Authentication Agent client computer. The node secret is transferred from Authentication Manager to Authentication Agent during initial authentication. Authentication problems may occur if the node secret on the Authentication Agent client computer does not match the one in the Authentication Manager database.

When the Auto-Registration utility connects to Authentication Manager, Authentication Manager detects when the node secret on the Authentication Agent client no longer matches the one stored in the Agent host record in the Authentication Manager database. Authentication Manager clears the node secret in the Agent host record and causes Authentication Agent to clear the node secret on the Authentication Agent client computer. Authentication Manager generates a new node secret and downloads it to the Authentication Agent client computer during the next authentication. For information on troubleshooting node secret issues, see [“Node Verification Fails”](#) on page 72. For details on using the Node Secret utility, see [“Use the Node Secret Load Utility”](#) on page 47.

Automated Registration and Offline Authentication

Offline authentication extends RSA SecurID authentication to users when the connection to RSA Authentication Manager is not available (for example, when users work away from the office, or when network conditions make the connection temporarily unavailable). If offline authentication is enabled, Authentication Manager generates offline data (also called offline days) and downloads it to the Authentication Agent client computer when Authentication Agent connects to the RSA Authentication Manager server.

Authentication Agent launches the Auto-Registration utility during RSA SecurID authentication to the local Windows desktop. If the Auto-Registration utility is unable to connect to Authentication Manager during the process, Authentication Agent checks for offline data. If offline data exists, Authentication Agent attempts to authenticate the user offline. If offline data does not exist, Authentication Agent attempts an online authentication to Authentication Manager. If online authentication fails, Authentication Agent issues a message that authentication was not successful. For more information, see [“Offline Authentication”](#) on page 55.

Maintain the Primary IP Address of the Authentication Agent Host

Each Agent host’s primary IP address must be identified in its Agent host record in the RSA Authentication Manager database. You can also list other IP addresses for the host as “secondary nodes” for failover.

If your RSA Authentication Manager system automatically registers Agent hosts, the primary IP address of each Agent host is automatically entered in the Authentication Agent record on RSA Authentication Manager. The address is updated in the record whenever it changes. For more information, see [“Automatic Registration Process”](#) on page 55.

If your system does not use automatic registration, you must ensure that the RSA Authentication Manager administrator knows the primary and secondary IP address of the Authentication Agent host as soon as the Authentication Agent host is initially configured. If an Agent host address changes, inform the RSA Authentication Manager administrator immediately so that the administrator can update the Authentication Agent host record in RSA Authentication Manager.

If Agent hosts are registered manually, the RSA Authentication Manager administrator must make sure the primary IP address in the Authentication Agent host record in the RSA Authentication Manager database matches the one specified in the RSA Control Center, the Authentication Agent host record, or the load balancing options (**sdopts.rec**) file. If the addresses do not match, communication between the Authentication Agent host and the RSA Authentication Manager server fails. If secondary IP addresses are specified for the Authentication Agent host, these must also be entered in the record, and all addresses must be updated if they change.

Multidomain Group Support

When you select a Windows group as an RSA Authentication Agent challenge group using the GPO Policy templates, all users in the group are challenged by RSA SecurID. Authentication Agent supports all Windows groups. For more information about setting up challenge groups, see the *Group Policy Object Template Guide*.

There are many different combinations of Windows groups; universal, global, and domain local. Windows also allows groups to be nested within other groups. It is important to understand the possible combinations of groups so that when you challenge or exclude a group from an RSA SecurID challenge, you get the results that you expect.

The following guidelines determine which users are challenged by RSA SecurID:

- Users in a Windows group are challenged when the Windows group is in a challenge group.
- Users in a Windows group are not challenged when the Windows group is in an excluded challenge group.

The following table lists an example of a multidomain environment that has two domains and different types of groups. All of the users and groups are in the same forest. Authentication Agent cannot determine the membership of a user if the user or group is in a different forest.

Example of Groups and Member in a Multidomain Environment

Type of Group	Description	Member
Universal Groups		
U1D1	Universal Group 1 in Domain 1	User 1 (who is in Domain 1)
U2D2	Universal Group 2 in Domain 2	User 2 (who is in Domain 2)
U3D1	Universal Group 3 in Domain 1	U1D1 U2D2 G1D1 G3D1
Global Groups		
G1D1	Global Group 1 in Domain 1	User 3 (who is in Domain 1)
G2D2	Global Group 2 in Domain 2	User 4 (who is in Domain 2)
G3D1	Global Group 3 in Domain 1	G2D2

Example of Groups and Member in a Multidomain Environment

Type of Group	Description	Member
Domain Local Groups		
L1D1	Domain Local Group 1 in Domain 1	User 5 (who is in Domain 1) User 6 (who is in Domain 2)
L2D1	Domain Local Group 2 in Domain 1	U3D1
L3D1	Domain Local Group 3 in Domain 1	G1D1 G3D1

The following table shows the users who are challenged to log on using RSA SecurID authentication or excluded from it depending on what groups you selected in the previous table.

Challenge or Exclude Group Settings

Group Setting	Users Challenged or Excluded
U1D1	User 1
U3D1	User 1, User 2, User 3, User 4
G1D1	User 3
G3D1	User 4
L1D1	User 5, User 6
L2D1	User 1, User 2, User 3, User 4
L3D1	User 3, User 4

Automatic Password Synchronization

When password changes are made on computers running RSA Authentication Agent, passwords are synchronized in the corresponding RSA Authentication Manager accounts. If a user's password is changed out-of-band (either from a computer not running Authentication Agent or by an administrator on the domain controller), however, the password is not automatically synchronized unless you take the following steps:

1. Install the Authentication Agent on all of the domain controllers in your environment. Restart your domain controllers after the installation has completed. Installing the Authentication Agent installs the password synchronization component that is required for out-of-band password synchronization. The domain controllers must be running the offline authentication feature.

Note: You are not required to enable the RSA SecurID challenge on the domain controllers, because the challenge and password synchronization are independent of each other.

2. Perform a test authentication on the domain controllers.
The test authentication establishes node secrets between the domain controllers and RSA Authentication Manager. The node secrets allow communication between the domain controllers and Authentication Manager.
3. Configure the password synchronization component by specifying settings in the RSA Group Policy Object templates. If you use both the Synchronize User Passwords template and the Challenge Users template on the domain controller, passwords will be synchronized for users in either group. For more information, see the *Group Policy Object Template Guide*.

If you install Authentication Agent on the domain controllers, but do not use the password synchronization setting to specify which users should have their passwords synchronized, challenge settings on the domain controller determine the users for whom passwords are synchronized. For example, if you set the challenge for all users, but you do not set up password synchronization, passwords are synchronized for all users.

5

Troubleshooting

- [Offline Authentication and the Auto-Registration Utility](#)
- [Authentication Issues](#)
- [Diagnose Authentication Issues](#)
- [Error and Event Viewer Log Messages](#)

The following sections contain details on connection and authentication issues you may encounter while using Authentication Agent. This chapter also includes troubleshooting information and details on error messages. For additional troubleshooting information, log on to RSA SecurCare Online at <https://knowledge.rsasecurity.com>.

Note: RSA SecurCare Online is only available to customers who have a valid software service contract.

Offline Authentication and the Auto-Registration Utility

If you perform a custom installation of RSA Authentication Agent for Microsoft Windows and you choose to install the Auto-Registration utility, Authentication Agent launches it when users authenticate with their RSA SecurID passcode to access the local desktop. Auto-Registration determines whether the IP address of the computer has changed. If the IP address has changed, the service updates it in the Authentication Manager database.

If the Auto-Registration utility cannot connect to Authentication Manager, Authentication Agent checks for offline data. If offline data exists, Authentication Agent attempts to authenticate the user offline. If offline data does not exist, Authentication Agent attempts an online authentication to Authentication Manager. If online authentication fails, Authentication Agent issues a message to indicate that the authentication process failed.

The delay between an authentication attempt and notification of authentication status depends on your configuration. For example, if you have a configuration of one RSA Authentication Manager Primary instance and five replica instances, each with one alias in addition to the main IP address, automatic registration spends two seconds attempting to connect to the Authentication Manager server at each IP address assigned to each Authentication Manager server. Each Authentication Manager server can have one primary IP address and three alias IP addresses.

For this configuration, if none of the Authentication Manager instances are available, the Auto Registration utility takes 24 seconds before it determines that the Authentication Manager server is unavailable. The utility then instructs Authentication Agent to attempt offline authentication. If the user is not set up for offline authentication, the Authentication Agent host attempts to authenticate online.

By default, Authentication Agent attempts to authenticate to Authentication Manager five times and, by default, each attempt takes five seconds. This equals a total elapsed time of 25 seconds. The 24 seconds that the Auto-Registration utility requires, plus the 25 seconds for attempted authentication equals a total wait time of 49 seconds between the authentication attempt and notification of authentication status.

Authentication Issues

The following sections describe issues that you may encounter while running Authentication Agent.

RSA SecurID 800 Driver Might Not Install Automatically

The RSA SecurID 800 Authenticator (SecurID 800) has a built-in smart card reader. On most systems, the first time you insert the SecurID 800 into a USB port, the Microsoft Found New Hardware wizard automatically recognizes the device and installs the required Microsoft CCID USB driver. If a system cannot automatically install the driver, you can manually install it through the Microsoft web site (<http://catalog.update.microsoft.com/v7/site/Home.aspx>).

For more information on manually installing the driver, see the SecurID 800 Authenticator Shipment Information file that came with the SecurID 800 order.

Authentication Fails After Changing the 'Send Domain and Username Option'

Whenever you apply a new GPO Template to users, you may need to restart the computer for the policy to take effect.

Test Authentication Succeeds, but Actual Authentication Fails

If the test authentication succeeds, but actual authentication fails, restart the Authentication Agent computer. Authentication Manager automatically creates and sends the node secret to the agent in response to the first successful authentication on the agent. Therefore, if you restart the Authentication Agent computer before a node secret exists, Authentication Agent remains unaware of the node secret even after Authentication Manager passes it to the Authentication Agent host computer.

Important: This scenario only occurs if you did not enable Auto-Registration on RSA Authentication Manager. If you enable it (and install the Auto-Registration utility when you install Authentication Agent), you should not experience this issue.

Node Verification Fails

If the node secret on the Authentication Agent host is corrupted or does not match the node secret in the Authentication Manager database, encrypted communications between Authentication Agent and Authentication Manager cannot work. If this happens, the message **Access Denied, Node Verification Failed** is logged in the Authentication Manager Activity monitor.

Important: If Authentication Manager allows Auto-Registration and you installed the Auto-Registration utility when you installed Authentication Agent, try to resolve the node secret issues listed in this section without user intervention.

The following events can cause node verification failure:

- The Authentication Manager successfully authenticates a user and sends the node secret to the RSA Authentication Agent 7.2, along with a successful authentication message. Authentication Agent times out or fails (for example, due to a power failure) before storing the node secret.
- An administrator uninstalls Authentication Agent and then installs it again. When Authentication Agent is uninstalled, the node secret is removed.
- Authentication Agent is not identified in the Authentication Manager database. This event may generate either a “Node Verification Failed” error message or an “Agent Host Unknown” error message.
- You are using Authentication Manager replica instances, and the replica instance that sent the node secret to Authentication Agent has not yet notified other replica instances. In this case, some users can successfully authenticate and others cannot.
- You are using replica instances, and one or more replica instances are not running. In this case, some users can successfully authenticate and others cannot.
- You clear the node secret on Authentication Agent or Authentication Manager, but not on both.
- You clear the node secret on Authentication Agent and Authentication Manager, but do not restart Authentication Agent if it does not have the Auto-Registration utility installed.
- You enter an invalid user name on the first authentication after clearing the node secret.

Correct a Node Verification Failure

After you review the events that can cause node verification failure in the previous section, if the Auto-Registration utility is not installed and enabled on Authentication Manager, you can correct the node verification failure.

To correct the node verification failure:

1. Clear the node secret from the Authentication Agent host.
2. At the same time, your Authentication Manager administrator must clear the node secret specified for the Authentication Agent host in the Authentication Manager database.
3. Perform a test authentication on the Authentication Agent host.

Important: You must clear the node secret on both the Authentication Agent host and the Authentication Manager server.

For instructions on how to clear the node secret on Authentication Agent, see the RSA Authentication Agent (SecurID) Help. For instructions on how to clear the node secret on Authentication Manager, see the RSA Security Console Help.

Enable Tracing

You can enable tracing from the RSA Control Center to diagnose a range of authentication issues. Typically, you would not enable tracing unless instructed to do so by RSA Customer Support. Customer Support will also instruct you on which components to trace and the levels to set for the tracing.

Note: Tracing is disabled by default. When enabled, the tracing output files are written to **C:\ProgramData\RSA\Logfiles** for Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2.

To enable tracing:

1. From the computer with Authentication Agent installed, open the RSA Control Center.
2. Click **Advanced Tools**.
3. Click **Tracing**.
4. As directed by Customer Support, configure the tracing settings.
5. Click **OK**.

Diagnose Authentication Issues

The following sections describe tasks that you can perform to help diagnose authentication issues.

Verify the Accuracy of the Computer Clock

If a user cannot authenticate, make sure the clock on the user's computer is accurate. If the computer clock drifts from its previous setting, the user may not be able to authenticate.

Verify the System Configuration (**sdconf.rec**) File

If the RSA Authentication Agent 7.2 and the Authentication Manager computers do not have compatible copies of the system configuration file (**sdconf.rec**) file, the computers will not be able to communicate with each other.

To make sure you have the correct **sdconf.rec** file, verify the file settings by opening the Server Environment dialog box.

To view the Server Environment dialog box and verify the **sdconf.rec** file:

1. Open the RSA Control Center.
2. Click **Server Environment**. The left side of the dialog box displays information about the status of the RSA Authentication Manager server and how it communicates with the agent.

3. If you receive an error message, “Unable to retrieve server environment,” the system configuration (**sdconf.rec**) file is corrupt. You must replace the **sdconf.rec**.
For more information about replacing the file, see the [“Replace the System Configuration \(sdconf.rec\) File.”](#)

Replace the System Configuration (sdconf.rec) File

When you view the system configuration file in the previous section, if you receive an “Unable to retrieve server environment” error message, the system configuration (**sdconf.rec**) file is corrupt and you must replace it.

To replace the **sdconf.rec** file:

1. Locate the system configuration (**sdconf.rec**) file on the computer.
2. Obtain a new **sdconf.rec** file from your RSA Authentication Manager administrator.
3. Open the folder with the corrupt **sdconf.rec** file and replace it with the new file.

Important: Make sure that your anti-spy or anti-virus software does not automatically remove the node secret or **sdconf.rec** file.

Error and Event Viewer Log Messages

This section lists RSA Authentication Agent for Microsoft Windows error and event messages and describes the circumstances that cause the error. The messages are listed alphabetically.

AVOID command has invalid IP address in SDOPTS.REC file.

The IP address associated with the AVOID parameter in the **sdopts.rec** file is not valid. For information about creating a correctly formatted **sdopts.rec** file, see [“Manage an sdopts.rec File”](#) on page 82.

Cannot AVOID default IP Address in SDOPTS.REC file address.

The AVOID parameter does not work with the default IP address specified in the **sdopts.rec** file. For information about creating a correctly formatted **sdopts.rec** file, see [“Manage an sdopts.rec File”](#) on page 82.

Can't create socket during initialization in SecurID Authentication. The data is the WINSOCK error code.

Socket services may not have started. Check the Event Log to find out if there is a problem with the network card or the TCP/IP services.

Also, make sure echo services are running on your Authentication Manager by doing one of the following:

- If the Authentication Manager is running on a Windows computer, open the Network control panel, and confirm that **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.
- If the Authentication Manager is running on a UNIX computer, confirm that the **echo** service is running on the Authentication Manager computer. See your UNIX operating system documentation for information about starting the **echo** service.

Data download error encountered for user: <user name>.

An error occurred while offline data was being downloaded for the specified user.

Duplicate AVOID statements in SDOPTS.REC file.

There are two identical AVOID statements in the **sdopts.rec** file. For information about creating a correctly formatted **sdopts.rec** file, see [“Manage an sdopts.rec File”](#) on page 82.

Failed to create service thread, aborting.

Too many other processes were running, so the service did not start.

Incorrect size for file: sdconf.rec.

The **sdconf.rec** file was probably not copied in binary mode. Ask the Authentication Manager administrator for a new copy of **sdconf.rec**.

File not found: aceclnt.dll.

Software may have been installed incorrectly or **aceclnt.dll** may have been deleted. Reinstall the RSA Authentication Agent for Microsoft Windows software from the MSI file (**RSA Authentication Agent.msi**) to correct the problem.

File not found: sdconf.rec.

The **sdconf.rec** file is not in the **HKLM\Software\RSA\RSA Authentication Agent\AuthDataDir** directory. It was either removed or never copied from the Authentication Manager. Ask your Authentication Manager administrator for a new copy of **sdconf.rec**.

Initialization of the Offline Authentication Service Failed.

The offline authentication service failed to start. If this error recurs, restart the computer.

Network Timeout - Authentication Manager was responding but has now stopped.

Make sure the Authentication Manager process is running on the server. Check for a network problem such as a router malfunction or unplugged network cable.

Offline Authentication: Access Denied.

The user's attempt to authenticate offline was unsuccessful.

Offline Authentication: Access Denied - Passcode Reuse Attack Detected.

Someone attempted to reuse a passcode that the user entered to authenticate offline.

Offline Authentication: Access Denied - Previous Tokencode.

The user's attempt to authenticate offline was unsuccessful because the user entered the previously issued tokencode instead of the current one.

Offline Authentication: Authentication Failure Limit Reached. Only Emergency Access Authentication Allowed.

The user's attempt to authenticate offline was unsuccessful and the user has been locked out of the system. The user must contact the Help Desk for an emergency access code.

Offline Authentication: Emergency Access Passcode Accepted.

The user successfully authenticated using an emergency access passcode.

Offline Authentication: Emergency Access Tokencode Accepted.

The user successfully authenticated using an emergency access tokencode.

Offline Authentication: Passcode Accepted.

The user has successfully authenticated offline.

The Offline Authentication service ended abnormally.

The offline authentication service stopped due to an uncommon condition.

The Offline Authentication service was started. Port: *port*.

The offline authentication service was started and is listening on the specified local port.

The Offline Authentication service was stopped.

The offline authentication service was stopped.

The Offline Authentication Time Offset was adjusted to *<time>*.

The clock setting on RSA Authentication Agent for Microsoft Windows or Authentication Manager changed.

User *<user name>* canceled out of New PIN routine.

The user canceled the authentication attempt in New PIN mode.

User *<user name>* canceled Authentication routine.

The user canceled without entering a user name.

User *<user name>*: ACCESS DENIED.

The user was denied access. Check the Authentication Manager Activity Log for the specific reason.

User *<user name>*: ACCESS DENIED. Next Tokencode failed.

The user failed to authenticate in Next Tokencode mode and must attempt to authenticate again.

User *<user name>*: ACCESS DENIED. Server signature invalid.

This message indicates that the identity of the Authentication Manager could not be verified by Authentication Agent. If you see this message, contact RSA Customer Support.

User *<user name>*: canceled out of Next Tokencode routine.

The user canceled out of the Next Tokencode process.

User *<user name>*: New PIN accepted.

The user's new RSA SecurID PIN was verified.

User *<user name>*: New PIN rejected.

The RSA SecurID PIN was rejected by the Authentication Manager. The user needs to reauthenticate to set the RSA SecurID PIN. Check the Authentication Manager Activity Log.

User <user name>: PASSCODE accepted.

The user's passcode was accepted.

User <user name>: Reserve password accepted.

The user was prompted for the reserve password and entered it correctly.

User <user name>: Successfully logged on with Next Tokencode.

Authentication Manager accepted the next tokencode and granted access to the user.

USESERVER and AVOID cannot both be used in sdopts file.

The **sdopts.rec** file is trying to use both USESERVER and AVOID. For information about creating a correctly formatted **sdopts.rec** file, see "[Manage an sdopts.rec File](#)" on page 82.

A

Configuring Automatic Load Balancing

- [Automatic Load Balancing](#)
- [Manage an sdopts.rec File](#)

Automatic Load Balancing

You configure RSA Authentication Agent to automatically balance authentication request loads by creating a load balancing options (**sdopts.rec**) file. The **sdopts.rec** file is a text file stored on the Authentication Agent host (the machine on which an agent is installed). Within the file, you can specify dynamic or manual load balancing.

Important: You must log on with an administrator account if you plan to modify the **sdopts.rec** file.

Dynamic Load Balancing

With dynamic load balancing, Authentication Agent sends a time request to each RSA Authentication Manager server in the realm and determines a priority list based on the response time of each Authentication Manager server. The Authentication Manager server with the fastest response time gets the highest priority and receives the greatest number of authentication requests. Other Authentication Manager servers get lower priorities and fewer requests. This arrangement lasts until Authentication Agent sends another time request or times out.

To perform dynamic load balancing, Authentication Agent connects to the Authentication Manager server through firewalls by using alternate IP addresses (aliases) for the Authentication Manager servers. The Authentication Manager servers provide the aliases to Authentication Agent upon request. The addresses are stored in the configuration record file (**sdconf.rec**) on the Authentication Agent host.

You specify dynamic load balancing by excluding the **USESERVER** statement from the **sdopts.rec** file. For more information, see “[Manage an sdopts.rec File](#)” on page 82.

Manual Load Balancing

With manual load balancing, you specify the RSA Authentication Manager server that each Agent host uses. You also assign a priority to each Authentication Manager server so Authentication Agent can direct authentication requests to some Authentication Manager servers more frequently than others. You specify manual load balancing by including the **USESERVER** statement in the **sdopts.rec** file and associating priority settings with each Authentication Manager server you specify for use. For more information, see “[Manage an sdopts.rec File](#)” on page 82.

Manage an `sdopts.rec` File

This section describes the components that you can use to create an `sdopts.rec` file. It also gives examples of ways you can use the components to set up load balancing.

Create an `sdopts.rec` File

You can create and edit an `sdopts.rec` file using any text editor. After you create the file, save it in the directory specified by the following registry setting: **AuthDataDir** value under the **HKLM\Software\RSA\RSA Authentication Agent** key. To protect the file from unauthorized changes, change the permission settings so that only administrators can modify the file.

Important: Each time you modify the `sdopts.rec` file, restart Authentication Agent to register the changes.

The file can include:

- Comment lines, each preceded by a semicolon.
- Keyword-value pairs, which can be any of the following:
 - **CLIENT_IP=*ip_address***. Specifies an overriding IP address for the Authentication Agent host. The **CLIENT_IP** keyword can appear only once in the file. For information, see [“Specify an Overriding IP Address”](#) on page 87. (Authentication Agent ignores this setting if the IP override is already set through the **Advanced Tools** option in the RSA Control Center. For more information, see the RSA Authentication Agent (SecurID) Help.)
 - **USESERVER=*ip_address, priority***. Specifies an RSA Authentication Manager server to receive authentication requests from the Authentication Agent host according to a specified priority value. Use one setting for each RSA Authentication Manager server that the Authentication Agent host uses. The combined maximum number of Authentication Manager servers you can specify in the `sdopts.rec` and `sdconf.rec` files is 11.

Note: Including this value in the `sdopts.rec` file enables manual load balancing.

Each **USESERVER** keyword value must consist of the actual RSA Authentication Manager IP address separated by a comma from the assigned priority. The priority specifies if or how often an RSA Authentication Manager server receives authentication requests. The following table lists the priority values that you can specify.

Priority	Meaning
2–10	Send authentication requests to this RSA Authentication Manager server using a randomized selection based on the assigned priority of the Authentication Manager server. The range is from 2–10. The higher the value, the more requests the Authentication Manager server receives. A Priority 10 Authentication Manager server receives about 24 times as many requests as a Priority 2 Authentication Manager server.
1	Use this RSA Authentication Manager only if no Authentication Manager servers of higher priority are available.
0	Ignore this RSA Authentication Manager server. A Priority 0 Authentication Manager server can only be used in special circumstances: <ul style="list-style-type: none"> • It must be one of the four Authentication Manager servers listed in the sdconf.rec file. • The Priority 0 Authentication Manager server can only be used for the initial authentication of Authentication Agent, unless all Authentication Manager servers with priorities of 1–10 listed in the sdopts.rec file are known as unusable to Authentication Agent. <p>Generally, a priority value of 0 allows you to put an entry in the file for an Authentication Manager server without using it. You can change the priority value if you decide to use the Authentication Manager server.</p> <p>Note: You must enter keywords in uppercase.</p> <p>If none of the servers with USESERVER statements are responsive, then the default server is the master (if one exists) or the Authentication Manager server used to create the sdconf.rec file is the master.</p>

You must assign a priority to each RSA Authentication Manager that you add to the **sdopts.rec** file. Otherwise, the entry is invalid. The IP addresses in the file are verified against the list of valid RSA Authentication Manager servers that Authentication Agent receives as part of its initial authentication.

- **ALIAS=ip_address, alias_ip_address_1, alias_ip_address_2, alias_ip_address_3.** Specifies one or more alternate IP addresses (aliases) for an Authentication Manager server in addition to the aliases listed for the Authentication Manager server in the **sdconf.rec** file. You can specify up to three additional aliases in the **sdopts.rec** file.

The value for the **ALIAS** keyword must consist of the actual IP address for the RSA Authentication Manager server, followed by up to three aliases for that Authentication Manager server. Authentication Agent sends timed requests to the actual and the aliases.

Only the actual IP address specified by the **ALIAS** keyword must be known by the specified RSA Authentication Manager server. In addition, the actual IP address must be included on any Authentication Manager server list received by Authentication Agent. The Authentication Manager server list provides actual and alias IP address information about all known Authentication Manager servers in the realm. Authentication Agent receives the list from the Authentication Manager server after Authentication Manager validates an authentication request.

- **ALIASES_ONLY=*ip_address***. When you provide an actual IP address of an RSA Authentication Manager server as the value, this keyword tells Authentication Agent to use only the alias IP addresses to contact Authentication Manager.

When you do not provide a value, this keyword tells Authentication Agent to send requests only to the RSA Authentication Manager servers that have alias IP addresses assigned to them. You can create exceptions by including no more than 10 **IGNORE_ALIASES** keywords in the **sdopts.rec** file to specify which Authentication Manager servers must be contacted through their actual IP addresses. For an example showing these exceptions, see [“Specify Alias IP Addresses for Use or Exclusion”](#) on page 86. (If you use this keyword, make sure that at least one RSA Authentication Manager has an alias IP address specified for it in the **sdconf.rec** file or in the **sdopts.rec** file.)

- **IGNORE_ALIASES=*ip_address***. When you do not provide a value, this keyword specifies that all alias IP addresses found in the **sdopts.rec** and **sdconf.rec** files, or on the RSA Authentication Manager list, are ignored. You can create exceptions by including no more than 10 **ALIASES_ONLY** keywords in the **sdopts.rec** file to specify which Authentication Manager servers must be contacted through their alias IP addresses. For an example showing these exceptions, see [“Specify Alias IP Addresses for Use or Exclusion”](#) on page 86.

When you provide an actual IP address as the value, this keyword tells Authentication Agent to use only the actual IP address to contact Authentication Manager.

- **AVOID=*ip_address***. When you provide an actual IP address of an RSA Authentication Manager server as a value, this keyword tells Authentication Agent to exclude this Authentication Manager server from use during dynamic load balancing.

Important: Use the **AVOID** keyword only for dynamic load balancing. Do not use it with the **USESERVER** keyword for manual load balancing.

Exclude an Authentication Manager Server During Dynamic Load Balancing

In dynamic load balancing, you exclude an RSA Authentication Manager server from use for authentication by including the **AVOID** keyword in the **sdopts.rec** file. When you provide an actual IP address of an RSA Authentication Manager server as a value, this keyword tells Authentication Agent to exclude this Authentication Manager server from use during dynamic load balancing.

Important: Use the **AVOID** keyword only for dynamic load balancing. Do not use it with the **USESERVER** keyword for manual load balancing. If the **AVOID** keyword is included in an **sdopts.rec** file that includes a **USESERVER** statement, the **AVOID** statement is considered an error.

If you use the **AVOID** statement with the IP address of the default RSA Authentication Manager server, the statement is ignored unless another Authentication Manager server is available. The default Authentication Manager server is the one where the **sdconf.rec** file was created. If an Authentication Manager server is designated as the master, however, it becomes the default Authentication Manager server regardless of where the **sdconf.rec** file was created.

The following example shows how to use the **AVOID** keywords in the **sdopts.rec** file:

```
AVOID=192.100.123.5
```

In this example, the RSA Authentication Manager server with the IP address 192.100.123.5 will not be used for authentication.

Configure Manual Load Balancing

You configure manual load balancing by including the **USESERVER** keyword in the **sdopts.rec** file to specify the IP addresses of the RSA Authentication Manager servers that you want each Agent host to use.

You can list the IP addresses in the **sdopts.rec** file in any order, but you must list each separately, one per line. The following example shows how to use the **USESERVER** keywords to specify the IP addresses.

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).
;Do not put a blank space between a keyword and its
;equal sign. Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from a priority
;value.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
```

In this example, the Authentication Manager server identified by IP address 192.168.10.23 receives more authentication requests than Authentication Manager server 192.168.10.22. Authentication Manager server 192.168.10.20 is used only if the Authentication Manager servers of higher priority are unavailable. Authentication Manager server 192.168.10.21 is ignored except in rare circumstances (as described in [“Manage an sdopts.rec File”](#) on page 82).

Note: You can use the **USESERVER** and **ALIAS** keywords together in the **sdopts.rec** file. However, **USESERVER** keywords do not affect the alias addresses used to connect to the Authentication Manager servers, and **ALIAS** keywords have no effect on which Authentication Manager servers are specified for use.

Specify Alias IP Addresses for Use or Exclusion

You can use the **sdopts.rec** file to specify alias IP addresses for use or for exclusion.

Important: Authentication Agent ignores this setting if the IP override is already set through the **Advanced Settings** option in the RSA Control Center. For more information on setting the IP address through the Control Center, see the RSA Authentication Agent (SecurID) Help.

You can list the settings in the **sdopts.rec** file in any order, but you must list each setting separately, one setting per line. The following example shows how to use the **ALIAS** keywords in the **sdopts.rec** file.

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).
;Do not put a blank space between a keyword and its
;equal sign. Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from a priority
;value.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
ALIAS=192.168.10.23, 192.168.4.1, 192.168.4.2, 192.168.4.3
ALIAS=192.168.10.22, 192.168.5.2, 192.168.5.3
ALIAS=192.168.10.20, 192.168.5.1
ALIAS=192.168.10.21, 0, 192.168.1.1
ALIAS_ONLY=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

In this example, the default is to use alias or actual IP addresses, with some exceptions. The RSA Authentication Manager server with the actual IP address 192.168.10.23 has three alias addresses specified for it, while Authentication Manager servers 192.168.10.20 and 192.168.10.21 each have only one alias. RSA Authentication Manager server 192.168.10.22 has two alias addresses. The aliases specified by the **ALIAS** keywords are additions to any aliases specified in the **sdconf.rec** file and in the RSA Authentication Manager server.

This example shows how to use the **USESERVER** and **ALIAS** keywords together in the **sdopts.rec** file. However, **USESERVER** keywords do not affect the alias addresses used to connect to the Authentication Manager servers, and **ALIAS** keywords have no effect on which Authentication Manager servers are specified for use.

In this example, the default is to use aliases with two exceptions. RSA Authentication Manager server 192.168.10.23, as specified by the **ALIASES_ONLY** keyword, will be contacted only through its alias IP addresses. RSA Authentication Manager server 192.168.10.22, specified by the **IGNORE_ALIASES** keyword, will be contacted only by using its actual IP address.

In the following example, the default is to ignore aliases, with two exceptions:

```
IGNORE_ALIASES
ALIASES_ONLY=192.168.10.23
ALIASES_ONLY=192.168.10.22
```

The **ALIASES_ONLY** exceptions specify that Authentication Agent should send its requests to RSA Authentication Manager server 192.168.10.23 and 192.168.10.22 by using only their alias IP addresses.

In the following example, the default is to use aliases, with two exceptions:

```
ALIASES_ONLY
IGNORE_ALIASES=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

The **IGNORE_ALIASES** exceptions specify that Authentication Agent should send its requests to RSA Authentication Manager server 192.168.10.23 and 192.168.10.22 by using only their actual IP addresses.

Specify an Overriding IP Address

When Authentication Agent runs on a host that has multiple network interface cards, and therefore multiple IP addresses, you must specify a primary Agent host IP address to use for encrypted communications between Authentication Agent and RSA Authentication Manager. Agent hosts typically attempt to discover their own IP addresses. An Agent host with multiple addresses might select one that is unknown to RSA Authentication Manager, making communication between Authentication Agent and Authentication Manager impossible. You can specify an overriding primary IP address by including the **CLIENT_IP** keyword in an **sdopts.rec** file on the Authentication Agent host.

Note: The Dynamic Host Configuration Protocol (DHCP) allocates IP addresses to Agent hosts dynamically. To avoid address conflicts, install the Auto-Registration utility when you install Authentication Agent. For more information, see Chapter 3, [“Installing RSA Authentication Agent”](#) and Chapter 5, [“Troubleshooting.”](#)

To specify an IP address override in the **sdopts.rec** file, follow this example:

```
CLIENT_IP=192.168.10.19
```

This statement ensures that the Authentication Agent host always uses the specified IP address to communicate with Authentication Manager.

Important: Authentication Agent ignores this setting if the computer has the IP address override option set in the RSA Control Center. However, if you installed the Auto-Registration utility (during or after the Authentication Agent installation process), the address that the utility registers overrides the IP setting in the Control Center. (The **IP address override setting** field also appears inactive once you install the Auto-Registration utility.) For more information on setting the IP address through the Control Center, see the RSA Authentication Agent (SecurID) Help.

Glossary

Term	Definition
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.
challenge group	A group of users that will be challenged by the RSA SecurID Agent.
connected	Refers to a USB authenticator that is plugged into a USB port or extender cable.
Credential Provider	See Microsoft logon (Credential Provider)
disconnected	Refers to a USB authenticator that is not connected to a USB port or extender cable.
domain	A group of server and client machines that exist in the same security structure. Domains are defined by the administrator and share a common database.
emergency access	Alternative procedures that users can follow in an emergency to gain access to their machines or other protected resources when they do not have access to their normal credentials.
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.
exempt administrator account	An agent group that is exempt from challenge.
local authentication client	An RSA Authentication Agent component that requires users to enter valid RSA SecurID passcodes to access their Microsoft Windows desktops

Term	Definition
Microsoft logon (Credential Provider)	A logon method that uses the Microsoft Credential Provider and presents standard Windows logon dialog boxes for Microsoft Windows 7, Vista, and Windows Server 2008.
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.
notification area	An area on the taskbar of a computer using Windows that is used to display notifications to the user. The area contains small icons for each notification facility.
notification icon	An icon in the notification area that may contain a pop-up icon used to tell users of events or actions to take.
offline authentication	An option in RSA Authentication Agent that requires users to enter RSA SecurID passcodes to authenticate to their Windows desktops even when their computers are not connected to the RSA Authentication Manager through the network.
offline data	Data generated by the RSA Authentication Manager and downloaded to the agent to enable offline authentication. This term is used in administrator documentation. See also offline days.
offline days	Data generated by the RSA Authentication Manager and downloaded to the agent to enable offline authentication. This term is used in end-user documentation. See also offline data.
offline days status icon	An icon in the Windows notification area that tells users the general status of their supply of offline days.
offline emergency access	An alternate way for users to access protected resources while offline without using their normal credentials.
passcode	A code used in RSA SecurID authentication to gain access to a protected resource. It is made up of two factors: a Personal Identification Number (PIN) and the tokencode (random number) currently displaying on the front of an RSA SecurID token.
remote authentication client	A remote authentication client computer that hosts the RSA Authentication Agent remote authentication client component.

Term	Definition
refresh offline days	Enables users to get more offline days.
reserve password	<p>An emergency access method that enables the administrator to authenticate to a user's protected computer as that user without entering an RSA SecurID passcode under the following circumstances:</p> <ul style="list-style-type: none"> • The offline authentication service is not running on the local computer • The computer cannot connect to RSA Authentication Manager
RSA Credential Provider	A replaceable DLL component that performs user identification and authentication interactions during logon for Windows 7, Vista, and Windows Server 2008.
RSA SecurID 800 Authenticator	An authenticator that users can use as a smart card or as a SecurID token. Users can attach the SecurID 800 to a USB port for SecurID authentication or use it as a handheld device, depending on the RSA application they use.
RSA SecurID Connected Authenticator	The software used with a connected RSA SecurID 800 Authenticator. The software is installed on the desktop and is accessed through the RSA Control Center.
RSA SecurID PIN	A user-created or system-generated PIN (personal identification number) that is used with a tokencode to generate a passcode.
Server administrator	A person with access to certain administrative features on an RSA Authentication Manager software product through the administration user interface. The administrator privileges may range from viewing information stored on the server to performing user-specific and system-wide operations.
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.
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).
USB authenticator	A hardware authenticator with a connector for connecting the authenticator to a USB port.
Windows account	A user name, password, and domain that identify a particular user to the Windows operating system.

Term	Definition
Windows password integration	A feature that integrates the Microsoft Windows password into the RSA SecurID logon process.

Index

A

- account privileges, 41
- agent
 - definition, 89
- agent auto-registration utility
 - definition, 89
- agent host
 - definition, 89
- Agent Host Auto-Registration utility
 - affect on the node secret, 66
- alias IP addresses, excluding from load balancing, 86
- ALIAS keyword, 83, 86
- ALIASES_ONLY keyword, 84
- Authentication Agent
 - description, 9
 - managing with GPO templates, 12
- authentication problems, diagnosing, 74
- authentication, offline, 10, 55
- authenticator
 - supported, 17
 - using, 17
- Automated Agent Host Registration and Update utility
 - configuring for exemptions, 65
- automatic
 - refresh of offline days, 57
 - update of IP addresses, 13
- Auto-Registration utility
 - behavior during offline authentication, 67
 - overview, 64
- AVOID keyword, 84, 85

C

- challenge
 - options, 10
- challenge group
 - definition, 89
- challenging users, 10
- Citrix ICA Client, 24
- CLIENT_IP keyword, 82, 87
- command line, 43
- configuration wizard, 38
- connected
 - definition, 89
- Control Center, 18

- creating
 - sdopts.rec file, 82

D

- deploying installation package, 42
- description
 - RSA Control Center, 18
- description, Authentication Agent, 9
- diagnosing authentication problems, 74
- disconnected
 - definition, 89
- documentation, 7
- dynamic load balancing
 - excluding an Authentication Manager, 85
 - overview, 81

E

- elevated privileges, installing product with, 41
- emergency access, 60
 - for administrators, 11
 - offline, 60
- encrypted communication, 47
- error messages, 76
- Event Viewer
 - log messages, 76
- ExcludeAdaptor, 65
- exempt administrator account, 11

G

- Group Policy Object (GPO) templates, 12

I

- icon, notification area, 59
- IGNORE_ALIASES keyword, 84
- installation
 - command line, 43
 - language, 16, 46
 - methods, 32
 - multiple computers, 38
 - repair, 50
 - silent, 38
 - single computer, 36
- installation package
 - deploying, 42
- IP addresses, automatic update, 13

K

keywords

- ALIAS, 83, 86
- ALIASES_ONLY, 84
- AVOID, 84, 85
- CLIENT_IP, 82, 87
- IGNORE_ALIASES, 84
- USESERVER, 81, 82, 85

L

- language, 46
 - uninstall, 53
- language, for installation, 16
- load balancing, 81
 - dynamic, 81
 - excluding alias IP addresses, 86
 - maintaining primary IP addresses, 67
 - manual, 81
 - specifying an overriding IP address, 87
- logs
 - Event Viewer, 76

M

- managed applications, 41
- managing Authentication Agent, 12
- manual load balancing
 - configuring, 85
 - overview, 81
- modifying options, 48

N

- node secret, 47
- node secret, clearing and replacing, 72
- node verification failure, 72
- notification icon, 59

O

- offline authentication, 10, 55, 62
 - for remote users, 62
- offline days
 - checking the supply, 59
 - managing, 57
 - refreshing
 - automatically, 57
 - when there is a network connection, 57
 - without network connection, 58
- offline days status, 59
- options for challenging users, 10

- overriding IP address, specifying for load balancing, 87

P

- password integration, 11
- ports, required, 21
- preparations
 - RSA SecurID users, 30
- primary IP addresses, maintaining, 67
- product
 - description, 9

R

- refreshing offline days
 - when there is a network connection, 57
 - without network connection, 58
- reinstall properties, 48
- remote access products, 24
- Remote Desktop Connection, 24
- remote users, 62
- removing Authentication Agent, 51
- repairing an installation, 50
- required operating systems, 22
- required ports, 21
- requirements, 21
- RSA Control Center, 18
- RSA SecurID users, preparing, 30

S

- sdconf.rec file
 - copying from RSA Authentication Manager, 26
 - viewing, 74
- sdopts.rec file
 - creating, 82
- sdopts.rec file, creating, 82
- settings
 - node secret, 72
- silent installation, 38
- status, offline days, 59

T

- tokencode, emergency, 60

U

- uninstalling Authentication Agent, 51
- uninstalling language, 53
- updating IP addresses automatically, 13

upgrade
 RSA Authentication Agent 7.0 for
 Microsoft Windows, 51
upgrade to Windows Vista, 51
users, challenging, 10

USESERVER keyword, 81, 82, 85

W

Windows password integration, 11