RSA® Authentication Agent 1.5 for Citrix® StoreFront™ Installation and Administration Guide

Contact Information

See the RSA corporate website for regional Customer Support telephone and fax numbers:
https://www.rsa.com/en-us/services/rsa-product-and-customer-support

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of Dell Inc. throughout the world. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **http://www.emc.com/legal/emc-corporation-trademarks.htm**.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell Inc. or its subsidiaries, 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 Dell Inc.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA SecurCare Online. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

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

Distribution

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

Dell 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." DELL INC. 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.

February 2018

Contents

Preface

About This Guide

This guide describes how to install and configure RSA® Authentication Agent for Citrix® StoreFront™. It is intended for administrators who deploy, configure, and manage the product. Do not make this guide available to the general user population.

The document assumes you have experience administering Citrix StoreFront and Citrix NetScaler Gateway™. It also assumes you have experience with RSA Authentication Manager or are working with an RSA Authentication Manager administrator.

Product Documentation

The product documentation is available from the following web locations:

- **https://www.rsa.com/en-us/products/rsa-securid-suite/rsa-securid-access/securid-authentication-agents.html**
- **https://community.rsa.com/**

Release Notes. Provides information about this release and about known issues.

Configuring Citrix StoreFront for Delegated Forms Authentication with RSA SecurID. Describes procedures to check the current Delegated Forms Authentication (DFA) configuration for Citrix StoreFront, and enable or disable RSA SecurID authentication for DFA.

RSA Control Center Help. Describes administrator tasks performed in the RSA Control Center. To view Help, click the **Help** option in RSA Control Center.

Related Documentation

RSA Authentication Manager Administrator's Guide. Provides information about how to administer users and security policies. See RSA Link: **https://community.rsa.com/docs/DOC-40601#am**.

Support and Service

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

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

Before You Call Customer Support

Make sure that you have direct access to the server running Agent for Citrix StoreFront.

Have the following information available when you call:

- Your RSA Customer/License ID. Agent for Citrix StoreFront is free to customers. Use the RSA Authentication Manager software version number as your Customer/License ID. To find this number, in RSA Security Console, click **Help > About RSA Security Console**, then click the **See Software Version Information** link.
- The make and model of the server where the problem occurs.
- The name and version of the operating system where the problem occurs.

1 RSA Authentication Agent for Citrix StoreFront

Overview of Authentication Services

RSA Authentication Agent for Citrix StoreFront is software that provides Citrix StoreFront with methods for authenticating users inside and outside of the corporate firewall. The Agent supports two types of authentication:

- RSA SecurID®
- RSA Authentication Manager Risk-Based Authentication (RBA)

To extend either form of authentication to users outside of the corporate firewall, the Agent must be used with Citrix NetScaler Gateway and the Citrix Delegated Forms Authentication (DFA) feature. See Chapter 5, "Citrix Delegated Forms Authentication" on page 37.

RSA SecurID

RSA SecurID protects resources using two-factor authentication with hardware and software-based tokens. When Agent for Citrix StoreFront authenticates users with RSA SecurID, a user is prompted for an RSA SecurID passcode when attempting to log on to a StoreFront store. The Agent verifies the passcode against RSA Authentication Manager and, if successful, StoreFront grants access to the protected resource.

For instructions on configuring SecurID authentication, see Chapter 4, "Configuring and Managing the Agent for Citrix StoreFront" on page 29.

Risk-Based Authentication

RBA applies knowledge of the client device and user behavior to assess the potential risk of an authentication request. For authentication attempts with elevated risk levels, users are further challenged to confirm their identity. When RBA is enabled together with Windows Password Integration (WPI), a user who successfully authenticates is logged on to a StoreFront store and is not required to enter separate credentials. For details on WPI, see "Windows Password Integration" on page 10.

For information on enabling the Agent to integrate with RBA, see Chapter 6, "Enabling RSA Authentication Manager Risk-Based Authentication" on page 41.

RSA Authentication Agent Auto-Registration Utility

The Agent for Citrix StoreFront must be registered with RSA Authentication Manager to authenticate users. RSA Authentication Manager identifies agents by IP address, and uses a node secret that is specific to each Agent to protect authentication information while in transit.

The RSA Authentication Agent Auto-Registration utility is an optional feature of Agent for Citrix StoreFront. This utility registers the Agent with RSA Authentication Manager and updates the IP address and node secret as needed, without manual intervention.

Consider using Auto-Registration if your network uses the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses, or in environments that use wireless and Virtual Private Network (VPN) connections to access the corporate network. Installation instructions for the Auto-Registration utility are described in Chapter 3, "Installing the Agent for Citrix StoreFront" on page 21.

You can configure the Auto-Registration utility to exclude specific network adapters from automatic IP address registration. For more information, see "Exclude Specific Network Adapters from Auto-Registration" on page 29.

Note: The Auto-Registration utility is not supported in a Citrix StoreFront server group. Select the Auto-Registration utility only if the StoreFront deployment consists of a single server with no load balancer.

Windows Password Integration

Windows Password Integration is an optional feature of RSA Authentication Manager, and is disabled by default. When the feature is enabled, the Agent for Citrix StoreFront can retrieve a Windows password from RSA Authentication Manager and use it during logon to Citrix StoreFront. Users provide Windows passwords only during initial authentication. At that time, the Agent stores the Windows passwords with user authentication data in RSA Authentication Manager. During subsequent authentications, users enter only their user names and RSA SecurID passcodes. The Agent for Citrix StoreFront uses stored passwords for authentication to Active Directory.

You can enable Windows password integration system-wide, on an individual Agent basis, or by groups. For example, to enable Agent for Citrix StoreFront, you create an Agent record in the RSA Authentication Manager database. You can enable Windows password integration for all of the Agent for Citrix StoreFront computers in the database, or select certain computers. For more information about RSA Authentication Manager, see the Help at RSA Link.

When users change the Windows password from within a Citrix StoreFront session, the Agent for Citrix StoreFront automatically synchronizes the password in corresponding accounts in the RSA Authentication Manager database. If a user's password is changed outside of such a session, the password stored on Authentication Manager will not be updated. However, when the stored password is later retrieved by the Agent for Citrix StoreFront, the user is prompted to enter the correct password and the password is stored on Authentication Manager.

RSA Authentication Agent Offline Local Service

The Agent for Citrix StoreFront does not support the Offline Authentication feature provided by the RSA Authentication Agent for Microsoft Windows. However, the Windows Password Integration feature depends on the RSA Authentication Agent Offline Local service. If you are using Windows Password Integration, do not disable this service.

Note: The Agent for Citrix StoreFront configures the Offline service to not download user offline data.

RSA Control Center

RSA Control Center is the administration application for the Agent for Citrix StoreFront. In the Agent Control Center, you can perform the following tasks.

Task	Description
Test Authentication	Submits RSA SecurID credentials (SecurID username and passcode) to Authentication Manager in order to verify that Agent for Citrix StoreFront can authenticate against RSA Authentication Manager. For more information, see "Perform a Test Authentication" on page 24.
Tracing	Generates log files for troubleshooting. For more information, see "Enable Tracing" on page 47.
IP Address Override	Specifies the primary IP address to use when the server hosting Agent for Citrix StoreFront has multiple IP addresses. RSA Authentication Manager uses the IP address to identify the Agent. This feature helps prevent Agent authentication failures. For more information, see "Enable an IP Address Override" on page 34.
Clear Node Secret	Clears the node secret from the agent host. For more information, see "Clear the Node Secret" on page 35.
Server Environment	Displays information about your Authentication Manager server environment so you can check the primary and replica RSA Authentication Manager servers, and check that Agent for Citrix StoreFront is communicating with the correct RSA Authentication Manager server.

Open RSA Control Center and Access Help

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

- On Windows 2008 R2, click **Start > All Programs > RSA > RSA Agent Control Center**.
- On Windows 2012, click **Start > RSA Agent Control Center**.
- On Windows 2012 R2, click **Start > Apps > RSA Agent Control Center**.
- On Windows Server 2016, click **Start > Apps > RSA Agent Control Center**.

To access RSA Control Center Help, launch the RSA Control Center and click **Help > RSA Authentication Agent for Citrix StoreFront**.

Citrix StoreFront Management Console

The Citrix StoreFront Management Console (MMC) is the primary interface for enabling, disabling, and managing **RSA SecurID** authentication on the StoreFront server after the Agent for Citrix StoreFront is installed.

You use the Citrix StoreFront MMC to perform the following Agent for Citrix StoreFront tasks:

- Add or remove the **RSA SecurID** authentication method from the list of methods that can be enabled and disabled. Removing the **RSA SecurID** authentication method from the list does not uninstall it from your system. For more information, see "Install or Uninstall the RSA SecurID Authentication Method for a Store" on page 32.
- Enable or disable the **RSA SecurID** authentication method. Enabling the **RSA SecurID** authentication method automatically overrides the Citrix **User name and password** authentication method. When the **RSA SecurID** authentication method is disabled, you can use other available methods. For more information, see "Add or Remove a StoreFront Server in a Server Group Configured to Use the RSA SecurID Authentication Method" on page 33.
- Include the domain name as part of the user name sent to Authentication Manager when authenticating. For more information, see "Manage the RSA SecurID Authentication Send Domain Option" on page 33.

Open the Citrix StoreFront Management Console

To open the Citrix StoreFront MMC, do one of the following:

- On Windows 2008 R2, click **Start > All Programs > Citrix > Citrix StoreFront**.
- On Windows 2012, click **Start > Citrix StoreFront**.
- On Windows 2012 R2, click **Start > Apps > Citrix StoreFront**.

- On Windows Server 2016, click **Start > Apps > Citrix StoreFront**.

Note: The procedures in this document assume that the Citrix StoreFront MMC is configured to display three panes. A left **Console tree** pane, a center **Results** pane, and a right **Actions** pane.

Coexistence With RSA Authentication Agent for Microsoft Windows

The RSA Authentication Agent for Windows (the Windows Agent) is authentication software that protects logon to Windows computers by requiring users to authenticate with RSA SecurID. The Agent for Citrix StoreFront and the Windows Agent share several product components: the RSA Control Center, Agent Auto-Registration, SecurID Authentication and the Offline service.

Both Agents can be installed on a Citrix StoreFront server with the following limitations:

- The Agent Auto-Registration feature can only be installed by one Agent at a time.
- When both products are installed, the version of RSA Control Center installed by the Windows Agent supersedes the version installed by the Agent for Citrix StoreFront. However, the RSA Control Center will contain the features and Help topics from both Agents.
- When both products are installed, the Offline Authentication feature of the Windows Agent is unavailable because the Agent for Citrix StoreFront disables the download of offline data. This can be re-enabled by changing a registry value, as follows.

  1. Open the Registry Editor:

     Click **Start**. Type **regedit** in the search box, and click **regedit** in the results list under **Programs**.

  2. Open the key:

     HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT

  3. Change the value of **NoDADownload** (a REG_DWORD) from **1** to **0**.

Note: When installing both Agents, RSA recommends that you install the RSA Authentication Agent for Windows first.

Citrix StoreFront Support for RSA Authentication Manager Features

The following table shows the RSA Authentication Manager features supported by Citrix StoreFront.

RSA Authentication Manager Feature	Supported
RSA SecurID authentication using native RSA SecurID protocol	✓
RSA SecurID authentication using RADIUS protocol	
On-demand authentication (ODA) using native RSA SecurID protocol	✓
ODA using RADIUS protocol	
Risk-based authentication (RBA)	✓
RBA with single sign-on	✓
Password integration	✓
RSA Authentication Manager replica support	✓
Secondary RADIUS server support	
RSA SecurID software token automation	
RSA SecurID 800 Authenticator automation	
RSA SecurID protection of administrative interface	

Language Support

Agent for Citrix StoreFront provides localized (translated) Citrix StoreFront web pages. The localized pages display according to the language preferences presented by the web browser. Localized pages are provided for US English and the following languages:

- German (de)
- Chinese (zh-CN)
- Chinese (zh-Hans)
- Chinese (zh-Hant)
- Chinese (zh-tw)
- French (fr)
- Japanese (ja)
- Korean (ko)
- Latin Spanish (es)
- Russian (ru)

Note: The RSA UI in the Citrix StoreFront Management console, this *Installation and Administration Guide*, and other documentation for RSA Agent for Citrix StoreFront are provided in English only.

2 Preparing for Installation

System Requirements

The RSA Authentication Agent for Citrix StoreFront requires the following system components:

- Windows operating system:
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2
- Citrix StoreFront 3.12 or 3.13
- Microsoft .NET Framework 4.5 or later

Note: Windows Server 2008 R2 does not include the Microsoft .NET Framework 4.5 by default, but you can download an installer from Microsoft.

In addition to the hardware requirements imposed by the above components, the Agent for Citrix StoreFront requires a minimum of 50 MB free disk space.

Security Considerations

The Agent for Citrix StoreFront provides authentication services to Citrix StoreFront through a programming interface defined by Citrix. To protect user credentials that flow through this interface, RSA recommends that you configure your Citrix environment (StoreFront and, if applicable, NetScaler Gateway) to use HTTPS to secure communications between Citrix StoreFront and users. RSA also recommends that you configure Microsoft Internet Information Services (IIS), which hosts the Citrix StoreFront services, and the Microsoft TLS/SSL Security Provider (used by IIS) to use Transport Layer Security (TLS) v1.2 or later.

For information on configuring Citrix StoreFront to use HTTPS, see the Citrix documentation website at **https://www.citrix.com/support/**. Search on the keywords *https* and *StoreFront*.

For information on configuring the Microsoft TLS/SSL Security Provider to use TLS v1.2, see the Microsoft documentation at **http://support.microsoft.com**. Search on *How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll*.

For guidance on configuring TLS, refer to the National Institute of Standards and Technology publications on Computer Security at **http://csrc.nist.gov/publications/PubsSPs.html**. Search on *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

Required TCP/IP Ports

The following TCP/IP ports must be available for use by Agent for Citrix StoreFront and RSA Authentication Manager.

Port	Description
5500/udp	Authentication Manager uses this port to listen. The Agent for Citrix StoreFront connects to this port during authentication.
5550/tcp	The optional RSA Authentication Agent Auto-Registration utility uses this port to automatically register the Agent with RSA Authentication Manager.
5580/tcp	Must be available if Password Integration is required. Authentication Manager uses this port to support changes to users' Windows passwords. The RSA Authentication Agent Offline Local service connects to this port.

Supported Web Browsers

Agent for Citrix StoreFront supports the following web browsers:

- Edge (38) on Windows 10
- Internet Explorer (9, 10, and 11)
- Google Chrome (64)
- Mozilla Firefox (58)
- Safari on OS Yosemite
- Android Web Browser on Android 7.0
- Safari on iOS 10.2

Important: JavaScript must be enabled in the browser.

RSA Authentication Manager Requirements

Agent for Citrix StoreFront requires RSA Authentication Manager 8.2 SP1 or later.

User Authentication Requirements

Users must have an RSA hardware or software authenticator in order to authenticate to Citrix StoreFront resources protected with RSA SecurID.

Note: The RSA SecurID 800 Hybrid Authenticator (SecurID 800) can be used in disconnected mode only.

Users must be enabled for Risk-Based Authentication (RBA) in order to authenticate to Citrix StoreFront resources protected with RBA.

Preinstallation Tasks

- Obtain the RSA Authentication Manager configuration file (**sdconf.rec).**
- Obtain the RSA Authentication Manager server certificate (**server.cer**) file if you plan to use the Authentication Agent Auto-Registration utility.
- Prepare users for RSA SecurID authentication.
- If applicable, prepare users for RSA Authentication Manager Risk-Based Authentication (RBA)

Obtain the RSA Authentication Manager Configuration File

To configure communication between Agent for Citrix StoreFront and Authentication Manager, you must generate the RSA Authentication Manager configuration file, **sdconf.rec**, in RSA Authentication Manager and make it accessible while installing the Agent.

The **sdconf.rec** file contains a snapshot of the server information available at the time the file was generated.

Procedure

1. Log on to the RSA Authentication Manager Security Console as an administrator.
2. Select **Access > Authentication Agents > Generate Configuration File**.
3. Using the default settings, select **Generate Config File**.
4. Click the **Download Now** link and save the file in a location accessible during the the Agent the Agent installation.
5. Unzip the **AM_Config.zip** file so that the contents can be used.

Note: To ensure successful RSA SecurID authentication, use a copy of the **sdconf.rec** file generated from an Authentication Manager server that performs authentication. (The authentication service must be running on that server.)

Download the the RSA Authentication Manager Server Certificate for Auto-Registration

The RSA Authentication Manager server certificate file (**server.cer**) is required for installing the RSA Authentication Agent Auto-Registration utility.

If you do not install the Auto-Registration utility, you must manually register the Agent in the RSA Authentication Manager database. For more information, see "Register the Agent in RSA Authentication Manager" on page 23.

Note: If you are installing the RSA Authentication Agent Auto-Registration utility, Authentication Manager must be configured to allow automatic agent host registration. For more information, see the *RSA Authentication Manager Administrator's Guide* or RSA Authentication Manager Help.

Procedure

1. Log on to the RSA Authentication Manager Security Console as an administrator.
2. Select **Access > Authentication Agents > Download Server Certificate File**.
3. Click **Download Now** and save the file to a location accessible during the Agent installation.

Prepare Users for RSA SecurID or RBA Authentication

Before deploying Agent for Citrix StoreFront, review the following sections in the AM Help on RSA Link and perform the appropriate tasks.

- "Deploying and Administering RSA SecurID Tokens"
- "Deploying Risk-Based Authentication"

Provide your users with authentication instructions.

3 Installing the Agent for Citrix StoreFront

The installation program installs the following items:

- RSA Authentication Agent for Citrix StoreFront
- RSA Control Center
- RSA Authentication Manager configuration file
- (Optional) Auto-Registration utility
- (Optional) RSA Authentication Manager Server Certificate

Install Agent for Citrix StoreFront

To install Agent for Citrix StoreFront, you can either use the Install Wizard, which guides you through the installation process, or run the installation program from the command-line.

Prerequisites

You must have administrator rights for the Citrix StoreFront server on which you are installing Agent for Citrix StoreFront.

Before installing, perform the following tasks:

- Close the Citrix StoreFront Management Console.
- Copy **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to deploy the product.
- Copy **sdconf.rec** (and **server.cer**, if you want to install Auto-Registration) to the same folder.
  - The Install Wizard prompts you to browse and select the files.
  - The command-line installation collects these files from the folder from which it is run.

Installation Considerations for Citrix StoreFront Server Groups

If you are installing Agent for Citrix StoreFront in a Citrix StoreFront server group, observe the following guidelines:

- You can create a script to push command-line installation to each server in the server group.
- The Auto-Registration utility is not supported in a server group.
- You must install the Agent for Citrix StoreFront on each server before propagating changes across the server group.

Install Using the Install Wizard

Procedure

1. Log on to the Citrix StoreFront server where you want to install the Agent.
2. In the folder where you copied the package file, double-click **RSA Authentication Agent for Citrix StoreFront x64.msi** to start the installation wizard.
3. Click **Next** to continue.
4. Read the License Agreement or click **Print** to print it. Select **I accept the terms in the license agreement** and click **Next**.
5. (Optional) To install the Auto-Registration utility, select **Will be installed on the local hard drive** from the **Auto-Registration Utility** drop-down list.
6. Click **Next**.
7. Click **Browse** to locate and open the system configuration file (**sdconf.rec**). Click **Next**.
8. If you are installing the Auto-Registration utility, click **Browse** to locate and open the server certificate file (**server.cer**). Click **Next**.
9. Click **Install**.
10. When installation completes, click **Finish**.

Install Using Command-Line Options

Run the command-line installation on individual Citrix StoreFront servers, or execute the command on multiple servers using a script or third-party product, such as Microsoft System Center Configuration Manager (ConfigMgr) or IBM Tivoli.

Before You Begin

Know how to install software using the msiexec command-line options. For more information on msiexec commands, visit **http://technet.microsoft.com**.

Procedure

1. Open an administrator command prompt.
2. Navigate to the directory that contains the **RSA Authentication Agent for Citrix StoreFront x64.msi** package file. Otherwise, provide the full pathname to the package file on the command-line.
3. Do one of the following:
   - To install the Agent, use a command similar to the following:

     ```
     msiexec /qn /i "RSA Authentication Agent for Citrix StoreFront x64.msi"
     ```
   - To install the Agent and the Auto-Registration utility, use a command similar to the following:

     ```
     msiexec /qn /i "RSA Authentication Agent for Citrix StoreFront x64.msi" ADDLOCAL=AgentAutoRegistration
     ```

In the previous examples, the `/qn` switch instructs the installer to run in silent mode, suppressing all UI elements. To log any errors, add the `/lv` (log verbose) option at the end of the command. Store the log file, for example, **install.log**, in a known location such as **%USERPROFILE%**.

4. (Optional) To install the product on multiple Citrix StoreFront servers, execute the command on the servers using a script or a third-party product, such as System Center Configuration Manager (ConfigMgr) from Microsoft or IBM Tivoli.

Post-Installation

After installing the Agent, perform the following tasks, in order.

1. Register the Agent in RSA Authentication Manager.
   - If you installed the Auto-Registration utility, the Agent is automatically registered during installation.
   - If you did not install the Auto-Registration utility, manually register the Agent as an agent host in RSA Authentication Manager. For more information, see "Register the Agent in RSA Authentication Manager" on page 23.
2. Perform a test authentication to verify the connection to Authentication Manager and generate a node secret, if one does not already exist. For more information, see "Perform a Test Authentication" on page 24.

   Note: You can optionally establish the node secret using the Node Secret Load utility. For more information, see "Use the Node Secret Load Utility" on page 30. You can optionally verify the connection to Authentication Manager from RSA Control Center. (Open Control Center and click **Server Environment**.)

3. Configure Citrix StoreFront to use the **RSA SecurID** authentication method. For more information, see "Install or Uninstall the RSA SecurID Authentication Method for a Store" on page 32.

Register the Agent in RSA Authentication Manager

After you install Agent for Citrix StoreFront, you must register it with RSA Authentication Manager. Use the following instructions to manually register the Agent.

Note: If you installed the Auto-Registration utility, you can skip this section.

Before You Begin

Know the following information:

- Host name
- IP addresses for network interfaces

Note: If you are using Agent for Citrix StoreFront with a Citrix StoreFront server group, register a load-balanced StoreFront server group as a single RSA SecurID agent on Authentication Manager, using the load balancer's IP address and host name. Register each StoreFront server's IP address as an alternate IP address for the Agent.

Procedure

1. Log on to the RSA Authentication Manager Security Console.
2. Click **Access > Authentication Agents > Add New**.
3. Enter the required information. Make sure the Agent Type is set to **Standard Agent** (default setting).

   Authentication Manager uses this setting to determine how to communicate with Citrix StoreFront.
4. Click **Save**.

Create the Agent Node Secret

If you are using Agent for Citrix StoreFront with a Citrix StoreFront server group, the node secret must be the same for all Agents in the group. Use the Node Secret Load Utility to download the node secret from Authentication Manager and install it on each StoreFront server in the group. For more information, see "Use the Node Secret Load Utility" on page 30.

Perform a Test Authentication

To verify that the Agent can authenticate successfully, run a test authentication. A test authentication sends a user name and SecurID passcode to the configured RSA Authentication Manager server. A test authentication also generates a node secret, if one does not already exist, and downloads it to the agent host.

Before You Begin

The Agent for Citrix StoreFront must have a network connection to Authentication Manager.

Procedure

1. Open RSA Control Center.
2. Under **SecurID Settings**, click **Advanced Tools**.
3. Click **Test Authentication**.
4. In the **Choose authenticator** field, leave the default setting **Handheld token**.
5. In the **User Name** field, leave the current user name or change it to the appropriate name.
6. In the **SecurID Passcode** field, do one of the following:
   - If you use a hand-held authenticator or software token and have not set a SecurID PIN, enter the current tokencode. Click **OK**. The Set New RSA SecurID PIN dialog box opens. Go to step 7.

- If you use a hand-held authenticator or a software token that has a SecurID PIN, enter the passcode. Click **OK**. Go to step 9, if necessary.
- If you use a static passcode, enter the passcode and click **OK**. If you have not set a SecurID PIN, the Set New RSA SecurID PIN dialog box appears. Go to step 7.

7. To set a PIN, follow the instructions in the Set New RSA SecurID PIN dialog box.
   - If prompted to receive a system-generated PIN, click **Next**. When you are ready to memorize the PIN, click **Finish**. Memorize the PIN.
   - If prompted to create your PIN, enter a PIN in the **SecurID PIN** field. Re-enter the same PIN in the **Confirm SecurID PIN** field. Click **Finish**.
8. If you use a hand-held authenticator or software token, after your PIN is set, enter the PIN followed by the tokencode in the **Next passcode** field.

   If the authenticator has a PIN entry field, enter the PIN into the device to generate a passcode. Enter the passcode and click **OK**.

   If you use a static passcode, enter the static passcode in the **Next passcode** field and click **OK**.
9. If you are prompted to enter the next tokencode to confirm your possession of the authenticator and synchronize it with RSA Authentication Manager, wait for the tokencode to change on your authenticator. Enter the new tokencode in the **Next** Add a StoreFront server to an existing StoreFront server group that is already configured to use RSA SecurID authentication.**tokencode** field and click **OK**.

If you cannot authenticate, review your Authentication Manager settings on the Server Environment page in the RSA Control Center.

Modify an Installation

Modifying the Agent installation allows you to add or remove the RSA Authentication Agent Auto-Registration utility. You can either use the Install Wizard or use command-line options.

Prerequisites

Before modifying the installation, perform the following tasks:

- Copy **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to deploy the product.
- (Optional) If you want to add the Auto-Registration utility, copy the **server.cer** file to the folder that contains the MSI file. During the modification, the installation program collects this file from the folder from which it is run.
- (Optional) Create a script to push the command-line installation to all Citrix StoreFront servers in the server group.

Modify the Installation Using the Install Wizard

Run the Install Wizard individually on each server in your Citrix StoreFront server group.

Procedure

1. In the folder where you copied the package file, double-click **RSA Authentication Agent for Citrix StoreFront x64.msi** to run the installer.
2. Click **Next**.
3. Select **Modify**, then click **Next**.
4. From the **Agent Host Auto-Registration Utility** drop-down list, select one of the following options:
   - **Will be installed on local hard drive**
   - **Entire feature will be installed on local hard drive**
   - **Entire feature will be unavailable**
5. Click **Next**.
6. To add the Auto-Registration utility, click **Browse** to locate and open the **server.cer** file you want to use.
7. Click **Next**.
8. Click **Install**.
9. Click **Finish** to exit the wizard.

Modify the Installation Using the Command Line

Run the command-line command on each Citrix StoreFront server individually, or execute the command on multiple servers using a script or third-party product, such as Microsoft System Center Configuration Manager (ConfigMgr) or IBM Tivoli.

Before You Begin

Know how to install software using the msiexec command-line. For more information on msiexec commands, visit **http://technet.microsoft.com**.

Procedure

1. Open a command prompt, and do one of the following:
   - To add the Auto-Registration utility, use a case-sensitive msiexec command similar to the following example:

     ```
     msiexec /qn /i "RSA Authentication Agent for Citrix
     StoreFront x64.msi" REINSTALLMODE=vomus
     ADDLOCAL=AgentAutoRegistration
     ```

   - To remove the Auto-Registration utility, use a case-sensitive msiexec command similar to the following example:

     ```
     msiexec /qn /i "RSA Authentication Agent for Citrix
     StoreFront x64.msi" REINSTALLMODE=vomus
     ```

```
REMOVE=AgentAutoRegistration
```

In the previous examples, the `/qn` switch instructs the installer to run in silent mode, suppressing all UI elements.

2. (Optional) To modify the installation for multiple Citrix StoreFront servers, execute the command on the servers using a script or a third-party product, such as System Center Configuration Manager (ConfigMgr) from Microsoft or IBM Tivoli.

Repair an Installation

You can repair the Agent for Citrix StoreFront installation either by using the Install Wizard, which guides you through the modification process, or by using command-line options.

Repairing an installation replaces missing files in a damaged installation.

Prerequisites

Before repairing the installation, copy **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to deploy the product.

Repair the Installation Using the Install Wizard

Procedure

1. In the folder where you copied the package file, double-click **RSA Authentication Agent for Citrix StoreFront x64.msi** to run the installer.
2. Click **Next**.
3. Select **Repair**, then click **Next**.
4. Click **Repair**.
5. Click **Finish** to exit the wizard.

Repair the Installation From the Command Line

Procedure

1. Open a command prompt.
2. Navigate to the directory that contains the **RSA Authentication Agent for Citrix StoreFront x64.msi** package file. Otherwise, provide the full pathname to the package file on the command-line.
3. Enter a command similar to the following example:

   ```
   msiexec /qn /fvomus "RSA Authentication Agent for Citrix StoreFront x64.msi"
   ```

   In the previous example, the `/qn` switch instructs the installer to run in silent mode, suppressing all UI elements.

Uninstall the Agent

You can uninstall Agent for Citrix StoreFront either by using the Windows Control Panel, or by running the installation program from the command-line. To uninstall the product from multiple servers, you must use the command-line.

Prerequisites

Before uninstalling, perform the following tasks:

- If you have configured Delegated Forms Authentication (DFA) to use RSA SecurID authentication, set DFA authentication back to the default Citrix **Username and password** method. See "Enable RSA SecurID Authentication for DFA" on page 38.
- Remove the RSA SecurID authentication method. See "Install or Uninstall the RSA SecurID Authentication Method for a Store" on page 32.
- Close the Citrix StoreFront management console.

Uninstall Using Windows Control Panel

Procedure

1. From the Start menu, click **Control Panel > Programs > Programs and Features**.
2. In the program list, click **RSA Authentication Agent for Citrix StoreFront**.
3. Click **Uninstall**.
4. Restart the server if prompted. If you cancel the uninstall process at any time, the application reverts to its previous state.

Uninstall Using the Command Line

Procedure

1. Copy **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to uninstall the product.
2. Open a command prompt.
3. 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.

   ```
   msiexec /qn /x "RSA Authentication Agent for Citrix StoreFront x64.msi" /lv uninstall.log
   ```

   In the previous example, the `/qn` switch instructs the installer to run in silent mode, suppressing all UI elements. To log any removal errors, use the `/lv` (log verbose) option. Store the log file, for example, uninstall.log, in a known location such as %USERPROFILE%.
4. (Optional) To uninstall the product from multiple servers, execute the command on the servers using a script or a third-party product, such as System Center Configuration Manager (ConfigMgr) from Microsoft or IBM Tivoli.

4 Configuring and Managing the Agent for Citrix StoreFront

The Agent for Citrix StoreFront leverages the following features of the Citrix StoreFront **User name and password** authentication method.

- Configure trusted domains from which users can log on and optionally include the domain list in a drop down menu on the passcode dialog.
- Set whether and when users can change their passwords.

Note: If you add a StoreFront server that has Citrix StoreFront and the Agent installed to an existing server group, the authorizing StoreFront in the group propagates the server configuration, including RSA SecurID settings, to the new StoreFront server.

For instructions on using these Citrix StoreFront features, see the Citrix documentation at **http://docs.citrix.com**

Exclude Specific Network Adapters from Auto-Registration

To reduce network traffic and maximize performance, you can configure the Auto-Registration utility to exclude specific network adapters from automatic IP address registration. For example, you can specify that changes to the IP addresses of devices such as VMware hosts or wireless routers do not trigger automatic registration.

The Auto-Registration utility ignores changes to the IP addresses of devices named in the ExcludeAdapters string value list.

Procedure

1. Log on to the Citrix StoreFront server hosting Agent for Citrix StoreFront.
2. Click **Start** > **Apps** > **Run**.
3. In the **Open** field, type **regedit** and click **OK**.
4. Navigate to **HKLM\ SOFTWARE\RSA\RSA Authentication Agent\AgentAutoRegistration**.
5. Right-click **AgentAutoRegistration**, and select **New > String Value**.
6. For the new string value name, enter **ExcludeAdapters**.
7. In the right pane of the Registry Editor window, right-click **ExcludeAdapters**, and click **Modify**.

8. Enter data values for each network adapter you want the Auto-Registration utility to exclude from monitoring.

   The data values are case-sensitive. Use semicolons to separate the values for each adapter. For example, if you enter VPN;VMware, all adapters whose names include VPN and all adapters whose names include VMware are excluded from Auto-Registration.

Maintain the Primary IP Address of the Agent

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

If you install and enable the RSA Authentication Agent Auto-Registration utility for an Agent, the Agent's primary IP address is automatically entered in the Authentication Manager agent record, and is automatically updated whenever it changes.

If your Authentication Manager environment is not configured to automatically register Agents, the Authentication Manager administrator must manually record the Agent's primary and secondary IP addresses in Authentication Manager. If an Agent's address changes, the administrator must update the Authentication Manager agent record accordingly.

If Agents are registered manually, the Authentication Manager administrator must ensure that the primary IP address in the Authentication Manager agent record matches the primary IP address specified in RSA Control Center (and in the load balancing options file **sdopts.rec,** if you are using automatic load balancing as described in Appendix A, "Configuring Automatic Load Balancing" on page 53). If the addresses do not match, communication between the Agent and Authentication Manager fails. If secondary IP addresses are specified for the Agent, these addresses must also be entered in the agent record, and all addresses must be updated if they change.

For more information, see "Enable an IP Address Override" on page 34.

Use the Node Secret Load Utility

Each Agent is associated with a unique node secret. The node secret allows the Agent and the RSA Authentication Manager server to use encrypted communications during the SecurID authentication process. If not previously established, Authentication Manager creates the node secret and downloads it to the agent host the first time a user successfully authenticates with a SecurID passcode.

Note: You must use the Node Secret Load utility when installing the Agent on a Citrix StoreFront server group.

You can create a node secret in RSA Authentication Manager and manually load it onto the agent host before users start authenticating with RSA SecurID.

The procedure to generate the node secret is described in the *RSA Authentication Manager Administrator's Guide* and RSA Security Console Help.

Procedure

1. Deliver the node secret from RSA Authentication Manager using a secure method.
2. Deliver the password with which the node secret was encrypted, separately, using a secure method.
3. Copy the node secret file and the **agent_nsload.exe** utility to the **C:\Program Files\Common Files\RSA Shared\Auth API** directory on the agent host.
4. Open a command prompt and navigate to the **C:\Program Files\Common Files\RSA Shared\Auth API** directory.
5. Run the utility using the following command syntax:

   `agent_nsload -f path -d "..\Auth Data"`

   where:

   The *path* argument is the directory location and name of the node secret file.

   `-d` (destination) is followed by the destination file path where you want to store the node secret. Enclose the file path in quotations.
6. When prompted, enter the password with which the node secret file was encrypted. The Node Secret Load utility loads the new node secret file onto the agent host.
7. Repeat this procedure for each Agent that requires extra encryption protection during the first RSA SecurID authentication.

See also: "Clear the Node Secret" on page 35.

Note: For a load-balanced StoreFront server group, download the node secret from Authentication Manager and install it on each StoreFront server in the group. The same node secret will also work for Authentication Agent for Windows if it is installed on the StoreFront servers.

Manage RSA SecurID Authentication Using the Citrix StoreFront Management Console

You use the Citrix StoreFront Management Console (MMC) to perform the following tasks:

- "Install or Uninstall the RSA SecurID Authentication Method for a Store" on page 32.
- "Add or Remove a StoreFront Server in a Server Group Configured to Use the RSA SecurID Authentication Method" on page 33.
- "Enable or Disable RSA SecurID Authentication" on page 33.

- "Manage the RSA SecurID Authentication Send Domain Option" on page 33.

Note: For a load-balanced StoreFront server group, configure RSA SecurID authentication settings on one StoreFront and then propagate them to the server group.

Install or Uninstall the RSA SecurID Authentication Method for a Store

Before You Begin

You must install the RSA SecurID authentication method for each store that you want to protect with RSA SecurID.

Procedure

1. Open the Citrix StoreFront management console.
2. Select **Stores** in the **Console tree**.
3. In the **Stores list**, select the store for which you want to install or uninstall the RSA SecurID authentication method.
4. Click **Manage Authentication Methods** in the **Action pane**.
5. From the Advanced drop-down menu, click **Install or uninstall authentication methods**.
6. Do one of the following:
   - To install the authentication method, check the box for **RSA SecurID**.
   - To uninstall the authentication method, clear the box for **RSA SecurID**.
7. Click **OK** to close the **Install or Uninstall Authentication Methods** dialog box.
8. Click **OK** to close the close the **Manage Authentication Methods** dialog box.
9. (Optional) To propagate the changes to members of a StoreFront Server Group:
   a. Select **Server Group** in the **Console tree**.
   b. Use the **Propagate Changes** action to propagate the settings to the members of the server group.

Note: The Agent for Citrix StoreFront must be installed on all members of the server group.

Add or Remove a StoreFront Server in a Server Group Configured to Use the RSA SecurID Authentication Method

Before You Begin

Agent for Citrix StoreFront must be installed on the StoreFront server that you are adding to the group.

Procedure

1. Open the Citrix StoreFront management console on one of the StoreFront servers in the server group.
2. Select **Server Group** in the console tree and use the **Add Server** action to add the new server to the StoreFront server group.
3. Use the **Propagate Changes** action to propagate the server configuration, including RSA SecurID authentication settings to the new server.

Enable or Disable RSA SecurID Authentication

Before You Begin

RSA SecurID must appear in the Citrix StoreFront management console list of available authentication methods.

Procedure

1. Open the Citrix StoreFront management console.
2. Select **Stores** in the **Console tree**.
3. In the **Stores list**, select the store for which you want to enable or disable RSA SecurID authentication.
4. Click **Manage Authentication Methods** in the **Action pane**.
5. Do one of the following:
   - To enable the method, check the box for RSA SecurID.
   - To disable the method, clear the box for RSA SecurID.
6. Click **OK**.

Manage the RSA SecurID Authentication Send Domain Option

When RSA SecurID authentication is enabled, you can enable or disable the option **Send domain and user name to Authentication Manager**.

Enable this option if you created the user account in RSA Authentication Manager with a domain name and user name (*domain_name\user_name*).

Note: The Agent does not support RSA Authentication Manager user accounts in UPN format (*user_name@domain_name*).

Procedure

1. Open the Citrix StoreFront management console.
2. Select **Stores** in the **Console tree**.
3. In the **Stores list**, select the store for which you want to manage the Send Domain option.
4. Click **Manage Authentication Methods** in the **Action pane**.
5. Select **Manage SecurID Options** from the drop-down menu in the **Settings** column for RSA SecurID.
6. Check (to enable) or clear (to disable) the checkbox **Send domain and user name to Authentication Manager**.
7. Click **OK**.

Configure the Agent for Citrix StoreFront Using the RSA Control Center

You use the RSA Control Center to perform the following tasks:

- "Enable an IP Address Override" on page 34.
- "Clear the Node Secret" on page 35.

Enable an IP Address Override

On a Citrix StoreFront server that has multiple network interface cards and multiple IP addresses, if you plan to use different addresses to connect to RSA Authentication Manager from the agent host at different times, you must:

- Register one IP address as the primary in RSA Authentication Manager and designate it as the IP address override in RSA Control Center.
- Register the other IP addresses belonging to the agent host as secondary addresses in RSA Authentication Manager.

For information about registering IP addresses in RSA Authentication Manager, see the RSA Authentication Manager documentation.

Procedure

1. On the Citrix StoreFront server, open the RSA Control Center.
2. Under **SecurID Settings**, click **Advanced Tools**.
3. Click **IP Address Override**.
4. In the **IP Address Override** field, enter the IP address that is designated as the primary address in RSA Authentication Manager.
5. Click **OK**.

Clear the Node Secret

If the Agent's node secret does not match the node secret on RSA Authentication Manager, encrypted communications between the Agent and RSA Authentication Manager cannot occur. If this happens, you must clear the node secret on the Agent and on RSA Authentication Manager.

If the RSA Authentication Agent Auto-Registration service is installed, and RSA Authentication Manager is configured to allow Agents to auto-register, there is typically no need to clear the node secret on the Agent. However, a node secret mismatch can occur in specific situations. For example, if an RSA Authentication Manager administrator uses the Security Console to unregister an instance of Agent for Citrix StoreFront in RSA Authentication Manager, the node secret will become mismatched, and you will need to clear the node secret.

Procedure

1. On the Citrix StoreFront server, open the RSA Control Center.
2. Under **SecurID Settings**, click **Advanced Tools**.
3. Click **Clear Node Secret**.
4. Click **Yes**.
5. If the Auto-Registration service is disabled or not installed, clear the node secret for this Agent from Authentication Manager. For instructions, see the RSA Authentication Manager Security Console Help.

5 Citrix Delegated Forms Authentication

The Citrix Delegated Forms Authentication (DFA) protocol enables StoreFront to provide authentication services to NetScaler Gateway. DFA is a prerequisite for extending the Agent for Citrix StoreFront to authenticate users with either RSA SecurID or RBA.

Complete these high-level steps to enable DFA for Citrix StoreFront to provide RSA SecurID authentication services to Citrix NetScaler gateway.

1. Protect logon to StoreFront with RSA SecurID authentication using the RSA Agent for StoreFront. See Chapter 4, "Configuring and Managing the Agent for Citrix StoreFront" on page 29.
2. Enable DFA on Citrix StoreFront and protect DFA with RSA SecurID, as described in "Enable RSA SecurID Authentication for DFA" on page 38.
3. Configure NetScaler Gateway to use DFA to authenticate to Citrix StoreFront. Refer to the DFA configuration steps described in the RSA Ready Technology Integrations "RBA Implementation Guide" on RSA Link at **https://community.rsa.com/docs/DOC-66800**.
4. Configure StoreFront to provide remote access through NetScaler Gateway. For guidance on configuring DFA on NetScaler Gateway, see the Citrix documentation website at **http://docs.citrix.com** and search on "Configure NetScaler Gateway connection settings".

Note: If you configure DFA on a StoreFront server in a StoreFront server group, you must propagate changes to all servers in the group.

Note: If you set the optional `-tenantID` parameter when running the `Install-DFAServer` command, then you must include that tenantID in the `-VirtualPath` used in all of the commands in this chapter, as follows:

`-VirtualPath /Citrix/DelegatedForms/<tenantID>/Default`

These PowerShell commands are also described in the *Configuring Citrix StoreFront for Delegated Forms Authentication with RSA SecurID* document. You can access this document through the Citrix StoreFront Management Console, or download the latest version from RSA Link.

Enable RSA SecurID Authentication for DFA

Before You Begin

Install and configure the DFA server on Citrix StoreFront. Follow the instructions in the *StoreFront Services Delegated Forms Server Management ReadMe* document provided by Citrix at **<Citrix StoreFront installation directory>\Management\Cmdlets\DFAServerFPReadMe.rtf**.

Procedure

1. Open a PowerShell command window and load the Citrix StoreFront modules using the **ImportModules.ps1** script provided by Citrix, as described in the *StoreFront Services Delegated Forms Server Management ReadMe.*
2. Enter the following command to add the Custom Forms protocol to DFA:

   ```
   Add-STFAuthenticationServiceProtocol -Name CustomForms
   -AuthenticationService (Get-STFAuthenticationService
   -VirtualPath /Citrix/DelegatedForms/Default)
   ```

3. Enter the following command to protect DFA with RSA SecurID authentication:

   ```
   Set-DSDFAProperty -conversationfactory SecurIDAuthentication
   ```

4. (Optional) Enter the following command to configure Trusted Domains for DFA:

   ```
   Set-STFExplicitCommonOptions -authenticationservice
   (Get-STFAuthenticationService -VirtualPath
   /Citrix/DelegatedForms/Default) -Domains @("domain1”,
   “domain2") -DefaultDomain "domain1"
   ```

Disable RSA SecurID Authentication for DFA

Procedure

1. Open a PowerShell command window and load the Citrix StoreFront modules using the **ImportModules.ps1** script provided by Citrix, as described in the *StoreFront Services Delegated Forms Server Management ReadMe.*
2. Enter the following command to reset DFA protection to default Citrix username and password authentication:

   ```
   Set-DSDFAProperty -conversationfactory
   ExplicitAuthentication
   ```

3. Enter the following command to remove the Custom Forms protocol from DFA:

   ```
   Remove-STFAuthenticationServiceProtocol -Name CustomForms
   -AuthenticationService (Get-STFAuthenticationService
   -VirtualPath /Citrix/DelegatedForms/Default)
   ```

4. (Optional) Enter the following command to clear the Trusted Domains for DFA:

```
Set-STFExplicitCommonOptions -authenticationservice
(Get-STFAuthenticationService -VirtualPath
/Citrix/DelegatedForms/Default) Domains @() -DefaultDomain
""
```

Note: You must disable RSA SecurID authentication for DFA before you can uninstall the RSA Authentication Agent for Citrix Storefront.

6 Enabling RSA Authentication Manager Risk-Based Authentication

RSA Authentication Manager provides an implementation of Risk-Based Authentication (RBA) that you can use to protect logon to Citrix StoreFront by users who authenticate through NetScaler Gateway. When enabled, users who authenticate using RBA are logged on through StoreFront and are not required to enter credentials a second time.

Enabling RBA to protect StoreFront involves the following steps:

1. Protect logon to StoreFront with RSA SecurID authentication using the RSA Agent for StoreFront. See Chapter 4, "Configuring and Managing the Agent for Citrix StoreFront" on page 29.
2. Enable Citrix Delegated Forms Authentication (DFA) to extend RSA SecurID authentication through NetScaler Gateway. See Chapter 5, "Citrix Delegated Forms Authentication" on page 37.
3. Install the RSA Risk-Based Authentication Helper web application to provide a connection point between RBA authentication and the RSA Agent for StoreFront. See "Install the RBA Helper" on page 42.
4. Integrate RSA Authentication Manager and NetScaler Gateway with the RSA Agent for StoreFront. See "Integrate Authentication Manager RBA with Citrix NetScaler and RSA Authentication Agent for Citrix StoreFront" on page 44.

RSA Authentication Manager Risk-Based Authentication Helper

The RSA Authentication Manager Risk-Based Authentication Helper (RBA Helper) is a web application that connects the RSA Authentication Manager implementation of RBA and the Agent for Citrix StoreFront. The RBA Helper installer is available as part of RSA Authentication Agent for Citrix StoreFront.

The RBA Helper does the following:

- Provides a form to which Authentication Manager can post the output from a successful RBA authentication.
- Redirects the authentication to a NetScaler virtual server that invokes DFA to Citrix StoreFront.

Install the RBA Helper

To install the RBA Helper, you can either use the Install Wizard, which guides you through the installation process, or run the installation program from the command line.

Before You Begin

You must have administrator rights for the server on which you are installing the RBA Helper.

Verify that the server on which you are installing the RBA Helper meets the following requirements:

- .NET Framework 4.5 or later
  - ASP.NET 4.5 enabled
- Internet Information Services (IIS)
  - Version 7.5, 8.0, 8.5, or 10.0
  - Web Server role with ASP.NET 4.5 enabled
  - HTTPS enabled

Copy the installer (**RSA Authentication Manager Risk-Based Authentication Helper x64.msi)** to a folder on the system.

Note: The Install Wizard installs the RBA Helper to the default web site. To install the RBA Helper to a different web site, install the RBA Helper using the command line.

Security Considerations

The RBA Helper must be accessed through HTTPS in order to integrate Authentication Manager RBA with the Agent for Citrix StoreFront, and to protect user RBA credentials in transit. RSA recommends that you configure Microsoft Internet Information Services (IIS), which hosts the RBA Helper, to use HTTPS and configure the Microsoft TLS/SSL Security Provider (used by IIS) to use Transport Layer Security (TLS) v1.2 or later.

For information on configuring IIS to use HTTPS, see the Microsoft IIS documentation website at **http://www.iis.net**. Search on *TLS/SSL*.

For information on configuring the Microsoft TLS/SSL Security Provider to use TLS v1.2, see the Microsoft documentation at **http://support.microsoft.com**. Search on *How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll*.

For guidance on configuring TLS, refer to the National Institute of Standards and Technology publications on Computer Security at **http://csrc.nist.gov/publications/PubsSPs.html**. Search on *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

Install Using the Install Wizard

Procedure

1. In the folder where you copied the installer file, double-click **RSA Authentication Manager Risk-Based Authentication Helper x64.msi** to start the installation wizard.
2. Click **Next** to continue.
3. Read the License Agreement or click **Print** to print it. Select **I accept the terms in the license agreement** and click **Next**.
4. Click **Install**.
5. When installation completes, click **Finish**.

Install Using Command-Line Options

Procedure

1. Open an administrator command prompt.
2. Navigate to the folder where you copied the installer file. Otherwise, provide the full pathname to the installer file on the command line.
3. Do one of the following:
   - To install RBA Helper to the default web site, use a command similar to the following:

     ```
     msiexec /qn /i "RSA Authentication Manager Risk-Based
     Authentication Helper x64.msi"
     ```

   - To install RBA Helper to a different web site, use a command similar to the following:

     ```
     msiexec /qn /i "RSA Authentication Manager Risk-Based
     Authentication Helper x64.msi"
     PARENT_WEBSITE="<Non-default web site>"
     ```

Note: The RBA Helper installer does not create a web site if the named web site does not exist. In that case, the installer installs the RBA Helper to the default web site.

Post-Installation

Before You Begin

Verify that the RBA Helper web application is running.

Procedure

1. Open Internet Information Services (IIS) Manager.
2. In the Connections Pane, open **Sites > Default Web Site** (or the web site to which the RBA Helper has been installed).
3. Verify that the RBA Helper has been installed as a web application.
   a. Right-click **RSAAuthMgrRbaHelper**.
   b. Confirm that **Manage Application** appears as an option in the context menu.

Integrate Authentication Manager RBA with Citrix NetScaler and RSA Authentication Agent for Citrix StoreFront

Refer to the RBA configuration steps described in the *RBA Implementation Guide*, available on RSA Link at **https://community.rsa.com/docs/DOC-66800**.

7 Troubleshooting

This chapter provides troubleshooting information and provides details about error messages. For additional troubleshooting information, log on to RSA Link at **https://community.rsa.com**. RSA SecurCare Online is available to customers who have a valid software service contract.

Installation and Uninstallation Issues

If the installation or uninstallatoin does not succeed, examine the log file to determine what issue might have caused the failure. If you are using an interactive installation, the installer halts and an error appears.

Problem	Resolution
Citrix StoreFront is not installed on the system.	Contact Citrix to download and install Citrix StoreFront. Restart the installation program.
Microsoft .NET Framework 4.5 or later is not installed on the system.	Contact Microsoft to download and install .NET Framework 4.5. Restart the installation program.
Installation fails when you select to install the Auto-Registration Utility with RSA Authentication Agent for Citrix StoreFront, and it is already installed with RSA Authentication Agent for Windows.	The Auto-Registration Utility can only be installed by one Authentication Agent. Do not select the Auto-Registration Utility if it is already installed with RSA Authentication Agent for Windows. Restart the installation program.
The Citrix StoreFront Agent cannot be uninstalled if Citrix StoreFront has already been uninstalled.	Reinstall Citrix StoreFront and close the Citrix StoreFront MMC (which opens automatically). Uninstall the Agent for Citrix StoreFront and then uninstall Citrix StoreFront.

Coexistence with the RSA Authentication Agent for Windows Issues

This section describes issues that might occur when the RSA Authentication Agent for Windows (Windows Agent) and the RSA Authentication Agent for Citrix StoreFront (Citrix Agent) are both installed on a Citrix StoreFront server.

Problem	Resolution
The Offline Authentication feature of the Windows Agent is unavailable when both Agents are installed.	The Agent for Citrix StoreFront disables the download of offline data. To re-enable this function, follow these steps: **Procedure** 1. Open the Registry Editor: Click **Start**. Type **regedit** in the search box, and click **regedit** in the results list under Programs. 2. Open the key: **HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT** 3. Change the value of **NoDADownload** (a REG_DWORD) from **1** to **0**.
The version of RSA Control Center installed by the Windows Agent supersedes the version of RSA Control Center installed by the Agent for Citrix StoreFront.	This is intended behavior. The Windows Agent RSA Control Center contains all of the features and Help topics from both Agents.
Citrix Agent Help is unavailable from the RSA Control Center when the Windows Agent is installed to a custom location after the Citrix Agent is installed.	RSA Control Center cannot locate the Help files that the Citrix Agent installs. To place a copy of the Help files for the Citrix Agent in the location that the Windows Agent expects, follow these steps. **Procedure** 1. Locate the directory containing the Windows Agent Help. For example, if you installed the Windows Agent to C:\Program Files\RSA2\RSA Authentication Agent, the Help files will be in a directory named C:\Program Files\RSA2\RSA Authentication Agent\Help. 2. Navigate to the directory containing the Citrix Agent Help files: C:\Program Files\RSA\RSA Authentication Agent\Help\Citrix. 3. Copy the Citrix directory to the directory identified in step 1. For example, copy C:\Program Files\RSA\RSA Authentication Agent\Help\Citrix to C:\Program Files\RSA2\RSA Authentication Agent\Help. **Note:** When you uninstall the Citrix Agent, you will need to manually delete the copy of the Citrix Agent Help files.

Authentication Issues

This section describes tasks to help you diagnose authentication issues.

Enable Tracing

You can enable tracing from RSA Control Center to diagnose authentication issues. Typically, you only enable trace logging when instructed to do so by RSA Customer Support. Customer Support will also tell you 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**. The location where log files are saved is configurable in the Tracing section in RSA Control Center.

Procedure

1. On the agent host where authentication issues are occurring, open RSA Control Center.
2. Click **Advanced Tools**.
3. Click **Tracing**.
4. As directed by Customer Support, configure the tracing settings.
5. Click **OK**.

Verify the RSA Authentication Manager Configuration File (sdconf.rec)

If the agent hosts and the RSA Authentication Manager server do not have compatible copies of the system configuration file (**sdconf.rec**), the servers 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.

Procedure

1. Open the RSA Control Center.
2. Click **Advanced Tools > 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 the error message, "Unable to retrieve server environment," the system configuration (**sdconf.rec**) file is corrupt. You must replace the **sdconf.rec** file.

   For more information about replacing the **sdconf.rec** file, see "Replace the RSA Authentication Manager Configuration File (sdconf.rec)" on page 48.

Replace the RSA Authentication Manager Configuration File (sdconf.rec)

Follow these steps to replace a corrupt **sdconf.rec** file.

Procedure

1. Obtain a new **sdconf.rec** file from RSA Authentication Manager.
2. Navigate to the **C:\Program Files\Common Files\RSA Shared\Auth Data** directory, where the existing **sdconf.rec** file is stored on the agent host.
3. Replace the existing **sdconf.rec** file with the new file.

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

Replace the RSA Authentication Manager Server Certificate File (server.cer)

Follow these steps to replace a corrupt **server.cer** file.

Procedure

1. Obtain a new **server.cer** file from RSA Authentication Manager.
2. Open **Administrative Tools > Services** and stop the **RSA Authentication Agent Auto-Registration** service.
3. Navigate to the directory C:\Program Files\RSA\RSA Authentication Agent\Agenthost Autoreg Utility\, where the existing **server.cer** file is stored.
4. Replace the existing **server.cer** file with the new file.
5. Start the **RSA Authentication Agent Auto-Registration** service.

RSA Authentication Manager Risk-Based Authentication Helper Issues

This section describes tasks that you can perform to diagnose issues that you might encounter when supporting integration with Authentication Manager Risk-Based Authentication (RBA).

Enable Tracing

You can enable tracing from RSA Control Center to diagnose issues with the RSAAuthMgrRbaHelper web application. 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

Procedure

1. On the agent host where authentication issues are occurring, open RSA Control Center.
2. Click **Advanced Tools**.

3. Click **Tracing**.
4. As directed by Customer Support, configure the tracing settings.
5. Click **OK**.

Note: When enabled, the tracing output files are written to C:\ProgramData\RSA\Logfiles. The location where log files are saved is configurable in the Tracing section in RSA Control Center.

Enable Display of the RSAAuthMgrRbaHelper Form

By default, RSAAuthMgrRbaHelper does not display the form used to support integration with RBA. You can enable RSAAuthMgrRbaHelper to display the form if instructed to do so by RSA Customer Support.

Procedure

1. Open Internet Information Services (IIS) Manager.
2. In the Connections Pane, open **Sites > Default Web Site**, or the web site where RSAAuthMgrRbaHelper is installed.
3. Select **RSAAuthMgrRbaHelper**.
4. In the Actions pane, select **Explore**.
5. From the Explorer window that opens, use a text editor to open the **web.config** file.
6. Find the `<add key="allowHttpGet" value="false"/>` attribute under the `<appSettings>` element.
7. Change the value from **false** to **true**.
8. Save the **web.config** file.
9. To verify that the form can be displayed, select **Browse*:80 (http)** or **Browse*:443 (https)** in the Actions pane. Internet Explorer displays the RBA Helper form.

   Note: If you select **Browse*:443 (https)**, a certificate warning might appear because IIS Manager uses a server name of **localhost**, which is unlikely to match the server attribute in the SSL certificate. You can ignore this warning.

Error and Event Viewer Log Messages

The Agent for Citrix StoreFront writes error and event messages to the Windows Event Viewer in the following categories:

- ACECLIENT
- AuthAPIService
- RSA Agent Auto Registration
- RSA Authentication Agent Auto-Registration
- RSA Control Center
- RSA SecurID Authenticator

Message	Description
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 "Create an sdopts.rec File" on page 54.
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 "Create an sdopts.rec File" on page 54.
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 "Create an sdopts.rec File" on page 54.
Incorrect size for file: sdconf.rec	The **sdconf.rec** file was probably not copied in binary mode. Ask the RSA Authentication Manager administrator for a new copy of **sdconf.rec**.
File not found: aceclnt.dll	Software might have been installed incorrectly or **aceclnt.dll** deleted. Reinstall the Citrix Agent software from the MSI file (**RSA Authentication Agent for Citrix StoreFront x64.msi**).
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 RSA Authentication Manager. Ask your RSA Authentication Manager administrator for a new copy of **sdconf.rec**.
Network Timeout - RSA Authentication Manager was responding but has now stopped.	Make sure the RSA Authentication Manager process is running on the server. Check for a network problem such as a router malfunction or an unplugged network cable.
User <*user name*> canceled out of New PIN routine	The user canceled the authentication attempt in New PIN mode.

Message	Description
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 RSA 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.	The identity of the RSA 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 RSA Authentication Manager. The user needs to reauthenticate to set the RSA SecurID PIN. Check the RSA Authentication Manager Activity Log.
User <*user name*>: PASSCODE accepted	The user's passcode was accepted.
User <*user name*>: Successfully logged on with Next Tokencode	RSA 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 "Create an sdopts.rec File" on page 54.

A Configuring Automatic Load Balancing

Automatic Load Balancing

This appendix explains how to configure RSA Authentication Agent for Citrix StoreFront 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 agent host. Within the file, you can specify dynamic or manual load balancing.

Important: You must log on to the agent host with an administrator account to modify the **sdopts.rec** file.

Dynamic Load Balancing

With dynamic load balancing, Agent for Citrix StoreFront 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 server. The RSA Authentication Manager server with the fastest response time gets the highest priority and receives the greatest number of authentication requests. Other RSA Authentication Manager servers get lower priorities and fewer requests. This arrangement lasts until the Agent sends another time request or a connection times out.

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

You specify dynamic load balancing by excluding the **USESERVER** statement from the **sdopts.rec** file. For more information, see "Create an sdopts.rec File" on page 54.

Manual Load Balancing

For manual load balancing, you specify the RSA Authentication Manager servers that each agent host uses. You also assign a priority to each RSA Authentication Manager server so the Agent can direct authentication requests to some servers more frequently than others. You enable manual load balancing by including the **USESERVER** statement in the **sdopts.rec** file and associating priority settings with each RSA Authentication Manager server you specify for use. For more information, see "Create an sdopts.rec File" on page 54.

Create 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.

You create and edit an **sdopts.rec** file using any text editor. After you create the file, save it in the directory specified by the **AuthDataDir** registry 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 the AuthAPIService to register the changes.

You must enter keywords in uppercase. The file can include comment lines, each preceded by a semicolon, and keyword-value pairs, as follows.

- **CLIENT_IP=*ip_address***. Specifies an overriding IP address for the agent host. The **CLIENT_IP** keyword can appear only once in the file. For information, see "Specify an Overriding IP Address" on page 59. the Agent ignores this setting if an IP address override is already set through the Advanced Tools category in the RSA Control Center. For more information, see the the Agent Help.
- **USESERVER=*ip_address*, *priority***. Specifies an RSA Authentication Manager server IP address to receive authentication requests from the agent host according to a specified priority value. Use one IP address and priority setting for each RSA Authentication Manager server. The combined maximum number of RSA Authentication Manager servers you can specify in the **sdopts.rec** file 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 server IP address and the assigned priority value, separated by a comma. The priority value specifies if or how often an RSA Authentication Manager server receives authentication requests.

  You must assign a priority to each RSA Authentication Manager server 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 the Agent receives as part of its initial authentication.

The following table lists the priority values that you can specify.

Priority Value	Meaning
2–10	Send authentication requests to this RSA Authentication Manager server using a randomized selection based on the assigned priority of the server. The range is from 2–10. The higher the value, the more requests the server receives. A Priority 10 RSA Authentication Manager server receives about 24 times as many requests as a Priority 2 server.
1	Send authentication requests to this RSA Authentication Manager server only if no servers of higher priority are available.
0	Ignore this RSA Authentication Manager server. A Priority 0 server can only be used in these special circumstances: • It must be one of the RSA Authentication Manager servers listed in the **sdconf.rec** file. • It can only be used for the initial authentication of the Agent, unless all RSA Authentication Manager servers with priorities of 1–10 listed in the **sdopts.rec** file are unavailable to the Agent. Generally, a priority value of 0 allows you to put an entry in the file for an RSA Authentication Manager server without using that server. You can change the priority value if you decide to use the server later. If none of the servers with **USESERVER** statements are responsive, then the default server is the master (if one exists) or the RSA Authentication Manager server used to create the **sdconf.rec** file is the master.

- **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 RSA Authentication Manager server in addition to those listed 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 comma-separated aliases for that server. the Agent sends timed requests to the actual IP address 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 RSA Authentication Manager server list received by the Agent. The RSA Authentication Manager server list provides actual and alias IP address information about all known RSA Authentication Manager servers in the realm. the Agent receives the list from the RSA Authentication Manager server after RSA 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 the Agent to use only the alias IP addresses to contact RSA Authentication Manager.

  When you do not provide a value, this keyword tells RSA Authentication Manager to send requests only to the RSA Authentication Manager servers that have alias IP addresses assigned. You can create exceptions by including no more than 10 **IGNORE_ALIASES** keywords in the **sdopts.rec** file to specify which RSA 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 58.

  If you use this keyword, make sure that at least one RSA Authentication Manager server 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 server list, are ignored. You can create exceptions by including no more than 10 **ALIASES_ONLY** keywords in the **sdopts.rec** file to specify which RSA 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 58.

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

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

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 the Agent to exclude the server from use during dynamic load balancing.

If you use the **AVOID** statement with the IP address of the default RSA Authentication Manager server, the statement is ignored unless another server is available. The default RSA Authentication Manager server is the one where the **sdconf.rec** file was created. If an RSA Authentication Manager server is designated as the master, however, it becomes the default 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 them 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 RSA Authentication Manager server identified by IP address 192.168.10.23 receives more authentication requests than server 192.168.10.22. RSA Authentication Manager server 192.168.10.20 is used only if the servers of higher priority are unavailable. RSA Authentication Manager server 192.168.10.21 is ignored except in rare circumstances (as described in “Create an sdopts.rec File” on page 54).

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: the Agent ignores alias settings if the IP address override is already set through the Advanced Settings option in RSA Control Center. For more information on setting the IP address through Control Center, see "Enable an IP Address Override" on page 34.

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.

Note: 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 RSA Authentication Manager servers, and **ALIAS** keywords have no effect on which RSA Authentication Manager servers are specified for use.

```
;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 the example above, 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, while 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 list.

In the example above, 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 the Agent should send its requests to RSA Authentication Manager servers 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 the Agent should send its requests to RSA Authentication Manager servers 192.168.10.23 and 192.168.10.22 by using only their actual IP addresses.

Specify an Overriding IP Address

On a Citrix StoreFront server with multiple network interface cards and multiple IP addresses, you must specify a primary agent host IP address to use for encrypted communications between the 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 the Agent and RSA Authentication Manager impossible.

You specify an overriding primary IP address by including the **CLIENT_IP** keyword in an **sdopts.rec** file on the 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 the Agent. For more information, see Chapter 3, "Installing the Agent for Citrix StoreFront" and Chapter 7, "Troubleshooting."

The following example shows how to specify an IP address override in the **sdopts.rec** file:

```
CLIENT_IP=192.168.10.19
```

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

Important: the Agent ignores this setting if the IP address override option is set in the RSA Control Center. However, if you installed the Auto-Registration utility (during or after the initial the Agent installation), the address that the Auto-Registration utility registers overrides the IP address 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 "Enable an IP Address Override" on page 34.