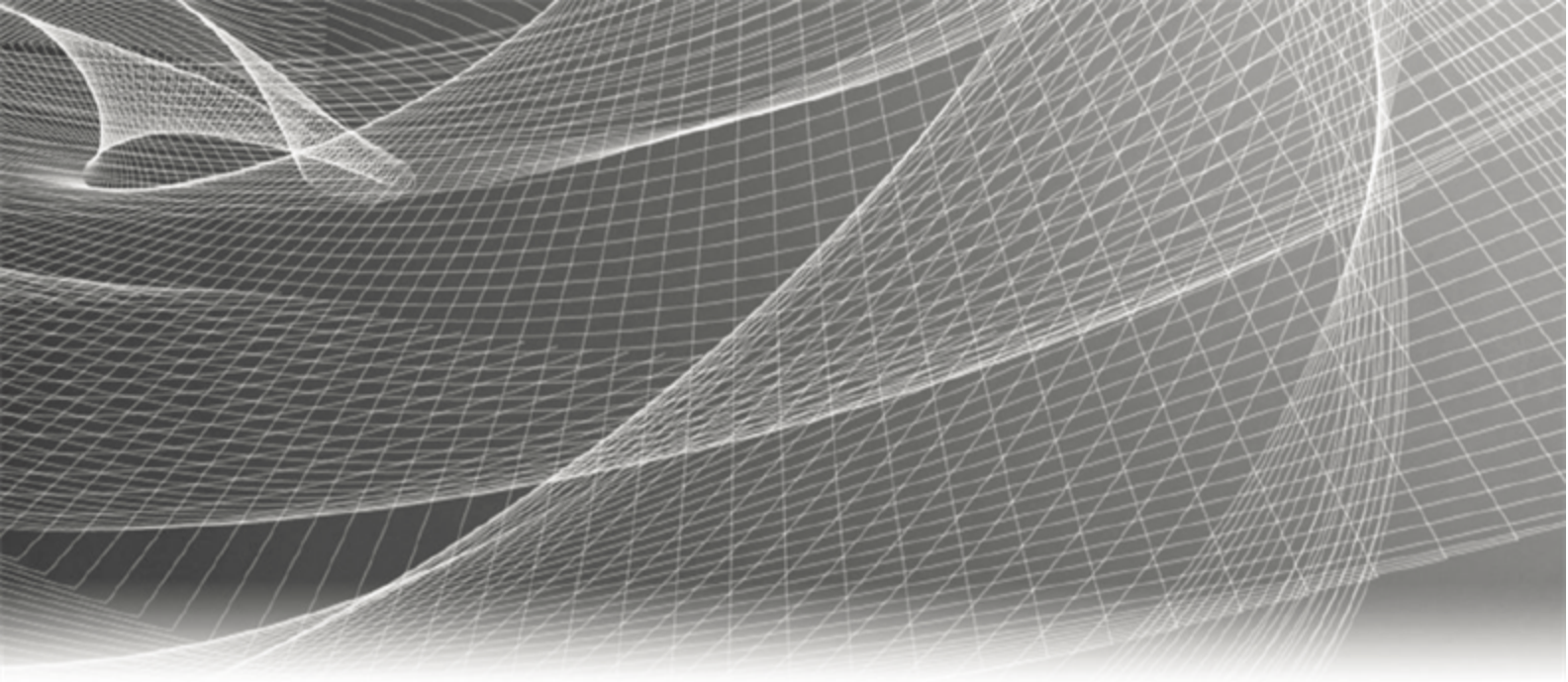

RSA SECURID® ACCESS

RSA® Authentication Agent 2.0.4 for Citrix StoreFront Administrator's Guide

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

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

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. 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 RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license. RSA 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." RSA 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.

April 2022

Contents

Preface

Audience

This guide is for network and system administrators who deploy, configure, and manage Authentication Agent for Citrix StoreFront.

The document assumes you have experience using Citrix StoreFront. It also assumes you have experience with Authentication Manager or the Cloud Authentication Service, or you are working with an administrator for those products.

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 problems, product documentation, community discussions, and case management.

RSA Ready Partner Program

The RSA Ready Partner Program website at https://community.securid.com/t5/securid-integrations/tkb-p/securid-access-integrations 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.

Chapter 1: Authentication Agent for Citrix StoreFront

Authentication Agent for Citrix StoreFront Overview

Authentication Agent for Citrix StoreFront is authentication software that provides Citrix StoreFront with additional methods for authenticating users either inside or outside the corporate firewall. When attempting to access a StoreFront store, users provide their usernames and passwords for primary authentication, and Agent for Citrix StoreFront prompts them to complete one or more additional authentication methods, depending on the configured authentication mode. The agent supports the following authentication modes:

- **RSA Cloud Authentication Service (CAS mode)**. The agent connects to your existing Cloud Authentication Service deployment, which supports these authentication methods:
    - Approve
    - Authenticate Tokencode
    - Device Biometrics
    - SMS Tokencode
    - Voice Tokencode
    - RSA SecurID Token (requires integration between the Cloud Authentication Service and Authentication Manager)
- **Authentication Manager With REST API Endpoint (AM REST mode)**. The agent connects to your existing Authentication Manager deployment using the REST API endpoint over IPv4 or IPv6, which supports these authentication methods:
    - RSA SecurID Token
    - Authenticate Tokencode (requires integration between the Cloud Authentication Service and Authentication Manager)
- **Authentication Manager With UDP Protocol (AM UDP mode)**. The agent connects to your existing Authentication Manager deployment using the UDP protocol, which supports the RSA SecurID Token and risk-based authentication (RBA). For more information, see Risk-Based Authentication below.

Full documentation for Authentication Manager and the Cloud Authentication Service is available on RSA Link.

For any authentication mode, if you want to extend authentication to users outside the corporate firewall, you must use the agent in conjunction with Citrix NetScaler Gateway and Citrix Delegated Forms Authentication (DFA). For more information, see Citrix Delegated Forms Authentication on page 56.

Agent for Citrix StoreFront is compatible with the Federal Information Processing Standard (FIPS), a United States government computer security standard used to approve cryptographic modules. For more information, see Enable or Disable FIPS on Windows Server Operating Systems on page 43

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 Citrix StoreFront User Name and Password Features Used by the Agent on page 38.

Risk-Based Authentication

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 (WPI) on the next page.

RBA is supported only when Agent for Citrix StoreFront is configured in AM UDP mode. For more information on integrating the Agent with RBA, see Enabling RSA Authentication Manager Risk-Based Authentication on page 60.

Supported Authentication Methods for Agent for Citrix StoreFront

Scenario	Authentication Methods
Agent for Citrix StoreFront connects to the Cloud Authentication Service	The following methods are supported: • Approve • Authenticate Tokencode • Device Biometrics • SMS Tokencode • Voice Tokencode • RSA SecurID Token (requires integration between the Cloud Authentication Service and Authentication Manager)
Agent for Citrix StoreFront connects to Authentication Manager with the UDP protocol	You can authenticate with RSA SecurID Token and risk-based authentication (RBA).
Agent for Citrix StoreFront connects to Authentication Manager with the REST protocol.	The following methods are supported: • RSA SecurID Token • Authenticate Tokencode (requires integration between the Cloud Authentication Service and Authentication Manager)
Direct connection to the Cloud Authentication Service uses RSA Authentication Manager 8.5 as a secure proxy server.	• Cloud Authentication Service methods are supported. • Users are prompted for Authenticate Tokencode if the Cloud Authentication Service or the connection between Authentication Manager and the Cloud Authentication Service is temporarily unavailable or too slow. If Patch 2 or later is applied to Authentication Manager 8.5, users are prompted for Authenticate Tokencode or RSA SecurID passcode.
Direct connection to RSA Authentication Manager 8.5 with the UDP protocol or the REST protocol. Authentication Manager is connected to the Cloud Authentication Service.	• Authentication Manager and Cloud Authentication Service methods are supported. • Users are prompted for Authenticate Tokencode or RSA SecurID passcode if the Cloud Authentication Service or the connection between Authentication Manager and the Cloud Authentication Service is temporarily unavailable or too slow.

RSA Authentication Agent Auto-Registration Utility

When configured in AM UDP mode, Agent for Citrix StoreFront must be registered with Authentication Manager to authenticate users. 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 that is supported only in AM UDP mode. This utility registers the Agent with 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 Install the Agent on page 26.

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 38.

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 (WPI)

Windows Password Integration (WPI) is an optional Authentication Manager feature that you can enable for Agent for Citrix StoreFront if the agent is configured in AM UDP or AM REST mode.

When the feature is enabled, Agent for Citrix StoreFront can retrieve a Windows password from Authentication Manager and use it during logon to Citrix StoreFront. Users provide Windows passwords only the first time they authenticate. At that time, the agent stores the Windows passwords with user authentication data in Authentication Manager. During subsequent authentications, users enter only their usernames and RSA SecurID passcodes. Agent for Citrix StoreFront uses stored passwords for authentication to Active Directory.

When users change the Windows password from within a Citrix StoreFront session, Agent for Citrix StoreFront automatically synchronizes the password in corresponding accounts in the 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 Agent for Citrix StoreFront later retrieves the stored password, the user is prompted to enter the correct password and the password is stored on Authentication Manager.

You enable WPI from the offline authentication policy settings in the Security Console. You can enable Windows password integration for all Agent for Citrix StoreFront computers in the database, or select certain computers. If the agent is configured in AM UDP mode, this is the only required step.

If the agent is configured in AM REST mode, you must also obtain the security configuration file (**sdconf.rec**) and node secret file (**<AgentName>_NodeSecret.zip**) from Authentication Manager, copy them to each agent computer, and specify their file paths when installing or configuring the agent.

Note: If RSA Authentication Agent for Microsoft Windows is already installed and configured with a node secret on the Citrix StoreFront server, Agent for Citrix StoreFront includes an option to use the same node secret to enable WPI in AM REST mode.

For more information, see the Authentication Manager documentation on RSA Link.

RSA Authentication Agent Offline Local Service

Agent for Citrix StoreFront does not support the Offline Authentication feature provided by RSA Authentication Agent for Microsoft Windows. However, if Agent for Citrix StoreFront is installed in AM UDP mode, Windows Password Integration depends on the RSA Authentication Agent Offline Local Service. If you are using Windows Password Integration for either agent, do not disable this service.

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

Coexistence With RSA Authentication Agent for Microsoft Windows

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

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

- When installing both agents, RSA recommends that you install the Windows Agent first.
- The Agent Auto-Registration feature can only be installed by one agent at a time.
- 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. To 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: If the Windows Agent is already installed and configured with a node secret on the Citrix StoreFront server, Agent for Citrix StoreFront includes an option to use the same node secret to enable WPI in AM REST mode. RSA recommends that you select this option during initial installation if you need to enable WPI, and only use the **Manage WPI** settings in the Manage SecurID Options menu if you switch from AM UDP or CAS mode to AM REST mode after initial installation.

Citrix StoreFront Support for RSA Authentication Manager Features

Agent for Citrix StoreFront supports these Authentication Manager when installed in AM UDP or AM REST mode:

- RSA SecurID authentication using native RSA SecurID protocol
- On-demand authentication (ODA) using native RSA SecurID protocol
- Risk-based authentication (RBA)
- RBA with single sign-on
- Password integration
- RSA Authentication Manager replica support

The following features are not supported:

- RSA SecurID authentication using RADIUS protocol
- ODA using RADIUS protocol
- Secondary RADIUS server support
- RSA SecurID software token automation
- RSA SecurID 800 Authenticator automation
- RSA SecurID protection of administrative interface
- Cloud Authentication Service Emergency Tokencode

Language Support

Agent for Citrix StoreFront provides localized (translated) Citrix StoreFront user-facing authentication web pages which display according to the language preferences presented by the user's web browser. Localized pages are provided in the following languages:

- US English (en-us)
- German (de)
- Chinese (zh-cn)
- Chinese (zh-tw)
- French (fr)
- Japanese (ja)
- Korean (ko)
- Latin Spanish (es)
- Russian (ru)

Chapter 2: Preparing for Installation

System Requirements

Authentication Agent for Citrix StoreFront requires the following system components:

- One of the following Windows operating systems:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012

  Note: Windows Server Core mode is not supported.
- One of the following Citrix StoreFront versions:
  - 3.12 and 3.13 are supported on Windows Servers 2012, 2012 R2, and 2016
  - 3.16 is supported on Windows Servers 2012 R2 and 2016
    - Microsoft PowerShell 3.0 or later
    - Microsoft .NET Framework 4.5 or later
  - 1912.0.4000.6 LTSR is supported on Windows Servers 2012 R2, 2016, and 2019
    - Microsoft .NET Framework 4.5.1 or later
  - 2203.0.0.36 LTSR is supported on Windows Servers 2016 and 2019
    - Microsoft .NET Framework 4.7.2 or later

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

Security Considerations

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 do the following:

- Configure your Citrix environment (StoreFront and, if applicable, NetScaler Gateway) to use HTTPS to secure communications between Citrix StoreFront and users.
- 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 configuration instructions, see the following references.

Task	Reference	Search Keywords
Configuring Citrix StoreFront to use HTTPS	https://www.citrix.com/support/	*https*, *StoreFront*
Configuring the Microsoft TLS/SSL Security Provider to use TLS v1.2	http://support.microsoft.com	*How to restrict the use of certain cryptographic algorithms and*

Task	Reference	Search Keywords
		protocols in Schannel.dll
Configuring TLS	http://csrc.nist.gov/publications/PubsSPs.html	*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.

Port	Authentication Mode	Description
5500/udp	AM UDP	Authentication Manager uses this port to listen. Agent for Citrix StoreFrontconnects to this port during authentication.
5550/tcp	AM UDP	RSA Authentication Agent Auto-Registration uses this port to automatically register Agent for Citrix StoreFront with Authentication Manager.
5580/tcp	AM UDP/AM REST	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.
5555/tcp	AM REST	Used by default for REST protocol communication between the agent and Authentication Manager primary and replica instances. The Authentication Manager administrator can change which port is used for this purpose.
443/tcp	CAS	Used for REST protocol communication between the agent and the Cloud Authentication Service.

Supported Web Browsers

RSA tested the following web browsers with RSA Authentication Agent 2.0.4 for Citrix StoreFront:

- Google Chrome, version 100.0.4896.75 (64-bit)
- Internet Explorer 11
- Microsoft Edge, version 100.0.1185.36 (64-bit)
- Mozilla Firefox ESR 99.0 (64-bit)

Note: JavaScript must be enabled in the browser.

Authentication Manager Requirements

Agent for Citrix StoreFront requires Authentication Manager 8.4 or later.

When you connect the Agent for Citrix StoreFront to Authentication Manager 8.5, you can use Authentication Manager as a secure proxy server that sends any authentication requests that Authentication Manager cannot validate directly to the Cloud Authentication Service.

This feature does not support certain Authentication Manager features, such as enabling and disabling or restricting agents, and failover to replica instances for agents.

User Authentication Requirements

For AM UDP mode, users must have an RSA SecurID hardware or software token to successfully authenticate. Users must be enabled for risk-based authentication (RBA) in order to authenticate to Citrix StoreFront resources protected with RBA.

For AM REST mode, users must have an RSA SecurID hardware or software token, or a registered mobile device with the SecurID Authenticate app installed.

For CAS mode, the following requirements apply:

- To use Approve, Device Biometrics, or Authenticate Tokencode, users must install the RSA SecurID Authenticate app and register a compatible mobile device.
- To use SMS Tokencode and Voice Tokencode, the user's phone number must be recorded in an identity source connected to the Cloud Authentication Service, and the phone number attribute must be synchronized with the Cloud Authentication Service.
- To use RSA SecurID Token, Authentication Manager must be integrated with the Cloud Authentication Service, and users must have SecurID hardware or software tokens.
- The access policy configured for the agent must allow the authentication methods you want to make available to Citrix StoreFront users.

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

Preinstallation Tasks

Before installing Agent for Citrix StoreFront, Import the Trusted Root Certificate for Authentication Manager or the Cloud Authentication Service on page 20, then perform the tasks for the authentication mode you want to configure.

If you are using Authentication Manager 8.5 as a secure proxy server to the Cloud Authentication Service, you can use Authentication Manager with REST protocol mode or Cloud Authentication Service mode, depending upon the authentication methods that are required. In each case, the Agent for Citrix StoreFront connects to Authentication Manager. Collect the required information that is listed in the Authentication Manager with the REST protocol preinstallation tasks.

Preinstallation Tasks for AM UDP Mode

- Obtain the RSA Authentication Manager Configuration File on the facing page (**sdconf.rec**).
- (Optional) If you plan to use the Authentication Agent Auto-Registration utility, Download the Authentication Manager Server Certificate for Auto-Registration on page 20 **(server.cer**).
- Make sure your users are familiar with the RSA SecurID token or RBA authentication process.

Preinstallation Tasks for AM REST Mode

- Obtain the REST Authentication URL for the Primary Authentication Manager Instance below.
- (Optional) Obtain the REST authentication URL for any Authentication Manager replica instances you plan to connect to the agent.
- Obtain the REST authentication API access key for Authentication Manager. For instructions, see Configure the RSA SecurID Authentication API for Authentication Agents on RSA Link.
- (Optional) If you plan to enable WPI:
    - Obtain the RSA Authentication Manager Configuration File below (**sdconf.rec**).
    - Obtain the node secret file from the Security Console. For instructions, see Manage the Node Secret on RSA Link.
- If you plan to install the agent from the command line, Create a Configuration Input File for Command Line Installation on page 21.
- Make sure your users are familiar with the RSA SecurID token authentication process.

Preinstallation Tasks for CAS Mode

- Obtain the REST Authentication URL for the Cloud Authentication Service on the next page
- Obtain the REST authentication API access key for the Cloud Authentication Service. For instructions, see Add an RSA SecurID Authentication API Key on RSA Link.
- If you plan to install the agent from the command line, Create a Configuration Input File for Command Line Installation on page 21.
- Make sure your users are familiar with the Cloud Authentication Service authentication process. For more information, see Cloud Authentication Service Rollout to Users on RSA Link.

Obtain the RSA Authentication Manager Configuration File

To install Agent for Citrix StoreFront in AM UDP mode, or to configure WPI in AM REST mode, you must generate the Authentication Manager configuration file (**sdconf.rec**) in Authentication Manager, copy it to the agent host computer, and specify its directory location when you install or configure the agent.

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

Before you begin

Use a copy of **sdconf.rec** generated from an Authentication Manager server that performs authentication. (The authentication service must be running on that server.)

Procedure

1. Log onto the 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 to the agent during installation or configuration.
5. Unzip the **AM_Config.zip** file so that the contents can be used.

Obtain the REST Authentication URL for the Primary Authentication Manager Instance

To configure Agent for Citrix StoreFront in AM REST mode, you must provide the REST authentication URL for

your primary Authentication Manager instance using the following format:

`https://<hostname>:<port>/mfa/v1_1/`

Obtain the *<hostname>* value from the **Fully Qualified Domain Name** field on the **Administration > Network > Appliance Network Settings** page of the Authentication Manager Operations Console. The default *<port>* is 5555.

Obtain the REST Authentication URL for the Cloud Authentication Service

To configure Agent for Citrix StoreFront in CAS mode, you must provide the REST authentication URL for the Cloud Authentication Service using the following format:

`https://<hostname>:<port>/mfa/v1_1/`

Obtain the *<hostname>* from the Cloud Administration Console. Click **My Account > Company Settings > Authentication API Keys**. Copy the **RSA SecurID Authentication API REST URL**. The default PORT is 443.

Download the Authentication Manager Server Certificate for Auto-Registration

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

If you install Agent for Citrix StoreFront in AM UDP mode, and you do not install the Auto-Registration utility, you must manually register the agent in the Authentication Manager database. For more information, see Register the Agent in Authentication Manager on page 30.

Before you begin

To use the Authentication Agent Auto-Registration utility, Authentication Manager must be configured to allow automatic agent host registration. For more information, see Automatic Agent Registration on RSA Link.

Procedure

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

Import the Trusted Root Certificate for Authentication Manager or the Cloud Authentication Service

Before installing the agent, you must import the trusted root CA certificate from Authentication Manager or the Cloud Authentication Service, depending on the authentication mode you are configuring for the agent.

If you are using Authentication Manager 8.5 as a secure proxy server to the Cloud Authentication Service, you require an Authentication Manager certificate.

Perform this procedure on each computer where Agent for Citrix StoreFront will be installed.

Before you begin

Obtain the trusted root CA certificate from your Authentication Manager or Cloud Authentication Service administrator and copy it to a location on the computer where you will install the agent. For instructions, see the knowledgebase article How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate.

Procedure

1. Sign into the computer where you will install the agent.
2. Run **mmc.exe** to open the Microsoft Management Console.
3. Click **File > Add/Remove Snap-In**.
4. Double-click **Certificates**.
5. Select **Computer Account**, then click **Next**.
6. Select **Local Computer**, then click **Finish**.
7. Click **OK**.
8. Navigate to **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.
9. Right-click **Certificates** and select **All Tasks > Import**.
10. Click **Next**.
11. Click **Browse**, then select the certificate you would like to import and click **Open**.
12. Click **Next**.
13. Select **Place all certificates in the following store**.
14. Click **Browse**, then select **Trusted Root Certification Authorities** and click **OK**.
15. Click **Next**.
16. Click **Finish & OK**.

Create a Configuration Input File for Command Line Installation

Before you install Agent for Citrix StoreFront in AM REST or CAS mode using the command line, you must create an input file to pass configuration inputs to the installer. The input file is a text file containing key-value pairs that specify agent installation parameters.

If you are using Authentication Manager 8.5 as a secure proxy server to the Cloud Authentication Service, choose an authentication mode that supports the type of authentication you require, and enter an Authentication Manager Server URL and Access Key.

Before you begin

Complete the Preinstallation Tasks on page 18 for the authentication mode you want to configure.

Procedure

1. Create a text file with any file name and extension. For example, **input.txt**.
2. Open the file for editing.
3. Add the following string to specify the Authentication Mode:
   `AUTHENTICATION_MODE= <#>`
   where *<#>* is either `1` for AM REST mode or `2` for CAS mode.
4. Add the following string to specify the Server URL:
   `SERVER_URL= https://<hostname>:<port>/mfa/v1_1/`
   where *<hostname>* is the REST authentication URL for either the Cloud Authentication Service or the primary Authentication Manager instance in your deployment, depending on the authentication mode you specified. The default *<port>* is either 5555 for AM REST mode or 443 for CAS mode.

   If you are using Authentication Manager 8.5 as a proxy server to the Cloud Authentication Service,

specify the Server URL for communication between the authentication agent and the Authentication Manager primary instance.

5. Add the following string to specify the Agent Name:
   `AGENT_NAME= <examplename>`
   where *<examplename>* is the name you choose to identify the agent in Authentication Manager or in mobile notifications sent through the Cloud Authentication Service.
6. Add the following string to specify the Access Key:
   `ACCESS_KEY= <accesskey>`
   where *<accesskey>* is the access key you obtained for either Authentication Manager or the Cloud Authentication Service, depending on the authentication mode.

   If you are using Authentication Manager 8.5 as a proxy server, specify the Access Key for securely passing authentication requests to Authentication Manager.
7. (Optional) For AM REST mode, add the following string to specify Replica Server URLs:
   `REPLICA_URLS= <https://hostname2:port/mfa/v1_1, https://hostname3:port/mfa/v1_1, https://hostname4:port/mfa/v1_1>`
   where *<https://hostname2:port/mfa/v1_1, https://hostname3:port/mfa/v1_1, https://hostname4:port/mfa/v1_1>* is a comma-separated list of URLs for the replica servers in your deployment.
8. (Optional) For AM REST mode, do one of the following if you need to enable WPI:
   - Add the following strings to specify a node secret file generated by Authentication Manager:
     `NSFILENAME=<nodesecretfilename>`
     `NSPASSWORD=<nodesecretpassword>`
     where *<nodesecretfilename>* is the file name of the node secret file you copied to the agent installer directory and *<nodesecretpassword>* is the password that was used to encrypt the node secret file.
   - Add the following string to specify whether to use the existing node secret file from Agent for Microsoft Windows if it is already installed on the Citrix StoreFront server:
     `USE_LAC_NODESECRET=<true>`
9. For CAS mode, add the following string to specify the access policy the agent will use:
   `ACCESS_POLICY= <accesspolicy>`
   where *<accesspolicy>* is the exact name (including case sensitivity) of the access policy as specified in the Cloud Administration Console.
10. (Optional) For CAS mode, add the following string if you need to disable collection of risk data during authentication:
    `RISK_COLLECTION_ENABLED= false`
    If you do not add this string, risk data collection is enabled by default.

    Note: If you disable risk data collection, you cannot use the Identity Confidence access policy attribute to determine user authentication requirements.
11. (Optional) For CAS mode, add the following string if you need to disable collection of location data during authentication:
    `LOCATION_COLLECTION_REQUIRED= false`
    If you do not add this string, location data collection is enabled by default.

Note: If you disable location data collection, you cannot use the Trusted Location access policy attribute to determine user authentication requirements.

12. Save the file to the Citrix StoreFront server where you want to install the agent.

After you finish

Point to the input file you created by including the following in the console command when you install the agent using the command line:

`INPUTFILE=<absolute\file\path\input.txt>`

where *<absolute\file\path\input.txt>* is the absolute file path for the input file.

Chapter 3: Installing the Agent for Citrix StoreFront

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 the Agent

The installation program installs the following items, depending on the options you select during installation:

- Authentication Agent for Citrix StoreFront
- (Optional) Auto-Registration utility
- (Optional) Windows Password Integration

You can either use the Install Wizard, which guides you through the installation process, or use the command line, which allows for silent installation and can be used with custom scripts to install the agent on multiple servers.

Install Using the Install Wizard

The install wizard provides a simple graphical interface for installing Agent for Citrix StoreFront. Run the install wizard on each Citrix StoreFront server where you want to install the agent.

Before you begin

- You must have administrator rights for the Citrix StoreFront server on which you are installing Agent for Citrix StoreFront.
- Close the Citrix StoreFront Management Console.
- Copy the installation package to a folder on the system where you want to install the agent.

  Note: Make sure to preserve the directory structure when you copy the installation files.

- Copy the following files to the same folder as the installer:
  - **sdconf.rec** (for AM UDP mode, or if you want to configure WPI for AM REST mode)
  - **server.cer** (for AM UDP mode, if you want to install Auto-Registration)
  - **<AgentName>_NodeSecret.zip** (for AM REST mode, if you want to configure WPI)

  Note: The Install Wizard prompts you to browse and select the files during installation.

Procedure

1. Log on to the Citrix StoreFront server where you want to install Agent for Citrix StoreFront.
2. In the folder where you copied the installation files, double-click **RSA Authentication Agent for Citrix StoreFront x64.msi** to start the installation wizard.
3. Click **Next** to continue.

4. Read and accept the License Agreement or click **Print** to print it. Click **Next**.
5. Select the authentication mode you want to configure for the agent, and click **Next**.
6. Perform the steps for your authentication mode:
    - For **RSA Cloud Authentication Service (CAS mode)**:
        a. In the **Server URL** field, enter the REST authentication URL for the Cloud Authentication Service.

        If you are using Authentication Manager 8.5 as a proxy server in Cloud Authentication Service mode, enter the Server URL and Access Key for securely passing authentication requests to Authentication Manager.

        b. In the **Access Key** field, enter the REST authentication API access key for the Cloud Authentication Service.
        c. In the **Access Policy** field, enter the name of the access policy that the agent will use as it appears in the Cloud Administration Console.
        d. In the **Agent Name** field, enter a name for the agent. The name you specify is used to identify the agent in mobile notifications sent through the Cloud Authentication Service.
        e. (Optional) Select **Enable location data collection during authentication** to allow the agent to collect HTML5 geolocation data during user authentication, which includes longitude, latitude, and a timestamp.
        f. (Optional) Select **Enable risk data collection during authentication** to allow the agent to collect device fingerprint data and other information during authentication.
        g. Click **Next**.
    - For **Authentication Manager With REST Protocol (AM REST mode)**:
        a. In the **Server URL** field, enter the REST authentication URL for the primary Authentication Manager instance.
        b. In the **Access Key** field, enter the REST authentication API access key for Authentication Manager.
        c. In the **Agent Name** field, enter a name for the agent. The name you specify is used to identify the agent in Authentication Manager
        d. (Optional) In the **Replica URLs** field, enter the REST authentication URL for a replica Authentication Manager instance, and click **+** to add it to the replica server list. Repeat this step to add up to 15 replica servers.
        e. Click **Next**.
        f. (Optional) Select **Enable Windows Password Integration** to enable WPI, then do the following:
            i. (Optional) If Agent for Windows is installed on the Citrix StoreFront server, and you want to use the existing node secret for Agent for Citrix StoreFront, select **Use Node Secret from Agent for Windows** and skip to step **g**.
            ii. Click **Browse** and specify the directory location for the configuration file **sdconf.rec**.
            iii. Click **Browse** and specify the directory location for the node secret file **<AgentName>_NodeSecret.zip**.
            iv. Enter the password with which the node secret file was encrypted.

g. Click **Next**.

- For **Authentication Manager With UDP Protocol (AM UDP mode)**:
  a. (Optional) To install the Auto-Registration utility, select **Will be installed on the local hard drive** from the **Auto-Registration Utility** drop-down list.
  b. Click **Next**.
  c. Click **Browse** to locate and open the system configuration file (**sdconf.rec**).
  d. Click **Next**.
  e. If you are installing the Auto-Registration utility, click **Browse** to locate and open the server certificate file (**server.cer**).
  f. Click **Next**.

7. Click **Install**.
8. When installation completes, click **Finish**.

Install Using Command Line Options

You can use the command line installer to perform a silent installation, or execute the command on multiple servers simultaneously, using a script or third-party product.

Before you begin

- You must have administrator rights for the Citrix StoreFront server on which you are installing Agent for Citrix StoreFront.
- Know the basics of software installation using the msiexec command line options. For more information, visit http://technet.microsoft.com
- If you are installing the agent in AM REST or CAS mode, you must Create a Configuration Input File for Command Line Installation on page 21.
- Close the Citrix StoreFront Management Console.
- Copy the installation package to a folder on the system where you want to install the agent.

  Note: Make sure to preserve the directory structure when you copy the installation files.

- Copy the following files to the same folder as the installer:
  - **sdconf.rec** (for AM UDP mode, or if you want to configure WPI for AM REST mode)
  - **server.cer** (for AM UDP mode, if you want to install Auto-Registration)
  - **<AgentName>_NodeSecret.zip** (for AM REST mode, if you want to configure WPI)

  Note: The command-line installation collects the files from the folder where it is run.

Procedure

1. Open an administrator command prompt.
2. Navigate to the directory that contains the **RSA Authentication Agent for Citrix StoreFront x64.msi** file, or provide the full pathname to the package file on the command line.

Depending on the authentication mode and optional features you want to configure for the agent, do one of the following:

- For **AM UDP mode**, use a command similar to the following:

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

- For **AM UDP mode 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`
- For **AM REST or CAS mode**, use a command similar to the following:
  `msiexec /qn /i "RSA Authentication Agent for Citrix StoreFront x64.msi" INPUTFILE=<absolute\file\path\input.txt>`
  where *<absolute\file\path\input.txt>* is the absolute file path of the configuration input file you created. The parameters in the input file specify the authentication mode and other features that will be configured by the installer.

Note: 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%**.

After you finish

If you installed the agent using a configuration input file, secure or delete the file, as it contains sensitive data.

Upgrading from Agent for Citrix StoreFront 2.0 or Later

If Agent for Citrix StoreFront version 2.0 or later is already installed on your Citrix StoreFront server, the installer preserves previous settings and upgrades the agent to the current version.

You can perform an upgrade installation using the install wizard or the command line. The install wizard detects the existing agent version and displays a warning which you must accept to proceed. The command-line installation performs the upgrade automatically.

Upgrading from Agent for Citrix StoreFront 1.5

If Agent for Citrix StoreFront version 1.5 is already installed on your Citrix StoreFront server, the installer preserves previous settings, upgrades the agent to the current version, and automatically configures AM UDP mode.

You can perform an upgrade installation using the install wizard or the command line. The install wizard detects the existing agent version and displays a warning which you must accept to proceed. The command-line installation performs the upgrade automatically when you run the command to install the agent in UDP mode.

Post-Installation

After installing Agent for Citrix StoreFront, perform the tasks for the authentication mode you selected, in order.

Post-Installation Tasks For AM UDP Mode

1. Register the Agent in 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 Authentication Manager. For instructions, see Register the Agent in Authentication Manager below.
2. Perform a test authentication to verify the connection to Authentication Manager and generate a node secret, if one does not already exist. For instructions, see Perform a Test Authentication on page 51. You can optionally establish the node secret using the Node Secret Load utility. This method is useful for troubleshooting or resolving note secret issues when Agent for Citrix StoreFront and Agent for Microsoft Windows are installed on the same computer. For instructions, see Manually Load the Node Secret on page 39.
3. Configure Citrix StoreFront to use **RSA SecurID** authentication. For instructions, see Install or Uninstall RSA SecurID Authentication for a Store on page 44.

Post-Installation Tasks for AM REST Mode

1. Register the Agent in Authentication Manager below.
2. Configure Citrix StoreFront to use **RSA SecurID** authentication. For instructions, see Install or Uninstall RSA SecurID Authentication for a Store on page 44.
3. (Optional) Configure additional settings such as Load Balancing Scheme, Request Timeout, Read Timeout, and Retry Count using the Manage SecurID Options page. For instructions, see Manage Agent Settings on page 45.
4. (Optional) Test the connection to the Cloud Authentication Service by entering `https://HOSTNAME:PORT/mfa/v1_1` in a browser or http client.

   Because you are not currently authenticating, you will see a message that the site is forbidden or unauthorized. This is expected for the test.

Post-Installation Tasks for CAS Mode

1. Configure Citrix StoreFront to use **RSA SecurID** authentication. For instructions, see Install or Uninstall RSA SecurID Authentication for a Store on page 44.
2. (Optional) Configure additional settings such as Request Timeout, Read Timeout, and Retry Count using the Manage SecurID Options page. For instructions, see Manage Agent Settings on page 45.
3. (Optional) Test the connection to the Cloud Authentication Service by entering `https://HOSTNAME:PORT/mfa/v1_1` in a browser or http client.

   Because you are not currently authenticating, you will see a message that the site is forbidden or unauthorized. This is expected for the test.

Register the Agent in Authentication Manager

After you install Agent for Citrix StoreFront in AM UDP or AM REST mode, you must register it with Authentication Manager.

Note: If the agent is in AM UDP mode and you installed the Auto-Registration utility, you do not need to manually register the agent.

Before you begin

Obtain the following:

For AM UDP mode:

- 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 in 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.

  For more information on registering the agent in AM UDP mode, see https://community.rsa.com/docs/DOC-77208 on RSA Link.

For AM REST mode:

- Logical Agent Name
- **<AgentName>_NodeSecret.zip** (only if WPI is enabled)
- **sdconf.rec** (only if WPI is enabled)

  For more information on registering the agent in AM REST mode, see https://community.rsa.com/docs/DOC-76818 on RSA Link.

Procedure

1. Log onto the 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 Agent for Citrix StoreFront is installed in AM UDP mode, or in AM REST mode with WPI enabled, and your deployment includes a Citrix StoreFront server group where multiple servers are running the agent, the node secret must be the same for all agents in the group. For AM REST mode, you specify the node secret file when you enable WPI in the installer or on the Manage SecurID Options page. In UDP mode, you must use the Node Secret Load Utility to install the node secret on each StoreFront server in the group. For more information, see Manually Load the Node Secret on page 39.

For instructions on generating the node secret in the Security Console, see Manage the Node Secret on RSA Link.

Modify an Installation

If you installed the agent in AM UDP mode, you can modify the installation to add or remove the RSA Authentication Agent Auto-Registration utility. You can modify the installation using the install wizard or command-line options.

Modify the Installation Using the Install Wizard

Use this procedure to modify the installation using the install wizard.

Before you begin

- Copy the download package containing **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to modify the installation.
- If you are adding 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.
- If you are removing the Auto-Registration utility, do the following:
    - Remove the RSA SecurID authentication method. See Install or Uninstall RSA SecurID Authentication for a Store on page 44.
    - Close the Citrix StoreFront management console.

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. If you are adding 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

Use this procedure to modify an agent installation using the command line.

Before you begin

- Know how to install software using the msiexec command-line. For more information on msiexec commands, visit http://technet.microsoft.com.
- Copy the download package containing **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to modify the installation.
- If you are adding 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.

- If you are removing the Auto-Registration utility, do the following:
  - Remove the RSA SecurID authentication method. See Install or Uninstall RSA SecurID Authentication for a Store on page 44.
  - Close the Citrix StoreFront management console.

Procedure

1. Open a command prompt, and do one of the following:
2. 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"
   ADDLOCAL=AgentAutoRegistration
   ```
3. 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"
   REMOVE=AgentAutoRegistration
   ```

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

Repair an Installation

Repairing an installation replaces missing files in a damaged 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.

Repair the Installation Using the Install Wizard

The installation wizard provides a simple graphical interface for repairing the agent installation.

Before you begin

Copy the download package containing **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to repair the installation.

Procedure

1. In the folder where you copied the package, 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 Using the Command Line

You can repair an agent installation using the command line. Use the command line to perform a silent installation, or execute the command on multiple servers simultaneously, using a script or third-party product.

Before you begin

- Know how to install software using the msiexec command-line. For more information on msiexec commands, visit http://technet.microsoft.com.
- Copy the download package containing **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to repair the installation.

Procedure

1. Open a command prompt.
2. Navigate to the directory that contains **RSA Authentication Agent for Citrix StoreFront x64.msi**, or provide the full pathname to the package file on the command-line.
3. Enter the following command:
   ```
   msiexec /qn /fvomus "RSA Authentication Agent for Citrix StoreFront x64.msi"
   ```

Note: 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.

Uninstall Using Windows Control Panel

Perform the following procedure to uninstall the agent from the Windows Control Panel.

Before you begin

- 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 56.
- Remove the RSA SecurID authentication method. See Install or Uninstall RSA SecurID Authentication for a Store on page 44.
- Close the Citrix StoreFront management console.

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 Install Wizard

Perform the following procedure to uninstall the agent using the install wizard.

Before you begin

- Copy the download package containing **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the computer where you want to uninstall the agent.
- 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 56.
- Remove the RSA SecurID authentication method. See Install or Uninstall RSA SecurID Authentication for a Store on page 44.
- Close the Citrix StoreFront management console.

Procedure

1. In the folder where you copied the installation files, double-click **RSA Authentication Agent for Citrix StoreFront x64.msi** to start the installation wizard.
2. Click **Next**.
3. Select **Remove**, then click **Next**.
4. Click **Remove**.
5. Click **Finish** to exit the wizard.

Uninstall Using the Command Line

Perform the following procedure to uninstall the agent from the command line.

Before you begin

- Copy the download package containing **RSA Authentication Agent for Citrix StoreFront x64.msi** to a folder on the system where you want to uninstall the product.
- 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 56..
- Remove the RSA SecurID authentication method. See Install or Uninstall RSA SecurID Authentication for a Store on page 44.
- Close the Citrix StoreFront management console.

Procedure

1. Open a command prompt.
2. Enter a command similar to the following with the `/x` (REMOVE=ALL) option and the fully qualified pathname:
   ```
   msiexec /qn /x "RSA Authentication Agent for Citrix StoreFront x64.msi" /lv uninstall.log
   ```

   Note: 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%.
3. (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.

Chapter 4: Configuring and Managing the Agent for Citrix StoreFront

Citrix StoreFront User Name and Password Features Used by the Agent

You can use the following features of the Citrix StoreFront **User name and password** authentication method with the Agent for Citrix StoreFront:

- 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 install Citrix StoreFront and the agent on a server, and add that server 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

If Agent for Citrix StoreFront is installed in AM UDP mode and Auto-Registration is enabled, you can configure the Auto-Registration utility to exclude specific network adapters from automatic IP address registration. In some cases, this can reduce network traffic and maximize performance. 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

If Agent for Citrix StoreFront is installed in AM UDP mode, each agent host's primary IP address must be

identified in its agent record in the 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 on the Manage SecurID Options page (and in the load balancing options file **sdopts.rec,** if you are using automatic load balancing as described in Automatic Load Balancing on page 72). If the addresses do not match, communication between Agent for Citrix StoreFront 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 50.

Manually Load the Node Secret

When installed in AM UDP mode, each instance of the agent is associated with a unique node secret. The node secret allows the agent and the Authentication Manager server to use encrypted communications during the SecurID authentication process.

If not previously established, Authentication Manager automatically creates the node secret and downloads it to the agent host the first time a user successfully authenticates with a SecurID passcode.

This task describes how to manually load the node secret onto the agent host before users start authenticating with RSA SecurID.

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

Before you begin

Generate the node secret. For instructions, see Manage the Node Secret on RSA Link.

Procedure

1. Deliver the node secret from 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 Node Secret Load utility using the following command syntax:
   `agent_nsload -f path -d "..\Auth Data"`
   where *path* is the directory location and name of the node secret file, and `-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 used to encyrpt the node secret file. 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.

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 also works for RSA Authentication Agent for Microsoft Windows if it is installed on the StoreFront servers.

Configure Logging Options for AM REST Mode or CAS Mode

Logging is enabled by default when you install Agent for Citrix StoreFront in AM REST mode or CAS mode.. You can customize logging options by manually editing the **C:\<*AgentInstallDirectory*>\config\log4net.config** file. You can change the following parameters using the log file syntax provided.

Note: You must restart Microsoft Internet Information Services (IIS) after modifying **log4net.config**.

Default Log Format

You can specify the logging format. Specify `SizeBasedRotation`, `TimeBasedRotation`, or `CompositeRotation`, as shown:

```
<root>
<level value="ALL" />
<appender-ref ref="SizeBasedRotation"/>
</root>
```

The default format is size-based logging.

Options for Size-Based Logging

Configure options for size-based logging by editing the following parameters.

Log Rotation

You can enable log rotation by setting the appender tag as shown:

```
<appender name="SizeBasedRotation" type="log4net.Appender.RollingFileAppender">
```

Log File Name

You can specify the name of the log file. For example:

```
<file value="C:\kit\SizeBasedLogFile.log"/>
```

Log File Size

You can specify the maximum log file size. For example:

```
<maximumFileSize value="10MB" />
```

The default maximum file size is 10MB.

Log File Count

You can specify the maximum number of log files to be saved. When the maximum log file count is reached, older log files are overwritten.

```
<maxSizeRollBackups value="10" />
```

Default log file count is 10.

Log Levels

Agent features log levels in the following sequence: Debug > Info > Warn > Error > Fatal

The agent will log all messages between the minimum and maximum levels you specify. The following example values will log all messages for the Info, Warn, Error, and Fatal levels, but will not log Debug messages:

```
<filter type="log4net.Filter.LevelRangeFilter">
<levelMin value="INFO" />
<levelMax value="FATAL" />
</filter>
```

Options for Time-Based Logging

Configure options for time-based logging by editing the following parameters.

Log Rotation

You can enable log rotation by setting the appender tag as shown:

```
<appender name="TimeBasedRotation" type="log4net.Appender.RollingFileAppender">
```

Log Levels

Agent features log levels in the following sequence: Debug > Info > Warn > Error > Fatal

The agent will log all messages between the minimum and maximum levels you specify. The following example values will log all messages for the Info, Warn, Error, and Fatal levels, but will not log Debug messages:

```
<filter type="log4net.Filter.LevelRangeFilter">
<levelMin value="INFO" />
<levelMax value="FATAL" />
</filter>
```

Log File Name

You can specify the name of the log file. For example:

```
<file value="C:\kit\DateBasedLogFile.log"/>
```

Log File Date Pattern

The log file name will be appended with the date pattern you specify. For example:

```
<datePattern value="-yyyyMMdd-HHmm" />
```

Options for Composite Logging

When composite logging is configured, log files will be overwritten based on either date or size, depending on which specified condition is met first. Use the following syntax as a basic composite logging configuration

template, then modify parameters as necessary for your deployment.

```
<appender name="TimeBasedLogFile" type="log4net.Appender.RollingFileAppender">
<file value="C:\kit\DateBasedLogFile.log"/>
<lockingModel type="log4net.Appender.FileAppender+MinimalLock" />
<encoding value="utf-8" />
<appendToFile value="true" />
<rollingStyle value="Composite" />
<datePattern value=".yyMMddHHmm.'log'" />
<preserveLogFileNameExtension value="true" />
<maximumFileSize value="1MB" />
<staticLogFileName value="true" />
<maxSizeRollBackups value="5" />
<layout type="log4net.Layout.PatternLayout">
<conversionPattern value="%d %-5p %c - %m%n" />
</layout>
<filter type="log4net.Filter.LevelRangeFilter">
<levelMin value="INFO" />
<levelMax value="FATAL" />
</filter>
</appender>
```

Log Rotation

You can enable log rotation by setting the appender tag as shown:

```
<appender name="TimeBasedLogFile" type="log4net.Appender.RollingFileAppender">
```

Log Levels

Agent features log levels in the following sequence: Debug > Info > Warn > Error > Fatal

The agent will log all messages between the minimum and maximum levels you specify. The following example values will log all messages for the Info, Warn, Error, and Fatal levels, but will not log Debug messages:

```
<filter type="log4net.Filter.LevelRangeFilter">

<levelMin value="INFO" />

<levelMax value="FATAL" />

</filter>
```

Log File Name

You can specify the name of the log file. For example:

```
<file value="C:\kit\DateBasedLogFile.log"/>
```

Log File Date Pattern

The log file name will be appended with the date pattern you specify. For example:

```
<datePattern value=".yyMMddHHmm.'log'" />
```

Note: In this composite logging configuration, your log files will have the following naming format: 2010-11-02_15_05.log.0, 2010-11-02_15_05.log.1, etc.

Enable or Disable FIPS on Windows Server Operating Systems

The Federal Information Processing Standard (FIPS) is a United States government computer security standard used to approve cryptographic modules. Agent for Citrix StoreFront is compatible with FIPS. Perform this procedure to enable FIPS mode on all Windows Server versions supported by Agent for Citrix StoreFront.

Procedure

1. Sign into the Citrix StoreFront server as an administrator.
2. Click **Start > Control Panel > Administrative Tools > Local Security Policy**.
   The **Local Security Settings** window appears.
3. In the navigation pane, click **Local Policies**, then **Security Options**.
4. In the right-side pane, double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**.
5. In the dialog box that appears, click **Enabled** or **Disabled** based on your deployment requirements, and then click **Apply**.
6. Click **OK**.
7. Close the **Local Security Settings** window.

Manage RSA SecurID Authentication Using the Citrix StoreFront Management Console

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

To modify the following settings, see Open the Citrix StoreFront Management Console below.

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

- Add or remove RSA SecurID from the list of authentication methods that can be enabled and disabled. For more information, see Install or Uninstall RSA SecurID Authentication for a Store on the next page.
- Enable or disable RSA SecurID authentication. Enabling it automatically overrides Citrix **User name and password** authentication. When RSA SecurID authentication is disabled, you can use other available methods. For more information, see Enable or Disable RSA SecurID Authentication on page 45.
- Add or Remove a StoreFront Server in a Server Group Configured to Use RSA SecurID Authentication on the next page.
- Access additional Agent for Citrix StoreFront configuration settings on the Manage SecurID Options page. For more information, see Manage Agent Settings on page 45.

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

Open the Citrix StoreFront Management Console

Open the Citrix StoreFront Management Console to access options for enabling, disabling, and configuring RSA

SecurID authentication and agent settings on the StoreFront server.

Procedure

Do one of the following, depending on the operating system on the StoreFront server:

- 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.

Install or Uninstall RSA SecurID Authentication for a Store

This procedure adds or removes RSA SecurID authentication from the list of authentication providers that can be enabled and disabled for Citrix StoreFront. Removing RSA SecurID authentication from the list does not uninstall the agent from your system.

Note: You must install RSA SecurID authentication for each store that you want the agent to protect.

Procedure

1. Open the Citrix StoreFront Management Console on the previous page.
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 RSA SecurID authentication, check the box for **RSA SecurID**.
   - To uninstall RSA SecurID authentication, 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: 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 RSA SecurID Authentication

If you install Citrix StoreFront and the agent on a server, and add that server to an existing server group, the authorizing StoreFront in the group propagates the server configuration, including RSA SecurID authentication settings, to the new StoreFront server.

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 page 43 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

Enabling RSA SecurID authentication automatically overrides Citrix **User name and password** authentication. When RSA SecurID authentication is disabled, you can use other available methods.

Before You Begin

Install or Uninstall RSA SecurID Authentication for a Store on the previous page. **RSA SecurID** must appear in the Citrix StoreFront management console list of available authentication providers.

Procedure

1. Open the Citrix StoreFront Management Console on page 43.
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 RSA SecurID authentication, check the box for **RSA SecurID**.
   - To disable RSA SecurID authentication, clear the box for **RSA SecurID**.
6. Click **OK**.

Manage Agent Settings

Use the Manage SecurID Options page to change authentication modes and configure other Agent for Citrix StoreFront features. The page displays different options depending on the authentication mode you select.

To modify these settings, see Open the Manage SecurID Options Page on page 49.

AM UDP Mode Options

Option	Description
Full path of sdconf.rec file	Click **Browse** to specify the location of the Authentication Manager configuration file, **sdconf.rec**. Obtain this file from the Authentication Manager administrator.
Enable Auto Registration	When enabled, Auto Registration registers the agent with Authentication Manager and updates the IP address and node secret as needed, without manual intervention. The RSA Authentication Agent Auto-Registration utility must be installed before you can enable this feature.
Full path of server.cer file:	Click **Browse** to specify the location of the server certificate file, **server.cer**. Obtain this file from the Authentication Manager administrator.
Advanced Tools	This submenu contains the following options: • Test Authentication: Submits RSA SecurID username and passcode to Authentication Manager to verify that

Option	Description
	Agent for Citrix StoreFront can authenticate. Follow the on-screen prompts to provide authentication credentials and create an RSA SecurID PIN, if necessary. For more information, see Perform a Test Authentication on page 51. • Tracing: Generates log files for troubleshooting authentication issues. Typically, you only enable tracing when instructed to do so by RSA Customer Support, who will specify which trace level to set and which components to trace. For more information, see Enable Tracing on page 52. • IP Address Override: Specifies the primary IP address to identify Agent for Citrix StoreFront when the server hosting the agent has multiple IP addresses. You must also specify this address when registering the agent in the Authentication Manager Security Console. This feature is unavailable when Auto Registration is enabled. For more information, see Enable an IP Address Override on page 50.
Server Environment	Displays information about your Authentication Manager server environment so you can check the primary and replica instances, and make sure Agent for Citrix StoreFront is communicating with the correct Authentication Manager server.
Clear Node Secret	Clears the node secret from the agent. You may need to clear and replace the node secret if a mismatch occurs. For example, if an administrator unregisters the agent in the Authentication Manager Security Console. For more information, see Clear the Node Secret on page 50.
Send domain and user name to Authentication Manager	Specifies whether the agent sends a user's domain together with the user name when contacting Authentication Manager for an authentication request. Enable this option if user accounts in your deployment use a domain\username format. **Note:** The agent does not support Authentication Manager accounts in UPN format (username@domainname).

AM REST Mode Options

Option	Description
Server URL	Specifies the REST authentication URL for your primary Authentication Manager instance using the following format: `https://HOSTNAME:PORT/mfa/v1_1/` Obtain the *HOSTNAME* value from the **Fully Qualified Domain Name** field on the **Administration > Network > Appliance Network Settings** page of the Operations Console. The default *PORT* is 5555.
Access Key	Specifies the REST authentication API access key for Authentication Manager. To obtain the API access key, see Configure the RSA SecurID Authentication API for Authentication Agents on RSA Link.
Agent Name	Specifies a name that is used to identify the agent in Authentication Manager.
Replica URLs	Specifies the REST authentication URLs for your replica Authentication Manager instances. Enter a URL and click **+** to add it to the list. Select a URL from the list and click **-** to remove it. You can add up to 15 replica URLs.
Request Timeout	Specifies the maximum number of seconds allowed for the agent to complete each

Option	Description
	transaction with Authentication Manager. Range: 1-180 Default: 180 **Note:** If an Authentication Manager instance becomes unavailable, users may experience a delay during authentication while the agent attempts to contact a replica instance. Setting a lower Request Timeout value can reduce this delay.
Read Timeout	Specifies the maximum number of seconds allowed for the agent to connect to the Authentication Manager server and read the response. Range: 1-180 Default: 60
Retry Count	Specifies the number of times the agent will try to contact an Authentication Manager instance if the first attempt is unsuccessful. If replicas are configured, the agent attempts to contact the next replica instance when the retry count is reached. Range: 1-5 Default: 1
Server Refresh Interval	Specifies the number of minutes between polling attempts to determine whether the Authentication Manager service is available. Minimum: 5 Default: 5
Load Balancing	Specifies the method used to distribute authentication requests among configured Authentication Manager replica servers. The agent supports these modes: • Weighted Round Robin (default) The agent periodically measures the time taken by each server to process an authentication request, and distributes more requests to faster servers and fewer requests to slower servers. • Round Robin The agent distributes requests to each server in sequence, in the order the servers were added by the administrator.
Enable WPI	Enables or disables Windows Password Integration. When WPI is enabled and configured, users provide Windows passwords only the first time they authenticate. The agent retrieves stored passwords during subsequent authentications, and does not prompt for Windows password. Click **Manage WPI** for additional configuration settings required to enable WPI. **Note:** You must also enable WPI from the offline authentication policy settings in the Security Console for this setting to work.
Manage WPI	This submenu contains the following WPI settings: • Use Node Secret from UDP:

Option	Description
	If the agent was previously configured in UDP mode, check this box to use the previously generated node secret. • Full path of **sdconf.rec** file: Click **Browse** to specify the location of the Authentication Manager configuration file, **sdconf.rec**. • Full path of ***<AgentName>*_NodeSecret.zip** file: Click **Browse** to specify the location of the Authentication Manager node secret file, ***<AgentName>*_NodeSecret.zip**. • Enter the password used to encrypt ***<AgentName>*_NodeSecret.zip**: This is the password specified when the node secret file was generated in the Security Console. • Generate Node Secret: Click this button to generate the node secret used during encrypted communication between the agent and Authentication Manager.
Send domain and user name to Authentication Manager	Specifies whether the agent sends a user's domain together with the user name when contacting Authentication Manager for an authentication request. Enable this option if user accounts in your deployment use a domain\username format. **Note:** The agent does not support Authentication Manager accounts in UPN format (username@domainname).

CAS Mode Options

Option	Description
Server URL	Specifies the REST authentication URL for the Cloud Authentication Service using the following format: `https://hostname:port/mfa/v1_1/` Obtain the *<hostname>* from the Cloud Administration Console. Click **My Account > Company Settings > Authentication API Keys**. Copy the **RSA SecurID Authentication API REST URL**. The default PORT is 443. **Note:** If you are using Authentication Manager 8.5 as a proxy server, enter the REST authentication URL for Authentication Manager. See the Server URL row in the AM REST Mode Options table.
Access Key	Specifies the REST authentication API access key for the Cloud Authentication Service. To obtain the API access key, see Add an RSA SecurID Authentication API Key on RSA Link. **Note:** If you are using Authentication Manager 8.5 as a proxy server, enter the REST authentication API access key for Authentication Manager. See the Access Key row in the AM REST Mode Options table.
Agent Name	Specifies a name that is used to identify the agent in mobile notifications sent through the Cloud Authentication Service.
Access Policy	Specifies the exact name (including case sensitivity) of the Cloud Administration Console access policy that the agent will use. For information on viewing and adding access policies, see Manage Access Policies on RSA Link.

Option	Description
Request Timeout	Specifies the maximum number of seconds allowed for the agent to complete each transaction with the Cloud Authentication Service. Range: 1-180 Default: 180
Read Timeout	Specifies the maximum number of seconds allowed for the agent to connect to the Cloud Authentication Service and read the response. Range: 1-180 Default: 60
Retry Count	Specifies the number of times the agent will try to contact the Cloud Authentication Service if the first attempt is unsuccessful. Range: 1-5 Default: 1
Prompt for Windows Password after RSA SecurID Authentication	Specifies whether the agent prompts users for their Windows password after they complete all required SecurID authentication methods. By default, the agent prompts for Windows password first.
Enable Risk Collection	Specifies whether to enable collection of device fingerprint data and other information during authentication, which the Cloud Authentication Service can use to establish a level of identity confidence for a user. Access policies can use the Identity Confidence attribute to make it easier for users with high identity confidence to authenticate. See Condition Attributes for Access Policies on RSA Link for more information. **Note:** Regardless of this setting, the agent always collects initiating IP address, user agent, and HTTP header information during user authentication, which the Cloud Authentication Service can use to determine authentication requirements according to the configured access policy.
Enable Location Collection	Specifies whether to enable collection of HTML5 geolocation data during user authentication, which includes longitude, latitude, and a timestamp. Access policies can use the Trusted Location attribute to make it easier for users to authenticate from specific locations. For more information, see Condition Attributes for Access Policies on RSA Link. **Note:** Regardless of this setting, the agent always collects initiating IP address, user agent, and HTTP header information during user authentication, which the Cloud Authentication Service can use to determine authentication requirements according to the configured access policy.

Open the Manage SecurID Options Page

Open the Manage SecurID Options page to access settings that allow you to change authentication modes and configure other Agent for Citrix StoreFront features.

Procedure

1. Open the Citrix StoreFront Management Console on page 43.
2. In the **Stores list**, select a store for which Agent for Citrix StoreFront is configured as an authentication method.
3. Click **Manage Authentication Methods** in the **Action pane**.
4. Select **Manage SecurID Options** from the drop-down menu in the **Settings** column for RSA SecurID.

Enable an IP Address Override

If Agent for Citrix StoreFront is installed in AM UDP mode on a server that has multiple network interface cards and multiple IP addresses, and you plan to use different addresses to connect to Authentication Manager from the agent host at different times, you must:

- Register one IP address as the primary in Authentication Manager and designate it as the IP address override from the Manage SecurID Options page.
- Register the other IP addresses belonging to the agent host as secondary addresses in Authentication Manager.

For information about registering IP addresses in Authentication Manager, see Add an Authentication Agent on RSA Link.

Procedure

1. Open the Citrix StoreFront Management Console on page 43.
2. Open the Manage SecurID Options Page on the previous page.
3. Make sure AM UDP is selected in the **Authentication Mode** drop-down menu.
4. Click **Advanced Tools**.
5. Click **IP Address Override**.
6. In the **IP Address Override** field, enter the IP address that is designated as the primary address in Authentication Manager.
7. Click **OK**.

Clear the Node Secret

When the agent is installed in AM UDP mode, if the agent's node secret does not match the node secret on Authentication Manager, encrypted communications between Agent for Citrix StoreFront and Authentication Manager cannot occur. If this happens, you must clear the node secret on the agent and on Authentication Manager.

If the RSA Authentication Agent Auto-Registration service is installed, and 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 administrator uses the Security Console to unregister an instance of Agent for Citrix StoreFront in Authentication Manager, the node secret will become mismatched, and you will need to clear the node secret.

Procedure

1. Open the Citrix StoreFront Management Console on page 43.
2. Open the Manage SecurID Options Page on the previous page.
3. Make sure AM UDP is selected in the **Authentication Mode** drop-down menu.

4. Click **Clear Node Secret**.
5. Click **Yes**.
6. If the Auto-Registration service is disabled or not installed, clear the node secret for this agent from Authentication Manager. For instructions, see Refresh the Node Secret on RSA Link.

View the Server Environment Information

You can view information about your Authentication Manager server environment in the agent options to verify whether the environment is set up correctly.

Administrators typically view the server environment information to check the primary and replica Authentication Manager servers, and to check that Agent for Citrix StoreFront is communicating with the correct Authentication Manager server.

Procedure

1. On the Citrix StoreFront server, Open the Citrix StoreFront Management Console on page 43.
2. Open the Manage SecurID Options Page on page 49.
3. Make sure AM UDP is selected in the **Authentication Mode** drop-down menu.
4. Click **Server Environment**.
5. In the **Select server to view** field, leave the default server or select another one from the drop-down list, if applicable. If you select another server, click **Refresh** to view the information for that server.

Perform a Test Authentication

If the Agent for Citrix StoreFront is configured in AM UDP mode, you can perform a test authentication to verify that the agent can authenticate successfully. A test authentication sends a user name and RSA SecurID passcode to the configured 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

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

Procedure

1. On the Citrix StoreFront server, Open the Citrix StoreFront Management Console on page 43.
2. Open the Manage SecurID Options Page on page 49.
3. Make sure AM UDP is selected in the **Authentication Mode** drop-down menu.
4. Click **Advanced Tools**.
5. Click **Test Authentication**.
6. In the **User Name** field, leave the current user name or enter an appropriate name.
7. In the **SecurID Passcode** field, do one of the following:
   - If you have not set a SecurID PIN, enter the current tokencode. Click **OK**. The Set New RSA SecurID PIN dialog box opens. Go to step 8.
   - If you already have a SecurID PIN, enter the passcode. Click **OK**. Go to step 10, if necessary.
8. To set a PIN, follow the instructions in the Set New RSA SecurID PIN dialog box.
   - If Authentication Manager is configured to issue system-generated PINs, you will be prompted to memorize your new PIN, then click **OK**. If you click **Cancel**, the new PIN will not be set.

- 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**.

9. Once your PIN has been 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, and then enter the passcode. Click **OK**.
10. If you are prompted to enter the next tokencode to confirm your possession of the authenticator and synchronize it with Authentication Manager, wait for the tokencode to change on your authenticator. Enter the new tokencode in the **Next tokencode** field and click **OK**.

If you cannot authenticate, review your Authentication Manager settings on the Server Environment screen of the Manage SecurID Options page.

Enable Tracing

If Agent for Citrix StoreFront is installed in AM UDP mode, you can enable tracing 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**. You can change this location.

To configure logging when the agent is installed in AM REST or CAS mode, see Configure Logging Options for AM REST Mode or CAS Mode on page 40.

Procedure

1. On the agent host where issues are occurring, Open the Citrix StoreFront Management Console on page 43.
2. Open the Manage SecurID Options Page on page 49.
3. Make sure AM UDP is selected in the **Authentication Mode** drop-down menu.
4. Click **Advanced Tools**.
5. Click **Tracing**.
6. Configure the tracing settings as directed by Customer Support.
7. Click **OK**.

Change the Authentication Mode After Initial Installation

You can change the authentication mode for Agent for Citrix StoreFront after initial installation.

For example, if you are using Authentication Manager 8.5 as a secure proxy server to the Cloud Authentication Service, you might want the Cloud Authentication Service to handle all user authentication.

Procedure

1. Open the Citrix StoreFront Management Console on page 43
2. Open the Manage SecurID Options Page on page 49
3. From the **Authentication Mod**e drop-down menu, select the authentication mode you want to configure.
4. Configure agent settings for the authentication mode you selected as required for your deployment. For more information, see Manage Agent Settings on page 45.

Enable WPI for AM REST Mode After Initial Installation

If you did not enable WPI when you first installed the agent in AM REST mode, or if you changed to AM REST mode after initial installation, you can enable it at any time.

Procedure

1. Open the Citrix StoreFront Management Console on page 43.
2. Open the Manage SecurID Options Page on page 49.
3. Make sure AM REST is selected in the **Authentication Mode** drop-down menu.
4. Select **Enable Windows Password Integration (WPI)**.
5. Click **Manage WPI**.
6. If the agent was previously installed and configured in AM UDP mode and still uses the same agent name, select **Use Node Secret from UDP mode**, then proceed to step 10. Otherwise, proceed to step 7.
7. Click **Browse** and specify the directory location for the configuration file **sdconf.rec**.
8. Click **Browse** and specify the directory location for the node secret file ***<AgentName>_*** **NodeSecret.zip**.
9. In the **Enter the password with which _NodeSecret.zip was encrypted** field, enter the encryption password.
10. Click **OK**.

Note: You must also enable WPI for Agent for Citrix StoreFront from the offline authentication policy settings in the Security Console.

Chapter 5: Citrix Delegated Forms Authentication

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 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 Agent for Citrix StoreFront. See Enable or Disable RSA SecurID Authentication on page 45.
2. Enable DFA on Citrix StoreFront and protect DFA with RSA SecurID, as described in Enable RSA SecurID Authentication for DFA below.
3. Apply custom scripts to enable NetScaler themes to support RSA SecurID authentication. See Apply RSA SecurID Authentication Scripts to NetScaler Themes on page 58.
4. Configure NetScaler Gateway to use DFA to authenticate to Citrix StoreFront.
   See the DFA configuration steps described in the RSA Ready Technology Integrations *SecurID Access Implementation Guide for Citrix NetScaler Gateway* on RSA Link at https://community.rsa.com/docs/DOC-66800.
5. 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

Perform the following procedure to enable 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. To add the Custom Forms protocol to DFA, enter the following command:

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

3. To protect DFA with RSA SecurID authentication, enter the following command:

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

4. (Optional) If the User IDs of your RSA Authentication Manager users are not fully qualified and you want to protect DFA with RBA, you need to configure Trusted Domains for DFA. Enter the following command:

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

Disable RSA SecurID Authentication for DFA

Perform the following procedure to disable SecurID authentication for DFA.

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

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. To reset DFA protection to default Citrix username and password authentication, enter the following command:

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

3. To remove the Custom Forms protocol from DFA, enter the following command:

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

4. (Optional) To clear the Trusted Domains for DFA, enter the following command:

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

Apply RSA SecurID Authentication Scripts to NetScaler Themes

Before Agent for Citrix StoreFront can provide RSA SecurID authentication through Citrix NetScaler, you must manually modify user portal theme files and scripts on the NetScaler appliance.

Note: Agent for Citrix StoreFront supports only the "RfWebUI" and "X1" NetScaler themes, or custom themes created using those themes as templates.

Before you begin

- Copy **open-sans.woff**, **SecurID.js**, and **SecurID.css** from the NetScaler folder in the agent installation directory on the Citrix StoreFront server to a location on the NetScaler appliance.
- (Optional) If you want to use a custom theme, create a new portal theme on the NetScaler appliance using either "RfWebUI" or "X1" as a theme template (theme-copy), then bind the theme to the virtual server and apply it. See your Citrix documentation for more information.

Procedure

1. Log onto the NetScaler appliance.
2. Copy **open-sans.woff** to one of the following directories, depending on your theme:
    - For default themes: **/var/netcscaler/logon/LogonPoint/custom/**
    - For custom themes: **/var/netcscaler/logon/themes/theme-copy/**
3. In the same directory, append the contents of **SecurID.css** and **SecurID.js** to **the style.css** and **script.js** files, respectively.

Chapter 6: Enabling Authentication Manager Risk-Based Authentication

Enabling RSA Authentication Manager Risk-Based Authentication

When Agent for Citrix StoreFront is installed in AM UDP mode, you can enable Authentication Manager Risk-Based Authentication (RBA) to protect logon to Citrix StoreFront by users who authenticate through NetScaler Gateway. 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 Agent for Citrix StoreFront. See Manage RSA SecurID Authentication Using the Citrix StoreFront Management Console on page 43.
2. Enable Citrix Delegated Forms Authentication (DFA) to extend RSA SecurID authentication through NetScaler Gateway. See Citrix Delegated Forms Authentication on page 56.
3. Install the RSA Risk-Based Authentication Helper web application to provide a connection point between RBA authentication and Agent for Citrix StoreFront. See Install the RBA Helper below.
4. Integrate Authentication Manager and NetScaler Gateway with Agent for Citrix StoreFront. For instructions, see the RSA Ready Technology Integrations *SecurID Access Implementation Guide for Citrix NetScaler Gateway* on RSA Link at https://community.rsa.com/docs/DOC-66800.

Authentication Manager Risk-Based Authentication Helper

The Authentication Manager Risk-Based Authentication Helper (RBA Helper) is a web application that connects Authentication Manager RBA and Agent for Citrix StoreFront. The RBA Helper installer is available as part of 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 use the Install Wizard or the command line.

Note: Agent for Citrix StoreFront supports RBA Helper version 1.5 or later. You do not need to install a new version of RBA Helper if version 1.5 or later is already installed.

Security Recommendations

The RBA Helper must be accessed through HTTPS in order to integrate Authentication Manager RBA with 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. For information on configuring IIS to use HTTPS, see the Microsoft IIS documentation website at http://www.iis.net. Search on *TLS/SSL*.

RSA also recommends that you configure the Microsoft TLS/SSL Security Provider (used by IIS) to use Transport

Layer Security (TLS) v1.2 or later. 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

Perform the following procedure to install the RBA Helper using the install wizard.

Before you begin

- Confirm that you have addressed the security recommendations.
- 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 the download package containing **RSA Authentication Manager Risk-Based Authentication Helper x64.msi** to a folder on the computer where you want to install the RBA Helper.

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.

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 and accept the License Agreement or click **Print** to print it. Click **Next**.
4. Click **Install**.
5. When installation completes, click **Finish**.

After you finish

Verify That RBA Helper is Working on the next page

Install Using Command-Line Options

You can install the RBA Helper from the command line.

Before you begin

- Confirm that you have addressed the security recommendations.
- 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 the download package containing **RSA Authentication Manager Risk-Based Authentication Helper x64.msi** to a folder on the computer where you want to install the RBA Helper.

Procedure

1. Open an administrator command prompt.
2. Navigate to the folder where you copied the installer file, or 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>"
     ```

   If the specified site does not exist, the installer installs the RBA Helper to the default web site.

After you finish

Verify That RBA Helper is Working below

Verify That RBA Helper is Working

After installing the RBA Helper, perform the following procedure to verify that it is working.

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.
4. Right-click **RSAAuthMgrRbaHelper**.
5. Confirm that **Manage Application** appears as an option in the context menu.

Chapter 7: Troubleshooting

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.

Installation and Uninstallation Issues

If the installation or uninstallatoin does not succeed, examine your log file (for example, **%USERPROFILE%\install.log**) 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.	Contact Citrix to download and install Citrix StoreFront. Restart the installation program.
Microsoft .NET Framework 4.5 or later is not installed.	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.
Agent for Citrix StoreFront cannot be uninstalled if Citrix StoreFront has already been uninstalled.	Reinstall Citrix StoreFront and close the Citrix StoreFront MMC (which opens automatically). Uninstall Agent for Citrix StoreFront and then uninstall Citrix StoreFront.
The Citrix StoreFront Management Console stops responding if it is running during Agent for Citrix StoreFront installation.	Close the Citrix StoreFront Management Console before installing Agent for Citrix StoreFront.

Interface Issues

This section describes issues related to interface components used by Agent for Citrix StoreFront.

Problem	Resolution
Shared Citrix StoreFront stores do not display the updated Agent for Citrix StoreFront configuration interface after the agent is upgraded from version 1.5 to 2.0	Do the following: Disable and then re-enable RSA SecurID authentication for the shared store. For more information, see Enable or Disable RSA SecurID Authentication on page 45.
SecurID Citrix StoreFront Agent fails to load Citrix management console (MMC) on Windows Server	To solve this issue, you must import the DigiCert Trusted Root G4 certificate. **Problem**: On Windows Server 2012 R2 systems that do not

Problem	Resolution
	have have direct access to the Microsoft Updates site, the Citrix StoreFront management console (MMC) fails to load. This is because the digital signature of an RSA PowerShell script is rooted in a Digicert-issued certificate authority that is not included in the set of Trusted Root Certification Authorities that shipped 'in-box' on Server 2012 R2. **Workaround**: Obtain the the 'DigiCert Trusted Root G4' from digicert.com and use the MMC 'Certificates' snap-in to import it to the Computer's 'Trusted Root Certification Authorities' store.

Coexistence with RSA Authentication Agent for Microsoft Windows Issues

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

Problem	Resolution
Offline Authentication for the Windows Agent is unavailable when both agents are installed.	Agent for Citrix StoreFront disables the download of offline data. To re-enable this function: 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**.
After uninstalling either agent, the **OASVC_LOCAL** service cannot be restarted.	Repair the installation for the authentication agent that is still installed on the Citrix StoreFront server. To repair Agent for Citrix StoreFront, see Repair an Installation on page 33.
After an administrator clears the node secret using RSA Control Center for the Windows Agent, Citrix StoreFront authentication fails in AM UDP mode, and the Citrix Agent displays a node secret mismatch error.	Do the following: 1. Restart **AuthAPIService** and **sdadmreg** on the Citrix StoreFront server. 2. Perform a test authentication using RSA Control Center for the Windows Agent.
After an administrator clears the node secret using RSA Control Center for the Windows Agent, WPI stops working for the Citrix Agent in AM REST mode. This issue occurs only if the Windows Agent and Citrix	Do the following: 1. Perform a test authentication using RSA Control Center for the Windows Agent. 2. In the Manage SecurID Options page for the Citrix Agent, click **Manage WPI**, then select **Use Node Secret from UDP mode**.

Problem	Resolution
Agent use the same Agent Name.	
After an administrator clears the node secret for the Citrix Agent in AM UDP mode, Windows Agent authentication fails. This issue occurs only if Agent Auto-registration is installed for the Windows Agent.	Restart sdadmreg on the Citrix StoreFront server.
After an administrator clears the node secret or generates a new node secret for the Citrix Agent in AM REST mode, Windows Agent authentication fails, and the Windows Agent displays the error message "Node secret mismatch: cleared on agent but not in server". This issue occurs only if the Windows Agent and Citrix Agent use the same Agent Name.	Do the following: 1. Clear the node secret for the Windows Agent in Authentication Manager. 2. Perform a test authentication using RSA Control Center for the Windows Agent. 3. In the Manage SecurID Options page for the Citrix Agent, click **Manage WPI**, then select **Use Node Secret from UDP mode**.
Windows Agent services stop after changing the Citrix Agent authentication mode.	Repair the Windows Agent installation.

Delegated Forms Authentication (DFA) Issues

This section describes issues related to DFA.

Problem	Resolution
If an optional tenantID was set when the DFA server was installed, PowerShell commands that rely on the VirtualPath fail.	Include the tenantID for commands that rely on VirtualPath. For example: Replace: (Get-STFAuthenticationService -VirtualPath /Citrix/DelegatedForms/Default) with: (Get-STFAuthenticationService -VirtualPath /Citrix/DelegatedForms/[tenantID]/Default)

Logging Issues

This section describes issues related to logs generated by Agent for Citrix StoreFront.

Problem	Resolution
Changes to logging configuration or to options in the Citrix StoreFront management console are not reflected in the agent logs when custom forms are enabled.	Disable and then re-enable custom forms.
If Agent for Citrix StoreFront is configured in AM UDP mode and the tracing is set to save logs to a custom location, the logs folder is not automatically deleted when the agent is uninstalled.	Manually delete the custom log directory after uninstalling the agent.

Authentication Issues

This section describes issues related to authentication and procedures you can use to help resolve them.

Issue	Resolution
Authentication Manager and the agent host cannot communicate. The Agent for Citrix StoreFront is installed in AM UDP mode.	Authentication Manager and the agent host might not have compatible copies of the system configuration file (**sdconf.rec**). Make sure you have the correct **sdconf.rec** file: 1. Open the Citrix StoreFront Management Console on page 43. 2. Open the Manage SecurID Options Page on page 49. 3. Make sure AM UDP is selected in the **Authentication Mode** drop-down menu. 4. Click **Server Environment**. The left side of the dialog box displays information about the status of the Authentication Manager server and how it communicates with the agent.
You receive an "Unable to retrieve server environment" error message when attempting to verify the system configuration (**sdconf.rec**) file using the Server Environment option on the Manage SecurID Options page and the Agent for Citrix StoreFront is installed in AM UDP mode.	The **sdconf.rec** file is corrupt and must be replaced. 1. Obtain a new **sdconf.rec** file from 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. **Note:** Make sure that your anti-spyware or anti-virus software does not automatically remove the node secret or **sdconf.rec** file.
You are experiencing authentication problems when the Agent for Citrix StoreFront is installed in AM UDP mode.	You may need to replace a corrupt **server.cer** file to resolve authentication problems.

Issue	Resolution
	1. Obtain a new **server.cer** file from 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.
The agent does not log location details when users authenticate using Mozilla Firefox.	Instruct users to enable geolocation collection in FireFox using the following steps: 1. Enter about:config from the address bar. 2. Change the value for geo.wifi.ui to: https://location.services.mozilla.com/v1/geolocate?key=test
After changing the authentication mode from AM REST to AM UDP, authentication fails, and the agent displays the error message "Node secret mismatch: cleared on agent but not on server".	Clear the node secret for the agent in the Authentication Manager Security Console, then perform a test authentication from the Manage SecurID Options page of the Citrix StoreFront management console. For more information, see Perform a Test Authentication on page 51.
Authentication fails in AM REST mode, and Citrix StoreFront displays the error message "Cannot complete your request".	Do the following: • Check the agent logs for certificate validation errors and import valid trusted root certificates if necessary. For more information, see Import the Trusted Root Certificate for Authentication Manager or the Cloud Authentication Service on page 20. • Check the agent logs for REST config file errors and repair the agent installation if necessary. For more information, see Repair an Installation on page 33.

Diagnosing RSA Authentication Manager Risk-Based Authentication Helper Issues

You can perform tasks to diagnose issues that you might encounter when supporting integration with Authentication Manager risk-based authentication (RBA).

An initial task is enabling tracing. For more information, see Enable Tracing on page 52. Additional tasks are described below.

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

If Agent for Citrix StoreFront is installed in AM UDP mode, error and event messages are written to the Windows Event Viewer in the following categories:

- ACECLIENT
- AuthAPIService
- RSA Agent Auto Registration
- RSA Authentication Agent Auto-Registration
- 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 Automatic Load Balancing on page 72.
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 Automatic Load Balancing on page 72.
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 Automatic Load Balancing on page 72.
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 might have been installed incorrectly or **aceclnt.dll**

Message	Description
	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 Authentication Manager. Ask your Authentication Manager administrator for a new copy of **sdconf.rec**.
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 an unplugged network cable.
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.	The identity of the Authentication Manager could not be verified by Authentication Agent. 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*>: 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 Automatic Load Balancing on page 72.

Appendix A: Configuring Automatic Load Balancing for AM UDP Mode

Automatic Load Balancing

If Agent for Citrix StoreFront is installed in AM UDP mode, you configure the Authentication Agent to automatically balance authentication request loads by creating a load balancing options file (**sdopts.rec**). 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. You must log on as an administrator if you plan to modify the **sdopts.rec** file.

Note: Load balancing is not configurable in CAS mode. In AM REST mode, you select a load balancing scheme when you install the agent or configure agent settings. For more information, see Manage Agent Settings on page 45

Dynamic Load Balancing

With dynamic load balancing, the Authentication Agent sends a time request to each Authentication Manager server in the realm and determines a priority list based on the response time of each 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 the Authentication Agent sends another time request or times out.

To perform dynamic load balancing, the 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 the 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 Create an sdopts.rec File below.

Manual Load Balancing

With manual load balancing, you specify the Authentication Manager server that each Authentication Agent host uses. You also assign a priority to each Authentication Manager server so the 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 Create an sdopts.rec File below.

Manage the Load Balancing Configuration File (sdopts.rec)

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.

Note: Each time you modify the **sdopts.rec** file, restart the 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 77. The Authentication Agent ignores this setting if the IP override is already set through the **Advanced Tools** option on the Manage SecurID Options page.
  - **USESERVER=ip_address, priority**. Specifies an Authentication Manager server to receive authentication requests from the Authentication Agent host according to a specified priority value. Use one setting for each 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. You must assign a priority to each Authentication Manager server that you add to the **sdopts.rec** file. Otherwise, the entry is invalid.

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

    Each **USESERVER** keyword value must consist of the actual Authentication Manager IP address separated by a comma from the assigned priority. The priority specifies if or how often an 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 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 Authentication Manager server only if no Authentication Manager servers of higher priority are available.
0	Ignore this Authentication Manager server. Use Priority 0 only under these circumstances: • The server must be one of the four Authentication Manager servers listed in the **sdconf.rec** file. • The server is only used for the initial authentication of Authentication Agent, unless all Authentication Manager servers with priorities of 1–10 in the **sdopts.rec** file are known as unusable to Authentication Agent. • Generally, priority 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.

Priority	Meaning
	Note: You must enter keywords in uppercase. • If none of the servers with **USESERVER** statements are responsive, then the default server is either the master (if one exists) or the Authentication Manager server used to create the **sdconf.rec** file.

The IP addresses in the file are verified against the list of valid Authentication Manager servers that the 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 aliases in the **sdopts.rec** file.

  The **ALIAS** keyword value contains the actual IP address for the Authentication Manager server, followed by up to three aliases for that Authentication Manager server. The 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 Authentication Manager server. In addition, the actual IP address must be included on any Authentication Manager server list received by the Authentication Agent. The Authentication Manager server list provides actual and alias IP addresses for all known Authentication Manager servers in the realm. The 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 Authentication Manager server as the value, this keyword instructs the Authentication Agent to use only the alias IP addresses to contact Authentication Manager.

  When you do not provide a value, this keyword instructs the Authentication Agent to send requests only to the 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 76. (If you use this keyword, make sure that at least one 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 in the **sdopts.rec** and **sdconf.rec** files, or on the 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 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 76.

  Specify an actual IP address as the value to instruct the Authentication Agent to use only the actual IP address to contact Authentication Manager.

- **AVOID=ip_address**. Specify an actual IP address of an Authentication Manager server to instruct the Authentication Agent to exclude this Authentication Manager server from use during dynamic load balancing.

  Note: 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 can use the **AVOID** keyword in the **sdopts.rec** file with an actual IP address of an Authentication Manager server as a value to instruct the Authentication Agent to exclude this Authentication Manager server from use during dynamic load balancing.

Note: 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 Authentication Manager server, the statement is ignored unless another Authentication Manager server is available. The default Authentication Manager server is where the **sdconf.rec** file was created. If an Authentication Manager server is designated as the master, however, the master 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 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 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 Create an sdopts.rec File on page 72.

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 do not affect 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.

Note: The Authentication Agent ignores this setting if the IP override is already set through the **Advanced Settings** option on the Manage SecurID Options page. For more information, see Manage Agent Settings on page 45.

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. The default is to use alias or actual IP addresses, with some exceptions. The 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. 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 Authentication Manager server.

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

```
;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 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 instruct the Authentication Agent to send requests to the Authentication Manager server 192.168.10.23 and 192.168.10.22 using only 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 instructs the Authentication Agent to send requests to the Authentication Manager server 192.168.10.23 and 192.168.10.22 using only actual IP addresses.

Specify an Overriding IP Address

When the 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 the Authentication Agent and 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 Authentication Manager, making communication between the 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 Install the Agent on page 26.

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.

Note: The Authentication Agent ignores this setting if the IP address override option is set on the Manage SecurID Options page. However, if you installed the Auto-Registration utility, the address that the utility registers overrides the IP setting on the Manage SecurID Options page. (The **IP address override setting** field also appears inactive after you install the Auto-Registration utility.) For more information, see Manage Agent Settings on page 45.