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

Dell, RSA, the RSA Logo, EMC and other trademarks, are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

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

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

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

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA 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 Dell software described in this publication requires an applicable software license.

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

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

Copyright © 2007-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

May 2018

Revised: March 2019
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision History</td>
<td>7</td>
</tr>
<tr>
<td>Preface</td>
<td>9</td>
</tr>
<tr>
<td>Audience</td>
<td>9</td>
</tr>
<tr>
<td>Support and Service</td>
<td>9</td>
</tr>
<tr>
<td>RSA Ready Partner Program</td>
<td>9</td>
</tr>
<tr>
<td><strong>Chapter 1: Overview</strong></td>
<td>11</td>
</tr>
<tr>
<td>About RSA Authentication Agent for AD FS</td>
<td>12</td>
</tr>
<tr>
<td>When to Use Agent for AD FS</td>
<td>12</td>
</tr>
<tr>
<td>Feature Support</td>
<td>13</td>
</tr>
<tr>
<td>Language Support</td>
<td>13</td>
</tr>
<tr>
<td><strong>Chapter 2: Preparing for Installation</strong></td>
<td>15</td>
</tr>
<tr>
<td>Requirements and Compatibility</td>
<td>16</td>
</tr>
<tr>
<td>Operating System and AD FS Version Requirements</td>
<td>16</td>
</tr>
<tr>
<td>Network Requirements</td>
<td>16</td>
</tr>
<tr>
<td>RSA Authentication Manager Compatibility</td>
<td>16</td>
</tr>
<tr>
<td>RSA SecurID Authenticator and Device Requirements</td>
<td>16</td>
</tr>
<tr>
<td>Web Browser Compatibility</td>
<td>16</td>
</tr>
<tr>
<td>Configuration Settings and Required Information</td>
<td>17</td>
</tr>
<tr>
<td>Prepare Users for RSA SecurID Access Authentication</td>
<td>19</td>
</tr>
<tr>
<td>RSA Authentication Manager Mode</td>
<td>19</td>
</tr>
<tr>
<td>Cloud Authentication Service Mode</td>
<td>19</td>
</tr>
<tr>
<td><strong>Chapter 3: Installing the Agent</strong></td>
<td>21</td>
</tr>
<tr>
<td>Installation Methods</td>
<td>22</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>22</td>
</tr>
<tr>
<td>Install the Agent Using the Install Wizard</td>
<td>22</td>
</tr>
<tr>
<td>Create a Configuration Input File for Command Line Installation</td>
<td>23</td>
</tr>
<tr>
<td>Install the Agent Using the Command Line</td>
<td>24</td>
</tr>
<tr>
<td>Next Steps</td>
<td>25</td>
</tr>
<tr>
<td><strong>Chapter 4: Configuring and Managing the Agent</strong></td>
<td>27</td>
</tr>
<tr>
<td>Register the Agent in RSA Authentication Manager</td>
<td>28</td>
</tr>
<tr>
<td>Register or Unregister the Agent with Microsoft AD FS</td>
<td>28</td>
</tr>
</tbody>
</table>
Diagnose Authentication Issues ................................................................. 42
Verify the Accuracy of the Computer Clock .............................................. 42
Errors and Log Messages ........................................................................... 42
Agent Log Messages .................................................................................. 42
User-Facing Error Messages .................................................................... 43
Event Viewer Messages ............................................................................. 44
# Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Date</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>June 2018</td>
<td>Added more details about the REST server URL and the client key for the two REST Protocol authentication modes.</td>
</tr>
<tr>
<td>2</td>
<td>August 2018</td>
<td>Added a link to a knowledgebase article for exporting trusted root CA certificate.</td>
</tr>
<tr>
<td>3</td>
<td>October 2018</td>
<td>Corrected syntax errors in terminal commands for launching agent configuration utilities.</td>
</tr>
<tr>
<td>4</td>
<td>December 2018</td>
<td>Added new topic <a href="#">When to Use Agent for AD FS on page 12</a>, which describes ideal use cases and differentiating features for the agent as compared to SAML integration for AD FS. Corrected a URL and added clarification for a procedure step in <a href="#">Test MFA on Windows Server 2016 in Desktop Experience Mode on page 30</a>.</td>
</tr>
<tr>
<td>5</td>
<td>March 2019</td>
<td>Added details about case sensitivity of specified Cloud Authentication Service access policy.</td>
</tr>
</tbody>
</table>
Preface

Audience

This guide is for network and system administrators who deploy, configure, and manage RSA Authentication Agent for Microsoft AD FS.

The document assumes you have experience using Microsoft Active Directory® Federation Services (AD FS) for Windows Server®. It also assumes you have experience with RSA 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 www.rsaready.com provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.
Chapter 1: Overview

About RSA Authentication Agent for Microsoft AD FS ......................................................... 12
When to Use Agent for AD FS .......................................................................................... 12
Feature Support ............................................................................................................... 13
Language Support .......................................................................................................... 13
About RSA Authentication Agent for Microsoft AD FS

RSA Authentication Agent for Microsoft AD FS is authentication software that connects your Microsoft Active Directory Federation Services (AD FS) server to RSA SecurID Access using the REST protocol to provide multifactor authentication capabilities for AD FS.

When a user attempts to access an AD FS-protected resource, the user enters username and password credentials for primary authentication. Agent for AD FS then prompts the user to complete one or more additional authentication methods, depending on the configured authentication mode.

Agent for AD FS supports these authentication modes:

- **RSA Authentication Manager.** Connects the agent to an existing RSA Authentication Manager instance in your deployment, making the SecurID Token method available for user authentication. You use the Operations Console, Security Console, and Self-Service Console to manage identity sources, users, and tokens.

- **Cloud Authentication Service.** Connects the agent to the RSA SecurID Access Cloud Authentication Service, making the Authenticate Tokencode, Approve, Device Biometrics, SMS Tokencode, and Voice Tokencode methods available. If Authentication Manager is integrated with the Cloud Authentication Service, RSA SecurID Token can also be used to authenticate in this mode. You use the Cloud Administration Console to manage identity sources, users, access policies, and authentication methods.

  **Note:** RSA recommends Cloud Authentication Service mode for most deployments. For a complete list of features and benefits, see Cloud Authentication Service Overview on RSA Link.

When to Use Agent for AD FS

There are two distinct integration methods by which you can connect your Microsoft AD FS environment to the Cloud Authentication Service:

- RSA Authentication Agent for Microsoft AD FS (the agent described in this document)
- SAML identity provider configuration

For most scenarios, RSA recommends using Agent for AD FS.

By integrating Microsoft AD FS with the Cloud Authentication Service using the agent, you can continue to use your AD FS environment for authentication and SSO, while adding advanced RSA authentication methods for additional security. When authenticating through the agent, users have a streamlined experience that is presented entirely within the AD FS authentication interface.

In a SAML identity provider configuration, users are redirected from the AD FS interface to the RSA SecurID Access interface and back again, resulting in a functional but less-streamlined experience. If either of the following conditions apply to your deployment, RSA recommends using SAML identity provider configuration:

- You need to use FIDO token authentication (the agent does not support FIDO)
- You do not want to install or maintain additional software on your AD FS servers (the agent must be installed on each AD FS server)

For more information on using SAML identity provider configuration to integrate Microsoft AD FS with the Cloud Authentication Service, see https://community.rsa.com/docs/DOC-79812.
Feature Support

RSA Authentication Agent for Microsoft AD FS supports the following features:

- RSA SecurID Token authentication through RSA Authentication Manager using the REST protocol
- Up to 15 RSA Authentication Manager replicas
- Agent reporting (agent sends hostname, agent version, and operating system version to Authentication Manager 8.3 or later)
- Multifactor authentication through the Cloud Authentication Service using the REST protocol, with support for these methods:
  - RSA SecurID Token
  - RSA SecurID Authenticate Tokencode
  - Approve
  - Device Biometrics
  - SMS Tokencode
  - Voice Tokencode
- Supports TLS 1.2 encryption protocol (exclusively)
- Supports FIPS-enabled operating system environment
- Collection of risk and location data for use with Cloud Authentication Service access policies.

The following features are not supported by Agent for AD FS:

- FIDO token authentication
- Authentication method combinations that include FIDO token
- RSA SecurID authentication using legacy RSA SecurID UDP protocol
- RSA SecurID authentication using RADIUS protocol
- On-Demand authentication using native RSA SecurID protocol
- On-Demand authentication using RADIUS protocol
- Risk-based authentication through RSA Authentication Manager
- Risk-based authentication with single sign-on through RSA Authentication Manager
- Secondary RADIUS server support
- RSA SecurID software token automation
- RSA SecurID 800 Authenticator automation
- RSA SecurID protection of administrative interface

**Note:** It is not possible to upgrade older versions of Agent for AD FS to version 2.0.

Language Support

Localized (translated) authentication web pages for Authentication Agent for AD FS are available on RSA Link. You must download and enable the localized pages to make non-English languages available to users. When enabled, the localized pages display according to the language preferences set for the user's web browser. For instructions, see Add Localized Authentication Pages on page 34.
Localized pages are provided for US English and the following languages:

- French (fr)
- German (de)
- Italian (it)
- Japanese (ja)
- Korean (ko)
- Portuguese (pt)
- Russian (ru)
- Simplified Chinese (zh-Hans)
- Spanish (es)
Chapter 2: Preparing for Installation

Requirements and Compatibility ................................................................. 16
Configuration Settings and Required Information ........................................ 17
Prepare Users for RSA SecurID Access Authentication ................................ 19
Requirements and Compatibility

Before deploying RSA Authentication Agent for Microsoft AD FS, make sure your environment meets the following requirements.

Operating System and AD FS Version Requirements

<table>
<thead>
<tr>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012 R2 (Server Core or Desktop Experience) with AD FS 3.0</td>
<td>Windows Server 2016 (Server Core or Desktop Experience) with AD FS 4.0</td>
</tr>
</tbody>
</table>

**Note:** You must have system administrator privileges on the AD FS server, and Microsoft Active Directory Services must be running before you install Agent for AD FS.

Network Requirements

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5555</td>
<td>Used by default for REST protocol communication between the agent and Authentication Manager primary and replica instances when the agent is configured in Authentication Manager mode. The Authentication Manager administrator can change which port is used for this purpose.</td>
</tr>
<tr>
<td>443</td>
<td>Used for REST protocol communication between the agent and the Cloud Authentication Service when the agent is configured in Cloud Authentication Service mode.</td>
</tr>
</tbody>
</table>

RSA Authentication Manager Compatibility

RSA Authentication Manager 8.3 or later is required when Agent for AD FS is deployed in RSA Authentication Manager mode. Authentication Manager must be deployed and running before you install the agent.

RSA SecurID Authenticator and Device Requirements

Users must have an RSA SecurID hardware or software token to successfully authenticate when the agent is deployed in RSA Authentication Manager mode. RSA SecurID tokens are enabled in Authentication Manager.

For Cloud Authentication Service mode, users must install and register the RSA SecurID Authenticate app on a compatible device to authenticate using the Approve, Device Biometrics, or Authenticate Tokencode methods. SMS Tokencode and Voice Tokencode require that the user’s phone number is recorded in an identity source connected to RSA SecurID Access, and the phone number attribute is synchronized with the Cloud Authentication Service. To use the RSA SecurID Token method, 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 AD FS users.

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

Web Browser Compatibility

RSA has verified Authentication Agent for AD FS compatibility with the following web browsers:

- Internet Explorer (11)
- Google Chrome (66)
- Mozilla Firefox (58)
- Safari on Yosemite (9.1)
- Safari on iOS (11.3.1)
- Android Web Browser on Android 7.0

**Note:** JavaScript must be enabled in the browser.

## Configuration Settings and Required Information

You configure the basic settings required to set up the agent using the installer. You can edit those settings and additional options from the Agent for AD FS Configuration Utility after installing the agent. For instructions, see [Edit Settings Using the Agent for AD FS Configuration Utility on page 35](#).

The following table describes how to configure each setting. Before you install the agent, review these settings and obtain the necessary configuration information from your RSA Authentication Manager or Cloud Authentication Service administrator.

**Note:** The settings you can configure depend on the authentication mode you select.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Mode</td>
<td>Select an authentication mode:</td>
</tr>
<tr>
<td></td>
<td>- <strong>RSA Authentication Manager.</strong> Connects the agent to an existing RSA Authentication Manager instance in your deployment, making the SecurID Token method available for user authentication. You use the Operations Console, Security Console, and Self-Service Console to manage identity sources, users, and tokens.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Cloud Authentication Service.</strong> Connects the agent to the RSA SecurID AccessCloud Authentication Service, making the Authenticate Tokencode, Approve, Device Biometrics, SMS Tokencode, and Voice Tokencode methods available. If Authentication Manager is integrated with the Cloud Authentication Service, RSA SecurID Token can also be used to authenticate in this mode. You use the Cloud Administration Console to manage identity sources, users, access policies, and authentication methods.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> RSA recommends Cloud Authentication Service mode for most deployments. For a complete list of features and benefits, see <a href="#">Cloud Authentication Service Overview</a> on RSA Link.</td>
</tr>
<tr>
<td>Server URL</td>
<td>Enter the REST authentication URL for either the Cloud Authentication Service or your primary Authentication Manager instance using the following format: <a href="https://HOSTNAME:PORT/mfa/v1/">https://HOSTNAME:PORT/mfa/v1/</a>_</td>
</tr>
<tr>
<td></td>
<td>For Authentication Manager, obtain the <strong>HOSTNAME</strong> value from the <strong>Fully Qualified Domain Name</strong> field on the <strong>Administration &gt; Network &gt; Appliance Network Settings</strong> page of the Operations Console. The default <strong>PORT</strong> is 5555.</td>
</tr>
<tr>
<td></td>
<td>For the Cloud Authentication Service, obtain the <strong>HOSTNAME</strong> value from the <strong>Authentication Service Domain</strong> field on the <strong>Registration</strong> tab of the settings page for any identity router in the Cloud Administration Console. The default <strong>PORT</strong> is 443.</td>
</tr>
<tr>
<td>Access Key</td>
<td>Enter the REST authentication API access key for either RSA Authentication Manager or the Cloud Authentication Service, depending on your authentication mode.</td>
</tr>
<tr>
<td></td>
<td>To obtain the API access key, see the following on RSA Link:</td>
</tr>
<tr>
<td></td>
<td>- For RSA Authentication Manager, see <a href="#">Configure the RSA SecurID Authentication API for</a></td>
</tr>
</tbody>
</table>

Chapter 2: Preparing for Installation
<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Agents.</strong></td>
<td>- For the Cloud Authentication Service, see Add an RSA SecurID Authentication API Key.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Enter a name for the agent. The name you specify is used to identify the agent in Authentication Manager or in mobile notifications sent through the Cloud Authentication Service.</td>
</tr>
</tbody>
</table>
| Replica Server URLs | Enter the REST authentication URLs for the Authentication Manager replica instances in your deployment. If communication with the primary instance is interrupted, the agent attempts to connect to each replica in the order that they are configured.  
In the Install Wizard, you enter the URL for one replica at a time and click + to add it to the list, or select a URL from the list and click - to remove it.  
In the configuration utility, choose an option for configuring replica server URLs:  
**Add Replica URL.** Enter each replica URL when prompted.  
**Modify Existing Replica URL.** Enter the number of the URL you want to modify from the list, then enter the modified URL when prompted.  
**Delete Replica URL.** Enter the number of the URL you want to delete from the list. |
| Access Policy       | Enter the exact name (including case sensitivity) of the access policy that the agent will use as specified in the Cloud Administration Console. For information on viewing and adding access policies, see Manage Access Policies on RSA Link. |
| Request Timeout     | Enter the maximum number of seconds allowed for the agent to complete each transaction with Authentication Manager or the Cloud Authentication Service.  
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        | Enter the maximum number of seconds allowed for the agent to connect to the authentication server and read the response.  
Range: 1-180  
Default: 60 |
| Retry Count         | Enter the number of times the agent will try to contact the Cloud Authentication Service or an Authentication Manager instance if the first attempt is unsuccessful.  
If the agent is in Authentication Manager mode and replicas are configured, the agent attempts to contact the next replica when the retry count is reached. When the retry count is reached in Cloud Authentication Service mode, the connection fails.  
Range: 1-5  
Default: 3 |
| Server Refresh Interval | Enter the number of minutes between polling attempts to determine whether the Authentication Manager service is available.  
Minimum: 5 |
### Prepare Users for RSA SecurID Access Authentication

Before installing Agent for AD FS, complete the preparation tasks for the authentication mode you will configure.

**RSA Authentication Manager Mode**

- Assign hardware or software authenticators (tokens).
- Register users as RSA SecurID users in the Authentication Manager database and activate their tokens.
- Distribute hardware or software tokens. Provide instructions for importing a software token to the RSA SecurID app on new software token users’ devices.
- Provide instructions for setting a PIN. Agent for AD FS supports User-Created PIN and System-Generated PIN.
- Provide authentication instructions.

For instructions and guidance, see the [Authentication Manager 8.3 Administrator’s Guide](#) on RSA Link.

**Cloud Authentication Service Mode**

- Instruct users to install the RSA SecurID Authenticate app from the Apple App Store, Google Play, or Microsoft Store and complete device registration if they will authenticate using the Approve, Device Biometrics, or Authenticate Tokencode methods.
- If users will authenticate using the SMS Tokencode or Voice Tokencode methods, make sure each user’s phone number is registered with the Cloud Authentication Service. The SecurID Authenticate app and mobile device registration are not required for these authentication methods.
- If RSA Authentication Manager is integrated with the Cloud Authentication Service and users will authenticate using RSA SecurID tokens, assign, activate, and distribute tokens as described for RSA
Authentication Manager Mode above.

- Provide authentication instructions.

For instructions and guidance, see Cloud Authentication Service Help on RSA Link.
Chapter 3: Installing the Agent

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Methods</td>
<td>22</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>22</td>
</tr>
<tr>
<td>Install the Agent Using the Install Wizard</td>
<td>22</td>
</tr>
<tr>
<td>Create a Configuration Input File for Command Line Installation</td>
<td>23</td>
</tr>
<tr>
<td>Install the Agent Using the Command Line</td>
<td>24</td>
</tr>
<tr>
<td>Next Steps</td>
<td>25</td>
</tr>
</tbody>
</table>
Installation Methods

Install the agent using one of the following methods:

- **Install Wizard.** The Install Wizard guides you through the installation process. Run the Install Wizard on each AD FS server in your deployment.
- **Command Line.** The installer relies on command line options and an input file to define installation parameters, and can be run in silent mode, suppressing all interface elements. Run the command line installation on each AD FS server in your deployment.

Before You Begin

- Copy RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi to a folder on the system where you will install the agent.
- Obtain the API access key for either RSA Authentication Manager or the Cloud Authentication Service, depending on the authentication mode you will configure.
  - To obtain the API access key, see the following on RSA Link:
    - For RSA Authentication Manager, see [Configure the RSA SecurID Authentication API for Authentication Agents](#).
    - For the Cloud Authentication Service, see [Add an RSA SecurID Authentication API Key](#).
- For command line installation only:
  - Create an input file to pass configuration parameters to the installer. For instructions, see [Create a Configuration Input File for Command Line Installation on the facing page](#).
  - Make sure you are familiar with installing software using the msiexec command line. For more information, visit [http://technet.microsoft.com](http://technet.microsoft.com).

  **Note:** If Windows Server is installed in Server Core mode, you must invoke the installer from the command line.

Install the Agent Using the Install Wizard

Perform this procedure to install RSA Authentication Agent for Microsoft AD FS using the Install Wizard.

**Procedure**

1. Sign into the AD FS server where you want to install Agent for AD FS.
2. Double-click **RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi** to start the Install Wizard.
3. Click **Next**.
4. Read and accept the license agreement, then click **Next**.
5. Provide the required configuration parameters. See [Configuration Settings and Required Information on page 17](#) for details.
6. Click **Next**.
7. Click **Install**.
8. When installation is complete, click **Finish**.

### Create a Configuration Input File for Command Line Installation

To install Agent for AD FS 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. Complete the following procedure to create the input file.

#### Before you begin

Obtain the API access key for either RSA Authentication Manager or the Cloud Authentication Service, depending on the authentication mode.

To obtain the API access key, see the following on RSA Link:

- For RSA Authentication Manager, see [Configure the RSA SecurID Authentication API for Authentication Agents](#).
- For the Cloud Authentication Service, see [Add an RSA SecurID Authentication API Key](#).

#### Procedure

1. Create a text file with any file name and extension. For example, **input.txt**.
2. Add the following string to specify the Authentication Mode:
   ```
   AUTHENTICATION_MODE= <#>
   ```
   where `<#>` is either 1 for RSA Authentication Manager mode or 2 for Cloud Authentication Service mode.
3. Add the following string to specify the Server URL:
   ```
   SERVER_URL= <https://www.myexampleserver.com:5555/mfa/v1_1>
   ```
   where `<https://www.myexampleserver.com:5555/mfa/v1_1>` 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.
4. 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.
5. Add the following string to specify the Access Key:
   ```
   ACCESS_KEY= <accesskey>
   ```
   where `<accesskey>` is the access key you obtained for either RSA Authentication Manager or the Cloud Authentication Service, depending on the authentication mode.
6. Do one of the following:
   - For RSA Authentication Manager mode, add the following string to specify Replica Server URLs:
     ```
     ```
For Cloud Authentication Service mode, add the following string to specify the Access Policy:

```
ACCESS_POLICY= <accesspolicy>
```

where `<accesspolicy>` is the exact name (including case sensitivity) of the access policy as specified in the Cloud Administration Console.

7. (Optional) For Cloud Authentication Service 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 collection, you cannot use the Identity Confidence access policy attribute to determine user authentication requirements.

8. (Optional) For Cloud Authentication Service mode, add the following string 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 collection, you cannot use the Trusted Location access policy attribute to determine user authentication requirements.

9. Save the file to the AD FS 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.

- Secure or delete the input file after you install the agent, as it contains sensitive data.

**Install the Agent Using the Command Line**

Perform this procedure to install AD FS Agent using the command line.

This procedure assumes that you are familiar with installing software using the msiexec command line.

**Before you begin**

Create an input file to pass configuration parameters to the installer. For instructions, see Create a Configuration Input File for Command Line Installation on the previous page.

**Procedure**

1. Open an administrator command prompt.

2. Navigate to the directory that contains the **RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi** package file, or provide the full pathname to the package file on the command line.

3. To install AD FS Agent, use a command similar to the following:

```
msiexec /i "RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi" /L*v install.log /q INPUTFILE=<absolute\file\path\input.txt>
```

where `<absolute\file\path\input.txt>` is the absolute file path for the input file you created. The `/q` switch instructs the installer to run in silent mode.
After you finish

Secure or delete the input file, as it contains sensitive data.

Next Steps

After installing AD FS Agent, perform these steps:

1. Register the agent in RSA Authentication Manager. For instructions, see Register the Agent in RSA Authentication Manager on page 28.
2. Register the agent in the Windows Server Manager. For instructions, see Register or Unregister the Agent with Microsoft AD FS on page 28.
3. Import the trusted root CA certificate from either Authentication Manager or the Cloud Authentication Service. For instructions, see Import Trusted Root Certificate on page 33
4. Configure multifactor authentication settings for your environment. For instructions, see Configure Multifactor Authentication (MFA) on page 28.
5. (Optional) Configure additional settings such as Request Timeout, Read Timeout, and Retry Count using the configuration utility. For more information, see Edit Settings Using the Agent for AD FS Configuration Utility on page 35.
Chapter 4: Configuring and Managing the Agent

Register the Agent in RSA Authentication Manager .......................................................... 28
Register or Unregister the Agent with Microsoft AD FS .................................................. 28
Configure Multifactor Authentication (MFA) .................................................................... 28
Coexistence with RSA Authentication Agent 1.0.2 for Microsoft AD FS .......................... 32
Restart AD FS Services ........................................................................................................ 33
Import Trusted Root Certificate .......................................................................................... 33
Add Localized Authentication Pages .................................................................................. 34
Remove Localized Authentication Pages .......................................................................... 35
Edit Settings Using the Agent for AD FS Configuration Utility ........................................ 35
Enable or Disable FIPS on Windows Server 2016 or 2012 R2 ........................................... 36
Configure Logging ............................................................................................................... 36
RSA Group Policy Object Templates ..................................................................................... 38
Update Access Control List (ACL) Permissions .................................................................. 38
Repair an Installation .......................................................................................................... 39
Uninstall the Agent ............................................................................................................. 39
Register the Agent in RSA Authentication Manager

After you install Authentication Agent for AD FS, you must register it with Authentication Manager if you are using RSA Authentication Manager mode.

Before you begin

Make sure you know the Agent Name you specified when installing Agent for AD FS.

Procedure

1. Sign into the RSA 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 Microsoft AD FS.
4. Click Save.

Register or Unregister the Agent with Microsoft AD FS

After installing RSA Authentication Agent for Microsoft AD FS on all federation servers in your AD FS deployment, you must register the agent on the primary federation server using the RSA Agent for AD FS Configuration Utility. If you need to uninstall the agent, you must unregister it first.

Procedure

1. Sign into the primary AD FS server where you installed the agent.
2. Open a PowerShell command prompt.
3. Enter the following to run the Agent for AD FS Configuration Utility:
   cd 'C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\scripts'\MFAAuthProviderConfigSettings.ps1
4. From the Main Menu, do one of the following:
   - Enter 4 to select Register Agent.
   - Enter 5 to select Unregister Agent.

After you finish

Restart Active Directory Federation Services (adfssrv) on each server in the AD FS deployment. For instructions, see Restart AD FS Services on page 33.

Configure Multifactor Authentication (MFA)

After installing and registering Agent for AD FS, you must configure the Microsoft AD FS global authentication policy to enforce multifactor authentication using the agent. Perform the procedure appropriate for the operating system on your AD FS server.
Configure MFA on Windows Server 2016 or 2012 R2 in Desktop Experience Mode

Procedure

1. Click Start > Server Manager.
2. Click Tools > AD FS Management.
3. In the left-hand frame, click Service > Authentication Methods.
4. In the center frame, in the Multi-factor Authentication section, click Edit.
   The Edit Global Authentication Policy Window appears.
5. On the Multi-factor tab, select the checkbox for RSA SecurID Access Authentication v2.0, and verify that settings in the Users/Groups, Devices, and Locations sections are set appropriately for your environment.

   Note: If RSA Authentication Agent 1.0.2 for Microsoft AD FS is also installed in your AD FS environment, it appears on this page as RSA SecurID Authentication, and can be enabled or disabled using the corresponding checkbox.

6. Click OK.

After you finish

- Restart Microsoft Active Directory Federation Services (adfssrv). For instructions, see Restart AD FS Services on page 33.
- (Optional) Test the MFA configuration using the AD FS test page. For instructions, see Test MFA on Windows Server 2016 in Desktop Experience Mode on the next page or Test MFA on Windows Server 2012 R2 on the next page, depending on your operating system.

Configure MFA on Windows Server 2016 or 2012 R2 in Server Core Mode

Procedure

1. Sign into the AD FS server where you installed the agent.
2. Open a PowerShell command prompt.
3. Enter the following command to add Agent for AD FS as an additional authentication provider:
   ```powershell
   Set-AdfsGlobalAuthenticationPolicy -AdditionalAuthenticationProvider "SecurIDv2Authentication"
   ```
4. Enter the following command, and verify that SecurIDv2Authentication appears in the list of authentication providers returned:
   ```powershell
   Get-AdfsGlobalAuthenticationPolicy
   ```

   Note: If RSA Authentication Agent 1.0.2 for Microsoft AD FS is also installed in your AD FS environment, additional commands may be required. For instructions, see Configure Multifactor Authentication for Multiple Agent Versions on page 32.

After you finish

- Restart Microsoft Active Directory Federation Services (adfssrv). For instructions, see Restart AD FS Services on page 33.
- (Optional) Test the MFA configuration using the AD FS test page (Windows Server 2016 only). For instructions, see Test MFA on Windows Server 2016 in Server Core Mode on the facing page or Test MFA on Windows Server 2012 R2 below, depending on your operating system.

Test MFA on Windows Server 2012 R2

AD FS for Windows Server 2012 R2 includes a test page which you can use to verify that multifactor authentication and Agent for AD FS are configured and working properly. Perform this procedure to conduct a test authentication.

Procedure

1. Open a web browser and navigate to:
   https://<youradfs>.<yourdomain.com>/adfs/ls/idpinitiatedsignon
   where <youradfs> is the name of your AD FS server, and <yourdomain.com> is the name of your domain.
2. Enter appropriate credentials, and verify that authentication works properly.

Test MFA on Windows Server 2016 in Desktop Experience Mode

AD FS for Windows Server 2016 includes a test page which you can use to verify that multifactor authentication and Agent for AD FS are configured and working properly. Perform this procedure to enable the test page and conduct a test authentication if Windows is installed in Desktop Experience mode.

Procedure

1. Sign into the server where you installed the agent.
2. Open a Powershell command prompt.
3. Enter the following command to enable the test page:
   Set-AdfsProperties -EnableIdPInitiatedSignonPage:$true
4. Click Start > Server Manager.
5. Click Tools > AD FS Management.
6. In the left-hand frame, click Application Groups.
7. In the right-hand frame, click Add Application Group.
8. In the Name field, enter a name for the application group.
9. Select Template > Web browser accessing a web application.
10. Click Next.
11. In the Redirect URI field, enter:
    https://<youradfs>.<yourdomain.com>/adfs/ls/idpinitiatedsignon
    where <youradfs> is the name of your AD FS server, and <yourdomain.com> is the name of your domain.
12. Click Add.
13. Click Next.
14. Select Choose an access control policy > Permit everyone and require MFA.
15. Click Next.
16. Click Next.
17. Click Close.
18. In the center frame, select the application group you specified in Step 8.
19. In the right-hand frame, select Properties.
20. Select <Name> - Web application where <Name> is the application group you specified in Step 8.
21. Click Edit.
22. Under Identifiers > Relying party identifier, enter:
   http://<youradfs>.<yourdomain.com>/adfs/services/trust
   where <youradfs> is the name of your AD FS server, and <yourdomain.com> is the name of your domain.
   To get the correct value, run the get-adfsproperties command from PowerShell, and look for the identifier value.
23. Click Add.
24. Click OK.
25. In the left-hand frame, select Access Control Policies.
26. Double-click Permit everyone and require MFA.
27. Select the Assigned To tab.
28. Verify that <Name> - Web application is present in the Application Name list where <Name> is the application group you specified in Step 8.
29. Restart Microsoft Active Directory Federation Services (adfssrv). For instructions, see Restart AD FS Services on page 33.
30. Open a web browser and navigate to:
   https://<youradfs>.<yourdomain.com>/adfs/ls/idpinitiatedsignon
   where <youradfs> is the name of your AD FS server, and <yourdomain.com> is the name of your domain.
31. Enter appropriate credentials, and verify that authentication works properly.

Test MFA on Windows Server 2016 in Server Core Mode

AD FS for Windows Server 2016 includes a test page which you can use to verify that multifactor authentication and Agent for AD FS are configured and working properly. Perform this procedure to enable the test page and conduct a test authentication if Windows is installed in Server Core mode.

Procedure

1. Sign into the server where you installed the agent.
2. Open a Powershell command prompt.
3. Enter the following command to enable the test page:
   Set-AdfsProperties -EnableIdPInitiatedSignonPage:$true
4. Enter the following, and record the Identifier value returned by the command:
   Get-AdfsProperties
5. Enter the following commands to add the application group:
   New-AdfsApplicationGroup -Name <GroupName>
   Set-AdfsApplicationGroup -TargetApplicationGroupIdentifier <GroupName>
   where <GroupName> is a name you choose for the application group.
6. Enter the following command to add the ADFS Native Client Application to the application group:
   Add-AdfsNativeClientApplication -Name <ClientAppName> -Identifier <ID> -ApplicationGroupIdentifier <GroupName> -RedirectUri <IDPSignOnURL>
   where <ClientAppName> is the ADFS client application name, <ID> is an alphanumeric string you
choose, <Group Name> is the name of the group you chose in Step 5, and <IDPSignOnURL> is the fully qualified URL for the IDPInitiatedSignOn page.

7. Open a web browser and navigate to:
   https://<youradfs>.<yourdomain.com>/adfs/ls/idpinitiatedsignon
   where <youradfs> is the name of your AD FS server, and <yourdomain.com> is the name of your domain.

8. Enter the following commands to add the ADFS Web API Application:
   $IDs = @{"<ID>"","<IDPSignOnID>"}
   Add-AdfsWebApiApplication -Name <WebAPIAppName> -Identifier $IDs -AccessControlPolicyName
   "Permit everyone and require MFA" -ApplicationGroupIdentifier <GroupName>
   where <ID> is the alphanumeric string you specified in Step 6, <IDPSignOnID> is the Identifier value you obtained in Step 4, <WebAPIAppName> is the ADFS web API application name, and <GroupName> is the group name specified in Step 5.

9. Restart Microsoft Active Directory Federation Services (adfssrv). For instructions, see Restart AD FS Services on the facing page.

10. Open a web browser and navigate to:
    https://<youradfs>.<yourdomain.com>/adfs/ls/idpinitiatedsignon
    where <youradfs> is the name of your AD FS server, and <yourdomain.com> is the name of your domain.

11. Enter appropriate credentials, and verify that authentication works properly.

**Coexistence with RSA Authentication Agent 1.0.2 for Microsoft AD FS**

You can install RSA Authentication Agent 2.0 for Microsoft AD FS in an AD FS environment where version 1.0.2 of the agent already exists. When both versions of the agent are installed, you can choose which version AD FS uses for multifactor authentication, or you can enable both versions to let users choose the version they prefer when prompted to authenticate. Perform this procedure to configure the AD FS multifactor authentication policy for multiple agent versions.

When installing or uninstalling multiple agent versions:

- Always install and register version 1.0.2 before installing and registering version 2.0
- If you unregister and uninstall version 1.0.2, you must re-register version 2.0.
- Registering version 2.0 disables all other multifactor authentication providers configured for AD FS.
  Always reconfigure MFA after installing and registering version 2.0. For instructions, see Configure Multifactor Authentication (MFA) on page 28.

**Configure Multifactor Authentication for Multiple Agent Versions**

If the AD FS server is running Windows in Desktop Experience mode, you can enable or disable either version of the agent using the instructions provided in Configure Multifactor Authentication (MFA) on page 28. If Windows is running in Server Core mode, use the following procedure.

**Procedure**

1. Sign into the server where you installed both versions of the agent.
2. Open a PowerShell command prompt.
3. Do one of the following, depending on the agent or agents you want AD FS to use for multifactor authentication:
   - To enable only agent version 1.0.2, enter the following command:
     ```powershell
     Set-AdfsGlobalAuthenticationPolicy -AdditionalAuthenticationProvider "SecurIDAuthentication"
     ```
   - To enable only agent version 2.0, enter the following command:
     ```powershell
     Set-AdfsGlobalAuthenticationPolicy -AdditionalAuthenticationProvider "SecurIDv2Authentication"
     ```
   - To enable both agent versions, enter the following set of commands:
     ```powershell
     $METHODS = @("SecurIDAuthentication","SecurIDv2Authentication")
     Set-AdfsGlobalAuthenticationPolicy -AdditionalAuthenticationProvider $METHODS
     ```

After you finish

Restart Microsoft Active Directory Federation Services (adfssrv). For instructions, see Restart AD FS Services below.

**Restart AD FS Services**

After installing and registering Agent for AD FS, you must restart Active Directory Federation Services (adfssrv) on each AD FS server in your deployment.

Procedure

1. Sign into the AD FS server where you installed the agent.
2. Open a PowerShell command prompt.
3. Enter the following to run the Agent for AD FS Configuration Utility:
   ```powershell
   cd 'C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\scripts' \n   .\MFAAuthProviderConfigSettings.ps1
   ```
4. From the Main Menu, enter 3 to select Restart AD FS.

**Import Trusted Root Certificate**

After installing the agent, you must import the trusted root CA certificate from RSA Authentication Manager or the Cloud Authentication Service, depending on the authentication mode you configured during installation. You can obtain this certificate from your Authentication Manager or Cloud Authentication Service administrator. (For instructions, see the knowledgebase article How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate.)

Perform the procedure appropriate for the operating system on your AD FS server.

**Import Trusted Root Certificate in Desktop Experience Mode**

Perform this procedure on each AD FS server to import the certificate if Windows is running in Desktop Experience mode.

**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 AD FS server.

Procedure

1. Sign into the AD FS server where you installed the agent.
2. Run \windows\system32\microsoft.windows.adfs.agent.SAN.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.

Import Trusted Root Certificate in Server Core Mode

Follow this procedure to import the certificate in Server Core mode on each AD FS server where you install the agent.

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 AD FS server.

Procedure

1. Sign into the AD FS server where you installed the agent.
2. Open a PowerShell command prompt.
3. Enter the following commands to import the certificate:
   ```powershell
   Import-Module PKI
   Set-Location Cert:
   Get-ChildItem -Path <c:\CertDirectory\mycert.cer> | Import-Certificate -CertStoreLocation cert:\LocalMachine\Root
   where <c:\CertDirectory\mycert.cer> is the full file path of the certificate.
   ```

Add Localized Authentication Pages

Perform this procedure to make non-English AD FS Agent authentication pages available according to the language preferences set in each user’s web browser.
Before you begin

Download the language file package **ADFSAgentv2LocalizedPages.zip** from RSA Link:
https://community.rsa.com/community/products/securid/authentication-agent-AD FS/downloads/content

**Procedure**

1. Sign into the AD FS server where you installed the agent.
2. Copy the contents of **ADFSAgentv2LocalizedPages.zip** to `C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\lang\`, replacing any duplicate files.
3. Open a PowerShell command prompt.
4. Enter the following to run the Agent for AD FS localization script:
   ```powershell
cd 'C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\lang'
   .\MFAAuthProviderLocalization.ps1
   ``
5. Enter 1 to add and enable the localized language resource files.
6. Enter 3 to exit.

**After you finish**

Restart Microsoft Active Directory Federation Services (adfssrv). For instructions, see Restart AD FS Services on page 33.

**Remove Localized Authentication Pages**

Perform this procedure to remove non-English AD FS Agent authentication pages from the AD FS server.

**Procedure**

1. Sign into the AD FS server where you installed the agent.
2. Open a PowerShell command prompt.
3. Enter the following to run the Agent for AD FS localization script:
   ```powershell
cd 'C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\lang'
   .\MFAAuthProviderLocalization.ps1
   ``
4. Enter 2 to remove localized language resource files.
5. Enter 3 to exit.
6. Delete the language files from `C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\lang\`.

**After you finish**

Restart Microsoft Active Directory Federation Services (adfssrv). For instructions, see Restart AD FS Services on page 33.

**Edit Settings Using the Agent for AD FS Configuration Utility**

When you install Agent for AD FS, you configure basic settings using the installation wizard. If you need to modify those settings after installation, you can use the Agent for AD FS Configuration Utility. The configuration
utility provides options to view and edit agent settings, restart the AD FS service, and register or unregister the agent with Microsoft AD FS. Some settings are only available in the configuration utility.

Procedure

1. Sign into the AD FS server where you installed the agent.
2. Open a PowerShell command prompt.
3. Enter the following to run the Agent for AD FS Configuration Utility:
   ```
   cd 'C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\scripts' .\MFAAuthProviderConfigSettings.ps1
   ```
4. From the Main Menu, enter 2 to select Edit Settings.
   
   **Note:** You can enter 1 to select View Current Settings if you want to check the current configuration without making changes.

5. From the Edit Settings menu, enter the number of the setting you want to modify. This menu displays different options depending on the currently configured authentication mode.
6. Provide the required configuration parameters. See Configuration Settings and Required Information on page 17 for details.
7. Enter Y when prompted to return to the Main Menu, or enter N to proceed to the next configurable setting.
8. When you are done editing settings, enter 6 from the Main Menu to exit the configuration utility.

Enable or Disable FIPS on Windows Server 2016 or 2012 R2

The Federal Information Processing Standard (FIPS) is a United States government computer security standard used to approve cryptographic modules. Perform this procedure to enable FIPS on Windows Server 2016 or 2012 R2.

Procedure

1. Sign into the AD FS server as an administrator.
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.

Configure Logging

Logging is enabled by default when you install Agent for AD FS. You can customize logging options by manually editing the log4net.config file in the C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\config directory. You can change the following parameters using the log file syntax provided.
Note: You must restart Microsoft Active Directory Federation Services (adfssrv) after modifying log4net.config. For instructions, see Restart AD FS Services on page 33.

Default Log Format
You can specify the logging format. Specify either SizeBasedRotation or TimeBasedRotation 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:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\logs\rsa_adfs.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"/>
```

Chapter 4: Configuring and Managing the Agent
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:

```xml
<appender name="TimeBasedRotation" type="log4net.Appender.RollingFileAppender">
  <file value="c:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\logs\rsa_adfs.log"/>
</appender>
```

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:

```xml
<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:

```xml
<file value="c:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\logs\rsa_adfs.log"/>
```

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

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

RSA Group Policy Object Templates
The RSA Group Policy Object (GPO) template files allow you to configure additional settings for Authentication Agent for AD FS. For more information, see the Group Policy Object Template Guide. available on RSA Link: https://community.rsa.com/community/products/securid/authentication-agent-AD FS

Update Access Control List (ACL) Permissions
If you change the service account used for managing the AD FS server, you must transfer the required Agent for AD FS file permissions to the new service account. To transfer file permissions, run the ACL update script: C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\scripts\MFAAuthProviderACLSettings.ps1.
Repair an Installation

Repairing an installation replaces missing files in a damaged installation. You can repair the installation using the Install Wizard or the command line.

**Repair an Installation Using the Install Wizard**

**Procedure**

1. Copy *RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi* to a folder on the system where you want to repair the installation.
2. Double-click *RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi* to run the installer.
3. Click **Next**.
4. Select **Repair**, then click **Next**.
5. Click **Repair**.
6. Click **Finish** to exit the wizard.

**Note:** The installer may prompt you to close files or applications that will be modified during the repair process.

**Repair an Installation Using the Command Line**

**Procedure**

1. Copy *RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi* to a folder on the system where you want to repair the installation.
2. Open a command prompt.
3. Navigate to the directory that contains the *RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi* package file, or provide the full pathname to the package file on the command line.
4. Enter a command similar to the following.
   ```
   msiexec /f "RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi" /q /L*v repair.log
   ``
   The /q switch instructs the installer to run in silent mode.

**Uninstall the Agent**

You can uninstall the agent using Windows Control Panel, the Install Wizard, or the command line. To uninstall the product from multiple AD FS servers simultaneously, you must use the command line.

**Before You Begin**

Unregister the agent with Microsoft AD FS. For instructions, see Register or Unregister the Agent with Microsoft AD FS on page 28.

If you added non-English AD FS Agent authentication pages, remove them from the AD FS server. For instructions, see Remove Localized Authentication Pages on page 35.
Uninstall the Agent Using Windows Control Panel

Procedure
1. From the Start menu, click Control Panel > Programs > Programs and Features.
2. In the program list, click RSA Authentication Agent v2.0 for Microsoft AD FS.
3. Click Uninstall.
4. Restart the server if prompted. If you cancel the uninstall process, the application reverts to its previous state.

Uninstall the Agent Using the Install Wizard

Procedure
1. Copy RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi to a folder on the system where you want to uninstall the product.
2. Double-click RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi to run the installer.
3. Click Next.
4. Select Remove, then click Next.
5. Click Remove.
6. Click Finish to exit the wizard.

Uninstall the Agent Using the Command Line

Procedure
1. Copy RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi to a folder on the system where you want to uninstall the product.
2. Open a command prompt.
3. Enter the following command:
   ```
   msiexec /x "RSA Authentication Agent v2.0 for Microsoft AD FS x64.msi" /L*v uninstall.log /q FORCEUNINSTALL=false
   ```
   The /q switch instructs the installer to run in silent mode. FORCEUNINSTALL=false aborts the installation if the agent has not been unregistered from Microsoft AD FS.

After You Finish

If the C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\lang\ folder still exists after uninstallation, delete it and any files it contains.
Chapter 5: Troubleshooting

Installation Logs .............................................................................................................. 42
Diagnose Authentication Issues ....................................................................................... 42
Installation Logs

If you encounter problems while installing, repairing, or uninstalling the agent, check install.log, repair.log, or uninstall.log, respectively, for status and troubleshooting information. The log files are saved in the folder where you run the installer. This table describes the messages that may appear in the logs.

<table>
<thead>
<tr>
<th>Log Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation successful.</td>
<td>Installation is complete.</td>
</tr>
<tr>
<td>Uninstallation successful.</td>
<td>Uninstallation is complete.</td>
</tr>
<tr>
<td>Installation unsuccessful.</td>
<td>The installation was interrupted.</td>
</tr>
<tr>
<td>Invalid configuration parameters.</td>
<td>Installation unsuccessful.</td>
</tr>
<tr>
<td>Uninstallation unsuccessful.</td>
<td>The input file contains unexpected values for one or more configuration fields.</td>
</tr>
<tr>
<td>Missing required configuration parameters.</td>
<td>The input file does not contain values for one or more required install parameters.</td>
</tr>
<tr>
<td>Agent must be unregistered with Microsoft AD FS.</td>
<td>The agent cannot be uninstalled because it is currently registered with Microsoft AD FS.</td>
</tr>
</tbody>
</table>

Diagnose Authentication Issues

The following section contains details on issues you might encounter while using RSA Authentication Agent for Microsoft AD FS, troubleshooting information, and descriptions of common error messages. For additional troubleshooting information, sign into RSA Link at https://community.rsa.com.

Verify the Accuracy of the Computer Clock

If a user cannot authenticate, make sure the clock on the user’s computer or mobile device is accurate. If the computer clock or device clock is not synchronized with the RSA Authentication Manager clock, the user may not be able to authenticate.

Errors and Log Messages

Agent for AD FS displays user-facing errors and records administrator-facing logs and Microsoft Event Viewer messages that can help you identify problems.

Agent Log Messages

The following table lists sample log messages that the agent records for common error scenarios.

<table>
<thead>
<tr>
<th>Log Message</th>
<th>Error Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-04-27 04:41:01,784 [23] INFO</td>
<td>Communication with an Authentication Manager instance is interrupted due to network connection problems. The agent attempts the configured number of connection retries, then switches to the next configured replica instance.</td>
</tr>
<tr>
<td>ServerManager - getServerUrl():</td>
<td></td>
</tr>
<tr>
<td>returning server: https://&lt;youram-url1&gt;:5555/mfa/v1_1</td>
<td></td>
</tr>
<tr>
<td>ConnectionHandler - Retry Count:4</td>
<td></td>
</tr>
<tr>
<td>ConnectionHandler - Retry Count:3</td>
<td></td>
</tr>
</tbody>
</table>
### Log Message

| ConnectionHandler - Retry Count:2
| ConnectionHandler - Retry Count:1
| ServerManager - Marking this server state to DOWN: https://<youram-url1>:5555/mfa/v1_1
| ConnectionHandler - Failover to next URL.
| ServerManager - getServerUrl(): returning server: https://<youram-url2>:5555/mfa/v1_1
| AuthnRequestService - MFA Response is empty. Returning Null
| AuthnAdapter - Authentication step completed.
| 2018-05-10 02:47:24,969 [18] ERROR
| ConnectionHandler - No Servers Available for Authentication.
| Error in Server certificate validation: A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.
| Error in Server certificate validation: Certificate Not Available
| Error in Server certificate validation: Certificate Name Mismatch

### Error Scenario

- A connection failure occurs during authentication.
- The agent cannot connect to the Cloud Authentication Service or any Authentication Manager instance.
- A problem occurs while validating the server certificate due to incorrect certificate chain.
- Trusted certificates cannot be found.
- The common name to which an SSL certificate is issued does not match the name of the server URL.

### User-Facing Error Messages

The following table lists error messages that the agent displays to users for common error scenarios.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Error Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication timed out. Try again or contact your administrator.</td>
<td>No user activity is registered on the authentication page for more than 180 seconds. A 'Retry' button is provided to re-initialize the authentication.</td>
</tr>
<tr>
<td>No supported authentication methods found. Contact your administrator.</td>
<td>The only methods available in the access policy for the agent are either not supported by the agent, or cannot be completed by the user. For example, the FIDO authentication method, or the SMS and Voice methods when no phone number is available for the user.</td>
</tr>
<tr>
<td>Cannot authenticate. Contact your administrator.</td>
<td>One of the following is true:</td>
</tr>
</tbody>
</table>
### Error Message | Error Scenario
--- | ---
| You must install and register the RSA SecurID Authenticate app to complete authentication. | All methods available in the access policy for the agent require the RSA SecurID Authenticate app, but the user has not registered a device with the app.
| Unsuccessful authentication. Try again. | One of the following is true:
- The user provided invalid credentials.
- The user attempted to cancel and retry an Approve or Device Biometrics authentication multiple times in rapid succession, causing messages to arrive out of sequence.
- A corrupted message chain error occurred during authentication with any method.

### Event Viewer Messages

The following table lists sample messages that the agent records in Microsoft Event Viewer for common error scenarios.

| Event Viewer Message | Error Scenario |
--- | --- |
Encountered error during federation passive request. | The agent configuration file `C:\Program Files\RSA\RSA Authentication Agent\AD FS MFA Adapter\config\mfaconfig.json` is either missing or corrupt. Do the following:
- Copy and rename the backup file `mfaconfig.json.bkp` to `mfaconfig.json`, then restart the AD FS service.

Additional Data
Protocol Name: Saml
Relying Party: http://server.domain.com/AD FS/services/trust
Exception details:
System.PlatformNotSupportedException: Operation is not supported on this platform.
<table>
<thead>
<tr>
<th>Event Viewer Message</th>
<th>Error Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encountered error during federation passive request.</td>
<td>The agent is not registered with Microsoft AD FS. For instructions to register the agent, see</td>
</tr>
<tr>
<td>Additional Data</td>
<td>Register or Unregister the Agent with Microsoft AD FS on page 28.</td>
</tr>
<tr>
<td>Protocol Name:</td>
<td></td>
</tr>
<tr>
<td>Saml</td>
<td></td>
</tr>
<tr>
<td>Relying Party:</td>
<td></td>
</tr>
<tr>
<td><a href="http://server.domain.com/AD">http://server.domain.com/AD</a> FS/services/trust</td>
<td></td>
</tr>
<tr>
<td>Exception details:</td>
<td></td>
</tr>
<tr>
<td>An error occurred loading an authentication provider.</td>
<td>Agent files are either missing or corrupt.</td>
</tr>
<tr>
<td>Fix configuration errors using PowerShell cmdlets and restart the Federation Service.</td>
<td>Do the following:</td>
</tr>
<tr>
<td>Identifier: SecurIDv2Authentication</td>
<td>1. Use the installer to repair the agent.</td>
</tr>
<tr>
<td>Exception details:</td>
<td></td>
</tr>
<tr>
<td>An error occurred initializing the 'SecurIDv2Authentication' authentication provider.</td>
<td></td>
</tr>
</tbody>
</table>