Release Notes

RSA® Authentication Agent 2.0.3 for Microsoft® AD FS

July 2020

Introduction

This document lists what's new and changed in RSA Authentication Agent 2.0.3 for Microsoft AD FS. Read this document before installing the software. This document contains the following sections:

These *Release Notes* may be updated. The most current version can be found on RSA Link at *https://community.rsa.com/***.**

What's New in This Release

RSA Authentication Agent 2.0.3 for Microsoft AD FS includes the following new features and changes.

Support for Emergency Tokencode. The AD FS Agent 2.0.3 supports Emergency Tokencode as an authentication method for the Cloud Authentication Service. An updated language pack supports this method. See *Package Contents*.

Ability to Configure a Web Proxy for Authentication Requests. By default, the agent connects to RSA Authentication Manager or the Cloud Authentication Service using the web proxy configured using the Windows system and user settings. The new policy setting "Proxy server for connections to an RSA authentication server" allows you to configure a different web proxy that the agent uses for authentication requests. This policy setting can be configured using the version 2.0.3 GPO template. See *Package Contents*.

Fixed Issues. The cumulative AD FS Agent 2.0.3 release includes software updates to resolve customer issues.

New Features Introduced in RSA Authentication Agent 2.0.2 for Microsoft AD FS

RSA Authentication Agent 2.0.2 for Microsoft AD FS includes the following new features and changes.

Fixed Issues. The AD FS Agent 2.0.2 corrects cosmetic issues with Windows Server 2019 and resolves an issue with setting a PIN for Windows Hello for Business.

Updated the RSA GPO Templates to Allow Users to Set a Windows Hello for Business PIN. The RSA GPO templates are updated with a new policy setting to "Validate the Authentication Context." By default, RSA performs additional validation on the Authentication Context the AD FS Agent receives from the AD FS server during an authentication. RSA's additional validation depends on session cookies that are not set when provisioning a Windows Hello for Business PIN. To allow users to set a Windows Hello for Business PIN, disable this setting.

If you want to deploy the updated RSA GPO Templates, see Chapter 2, "Deploying Group Policy Object Templates" in the *RSA Authentication Agent 2.0.2 for Microsoft AD FS GPO Template Guide*

The root certificate and language pack were not updated for AD FS Agent 2.0.2. You can download or continue to use the AD FS Agent 2.0 versions of these files.

New Features Introduced in RSA Authentication Agent 2.0.1 for Microsoft AD FS

RSA Authentication Agent 2.0.1 for Microsoft AD FS includes the following new features and changes.

Support for Windows Server 2019. The AD FS Agent 2.0.1 has been qualified to run on Windows Server 2019 (Server Core or Desktop Experience) with AD FS 5.0.

The AD FS Agent 2.0.1 continues to support Windows Server 2012 R2 (Server Core or Desktop Experience) with AD FS 3.0 and Windows Server 2016 (Server Core or Desktop Experience) with AD FS 4.0.

Replace Windows Passwords with RSA SecurID as the Primary Authentication Method. Windows Server 2019 with AD FS 5.0 allows you to select RSA SecurID as the primary authentication method and Windows authentication as the secondary authentication method. Your users can authenticate with any of the multifactor authentication methods supported by RSA Authentication Manager or the Cloud Authentication Service, such as Authenticate Tokencode, Approve, or RSA SecurID Tokens.

Fixed issues. The AD FS Agent 2.0.1 corrects a potential problem with device biometrics authentication.

New Features Introduced in RSA Authentication Agent 2.0 for Microsoft AD FS

This section describes the major features and changes introduced in RSA Authentication Agent 2.0 for Microsoft AD FS. For more information on each feature, refer to the *RSA Authentication Agent 2.0.2 for Microsoft AD FS Administrator's Guide*.

Authentication Modes. The agent supports these authentication modes:

- **RSA Authentication Manager**. The agent connects to an existing Authentication Manager instance in your deployment using the REST protocol, making the RSA 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.

  Note: RSA Authentication Manager mode requires Authentication Manager 8.3 or later.

- **Cloud Authentication Service**. The agent connects to the Cloud Authentication Service using the REST protocol, 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.

Agent Reporting. In Authentication Manager mode, the agent sends details such as the hostname, agent version, and operating system version to Authentication Manager to help you manage your installed REST protocol agents. You can run reports that include these details using Authentication Manager 8.3 or later.

TLS 1.2 Support. The agent uses the TLS 1.2 encryption protocol for secure communications.

Support for FIPS-Enabled Operating System Environment. You can configure the operating system to work with the agent in Federal Information Processing Standard (FIPS) mode. FIPS is a United States government computer security standard used to approve cryptographic modules.

Risk Collection for the Cloud Authentication Service. The agent supports 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.

Coexistence with ADFS Agent Version 1.0.2. If you need to test agent version 2.0 before fully transitioning from version 1.0.2, you can install both versions together in the same AD FS environment. When both versions are installed, you can choose which version AD FS uses for multifactor authentication or enable both versions to let users decide which they prefer when they are prompted to authenticate.

Note: It is not possible to upgrade older versions of the agent to version 2.0.

Support for Stand-Alone AD FS Server and Federation Server Farm. You can install the agent on an individual AD FS server or a collection of servers in a federation server farm.

Package Contents

RSA Authentication Agent 2.0.3 for Microsoft AD FS is available at *https://community.rsa.com/community/products/securid/authentication-agent-adfs*. The downloads page displays SHA256 values that you can use to verify the authenticity of the product zip files.

The RSA Authentication Agent 2.0.3 for Microsoft AD FS package contains the following:

- **ADFSAgentv2LocalizedPages.zip**
- **RSA_Authentication_Agent_v2.0.3.62_ADFS.zip**
- **RSA_Authentication_Agent_v2.0.3.62_ADFS_GPO.zip**

The following table describes each file.

File	Description
ADFSAgentv2LocalizedPages.zip	Localized (translated) authentication web pages for RSA Authentication Agent for Microsoft AD FS. 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 the *RSA Authentication Agent 2.0.3 for Microsoft AD FS Administrator's Guide*.
RSA_Authentication_Agent_v2.0.3.62_ADFS.zip	Contains the following folders: • x64: The Windows Installer Packages for local installation of RSA Authentication Agent for Microsoft AD FS on 64-bit computers. • Licenses: Contains the RSA License Agreement.
RSA_Authentication_Agent_v2.0.3.62_ADFS_GPO.zip	Contains the Group Policy Object (GPO) administrative templates for managing authentication settings. For instructions, see the *RSA Authentication Agent 2.0.3 for Microsoft AD FS GPO Template Guide*.

Product Installation and Upgrade

You can use the installer MSI (**RSA Authentication Agent v2 for Microsoft AD FS x64.msi**) to install the AD FS Agent on a new system or directly upgrade an existing installation from AD FS Agent 2.0 or later.

Before You Begin

Administrator privileges are required.

Procedure

1. (Upgrades only) Unregister the current AD FS Agent on the primary federation server:
    a. Sign into the primary AD FS server where you installed the agent.
    b. Open a PowerShell command prompt, and 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
    ```

    c. From the Main Menu, enter 5 to select **Unregister Agent**.
2. On each federation server in your AD FS deployment, extract the files from the AD FS Agent kit. You can run the .msi file from any directory.
3. To install the AD FS Agent, double-click **RSA Authentication Agent v2 for Microsoft AD FS x64.msi** to start the Install Wizard, or from a command prompt, change the directory to the .msi file location, and run the following:

    ```
    msiexec /i "RSA Authentication Agent v2 for Microsoft AD FS x64.msi"
    ```

    To upgrade to the AD FS Agent, from a command prompt, change the directory to the .msi file location, and run the following:

    ```
    msiexec /i "RSA Authentication Agent v2 for Microsoft AD FS x64.msi" REINSTALL=ALL REINSTALLMODE=vomus
    ```

    If you encounter problems with the upgrade or want to create an installation log, run the following command instead:

    ```
    msiexec /i "RSA Authentication Agent v2 for Microsoft AD FS x64.msi" /l*v install.log REINSTALL=ALL REINSTALLMODE=vomus
    ```
4. Repeat steps 2 and 3 to install or upgrade the AD FS agent on all federation servers in your AD FS deployment.
5. Register the agent on the primary federation server:
    a. Sign into the Primary AD FS server where you installed the agent.
    b. Open a PowerShell command prompt.
    c. 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
    ```

    d. From the Main Menu, enter 4 to select **Register Agent**.

6. Restart Active Directory Federation Services (adfssrv) on each federation server in your AD FS deployment:
    a. Sign into each AD FS server where you installed the agent.
    b. Open a PowerShell command prompt.
    c. 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
    ```

    d. From the Main Menu, enter 3 to select **Restart AD FS**.
7. (Windows Server 2019 only) Change the AD FS theme from a right alignment to a center alignment. Do the following:
    a. On the Windows Server 2019 on which you installed or upgraded the agent, open a PowerShell command prompt.
    b. Enter the following to get details of the current theme:

    ```
    Get-AdfsWebConfig
    ```

    c. Enter the following to see the different themes that are supported by AD FS 2019:

    ```
    Get-AdfsWebTheme | Select Name
    ```

    d. Enter the following to change to a center alignment theme that is introduced in AD FS 2019:

    ```
    Set-AdfsWebConfig -ActiveThemeName DefaultAdfs2019
    ```

After you finish

- Test multifactor authentication on the AD FS agent. For instructions, see Chapter 4, “Configuring and Managing the Agent” in the *RSA Authentication Agent 2.0.3 for Microsoft AD FS Administrator’s Guide*. If you are unable to authenticate, see Chapter 5, “Troubleshooting,” in the *Administrator’s Guide*.
- (Optional) To allow users to set a Windows Hello for Business PIN or to authenticate from the iOS built-in mail app, you must download and deploy the updated RSA GPO templates that are available for AD FS Agent 2.0.2 or later and then disable the “Validate the Authentication Context” policy setting. For instructions, see Chapter 2, “Deploying Group Policy Object Templates” in the *RSA Authentication Agent 2.0.3 for Microsoft AD FS GPO Template Guide*.

Fixed Issues

The following issues are fixed in the cumulative AD FS Agent 2.0.3 release.

Issues Fixed in AD FS Agent 2.0.3

AAADFS-217. Fixed an issue that in some cases caused the AD FS Agent to send multiple verification requests for one unsuccessful authentication attempt.

AAADFS-202, AAADFS-212. Resolved an issue that in some cases caused a network connection failure between the AD FS Agent and the Cloud Authentication Service.

AADFS-185. The policy setting “AD FS username format sent to Authentication Manager” applies to RSA Authentication Manager and the Cloud Authentication Service. Updated the description in the GPO template and in the *RSA Authentication Agent 2.0.3 for Microsoft AD FS GPO Template Guide*.

AADFS-181. Fixed an issue in which the AD FS Agent did not support RSA Authentication Manager emergency access tokencodes that contain special characters.

Issues Fixed in AD FS Agent 2.0.2

AADFS-200. Resolved an issue in which users were unable to authenticate from the iOS built-in mail app from an external network.

AADFS-191. Corrected cosmetic issues with Windows Server 2019.

AADFS-182. Resolved an issue with setting a PIN for Windows Hello for Business

Issue Fixed in AD FS Agent 2.0.1

AADFS-179. Corrected a potential problem with device biometrics authentication.

Known Issues

This section describes known issues and workarounds.

Multifactor authentication fails with some versions of the iOS Safari web browser on non-English Windows Server operating systems

Tracking Number: AADFS-199

Problem: When the AD FS Agent is installed on non-English Windows Server operating systems, using some versions of the Safari web browser, such as iOS Safari 13.2, results in the error message Microsoft.Identity.Server.Web.WebConfigurationException.

Workaround: See the Microsoft TechNet article: *https://social.technet.microsoft.com/Forums/en-US/17425110-fe56-4ea5-bc11-3b67bd580b66/ad-fs-40-custom-mfa-provider-international-locales-and-style-sheet-exception?forum=ADFS*

Users unable to authenticate in the iOS built-in mail app

Tracking Number: AADFS-209

Problem: Users are unable to log on to the iOS built-in mail app, but they could log on to Microsoft Apps on the iphone, such as Teams and Outlook.

Workaround: Set the AD FS Agent policy setting “Validate the AD FS authentication context” to “Disabled.”

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.

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.

Trademarks

Intellectual Property Notice

Open Source License

This product may be distributed with open source code, licensed to you in accordance with the applicable open source license. If you would like a copy of any such source code, Dell Inc. or its subsidiaries will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. Dell Inc. or its subsidiaries may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to Dell Legal, 176 South St., Hopkinton, MA 01748, ATTN: Open Source Program Office.