SafeNet Agent for ADFS 2.43

CUSTOMER RELEASE NOTES

Build Number: 2.43.345
Issue Date: 6 December 2021
Document Part Number: 007-012590-004, Rev. E

Contents

Product Description

Active Directory Federation Services (AD FS) supports a federated identity management solution extending distributed identification, authentication, and authorization services to web-based applications across organization and platform boundaries.

Multi-Factor Authentication (MFA) has traditionally meant using a smart card or other second factor with AD-based authentication, such as Integrated Windows Authentication. This type of MFA can impose client-side requirements, such as smart card drivers, USB ports, or other client hardware or software that cannot always be expected with Bring Your Own Device (BYOD) client devices. AD FS introduces a pluggable MFA concept focused on integration with AD FS policy.

Resolved and Known Issues

Issue Severity and Classification

The following table serves as a key to the severity and classification of the issues listed in the **Resolved Issues** table and the **Known Issues** table, which can be found in the sections that follow.

Severity	Classification	Definition
C	Critical	No reasonable workaround exists
H	High	Reasonable workaround exists
M	Medium	Medium-level priority problems
L	Low	Low-level priority problems

Release Description

Release Summary – Active Directory Federation Services Agent 2.43

The SafeNet Agent for AD FS v2.43 resolves a customer-reported issue.

Resolved Issues

This release resolves an important issue since the previous release. Following list the details.

Severity	Issue	Synopsis
M	SASNOI-14088	**Summary:** Due to multiple IPs in header users were not able to authenticate. Authentication succeeds, when customer has configured header to contain multiple IP addresses.
M	SASNOI-14351	**Summary:** After upgrading to v2.41 or v2.42 date wise logging was disabled, now logs are generating with file location and date after the upgrade from v2.41 to v2.42 or v2.43.

Release Summary – Active Directory Federation Services Agent 2.42

The SafeNet Agent for AD FS v2.42 introduces new enhancements.

New Features and Enhancements

FIPS Support

> The FIPS mode within the operating system with AES-GCM and RSA key standards.

> The FIPS mode for decrypting the agent's BSID key.

Enhanced Security

> The **AES-GCM** encryption algorithm is now used to provide faster and a more secure way to protect data exchange between the SafeNet Agent for AD FS and the SAS/STA solution.

Release Summary – Active Directory Federation Services Agent 2.41

The SafeNet Agent for AD FS v2.41 resolves a customer-reported issue.

Resolved Issues

This release resolves an important issue since the previous release. Following list the details.

Severity	Issue	Synopsis
C	SASNOI-10621	**Summary:** The SafeNet Agent for AD FS now successfully facilitates iPhone users' login to Office365 with the PUSH authentication while using multiple ADFS server and Farm configuration on the agent.

Release Summary – Active Directory Federation Services Agent 2.42

The SafeNet Agent for AD FS v2.42 introduces new enhancement, and resolves a customer-reported issue.

AD FS 2019 (Windows Server 2019) Support

Support for AD FS 2019 (Windows Server 2019) is now added.

Use Alternate Login ID

On the **SAS MFA Plug-in Manager** window, on the **Policy** tab, under **Authentication Processing**, the **Use Alternate Login ID (e,g. Azure Login ID)** check box is added.

Resolved Issues

This release resolves an important issue since the previous release. Following list the details.

Severity	Issue	Synopsis
H	SASNOI-9909	**Summary:** Support for Authentication if alternate ID is used in Azure AD.

Release Summary – Active Directory Federation Services Agent 2.30

The SafeNet Agent for AD FS v2.30 introduces new enhancement, and resolves a customer-reported issue.

Support for Transport Layer Security v1.2

Support for Transport Layer Security (TLS) v1.2 protocol is now added.

Resolved Issues

This release resolves an important issue since the previous release. Following list the details.

Severity	Issue	Synopsis
M	SASNOI-9054	**Summary:** Descriptive instructions included for **Adding Relying Party Trust – Windows Server 2016** section.

Release Summary – Active Directory Federation Services Agent 2.21

Resolved Issues

This release resolves some important issues since the previous release. Following list the details.

Severity	Issue	Synopsis
H	SASNOI-7905	**Summary:** ACL and other reported vulnerabilities are now fixed for the agent.
H	SASNOI-7678	**Summary:** The agent is now able to fetch the correct IP (from multiple client IPs received in the Auth Request) and thus successfully perform the SafeNet authentication.
M	SASNOI-7476	**Summary:** The default registry key settings are now updated for the AD FS secondary server.

Release Summary – Active Directory Federation Services Agent 2.20

The SafeNet Agent for AD FS v2.20 introduces new features, enhances security and fixes customer-reported defects.

Proxy Settings

The **Proxy Settings** section (now available at **Start** > **All Programs** > **SafeNet** > **Agents** > **SAS MFA Plugin Manager** > **Communications**) ensures that if a proxy server is configured for the agent, all the requests will pass through the proxy.

For details, refer the *Installation and Configuration Guide*.

Active Directory Federation Services 4.0 Support

The SafeNet Agent for AD FS v2.20 now supports **AD FS 4.0**, which is the latest AD FS version released by Microsoft and comes bundled with **Windows Server 2016**. It has many new, useful in-built features for AD FS like support for multiple Lightweight Directory Access Protocol (LDAP) directories and greater flexibility for administering the AD FS configurations, off the shelf.

The SafeNet Agent for AD FS v2.20 accommodates these updates, on top of the existing features.

Character Support for Push SMS Grid Tokens

To quickly select PUSH, Grid or SMS (PGS) token to use with the AD FS agent, character support is now provided.

Irrespective of the option selected for the **Default OTP Policy** field, the 2FA **Passcode** field behaviour (if **Enter a passcode manually** option is selected) is decided by the character input; with ***p*** defaulting to trigger **PUSH** (OTP), ***s*** to **SMS** and ***g*** to **GrIDsure**.

On the other hand, if **Use my mobile to autosend a passcode** (default) option is selected for the **Passcode** field, a PUSH OTP will be triggered.

> **NOTE:** If we submit blank with **Enter a passcode manually** option selected for the **Passcode** field, the behaviour will be decided by the **Default OTP Policy** field.

Rebranding

The following components have been updated with Gemalto branding:

- Installation Wizard
- Management Console
- SafeNet Agent for AD FS Pages

Resolved Issues

This section describe the issues resolved in the SafeNet Agent for AD FS v2.20:

Severity	Issue	Synopsis
H	SASNOI-4298	**Summary:** To quickly select **P**USH, **G**rid or **S**MS (PGS) token to use with the AD FS agent, character support is now provided.
H	SASNOI-4167/ SASNOI-6258	**Summary:** MFA failure issue for AD FS agent deployed in an AD FS Farm is now resolved. The failures were encountered in both the cases, when an OTP is entered manually or if a Push OTP is requested, because the agent was sending an **@** symbol instead of the full username for authentication. The **@** symbol is not recognized by the SafeNet as a valid user name, thus resulting in failures. The AD FS agent is updated to work without Stickiness.
H	SASNOI-4128	**Summary:** The SafeNet MFA error, **SAML Message has wrong signature**, encountered while using SAML with MFA API is now resolved.
H	SASNOI-3573	**Summary:** Management UI (**Communications** tab of the **SAS MFA Plugin Manager**) now supports proxy settings, for single servers as well as for AD FS farm configurations.
H	SASIL-3180/ SASIL-2677	**Summary:** SafeNet Agent for AD FS now facilitates logon to Office 365 correctly with a case sensitive User ID.
H	SASIL-3067	**Summary:** SafeNet Agent for AD FS now operates correctly after performing a URL username parameter check.
H	SASIL-2912	**Summary:** SafeNet Agent for AD FS now operates correctly when working with a Relying Party.
C	SASIL-2833	**Summary:** SafeNet Agent for AD FS now operates correctly when working with a Device Registration Service.

Known Issues

This table provides a list of known issues as of the latest release.

Severity	Issue	Synopsis
H	SAS- 48759	**Summary:** Due to some technical limitations, Push OTP does not work for customers using Chrome or Edge browser. Push OTP users in an ADFS environment, do not receive push notification and hence are unable to complete their authentication journey. Customers using AD FS 4.0 on Windows Server 2016 and AD FS 3.0 on Windows Server 2012 are impacted. **Workaround:** • MFA is expected to work with push OTP service for Internet Explorer. • If Internet Explorer is not an option, we recommend the following to be executed from the ADFS server's command prompt, as a onetime activity: **Set-AdfsResponseHeaders -SetHeaderName "Content-Security-Policy" -SetHeaderValue "default-src 'self' https://*.sascloudservice.com https://*.safenetid.com 'unsafe-inline' 'unsafe-eval'; script-src 'self' https://ajax.googleapis.com 'unsafe-inline' 'unsafe-eval'; img-src 'self' data:;""**
H	SASNOI- 6483	**Summary:** SafeNet authentication may fail (with An error occurred. Contact your administrator for more information message) after installation or upgrade of an AD FS agent deployed in an AD FS Farm. In such a case, users will not be able to reach the SafeNet authentication page (after successful LDAP authentication) for all the requests serviced by secondary server(s). **Workaround:** After installation/ upgrade, restart the AD FS service in the secondary server(s).
M	SASIL-2102	**Summary:** When running Repair from Windows Control Panel, an error occurs. **Workaround**: None, will be fixed in a future release.

Compatibility and Upgrade Information

Interoperability

Operating Systems

> Windows Server 2012 R2*

> Windows Server 2016**

> Windows Server 2019***

NOTES:
SafeNet Agent for AD FS is only compatible with **AD FS 3.0 on Windows Server 2012 R2.*

***SafeNet Agent for AD FS is compatible with **AD FS 4.0** on Windows Server 2016 and 2019.*

****SafeNet Agent for ADFS is only compatible with **AD FS 2019** on Windows Server 2019.*

SafeNet Authentication Service

> SafeNet Authentication Service PCE 3.9.1 and later

> SafeNet Trusted Access

Additional Software Components

> Microsoft .NET Framework 4.8

> Microsoft PowerShell v3.0

Supported Web Browsers

> Internet Explorer 11

> Microsoft Edge (not supported on mobile devices)

> Mozilla Firefox

> Chrome

> Safari

Supported Authentication Methods

All tokens and authentication methods supported by SafeNet.

Upgrade

The SafeNet Agent for AD FS **v2.43** supports upgrade from **v2.01** onwards.

Upgrade from **v2.0** and earlier versions (i.e., **v1.0**, **v1.01**, **v2.0**) is not supported, but their settings can be migrated to the current version (**v2.43**).

For details, see *SafeNet Agent for AD FS v2.43 Installation and Configuration Guide*.

Product Documentation

The following product documentation is associated with the SafeNet Agent for AD FS 2.43:

- *SafeNet Agent for AD FS: Installation and Configuration Guide*

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click the **REGISTER** link.

Telephone Support

The support portal also lists telephone numbers for voice contact (Contact Us).

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.