

SafeNet Agent for AD FS 2.43

INSTALLATION AND CONFIGURATION GUIDE



Document Information

Product Version	2.43
Document Part Number	007-012546-004, Rev. F
Release Date	October 2023

Trademarks, Copyrights, and Third-Party Software

Copyright © 2023 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as “Thales”) information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make **any change or** improvement in the specifications data, information, and the like described herein, at any time.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE	6
Release Notes.....	6
Audience	6
Document Conventions.....	6
Command Syntax and Typeface Conventions	6
Notifications and Alerts	7
Related Documents.....	8
Support Contacts	8
Customer Support Portal	8
Telephone Support	8
Email Support	8
CHAPTER 1: Introduction	9
Applicability	9
Support for Push OTP Function.....	9
System Requirements.....	9
AD FS Overview.....	10
AD FS Authentication Concepts	10
Primary and Secondary Authentication	10
Authentication Flow	11
Invoking Multi-Factor Authentication.....	11
CHAPTER 2: Installation	12
Prerequisites	12
Pre-installation checklist	12
Adding Relying Party Trust – For AD FS 4.0 (on Windows Server 2016) and AD FS 2019 (on Windows Server 2019 and Windows Server 2022).....	12
Installing SafeNet Agent for AD FS.....	18
Upgrade and Migration.....	21
Upgrading to SafeNet Agent for AD FS 2.43.....	21
Migrating Settings to SafeNet Agent for AD FS 2.43.....	22
Removing Users and Groups.....	23
CHAPTER 3: Configuration	24
Configuring SafeNet Authentication Service Manager	24
Configuring Agent Key File	24
Configuring SafeNet Agent for AD FS	25
Policy	25
Communications	27
Logging	29
AD FS Federation Server Farm	30
Localization	32

Global Authentication Policy	37
Enforcing Multi-Factor Policies in AD FS 3.0 (on Windows Server 2012 R2) and AD FS 4.0 (on Windows Server 2016)	37
Checking Multi-Factor Policies in ADFS 2019 (on Windows Server 2019 and Windows Server 2022)	38
CHAPTER 4: Working with Office 365	40
Logging to Office 365	40
Sign-In Window Examples	41

PREFACE

This document describes how to install and configure SafeNet Agent for AD FS.

Release Notes

The Customer Release Notes (CRN) document provides important information about this release that is not included in other customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, and known issues for this release.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Agent for AD FS users and security officers, the key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Thales are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Document Conventions

This section describes the conventions used in this document.

Command Syntax and Typeface Conventions

This document uses the following conventions for command syntax descriptions, and to highlight elements of the user interface.

Convention	Description
bold	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > Command-line commands and options (Type dir /p.) > Button names (Click Save As.) > Check box and radio button names (Select the Print Duplex check box.) > Window titles (On the Protect Document window, click Yes.) > Field names (User Name: Enter the name of the user.)

	<ul style="list-style-type: none"> > Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) > User input (In the Date box, type April 1.)
<i>italic</i>	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document. For example: Refer to “ Error! Reference source not found. ” on page Error! Bookmark not defined.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a b c] [<a> <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a b c } { <a> <c> }	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Notifications and Alerts

Notifications and alerts are used to highlight important information or alert you to the potential for data loss or personal injury.

Tips

Tips are used to highlight information that helps to complete a task more efficiently.

TIP: This is some information that will allow you to complete your task more efficiently.

Notes

Notes are used to highlight important or helpful information.

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss.

CAUTION! Exercise caution. Contains important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

****WARNING**** Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Related Documents

The following document(s) contain related or additional information:

- > SafeNet Agent for AD FS v2.43: Customer Release Notes

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. 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.

CHAPTER 1: Introduction

Applicability

The information in this document applies to:

- > SafeNet Authentication Service PCE 3.9.1 and later
- > SafeNet Trusted Access

Support for Push OTP Function

The SafeNet Agent for Active Directory Federation Services (AD FS) supports the Push OTP function with MobilePASS+ for,

- > SafeNet Trusted Access
- > SafeNet Authentication Service PCE 3.9.1 and later

System Requirements

Platforms	<ul style="list-style-type: none"> > Windows Server 2012 R2* > Windows Server 2016** > Windows Server 2019*** > Windows Server 2022*** <p><u>Notes:</u></p> <p><i>*SafeNet Agent for AD FS is only compatible with AD FS 3.0 on Windows Server 2012 R2.</i></p> <p><i>**SafeNet Agent for AD FS is only compatible with AD FS 4.0 on Windows Server 2016.</i></p> <p><i>***SafeNet Agent for ADFS is only compatible with AD FS 2019 on Windows Server 2019 and Windows Server 2022.</i></p>
Architecture	64-bit
Additional Software Components	<ul style="list-style-type: none"> > Microsoft .NET Framework 4.8 > Microsoft PowerShell v3.0
Authentication Methods	All tokens and authentication methods supported by the SafeNet server.

Web Browsers

- > Internet Explorer 11
- > Microsoft Edge (not supported on mobile devices)
- > Mozilla Firefox
- > Google Chrome
- > Safari

AD FS Overview

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 the AD FS policy.

AD FS Authentication Concepts

The following lists some important AD FS concepts.

Primary and Secondary Authentication

Previous versions of AD FS have supported authenticating users against Active Directory using any of the following methods:

- > Integrated windows authentication
- > Username and password
- > Client certificate [client Transport Layer Security (TLS), including smart card authentication]

The above methods are still supported, but are now called “primary authentication” because Microsoft has introduced a new feature called secondary, or “additional”, authentication. This is where the SafeNet Agent for AD FS, an MFA plugin, comes in.

Secondary authentication occurs immediately after primary authentication and authenticates the same AD user. Once primary authentication is complete and successful, AD FS invokes the external authentication handler. This handler invokes an additional authentication provider, either an in-box AD FS provider or an external MFA provider, based on protocol inputs and policy. AD FS passes the primary authenticated user’s identity to the additional authentication provider, which performs the authentication and hands the result back. At this point, AD FS continues executing the authentication/ authorization policy and issues the token accordingly.

Authentication Flow

AD FS provides extensible MFA through the concept of additional authentication provider that is invoked during secondary authentication. External providers can be registered in AD FS. Once a provider is registered with AD FS, it is invoked from the AD FS authentication code via specific interfaces and methods that the provider implements and that AD FS calls. Because it provides a bridge between AD FS and an external authentication provider, the external authentication provider is also called as an AD FS MFA adapter.

Invoking Multi-Factor Authentication

There are two ways to configure AD FS to invoke multi factor authentication—policy configuration or via the WS-Federation or SAML protocol token request.

Via policy, AD FS introduces a new rule set called Additional Authentication Rules that are used for triggering MFA. As with many other settings in AD FS, you can set these rules at a global level or at the relying party trust level.

As part of the new rule set, AD FS introduces a new claim type and value to refer to MFA. When this claim type and value is generated via an additional authentication rule, AD FS will invoke the external authentication handler, and hence the provider(s) configured on the system. If more than one provider is enabled in AD FS, the user will see a method choice page that displays the friendly name of each provider and allows the user to select one by clicking on it.

CHAPTER 2: Installation

Prerequisites

Pre-installation checklist

Complete the following tasks before installation:

- > Enable AD FS
- > Install Microsoft .NET Framework 4.8

NOTE:

- > The installer will automatically download and install it on the **Primary Server** if it is not already available.
- > It needs to be installed manually on the **Secondary Server(s)** to enable the MFA after the installation/upgrade to this version.

- > Execute PowerShell command, if you are using AD FS 4.0:

```
Set-AdfsProperties -EnableIdpInitiatedSignonPage $true
```

[AD FS 4.0 login page, <https://<FQDNofTheFederationService>/adfs/ls/IdPInitiatedSignOn.aspx> is disabled, by default. Executing the PowerShell command enables the page.]

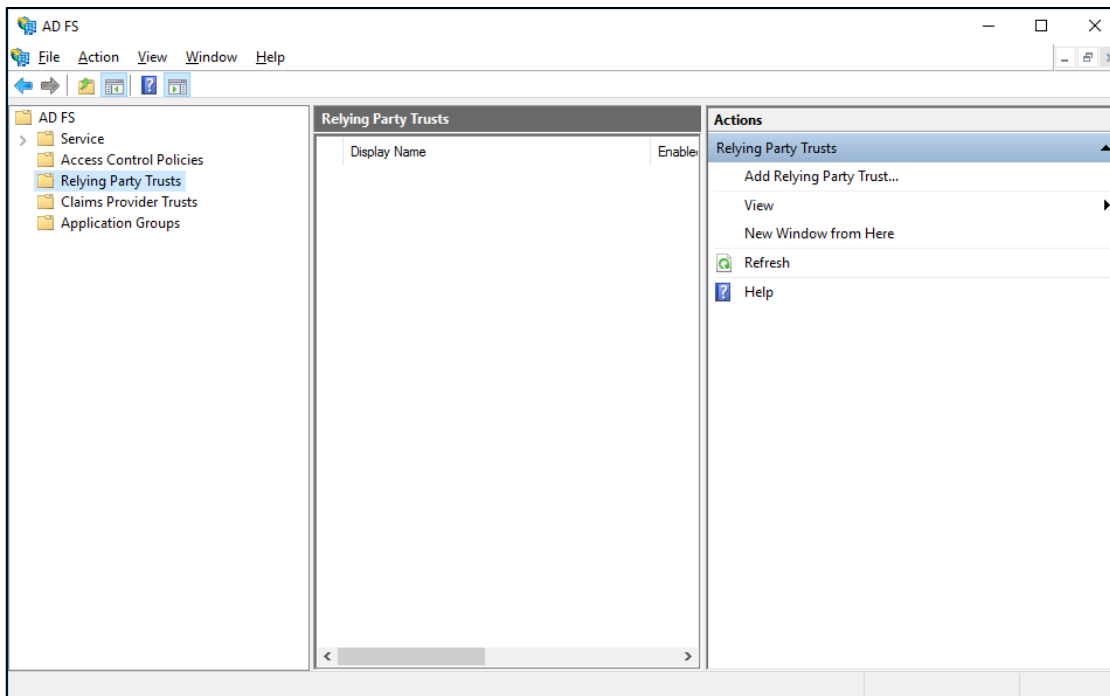
Adding Relying Party Trust – For AD FS 4.0 (on Windows Server 2016) and AD FS 2019 (on Windows Server 2019 and Windows Server 2022)

For **AD FS 3.0** (on **Windows Server 2012 R2**), the Relying Party Trust is already configured to **Device Registration**.

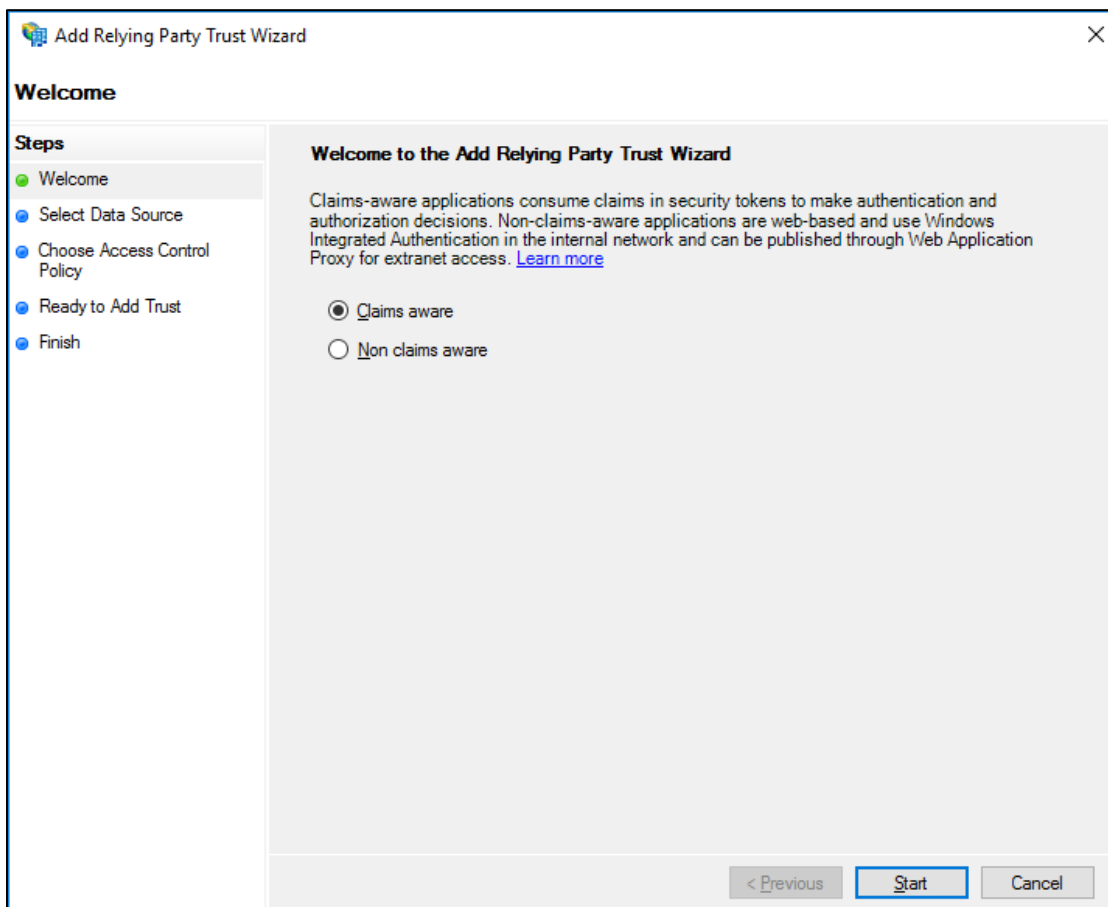
For **AD FS 4.0** (on **Windows Server 2016**) and **AD FS 2019** (on **Windows Server 2019** and **Windows Server 2022**), the Relying Party Trust needs to be added manually. Unless the relying party trust is configured, the MFA page will not appear. After a user successfully logs in, using the AD, perform the following steps to view the OTP page (with two sign in options):

1. Open AD FS Management.

2. Highlight **Relying Party Trusts**, and click **Add Relying Party Trust** from the **Actions** pane.



3. Select **Claims aware** radio option, and click **Start**.



4. Enter the URL of the metadata file.

`https://<fqdn>/federationmetadata/2007-06/federationmetadata.xml`

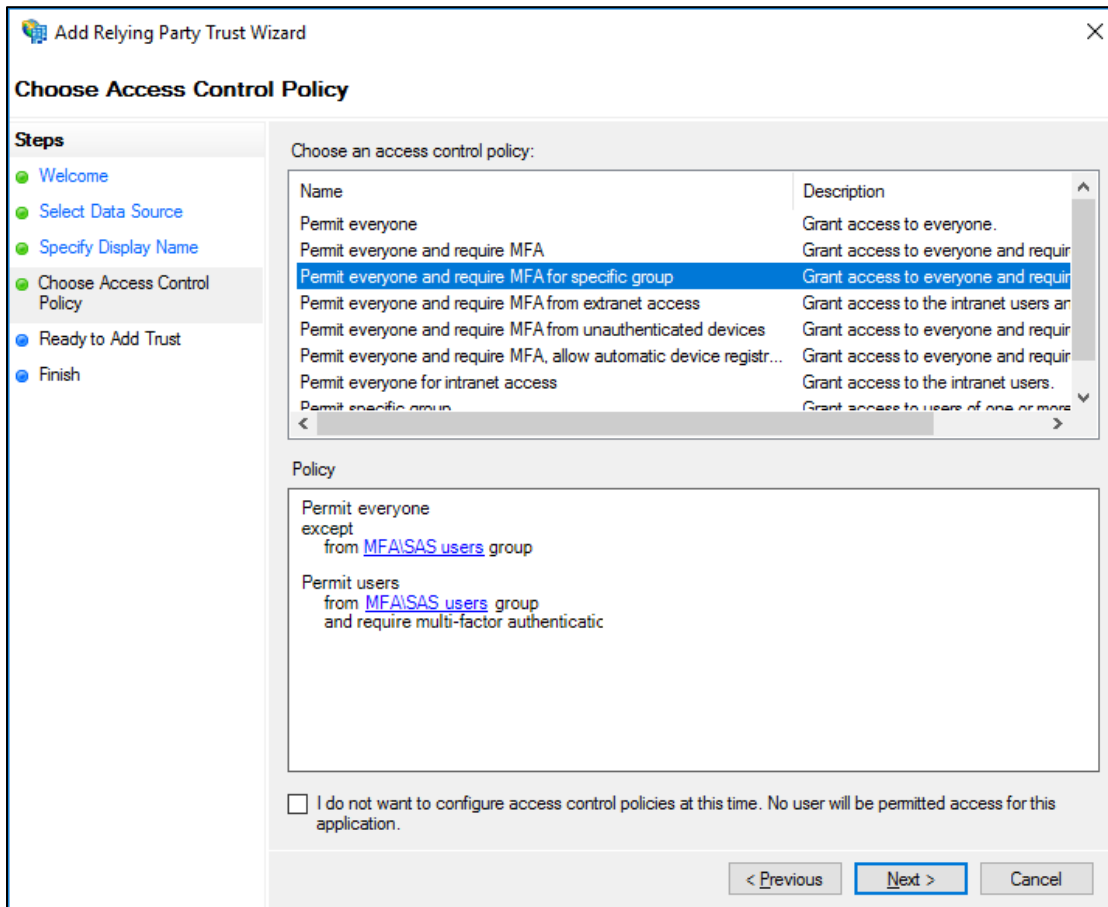
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Select Data Source'. On the left, a 'Steps' pane shows a progress indicator with five steps: 'Welcome' (completed), 'Select Data Source' (current step), 'Choose Access Control Policy', 'Ready to Add Trust', and 'Finish'. The main area contains the instruction: 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' (selected). Below it, text says 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' A text box labeled 'Federation metadata address (host name or URL):' contains the URL 'https://fs.mfa.local/federationmetadata/2007-06/federationmetadata.xml'. Below the text box is an example: 'Example: fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file'. Below it, text says 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' A text box labeled 'Federation metadata file location:' is empty, with a 'Browse...' button to its right. 3. 'Enter data about the relying party manually'. Below it, text says 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

5. In the **Display name** field, enter a display name, and click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Specify Display Name' step. The window title is 'Add Relying Party Trust Wizard' with a close button (X) in the top right corner. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists the following steps: 'Welcome' (completed), 'Select Data Source' (completed), 'Specify Display Name' (current step), 'Choose Access Control Policy' (pending), 'Ready to Add Trust' (pending), and 'Finish' (pending). The main area contains the instruction 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' text box containing 'fs.mfa.local'. Underneath is a 'Notes:' text area, which is currently empty. At the bottom right, there are three buttons: '< Previous' (disabled), 'Next >' (active/highlighted), and 'Cancel' (disabled).

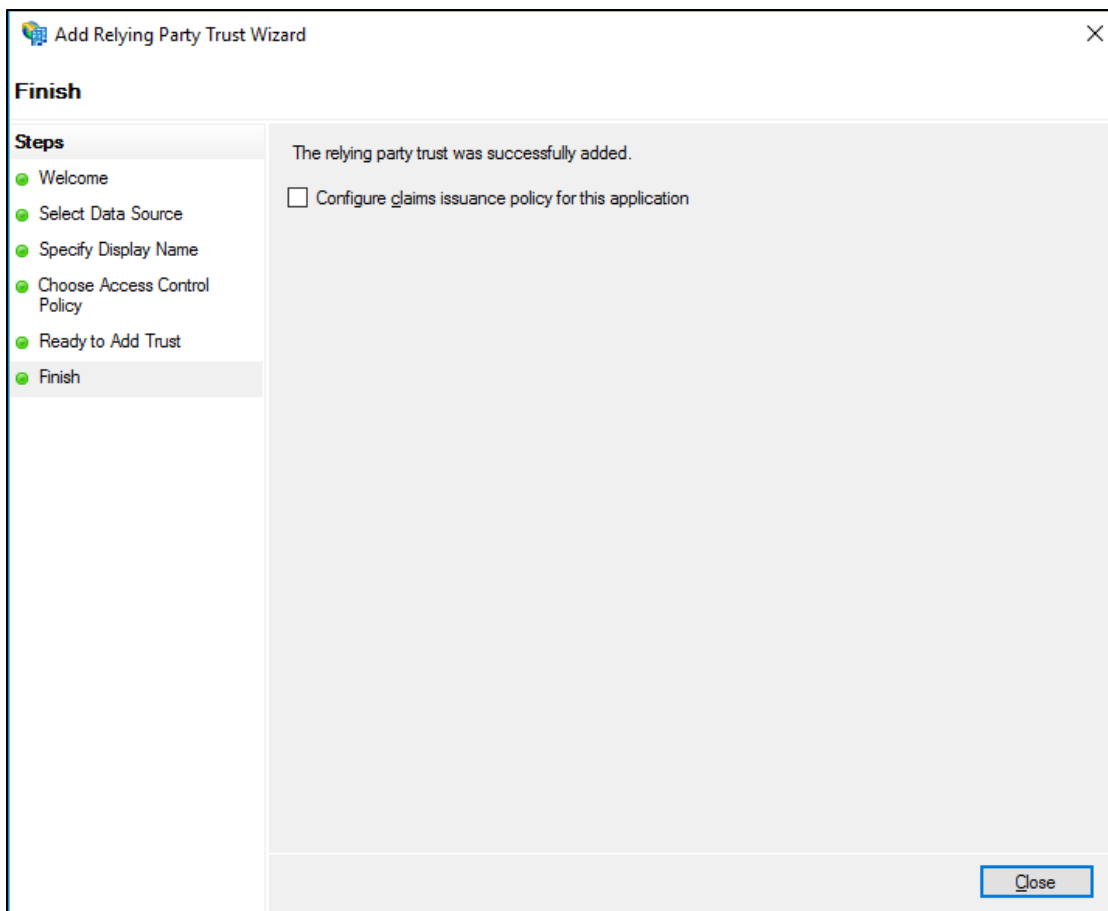
6. Select an Access Control Policy, and click **Next**.

In the following example, the **Permit everyone and require MFA for specific group** option is selected.



7. Click **Next**.

8. Clear the **Configure claims issuance policy for this application** checkbox, and click **Close**.



NOTE: Documentation to add Relying Party Trust for Windows Server 2016 references the Microsoft documentation. Please refer to the official documentation for detailed, accurate, and updated instructions

Technical Caveat

Known Issue

Due to some technical limitations, Push OTP does not work for customers using Chrome or Edge browsers. 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, it is recommended to execute the following command from the ADFS server's command prompt, as a one-time 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;""
```

NOTE: Alternatively, customers can upgrade to AD FS 2019 on Windows Server 2019 or Windows Server 2022 as the long-term fix.

Installing SafeNet Agent for AD FS

NOTE: Always work in **Run as administrator** mode when installing, uninstalling, enabling, or disabling the SafeNet Agent for AD FS.

To install the SafeNet Agent for AD FS:

1. Run as administrator the SafeNet Agent for AD FS installer:

```
SafeNetAuthentication Service Agent for ADFS.exe
```

2. On the **Welcome to the InstallShield Wizard for SafeNet Authentication Service Agent for ADFS** screen, click **Next**.



3. On **License Agreement** window, read the software license agreement and to proceed, select **I accept the terms in the license agreement**, and click **Next**.

The screenshot shows the 'License Agreement' window. At the top left, it says 'License Agreement' and 'Please read the following license agreement carefully.' The Gemalto logo is in the top right. The main content area is titled 'SOFTWARE LICENSE AGREEMENT' and contains the following text: 'IMPORTANT - READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THIS SOFTWARE. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, YOU MAY NOT INSTALL OR USE THIS SOFTWARE.' Below this text are two radio buttons: 'I accept the terms in the license agreement' (which is selected) and 'I do not accept the terms in the license agreement'. There is a 'Print' button to the right of the radio buttons. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

4. On **Customer Information** window, perform the following steps:
 - a. In the **User Name** field, enter your user name.
 - b. In the **Organization** field, enter the name of your organization.
 - c. Click **Next**.

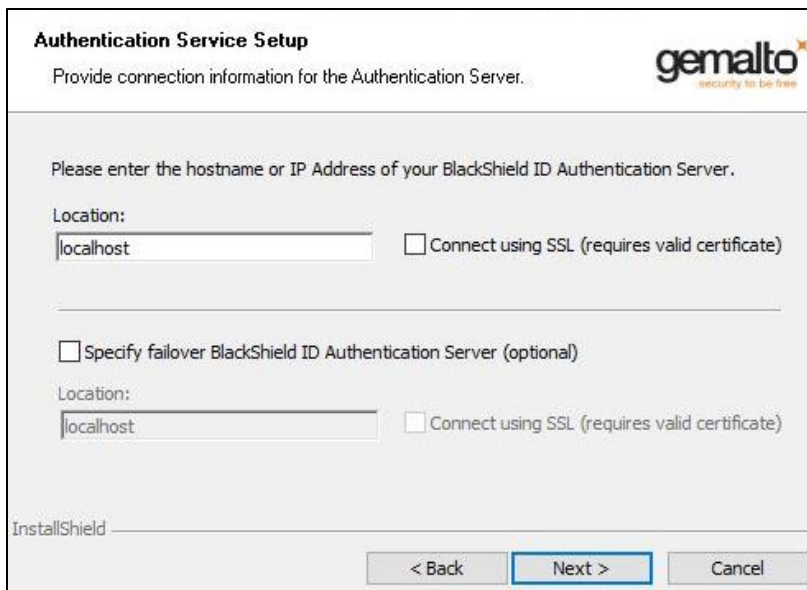
The screenshot shows the 'Customer Information' window. At the top left, it says 'Customer Information' and 'Please enter your information.' The Gemalto logo is in the top right. There are two text input fields: 'User Name:' with 'Windows User' entered, and 'Organization:' which is empty. Below these fields is the text 'Install this application for:' followed by two radio buttons: 'Anyone who uses this computer (all users)' (which is selected) and 'Only for me (Windows User)'. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

5. On **Destination Folder** window, do one of the following:

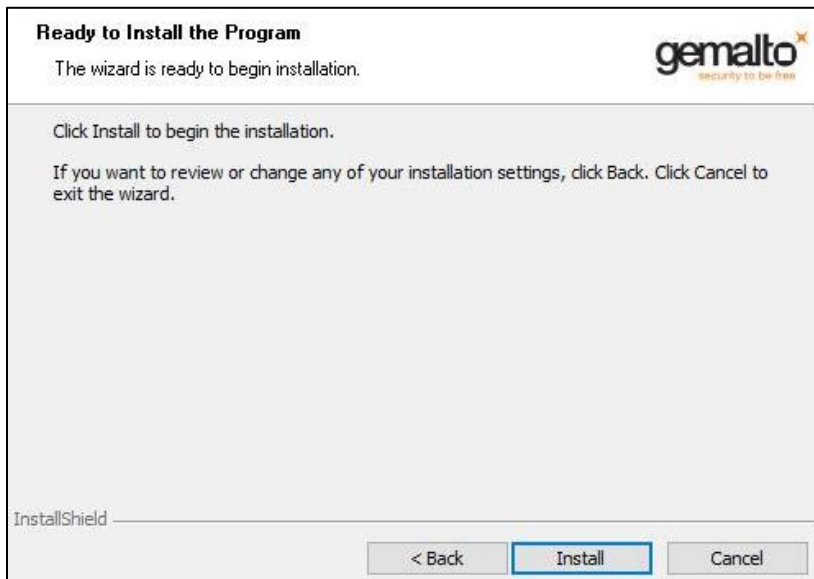
- a. To accept the default installation destination folder, click **Next**.
- b. To change the installation folder, other than the default one, click **Change**, and then browse to locate and select the required folder.
- c. Click **Next**.



6. On **Authentication Service Setup** window, enter the hostname or IP address of the SafeNet primary and failover servers.



7. On **Ready to Install the Program** window, click **Install**.



8. When the installation process completes, the **Installshield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.



Upgrade and Migration

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**).

Upgrading to SafeNet Agent for AD FS 2.43

To upgrade, execute the SafeNet Agent for AD FS v2.43 installation on the same computer (having) the installed version. Once the installation completes, enable the agent from the SAS MFA Plug-In Manager.

Migrating Settings to SafeNet Agent for AD FS 2.43

NOTES:

- Upgrade from existing installations earlier than version 2.01 is blocked, and will cause an error message indicating that uninstall is required.
- Always work in **Run as administrator** mode when installing, uninstalling, enabling, or disabling the SafeNet Agent for AD FS.
- Disable the agent first, before migrating its settings.

To migrate the settings, perform the following steps:

1. In the SafeNet Agent for AD FS v2.0 (or an earlier version) installation folder (C:\Program Files\SafeNet\SAS\SafeNetMFA\ini), copy the *SAFENET-MFA.ini* file and save it for later use.
2. Uninstall the SafeNet Agent for AD FS.
3. Delete all remaining installation folders (C:\Program Files\SafeNet\SAS\SafeNetMFA).
4. Install the latest version of SafeNet Agent for AD FS.
5. Replace the *SAFENET-MFA.ini* file in the latest version of SafeNet Agent for AD FS installation folder (C:\Program Files\SafeNet\SAS\SafeNetMFA\ini) with the file saved from the previous version.
6. Enable the SafeNet Agent for AD FS from the SAS MFA Plug-In Manager, and apply the settings.

Updating Localization Settings

After replacing the *SAFENET-MFA.ini* file in the latest version of SafeNet Agent for AD FS installation folder with the file saved from version 2.0 or earlier, and enabling the SafeNet Agent for AD FS in the SafeNet server, new messages related to the Push OTP function are added to the *.ini* file. However, these messages will be in English-USA, the default language. For localized languages, the phrases must be translated.

The affected messages include messages 2021 to 2029:

2021=Your request timed out. Please try again.
2022=Error when creating autosend message, Please contact administrator.
2023=Authentication process was canceled.
2024=Passcode was not autosent. Please try again or enter passcode.
2025=Auto push has failed, Authentication ID not found, Please contact administrator.
2026=Auto push has failed, Authentication ID conflicted, Please contact administrator.
2027=Auto push has failed, unknown error.
2028=Authentication failed.
2029=Authentication request was cancelled. Please try again.

To translate the messages, open the *SAFENET-MFA.ini* file in a text editor and edit the required text.

Removing Users and Groups

NOTE: It is not necessary to remove users and groups from the AD FS server if a later version of the SafeNet Agent for AD FS is to be installed.

After uninstalling or deactivating the SafeNet Agent for AD FS, the users and groups must be removed from the AD FS server. Failure to do so may result in subsequent failure to authenticate through the AD FS server.

NOTE: To deactivate the SafeNet Agent for AD FS, open the SAS MFA Plug-In Manager Policy tab and clear the **Enable Agent** checkbox.

See **Configuring SafeNet Agent for AD FS**.

To remove users and groups from the AD FS server 3.0:

1. In the AD FS management console, select **Authentication Policies > Per Relying Party Trust > Edit Custom Multi-factor Authentication**.
2. On the **Edit Authentication Policy for Device Registration Service** window, select the **Multi-factor** tab.
3. In the **Users/Groups** box, remove all listed users and groups.

To edit MFA policy for users and groups in the AD FS server 4.0:

1. In the AD FS management console, click **Relying Party Trust**.
2. Select the required Relying Party Trust application and **Edit Access Control Policy**.
3. Select any policy (from the **Access control policy** list) that does not require MFA, and apply the changes.

CHAPTER 3: Configuration

Configuring SafeNet Authentication Service Manager

Communication must be established between the SafeNet Agent for AD FS and the SafeNet server.

To configure, add an Auth Node in SAS/STA as follows:

1. In the SAS/STA management console, select **VIRTUAL SERVERS > COMMS > Auth Nodes**.
2. Enter the name or IP address of the computer where the SafeNet Agent for AD FS is installed.

For details, refer to the *SafeNet Authentication Service (SAS) Service Provider Administrator Guide*.

Configuring Agent Key File

This agent uses an encrypted key file to communicate with the authentication web service. This ensures all communication attempts made against the web service are from valid recognized agents.

A sample key file (*Agent.bsidkey*) has been installed for evaluation purposes; however, it is recommended to generate your own key file for a production environment, as the sample file is publicly distributed.

To load the key file:

1. In the SAS, select **COMMs** tab and download an agent key file from the **Authentication Agent Settings** section.
2. To open the **SAS MFA Plugin Manager**, select **Start > All Programs > SafeNet > Agents > SAS MFA Plugin Manager**.
3. Click **Communications** tab.
4. Click **Agent Encryption Key File** browse button and navigate to the agent key file.

NOTE: It is strongly recommended to use the default location for the Agent Encryption Key File, to avoid possible errors.

5. Click **Apply**.
6. Close and re-open the SAS MFA Plugin Manager.

NOTE: The final step, **Close and re-open the AD FS Agent Manager** is required to ensure that the new key file (*.bsidkey*) is recognized.

Configuring SafeNet Agent for AD FS

Configure the SafeNet Agent for AD FS in the SAS MFA Plugin Manager.

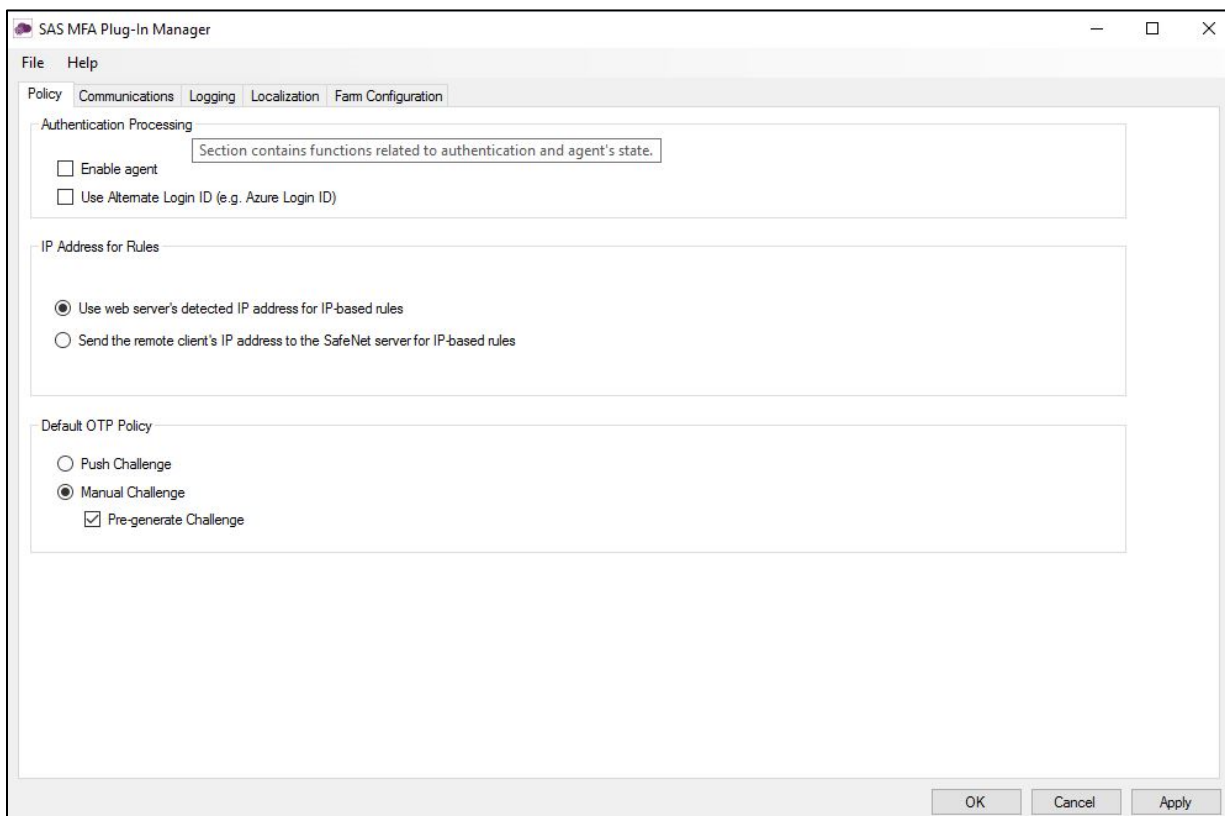
To open the SafeNet Agent for AD FS MFA Policy Manger:

Select **Start > All Programs > SafeNet > Agents > SAS MFA Plugin Manager**.

Policy

To configure the SafeNet Agent for AD FS policy:

1. On **SAS MFA Plug-In Manager** window, click **Policy** tab.



Complete the following fields, and click **Apply**.

Field	Description
Enable Agent	Select to enable the SAS for AD FS agent. Note: If you de-activate the agent, by clearing the Enable Agent checkbox, you must remove users and groups from the AD FS server. Failure to do so may result in failure of authentication though the AD FS Server. See Removing Users and Groups on page 23.
Use Alternate Login ID (e.g. Azure Login ID)	Select this option if you are using an alternate login ID in the connected AD application (for example, Azure).

Field	Description
IP Address for Rules	Select one of the following: <ul style="list-style-type: none"> > Use web server’s detected IP address for IP based rules > Send the remote client’s IP address to the SafeNet server for IP based rules
Default OTP Policy	Select from the following: <ul style="list-style-type: none"> > Push Challenge – to use the Push OTP Feature <p>Note: The SafeNet Agent for AD FS supports the Push OTP function with MobilePASS+ when working with SAS PCE/SPE 3.9.1 and later versions.</p> <ul style="list-style-type: none"> > Manual Challenge – For using any token <ul style="list-style-type: none"> • Pre-Generate Challenge– Select to display the grid. If this option is not selected, the user can display the GrIDsure grid by leaving the OTP field empty and clicking Submit.

Communications

1. On **SAS MFA Plug-In Manager** window, click **Communications** tab.

The screenshot shows the 'SAS MFA Plug-In Manager' window with the 'Communications' tab selected. The 'Authentication Server Settings' section includes:

- Primary Server IP: localhost (with a checked 'Use SSL (requires a valid certificate)' checkbox)
- Secondary Server IP (optional): (empty field, with an unchecked 'Use SSL (requires a valid certificate)' checkbox)
- Ignore server SSL certificate check: (unchecked checkbox)
- Agent Encryption Key File: c:\program files\safenet\sas\safenetmfa\bsidkey\Agent.bsIDKey (with a 'Browse...' button)
- TCP/IP Call Timeout (in seconds): 30 (dropdown menu)
- User ID Format: 'Include realm ("username@domain.com" is sent as SAS User ID)' (selected radio button)

 The 'Authentication Test' section has input fields for 'User Name' and 'Passcode', and a 'Test' button. The 'Server Status Check' section has a 'Test' button. The 'Proxy Settings' section has an unchecked 'Use Proxy' checkbox and fields for 'Proxy Server', 'Port', 'Username', and 'Password'. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

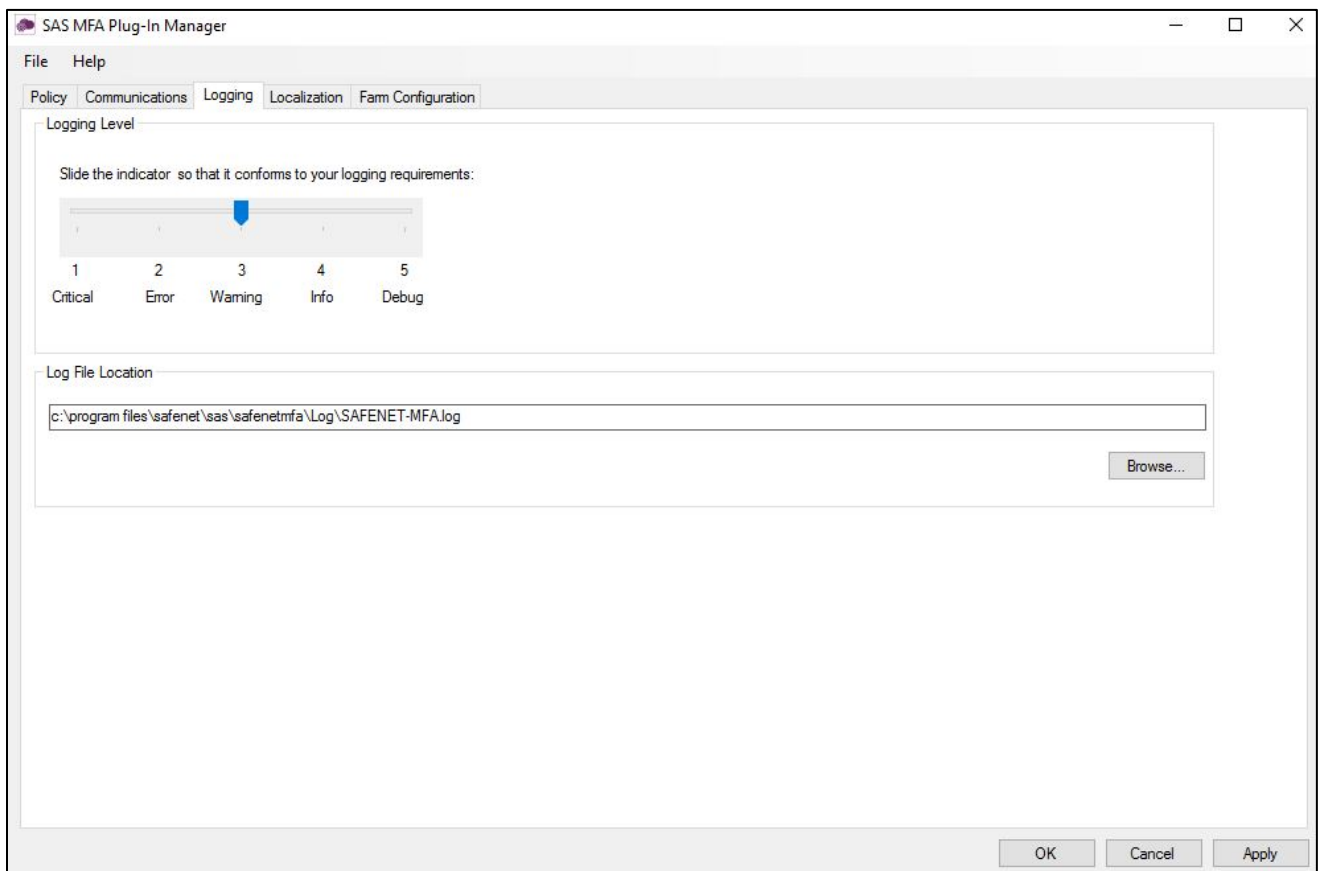
Complete the following fields, and click **Apply**:

Field	Description
Primary Server IP (IP:Port)	Used to configure the IP address/ hostname of the primary SafeNet server. The default is port 80. Alternatively, Use SSL can also be selected. The default TCP port for SSL requests is 443.
Secondary Server IP (optional)	Used to configure the IP address/ hostname of the failover SafeNet server. The default is port 80. Alternatively, Use SSL can also be selected. The default TCP port for SSL requests is 443.
Ignore server SSL certificate check	Select the checkbox to disable the SSL server certificate error check on the agent. It is unchecked by default. If customers are using the on-premise deployment of SAS/STA within a well-controlled network (where self-signed certificates are used and cannot be properly validated by the AD FS Agent), this checkbox needs to be selected. NOTE: We strongly recommend the use of SSL certificates.
Agent Encryption File Key	Used to specify the location of the SafeNet Agent for AD FS key file. For details, see Configuring Agent Key File .

Field	Description
TCP/IP Call Timeout (in seconds)	Sets the maximum timeout value in seconds for authentication requests sent to the SafeNet server.
User ID Format	<p>Select the required ID format for the SAS/STA usernames:</p> <ul style="list-style-type: none"> > Include Realm (“Username@domain.com” is sent as SAS/STA User ID) > Strip realm (“Username” is sent as User ID) <p>Note: The realm stripping feature applies to SAS/STA usernames only. Active Directory usernames are not affected.</p>
Authentication Test	<p>This function allows administrators to test authentication between the SafeNet Agent for AD FS and the SafeNet server.</p> <p>Enter User Name and Password and click Test. The result of the test is displayed in the Authentication Test Result text box.</p> <p>Notes:</p> <ul style="list-style-type: none"> • The behavior of the test will be in accordance with the realm stripping configuration. For example, if realm stripping has been activated and the user name is entered in the format username@domain, the domain will be removed. • The test works with manual OTP. Push OTP is not supported.
Server Status Check	This function performs a communication test to verify a connection to the SafeNet server.
Proxy Settings	<p>Enter the following details:</p> <ul style="list-style-type: none"> • Use Proxy: Select the checkbox to connect the SAS/STA via a proxy server. • Proxy Server: Enter IP address of the proxy server (mandatory). • Port: Enter proxy server port (mandatory). • Username: The proxy server user name (if required). • Password: The proxy server password (if required).

Logging

1. On **SAS MFA Plug-In Manager** window, click **Logging** tab.



Complete the following settings, and click **Apply**:

Field	Description
Logging Level	Set the required logging level (default value 3): 1 Critical - only critical 2 Error - critical and errors 3 Warning - critical, errors, and warnings 4 Info - critical, errors, warnings, and information messages. 5 Debug - all available information
Log File Location	Specifies the location of the log files. The log file is rotated on a daily basis.

AD FS Federation Server Farm

In an AD FS federation server farm using Windows Internal Database (WID), the first server in the farm acts as the primary server, hosting a read/write copy of the database. Secondary servers then replicate the configuration data into their read-only database. The secondary servers are fully functional federation members and can service the clients in the same way as the primary server. However, they are unable to write any configuration changes to the WID. Therefore, when the SafeNet Agent for AD FS is installed and configured on the primary server, to ensure that configuration is replicated on the secondary servers, the secondary servers must be included in the farm through the **Farm Configuration** tab.

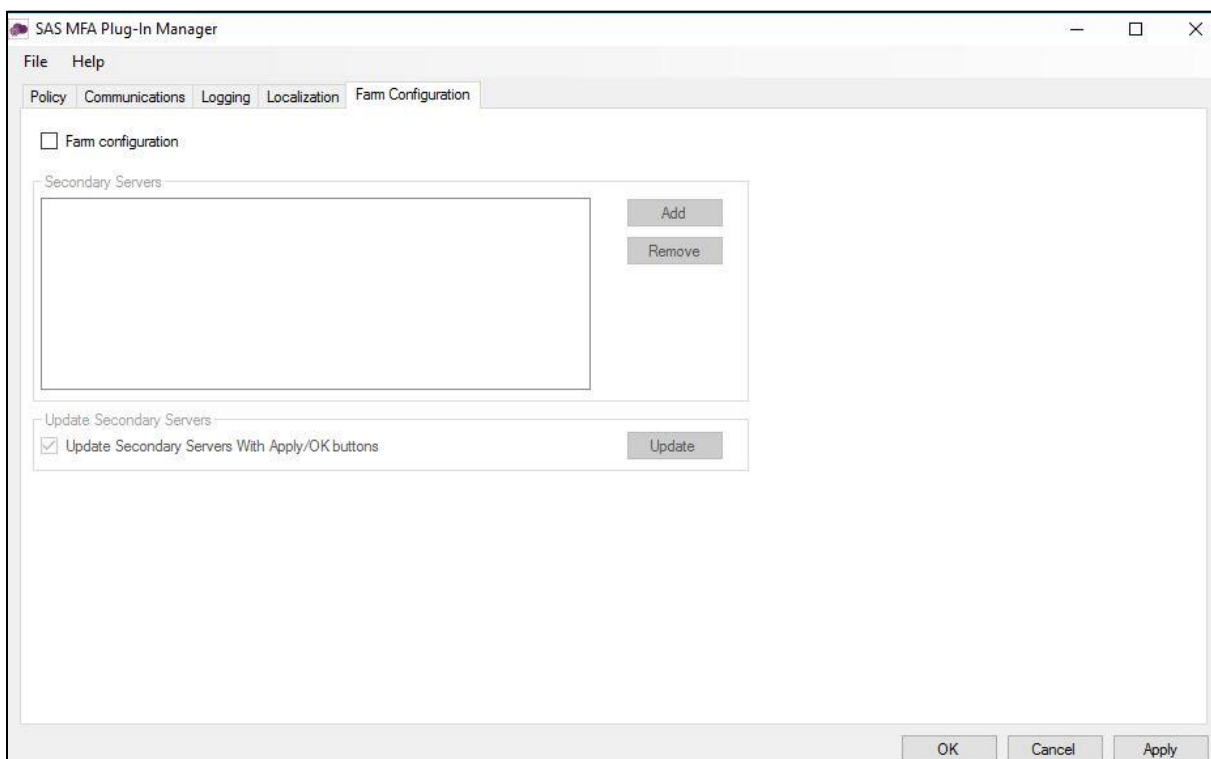
NOTE:

- You need to install the **.Net FW version 4.8** manually on the **Secondary Server(s)** to enable the MFA after installation/upgrade to the current version.
- To configure an AD FS Federation Server farm, you must be logged-in as a Domain Administrator.

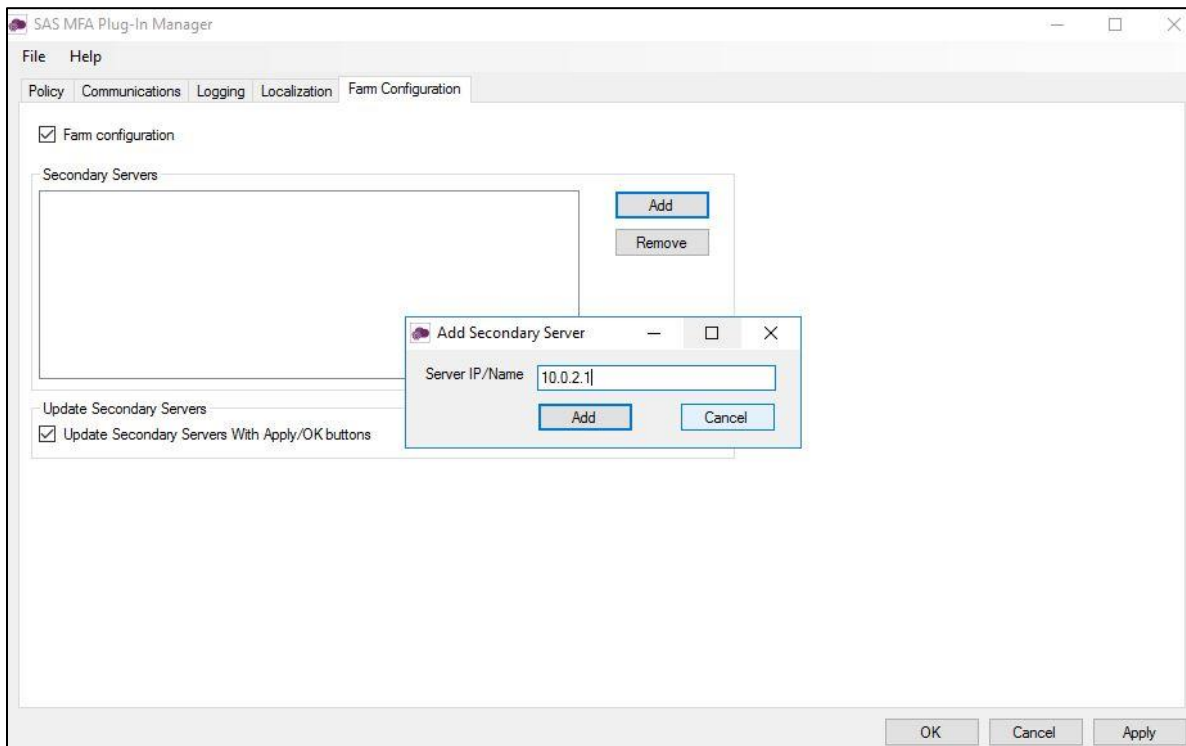
To configure the server farm:

NOTE: You first need to Enable the agent on **Primary Server**. Then, Disable the agent and click **Apply**.

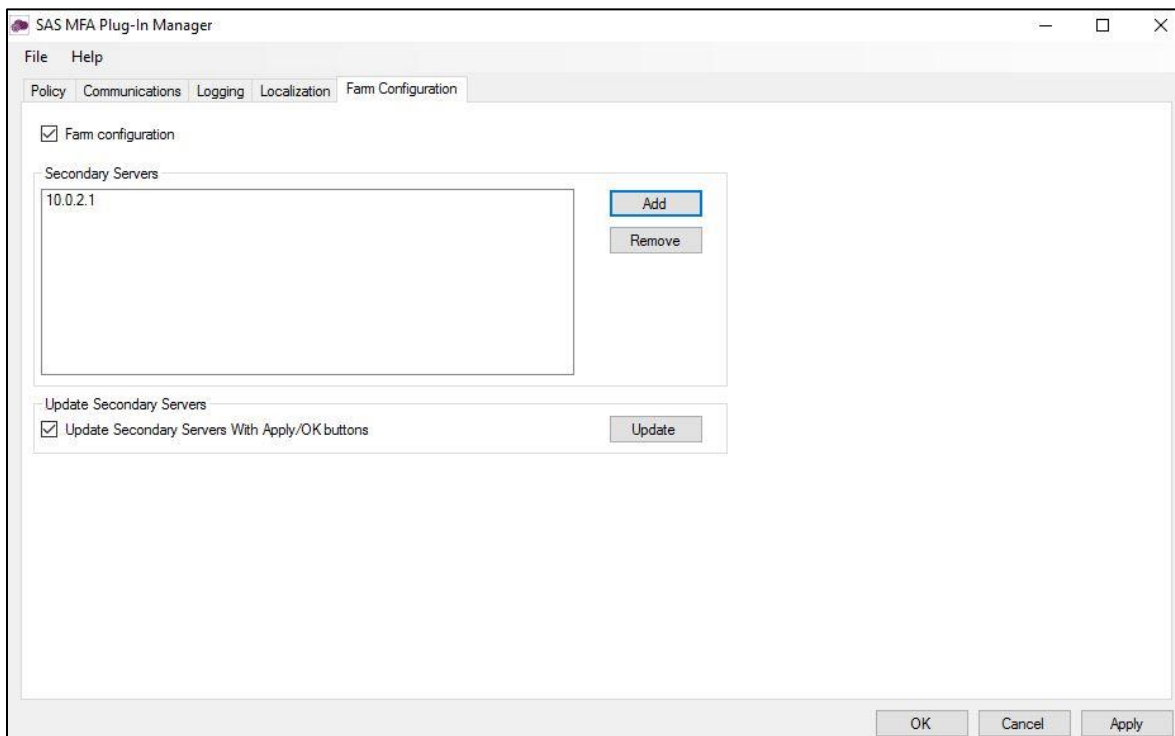
1. On **SAS MFA Plug-In Manager** window, click **Farm Configuration** tab.
2. Select **Farm configuration**.
3. Click **Add**.



4. In **Add Secondary Server** window, in the **Server IP/Name** field, enter the IP address or name of the server to be added, and click **Add**.



5. The server is added to the **Secondary Servers** list.



Repeat the above steps for each secondary server.

6. To update the configuration to secondary servers whenever the agent is activated, select **Update Secondary Servers With Apply/OK buttons**.
7. The secondary servers will be updated when you Enable the agent, click **OK** and **Apply**. To update immediately, select **Update**.

NOTE: Ensure that **Turn on file and printer sharing** option is selected for the **File and printer sharing** field (available at the following location):

Control Panel > All Control Panel Items > Network and Sharing Center > Advanced sharing settings > Domain

Following configuration of the AD FS federation server farm, the following folders are installed on each server:

C:\Program Files\SafeNet\SAS\SafeNetMFA

C:\Windows\Microsoft.NET\assembly\GAC_MSIL\SafenetExtAuthMethod

C:\Windows\Microsoft.NET\assembly\GAC_MSIL\AgentEncryptor

C:\Windows\Microsoft.NET\assembly\GAC_MSIL\log4net

Localization

Localization is controlled by the *INI* file, which is preconfigured for English-United States and French-Canadian.

NOTE: The French-Canadian text is for demonstration purposes only. The translation should be proofed by a professional translator before use.

Setting Additional Localizations

The *INI* file describes the available options for setting additional localizations. Adding a new localization to the *INI* file is a manual procedure.

NOTE: It is strongly recommended to make a backup of the *INI* file before making any changes.

To add a supported language:

1. Obtain the decimal Microsoft Locale ID (LCID) for the language, available [here](#).
2. Open the *INI* file
(**C:\Program Files\SafeNet\SAS\SafeNetMFA\ini\SAFENET_MFA.INI**) in a text editor.

In the AvailableLcids row, the supported languages are specified by their decimal LCID, separated by comma.

The *INI* includes the following by default.

AvailableLcids=1033,3084

where:

- 1033 is the decimal LCID English-United States, the equivalent of [SAFNET-DEFAULT] – DO NOT CHANGE.
- 3084 is the decimal LCID value for French-Canada.

In the **MFA Metadata** section of the */NI* file, the [SAFENET-DEFAULT] section lists the messages in English-United States.

[SAFENET-DEFAULT]

1001=Gemalto authentication successful
1002=Authentication failed. Please enter a correct passcode.
1003=Please enter the response to the server challenge:
1004=Please re-authenticate, using the next response. Your new PIN is:
1005=Please enter a new PIN.
1006=Please generate a new OTP, and use it to authenticate again.
1007=Your password has expired. Please enter a new password.
1008=Password change failed. Please enter a new password.
1009=PIN change failed. Please enter a new PIN.
1010=User Name cannot be empty.
1011=Not implemented. Please close the web browser.
1012=Please enter your PIN together with the characters corresponding to your chosen pattern.
1013=Please enter the response to the server challenge that was sent to your mobile device.
; Page Title
1014=Gemalto ADFS Multi-Factor Strong Authentication
1015=User Name:
1016=Passcode:
1017=New Password:
1018=Confirm New Password:
1019=New PIN:
1020=Confirm New PIN:
1021=Submit
1022=Copyright © 2023. Gemalto. All Rights Reserved.
1023=To log in, please enter a valid response to the server challenge.
1024=Use my mobile to autosend a passcode
1025=Enter a passcode manually
1026=I want to :

2000=Invalid incoming authentication context.
2001=Invalid incoming identity claim.
2002=The user authenticated by ADFS does not match the Gemalto session user.

2003=Could not get the authentication template file. Please see logs for error information.

2004=Failed to pre-generate a challenge for user [{0}].

2005=Invalid posted user. User name do not match with user in Gemalto session.

2006=New PIN / Password values are empty or do not match.

2007=Could not get the PIN / Password change template file. Please see logs for error information.

2021=Your request timed out. Please try again.

2022=Error when creating autosend message, Please contact administrator.

2023=Authentication process was canceled.

2024=Passcode was not autosent. Please try again or enter passcode.

2025=Auto push has failed, Authentication ID not found, Please contact administrator.

2026=Auto push has failed, Authentication ID conflicted, Please contact administrator.

2027=Auto push has failed, unknown error.

2028=Authentication failed.

2029=Authentication request was cancelled. Please try again

The [3084] section lists the same messages as in the [SAFENET-DEFAULT] section, but translated to French-Canada.

[3084]

1001 = Authentification réussie

1002 = L'authentification a échoué. Veuillez réessayer.

1003 = Veuillez répondre au défi du serveur :

1004 = Veuillez vous authentifier à nouveau en utilisant la réponse suivante. Votre nouveau code PIN est :

1005 = Veuillez saisir un nouveau code PIN.

1006 = Veuillez vous authentifier avec un nouvel OTP.

1007 = Votre mot de passe a expiré. Veuillez saisir un nouveau mot de passe.

1008 = Le changement de mot de passe a échoué. Veuillez saisir un nouveau mot de passe.

1009 = Le changement de PIN a échoué. Veuillez saisir un nouveau code PIN.

1010 = Le nom d'utilisateur ne peut pas être vide.

1011 = Non implémenté. Veuillez fermer le navigateur web.

1012 = Veuillez saisir votre code PIN en utilisant les caractères correspondant au modèle choisi.

1013 = Veuillez saisir la réponse au challenge du serveur qui a été envoyé à votre mobile.

; Titre de la page

1014 = Gemalto ADFS Authentification forte multi-facteurs

1015 = Nom d'utilisateur:

1016 = Passcode:
1017 = Nouveau mot de passe:
1018 = Confirmer le nouveau mot de passe:
1019 = Nouveau code PIN:
1020 = Confirmer le nouveau code PIN:
1021 = Envoyer
1022 = Copyright © 2023. Gemalto. Tous droits réservés.
1023 = Pour vous connecter, veuillez répondre au challenge du serveur.
1024=Utiliser mon appareil mobile pour l'envoi automatique d'un Passcode
1025=Saisir un passcode manuellement
2000 = contexte d'authentification invalide.
2001 = invalide revendication d'identité entrant.
2002 = L'utilisateur authentifié par ADFS ne correspond pas à l'utilisateur de la session Gemalto.
2003 = Impossible de trouver le fichier de modèle d'authentification . Veuillez regarder les logs pour obtenir plus d'information.
2004 = Impossible de générer un challenge pour l'utilisateur [{ 0 }] .
2005 = Utilisateur invalide : le nom d'utilisateur ne correspond pas à l'utilisateur de session Gemalto.
2006 = Le nouveau code PIN et le mot de passe sont vides ou ne correspondent pas.
2007 = Impossible d'obtenir le fichier modèle de PIN ou mot de passe. Veuillez regarder les logs pour obtenir plus d'information.
2021 = Le délai de votre demande a expiré. Veuillez réessayer.
2022 = Erreur survenue lors de la création du message d'envoi automatique. Veuillez contacter votre administrateur.
2023 = Le Processus d'authentification a été annulé.
2024 = Le passcode n'a pas été envoyé automatiquement. Veuillez reessayer ou saisir un passcode.
2025 = L'envoi de la notification a échoué. L'identifiant d'authentification est introuvable. Veuillez contacter votre administrateur.
2026 = L'envoi de la notification a échoué. Conflits d'identifiant d'authentification. Veuillez contacter votre administrateur.
2027 = L'envoi de la notification a échoué, erreur inconnue.
2028 = Authentification réussie.
2029 = L'authentification a été annulée. Veuillez réessayer.

- To add an additional language, add the decimal LCID to the AvailableLcids row, inserting a comma as a delimiter.

In the following example, we add German-Germany (1031)

```
AvailableLcids=1033,3084,1031
```

4. Add the description for the added LCID, inserting a comma as a delimiter.

```
Descriptions=SafeNet Multi Factor Authentication Adaptor (SMFAA) for Microsoft ADFS 2012 R2, SafeNet multi Factor Authentication Adaptor (SMFAA) pour Microsoft ADFS 2012 R2, <add description for LCID 1031>
```

5. Add the FriendlyNames for the added LCID, inserting a comma as a delimiter.

```
FriendlyNames=SafeNet-MFAA, SafeNet-MFAA, <add FriendlyName for LCID 1031>
```

6. In the **MFA Metadata** section, add a new subsection titled [decimal LCID] and translate the **MFA Metadata Entries** section of the additional support language strings, following the same pattern as used for the English-United States and French-Canadian language.

This example shows [1031], the decimal LCID for German-Germany.

```
[1031]
```

```
  [<String-ID>] = <String>
```

```
  [<String-ID>] = <String>
```

```
  [<String-ID>] = <String>
```

7. Repeat from step 3 (above) for each additional language.

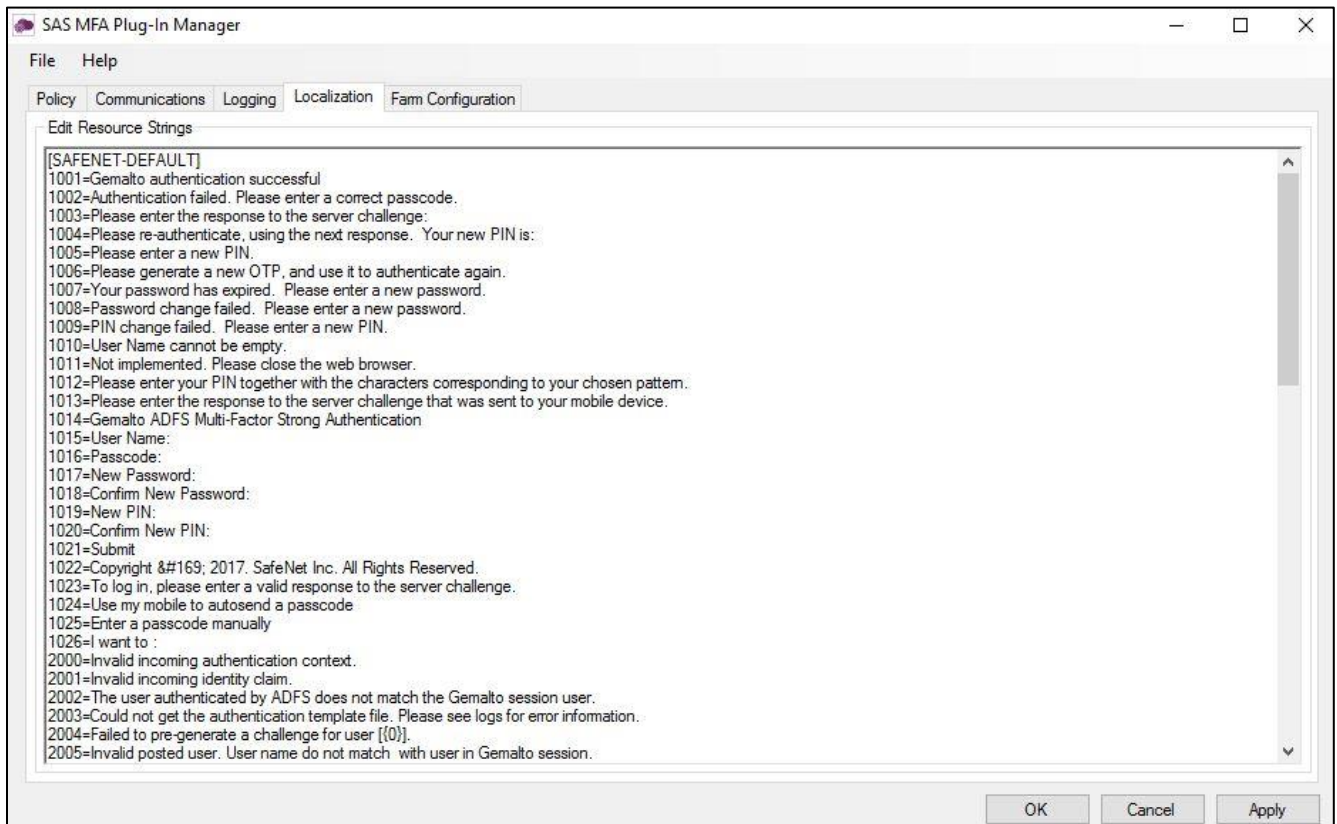
Viewing Localization Settings

NOTE: The localized text cannot be edited on the **Localization** tab interface. It must be edited in the *INI* file as described above.

See **Setting Additional Localization** on page 32.

To view the localization settings in the SafeNet AD FS Agent Manager:

1. To open the **SAS MFA Plug-In Manager**, click **Start > All Programs > SafeNet > Agents > SAS MFA Plug-In Manager**.
2. On **SAS MFA Plug-In Manager** window, click **Localization** tab to view the localization settings.



Global Authentication Policy

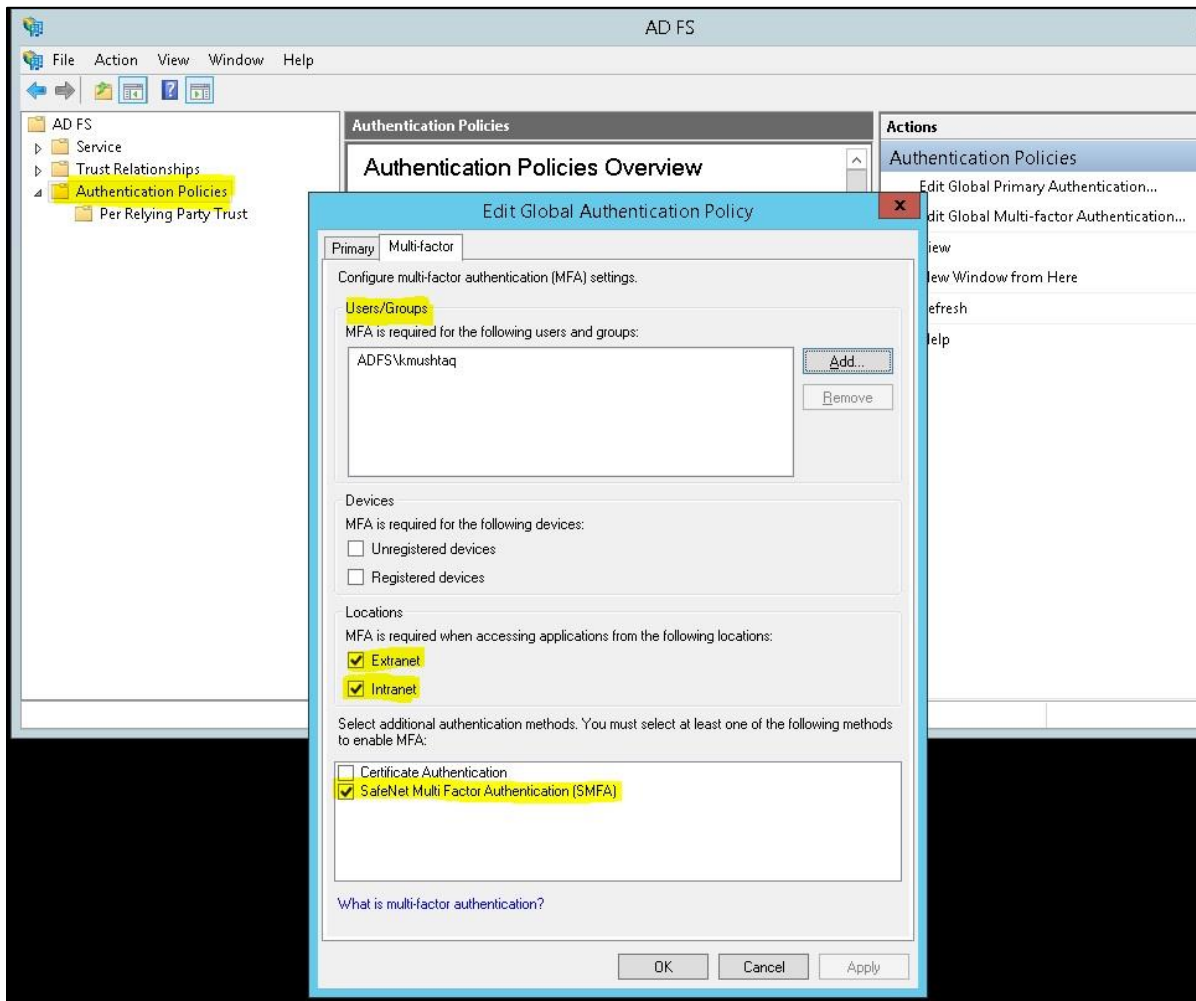
Enforcing Multi-Factor Policies in AD FS 3.0 (on Windows Server 2012 R2) and AD FS 4.0 (on Windows Server 2016)

Enabling the agent on the SafeNet AD FS **Agent Policy** tab (see [Configuring SafeNet Agent for AD FS](#) on page 25) registers the SafeNet AD FS Agent with AD FS and enables it at the global policy level.

After registration, you can enforce MFA policies at the required level in the **AD FS** window.

To enforce MFA policies:

1. Under AD FS, select **Authentication Policies**.
2. Select **Edit Global Authentication Policies**.
3. If required, in **Edit Global Authentication Policy** window, complete the following steps:



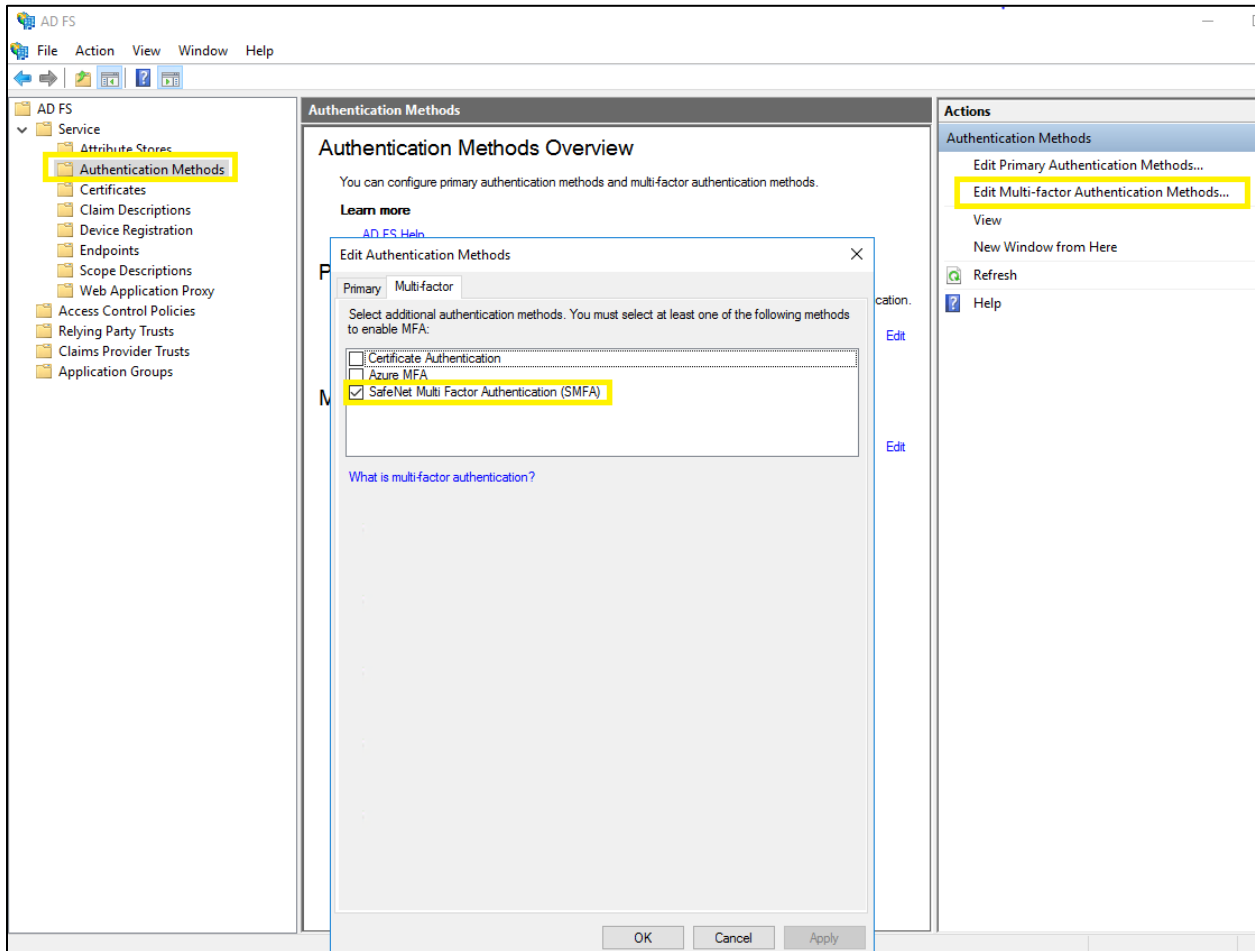
- a. Add the required users and groups (optional).
- b. Select **Extranet** or **Intranet** to specify if MFA is required when accessing applications at these locations.
- c. Select **SafeNet Multi Factor Authentication (SMFA)** method.
- d. Click **OK**.

Checking Multi-Factor Policies in ADFS 2019 (on Windows Server 2019 and Windows Server 2022)

Enabling the agent on the SafeNet AD FS **Agent Policy** tab (see [Configuring SafeNet Agent for AD FS](#) on page 25) registers the SafeNet AD FS Agent with AD FS and enables it at the global policy level.

To ensure that the MFA policies are enforced at the required level in the **AD FS** window, perform the steps:

1. Under AD FS > Service, select **Authentication Methods**.
2. Click **Edit Multi-factor Authentication Methods...** option from the right pane.
3. In **Edit Authentication Methods** window, ensure that the default option, **SafeNet Multi Factor Authentication (SMFA)** is selected.



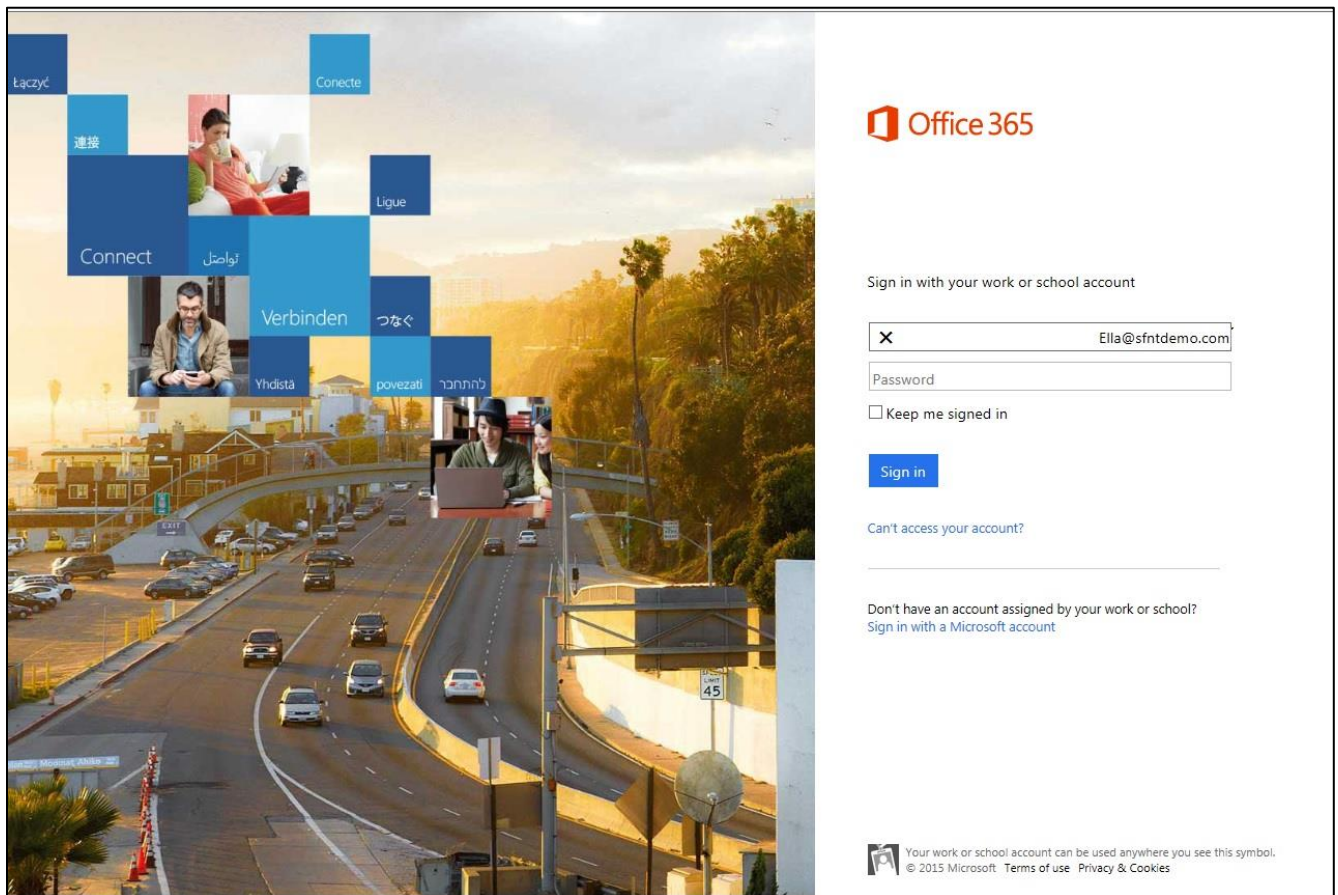
NOTE: If the agent is reinstalled or upgraded for Windows Server 2019 or Windows Server 2022 and if the AD FS admin enables the **Allow additional Authentication Provider as Primary** settings and from the list, chooses **SafeNet Multi Factor Authentication (SMFA)** as primary authentication, then under the **Additional Authentication** tab, the **SMFA** checkbox has to be cleared. This ensures that the primary authentication type doesn't conflict with the additional authentication type.

CHAPTER 4: Working with Office 365

Ensure that you have registered for the Microsoft Office 365 service and promoted your domain to a federated domain.

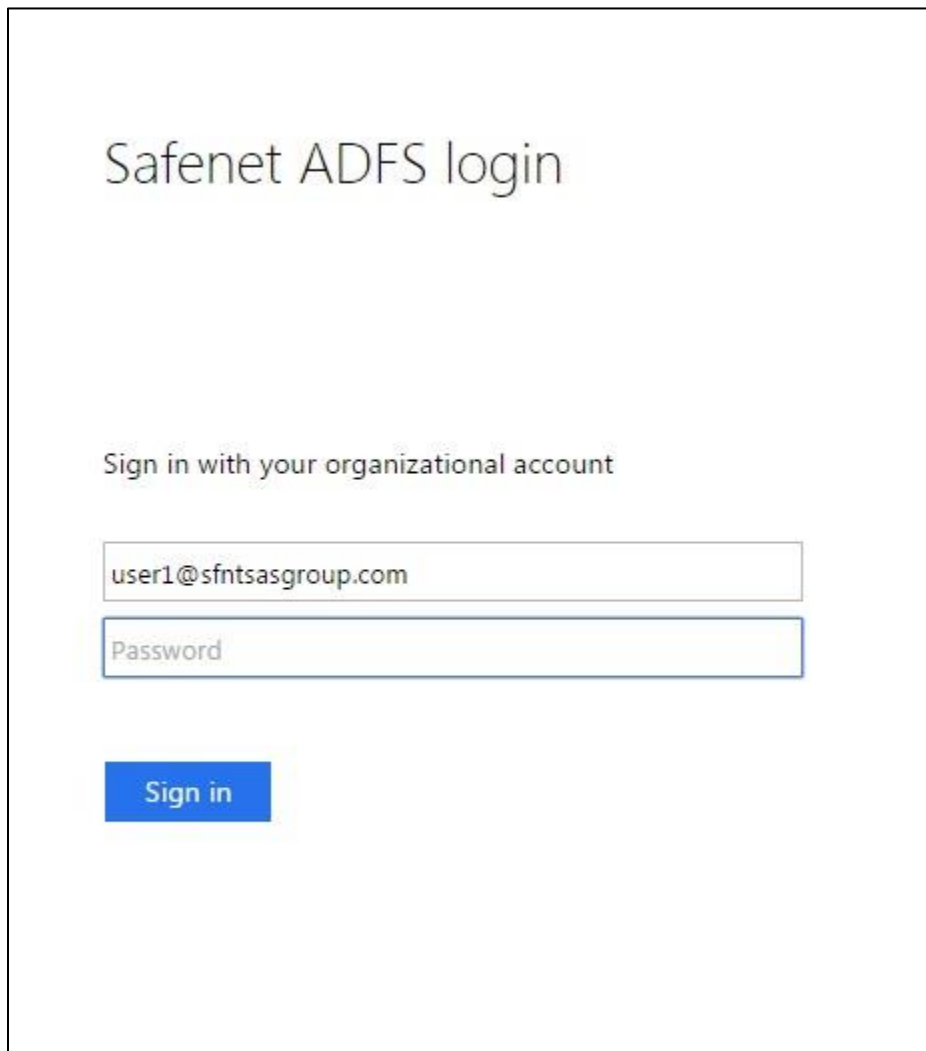
Logging to Office 365

1. Launch **AD FS Manager**.
2. Enable the agent and then enable **Forms Authentication** as the **Primary Authentication** method.
3. Force MFA at the **Extranet** or **Internet** level.
4. Force MFA at the Global or Individual SP level.
5. Open a browser and log in to [Microsoft Online](#).




Sign-In Window Examples

Primary Authentication (Windows Credentials)



The image shows a screenshot of a web-based login interface for Safenet ADFS. The title is "Safenet ADFS login". Below the title, there is a prompt: "Sign in with your organizational account". There are two input fields: the first contains the email address "user1@sfntasgroup.com" and the second is labeled "Password". Below the input fields is a blue button with the text "Sign in".

Secondary Authentication (SafeNet Grid Token)

Please enter your PIN together with the characters corresponding to your chosen pattern.

1	6	5	2	6
4	9	8	0	3
2	4	0	1	4
1	5	7	8	7
6	3	3	9	2

Passcode: