THALES

gemalto
a Thales company

SafeNet Agent for AD FS

INSTALLATION AND CONFIGURATION GUIDE

Document Information

Product Version	2.41
Document Part Number	007-012546-004
Release Date	January 2020

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries 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 Gemalto's 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, Gemalto 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, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto 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 Gemalto 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.

Gemalto 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 Gemalto be held liable for any third party actions and in particular in case of any

successful attack against systems or equipment incorporating Gemalto products. Gemalto 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

This document is intended for personnel responsible for maintaining your organization's security infrastructure. All products manufactured and distributed by Gemalto 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.

Customer 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 Gemalto 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 provides information on the conventions used in this document.

Notifications

This document uses notes, cautions, and warnings to alert you to important information that may help you to complete your task, or prevent personal injury, damage to the equipment, or data loss.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

> **NOTE:** Take note. Notes contain important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

> **CAUTION!** Exercise caution. Caution alerts contain 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. These elements use the following format:

> ****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.**

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: > 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.) > Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) > User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.

Related Documents

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

> SafeNet Agent for AD FS 2.41: Customer Release Notes

Support Contacts

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

Gemalto 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 Gemalto 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.gemalto.com, is a 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 on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

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

CHAPTER 1: Introduction

Applicability

The information in this document applies to:

- SafeNet Authentication Service PCE 3.7 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

Environment

Supported Platforms	> 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 only compatible with **AD FS 4.0** on Windows Server 2016.*
Supported Architecture	64-bit
Additional Software Components	> Microsoft .NET Framework 4.5 or above > Microsoft PowerShell v3.0
Supported Authentication Methods	All tokens and authentication methods supported by SafeNet

Supported Web Browsers	> Internet Explorer 11 > Microsoft Edge (not supported on mobile devices) > Mozilla Firefox > 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 4.5
- 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.]

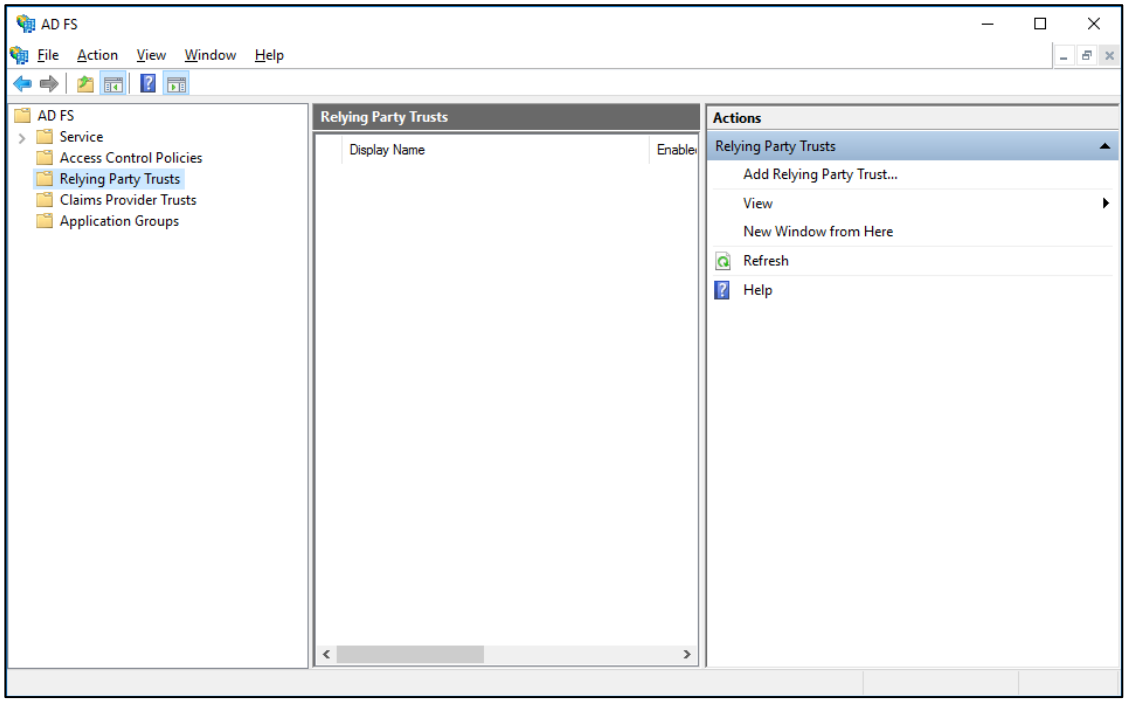
Adding Relying Party Trust – Windows Server 2016

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

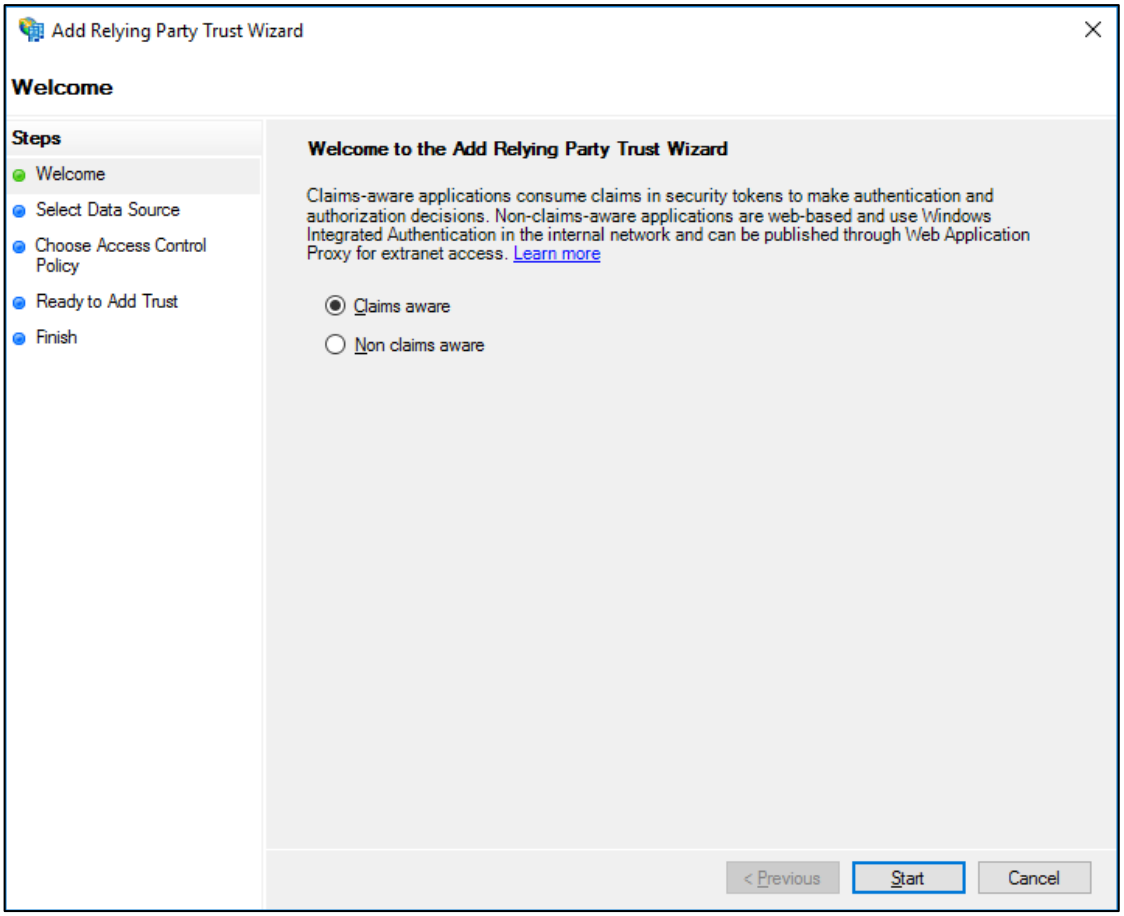
For **AD FS 4.0** (on **Windows Server 2016**), the Relying Party Trust needs to be added manually. Unless the relying party trust is configured, the Gemalto MFA page will not appear. After a user successfully logs in, using the AD, perform the following steps to view the Gemalto OTP page (with two sign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

1. Open AD FS Management.

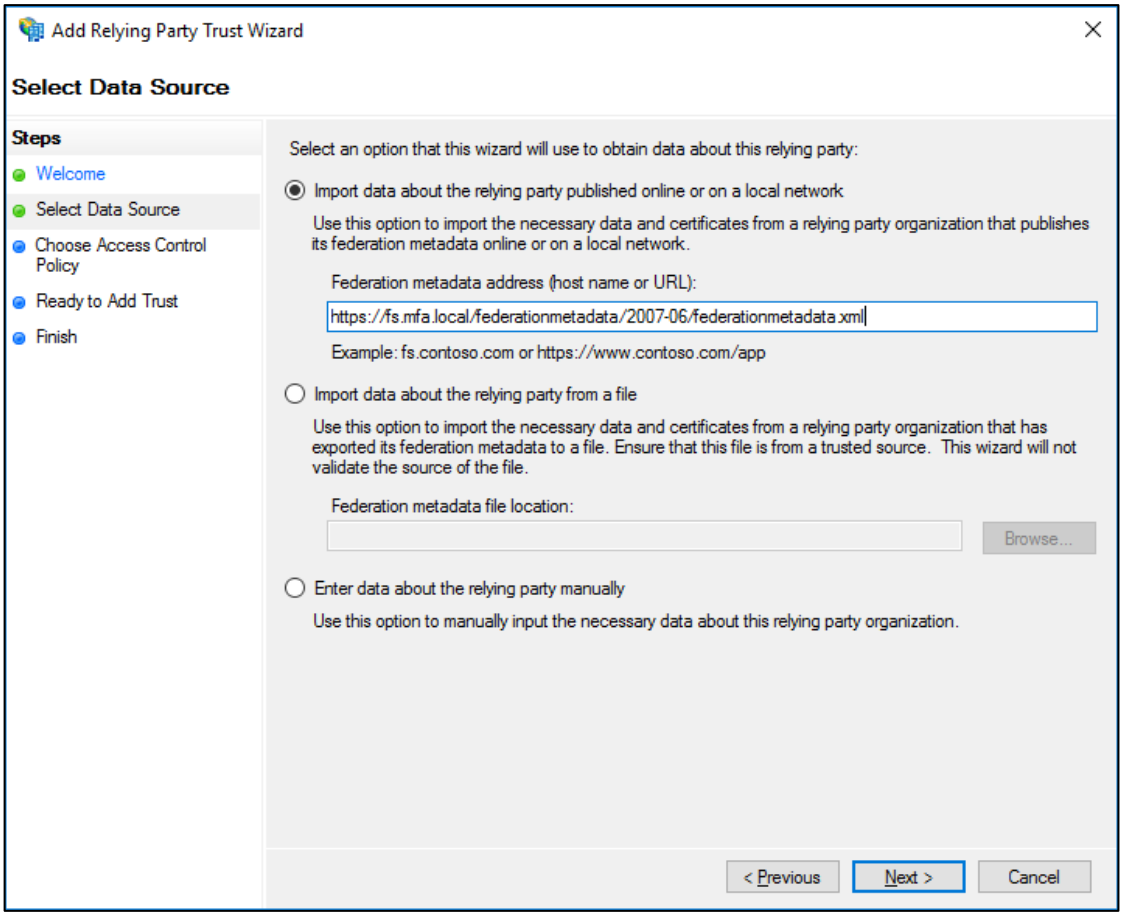
2. Highlight Relying Party Trusts, and click Add Relying Party Trust… from the Actions pane.



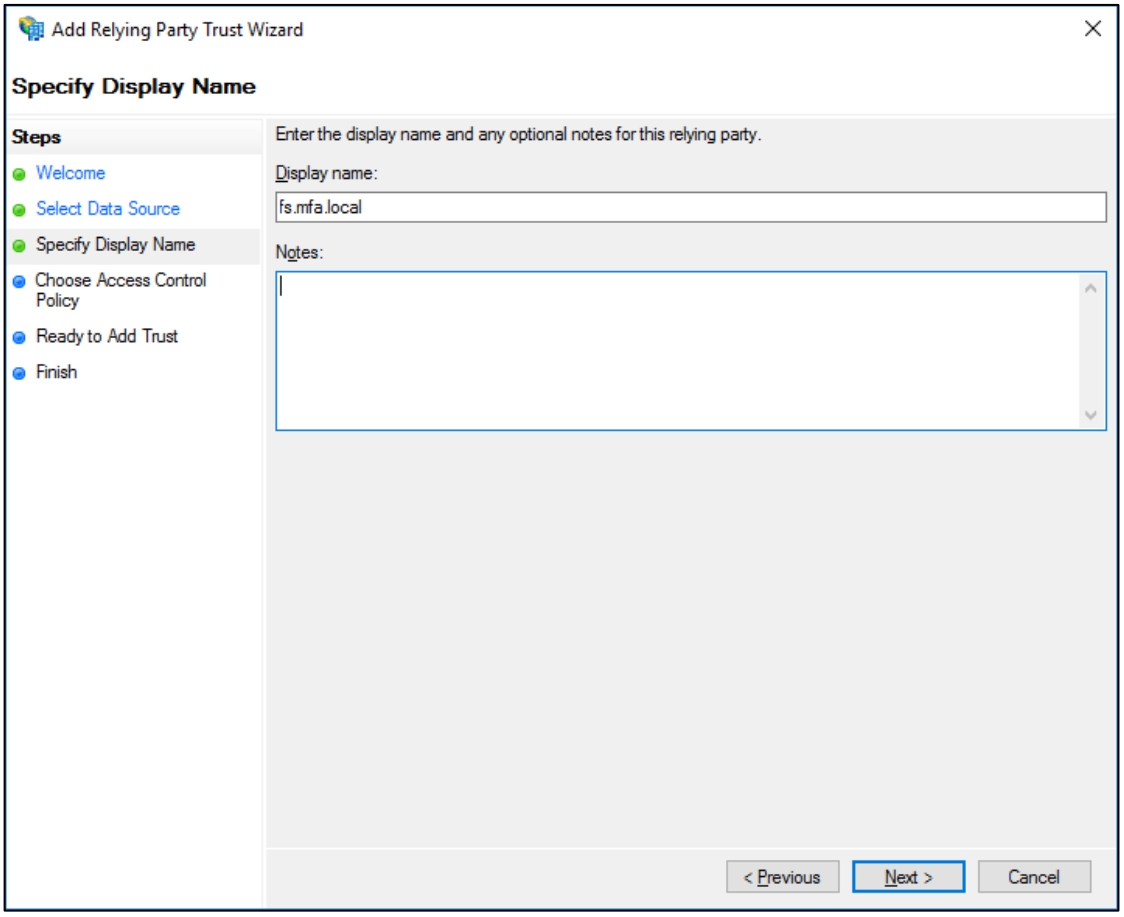
3. Select **Claims aware** radio option, and click **Start**.



4. Enter the URL of the metadata file.
`https://<fqdn>/federationmetadata/2007-06/federationmetadata.xml`

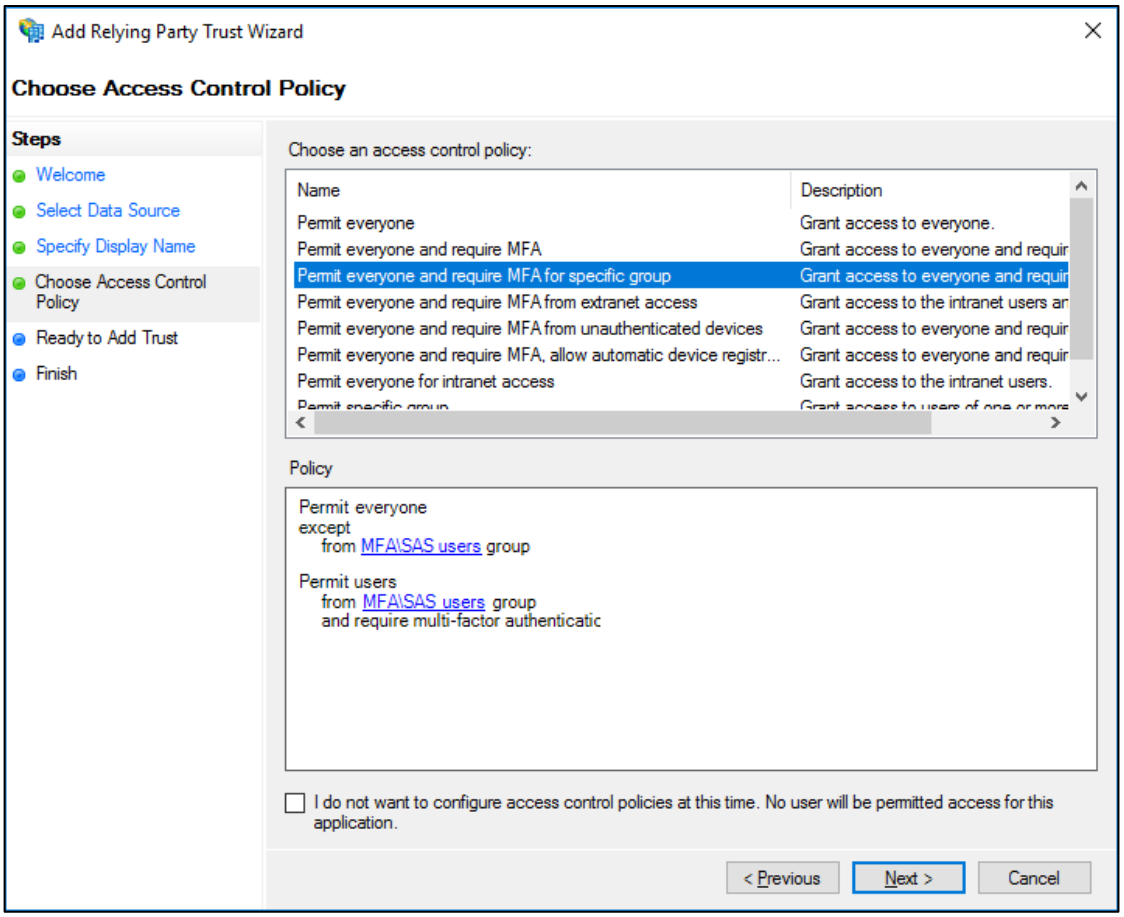


5. Enter a **Display name**, and click **Next**.



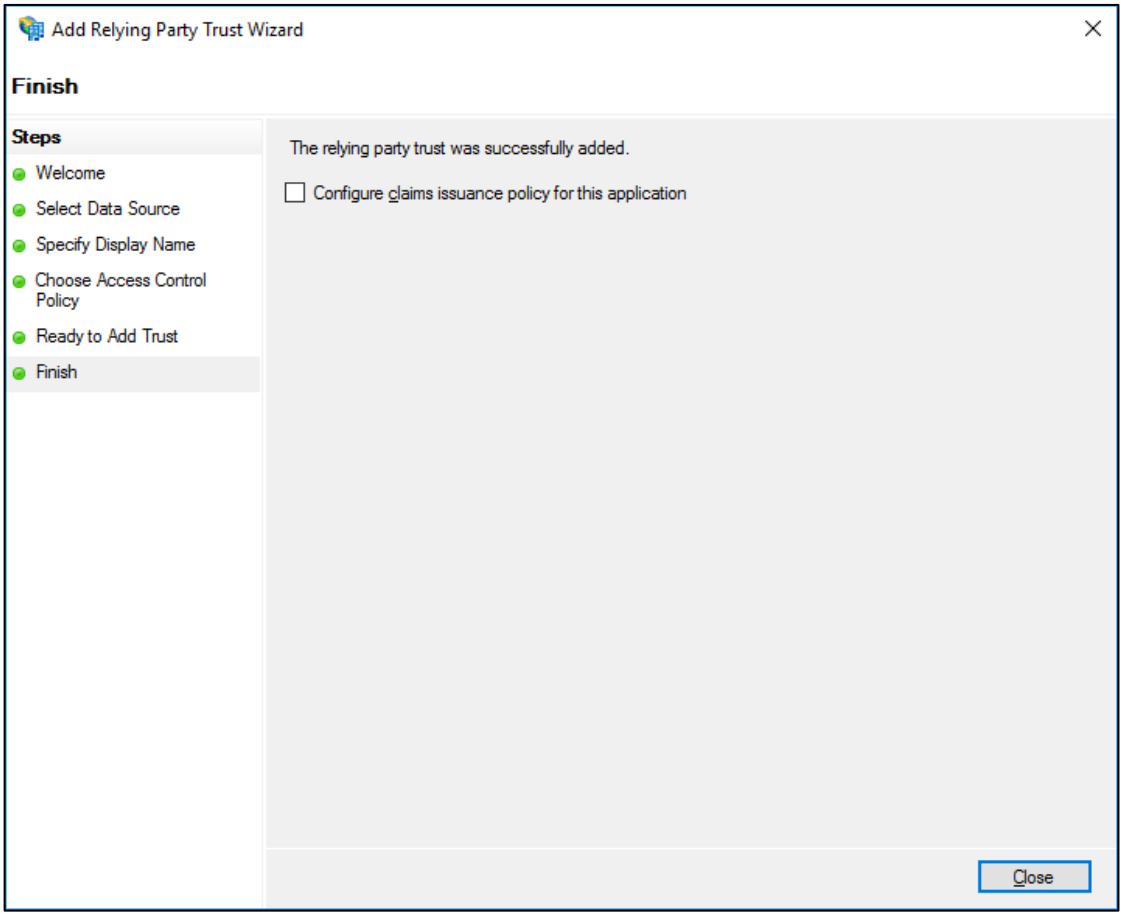
6. Select an Access Control Policy, and click **Next**.

   In our example, we have chosen the **Permit everyone and require MFA for specific group** option.



7. Click **Next**.

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



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

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:

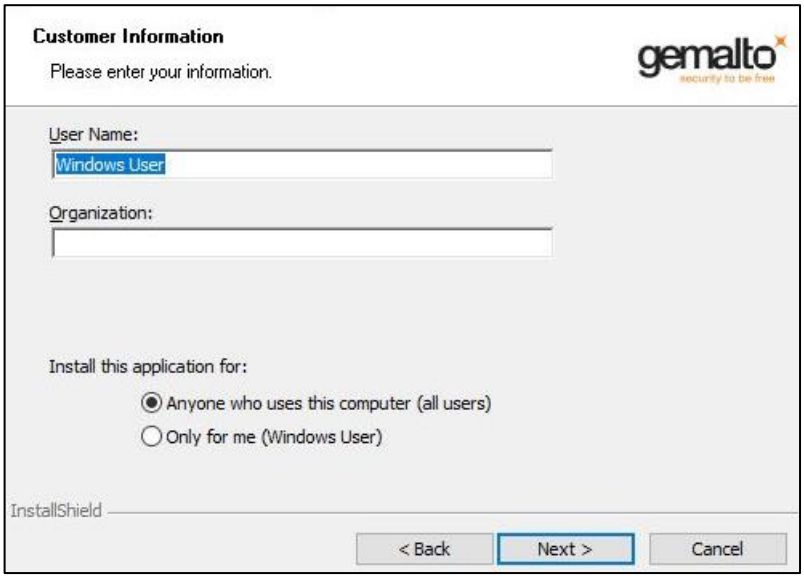
1. Run as administrator the SafeNet Agent for AD FS installer:

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

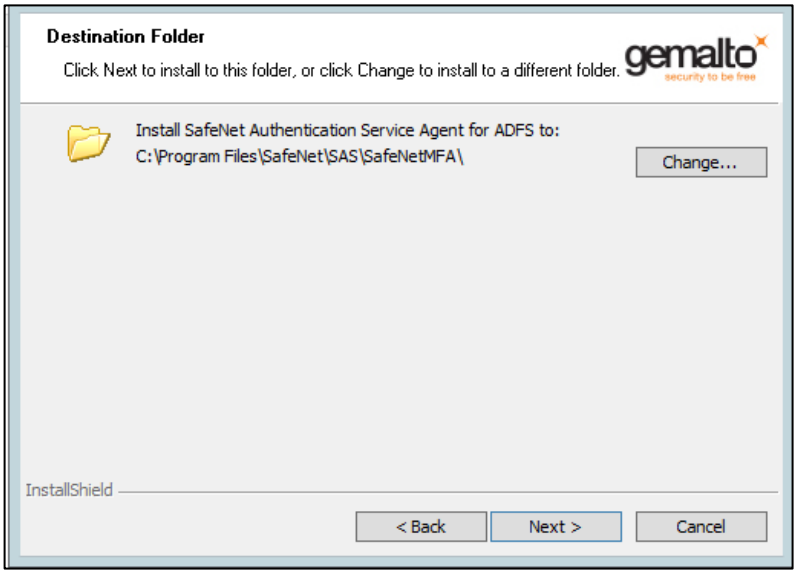
2. On the welcome **screen**, click **Next**.

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

4. On **Customer Information** window, enter **User Name** and **Organization**, and click **Next**.

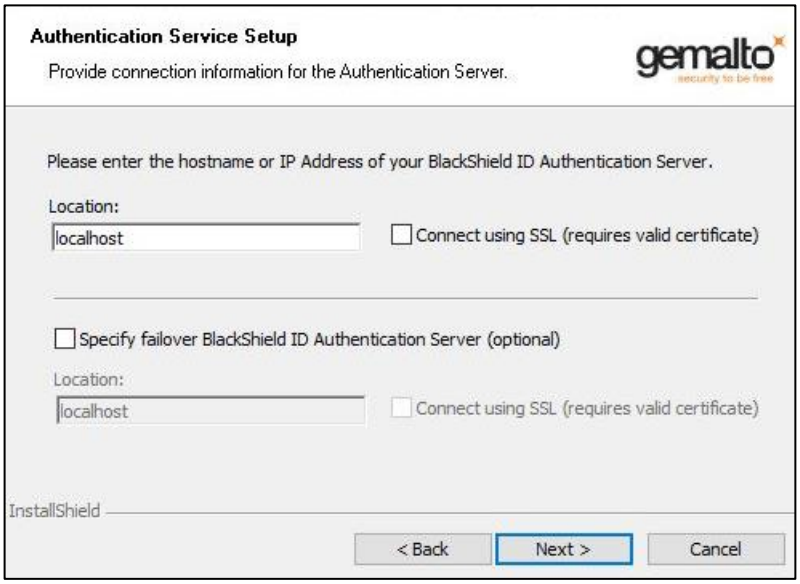


5. On **Destination Folder** window, do one of the following.

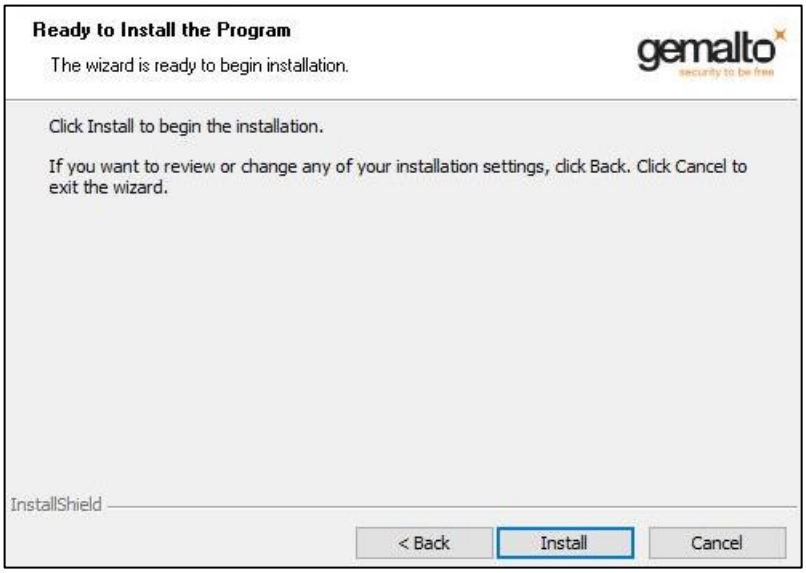


- To select the default installation destination folder, click **Next**.
- To select a different location, click **Change**, and browse to the appropriate location.

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 is completed, the **Installshield Wizard Completed** window is displayed. Click **Finish** to exit the installation wizard.

Upgrade and Migration

Any version later than **v2.0** (i.e., **v2.01**, **v2.02**, **v2.10**, **2.20**, **2.21**) can be upgraded to the SafeNet Agent for AD FS **v2.41**.

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 (**v2.41**).

Upgrading to SafeNet Agent for AD FS 2.41

To upgrade, execute the SafeNet Agent for AD FS v2.41 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 2.41

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 SafeNet Agent for AD FS v2.41.
5. Replace the *SAFENET-MFA.ini* file in the SafeNet Agent for AD FS v2.41 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 SafeNet Agent for AD FS v2.41 installation folder with the file saved from version 2.0 or earlier, and enabling the SafeNet Agent for AD FS in the SAS, 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 de-activating 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 de-activate 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** on page 26.

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. In **Edit Authentication Policy for Device Registration Service** window, select **Multi-factor** tab.
3. In **Users/Groups** box, remove all listed users and groups.

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

4. In the AD FS management console, click **Relying Party Trust**.
5. Select the required Relying Party Trust application and **Edit Access Control Policy**.
6. Select any policy (from the **Access control policy** list) which 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, we strongly recommend that you 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 **SafeNet MFA Plugin Manager**, select **Start > All Programs > SafeNet > Agents > SafeNet 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 SafeNet 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 SafeNet MFA Plugin Manager.

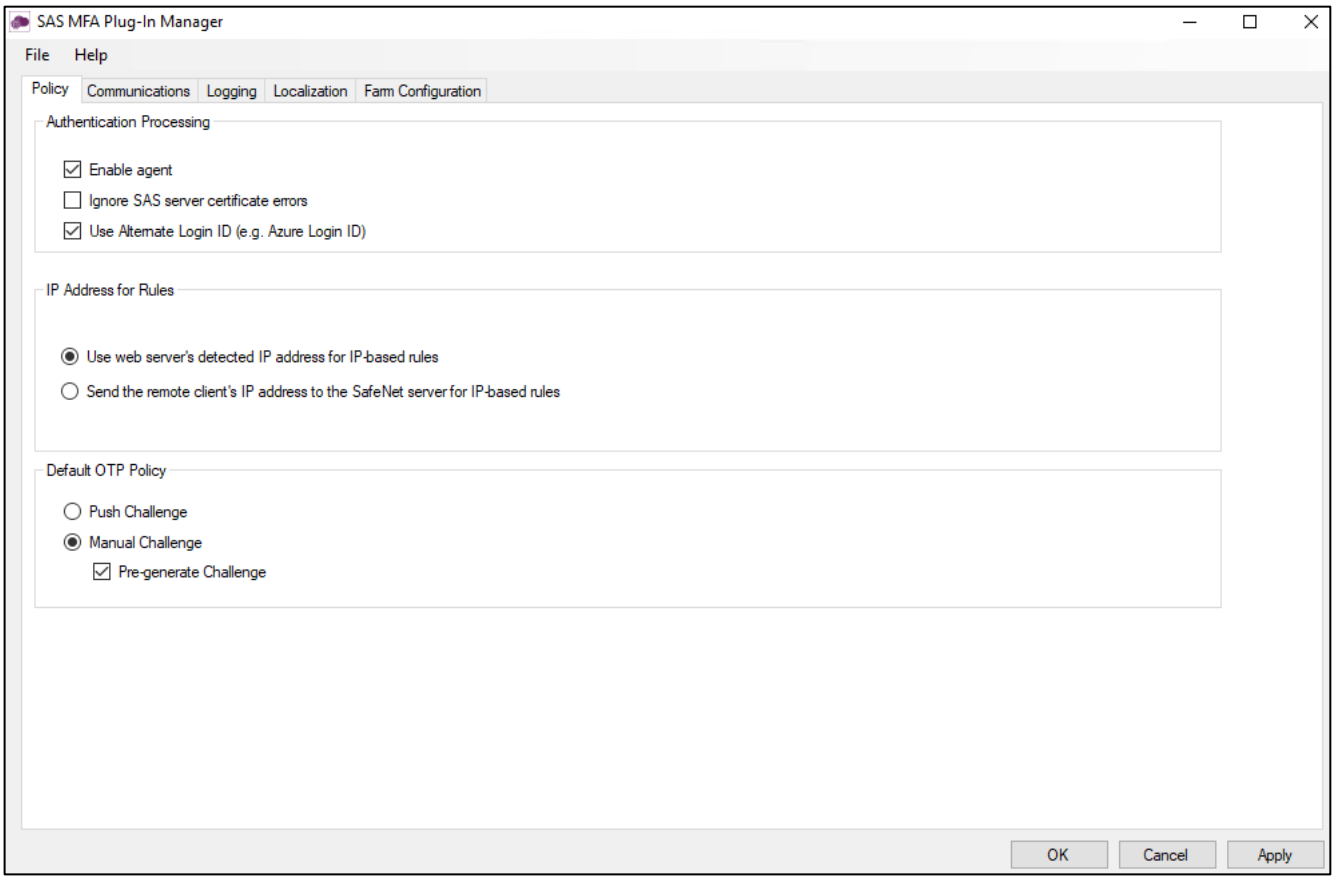
To open the SafeNet Agent for AD FS MFA Policy Manger:

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

Policy

To configure the SafeNet Agent for AD FS policy:

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



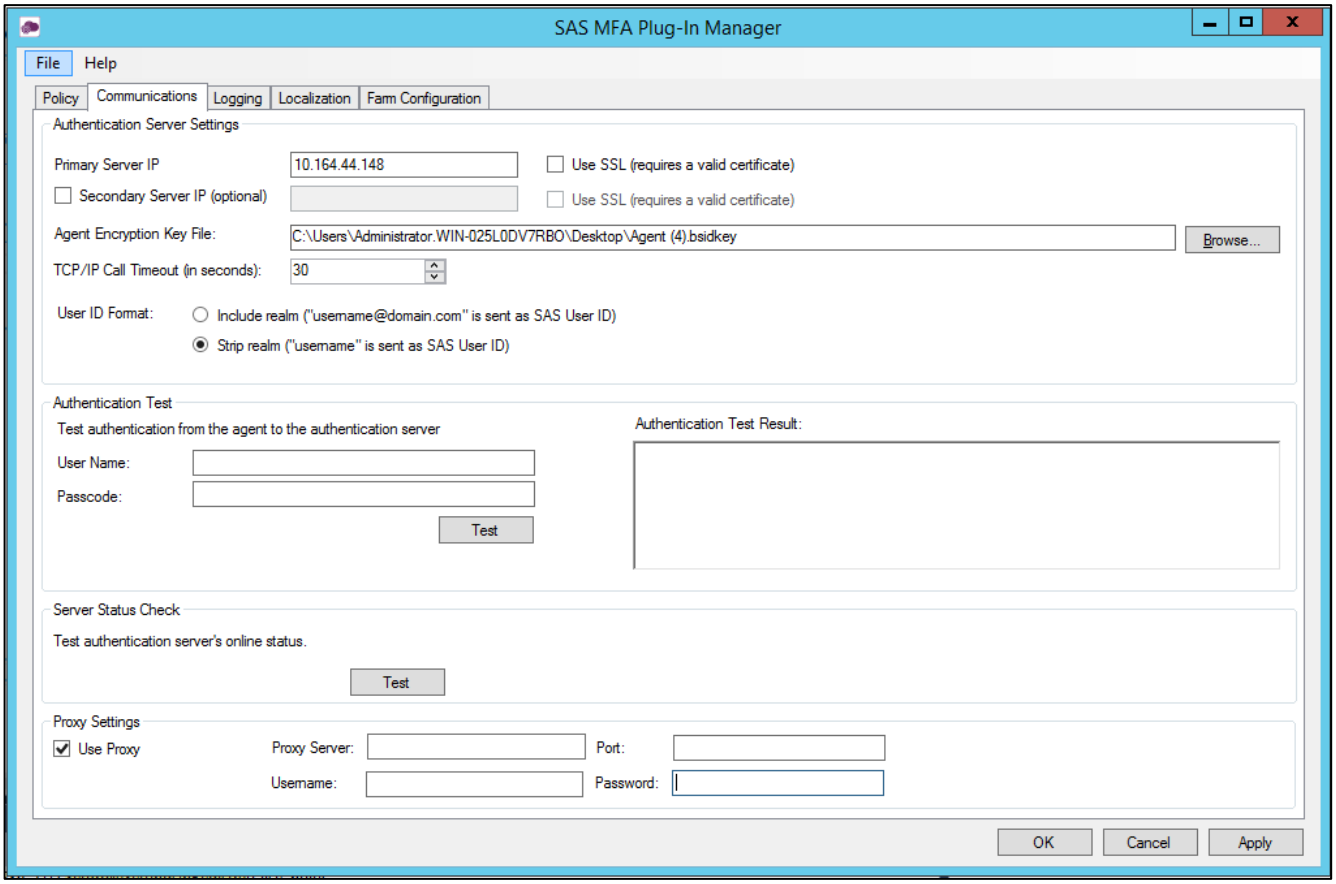
Complete the following fields, and click **Apply**.

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.
Ignore SAS Server certificate errors	Select to prevent checking of SAS certificate validity.

Field	Description
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**).
IP Address for Rules	Select one of the following: > **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: > **Push Challenge** – to use the Push OTP Feature **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. > **Manual Challenge** – For using any token • **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.



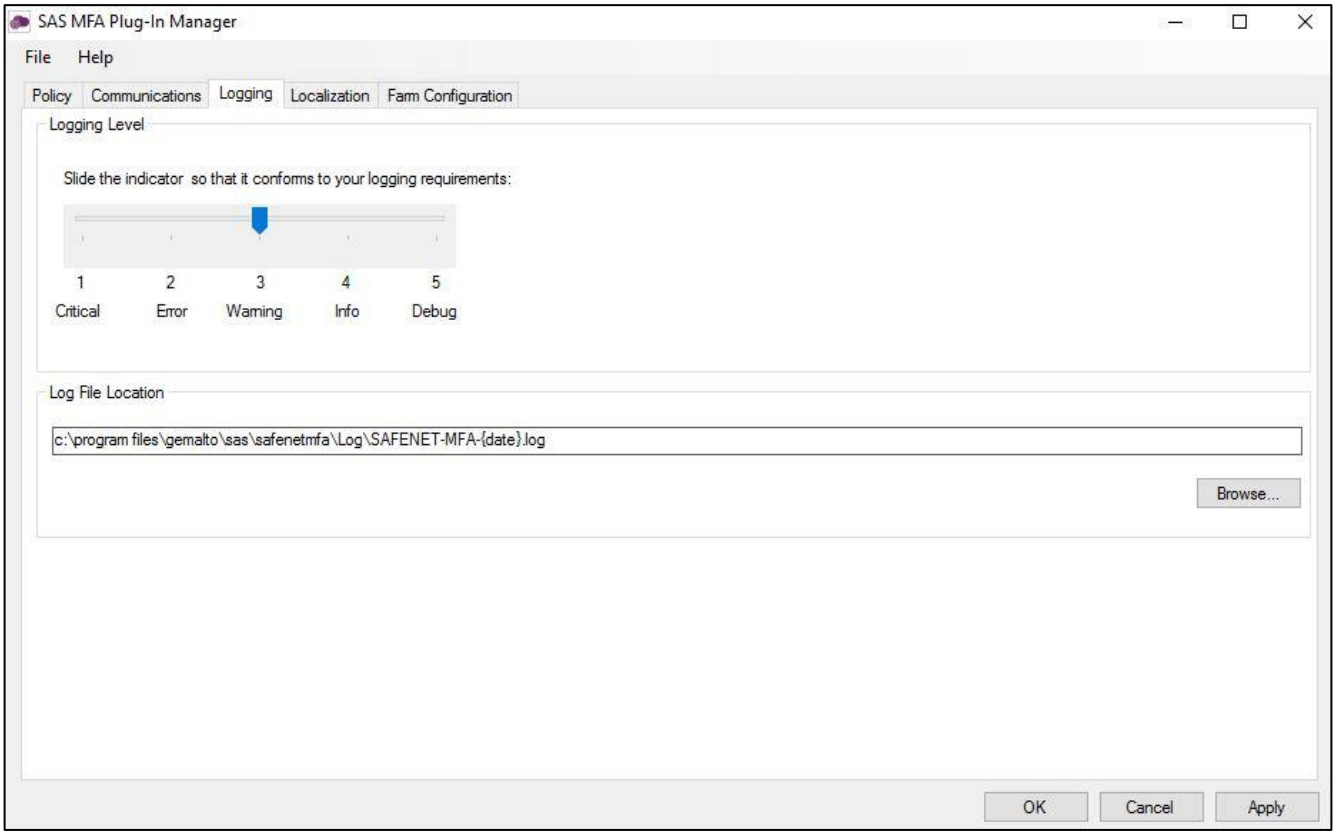
Complete the following fields, and click **Apply**:

Field	Description
Primary Server (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 (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.
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** on page 25.
TCP/IP Call Timeout (in seconds)	Sets the maximum timeout value in seconds for authentication requests sent to the SafeNet server.

Field	Description
User ID Format	Select the required ID format for the SAS/STA usernames: > **Include Realm ("Username@domain.com" is sent as SAS/STA User ID)** > **Strip realm ("Username" is sent as User ID)** **Note**: The realm stripping feature applies to SAS/STA usernames only. Active Directory usernames are not affected.
Authentication Test	This function allows administrators to test authentication between the SafeNet Agent for AD FS and the SafeNet server. Enter **User Name** and **Password** and click **Test**. The result of the test is displayed in the **Authentication Test Result** text box. **Notes**: • 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	Enter the following details: • **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

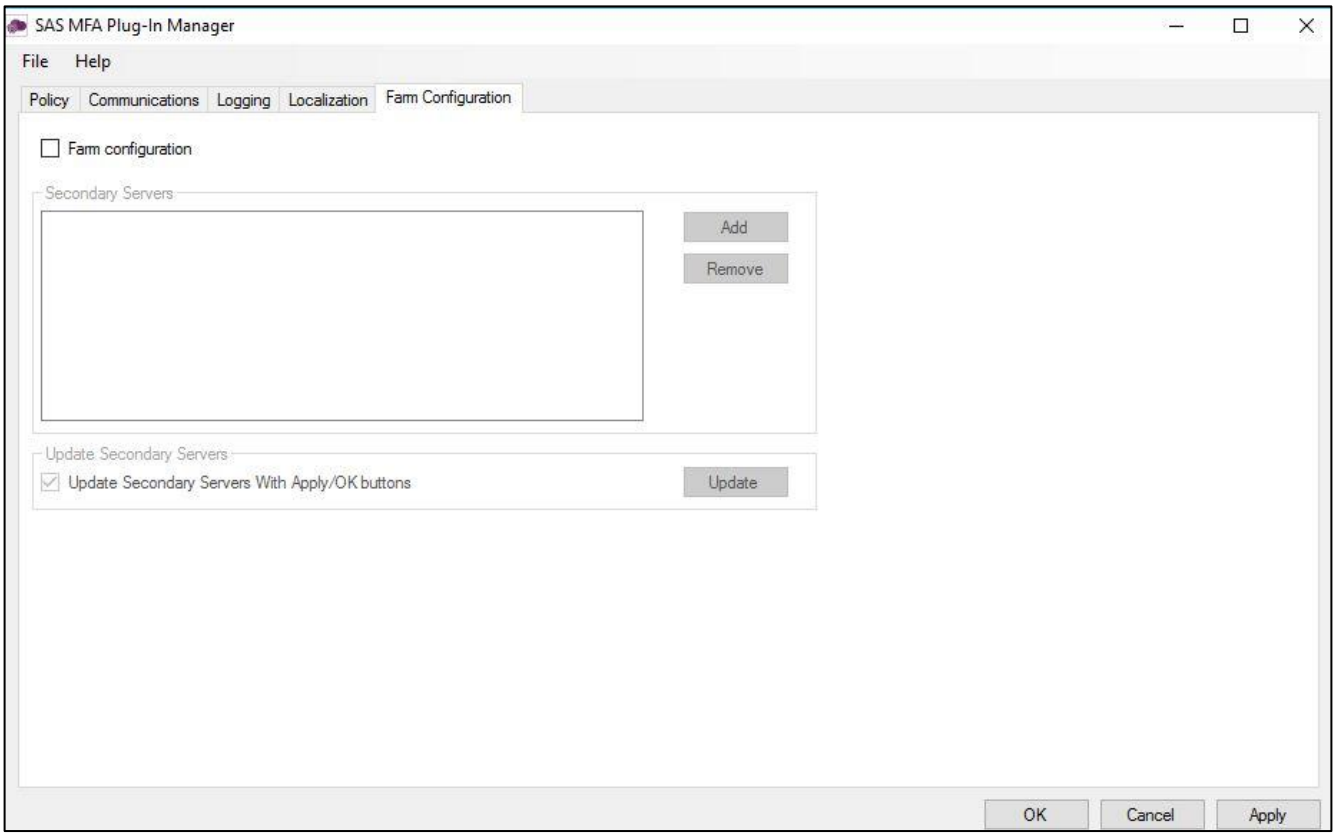
In an AD FS federation server farm using Windows Internal Database (WID), the first server in the farm acts as the primary server, hosting a read/write copy of the database. Secondary servers then replicate the configuration data into their read-only database. The secondary servers are fully functional 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.

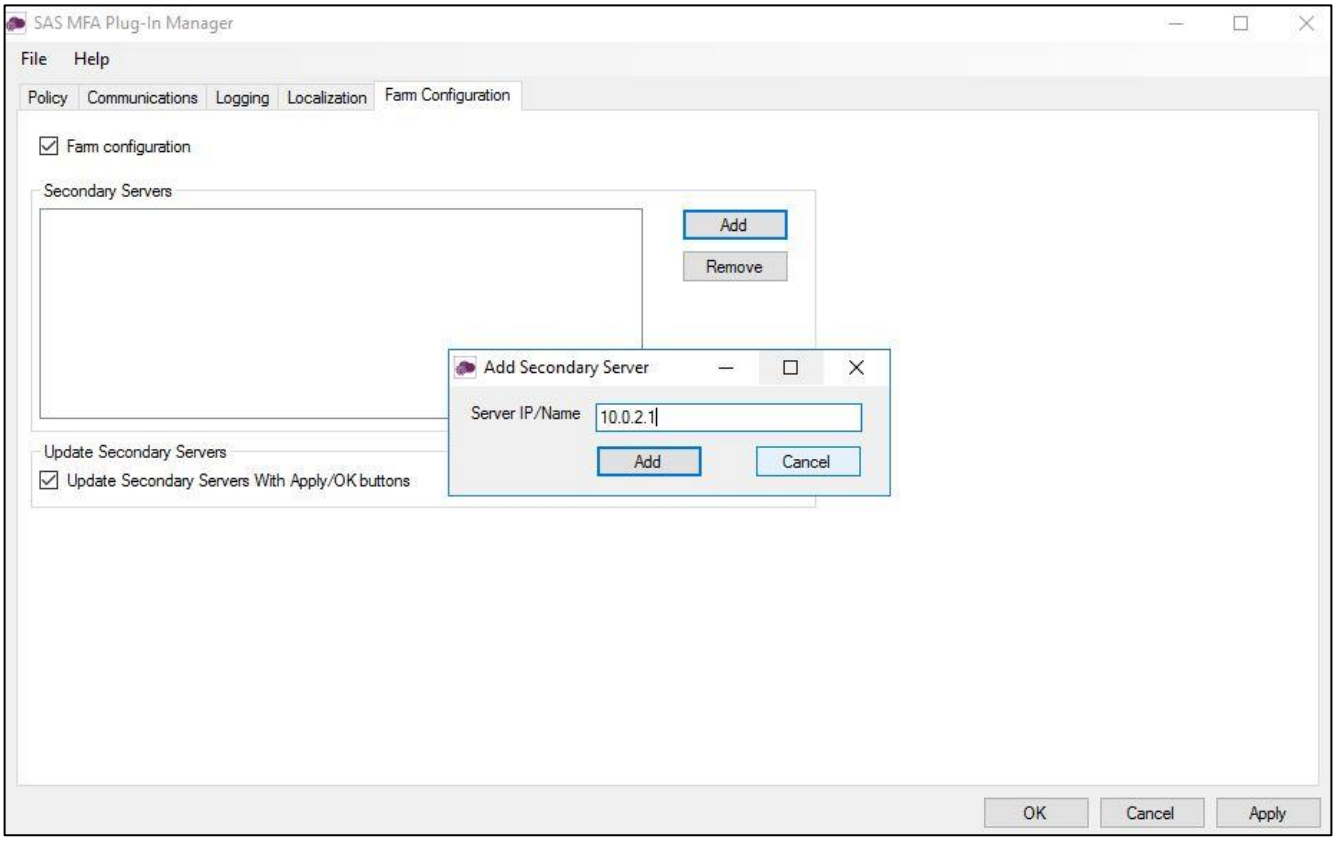
NOTE: To configure an AD FS Federation Server farm, you must be logged-in as a Domain Administrator.

To configure the server farm:

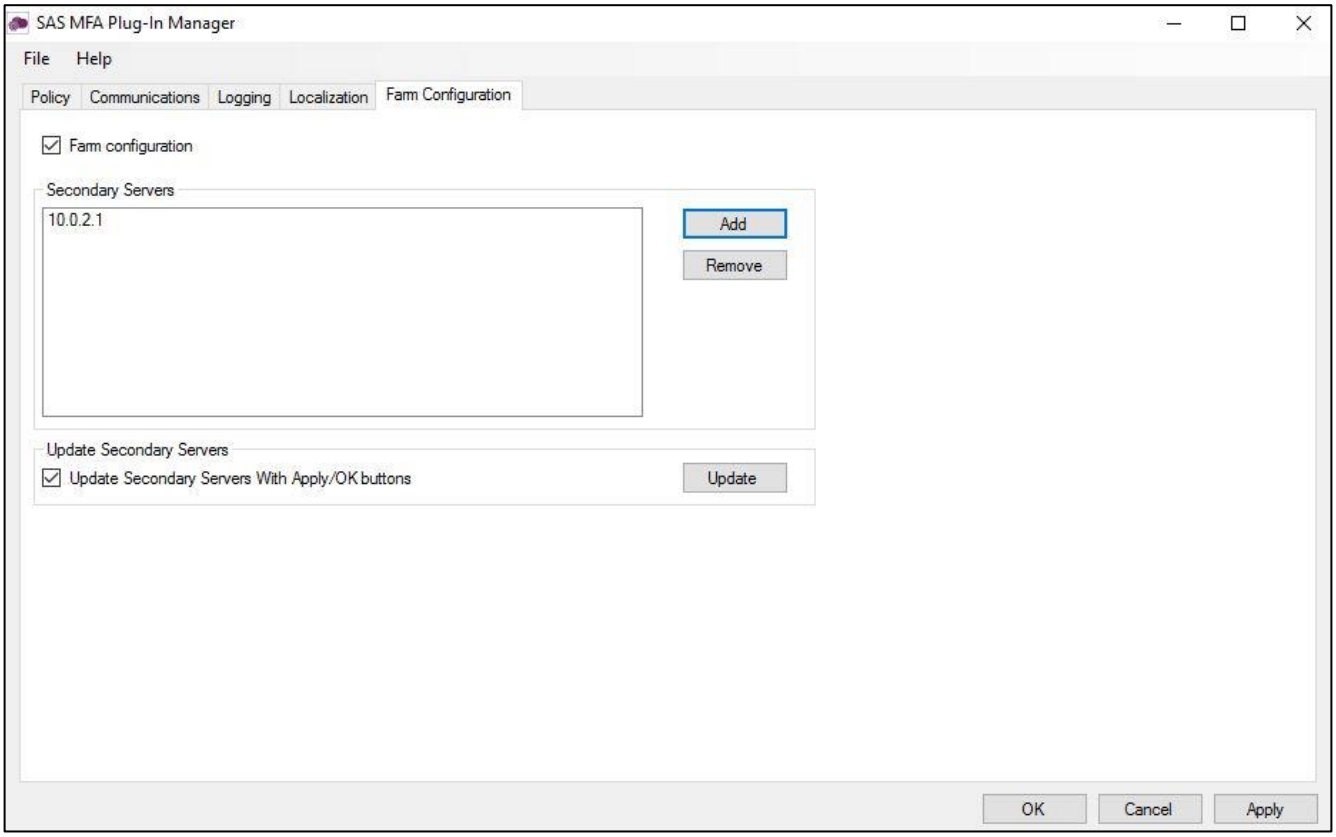
1. On **SAS MFA Plug-In Manager** window, click **Farm Configuration** tab.
2. Select **Farm configuration.**
3. Click **Add**.



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 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

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 *INI* 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 &#169; 2020. 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 mom 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 &#169; 2020. 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'indentifiant 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.

3. 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. 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>

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

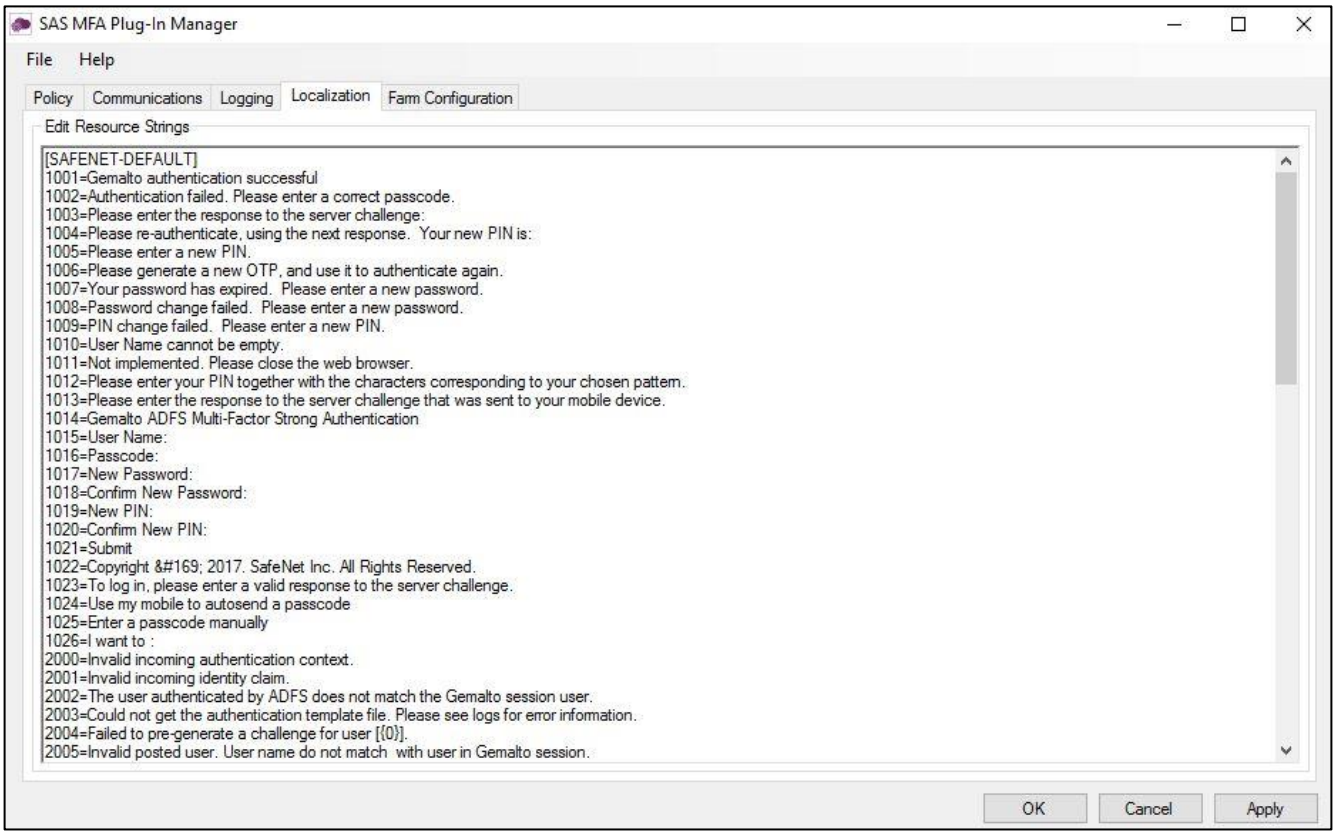
Viewing Localization Settings

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 34.

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 > SafeNet MFA Plugin Manager**.
2. On **SAS MFA Plug-In Manager** window, click **Localization** tab to view the localization settings.



Global Authentication Policy

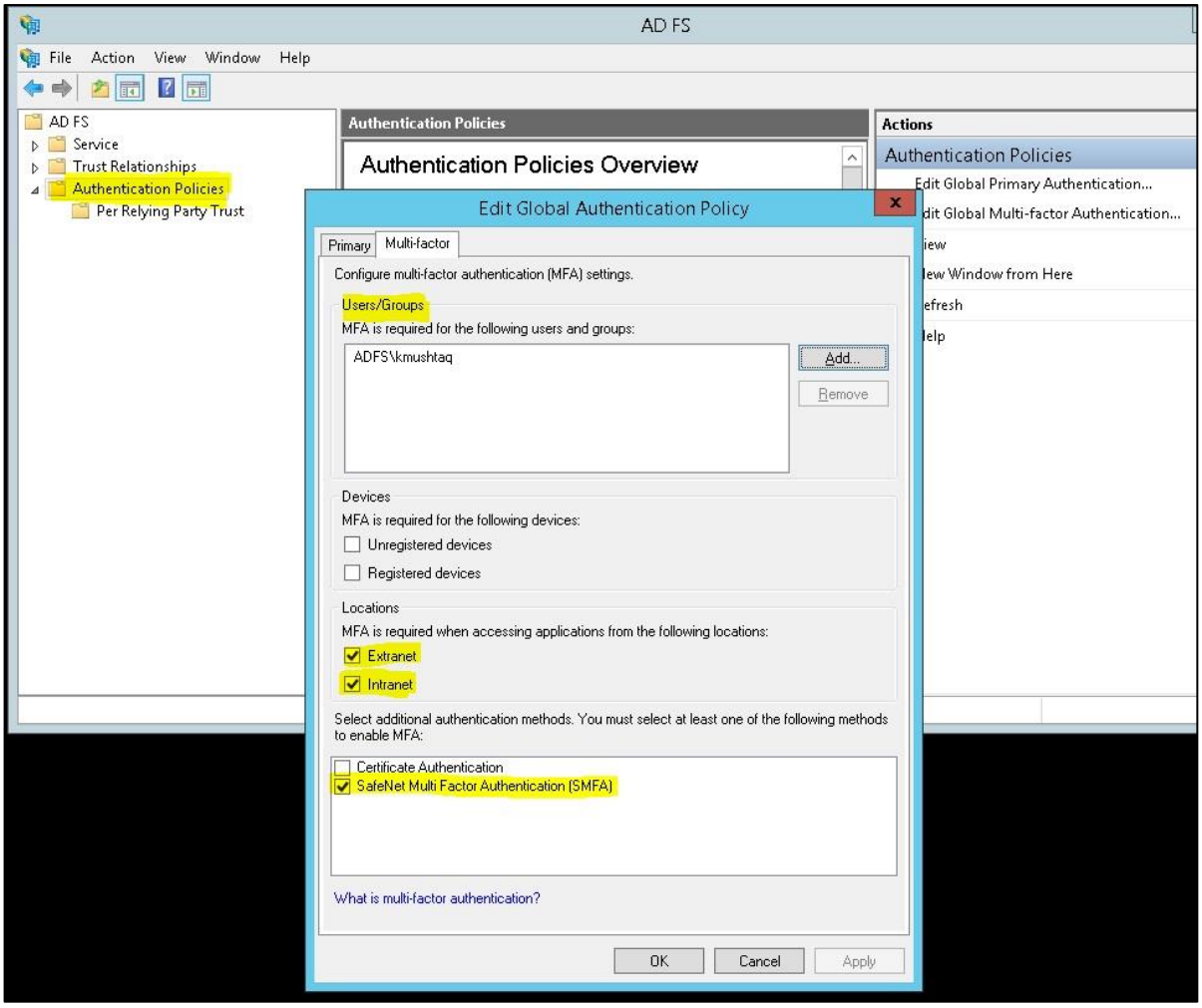
Enforcing Multi-Factor Policies in AD FS 3.0

Enabling the agent on the SafeNet AD FS **Agent Policy** tab (see **Configuring SafeNet Agent for AD FS** on page 26) 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:



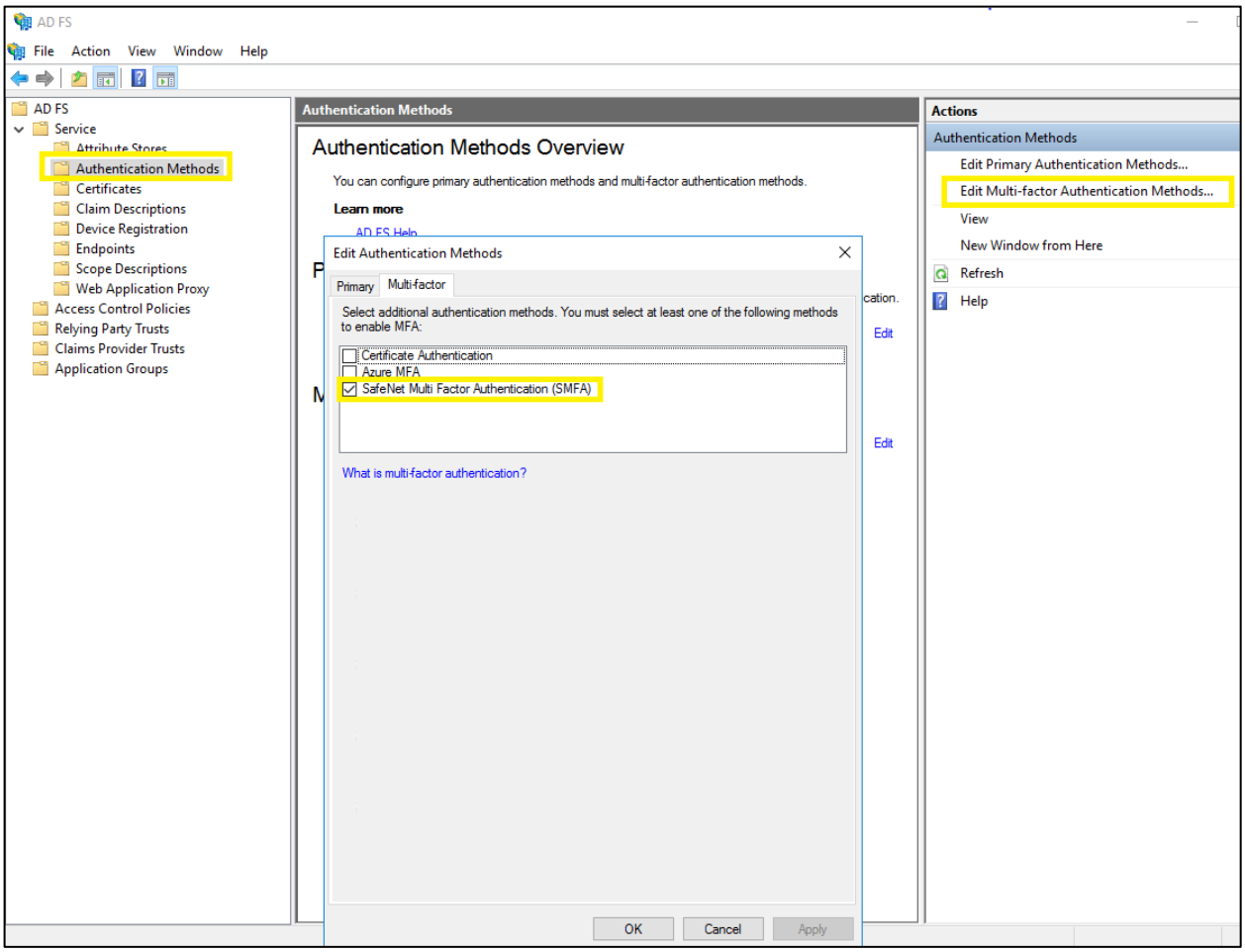
   a. Add the required users and groups (optional).
   b. Select **Extranet** or **Intranet** to specify if MFA is required when accessing applications at these locations.
   c. Select **SafeNet Multi Factor Authentication (SMFA)** method.
   d. Click **OK**.

Checking Multi-Factor Policies in AD FS 4.0

Enabling the agent on the SafeNet AD FS **Agent Policy** tab (see **Configuring SafeNet Agent for AD FS** on page 26) 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.



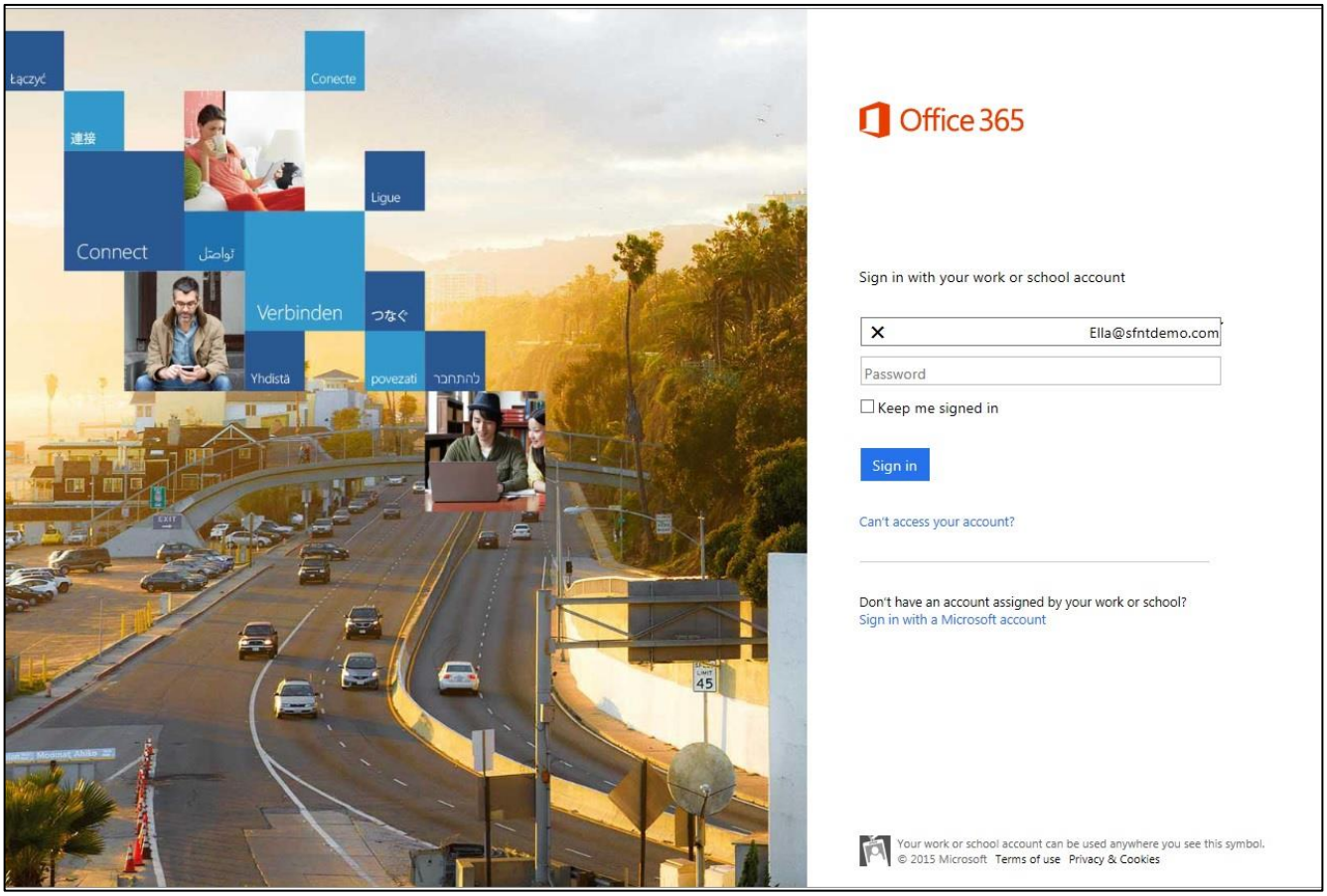
NOTE: If the agent is reinstalled or upgraded for Windows Server 2019 and if the AD FS admin enables the **Allow additional Authentication Provider as Primary** settings and from the list, chooses **SafeNet Multi Factor Authentication (SMFA)** as primary authentication, then under the **Additional Authentication** tab, the **SMFA** check-box 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.

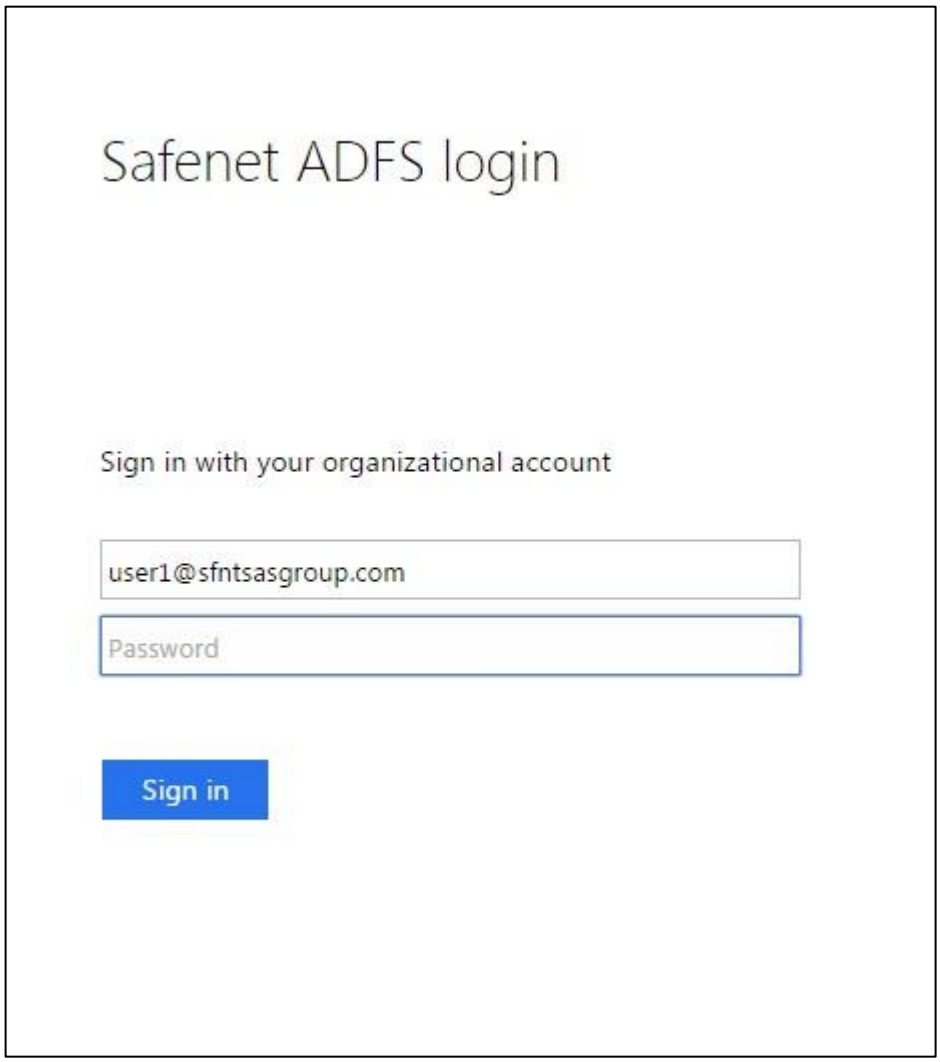
Logging to Office 365

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)



Secondary Authentication (SafeNet Grid Token)