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.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Product Version: 2.02
Document Part Number: 007-012546-001, Rev G
Release Date: 29 August 2016
# Contents

1 Preface ......................................................................................................................... 4  
   Audience ...................................................................................................................... 4  
   Related Documents ..................................................................................................... 4  
   Support Contacts ........................................................................................................ 4  

2 Introduction .................................................................................................................. 5  
   Applicability ................................................................................................................. 5  
   Support for Push OTP .................................................................................................. 5  
   Environment .................................................................................................................. 6  
   Overview of AD FS ...................................................................................................... 6  
   Authentication Concepts for AD FS in Windows Server 2012 R2 ......................... 7  
      Primary and Secondary Authentication .................................................................... 7  
      Authentication Flow .................................................................................................. 7  
      Invoking MFA ........................................................................................................... 7  

3 Installation .................................................................................................................... 8  
   Prerequisite Tasks ........................................................................................................ 8  
   Installing the SafeNet Authentication Service Agent for AD FS ................................ 8  
   Upgrading ...................................................................................................................... 9  
      Upgrading from SafeNet Authentication Service Agent for AD FS 2.01 to version 2.02 ................................................................. 9  
      Migrating Settings to SafeNet Authentication Service Agent for AD FS 2.02 from Versions 2.0 or Earlier ......................................................... 9  
      Updating Localization Settings following Migration ............................................ 10  
   Removing Users and Groups following Uninstall or De-activation of SafeNet Authentication Service Agent for AD FS ........................................ 11  

4 Configuring SafeNet Authentication Service Agent for AD FS .............................. 12  
   Configuring the SafeNet Authentication Service Manager ........................................ 12  
   Configuring the Agent Key File .................................................................................... 12  
   Configuring SafeNet Authentication Service Agent for AD FS ................................ 13  
      Configuring Policy .................................................................................................... 13  
      Configuring Communications ................................................................................... 14  
      Configuring an AD FS Federation Server Farm .................................................. 17  
   Configuring Localization ............................................................................................ 20  
      Setting Additional Localizations ............................................................................ 20  
      Viewing Localization Settings ............................................................................... 25  
   Setting Multi-Factor Policies in AD FS ....................................................................... 26  

5 Working with Microsoft Office 365 ............................................................................ 27  
   Logging On to Microsoft Office 365 ........................................................................... 27  
   Sign-In Window Examples ......................................................................................... 28
Preface

Audience

This document is intended for personnel responsible for maintaining your organization’s security infrastructure. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Gemalto, Inc. 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.

Related Documents

The following document contains related or additional information:

- SafeNet Authentication Service Agent for AD FS Customer Release Notes

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read 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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>US</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>
Introduction

Applicability

The information in this document applies to:

- SafeNet Authentication Service (SAS) Cloud Edition
- SafeNet Authentication Service (SAS) PCE/SPE

Support for Push OTP

SAS Agent for AD FS supports the Push OTP function with MobilePASS+ (SafeNet’s next generation mobile authenticator) with SAS Cloud Edition.

NOTE: Push OTP is not currently supported for SAS PCE/SPE.
Environment

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>Windows Server 2012 R2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Architecture</td>
<td>64-bit</td>
</tr>
</tbody>
</table>
| Additional Software Components | Microsoft .Net Framework 4.5  
                                 | Microsoft PowerShell v3.0 |
| Supported Authentication Methods | All tokens and authentication methods supported by SafeNet Authentication Service. |
| Supported Web Browsers    | Internet Explorer 8, 9, 10, 11  
                                 | Microsoft Edge (not supported on mobile devices)  
                                 | Firefox 3 and later  
                                 | Chrome  
                                 | Safari |

Overview of AD FS

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

Multi-factor authentication 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 BYOD client devices. AD FS introduces a pluggable MFA concept focused on integration with AD FS policy.
Authentication Concepts for AD FS in Windows Server 2012 R2

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 TLS, including smart card authentication)

The above methods are still supported in Windows Server 2012 R2, but are now called “primary authentication” because Microsoft has introduced a new feature called secondary, or “additional”, authentication. This is where SAS Agent for AD FS, a multi-factor authentication 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 what we call 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 multi-factor authentication through the concept of additional authentication providers that are 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 an AD FS MFA adapter.

Invoking MFA

There are two ways to configure AD FS in Windows Server 2012 R2 to invoke multi factor authentication—policy configuration or via the WS-Federation or SAML protocol token request.

Via policy, AD FS in Windows Server 2012 R2 introduces a new rule set called Additional Authentication Rules that are used for triggering multi factor authentication. 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 multi factor authentication. 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.
Installation

Prerequisite Tasks

Do the following before installation:

- In Windows Server 2012 R2, enable AD FS.

Installing the SafeNet Authentication Service Agent for AD FS

NOTE: Always work in Run as Administrator mode when installing or uninstalling SAS Agent for AD FS

To install the SAS AD FS Agent:

1. Run as administrator the SAS 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 window, click Next.
3. On the License Agreement window, select I accept the terms in the license agreement, and then click Next.
4. On the Customer Information window, enter User Name and Organization, and then click Next.
5. On the 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 the Authentication Service Setup window, enter the hostname or IP address of the SAS primary and failover servers.
7. On the Ready to Install the Program window, click Install.
   When the installation process is completed, the Installshield Wizard Completed window is displayed.
8. Click Finish to exit the installation wizard.
Upgrading

Upgrade from SAS Agent for AD FS 2.01 to version 2.02 is supported.
Upgrade from SAS Agent for AD FS 1.0, 1.01 and 2.0 is not supported, but their settings can be migrated to version 2.02.

Upgrading from SafeNet Authentication Service Agent for AD FS 2.01 to version 2.02

Upgrade is supported from SAS Agent for AD FS 2.01 to version 2.02
Upgrade from earlier versions is not supported.

To upgrade from SAS Agent for AD FS 2.01 to version 2.02:
Run the SAS Agent for AD FS 2.02 installation on the same computer as the installed version 2.01.

Migrating Settings to SafeNet Authentication Service Agent for AD FS 2.02 from Versions 2.0 or Earlier

Upgrade to SAS Agent for AD FS 2.02 from versions 1.0, 1.01 or 2.0 is not supported, however, you can migrate settings from these versions.

NOTE: Upgrade from existing installations earlier than version 2.01 is blocked, and will cause an error message indicating that uninstall is required.

To migrate settings to SAS Agent for AD FS 2.02 from version 2.0 or earlier:

1. In the SAS Agent for AD FS 2.0 or earlier installation folder (C:\Program Files\SafeNet\SAS\SafeNetMFA\ini), copy the SAFENET-MFA.ini file and save it for later use.
2. Uninstall SAS Agent for AD FS.
3. Delete all remaining installation folders (C:\Program Files\SafeNet\SAS\SafeNetMFA).
4. Install SAS Agent for AD FS 2.02.
5. Replace the SAFENET-MFA.ini file in the SAS Agent for AS FS 2.02 installation folder (C:\Program Files\SafeNet\SAS\SafeNetMFA\ini) with the file saved from the previous version.
### Updating Localization Settings following Migration

After replacing the SAFENET-MFA.ini file in the SAS Agent for AS FS 2.02 installation folder with the file saved from version 2.0 or earlier, and enabling SAS Agent for AD FS in 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:

<table>
<thead>
<tr>
<th>Message</th>
<th>Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021</td>
<td>Your request timed out. Please try again.</td>
</tr>
<tr>
<td>2022</td>
<td>Error when creating autosend message, Please contact administrator.</td>
</tr>
<tr>
<td>2023</td>
<td>Authentication process was canceled.</td>
</tr>
<tr>
<td>2024</td>
<td>Passcode was not autosent. Please try again or enter passcode.</td>
</tr>
<tr>
<td>2025</td>
<td>Auto push has failed, Authentication ID not found, Please contact administrator.</td>
</tr>
<tr>
<td>2026</td>
<td>Auto push has failed, Authentication ID conflicted, Please contact administrator.</td>
</tr>
<tr>
<td>2027</td>
<td>Auto push has failed, unknown error.</td>
</tr>
<tr>
<td>2028</td>
<td>Authentication failed.</td>
</tr>
<tr>
<td>2029</td>
<td>Authentication request was cancelled. Please try again</td>
</tr>
</tbody>
</table>

To translate the messages, open the SAFENET-MFA.ini file in a text editor and edit the required text.
Removing Users and Groups following Uninstall or De-activation of SafeNet Authentication Service Agent for AD FS

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

After uninstalling or de-activating SAS 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 SAS Agent for AD FS, open the SAS MFA Plug-In Manager Policy tab and clear the Enable Agent checkbox. See "Configuring SafeNet Authentication Service Agent for AD FS" on page 12.

To remove users and groups from the AD FS server:

1. In the AD FS window, select Authentication Policies > Per Relying Party Trust > Edit Custom Multi-factor Authentication.
2. In 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.
Configuring SafeNet Authentication Service Agent for AD FS

Configuring the SafeNet Authentication Service Manager

To configure SafeNet Authentication Service for AD FS:

1. In the SafeNet Authentication Service Manager, select Virtual Servers > COMMS > Auth Nodes.
2. Click Add.
3. Enter the IP address or range of addresses of the SAS Agent for AD FS computer.
4. Click Apply.

Configuring the 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 SAS, select the 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 the Communications tab.
4. Click the 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 Authentication Service Agent for AD FS

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

To open the SAS Agent for AD FS SAS MFA Policy Manger:
Select Start > All Programs > SafeNet > Agents > SafeNet MFA Plugin Manager.

Configuring Policy

To configure SAS Agent for AD FS policy:

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

2. Complete the fields as follows, and then click Apply.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Agent</td>
<td>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 following Uninstall or De-activation of SafeNet Authentication Service Agent for AD FS” on page 11.</td>
</tr>
<tr>
<td>Ignore SAS Server certificate errors</td>
<td>Select to prevent checking of SAS certificate validity.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
**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
  
  **Notes:**
  SAS Agent for AD FS supports the Push OTP function with MobilePASS+
  Push OTP is not currently supported for SAS PCE/SPE.

- **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.

**Configuring Communications**

1. Click the **Communications** tab.
2. Complete the fields as follows, and then click **Apply**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Server (IP:Port)</strong></td>
<td>Used to configure the IP address/hostname of the primary SAS server. The default is port 80. Alternatively, <strong>Use SSL</strong> can also be selected. The default TCP port for SSL requests is 443.</td>
</tr>
<tr>
<td><strong>Secondary Server (optional)</strong></td>
<td>Used to configure the IP address/hostname of the failover SAS server. The default is port 80. Alternatively, <strong>Use SSL</strong> can also be selected. The default TCP port for SSL requests is 443.</td>
</tr>
<tr>
<td><strong>Agent Encryption File Key</strong></td>
<td>Used to specify the location of the SAS Agent for AD FS key file. For details, see “Configuring the Agent Key File”, on page 12.</td>
</tr>
<tr>
<td><strong>TCP/IP Call Timeout (in seconds)</strong></td>
<td>Sets the maximum timeout value in seconds for authentication requests sent to the SAS server.</td>
</tr>
<tr>
<td><strong>User ID Format</strong></td>
<td>Select the required ID format for the SAS usernames:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Include Realm</strong> (“<a href="mailto:Username@domain.com">Username@domain.com</a>” is sent as SAS User ID)</td>
</tr>
<tr>
<td></td>
<td>- <strong>Strip realm</strong> (“Username” is sent as User ID)</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The realm stripping feature applies to SAS usernames only. Active Directory usernames are not affected.</td>
</tr>
<tr>
<td><strong>Authentication Test</strong></td>
<td>This function allows administrators to test authentication between the SAS Agent for AD FS and the SAS server. Enter <strong>User Name</strong> and <strong>Password</strong> and then click <strong>Test</strong>. The result of the test is displayed in the <strong>Authentication Test Result</strong> text box.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- The test works with manual OTP. Push OTP is not supported.</td>
</tr>
<tr>
<td><strong>Server Status Check</strong></td>
<td>This function performs a communication test to verify a connection to the SAS server.</td>
</tr>
</tbody>
</table>
3. Click the **Logging** tab. Select the required logging level and log file location, and then click **Apply**.

4. Complete the setting as follows, and then click **Apply**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
Configuring an 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 SAS 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 the SAS MFA Plug-In Manager window, click the Farm Configuration tab.
2. Select Farm configuration.
3. Click Add.
4. In the **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**.

![Add Secondary Server](image)

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

![Secondary Servers](image)

5. 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**.
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
Configuring 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 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 © 2015. Gemalto Inc. 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.

<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>Authentification réussie</td>
</tr>
<tr>
<td>1002</td>
<td>L'authentification a échoué. Veuillez réessayer.</td>
</tr>
<tr>
<td>1003</td>
<td>Veuillez répondre au défi du serveur :</td>
</tr>
<tr>
<td>1004</td>
<td>Veuillez vous authentifier à nouveau en utilisant la réponse suivante. Votre nouveau code PIN est :</td>
</tr>
<tr>
<td>1005</td>
<td>Veuillez saisir un nouveau code PIN.</td>
</tr>
<tr>
<td>1006</td>
<td>Veuillez vous authentifier avec un nouvel OTP.</td>
</tr>
<tr>
<td>1007</td>
<td>Votre mot de passe a expiré. Veuillez saisir un nouveau mot de passe.</td>
</tr>
<tr>
<td>1008</td>
<td>Le changement de mot de passe a échoué. Veuillez saisir un nouveau mot de passe.</td>
</tr>
<tr>
<td>1009</td>
<td>Le changement de PIN a échoué. Veuillez saisir un nouveau code PIN.</td>
</tr>
<tr>
<td>1010</td>
<td>Le mom d'utilisateur ne peut pas être vide.</td>
</tr>
<tr>
<td>1011</td>
<td>Non implémenté. Veuillez fermer le navigateur web.</td>
</tr>
<tr>
<td>1012</td>
<td>Veuillez saisir votre code PIN en utilisant les caractères correspondant au modèle choisi.</td>
</tr>
<tr>
<td>1013</td>
<td>Veuillez saisir la réponse au challenge du serveur qui a été envoyé à votre mobile.</td>
</tr>
<tr>
<td>1014</td>
<td>Gemalto ADFS Authentification forte multi-facteurs</td>
</tr>
<tr>
<td>1015</td>
<td>Nom d'utilisateur:</td>
</tr>
<tr>
<td>1016</td>
<td>Passcode:</td>
</tr>
<tr>
<td>1017</td>
<td>Nouveau mot de passe:</td>
</tr>
</tbody>
</table>
1018 = Confirmer le nouveau mot de passe:
1019 = Nouveau code PIN:
1020 = Confirmer le nouveau code PIN:
1021 = Envoyer
1022 = Copyright © 2015. Gemalto Inc. 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 = invalidate 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.
3. To add an additional language, add the decimal LCID to the AvailableLcids row, inserting a comma as 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 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 Localizations” on page 20.

To view the localization settings in the SAS 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 the **SAS MFA Plug-In Manager** window, click the **Localization** tab.
Setting Multi-Factor Policies in AD FS

Enabling the agent on the SAS AD FS Agent Policy tab (see “Configuring SafeNet Authentication Service Agent for AD FS” on page 12 (registers the SafeNet AD FS Agent with AD FS and enables it at the global policy level.

After registration, you can enforce multi-factor authentication (MFA) policies at the required level in the AD FS window.

To enforce MFA policies:

1. Under AD FS, select Authentication Policies.
3. If required, in the Edit Global Authentication Policy window, add the required users and groups (optional).
4. Select Extranet and/or Intranet to specify that MFA is required at these locations.
5. Select the SafeNet Multi Factor Authentication (SMFA) method.
Working with Microsoft Office 365

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

Logging On to Microsoft 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 https://portal.microsoftonline.com/.

**NOTE:** Leave the password field empty when logging-in, to enable redirection to AD FS.
Sign-In Window Examples

Primary Authentication (Windows Credentials)

Safenet ADFS login

Sign in with your organizational account

Username: user1@stetsasgroup.com
Password

Sign in

Secondary Authentication (SafeNet Grid Token)

Gemalto

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:

Submit