SafeNet Authentication Service
Configuration Guide

SAS Agent for AD FS
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012546-001, Rev C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>4 May 2015</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

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

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

Preface .................................................................................................................................. 4
Support Contacts .................................................................................................................. 4
CHAPTER 1 Introduction ...................................................................................................... 5
  Applicability ...................................................................................................................... 5
  Environment ....................................................................................................................... 5
  Overview ........................................................................................................................... 5
    New Authentication Concepts in AD FS in Windows Server 2012 R2 .............................................. 6
  Prerequisite Tasks .......................................................................................................... 7
CHAPTER 2 Installation and Upgrade .................................................................................. 8
  Installing the SAS Agent for AD FS .................................................................................. 8
  Upgrading the SAS Agent for AD FS ............................................................................... 9
CHAPTER 3 Configuring SAS AD FS Agent ...................................................................... 10
  Configuring the SafeNet Authentication Service Manager .................................................. 10
  Configuring the Agent Key File ....................................................................................... 10
  Configuring SAS Agent for AD FS .................................................................................. 11
  Configuring Localization .................................................................................................. 14
    Setting Additional Localizations ................................................................................... 14
    Viewing Localization Settings ....................................................................................... 17
  Setting Multi-Factor Policies in AD FS ............................................................................ 18
CHAPTER 4 Working with Microsoft Office 365 ................................................................. 19
  Logging On to Microsoft Office 365 ................................................................................. 19
    Sign-In Window Examples ............................................................................................ 20
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 SafeNet Customer Support. SafeNet 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 SafeNet 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 1: Support Contacts

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>SafeNet, Inc.</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>United States</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 Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
</tbody>
</table>
|                                | Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.
CHAPTER 1: Introduction

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**
  A cloud authentication service of SafeNet, Inc.

- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**
  The software used to build a SafeNet authentication service.

- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**
  A term used to describe the implementation of SAS-SPE on-premises.

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>
<tr>
<td>Additional Software Components</td>
<td>Microsoft .Net Framework 4.5</td>
</tr>
<tr>
<td></td>
<td>Microsoft PowerShell v3.0</td>
</tr>
</tbody>
</table>

Overview

Microsoft introduced multi-factor authentication (MFA) as part of Conditional Access policies in AD FS. Multi-factor authentication is one of the key elements of conditional access policies in AD FS in Windows Server 2012 R2. Multi-factor authentication has traditionally meant using a smart card or other second factor with AD-based authentication, such as Integrated 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. Because of this, AD FS introduces a new pluggable MFA concept focused on flexibility, integration with AD FS policy, and a consistent user experience.
New Authentication Concepts in 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 SafeNet AD FS Agent, 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 presents the friendly name of each provider and allows the user to select one by clicking on it.
Prerequisite Tasks

The following prerequisite tasks must be completed:

- In Windows Server 2012 R2, enable AD FS.
Installing the 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 Ready to Install the Program window, click Install.
   When the installation process is completed, the Installshield Wizard Completed window is displayed.
7. Click Finish to exit the installation wizard.
Upgrading the SAS Agent for AD FS

To upgrade the SAS AD FS Agent:
1. On the same computer as the installed AD FS Agent, run as administrator the SafeNet Authentication Service Agent for AD FSD installer:
   ```
   SafeNetAuthentication Service Agent for ADFS.exe
   ```

2. Click Yes to continue.
3. On the Welcome to the InstallShield Wizard for SafeNet Authentication Service Agent for ADFS window, click Next.
4. On the License Agreement window, select I accept the terms in the license agreement, and then click Next.
5. On the Ready to Install the Program window, click Install.
   When the installation process is completed, the Installshield Wizard Completed window is displayed.
6. Click Finish to exit the installation wizard.
CHAPTER 3
Configuring SAS AD FS Agent

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. To accomplish this, a key file is loaded and registered with SAS agents, and then a matching key file is installed and registered with the web service.

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 AD FS Agent Manager, select Start > All Programs > SafeNet > Agents > ADFS Agent.
3. Click the Communications tab.
4. Click the Agent Encryption Key File browse button and navigate to the agent key file.
5. Click Apply.
Configuring SAS Agent for AD FS

To configure the SAS Agent for AD FS:

1. Select Start > All Programs > SafeNet > Agents > ADFS Agent.
2. On the SAS MFA Plug-In Manager window, click the Policy tab.

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

<table>
<thead>
<tr>
<th>Enable/Disable Agent</th>
<th>Select this option to enable the SAS AD FS Agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Generate Challenge</td>
<td>Select this option to display the grid immediately following the first authentication step. If this option is not selected, the user can display the GrIDsure grid by leaving the OTP field empty and clicking Submit.</td>
</tr>
<tr>
<td>Ignore SAS Server certificate errors</td>
<td>Select this option if required to send the remote client’s IP address to the SAS Server.</td>
</tr>
<tr>
<td>IP Address for Rules</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Use web server’s detected IP address for IP based rules</td>
</tr>
<tr>
<td></td>
<td>• Send the remote client’s IP address to the SafeNet server for IP based rules</td>
</tr>
</tbody>
</table>
4. Click the Communications tab.

5. 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, Use SSL 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, Use SSL 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 10.</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>Strip realm from UPN (<a href="mailto:username@domain.com">username@domain.com</a> will be sent as username)</strong></td>
<td>Select if the SAS username is required without the suffix @domain. <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. <strong>Note:</strong> The behavior of the test will be in accordance with the realm stripping configuration. So, 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>
</tbody>
</table>
Server Status Check | This function performs a communication test to verify a connection to the SAS server.

6. Click the Logging tab. Select the required logging level and log file location, and then click Apply.

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

| Logging Level | Set the required logging level. For log levels 1, 2, and 3, only the initial connection between the agent and server attempts are logged. Log level 5 sets the agent in debug mode. The default value is 3. |
| Log File Location | Specifies the location of the log files. The log file is rotated on a daily basis. |
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 (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.

```ini
[SAFENET-DEFAULT]
1001=SafeNet authentication successful
1002=SafeNet authentication failed. Generate a new OTP, and then enter your PIN + new OTP.
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=SafeNet ADFS Multi-Factor Strong Authentication
1015=User Name:
1016=OTP:
1017=New Password:
1018=Confirm New Password:
1019=New PIN:
1020=Confirm New PIN:
1021=Submit
1022=Copyright &© 169; 2015. SafeNet Inc. All Rights Reserved.
1023=To log in, please enter a valid response to the server challenge.

2000=Invalid incoming authentication context.
2001=Invalid incoming identity claim.
2002=The user authenticated by ADFS does not match the SafeNet 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 SafeNet 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.
```
The [3084] section lists the same messages as in the [SAFENET-DEFAULT] section, but translated to French-Canada.

<table>
<thead>
<tr>
<th>Message Number</th>
<th>Message Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>SafeNet authentification réussie</td>
</tr>
<tr>
<td>1002</td>
<td>SafeNet authentification a échoué. Générer un nouveau OTP, puis entrez votre NIP + nouveau OTP.</td>
</tr>
<tr>
<td>1003</td>
<td>S'il vous plaît entrer dans la réponse au défi du serveur:</td>
</tr>
<tr>
<td>1004</td>
<td>S'il vous plaît authentifier, en utilisant la réponse suivante. Votre nouveau code PIN est:</td>
</tr>
<tr>
<td>1005</td>
<td>S'il vous plaît entrer un nouveau code PIN.</td>
</tr>
<tr>
<td>1006</td>
<td>S'il vous plaît générer un nouveau Bureau du Procureur, et l’utiliser pour s’authentifier à nouveau.</td>
</tr>
<tr>
<td>1007</td>
<td>Votre mot de passe a expiré. S'il vous plaît entrer un nouveau mot de passe.</td>
</tr>
<tr>
<td>1008</td>
<td>changement de mot de passe a échoué. S'il vous plaît entrer un nouveau mot de passe.</td>
</tr>
<tr>
<td>1009</td>
<td>changement de NIP a échoué. S'il vous plaît entrer un nouveau code PIN.</td>
</tr>
<tr>
<td>1010</td>
<td>Nom d'utilisateur ne peut être vide.</td>
</tr>
<tr>
<td>1011</td>
<td>Non implémenté. S'il vous plaît fermez le navigateur web.</td>
</tr>
<tr>
<td>1012</td>
<td>S'il vous plaît entrer votre code PIN ainsi que les caractères correspondant à votre modèle choisi.</td>
</tr>
<tr>
<td>1013</td>
<td>S'il vous plaît entrer dans la réponse au défi du serveur qui a été envoyé à votre appareil mobile.</td>
</tr>
<tr>
<td>1014</td>
<td>SafeNet Authentication ADFS multi-facteurs forte</td>
</tr>
<tr>
<td>1015</td>
<td>Nom d'utilisateur:</td>
</tr>
<tr>
<td>1016</td>
<td>PIN + OTP:</td>
</tr>
<tr>
<td>1017</td>
<td>Nouveau mot de passe:</td>
</tr>
<tr>
<td>1018</td>
<td>Confirmer le nouveau mot de passe:</td>
</tr>
<tr>
<td>1019</td>
<td>Nouveau code PIN:</td>
</tr>
<tr>
<td>1020</td>
<td>Confirmer le nouveau code PIN:</td>
</tr>
<tr>
<td>1021</td>
<td>Envoyer</td>
</tr>
<tr>
<td>1022</td>
<td>Copyright © 2015. SafeNet Inc. Tous droits réservés.</td>
</tr>
<tr>
<td>1023</td>
<td>Pour vous connecter, s'il vous plaît entrer une réponse valable à la question de serveur.</td>
</tr>
<tr>
<td>2000</td>
<td>contexte d'authentification entrant valide.</td>
</tr>
<tr>
<td>2001</td>
<td>invalide revendication d'identité entrant.</td>
</tr>
<tr>
<td>2002</td>
<td>L'utilisateur authentifié par ADFS ne correspond pas à l'utilisateur de la session SafeNet.</td>
</tr>
<tr>
<td>2003</td>
<td>Impossible de trouver le fichier de modèle d'authentification. S'il vous plaît voir les journaux pour obtenir des informations d'erreur.</td>
</tr>
<tr>
<td>2004</td>
<td>Impossible d'effectuer une pré-générer un défi pour l'utilisateur [ { 0 } ].</td>
</tr>
<tr>
<td>2005</td>
<td>invalide posté utilisateur. Nom d'utilisateur ne correspond pas à l'utilisateur en session SafeNet.</td>
</tr>
<tr>
<td>2006</td>
<td>valeurs = Nouveau code PIN / mot de passe sont vides ou ne correspondent pas.</td>
</tr>
<tr>
<td>2007</td>
<td>Impossible d'obtenir le fichier de changement de modèle NIP / mot de passe. S'il vous plaît voir les journaux pour obtenir des informations d'erreur.</td>
</tr>
</tbody>
</table>
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 steps 3 to 4 for each additional language.

Viewing Localization Settings

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

1. To open the AD FS Agent Manager, click Start > All Programs > SafeNet > Agents > ADFS Agent.
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 SAS Agent for AD FS” on page 11 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 Management window.

To enforce MFA policies:

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

Secondary Authentication (SafeNet Grid Token)