SafeNet Authentication Service
Integration Guide

Using SAS as an Identity Provider for MS Azure AD
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.

© 2015 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.

Document Part Number: 007-013304-001, Rev. A
Release Date: October 2015
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>4</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>SAS Authentication API Authentication using SAS Cloud</td>
<td>5</td>
</tr>
<tr>
<td>SAS Authentication API using SAS-SPE and SAS-PCE</td>
<td>5</td>
</tr>
<tr>
<td>SAS Authentication API Flow using SAS</td>
<td>6</td>
</tr>
<tr>
<td>Configuring a SAS Auth Node and Encryption Key</td>
<td>7</td>
</tr>
<tr>
<td>Configuring MS Azure AD and AD FS</td>
<td>8</td>
</tr>
<tr>
<td>Adding a Domain to Azure</td>
<td>9</td>
</tr>
<tr>
<td>Syncing a Domain to Azure</td>
<td>11</td>
</tr>
<tr>
<td>Verifying the AD Connect Installation</td>
<td>15</td>
</tr>
<tr>
<td>Enabling Azure AD Federated Domains</td>
<td>16</td>
</tr>
<tr>
<td>Configuring the AD FS Agent</td>
<td>18</td>
</tr>
<tr>
<td>Configuring the AD FS Authentication Policy</td>
<td>20</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>22</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SAS</td>
<td>22</td>
</tr>
<tr>
<td>Assigning Authenticators in SAS</td>
<td>22</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>23</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>25</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as MS Azure AD.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Azure Active Directory (Azure AD) is Microsoft’s multi-tenant cloud based directory and identity management service. Azure AD provides an easy-to-use solution to give employees and business partners single sign-on (SSO) access to thousands of cloud SaaS Applications such as Office365, Salesforce.com, DropBox, and Concur.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in MS Azure AD using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in MS Azure AD using SafeNet Authentication Service as an identity provider.

It is assumed that the MS Azure AD environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

MS Azure AD can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by service providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service (Cloud)**
- **MS Azure AD (Cloud)**
Audience

This document is targeted to system administrators who are familiar with MS Azure AD and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAS Authentication API Authentication using SAS Cloud

SAS Cloud provides a service for SAS Authentication API that is already implemented in the SAS Cloud environment and can be used using the Gemalto SafeNet SAS ADFS Agent.

SAS Authentication API using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with AD FS infrastructure, which uses a special on-premises agent called Gemalto SafeNet SAS ADFS Agent.
SAS Authentication API Flow using SAS

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”.

Gemalto SafeNet SAS ADFS Agent is an AD FS MFA adapter that provides users a way to authenticate through AD FS using SAS as a secondary authenticator.

The image below describes the dataflow of a multi-factor authentication transaction for MS Azure AD.

1. A user attempts Sign in to MS Azure AD. The user is redirected AD FS proxy server (WAP), then after successful authentication, is forwarded to SafeNet Authentication Service (SAS) for a secondary authentication (AD FS multi-factor authentication).
2. The user uses his SAS token for authenticating. SAS collects and evaluates the user’s credentials.
3. The SAS authentication reply is sent back to AD FS which returns a response to MS Azure AD, accepting or rejecting the user’s authentication request.
4. The user is granted or denied access to MS Azure AD.
Configuring a SAS Auth Node and Encryption Key

If the SAS server is not installed on the same machine as AD and AD FS, the following steps must be performed.

1. Log in to the SAS console with an Operator account.
2. Click VIRTUAL SERVERS > COMMS > Authentication Processing.
3. Click the Authentication Agent Settings link, and then click Download to download the encryption key file. (This file will be needed in step 4 in “Configuring the AD FS Agent” on page 18.)

4. Click VIRTUAL SERVERS > COMMS > Auth Nodes.
5. Click the Auth Nodes link.
6. Under Auth Nodes, click Add.
7. In the Add Auth Nodes section, complete the following fields, and then click Save:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a description for this node (for example, DC).</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the lowest IP address that will authenticate with SAS.</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter the highest IP address that will authenticate with SAS. (The low and high IP addresses may be the same, since the node is referencing a single machine.)</td>
</tr>
<tr>
<td>Exclude from PIN change requests</td>
<td>Do not select this check box.</td>
</tr>
</tbody>
</table>
Configuring MS Azure AD and AD FS

Configuring MS Azure AD and AD FS requires the following:

- Adding a Domain to Azure, page 9
- Syncing a Domain to Azure, page 11
- Verifying the AD Connect Installation, page 15
- Enabling Azure AD Federated Domains, page 16
- Configuring the AD FS Agent, page 18
- Configuring the AD FS Authentication Policy, page 20
Adding a Domain to Azure

2. Click Active Directory.

3. Click on your directory (for example, SFNTdemo), and the click Add domain.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. Enter the domain name, and then click **add**.

5. The domain is added but unverified. To verify the domain, you will need to add some values to your DNS. Follow Microsoft's guidelines, and then click **verify** when you're done.
6. The new domain is now verified and ready to use. To verify the domain, click the **DOMAINS** tab at the top of the screen.

![Image of Microsoft Azure Management Portal with the DOMAINS tab highlighted.](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

### Syncing a Domain to Azure

1. On the Windows Azure Management Portal, click **Active Directory**.

![Image of Microsoft Azure Management Portal with the Active Directory tab highlighted.](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
2. Click on your directory (for example, SFNTdemo).

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. Under Integrate with your local directory, click the Download Azure AD Connect link.

4. Install Azure AD Connect on a machine that is part of the domain to connect to Azure. On the Welcome window, click Continue.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. On the **Express Settings** window, click **Use express settings**.

![Express Settings](image1.png)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

6. On the **Connect to Azure AD** window, enter your Azure AD administrator username and password, and then click **Next**.

![Connect to Azure AD](image2.png)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
7. On the **Connect to AD DS** window, enter the domain administrator username and password, and then click **Next**.

![Connect to AD DS window](image1)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

8. On the **Configure** window, click **Install**.

![Configure window](image2)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
9. Click **Exit** when the configuration is complete. After the sync process starts, your AD users will be able to log in to Azure.

![Configuration complete](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

**Verifying the AD Connect Installation**

After you have successfully installed Azure AD Connect, you can verify that synchronization is occurring by signing in to the Azure portal, and then checking the last sync time.

1. Log into the Windows **Azure Management Portal**.
2. Click **Active Directory**.

![Active Directory](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
3. Click on your directory (in this case SFNTdemo).

4. Click the DIRECTORY INTEGRATION tab at the top of the screen and check the last sync time.

![Microsoft Azure AD Directory Integration Screenshot](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

**Enabling Azure AD Federated Domains**

The SAS Administrator Console settings are used to establish SafeNet Authentication Service (SAS) as the identity provider for Azure AD.

1. Log in to the AD FS server machine as Domain Admin.
2. Open **Windows Azure AD Module for Windows PowerShell**.
3. At the command prompt, type **Connect-MsolService**, and then press **Enter**.
4. On the **Enter Credentials** dialog box, type your Azure AD administrator's username and password, and then click **OK**.

![Enter Credentials dialog box](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

5. At the command prompt, type the following commands:
   a. `Set-MsolADFSContext -Computer <AD FS machine name>`, and then press **Enter**.
   b. `Convert-MsolDomainToFederated -DomainName <your domain name>`, and then press **Enter**.

![PowerShell command output](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

6. Open the **AD FS Management Console**.
7. **In the left pane, under Console Root, click AD FS > Trust Relationships > Relying Party Trusts.**

In the right pane, **Microsoft Office 365 Identity Platform** (currently this is the Azure Relying Party’s display name) should be listed as a trust.

![Console Root Tree](image)

*The screen image above is from Microsoft® software. Trademarks are the property of their respective owners."

**Configuring the AD FS Agent**

1. **Launch the MFA agent.**
2. **On the Policy tab, verify that the Enable agent and Pre-generate challenge check boxes are selected.**

![MFA Agent Settings](image)
3. On the **Communications** tab, in the **Primary Server** field, type the SAS server IP address or name (and the port if non-causal is used).

![SAS MFA Plug-in Manager](image)

4. If your SAS server is not installed on the same machine as AD and AD FS, the key encryption file must be loaded (the encryption key was downloaded in step 3 in “Configuring a SAS Auth Node and Encryption Key” on page 7).

5. Click **Apply**. Enabling the agent registers the SafeNet MFA adapter with AD FS, and enables it at a global policy level.

6. Verify your settings by testing authentication from the agent to the authentication server. To do so, under **Authentication Test**, enter your **User Name** and **Passcode**, and then click **Test**. The result of the test will be displayed in the **Authentication Test Result** window.

7. Click **OK**.
Configuring the AD FS Authentication Policy

1. In the AD FS Management Console, in the left pane, under AD FS, right-click Authentication Policies.
2. In the far-right pane, select Edit Global Primary Authentication.

1. In the far-right pane, select Edit Global Primary Authentication.

3. On the Primary tab, verify that Forms Authentication is checked for both Extranet and Intranet.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. On the Multi-factor tab, perform the following steps:
   a. Under Users/Groups, add the users and/or groups for which MFA will be required.
   b. Under Locations, choose Extranet and/or Intranet, according to your preferred configuration.
   c. Verify that SafeNet Multi Factor Authentication (SMFA) is selected as an additional authentication method.
   d. Click OK > Apply.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with MS Azure AD using SAML authentication requires:

- Synchronizing Users Stores to SAS, page 22
- Assigning Authenticators in SAS, page 22

Synchronizing Users Stores to SAS

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users who would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service - Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning Authenticators in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users authenticating through MS Azure AD.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS token
- MP-1 software token
- GrIDsure
- MobilePASS

Authenticators can be assigned to users in two ways:

- Manual provisioning—Assign an authenticator to users one at a time.
- Provisioning rules—the administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.
Refer to “provisioning” in the SafeNet Authentication Service - Subscriber Account Operator Guide to learn how to provision the different authentication methods to the users in the SafeNet Authentication Service User Store.


Running the Solution

After Azure AD is configured to use SafeNet Authentication Service as its identity provider, and SafeNet Authentication Service is configured to use AD FS as a SAML service provider, users can log in to the Azure portal using their AD credentials and SAS tokens.

2. Enter the account email to sign in with, and then click OK.

3. The AD FS login page is displayed. Enter your AD credentials, and then click Sign in.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. After successful login using the organizational credentials, SAS login page is displayed. Generate an OTP, and then enter it in the **OTP field**.

![SAS Login Page](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

5. Click **Submit**. After another successful login, you can now use your assigned applications without the need to re-authenticate (using Azure’s SSO capability).

![Applications Access](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
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, 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</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>