SafeNet Authentication Service
Push OTP Integration Guide

Using SAS as an Identity Provider for Office 365
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.
Contents

Third-Party Software Acknowledgement ........................................................................................................... 4
Description .......................................................................................................................................................... 4
Applicability ....................................................................................................................................................... 4
Environment ....................................................................................................................................................... 5
Audience ............................................................................................................................................................ 5
SAS Authentication API using SAS Cloud .......................................................................................................... 5
SAS Authentication API and Push Protocol Flow using SAS ........................................................................... 5
Push OTP Prerequisites ..................................................................................................................................... 6
Configuring Office 365 to Use SAS as an Identity Provider ............................................................................ 7
   Enabling Office 365 Federated Domains ....................................................................................................... 7
   Configuring the Gemalto SafeNet SAS Agent for AD FS ............................................................................... 8
   Configuring the AD FS Authentication Policy .............................................................................................. 10
Configuring SafeNet Authentication Service .................................................................................................. 11
   Creating Users Stores in SAS ....................................................................................................................... 11
   Assigning an Authenticator in SAS .............................................................................................................. 11
   Configuring SAS Auth Node and Encryption Key ...................................................................................... 12
   Enabling the Software Token Push OTP Setting .......................................................................................... 13
   Enabling the Allowed Targets Policy ......................................................................................................... 15
Running the Solution ........................................................................................................................................ 17
   Connecting to Office 365 ............................................................................................................................. 17
   Connecting to Office 365’s SharePoint ......................................................................................................... 20
Support Contacts ................................................................................................................................................ 24
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Office 365.

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.

Microsoft Office 365 is a cloud-based service that is designed to help meet your organization’s needs for robust security, reliability, and user productivity.

This document describes how to:

- Configure Office 365 to work with AD FS as an authenticator and SafeNet Authentication Service as a secondary authentication method.

It is assumed that the Office 365 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Office 365 can be configured to support multi-factor authentication in several modes. The AD FS MFA will be used for the purpose of working with the SafeNet Authentication Service Push OTP solution.

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It is likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to his or her smart phone.
- Assess the validity of the request with the information displayed on the screen.
- Respond quickly with a one-tap response to approve or deny the authentication.

Applicability

The information in this document applies to:

- SafeNet Authentication Service (SAS)—SafeNet’s cloud-based authentication service
- MobilePASS+ application
- Gemalto SafeNet SAS ADFS Agent 2.0
Environment

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

- SafeNet Authentication Service (SAS)
- Office 365—Web account
- AD FS—in Windows Server® 2012 R2

Audience

This document is targeted to system administrators who are familiar with Office 365, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAS Authentication API 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 and Push Protocol Flow using SAS

AD FS provides an 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 Agent for AD FS 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 Office 365.

1. A user attempts to log on to Office 365. The user is redirected to the AD FS proxy server (WAP).
2. After successful authentication, the user is forwarded to SafeNet Authentication Service (SAS) for a secondary authentication (AD FS multi-factor authentication).
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger an on-the-go authentication request.
   - The user receives a push notification on the configured mobile device to indicate there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token’s PIN code).
4. The SAS authentication reply is sent back to AD FS, which returns a response to Office 365, accepting or rejecting the user’s authentication request.
5. The user is granted or denied access to Office 365.

**Push OTP Prerequisites**

In order to use SAS OTP, you will need:
- SAS configured to enable OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+
- Gemalto SafeNet SAS Agent for AD FS—Version 2.0
Configuring Office 365 to Use SAS as an Identity Provider

Enabling Office 365 Federated Domains

The SAS Administrator Console settings are used to establish SafeNet Authentication Service (SAS) as the identity provider for Office 365.

1. Log in to the AD FS server machine as a domain administrator.
3. At the command prompt, type Connect-MsolService, and then press Enter.
4. On the Enter Credentials window, enter your Office 365 user name and password, and then click OK.
5. At the command prompt, type Convert-MsolDomainToFederated –DomainName <your domain name>, and then press Enter.
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** should be listed as a trust.

![Console Root screenshot](image)

**Configuring the Gemalto SafeNet SAS Agent for AD FS**

1. Run the Gemalto SafeNet SAS Agent for AD FS.
2. On the **Policy** tab, verify that **Enable agent** is selected, and the **Push Challenge** option is selected.

![Policy tab screenshot](image)

3. On the **Communications** tab, in the **Primary Server IP** field, enter the SAS server’s IP address or name (and port if non-causal is used). Also, make sure that **Strip realm from UPN** is selected.
4. In case the SAS server is not installed on the same machine as the AD and AD FS, the key encryption file needs to be loaded (as explained in “Configuring SAS Auth Node and Encryption Key” on page 12).

5. Click **Apply**. Enabling the agent registers the SafeNet MFA (multi-factor authentication) adapter with ADFS and enables it at a global policy level.

6. You can 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 under **Authentication Test Result**.

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

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

2. On the Primary tab, verify that Form Authentication is selected for both Extranet and Intranet.

3. Click the Multi-factor tab, and then perform the following steps:
   a. Under Users/Groups, add the users and/or groups for which MFA will be required.
   b. Select 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.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Office 365 using SAML authentication requires:

- Creating Users Stores in SAS, page 11
- Assigning an Authenticator in SAS, page 11
- Configuring SAS Auth Node and Encryption Key, page 12
- Enabling the Software Token Push OTP Setting, page 12
- Enabling the Allowed Targets Policy, page 15

Creating Users Stores in SAS

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that 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 additional 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 an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Office 365.

The following authenticators are supported:

- 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 Rules” in the SafeNet Authentication Service Subscriber Account Operator Guide to learn how to provision the different authentication methods to the users in the SAS user store.

Configuring SAS Auth Node and Encryption Key

In the event that 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 of “Configuring the Gemalto SafeNet SAS Agent for AD FS” on page 8.

4. Click Virtual Servers > COMMS > Auth Nodes.
5. Click the Auth Nodes link, and then click Add.
6. Complete the Auth Notes tab as follows:

<table>
<thead>
<tr>
<th>Auth Node Name</th>
<th>Enter a host description.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Name</td>
<td>Enter a resource name which will identify in a push notification which authentication node it relates to.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the low IP address.</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter the high IP address. (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>
Enabling the Software Token Push OTP Setting

1. Log in to the SAS console with an Operator account.
2. Click the **POLICY** tab, and then select **Token Policies**.

   ![Token Policies](image)

3. In the **Token Policies** module, click the **Software Token Push OTP Setting** link.

   ![Software Token Push OTP Setting](image)

4. Select **Enable Push OTP communication with MobilePass+**, and then click **Apply**.
Enabling the Allowed Targets Policy

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.

1. Log in to the SAS console with an Operator account.

2. Click the POLICY tab, and then select Token Policies.
3. In the **Token Policies** module, click the **Allow Targets Settings** link.

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application for this virtual server, and then click **Apply**.
Running the Solution

Connecting to Office 365

2. At the login prompt, enter your user name (including domain; for example, Bob@SafeNetdemos.com) and password, and then click Sign in.

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

3. You will be redirected to your organization’s login page. Enter your organizational user name and password, and then click Sign in.

After your credentials are authenticated by your organization’s AD FS, you are redirected to SAS to enter your one-time password (OTP).
4. Select **Use my mobile to autosend a passcode**, and then click **Submit**.

5. You will receive a push notification on the configured mobile device. Tap **Approve**.
6. Type the token PIN, and then tap **Continue** to send the approval with OTP to SAS.

A successful message is displayed on the configured mobile device.

![Message success](image)

After successful user authentication on SAS, you will be connected to the **Office 365 admin center**.

![Office 365 admin center](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
Connecting to Office 365’s SharePoint

1. To obtain your Office365 SharePoint URL, log in to the Office365 console as Administrator.

2. In the left pane, select Admin > SharePoint.

3. The Office 365 SharePoint URLs are listed. Using one of these URLs, open a new browser window and login.
4. At the login prompt, enter your user name (including domain; for example, Bob@SafeNetdemos.com) and password, and then click **Sign in**.

![Image](https://example.com/login.png)

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

5. You will be redirected to your organization's login page. Enter your organizational user name and password, and then click **Sign in**.

![Image](https://example.com/organization_login.png)

After your credentials are authenticated by your organization's AD FS, you are redirected to SAS to enter your one-time password (OTP).

6. Select **Use my mobile to autosend a passcode**, and then click **Submit**.

![Image](https://example.com/sas_login.png)
7. You will receive a push notification on the configured mobile device. Tap **Approve**.

8. Type the token PIN, and then tap **Continue** to send the approval with OTP to SAS.
A successful message is displayed on the configured mobile device.

After successful authentication on SAS, you will be connected to the **Office 365 SharePoint**.

*(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>Address</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>Phone</td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td></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>