SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for WordPress
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.

**Document Part Number:** 007-013606-001, Rev. A

**Release Date:** September 2016
## 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>SAML Authentication using SafeNet Authentication Service Cloud</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication Flow using SafeNet Authentication Service</td>
<td>6</td>
</tr>
<tr>
<td>SAML Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring WordPress</td>
<td>6</td>
</tr>
<tr>
<td>Installing and Activating the miniOrange SAML2.0 Plugin</td>
<td>7</td>
</tr>
<tr>
<td>Setting the WordPress Address (URL) as a Unique IP Address</td>
<td>10</td>
</tr>
<tr>
<td>Downloading the SafeNet Authentication Service Metadata</td>
<td>11</td>
</tr>
<tr>
<td>Configuring miniOrange SAML 2.0 Single Sign-On in WordPress</td>
<td>11</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>14</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SafeNet Authentication Service</td>
<td>14</td>
</tr>
<tr>
<td>Assigning an Authenticator in SafeNet Authentication Service</td>
<td>14</td>
</tr>
<tr>
<td>Adding WordPress as a Service Provider (SP) in SafeNet Authentication Service</td>
<td>15</td>
</tr>
<tr>
<td>Enabling SAML Services in SafeNet Authentication Service</td>
<td>19</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>23</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>27</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 WordPress.

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.

WordPress is an online, open source website creation tool. It is probably the easiest and most powerful blogging and website content management system (or CMS) in existence today. WordPress is largely associated with blogs as its main functionality is to allow easy blog experience.

This document describes how to:

- Configure SAML authentication in WordPress using SafeNet Authentication Service as an identity provider.

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

WordPress 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**
- **WordPress**—Version 4.5.3
- **miniOrange SAML 2.0 SSO plugin**—Premium version
Audience
This document is targeted to system administrators who are familiar with WordPress, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAML Authentication using SafeNet Authentication Service Cloud
SafeNet Authentication Service (SAS) Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.

SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE
In addition to the pure cloud-based offering, SafeNet Authentication Service (SAS) 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 the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.
SAML Authentication Flow using SafeNet Authentication Service

SafeNet Authentication Service (SAS) communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for WordPress.

1. A user attempts to log on to WordPress. The user is redirected to SafeNet Authentication Service (SAS). SAS collects and evaluates the user’s credentials.
2. SAS returns a response to WordPress, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service (SAS) to receive SAML authentication requests from WordPress, ensure that the end users can authenticate from the WordPress environment with a static password.

Configuring WordPress

Adding SafeNet Authentication Service (SAS) as an Identity Provider in WordPress requires:

- Installing and Activating the miniOrange SAML2.0 Plugin, page 7
- Setting the WordPress Address (URL) as a Unique IP Address, page 10
- Downloading the SafeNet Authentication Service Metadata, page 11
Installing and Activating the miniOrange SAML2.0 Plugin

1. In a web browser, open the following WordPress URL.
   https://<IP or FQDN>/wordpress/wp-admin

2. On the WordPress login window, enter the admin username and password (as configured during the installation), and then click Log In.

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

The WordPress administrator dashboard is displayed.

(The screen image above is from WordPress® software. Trademarks are the property of their respective owners.)
3. In the left pane, click **Plugins > Add New**.

![Plugins Add New](image1)

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

4. On the **Add Plugins** window, click **Upload Plugin**.

![Upload Plugin](image2)

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

5. Install a plugin. Click **Browse** to search and select the **miniOrange-saml-20-single-sign-on.zip** file.

![Browse Plugin](image3)

*(The screen image above is from WordPress® software. Trademarks are the property of their respective owners.)*
6. Click **Install Now** to start the plugin installation.

![Plugin installation screen](image)

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

7. A success message is displayed after the installation is complete. Click **Activate Plugin**.

![Plugin activation screen](image)

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

When activated, the **Plugin activated** message is displayed.

![Plugin activated screen](image)

*(The screen image above is from WordPress® software. Trademarks are the property of their respective owners.)*
## Setting the WordPress Address (URL) as a Unique IP Address

Configure WordPress so that SafeNet Authentication Service (SAS) is able to recognize the server on which WordPress is hosted.

1. On the WordPress administrator dashboard, in the left pane, click **Settings**.

   ![WordPress Settings](image)

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

2. On the General Settings window, in the **WordPress Address (URL)** field:
   a. Replace `localhost` with a unique IP or FQDN (of the machine) so that the SAM is able to recognize the server on which WordPress is hosted.

   ![WordPress General Settings](image)

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

3. Click **Save Changes**.
Downloading the SafeNet Authentication Service Metadata

Browse to the https://idp1.cryptocard.com/idp/shibboleth URL. The SafeNet Authentication Service (SAS) metadata will be downloaded automatically. Save the metadata locally on your machine.

Configuring miniOrange SAML 2.0 Single Sign-On in WordPress

1. On the WordPress administrator console, in the left pane, click miniOrange SAML 2.0 SSO, and then, in the right pane, on the SSO Login Settings tab, under Option 1: Use Default WordPress Login, ensure that the following are selected:
   - Check this option if you want to auto direct the user to IdP.
   - Checking this option creates a backdoor to login to your Website using WordPress credentials incase you get locked out of your IdP.

   **NOTE:** If you want to authenticate users through the administrator login console instead of the regular web page of WordPress, in the Relay State URL field, enter the administration console URL (for example, https://<WordPress server>/wordpress/wp-admin).

(The screen image above is from WordPress® software. Trademarks are the property of their respective owners.)
2. On the Identity Provider tab, select the Do not Use miniOrange Single Sign on service option.

![Identity Provider Tab](image1.png)

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

3. On the Service Provider tab, click Upload IDP Metadata to upload the SAS metadata.

![Service Provider Tab](image2.png)

(The screen image above is from WordPress® software. Trademarks are the property of their respective owners.)
4. Click **Browse** to search and select the SAS metadata you downloaded earlier in "Downloading the SafeNet Authentication Service Metadata" on page 11, and then click **Upload**.

5. The SAS details were added to WordPress miniOrange SAML 2.0 SSO plugin. The WordPress miniOrange SAML 2.0 SSO plugin is now configured with SAS as its Identity Provider.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with WordPress using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 14
- Assigning an Authenticator in SafeNet Authentication Service, page 14
- Adding WordPress as a Service Provider (SP) in SafeNet Authentication Service. page 15
- Enabling SAML Services in SafeNet Authentication Service, page 19

Synchronizing Users Stores to SafeNet Authentication Service

Before SafeNet Authentication Service (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 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 an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users authenticating through WordPress.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- 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 SAS user store.


**Adding WordPress as a Service Provider (SP) in SafeNet Authentication Service**

Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from WordPress. You will need the metadata of WordPress.

WordPress metadata is available at the administration console on the **MiniOrange SAML 2.0 SSO** menu, under the **Identity Provider** tab.

(The screen image above is from WordPress® software. Trademarks are the property of their respective owners.)
To add WordPress as a Service Provider in SafeNet Authentication Service:

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the COMMS tab, and then click SAML Service Providers.

3. In the SAML Service Providers module, click the SAML 2.0 Settings link.
4. Click **Add**.

5. Under **Add SAML 2.0 Settings**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly Name</strong></td>
<td>Enter the WordPress name.</td>
</tr>
<tr>
<td><strong>SAML 2.0 Metadata</strong></td>
<td>Select <strong>Upload Existing Metadata File</strong>. Click <strong>Choose File</strong>, select the Service Provider’s metadata file, and then click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

**NOTE:** The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer “Configure SAML Service” in the **SAML Configuration Guide**:

Under **Return Attributes**, add add the following attributes, and then click **Apply**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/CommonName">http://schemas.xmlsoap.org/claims/CommonName</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td>principal</td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>
WordPress is added as a service provider in the system.

### Enabling SAML Services in SafeNet Authentication Service

After WordPress has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules

### Using the SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML Service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.
2. Click the **ASSIGNMENT** tab, and then search for the required user.

![Search User](image1)

3. Click the appropriate user in the **User ID** column.

![Search User](image2)

4. Click **SAML Services**.

![Manager 1MC inc.](image3)

5. Click **Add**.

![SAML Services](image4)
6. Under **Add SAML Service**, do the following:
   a. From the **Service** menu, select the WordPress service provider.
   b. In **SAML Login ID** field, select the type of login ID (**User ID**, **E-mail**, or **Custom**) to be sent as a User ID to WordPress in the response.
   c. Click **Add**.

   The user can now authenticate to WordPress using SAML authentication.

### Using SAML Provisioning Rules

Use this module to enable groups of users to authenticate to SAML service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.
2. Click the **POLICY** tab, and then click **Automation Policies**.

3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.
5. Configure the following fields, and then click **Add**:

<table>
<thead>
<tr>
<th><strong>Rule Name</strong></th>
<th>Enter a name for the rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User is in container</strong></td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The <strong>Virtual Server groups</strong> box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the <strong>Used by rule</strong> box.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The <strong>Relying Parties</strong> box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to <strong>Rule Parties</strong> box.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>Select <strong>User ID</strong>. The <strong>User ID</strong> will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>

### Running the Solution

1. In a web browser, the following WordPress URL:
   
   https://<server name>/wordpress/wp-admin

2. You will be redirected to the SAS SAML login page. Enter your user name and then click **Login**.
SAS will trigger an on-the-go authentication request. You will then receive a push notification on the configured mobile device.

3. On the configured mobile device, tap **APPROVE** to approve the authentication request.
4. On the **TOKEN AUTHENTICATION** screen, enter the token PIN, and then tap **SUBMIT**.

A success message is displayed on mobile screen.
After successful user authentication, you will be logged in to WordPress.

(The screen image above is from WordPress® 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</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>