SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Drupal
# Contents

- Third-Party Software Acknowledgement ......................................................................................... 4
- Description ........................................................................................................................................ 4
- Applicability ..................................................................................................................................... 4
- Environment ...................................................................................................................................... 4
- Audience ........................................................................................................................................... 5
- SAML Authentication using SafeNet Authentication Service Cloud .................................................. 5
- SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE 5
- SAML Authentication Flow using SafeNet Authentication Service ..................................................... 6
- SAML Prerequisites ............................................................................................................................ 6
- Configuring Drupal .............................................................................................................................. 6
  - Downloading the SAS Metadata ......................................................................................................... 6
  - Installing SimpleSAMLphp .................................................................................................................. 6
  - Configuring SimpleSAMLphp as a Service Provider .......................................................................... 8
  - Configuring Drupal for SAML Authentication ................................................................................. 10
- Configuring SafeNet Authentication Service ....................................................................................... 14
  - Synchronizing Users Stores to SafeNet Authentication Service ...................................................... 14
  - Assigning an Authenticator in SafeNet Authentication Service ....................................................... 14
  - Adding Drupal as a Service Provider (SP) in SafeNet Authentication Service .................................. 15
  - Enabling SAML Services in SafeNet Authentication Service ............................................................... 18
- Running the Solution ............................................................................................................................ 25
- Support Contacts ................................................................................................................................. 27
Third-Party Software Acknowledgement

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

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.

Drupal is a free and open-source content management framework written in PHP, and distributed under the GNU General Public License. It is used as a backend framework for web sites worldwide, ranging from personal blogs to corporate, political, and government sites.

This document describes how to:

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

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

Drupal 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 – Private Cloud Edition (SAS-PCE)** — SafeNet’s cloud-based authentication service
- **Drupal**—Version 7.3
- **SimpleSAMLphp**—Version 1.13.2
• Simplesamlphp_auth module—Version 7.x-2.0
• CentOS—Version 6.6 x86_64
• MySQL—Version 5.5.43

Audience

This document is targeted to system administrators who are familiar with Drupal, 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 Drupal.

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

**SAML Prerequisites**

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

**Configuring Drupal**

To add SafeNet Authentication Service (SAS) as an Identity Provider in Drupal:

- Downloading the SAS Metadata, page 6
- Installing SimpleSAMLphp, page 6
- Configuring SimpleSAMLphp as a Service Provider, page 8
- Configuring Drupal for SAML Authentication, page 10

**Downloading the SAS Metadata**

1. Browse to the https://idp1.cryptocard.com/idp/shibboleth URL.
2. The SAS metadata will automatically download. Save it locally on your machine.

**Installing SimpleSAMLphp**

In this section, we will install SimpleSAMLphp. SimpleSAMLphp is an application written in PHP which can be used to provide SAML authentication. Drupal cannot act as a SAML service provider—SimpleSAMLphp acts as a SAML service provider on its behalf.
2. Extract the package in the /var directory, and then rename it to simplesamlphp.
3. Open the httpd.conf file in the /etc/httpd/conf directory, add the following section at the end of the file, and then save the file.

```html
<VirtualHost *:80>
    ServerName <IP/FQDN of server>
    DocumentRoot /var/www/html/
    Alias /simplesaml /var/simplesamlphp/www
    <Directory /var/simplesamlphp/www>
        Order allow,deny
        Allow from all
    </Directory>
</VirtualHost>
```

**NOTE:** Edit the DocumentRoot accordingly, if needed.

4. If SELinux is running on the server, use the following command to change the security context of SimpleSAMLphp:

```
chcon -Rt httpd_sys_content_t /var/simplesamlphp/
```

5. Log into MySQL, and create a database. A database can be created using the following command:

```
CREATE DATABASE <Database name>;
```

6. Open the config.php file, located in the /var/simplesamlphp/config directory, edit the following sections, and then save the file.

| Base URL | Enter the base URL of simplesamlphp. For example: 'baseuripath' => 'http://<IP/FQDN of server/simplesaml/', |
| Admin Password | Set an administrator password. This is required to access some of the pages in your simpleSAMLphp installation web interface. For example: 'auth.adminpassword' => 'setnewpasswordhere', |
| Secret Salt | Set a secret salt. This should be a random string. Some parts of the simpleSAMLphp require this salt to generate cryptographically secure hashes. For example, the following command can help you to generate a random string: `tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' /dev/urandom | dd bs=32 count=1 2>/dev/null;echo 'secretsalt' => 'randombytesinsertedhere', |
| Datastore | Change the SimpleSAMLphp session datastore from phpsession to mysql. For example: 'store.type' => 'sql', 'store.sql.dsn' => 'mysql:host=<Hostname/IP Address of MySQL server>;dbname=<Database name>', 'store.sql.username' => '<MySQL username>', 'store.sql.password' => '<User Password>',' |
7. Restart the apache server using the following command:

   service httpd restart

8. Open a web browser and browse to the simplesamlphp URL (for example, http://<IP/FQDN of server>/simplesaml). If simplesamlphp is successfully installed, you will see a page similar to the one shown below.

   ![SimpleSAMLphp installation page](image)

   (The screen image above is from UNINETT™. Trademarks are the property of their respective owners.)

### Configuring SimpleSAMLphp as a Service Provider

1. Open the `authsources.php` file located in the `/var/simplesamlphp/config` directory. Edit the following sections, and then save the file.

<table>
<thead>
<tr>
<th>Entity ID</th>
<th>Enter an entity ID for SimpleSAMLphp. For example: 'entityID' =&gt; 'Your entity ID',</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDP</td>
<td>Set the default IDP as SAS, by setting its value as SAS’ entity ID. The SAS entity ID can be found in its metadata. For example: 'idp' =&gt; 'SAS’s entity ID',</td>
</tr>
<tr>
<td>NameID Policy</td>
<td>Add this line after the 'idp' field: 'NameIDPolicy' =&gt; 'urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress',</td>
</tr>
</tbody>
</table>
2. Browse to the http://<IP/FQDN of server>/simplesaml/admin/metadata-converter.php URL.

3. Under XML metadata, paste the SAS metadata, and then click Parse. (If you have not already downloaded the SAS metadata, please refer to “Downloading the SAS Metadata” on page 6 for details.)

4. Copy the converted metadata to saml20-idp-remote, and then save the file locally.
5. Open the **saml20-idp-remote.php** file in the `/var/simplesamlphp/metadata` directory, paste the converted metadata into the file, as shown in the following example:

```php
/*
 * SAML 2.0 remote SP metadata for simplesamlphp.
 * Remember to remove the IDs you don't use from this file.
 */

/* guest SP. Allows users to sign up and register. Great for testing! */
<metadata xmlns="https:// fedids.org/p10982-x2007-04#spmeta" id="https://idp.example.com/idp/metadata">  
  <service entityID="https://idp.example.com/idp/metadata" xmlns="http://www.saml2.org/onum">  
    <nameID format="urn:oasis:names:tc:SAML:2.0:cm:entity:IDP">  
      <authority url="https://idp.example.com/idp/metadata"/>
    </nameID>
    <assertionConsumerService url="https://idp.example.com/idp/metadata"/>
    <singleLogoutService url="https://idp.example.com/idp/metadata"/>
    < logoutURL url="https://idp.example.com/idp/metadata"/>
    < assertionSigner>
    
```  

(The screen image above is from UNINETT™. Trademarks are the property of their respective owners.)

### Configuring Drupal for SAML Authentication

6. Download the **simplesamlphp_auth** module from the Drupal website. This module is used to integrate Drupal with the SimpleSAMLphp service provider.

7. Extract the package and move it to the Drupal **modules** directory (`../Drupal/modules`).

8. Open a web browser, browse to the Drupal account, and then login as a user with admin privileges.

(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)
9. In the navigation menu, click **Modules**.

![Modules](image1.png)

(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)

10. In the **OTHER** modules list at the bottom of the page, locate the **simpleSAMLphp authentication** module. Select the checkbox to enable the module, and then click **Save configuration**.

![Other Modules](image2.png)

(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)
11. In the navigation menu, click **Configuration**.

12. Under the **PEOPLE** section, click **SimpleSAMLphp Auth Settings**.

(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)
13. Complete the following details, and then click **Save Configuration**.

### BASIC SETUP

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate authentication via SimpleSAMLphp</td>
<td>Select this option to enable SAML authentication.</td>
</tr>
<tr>
<td>Installation directory</td>
<td>Change the directory if simplesamlphp is installed somewhere other than the default location.</td>
</tr>
</tbody>
</table>

### USER INFO AND SYNCING

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which attribute from simpleSAMLphp should be used as user’s name</td>
<td>Specify: <a href="http://schemas.xmlsoap.org/claims/CommonName">http://schemas.xmlsoap.org/claims/CommonName</a></td>
</tr>
<tr>
<td>Which attribute from simpleSAMLphp should be used as unique identifier for the user</td>
<td>Specify: <a href="http://schemas.microsoft.com/ws/2008/06/identity/claims/uid">http://schemas.microsoft.com/ws/2008/06/identity/claims/uid</a></td>
</tr>
<tr>
<td>Which attribute from simpleSAMLphp should be used as user mail address</td>
<td>Specify: <a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a></td>
</tr>
</tbody>
</table>

### USER PROVISIONING

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register Users</td>
<td>Select this option to enable Just-in-Time (JIT) provisioning.</td>
</tr>
</tbody>
</table>

### DRUPAL AUTHENTICATION

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow SAML users to set Drupal passwords</td>
<td>Select accordingly.</td>
</tr>
<tr>
<td>Allow authentication with local Drupal accounts</td>
<td>Select this option if you do not want to enforce SAML authentication.</td>
</tr>
</tbody>
</table>
Configuring SafeNet Authentication Service

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

- Synchronizing Users Stores to SafeNet Authentication Service, page 14
- Assigning an Authenticator in SafeNet Authentication Service, page 14
- Adding Drupal as a Service Provider (SP) in SafeNet Authentication Service, page 15
- Enabling SAML Services in SafeNet Authentication Service, page 18

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 Drupal.

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 Drupal 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 Drupal. You will need the Issuer ID and assertion consumer URL location of Drupal.

**To add Drupal 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**.

![COMMS tab](image)

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

![SAML Service Providers](image)

4. Click **Add**.

![Add button](image)
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>Friendly Name</td>
<td>Enter the Drupal name.</td>
</tr>
<tr>
<td>SAML 2.0 Metadata</td>
<td>Select <strong>Create New Metadata File</strong>.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>Enter the service provider EntityID as entered in step 1 in “Configuring SimpleSAMLphp as a Service Provider” on page 8.</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the Assertion Consumer URL. For example: <code>http://&lt;IP/FQDN of simpleSAMLphp server&gt;/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp</code></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**: [http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf](http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf)

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name</code></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</code></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>
http://schemas.xmlsoap.org/claims/EmailAddress  According to ThirdParty Product Requirements

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name  According to ThirdParty Product Requirements

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname  According to ThirdParty Product Requirements

http://schemas.xmlsoap.org/claims/CommonName  According to ThirdParty Product Requirements

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier  According to ThirdParty Product Requirements

principal  According to ThirdParty Product Requirements

Drupal is added as a service provider in the system.

Enabling SAML Services in SafeNet Authentication Service

After Drupal 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.

3. Click the appropriate user in the User ID column.
4. Click SAML Services.

5. Click Add.

6. Under Add SAML Service, do the following:
   a. From the Service menu, select the Drupal 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 UserID to Drupal in the response.
   c. Click Add.
The user can now authenticate to Drupal 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>Rule Name</th>
<th>Enter a name for the rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is in container</td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td>Groups</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>Parties</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>SAML Login ID</td>
<td>Select <strong>User ID</strong>. The User ID will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>
Running the Solution

Check the configured solution after successfully installing the SimpleSAMLphp and configuring the Drupal for SAML Authentication.

In the following solution, the user is enrolled with a GrIDsure token.

1. Open the web browser and enter the Drupal URL.

2. Click **Federated Log In**. The user will be redirected to the SAS **Login** page.

3. In the **User Name** field, enter the username, and then click **Login**.
4. The challenge grid is displayed. In the **Password** field, enter the characters from the grid that correspond to your PIP (personal identification pattern).

5. Click **Login**. If the credentials are valid, the user will be logged into the Drupal account.

(The screen image above is from Drupal™. 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. 4690 Millennium Drive Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>