

# SafeNet Authentication Service Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Drupal

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:** 007-013207-001, Rev. B

**Release Date:** June 2016

# 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-PCE5 .....	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:

- Deploy multi-factor authentication (MFA) options in Drupal using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- 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

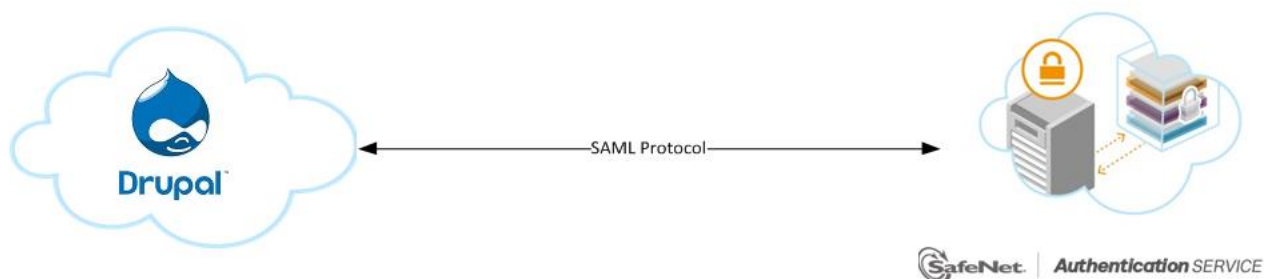
---

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.

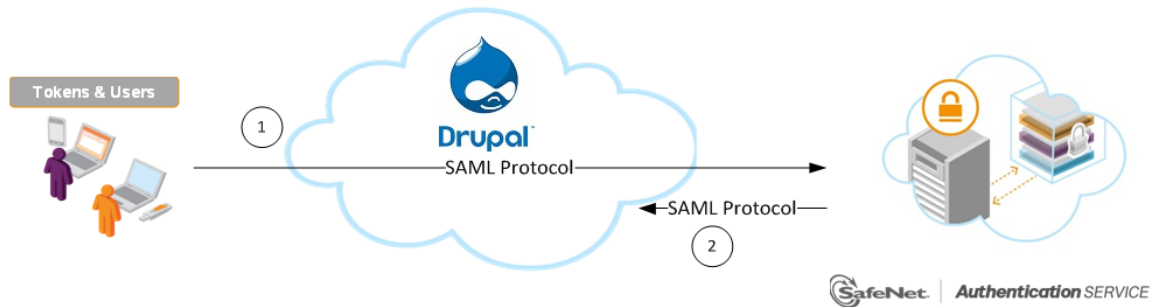
For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

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
- 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.

1. Download the SimpleSAMLphp service provider from their website—<https://simplesamlphp.org>.
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.

```
<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>
```

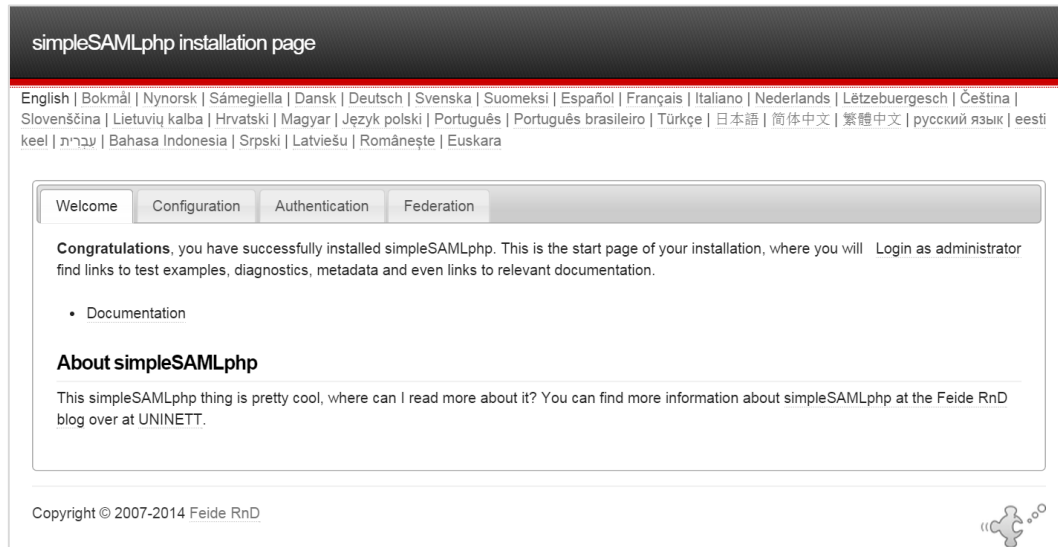


**NOTE:** Edit the **DocumentRoot** accordingly, if needed.

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.

<b>Base URL</b>	Enter the base URL of simplesamlphp. For example: <b>'baseurlpath' =&gt; 'http://&lt;IP/FQDN of server/simplesaml/'</b> ,
<b>Admin Password</b>	Set an administrator password. This is required to access some of the pages in your simpleSAMLphp installation web interface. For example: <b>'auth.adminpassword' =&gt; 'setnewpasswordhere'</b> ,
<b>Secret Salt</b>	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: <b>tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' &lt;/dev/urandom   dd bs=32 count=1 2&gt;/dev/null;echo</b> <b>'secretsalt' =&gt; 'randombytesinsertedhere'</b> ,
<b>Datastore</b>	Change the SimpleSAMLphp session datastore from phpsession to mysql. For example: <b>'store.type' =&gt; 'sql'</b> , <b>'store.sql.dsn' =&gt; 'mysql:host=&lt;Hostname/IP Address of MySQL server&gt;;dbname=&lt;Database name&gt;'</b> , <b>'store.sql.username' =&gt; '&lt;MySQL username&gt;'</b> , <b>'store.sql.password' =&gt; '&lt;User Password&gt;'</b> ,

- Restart the apache server using the following command:  
**service httpd restart**
- 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.



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

## Configuring SimpleSAMLphp as a Service Provider

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

<b>Entity ID</b>	Enter an entity ID for SimpleSAMLphp. For example: <b>'entityID' =&gt; 'Your entity ID',</b>
<b>IDP</b>	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: <b>'idp' =&gt; 'SAS's entity ID',</b>
<b>NameID Policy</b>	Add this line after the 'idp' field: <b>'NameIDPolicy' =&gt; 'urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress',</b>

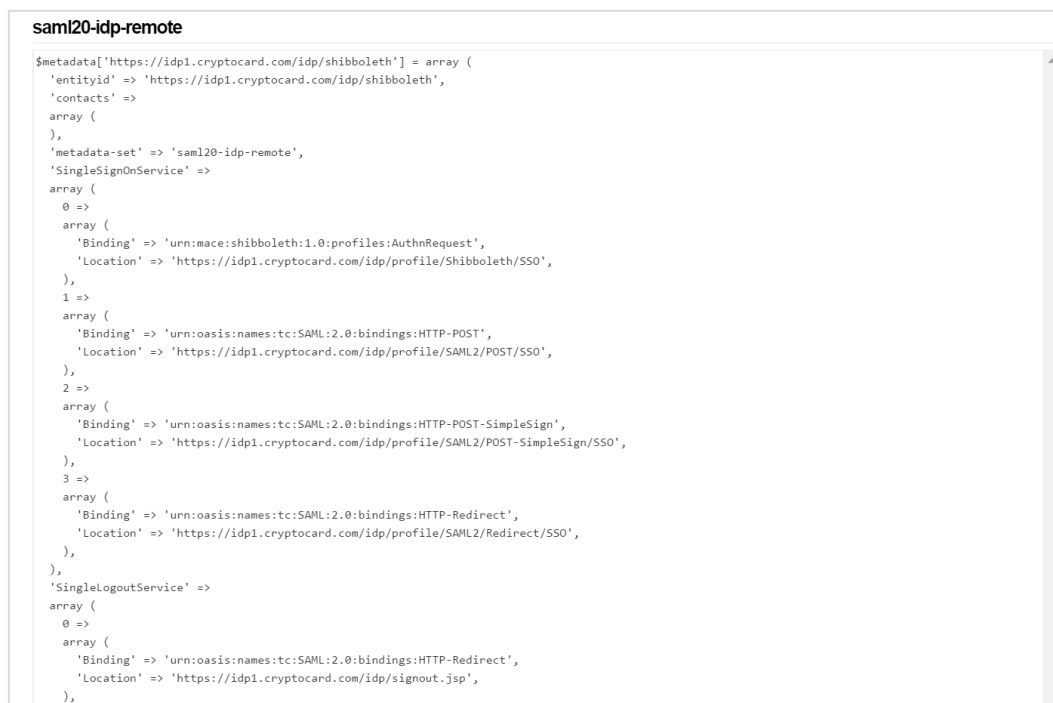


2. Browse to the **http://<IP/FQDN of server>/simplesaml/admin/metadata-converter.php** URL.



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

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.



```
$metadata["https://idp1.cryptocard.com/idp/shibboleth"] = array (
  'entityid' => 'https://idp1.cryptocard.com/idp/shibboleth',
  'contacts' =>
  array (
  ),
  'metadata-set' => 'saml20-idp-remote',
  'SingleSignOnService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:mace:shibboleth:1.0:profiles:AuthnRequest',
      'Location' => 'https://idp1.cryptocard.com/idp/profile/Shibboleth/SSO',
    ),
    1 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
      'Location' => 'https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO',
    ),
    2 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign',
      'Location' => 'https://idp1.cryptocard.com/idp/profile/SAML2/POST-SimpleSign/SSO',
    ),
    3 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO',
    ),
  ),
  'SingleLogoutService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'https://idp1.cryptocard.com/idp/signout.jsp',
    ),
  ),
)
```

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

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 IdP metadata for simpleSAMLphp.
 *
 * Remember to remove the IdPs you don't use from this file.
 *
 * See: https://simplesamlphp.org/docs/stable/simplesamlphp-reference-idp-remote
 */

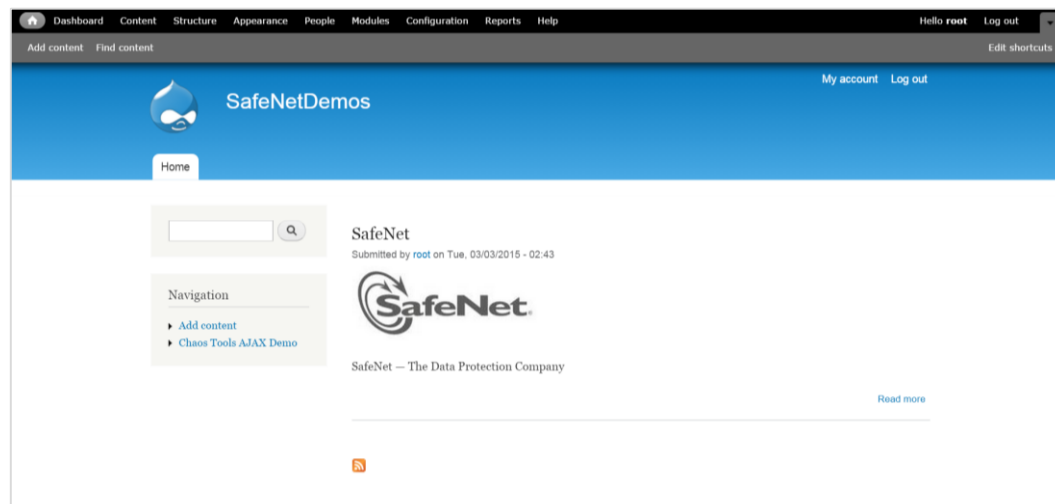
/**
 * Guest IdP. allows users to sign up and register. Great for testing!
 */
$metadata['https://idpl.cryptocard.com/idp/shibboleth'] = array (
    'entityid' => 'https://idpl.cryptocard.com/idp/shibboleth',
    'contacts' =>
        array (
        ),
    'metadata-set' => 'saml20-idp-remote',
    'SingleSignOnService' =>
        array (
            0 =>
                array (
                    'Binding' => 'urn:mace:shibboleth:1.0:profiles:AuthnRequest',
                    'Location' => 'https://idpl.cryptocard.com/idp/profile/Shibboleth/SSO',
                ),
            1 =>
                array (
                    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
                    'Location' => 'https://idpl.cryptocard.com/idp/profile/SAML2/POST/SSO',
                ),
            2 =>
                array (
                    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign',
                    'Location' => 'https://idpl.cryptocard.com/idp/profile/SAML2/POST-SimpleSign/SSO',
                ),
            3 =>
                array (
                    'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
                    'Location' => 'https://idpl.cryptocard.com/idp/profile/SAML2/Redirect/SSO',
                ),
        ),
    'SingleLogoutService' =>
        array (
            0 =>
                array (

```

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

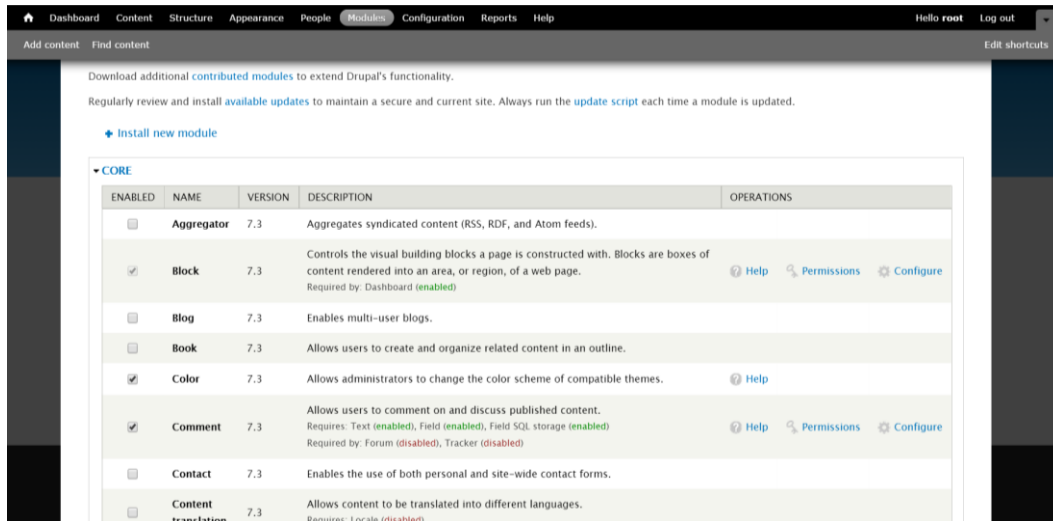
## Configuring Drupal for SAML Authentication

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.



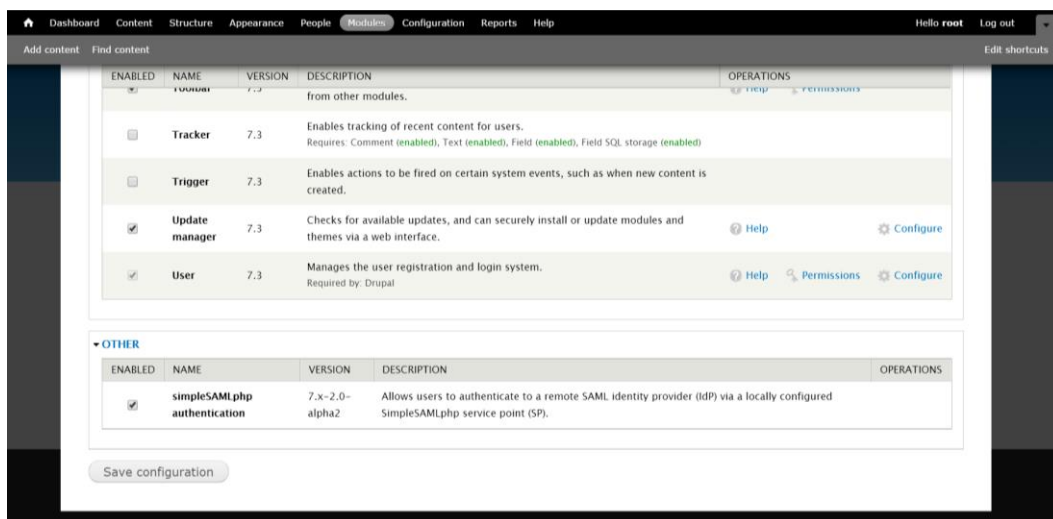
(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)

9. In the navigation menu, click **Modules**.



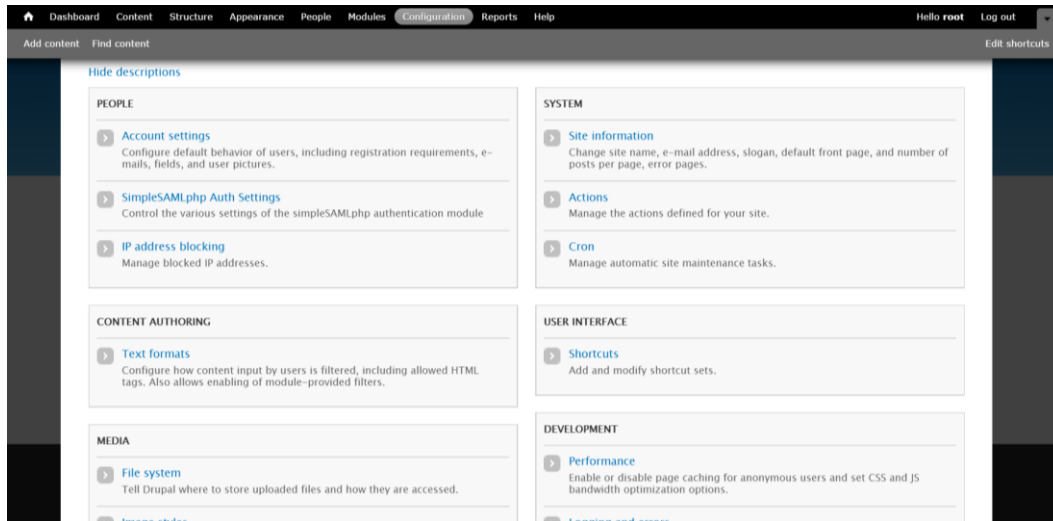
(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)

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**.



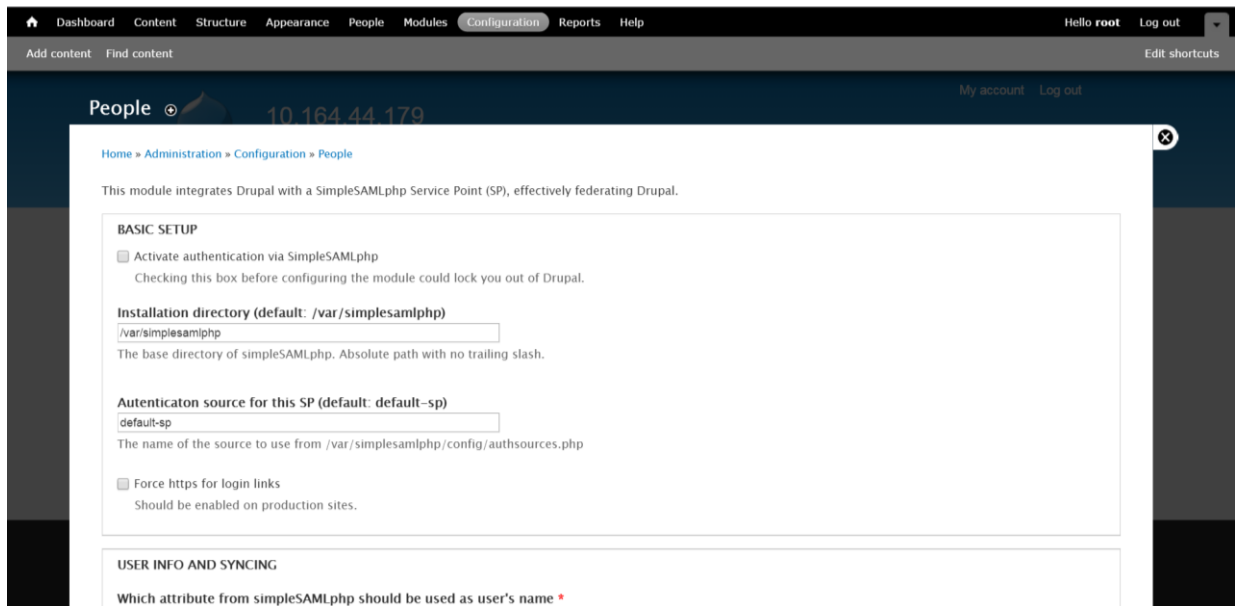
(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)

11. In the navigation menu, click **Configuration**.



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

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**.

<b>BASIC SETUP</b>	
<b>Activate authentication via SimpleSAMLphp</b>	Select this option to enable SAML authentication.
<b>Installation directory</b>	Change the directory if simplesamlphp is installed somewhere other than the default location.
<b>USER INFO AND SYNCING</b>	
<b>Which attribute from simpleSAMLphp should be used as user's name</b>	Specify: http://schemas.xmlsoap.org/claims/CommonName
<b>Which attribute from simpleSAMLphp should be used as unique identifier for the user</b>	Specify: http://schemas.microsoft.com/ws/2008/06/identity/claims/uid
<b>Which attribute from simpleSAMLphp should be used as user mail address</b>	Specify: http://schemas.xmlsoap.org/claims/EmailAddress
<b>USER PROVISIONING</b>	
<b>Register Users</b>	Select this option to enable Just-in-Time (JIT) provisioning.
<b>DRUPAL AUTHENTICATION</b>	
<b>Allow SAML users to set Drupal passwords</b>	Select accordingly.
<b>Allow authentication with local Drupal accounts</b>	Select this option if you do not want to enforce SAML authentication.

# 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*:

[http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet\\_Authentication\\_Service/Safenet\\_Authentication\\_Service\\_\\_Subscriber\\_Account\\_Operator\\_Guide/](http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/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.

[http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet\\_Authentication\\_Service/Safenet\\_Authentication\\_Service\\_\\_Subscriber\\_Account\\_Operator\\_Guide/](http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/)

## 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.

Shortcuts Manage: IMC Inc.

Create User

SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS

Authentication Activity

Authentication Metrics

Token States

SMS Credits

Allocation

Transaction Log

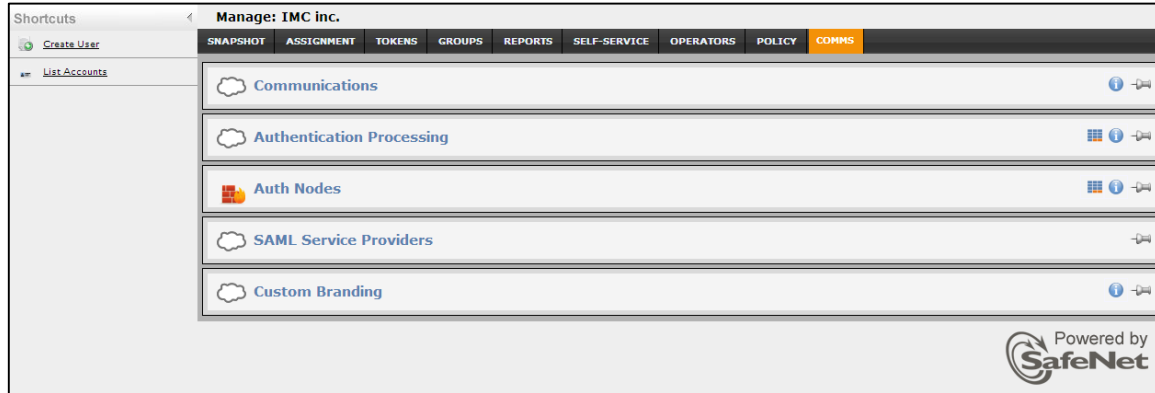
Service Start: 2013-07-17 Service Stop: 2016-02-05

Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

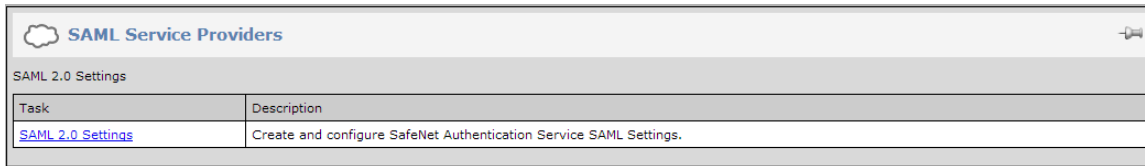
References

Powered by SafeNet

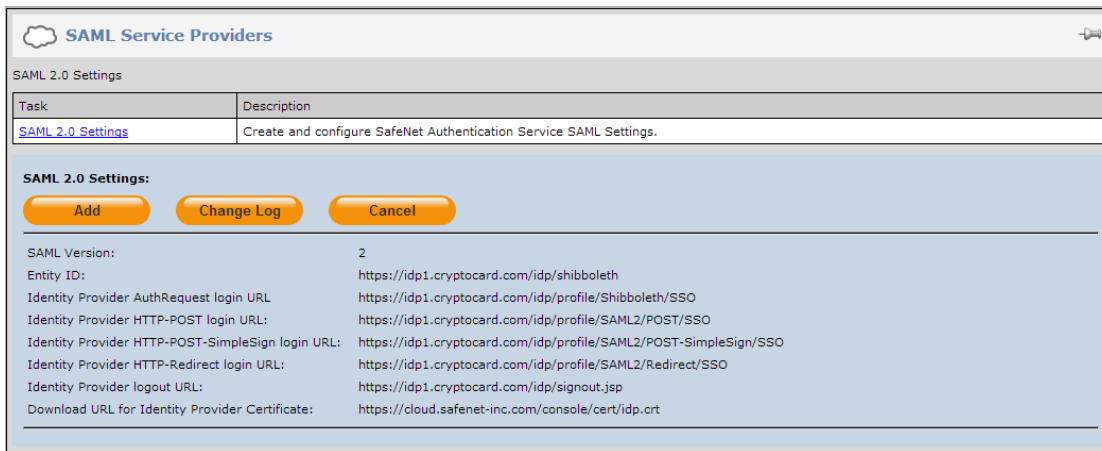
- Click the **COMMS** tab, and then click **SAML Service Providers**.



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



- Click **Add**.





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

<b>Friendly Name</b>	Enter the Drupal name.
<b>SAML 2.0 Metadata</b>	Select <b>Create New Metadata File</b> .
<b>Entity ID</b>	Enter the service provider EntityID as entered in step 1 in “  Configuring SimpleSAMLphp as a Service Provider” on page 8.
<b>Location</b>	Enter the Assertion Consumer URL. For example: <b>http://&lt;IP/FQDN of simpleSAMLphp server&gt;/simplesaml/module.php/saml/sp/saml2-acis.php/default-sp</b>



**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>

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

<b>Name</b>	<b>Value</b>
http://schemas.microsoft.com/ws/2008/06/identity/claims/uid	According to ThirdParty Product Requirements
http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name	According to ThirdParty Product Requirements
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	According to ThirdParty Product Requirements

<a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a>	According to ThirdParty Product Requirements
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	According to ThirdParty Product Requirements
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>	According to ThirdParty Product Requirements
<a href="http://schemas.xmlsoap.org/claims/CommonName">http://schemas.xmlsoap.org/claims/CommonName</a>	According to ThirdParty Product Requirements
<a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a>	According to ThirdParty Product Requirements
principal	According to ThirdParty Product Requirements

**Return Attributes**

Name	Value
X <a href="http://schemas.microsoft.com/ws/2006/06/identity/claims/uid">http://schemas.microsoft.com/ws/2006/06/identity/claims/uid</a>	UID
X <a href="http://schemas.microsoft.com/ws/2006/06/identity/claims/windowsaccountname">http://schemas.microsoft.com/ws/2006/06/identity/claims/windowsaccountname</a>	SAML Login ID
X <a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a>	Email address
X <a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a>	Email address
X <a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a>	Name
X <a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a>	Given name
X <a href="http://schemas.xmlsoap.org/claims/CommonName">http://schemas.xmlsoap.org/claims/CommonName</a>	Name
X <a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a>	Name
X <a href="#">principal</a>	Custom... <input type="text" value="principal"/>

[Add attribute](#)

Drupal is added as a service provider in the system.

**SAML 2.0 Settings:**

---

SAML Version: 2  
 Entity ID: <https://idp1.cryptocard.com/idp/shibboleth>  
 Identity Provider AuthRequest login URL: <https://idp1.cryptocard.com/idp/profile/Shibboleth/SSO>  
 Identity Provider HTTP-POST login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO>  
 Identity Provider HTTP-POST-SimpleSign login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/POST-SimpleSign/SSO>  
 Identity Provider HTTP-Redirect login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO>  
 Identity Provider logout URL: <https://idp1.cryptocard.com/idp/signout.jsp>  
 Download URL for Identity Provider Certificate: <https://cloud.safenet-inc.com/console/cert/idp.crt>

Service Provider	Entity ID	Edit	Remove	Resync
<a href="#">Drupal</a>	<a href="#">Drupal</a>			

## 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.

Shortcuts **Manage: IMC inc.**

Create User

SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS

Authentication Activity

Authentication Metrics

Token States

SMS Credits

Allocation

Transaction Log

Service Start: 2013-07-17 Service Stop: 2016-02-05

Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

References

Powered by SafeNet

2. Click the **ASSIGNMENT** tab, and then search for the required user.

Search User

Search User:

User ID:  Auth Method:  Container:

Last Name:  E-mail:  Account State:

Search Clear

Provision Delete Account Unlock

No Records

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

Search User

Search User:

User ID:  Auth Method:  Container:

Last Name:  E-mail:  Account State:

Search Clear

Provision Delete Account Unlock

User ID	Last Name	First Name	Account Owner	Auth Method	RADIUS Attr	Auth State	Account State	Container
<a href="#">BobH</a>	Hansen	Bob						Default

Displaying: 1 to 1 of 1

4. Click **SAML Services**.

Manage: IMC inc.

SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS

User Detail : BobH

Edit Delete Change Log Return

First Name: Bob Address: Phone: Alias #1:  
Last Name: Hansen Extension: Alias #2:  
User ID: BobH City: Emergency:  
E-mail: Bob@safenet-inc.com State: Account Owner:  
Mobile/SMS: Country: Custom #2:  
Container: Default Postal/Zip: Custom #3:

Tokens

Authentication Metrics

Authentication Activity

Access Restrictions

Group Membership

RADIUS Attributes (user)

SAML Services

5. Click **Add**.

SAML Services

Add Change Log

6. Under **Add SAML Service**, do the following:

- From the **Service** menu, select the Drupal service provider.
- 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.
- Click **Add**.

SAML Services

Add Change Log

Add SAML Service

Add Cancel

Service: Drupal

SAML Login ID: ☒ User ID ☐ Email ☐ Custom

The user can now authenticate to Drupal using SAML authentication.

SAML Services					
<a href="#">Add</a> <a href="#">Change Log</a>					
Index	SAML Service	User ID	Status		
1	Drupal	Bob	Active	<a href="#">Edit</a>	<a href="#">Remove</a>

## 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.

Shortcuts

Create User

Manage: IMC inc.

SNAPSHOT

ASSIGNMENT

TOKENS

GROUPS

REPORTS

SELF-SERVICE

OPERATORS

POLICY

COMMS

Authentication Activity

Authentication Metrics

Token States

SMS Credits

Allocation

Transaction Log

Service Start:

2013-07-17

Service Stop:

2016-02-05

Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

References

Powered by

SafeNet

2. Click the **POLICY** tab, and then click **Automation Policies**.

Manage: IMC inc.

SNAPSHOT

ASSIGNMENT

TOKENS

GROUPS

REPORTS

SELF-SERVICE

OPERATORS

POLICY

COMMS

User Policies

Token Policies

Role Management

Automation Policies

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

Manage: IMC inc.

SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS **POLICY** COMMS

User Policies

Token Policies

Role Management

Automation Policies

Use these policies to set rules for provisioning tokens, set a URL and options for self-enrollment.

Task	Description
<a href="#">Time Zone Offset</a>	Set the number of hours relative to UTC to be applied to reports
<a href="#">Provisioning Rules</a>	Create and edit provisioning rules.
<a href="#">Self-enrollment Policy</a>	Set the URL and options for self-enrollment.
<a href="#">SAML Provisioning Rules</a>	User account SAML creation.
<a href="#">Role Provisioning Rules</a>	Create and edit role provisioning rules.
<a href="#">Auto Remove</a>	Configure automatic removal of old reports

- Click **New Rule**.

Automation Policies

Use these policies to set rules for provisioning tokens, set a URL and options for self-enrollment.

Task	Description
<a href="#">Time Zone Offset</a>	Set the number of hours relative to UTC to be applied to reports
<a href="#">Provisioning Rules</a>	Create and edit provisioning rules.
<a href="#">Self-enrollment Policy</a>	Set the URL and options for self-enrollment.
<a href="#">SAML Provisioning Rules</a>	User account SAML creation.
<a href="#">Role Provisioning Rules</a>	Create and edit role provisioning rules.
<a href="#">Auto Remove</a>	Configure automatic removal of old reports

**SAML Provisioning Rules**

New Rule Change Log Cancel

No SAML Provisioning Rules

- Configure the following fields, and then click **Add**:

<b>Rule Name</b>	Enter a name for the rule.
<b>User is in container</b>	Users affected by this rule must be in the selected container.
<b>Groups</b>	The <b>Virtual Server groups</b> 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 <b>Used by rule</b> box.
<b>Parties</b>	The <b>Relying Parties</b> 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 <b>Rule Parties</b> box.
<b>SAML Login ID</b>	Select <b>User ID</b> . The User ID will be returned to the service provider in the SAML assertion.

SAML Provisioning Rules

New Rule

Change Log

Cancel

No SAML Provisioning Rules

Add SAML Auto-create Rule

Add

Cancel

Rule Name:

User is in container:

Default

Groups Filter:

Search

Virtual Server groups:

Used by rule:

Groups:

Users

Parties:

Relying Parties

Rule Parties

SAML Login ID:

User ID

Email

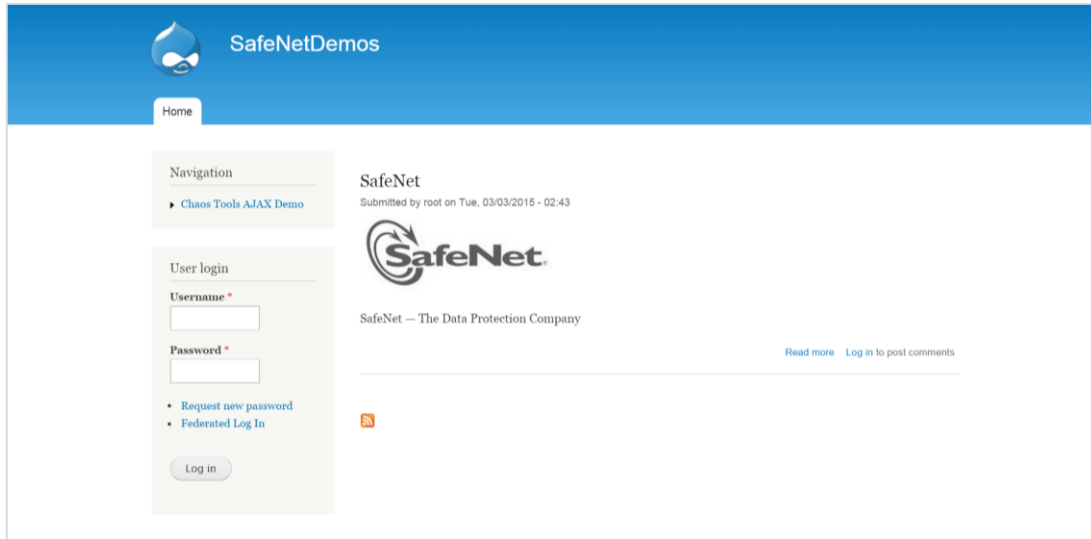


# Running the Solution

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

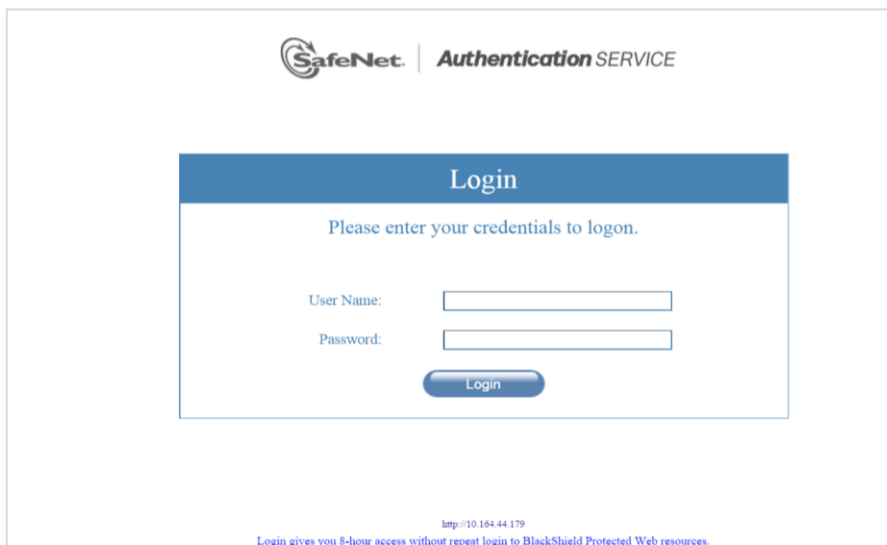
In the following solution, the user is enrolled with a GrIDSure token.

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




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

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**.



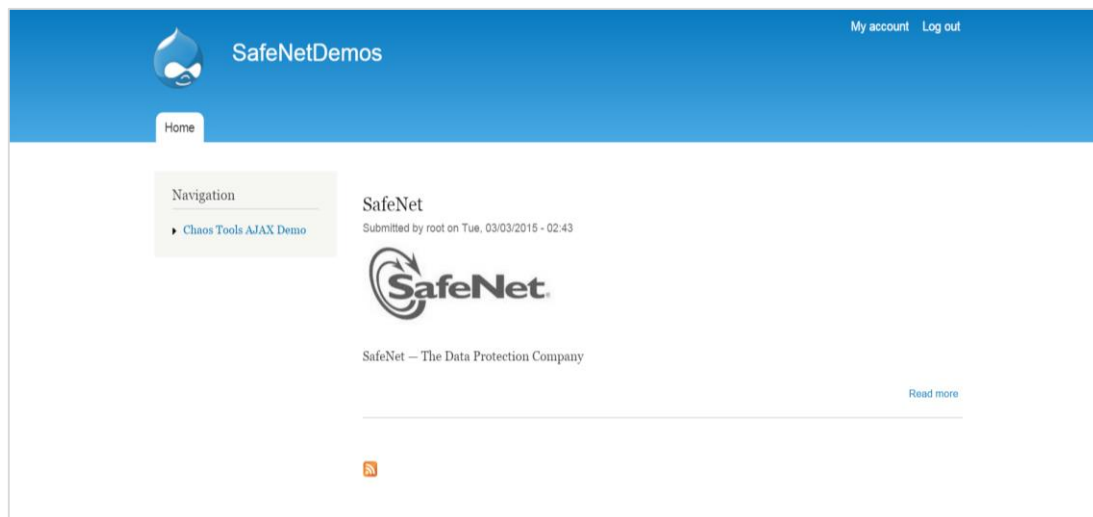
4. The challenge grid is displayed. In the **Password** field, enter the characters from the grid that correspond to your PIP (personal identification pattern).



The image shows the SafeNet Authentication SERVICE Login page. At the top, the SafeNet logo and "Authentication SERVICE" are displayed. Below this is a blue header with the word "Login". Under the header, the text "Please enter your credentials to login." is shown. In the center, there is a 5x5 grid of numbers. Below the grid is a "Password:" label followed by a text input field. At the bottom of the form is a blue "Login" button.

8	9	3	2	9
7	6	1	4	8
1	8	7	0	1
0	5	7	5	4
2	2	5	3	6

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.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	<a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a> 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.	