

SafeNet Authentication Manager Integration Guide

Using SAM 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: 007-013272-001, Rev. A

Release Date: September 2015

Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	4
Environment	4
Audience	5
SAML Authentication using SAM	5
Authentication Flow using SAM	5
SAML Prerequisites	5
Configuring SafeNet Authentication Manager	6
Synchronizing User Stores to SAM	6
Assigning a Token in SAM	6
Configuring SAM as an Identity Provider	7
Downloading the SAM's Metadata	9
Adding Drupal as a Service Provider in the Token Policy Object	10
Configuring Drupal	13
Installing the SimpleSAMLphp Application	13
Configuring SimpleSAMLphp as a Service Provider	15
Configuring Drupal	17
Running the Solution	20
Support Contacts	22

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto 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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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 back-end framework for websites 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 tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in Drupal using SafeNet Authentication Manager 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 Manager.

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 Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM 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:

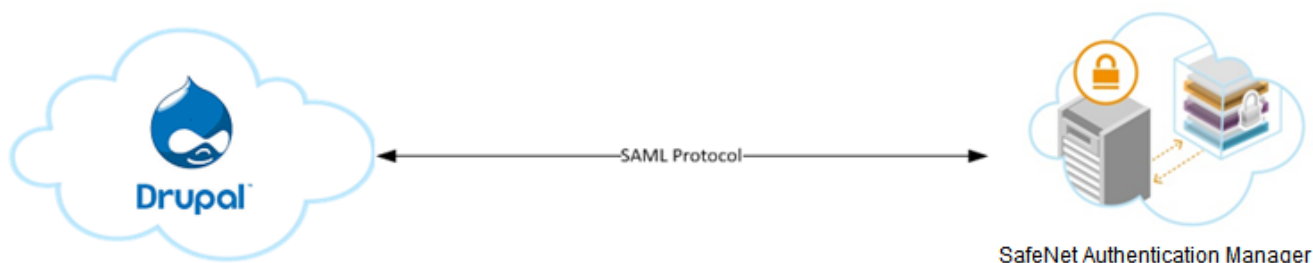
- **SafeNet Authentication Manager Version**—Version 8.2 (HF 679)
- **Drupal 7.3**
- **SimpleSAMLphp 1.13.2**
- **SimpleSamlphp_auth module 7.x-2.0-alpha2**
- **CentOS 6.6 x86_64**
- **MySQL 5.5.43**

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 Manager.

SAML Authentication using SAM

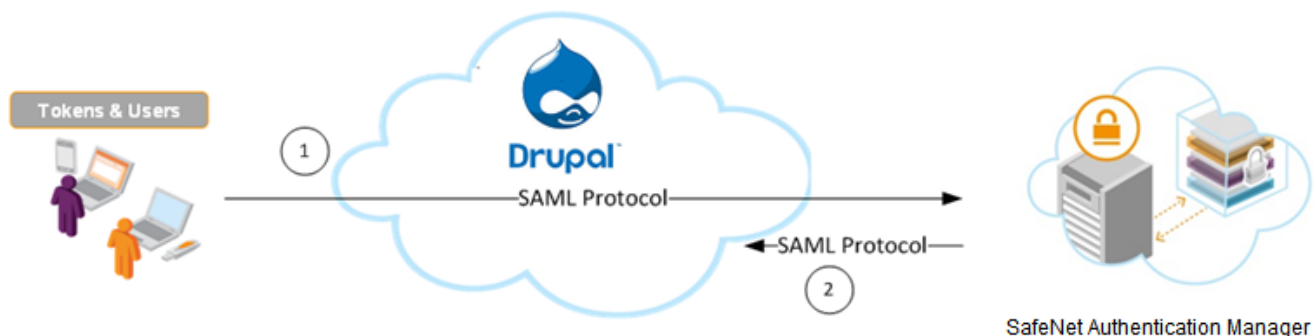
SAM provides a SAML authentication option that is already implemented in the SAM environment, and can be used without any installation.



Authentication Flow using SAM

SafeNet Authentication Manager 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 the SAM login portal. SAM collects and evaluates the user's credentials.
2. SAM returns a response to Drupal, accepting or rejecting the user's authentication request.

SAML Prerequisites

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

Configuring SafeNet Authentication Manager

Using SAM as an identity provider for Drupal requires the following:

- Synchronizing User Stores to SAM, page 6
- Assigning a Token in SAM, page 6
- Configuring SAM as an Identity Provider, page 7
- Downloading the SAM's Metadata, page 9
- Adding Drupal as a Service Provider in the Token Policy Object, page 10

Synchronizing User Stores to SAM

SAM manages and maintains tokens information in its data store, including the token status and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Microsoft Active Directory 2003, 2008, 2008 R2, 2012, and 2012 R2
- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Assigning a Token in SAM

SAM supports a number of token methods that can be used as a second authentication factor for users authenticating through Drupal.

The following tokens are supported:

- eToken PASS
- SafeNet GOLD
- SafeNet eToken 3400
- SafeNet eToken 3500
- eToken NG-OTP
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging

- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 4100
- SafeNet eToken PRO Smartcard
- SafeNet eToken 5100
- SafeNet eToken 5200
- SafeNet eToken 7300
- SafeNet eToken PRO
- eToken NG-Flash

Tokens can be assigned to users as follows:

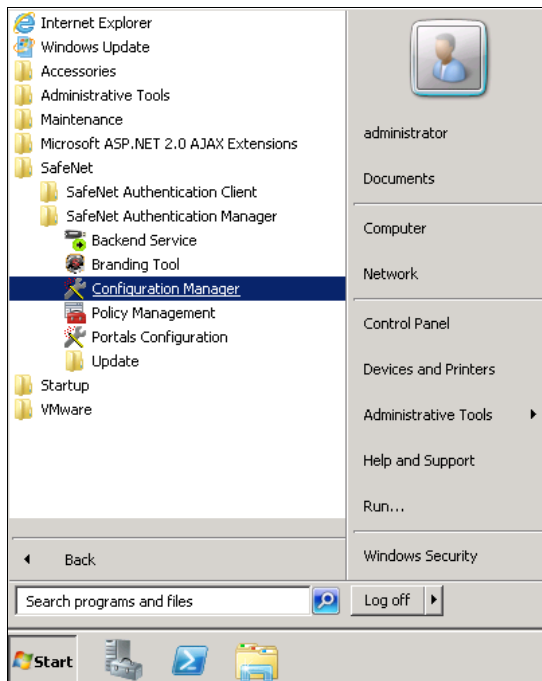
- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization's premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet's tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Configuring SAM as an Identity Provider

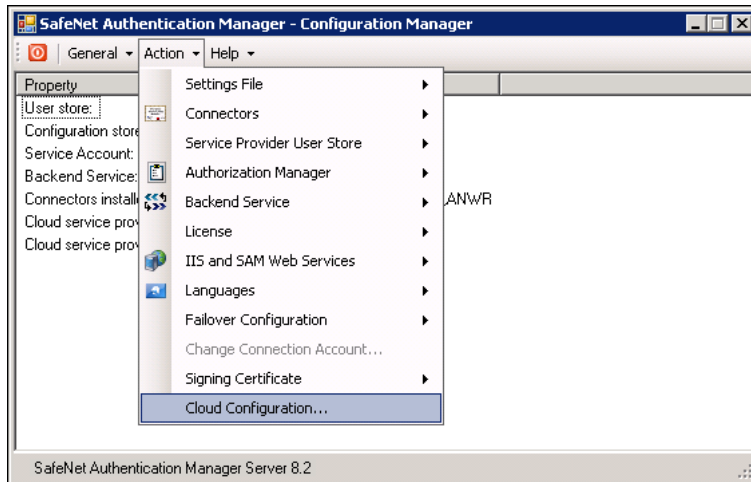
To use Drupal as a service provider and SAM as an identity provider, SAM must be configured as an identity provider.

1. From the Windows **Start** menu, click **Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.

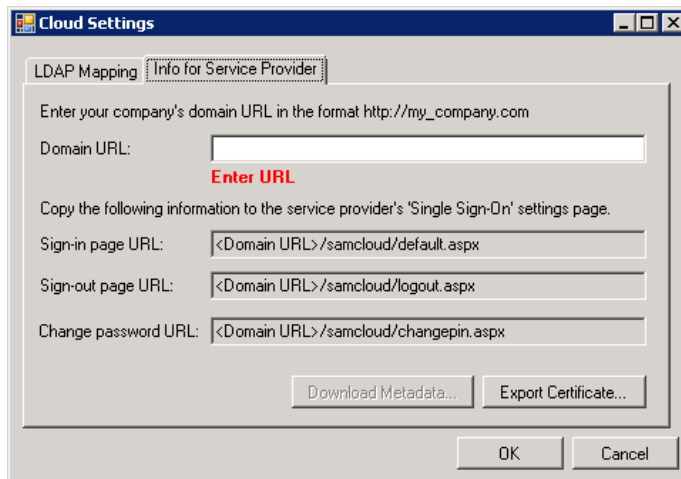


(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

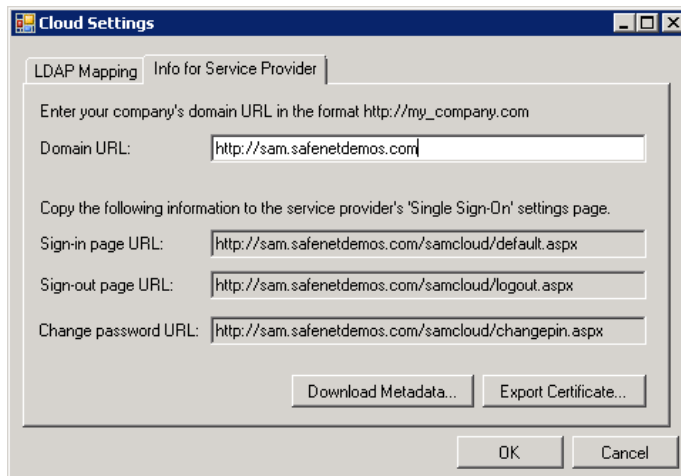
2. Click the **Action** tab, and then select **Cloud Configuration**.



3. Click the **Info for Service Provider** tab.
4. Type the web address of the SAM portal server in the **Domain URL** field.



The remaining fields are generated according to the Domain URL that was entered.

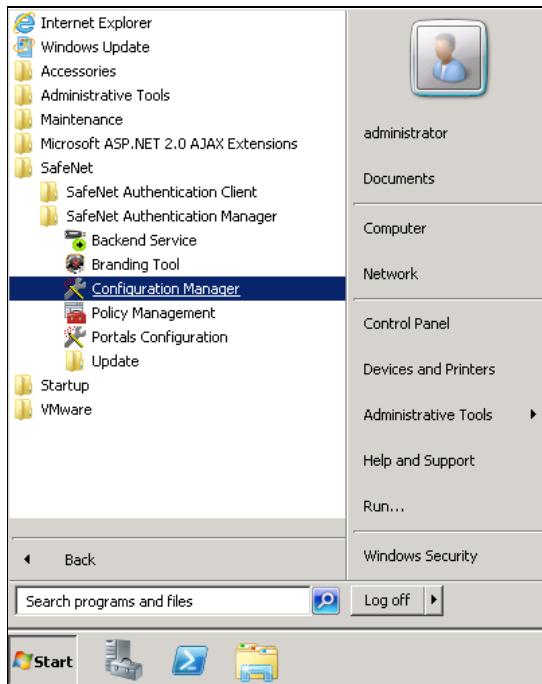


5. Click **OK**.

Downloading the SAM's Metadata

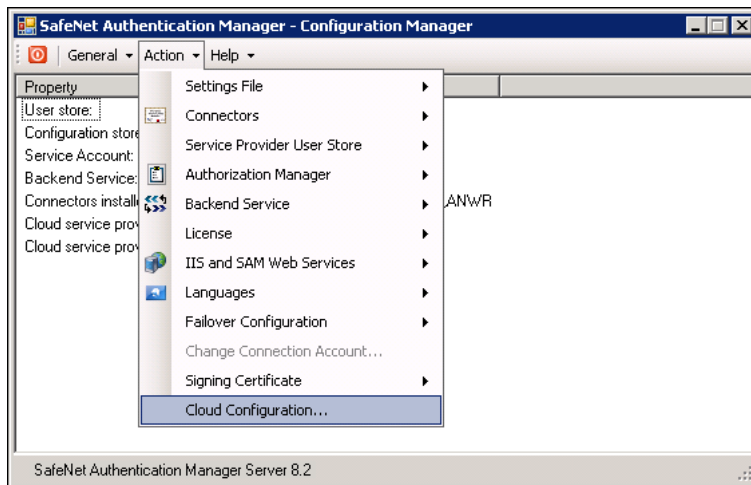
SAM metadata is required to configure the identity provider on Drupal for SAML authentication.

1. From the Windows **Start** menu, click **Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.



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

2. Click the **Action** tab, and then select **Cloud Configuration**.



3. On the **Cloud Settings** window, click the **Info for Service Provider** tab.

The screenshot shows the 'Cloud Settings' window with the 'Info for Service Provider' tab selected. The window contains several text input fields for configuration:

- Domain URL:
- Sign-in page URL:
- Sign-out page URL:
- Change password URL:

Below the input fields are two buttons: 'Download Metadata...' and 'Export Certificate...'. At the bottom of the window are 'OK' and 'Cancel' buttons.

4. Click **Download Metadata** and save the metadata file. This metadata file will be used later.
5. Click **OK**.

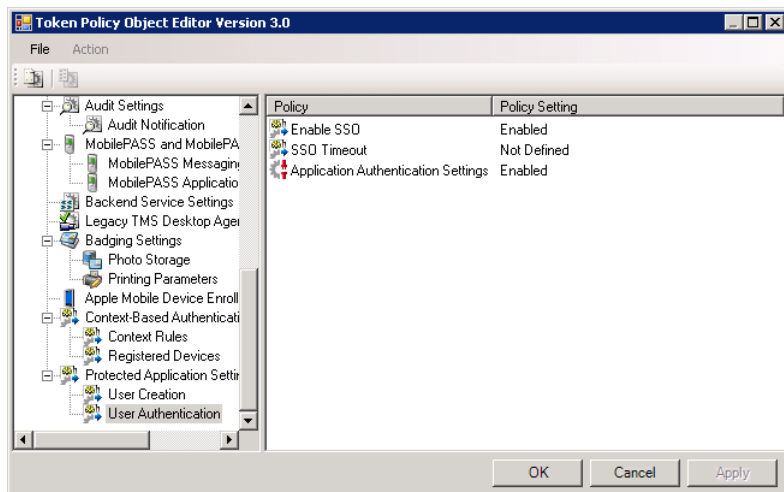
Adding Drupal as a Service Provider in the Token Policy Object

SAM's Token Policy Object (TPO) policies include Application Authentication Settings for SAML service providers. These settings are used by SAM's portal to communicate with service providers.

For general portal configuration, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

To edit the TPO for SAM's portal configuration:

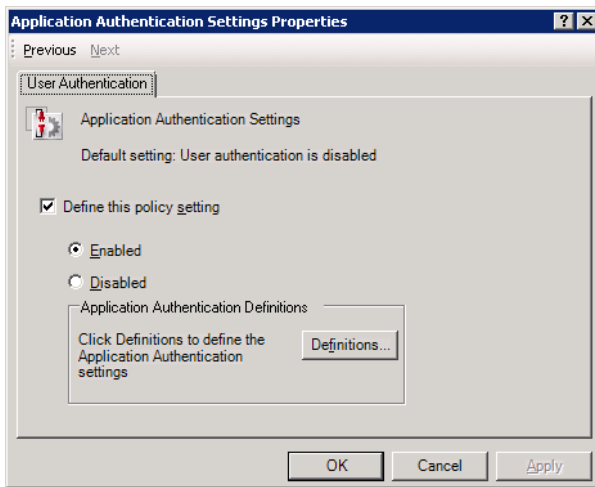
1. Open the **Token Policy Object Editor** for the appropriate group. Refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide* for more information.
2. In the left pane, click **Protected Application Settings > User Authentication**.



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

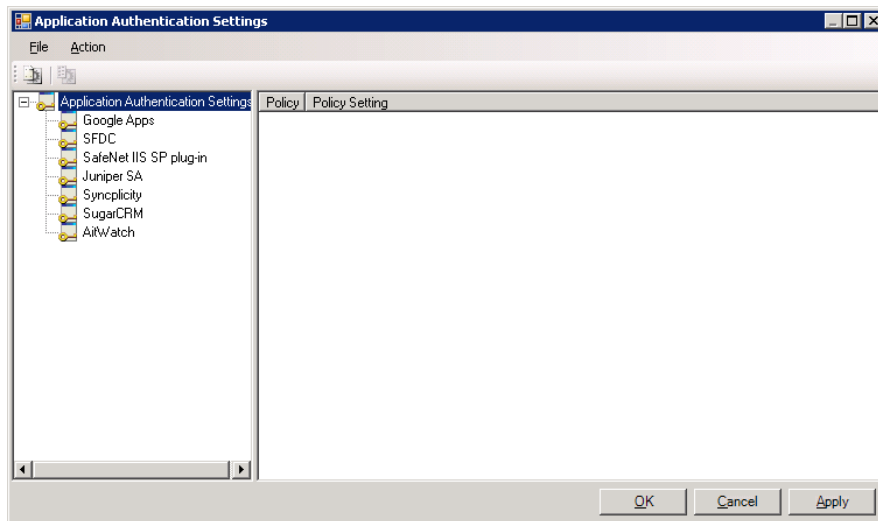
3. In the right pane, double-click **Application Authentication Settings**.

4. On the **Application Authentication Settings Properties** window, perform the following steps:
 - a. Select **Define this policy setting**.
 - b. Select **Enabled**.
 - c. Click **Definitions**.



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

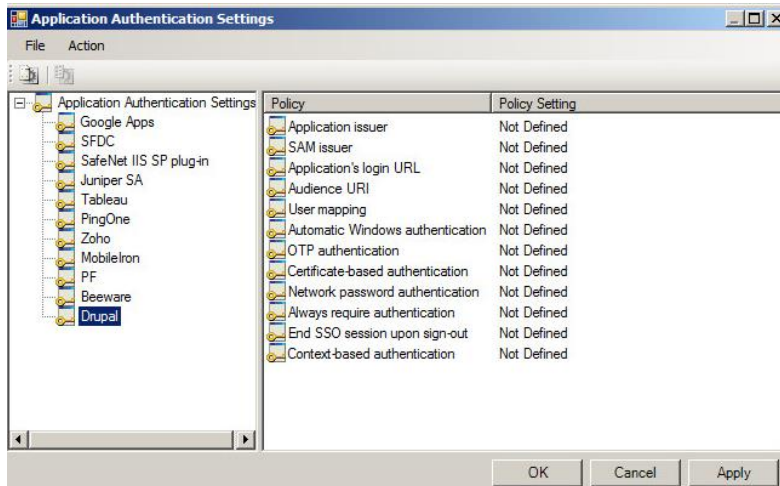
5. On the **Application Authentication Settings** window, right-click **Application Authentication Settings**, and then select **Create a new profile**.



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

6. In the left pane, right-click the new profile, and then rename the profile to a friendly name (for example, **Drupal**).

7. In the left pane, click the new profile.



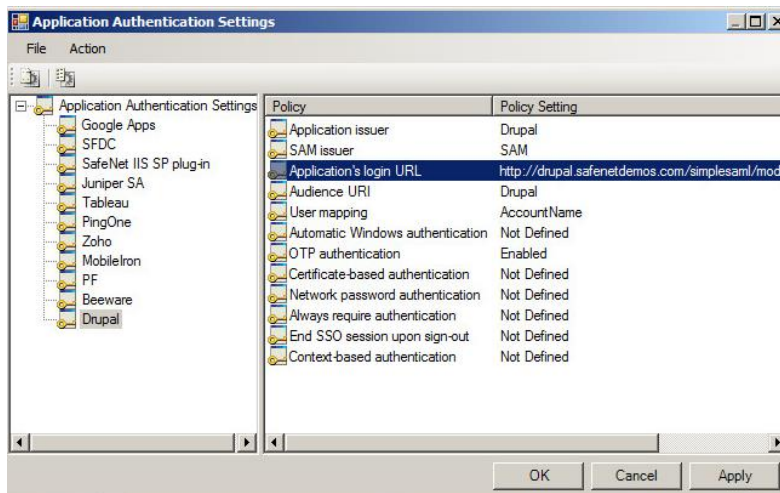
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

8. In the right pane, double-click on the following policies, and enter the appropriate information:

Application Issuer	Enter the Drupal entity ID. This should match the entity ID entered in step 1 in “Configuring SimpleSAMLphp as a Service Provider” on page 15.
SAM issuer	Enter the SAM entity ID. It should be same as in the SAM's metadata.
Application's login URL	Enter http://<IP/FQDN of SimpleSAMLphp server/simplesaml/module.php/saml/sp/saml2-acis.php/default-sp.
Audience URI	Enter the same value as you entered for Application Issuer .
User mapping	Select AccountName .

9. Enable the appropriate authentication methods for your organization. See the *SafeNet Authentication Manager Version 8.2 Administrator's Guide* for detailed information about authentication methods.

The following is an example of the completed policy settings in the **Application Authentication Settings** window:



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

10. Click **OK** until all of the **Token Policy Object Editor** windows are closed.

Configuring Drupal

To add SafeNet Authentication Manager as an identity provider in Drupal requires the following:

- Installing the SimpleSAMLphp Application, page 13
- Configuring SimpleSAMLphp as a Service Provider, page 15
- Configuring Drupal, page 17

Before you begin, make sure the SAM metadata is downloaded so that it is available for selection in the following procedure. If you have not already downloaded the SAM metadata, refer to “Downloading the SAM’s Metadata” on page 9.

Installing the SimpleSAMLphp Application

SimpleSAMLphp is an application written in PHP and it can be used to provide authentication.

1. Download the SimpleSAMLphp application from <https://simplesamlphp.org>.
2. Extract the package in the **/var** directory and rename it to **simplesamlphp**.
3. Open the **httpd.conf** file present in the **/etc/httpd/conf** directory, and then perform the following steps:
 - a. Add the following section at the end of 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>
```

- b. Edit the **DocumentRoot** element accordingly, if required.
 - c. Save the **httpd.conf** file, and then close it.
4. If the SELinux service is running on the server, run the following command to change the security context of SimpleSAMLphp:

```
chcon -Rt httpd_sys_content_t /var/simplesamlphp/
```
 5. Create a database in MySQL server.

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.

'baseurlpath' => 'http://<IP/FQDN of server/simplesaml/',

- **Admin Password:** Set an administrator password. This is needed to access some of the pages in your simpleSAMLphp installation web interface.

'auth.adminpassword' => 'setnewpasswordhere',

- **Secret Salt:** It should be a random string. Some parts of the simpleSAMLphp application need this salt to generate cryptographically secure hashes. The command below 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*.

'store.type' => 'sql',

'store.sql.dsn' => 'mysql:host=<IP Address/Hostname of MySQL server>;dbname=<Database name>',

'store.sql.username' => '<MySQL username>',

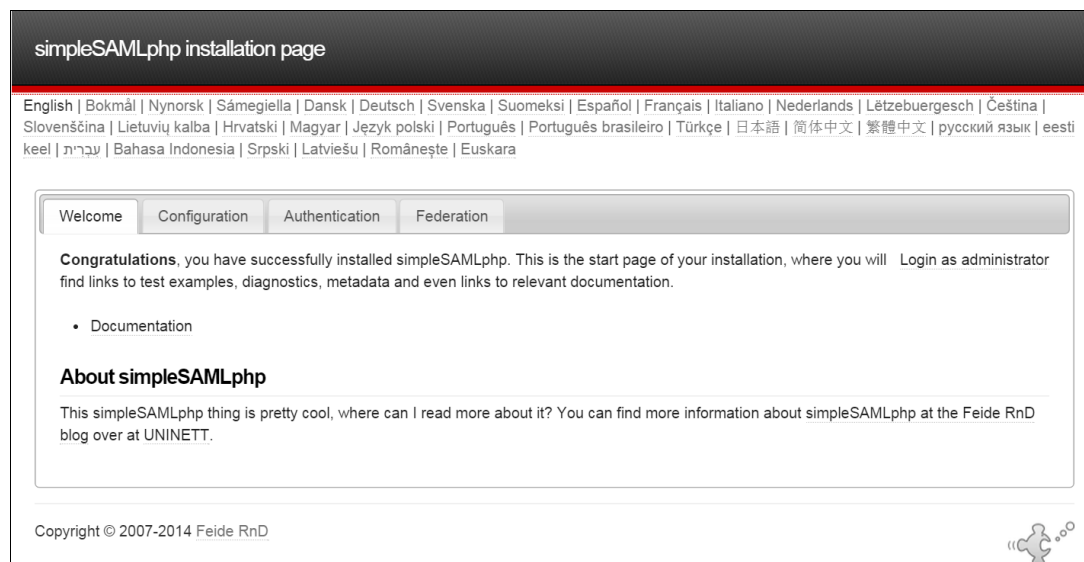
'store.sql.password' => '<User Password>',

7. Restart the apache server:

service httpd restart

8. In a web browser, open this URL: **http://<IP/FQDN of server>/simplesaml**

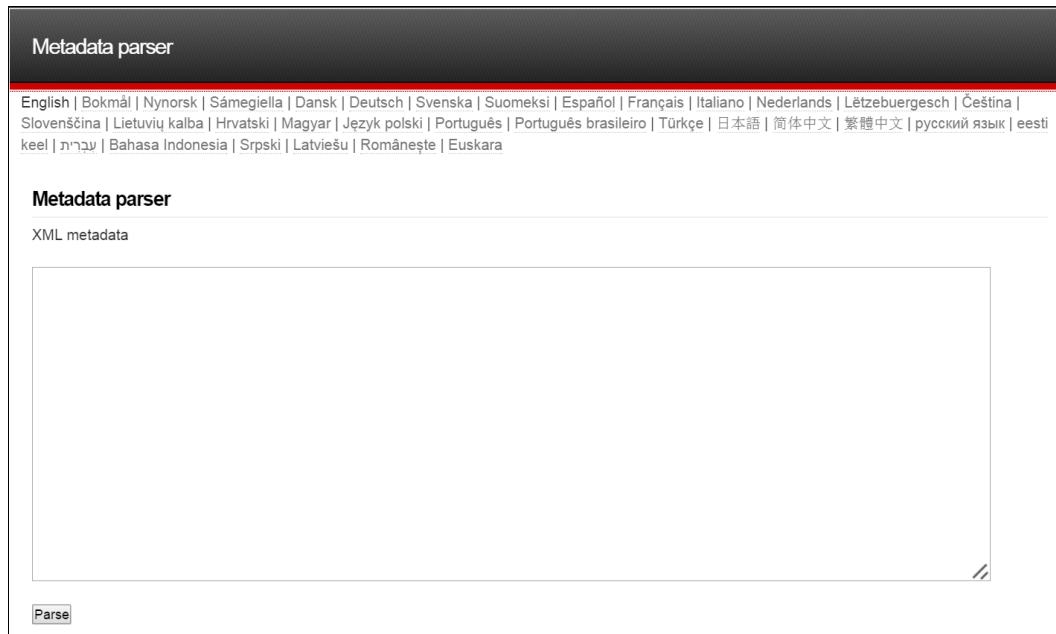
If the **SimpleSAMLphp** application is successfully installed, you will see a page as shown below:



Configuring SimpleSAMLphp as a Service Provider

Configure the SimpleSAMLphp application as a SAML service provider.

1. Open the **authsources.php** file located in the **/var/simplesamlphp/config** directory, edit the following, and then save the file.
 - **Entity ID:** Enter an entity ID for SimpleSAMLphp.
'entityID' => 'Your entity ID',
 - **IDP:** Set the default IDP as SAM by setting its value as SAM's entity ID. SAM's entity ID can be found in its metadata.
'idp' => 'SAM's entity ID',
2. In a web browser, open the following URL:
http://<IP/FQDN of server>/simplesaml/admin/metadata-converter.php
3. Paste the SAM's metadata (See "Downloading the SAM's Metadata" on page 9) in the **XML metadata** field, and then click **Parse**.



The screenshot shows the 'Metadata parser' web interface. At the top, there is a dark header with the title 'Metadata parser'. Below the header is a horizontal list of language links: English | Bokmål | Nynorsk | Sámegiella | Dansk | Deutsch | Svenska | Suomi | Español | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 简体中文 | 繁體中文 | русский язык | eesti keel | עברית | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara. Below the language links is a section titled 'Metadata parser' with a sub-label 'XML metadata'. This section contains a large, empty text area for pasting metadata. At the bottom left of the text area is a 'Parse' button.

- Copy the converted metadata under **saml20-idp-remote** and save it locally in a file.

```
Converted metadata

saml20-idp-remote

$metadata['SAM'] = array (
  'entityid' => 'SAM',
  'contacts' =>
  array (
  ),
  'metadata-set' => 'saml20-idp-remote',
  'SingleSignOnService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'http://sam.safenetdemos.com/samcloud/default.aspx',
    ),
    1 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
      'Location' => 'http://sam.safenetdemos.com/samcloud/default.aspx',
    ),
  ),
  'SingleLogoutService' =>
  array (
  ),
  'ArtifactResolutionService' =>
  array (
  ),
  'keys' =>
  array (
    0 =>
    array (
      'encryption' => false,
      'signing' => true,
      'type' => 'X509Certificate',
    ),
  ),
)
```

- Open the **saml20-idp-remote.php** file in the **/var/simplesamlphp/metadata** directory, paste the converted metadata in the file, and then save it so that it looks like the example shown below:

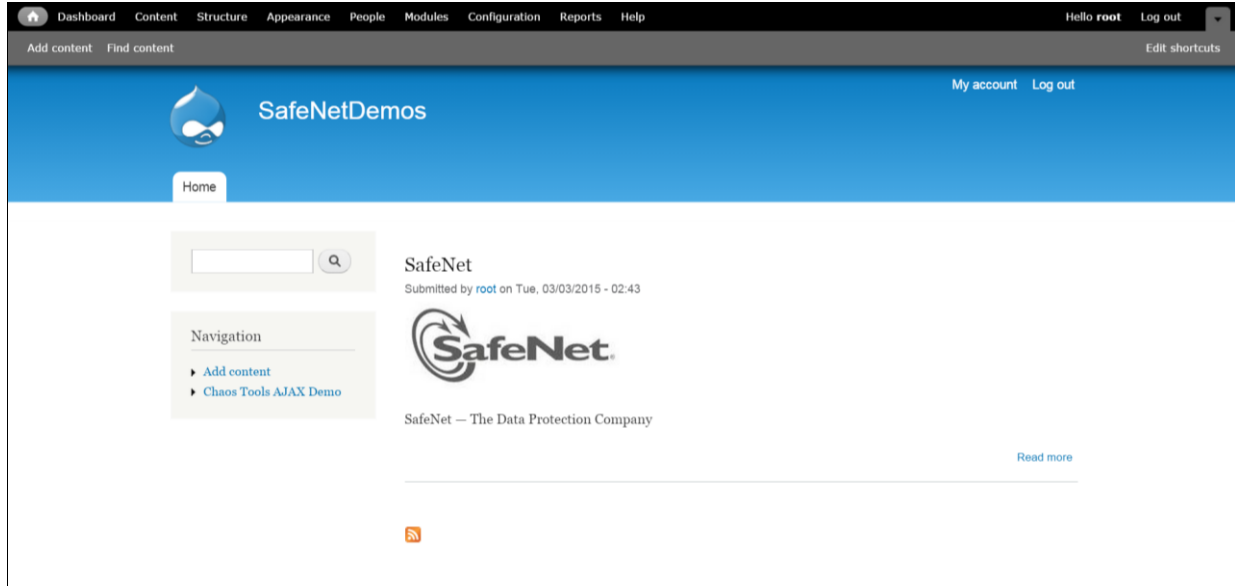
```
<?php
/**
 * SAML 2.0 remote IdP metadata for simpleSAMLphp.
 *
 * Remember to remove the IdPs you don't use from this file.
 *
 * See: https://simplesamlphp.org/docs/stable/simplesamlphp-reference-idp-remote
 */

/*
 * Guest IdP, allows users to sign up and register. Great for testing!
 */
$metadata['SAM'] = array (
  'entityid' => 'SAM',
  'contacts' =>
  array (
  ),
  'metadata-set' => 'saml20-idp-remote',
  'SingleSignOnService' =>
  array (
    0 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
      'Location' => 'http://sam.safenetdemos.com/samcloud/default.aspx',
    ),
    1 =>
    array (
      'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST',
      'Location' => 'http://sam.safenetdemos.com/samcloud/default.aspx',
    ),
  ),
  'SingleLogoutService' =>
  array (
  ),
  'ArtifactResolutionService' =>
  array (
  ),
  'keys' =>
  array (
    0 =>
    array (
      'encryption' => false,
      'signing' => true,
      'type' => 'X509Certificate',
    ),
  ),
)
```


Configuring Drupal

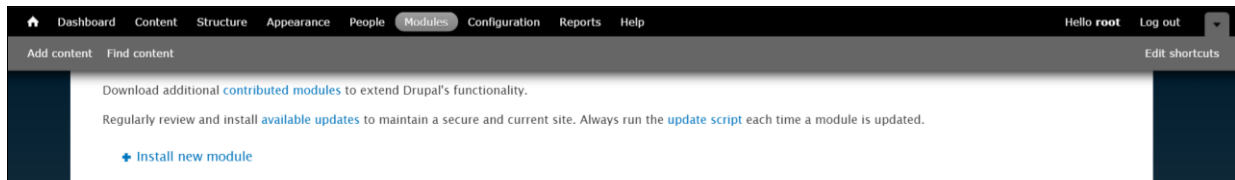
From the Drupal website, download the **simplesamlphp_auth** module. This module is used to integrate Drupal with the SimpleSAMLphp service provider.

1. Extract the package and move it to the Drupal **modules** directory (**../Drupal/modules**).
2. In a web browser, browse to the Drupal account, and then login as a user with administrator privileges.



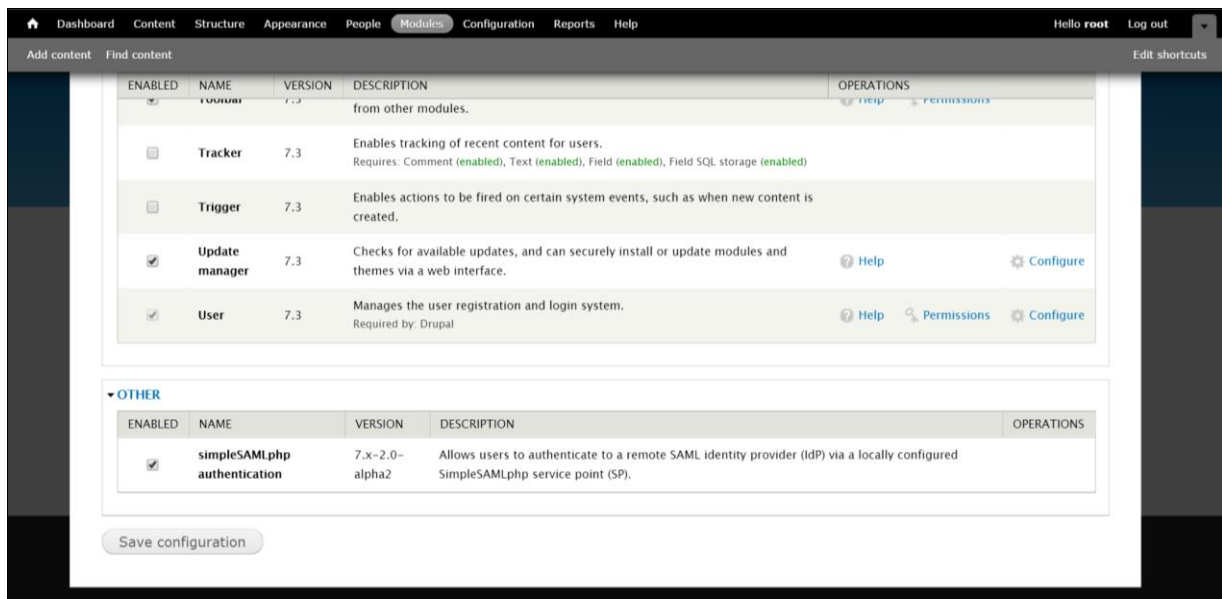
(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)

3. In the menu, click **Modules**.



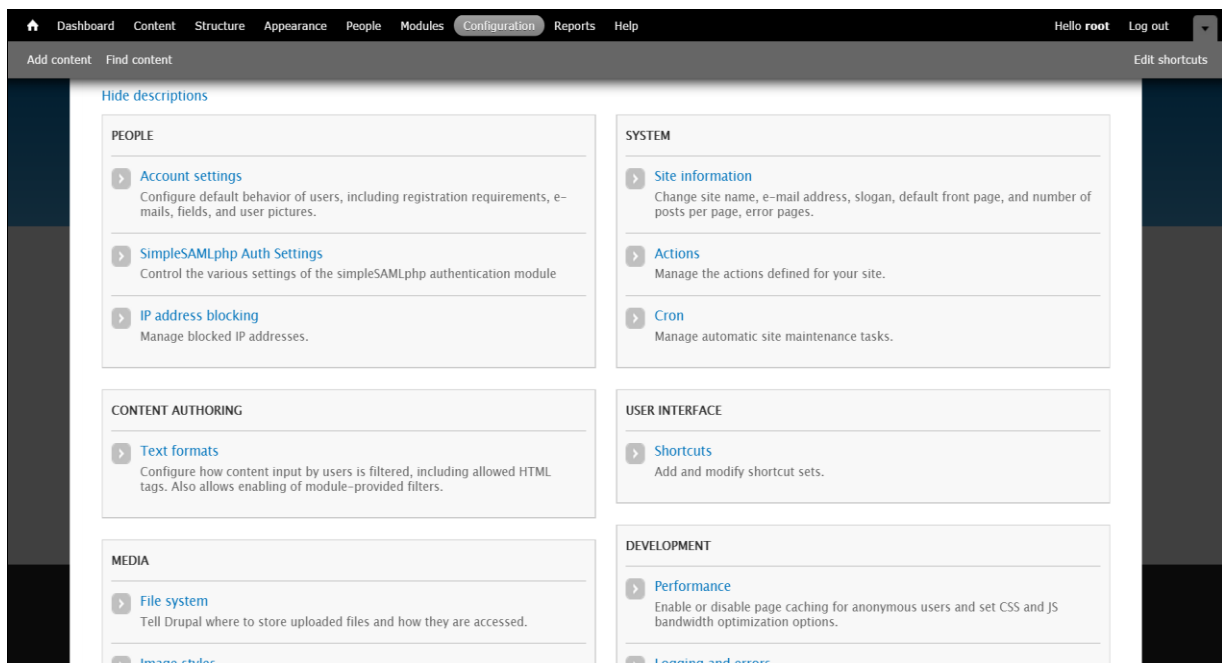
(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)

4. Under the **OTHER** section, locate the **simpleSAMLphp authentication** module, select the checkbox, and then click **Save configuration**.



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

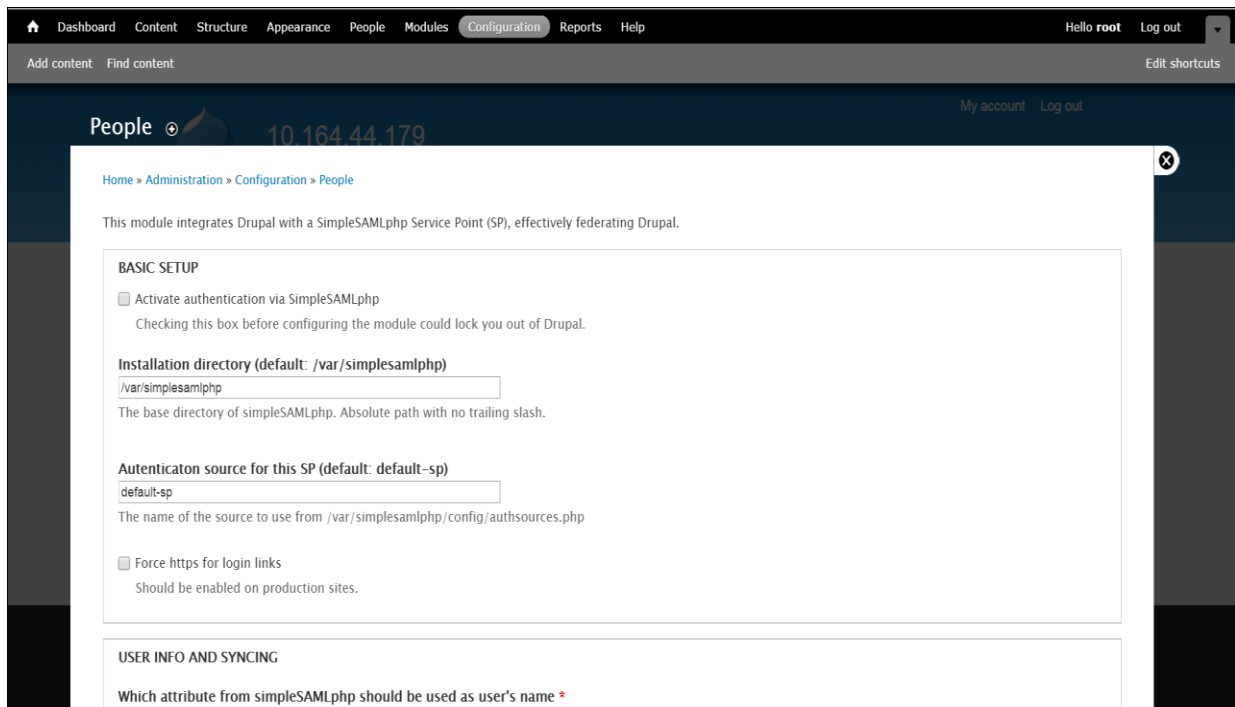
5. In the menu, click **Configuration**. Then, on the page, click the **SimpleSAMLphp Auth Settings** link.



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

6. Complete the following details, and then click **Save configuration**.

BASIC SETUP	
Activate authentication via SimpleSAMLphp	Select the checkbox to enable SAML authentication.
Installation directory	Change the directory if simplesamlphp is located elsewhere.
USER INFO AND SYNCING	
Which attribute from simpleSAMLphp should be used as user's name	urn:oid:0.9.2342.19200300.100.1.1
Which attribute from simpleSAMLphp should be used as unique identifier for the user	urn:oid:0.9.2342.19200300.100.1.1
Which attribute from simpleSAMLphp should be used as user mail address	urn:oid:0.9.2342.19200300.100.1.1
USER PROVISIONING	
Register Users	Select this option to enable just-in-time provisioning.
DRUPAL AUTHENTICATION	
Allow SAML users to set Drupal passwords	Select accordingly.
Allow authentication with local Drupal accounts	Select this option if you do not want to enforce SAML authentication.

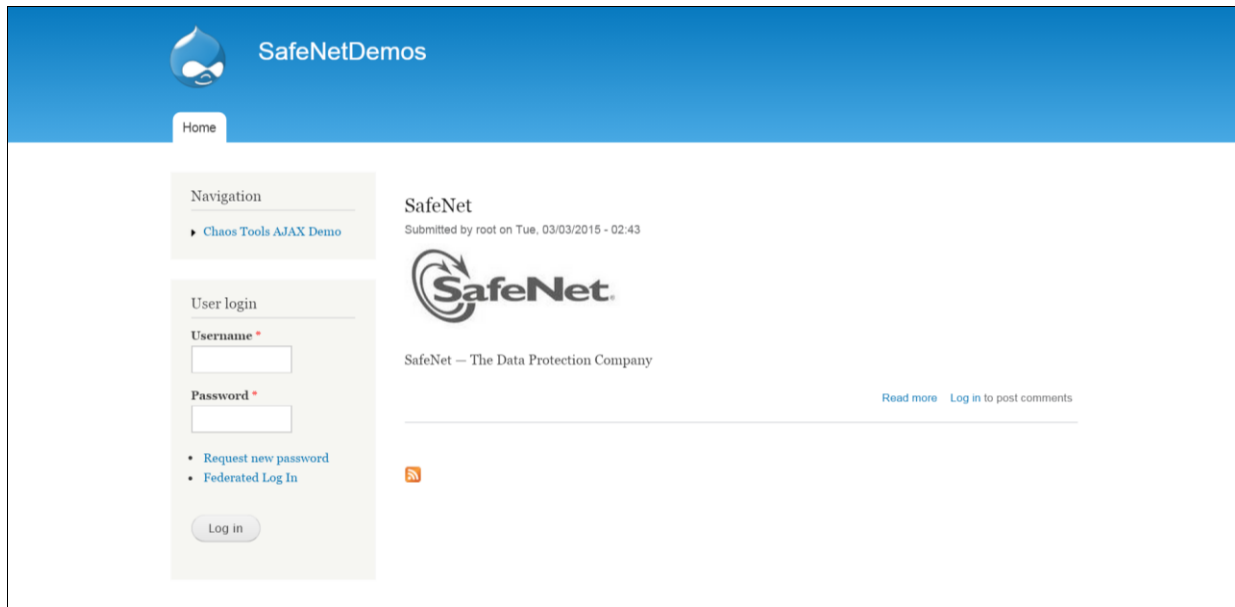


(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)

Running the Solution

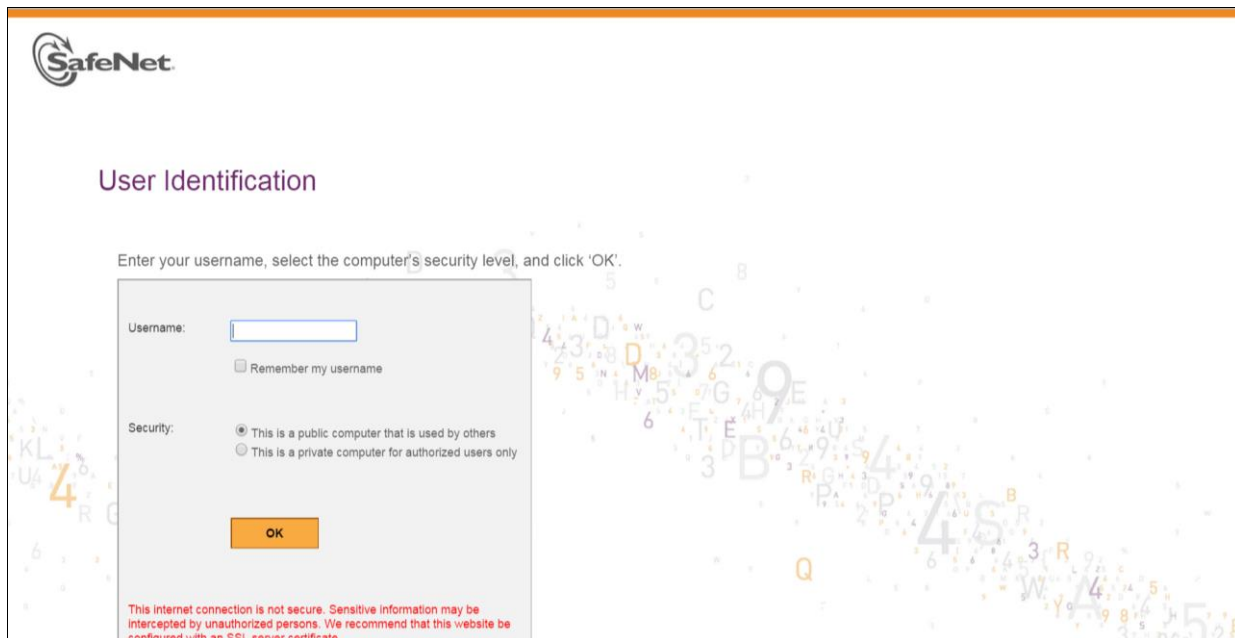
For this integration, the SafeNet eToken PASS is configured for authentication with the SAM solution.

1. In a web browser, browse to the Drupal login page, and then click the **Federated Log In** link.

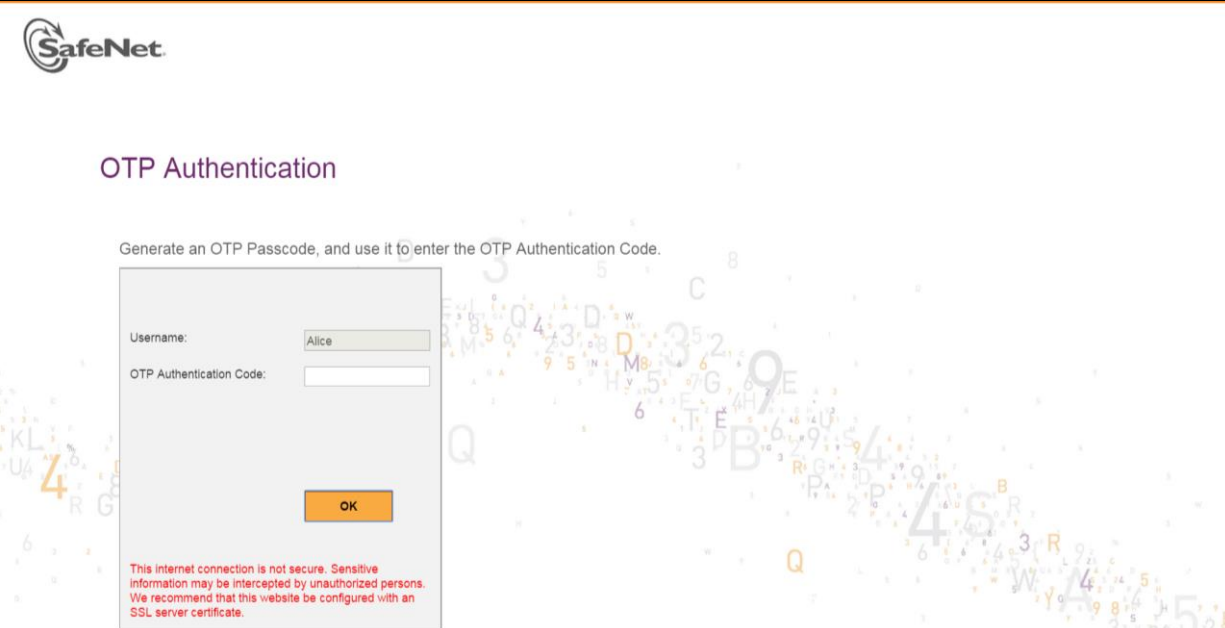


(The screen image above is from Drupal™. Trademarks are the property of their respective owners.)

2. You will be redirected to the SAM **User Identification** page. In the **Username** field, enter your username, and then click **OK**.

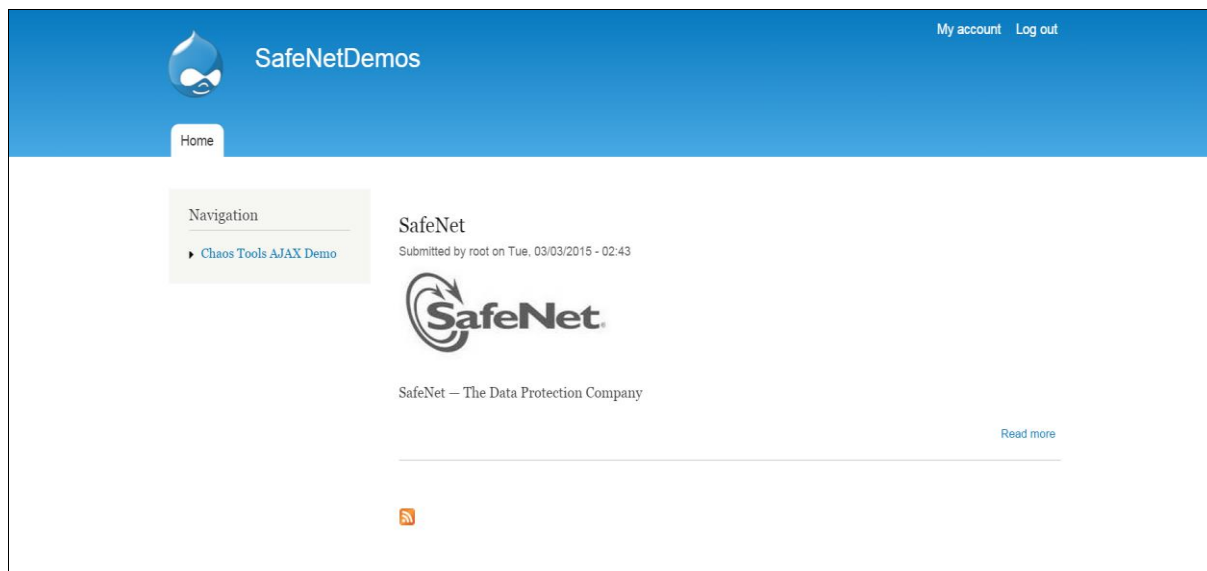


- You will be redirected to the **OTP Authentication** page. Generate a one-time password using the SafeNet token, enter it in the **OTP Authentication Code** field, and then click **OK**.



The image shows the SafeNet OTP Authentication page. At the top left is the SafeNet logo. Below it, the title "OTP Authentication" is displayed in purple. A instruction reads: "Generate an OTP Passcode, and use it to enter the OTP Authentication Code." Below this is a form with two input fields: "Username:" with the value "Alice" and "OTP Authentication Code:" which is empty. An orange "OK" button is positioned below the code field. At the bottom left of the form, a red warning message states: "This internet connection is not secure. Sensitive information may be intercepted by unauthorized persons. We recommend that this website be configured with an SSL server certificate." The background of the page is decorated with a pattern of floating numbers and letters.

After successful authentication, you are redirected to your 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	https://serviceportal.safenet-inc.com 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.	