

**Banco Interamericano de Desarrollo**

**SimpleSAML library and module configuration for Drupal CMS (Pantheon) authentication with IDB Azure platform**

**Ciudad de Panamá**

**April 22th, 2020**

****

**Document version**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Comments | Date | Responsable |
| 1.0 | Initial version | April 22th, 2020 | EBFactory |
| 1.1 | Updated version | May 26th, 2020 | EBFactory |
| 1.2 | Updated version | Jun 23th, 2020 | EBFactory |
| 1.3 | Updated version | Sep 30th, 2020 | EBFactory |

**Content**

[1 Requirements 4](#_Toc38565541)

[2 Site metadata for test and live environments. 5](#_Toc38565542)

[2.1 Submit Sevice Now work order 5](#_Toc38565543)

[2.2 Metadata files 6](#_Toc38565544)

[3 SimpleSAML library installation and configuration 6](#_Toc38565545)

[4 Drupal simplesamlphp\_auth module installation and configuration 12](#_Toc38565546)

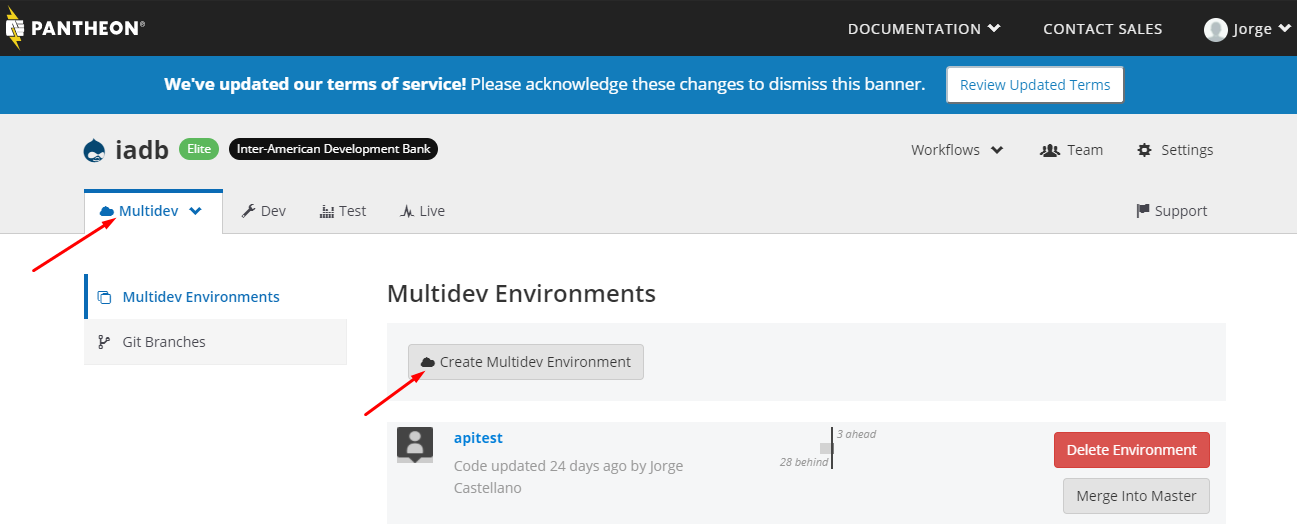
1. **Requirements**

In order to install the modules and library needed to authenticate via SSO the following requirement must be met:

* Use Docksal as a local development environment
* Have Composer as a package and library manager for PHP
* For testing, create an authentication environment called auth in pantheon, example: auth-sitename.pantheonsite.io
* The site is already in production and has a domain name

The steps described in this guide are based in the assumption that the above is true, however if your local environment is different but you are using composer you could still run the commands without the ***fin*** word used at the start of each command

Example to create the auth environment: Enter the dashboard of the project hosted in pantheon, click on "multidev" and then on "create multidev enviroment", enter "auth" as the name of the enviroment



*Disclaimer: this guide is based on the official documentation provided by* [*Pantheon*](https://pantheon.io/docs/shibboleth-sso) *and* [*SimpleSAMLphp*](https://simplesamlphp.org/) *library. This configuration can change any time please make sure you visit* [*https://pantheon.io/docs/sso*](https://pantheon.io/docs/sso) *and* [*https://pantheon.io/docs/shibboleth-sso*](https://pantheon.io/docs/shibboleth-sso)

***Make sure that the site has a fully functional domain in the form of xxx.iadb.org. If this step is not completed, then you will not be able to configure single sign-on on your site.***

1. **Site metadata for test and live environments.**
   1. **Submit a new Service Now work order**

(This step can only be done by the ITE BP) Use the following data as template for your request, this are the fields needed to be filled in the form:

**Reported** **source**: phone

**Action** **required**: create

**Category**: KIC Business Application

**Subcategory**: IDB External Website

**Component**: Functional

**Assignment** **group**: Active Directory

**Short** **Description**: Azure authentication for Drupal subsite {subdomain}.iadb.org *(change the string inside the {} to the required values)*

**Description**:   
Please create using as an example iadb.org site configuration

|  |  |  |
| --- | --- | --- |
|  | **Production** | **Test** |
| **Domain** | {Sitename} prod  domain: sitename.iadb.org | {Sitename} test domain: http://auth-sitename. pantheonsite.io |
| **Entity ID** | drupal\_{sitename}\_azure | drupal\_{sitename}\_azure\_test |

*(change the string inside the {} to the required values)*

**Example**:

A screenshot of a social media post

Description automatically generated

* 1. **Metadata files**

Active directory team will send you a response for the work order including two zip files containing the metadata files required for each environment. Each zip file has two files in it:

* .xml file (metadata)
* .cer file (ssl certificate)

The xml file will be used later in the configuration of the Identity Provider (IDP) metadata file.

**SimpleSAML library installation and configuration**

In the root folder of the project install SimpleSAML library

web$ fin composer require simplesamlphp/simplesamlphp  
web$ mkdir private  
web$ cp ./vendor/simplesamlphp/simplesamlphp/metadata-templates/saml20-idp-remote.php private/  
web$ cp ./vendor/simplesamlphp/simplesamlphp/config-templates/config.php private/simplesaml-config.php  
web$ cp ./vendor/simplesamlphp/simplesamlphp/config-templates/authsources.php private/simplesaml-authsources.php web$ ln -s ./vendor/simplesamlphp/simplesamlphp/www ./simplesaml

Open the file *private/simplesaml-config.php* and add the following lines before the beginning of the configuration array ($config)

if (!ini\_get('session.save\_handler')) {

ini\_set('session.save\_handler', 'file');

}

if (isset($\_ENV['PANTHEON\_ENVIRONMENT'])) {

$ps = json\_decode($\_SERVER['PRESSFLOW\_SETTINGS'], TRUE);

$host = $\_SERVER['HTTP\_HOST'];

$db = $ps['databases']['default']['default'];

$tempdir = $\_ENV['HOME'] . '/tmp/simplesaml';

}

else {

$tempdir = '/tmp/simplesaml';

$db = array (

'database' => 'default',

'username' => 'user',

'password' => 'user',

'host' => 'db',

'driver' => 'mysql',

'port' => '',

);

}

In the same file, find the line where the configuration file is set:

'baseurlpath' => 'https://'. $host .'/simplesaml/',

'auth.adminpassword' => '<NEW\_PASSWORD>'

Only in the case of pantheon servers, in the same file identify the last section "DATA STORE CONFIGURATION", replace from there all the code with the following:

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

| DATA STORE CONFIGURATION |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

'store.type' => 'sql',

'store.sql.dsn' => 'mysql:host='. $db['host'] .';port='. $db['port'] .';dbname='. $db['database'],

'store.sql.username' => $db['username'],

'store.sql.password' => $db['password'],

'store.sql.prefix' => 'SimpleSAMLphp',

'store.redis.host' => 'localhost',

'store.redis.port' => 6379,

'store.redis.prefix' => 'SimpleSAMLphp',

];

Create symbolic links for the configuration files in the private folder to the vendor Simplesaml library folder. This step needs to be done every time a composer update or composer install is run (For instance when you update Drupal)

web$ mkdir ./vendor/simplesamlphp/simplesamlphp/config/

web$ ln -s ../../../../private/simplesaml-config.php ./vendor/simplesamlphp/simplesamlphp/config/config.php

web$ ln -s ../../../../private/simplesaml-authsources.php ./vendor/simplesamlphp/simplesamlphp/config/authsources.php

web$ ln -s ../../../../private/saml20-idp-remote.php ./vendor/simplesamlphp/simplesamlphp/metadata/

Create a openssl certificate for the library

web$ mkdir cert

web$ cd cert

web$ openssl req -newkey rsa:3072 -new -x509 -days 3652 -nodes -out saml.crt -keyout saml.pe

Add the files to the repository, commit the changes and push to the remote brach

web$ git add .

web$ git commit -m “Simplesamlphp library configuration”

web$ git push origin master

Open the website add the path /simplesaml at the end

(example URL <https://mysite.pantheonsite.io/simplesaml/>) You will see a welcome screen to the SimplesamlPHP library like this:

A screenshot of a social media post

Description automatically generated

Click on the ***Federation*** tab and then on the ***XML to SimpleSAMLphp metadata converter*** link you will see at the end of the options:

A screenshot of a cell phone

Description automatically generated

Then you will need to authenticate with the library credentials set in the configuration file:

A screenshot of a cell phone

Description automatically generated

With the metadata parser you will be able to upload the metadata file provided by Active Directory team as a response of the work order. After you have uploaded the file click on the button parse:

A screenshot of a cell phone

Description automatically generated

The parsing process will return the lines of PHP code you need to add into the private/saml20-idp-remote.php

A screenshot of a social media post

Description automatically generated

In the file private/authsources.php, modify the following lines:

'entityID' => ‘your entity ID’,

'idp' => ‘entity ID url’

Open composer.json and add the following lines to the end of the file, the symbolic links must be the same as those configured in previous steps

"scripts": {

    "post-install-cmd": [

        "ln -sf ../../../../private/saml20-idp-remote.php ./vendor/simplesamlphp/simplesamlphp/metadata/",

        "ln -sf ../../../../private/simplesaml-authsources.php ./vendor/simplesamlphp/simplesamlphp/config/authsources.php",

        "ln -sf ../../../../private/simplesaml-config.php ./vendor/simplesamlphp/simplesamlphp/config/config.php"

        ]

    }

This will make when we update or reinstall the dependencies with composer correct the symbolic links

After you have updated the private/saml20-idp-remote.php file commit the changes and test in Pantheon the authentication process.

Important: The metadata you just uploaded is attached to the domain, so you need to push your changes to the correct branch/environment, when you finally do the configuration for live environment use the domain of the site to access and configure the SimpleSAML library.

web$ mkdir cert

web$ cd cert

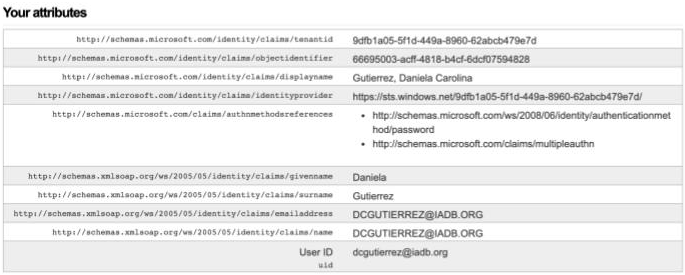
web$ openssl req -newkey rsa:3072 -new -x509 -days 3652 -nodes -out saml.crt -keyout saml.pe

Go to the library page again, and open the tab ***Test configured authentication sources*** and click on the link ***default-sp***

A screenshot of a cell phone

Description automatically generated

It should redirect you to the Windows Azure authentication system, or if you are already logged in it should directly show you the attributes for your account:



1. **Drupal simplesamlphp\_auth module installation and configuration**

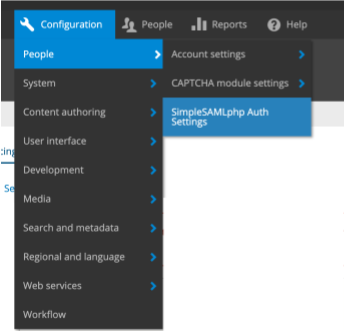
Install the module and enable it in the local environment:

web$ fin composer require drupal/simplesamlphp\_auth  
web$ fin drush en simplesamlphp\_auth -y

web$ fin refreshdb <BRANCH\_NAME>

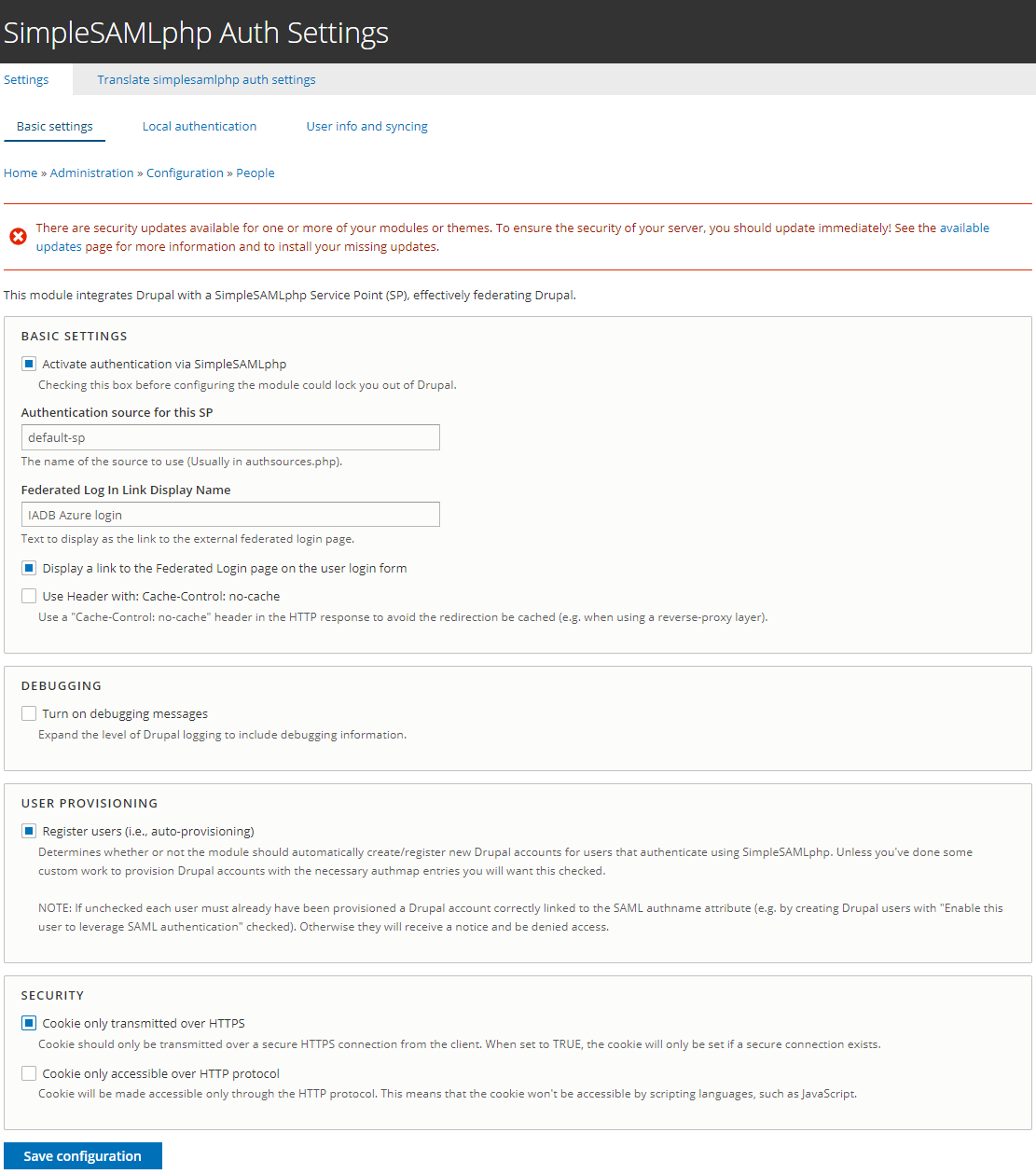
web$ fin drush cex

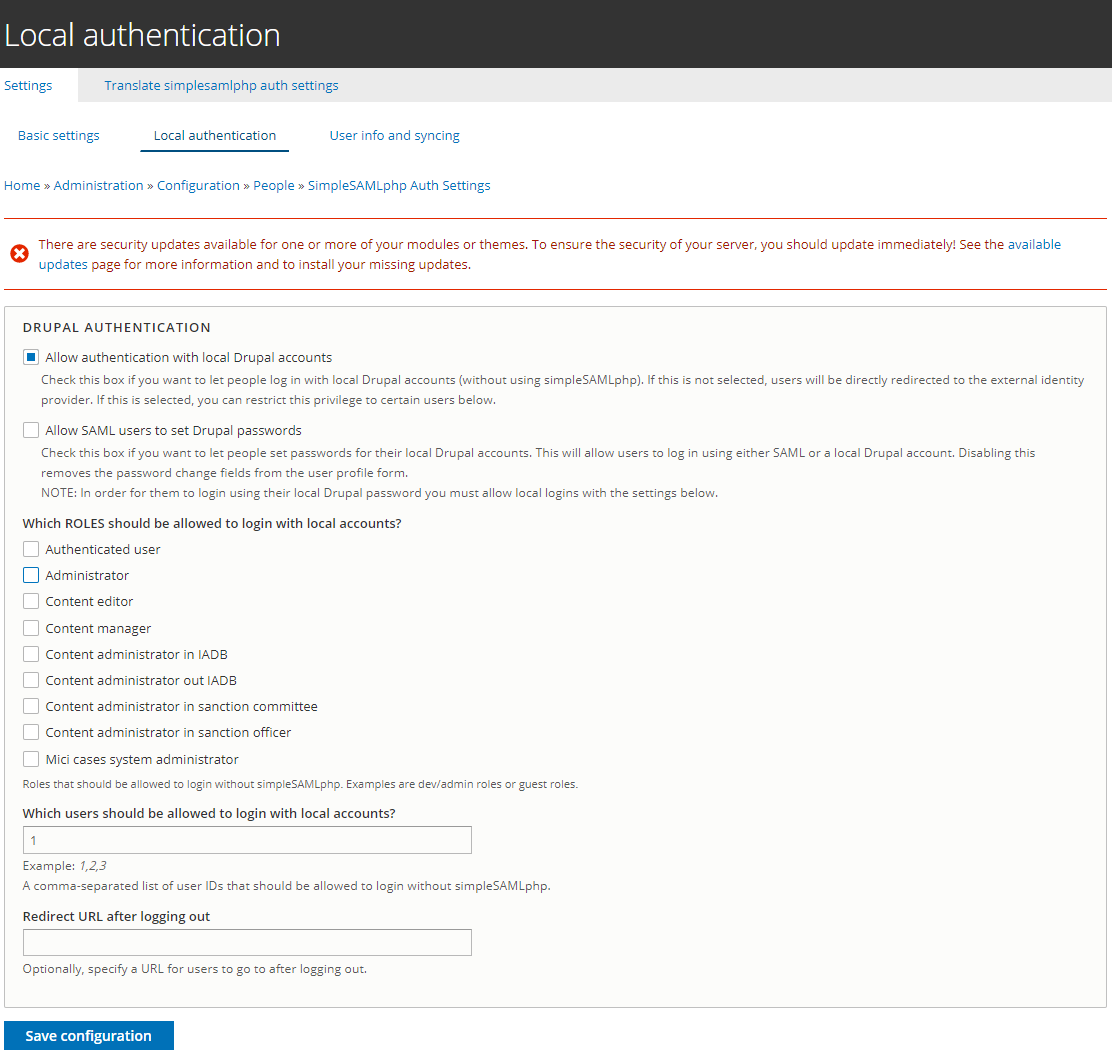
Open your local site and go to the module configuration

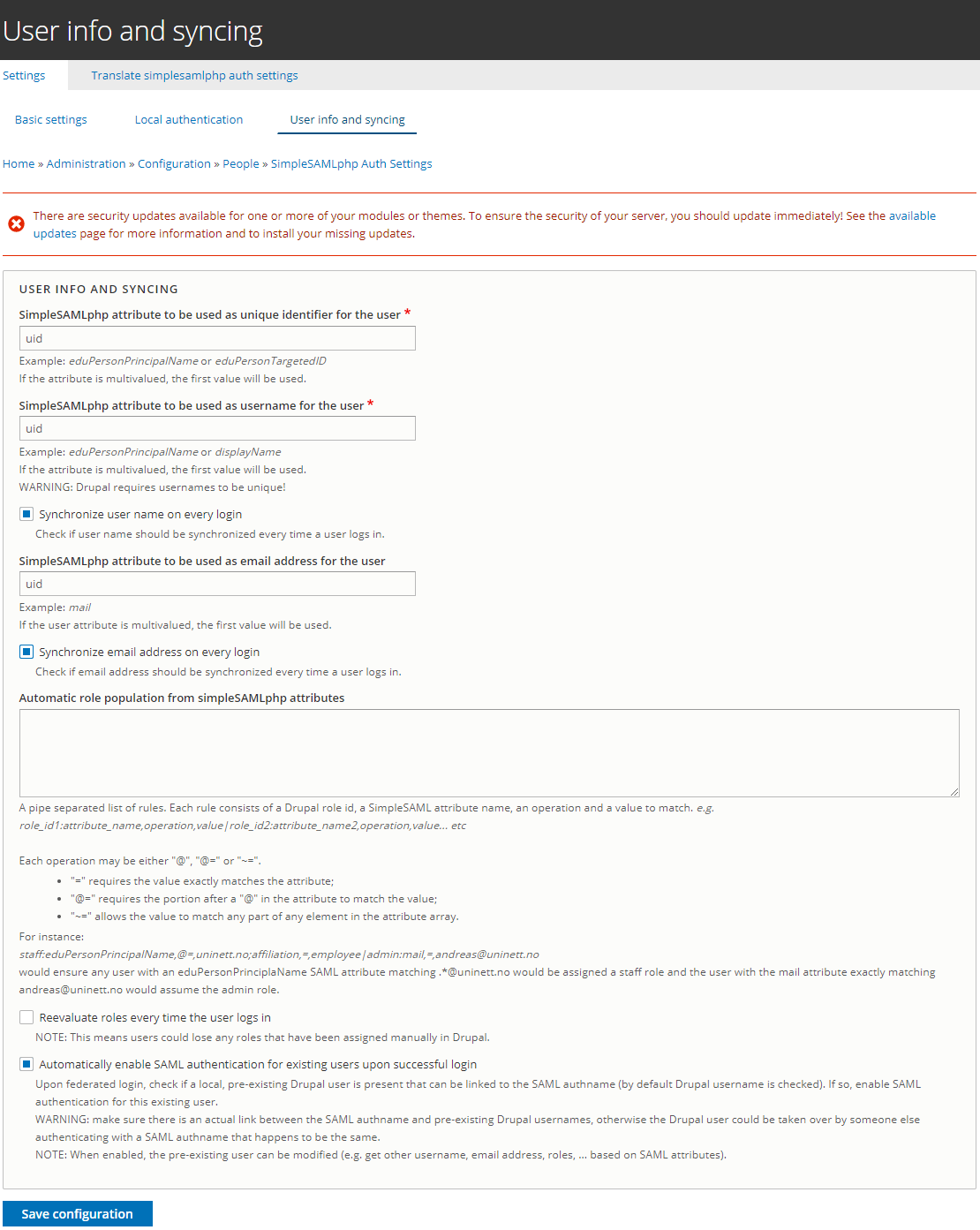


There are three steps in the configuration, start with the step ***User info and syncing then*** ***Local authentication*** and finally with the ***Basic settings*** *enabling* the module.

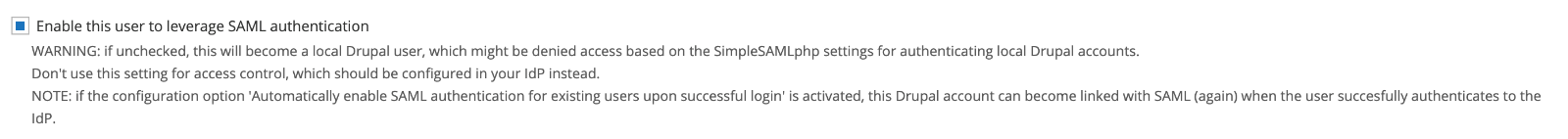
Fill the fields in the forms as shown in the next images:







Create the users and add the roles for them. Make sure the box ***Enable this user to leverage SAML authentication*** is marked before you save the user information.



Export configuration and push generated configuration files to the repository:

web$ fin drush cex -y  
web$ git add .  
web$ git commit -m “SimplesampPHP module configuration”  
web$ git push origin master

Deploy your changes until the desired environment.

Open your site user login URL <https://mysite.iadb.org/en/user/login> and you will see the ***IADB Azure login*** link that will take you to authenticate with Azure.

A screenshot of a social media post

Description automatically generated