SAML Single Sign-On with Pandora FMS

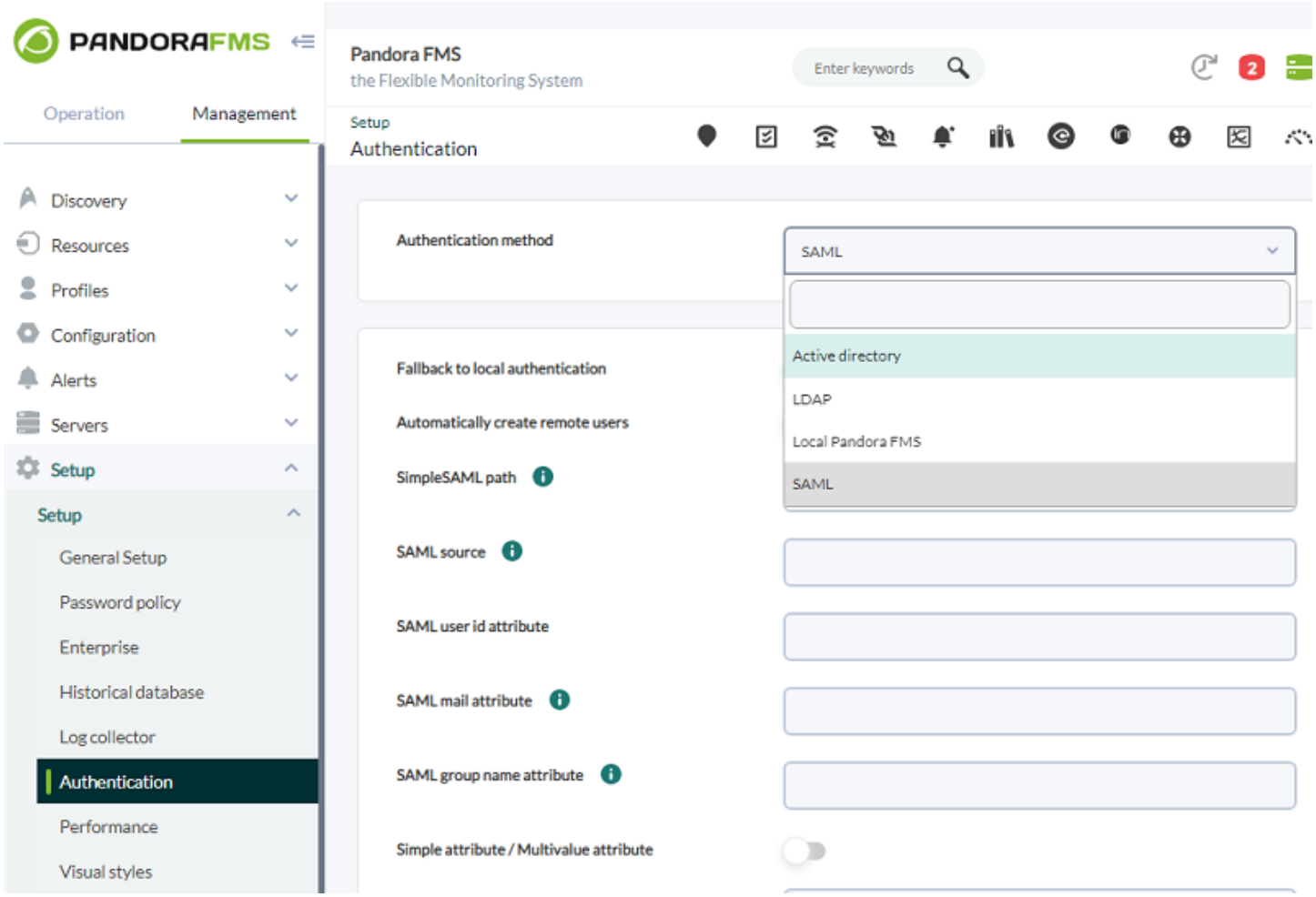
SAML Single Sign-On with Pandora FMS

SAML is an open XML-based authentication and authorization standard. Pandora FMS can work as a service provider with its internal SAML identity provider.

Administrators always authenticate against the local database.

Configuring Pandora FMS

It will be necessary to go to Management → Setup → Setup → Authentication and select SAML under Authentication method.



Configuring the service provider

To configure the service provider you will need to download SimpleSamlphp and install it in `/opt/simplesamlphp/`.

It will be necessary to configure an *endpoint* to manage the authentications at `/simplesaml`:

```
ln -s /opt/simplesamlphp/www /var/www/html/simplesaml
```

You will need to add your SP in `/opt/simplesamlphp/config/authsources.php`:

```
'test-sp' => [
       'saml:SP',
       'entityID' => 'http://app.example.com',
       'idp' => 'http://172.16.0.3:8080/simplesaml/saml2/idp/metadata.php',
   ],
```

The metadata of the `idP`:

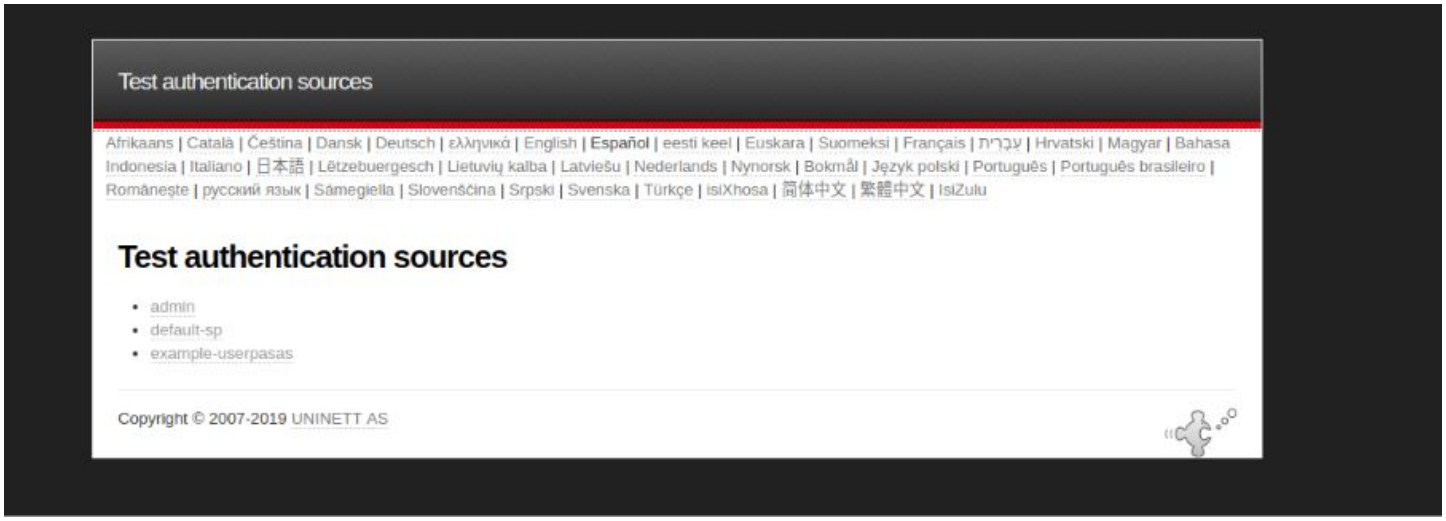
```
$metadata['http://172.16.0.3:8080/simplesaml/saml2/idp/metadata.php'] = array(
       'name' => array(
           'en' => 'Test IdP',
       ),
       'description' => 'Test IdP',
       'SingleSignOnService' =>
'http://172.16.0.3:8080/simplesaml/saml2/idp/SSOService.php',
       'SingleLogoutService' =>
'http://172.16.0.3:8080/simplesaml/saml2/idp/SingleLogoutService.php',
       'certFingerprint' => '119b9e027959cdb7c662cfd075d9e2ef384e445f',
   );
```

It is recommended to use certificate validation with direct certificate instead of `certFingerprint`.

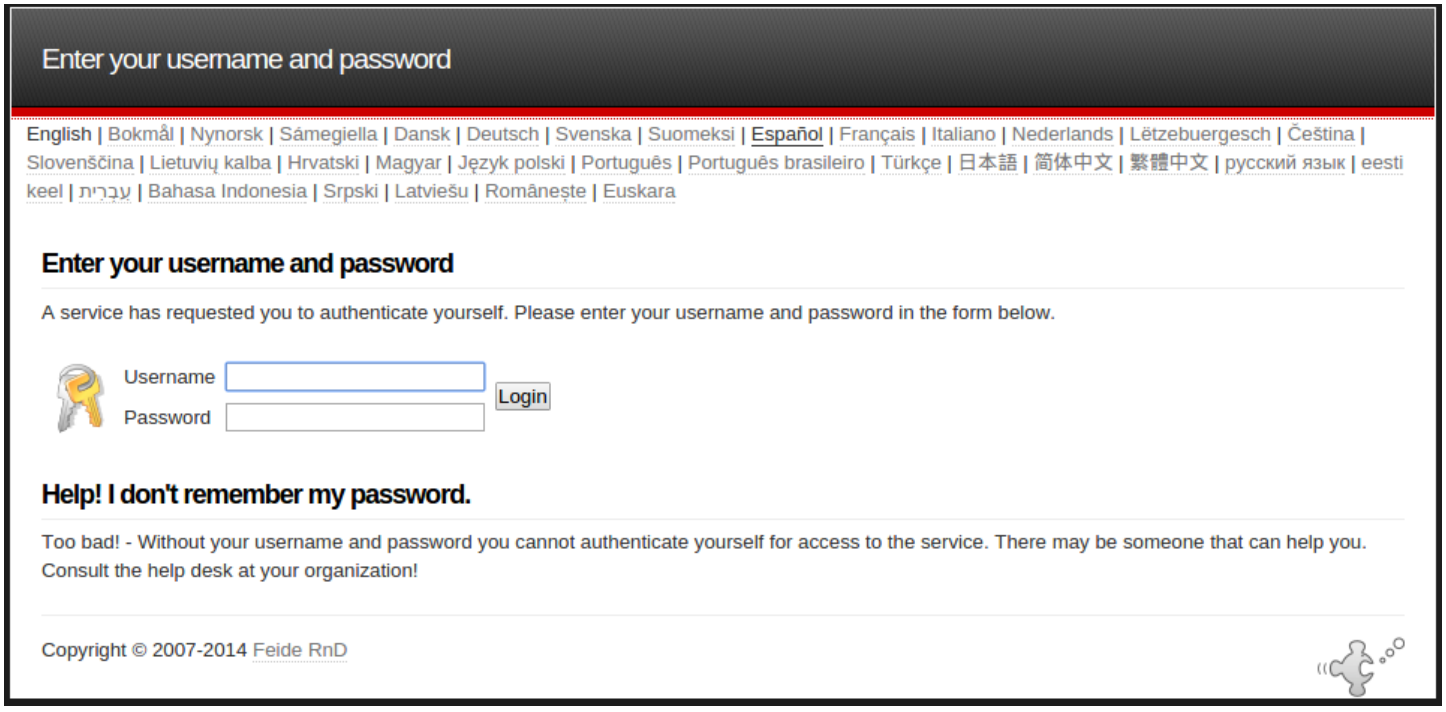
It is necessary to make sure that the file `/opt/simplesamlphp/lib/_autoload.php` exists.

Once simplesamlphp is installed, you can check if the *login* works directly in SAML. To do this, access the following IP address and select the authentication source.

```
http://<IP_ADDRESS>/simplesaml/module.php/core/authenticate.php
```



A *login* screen like the one below will appear where you will enter a SAML user and password that you created.



If the *login* is correct, a summary screen will appear with all the user's attributes.

The guide is also available at SimpleSAMLphp Service Provider QuickStart.

Configuring your identity provider

In order to properly generate SAML users in Pandora FMS, it is necessary to define in each one of them the following identification attributes that appear in the SAML configuration:

- Failback to local authentication: If disabled, it will not allow any users to log in that do not exist in SAML (except superadmin users). If authentication against SAML fails and this option is disabled, it

will not query the server database.
- Automatically create remote users: It will automatically create users when you log in for the first time using SAML in the tool. If disabled, it must be created manually beforehand.
- SimpleSAML path: It configures the path to the folder where the directory is located `simplesamlphp`.
- SAML Source: Name of the SAML source against which the requests are to be made. The name must match the source selected in:

```
http://<IP_ADDRESS>/simplesaml/module.php/core/authenticate.php
```

- SAML user id attribute: The field retrieved from SAML to be used as username (e.g. uid).
- SAML mail attribute: The field retrieved from SAML to be used as the user's email (e.g. email).
- SAML group name attribute: The field retrieved from SAML to be used as the user's group (e.g. group1PersonAffiliation).
- Profile attribute: The field retrieved from SAML to be used as a profile on user group (e.g. urn:profile_example:Operator Read).
- Simple attribute / Multivalue attribute: Option that allows to select whether to use a simple attribute for the Profile and Tag fields in Pandora FMS or a multivalue attribute.

In the case of choosing Simple attribute two new fields called Profile attribute and Tag attribute will appear where the names of the SAML attributes that will coincide with the name of the Profile and Tag in Pandora FMS when they are created will be selected.

When Multivalue attribute is selected, an attribute following this format must be used:

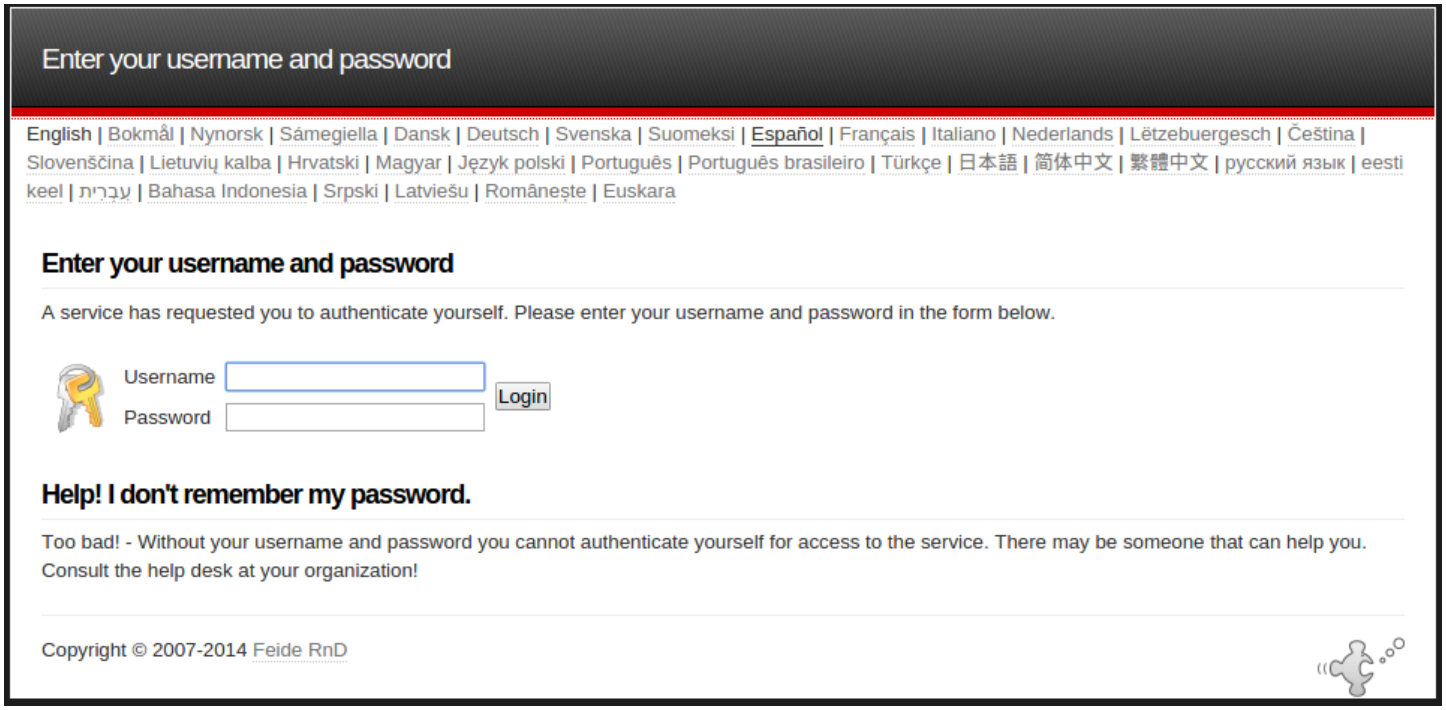
```
<Attribute Name="MULTIVALUE_ATTRIBUTE">
<AttributeValue>PREFIX:role:rolename</AttributeValue>
<AttributeValue>PREFIX:tag:tagname</AttributeValue>
</Attribute>
```

Once the attribute in the SAML is created and selected this way with the configuration in Pandora FMS, the following parameters will be indicated:

- SAML profiles and tag attribute: Name of the multivalue attribute.
- SAML profile and tags prefix: Prefix that will go before the role and tag keys in the attribute value. In the case of `urn:pfms:role:< rolename >` and `urn:pfms:tag:`, the prefix `urn:pfms` should be configured.

Login

It will be necessary to navigate in Pandora FMS Console and click on the Login button. It will redirect to the identity provider.



After a successful login you will be redirected back to Pandora FMS Console.

Back to Pandora FMS Documentation Index