SAML Single Sign-On with Pandora FMS

From:
https://pandorafms.com/manual/!777/
Permanent link:
https://pandorafms.com/manual/!777/en/documentation/pandorafms/technical_annexes/12_saml
2024/10/03 18:41

SAML Single Sign-On with Pandora FMS

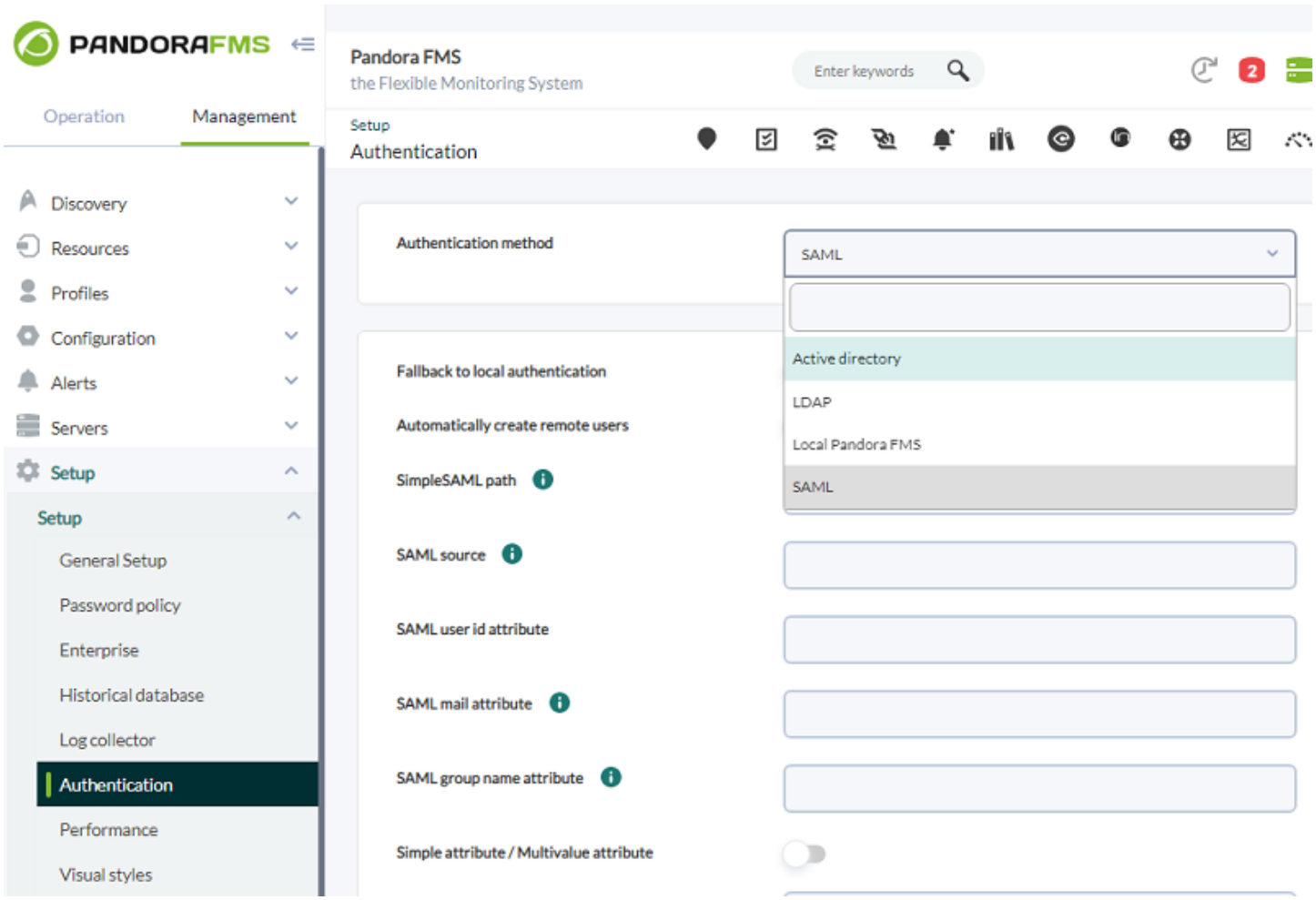
SAML Single Sign-On with Pandora FMS

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

Administrators are always authenticated against the local database.

Configuring Pandora FMS

Go to Management → Setup → Setup → Authentication and select SAML under Authentication method.



Configuring the service provider

To configure the service provider, first download SimpleSamlphp and install it in

/opt/simplesamlphp/.

Configure an *endpoint* to manage authentications in /simplesaml:

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

Add yous SP to authsources /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',
   ],
```

Register the IdP metadata:

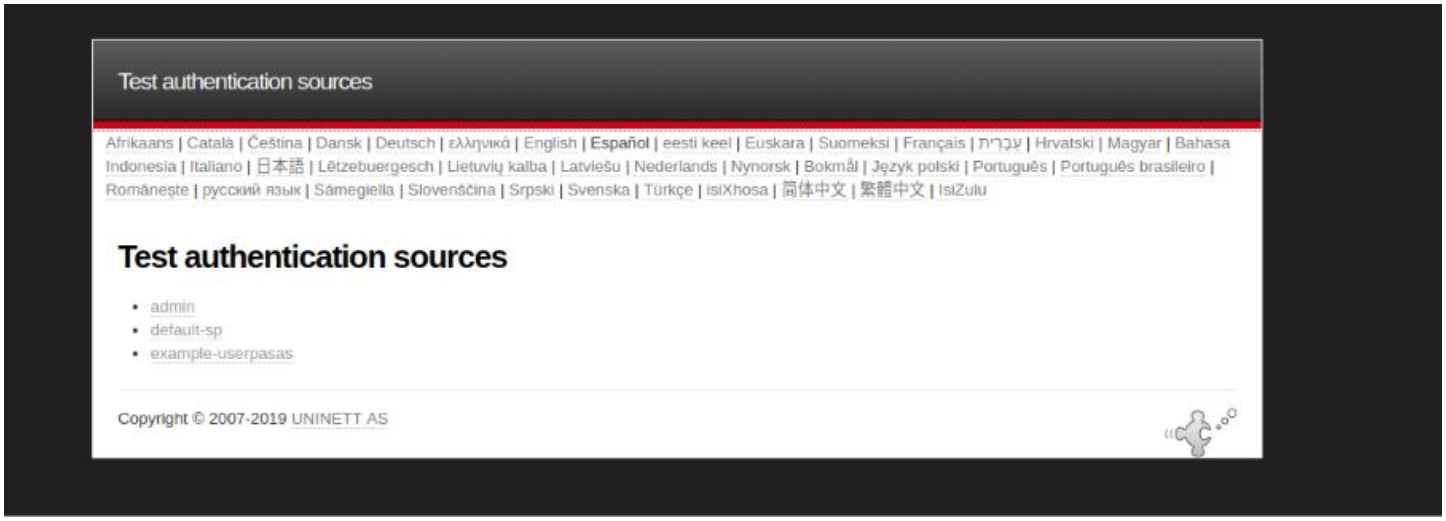
```
$metadata['http://172.16.0.3:8080/simplesaml/saml2/idp/metadata.php'] = array(
       'name' => array(
           'en' => 'Test IdP',
       ),
       'description' => 'Test IdP',
       'SingleSignOnService' =>
'http://172.16.0.3:8080/simplesaml/saml2/idp/SSOService.php',
       'SingleLogoutService'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

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

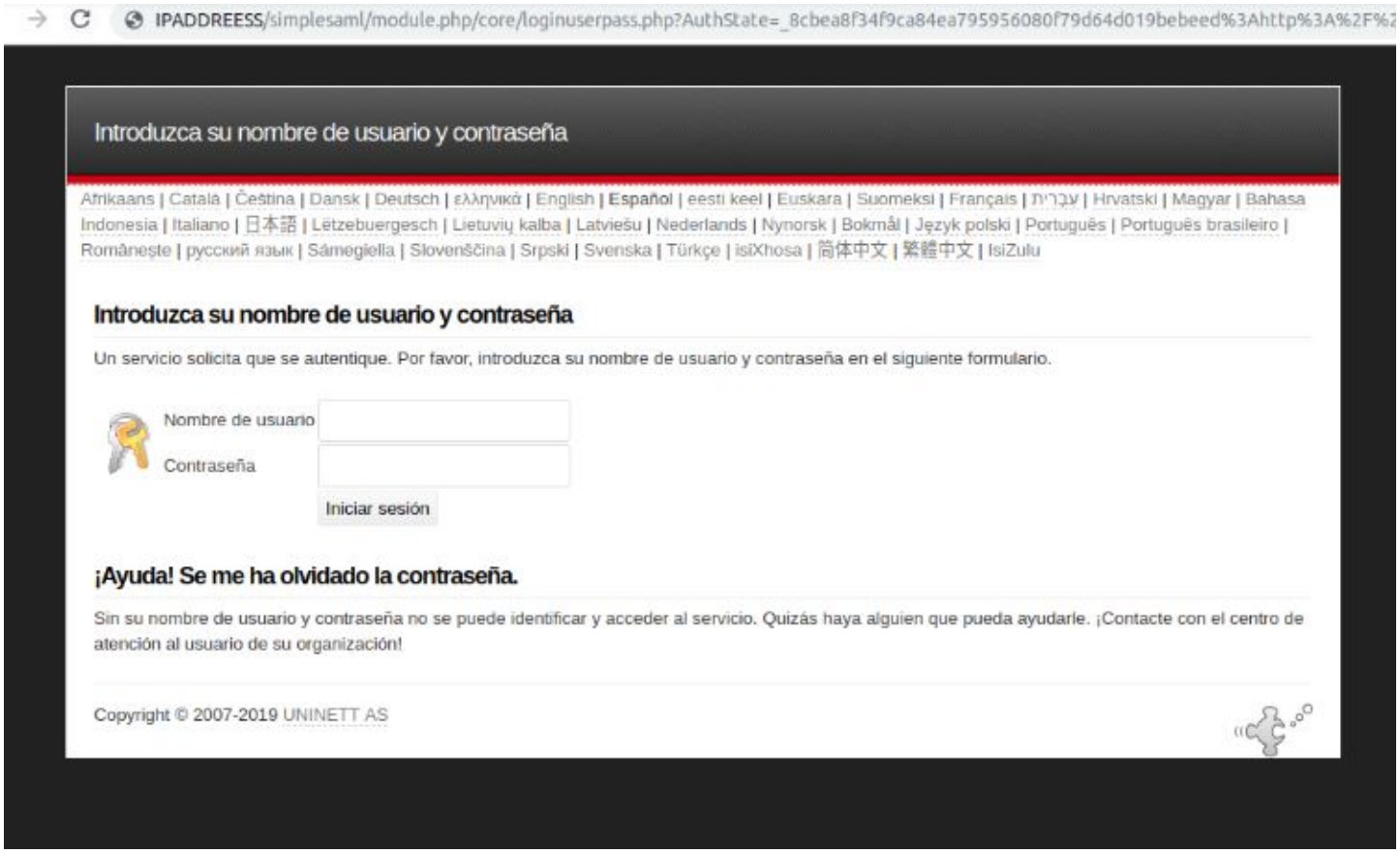
Make sure the file */opt/simplesamlphp/lib/_autoload.php* existd.

Once simplesamlphp is installed, check whether the login works directly in saml. For that purpose, go to the following IP and select the authentication source.

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



A login screen like the following will appear, where to enter the saml user and password you created.

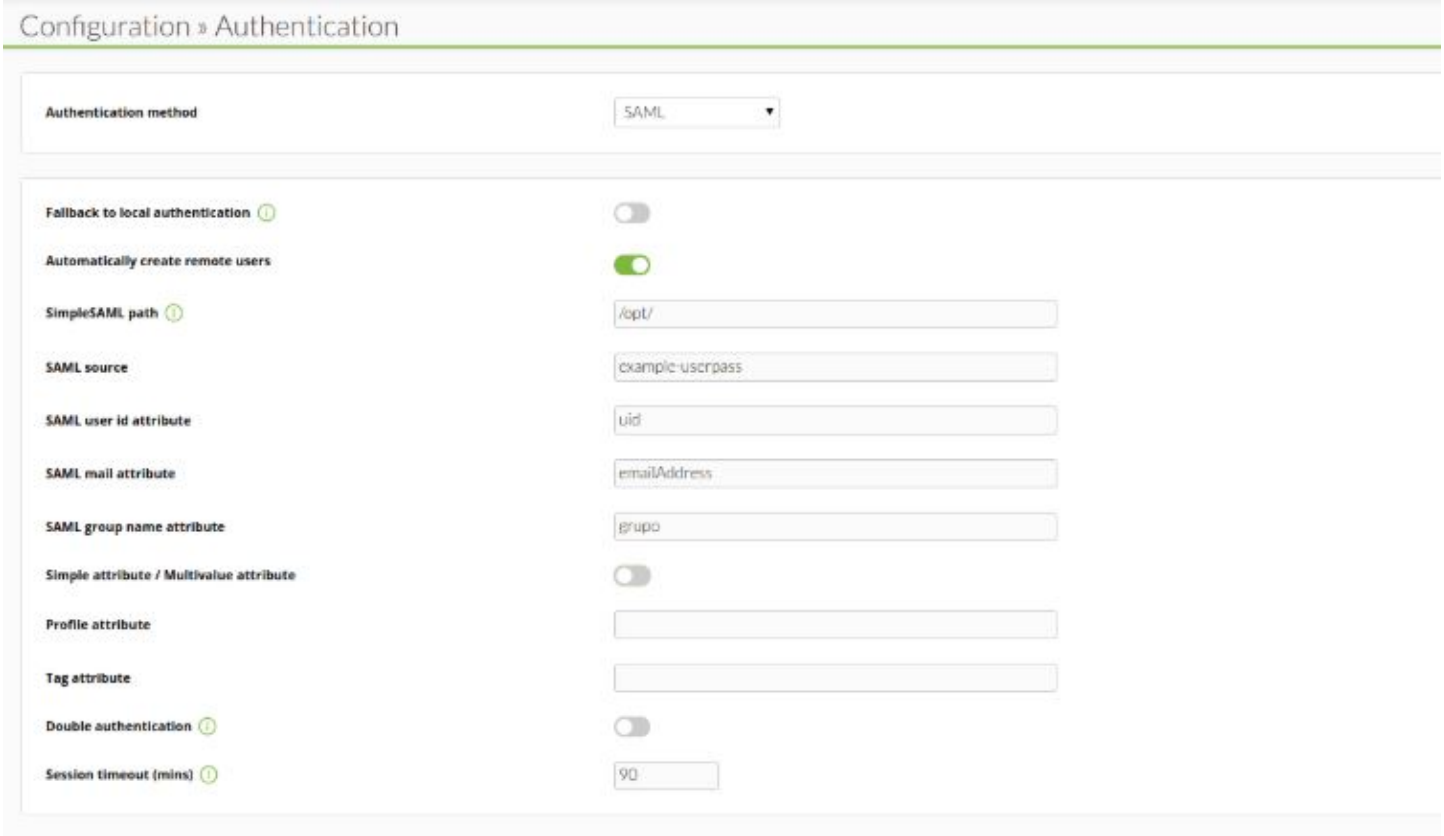


If the login is correct, a summary screen with all user attributes will appear.

You also have this guide available: SimpleSAMLphp Service Provider QuickStart.

Configuring your identity provider

For SAML users to be correctly generated in Pandora FMS, it is necessary to define in each and every one of them the following identifying attributes that appear in SAML configuration:



- Failback to local authentication> If disabled, it will not allow any user that does not exist in SAML to log in (except for tool administrator users). In case the authentication against SAML fails and this option is disabled, it will not check the server database.
- Automatically create remote users> It will create users automatically when logging in the tool for the first time through SAML. In case of it being disabled, it must have been previously created manually.
- SimpleSAML path> It configures the path to the folder where the directory simplesamlphp is located.
- SAML Source> Name of the SAML source where queries will be send to. The name must match the source selected in:

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

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

In case of using Simple attribute, two new fields called Profile attribute and Tag attribute will appear, where you may select the names of the SAML attributes that match the Profile and Tag name in Pandora FMS when created.

When selecting Multivalue attribute, use an attribute that follows this format:

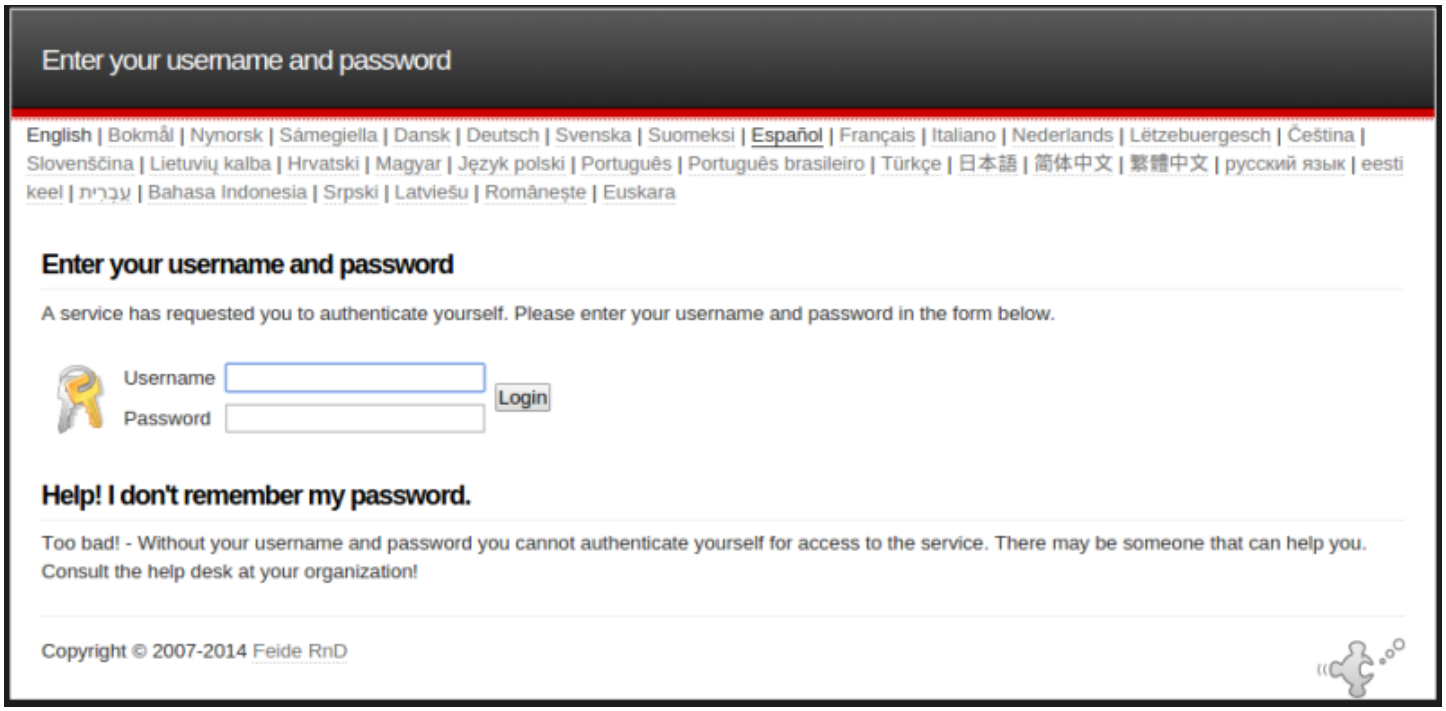
```
<Attribute Name="MULTIVALUE_ATTRIBUTE">
<AttributeValue>PREFIX:role:rolename</AttributeValue>
<AttributeValue>PREFIX:tag:tagname</AttributeValue>
</Attribute>
```

Once this attribute is created in SAML and selected in such a way, together with Pandora FMS configuration, it will indicate the following parameters:

- SAML profiles and tag attribute> Name of the multivalue attribute.
- SAML profile and tags prefix> Prefix that will precede the role and tag key in the value attribute. In case it is urn:artica:role:<rolename> and urn:artica:tag:<tagname> the urn:artica prefix must be configured.

Logging in

Go to Pandora FMS Console and click *Login*. You will be redirected to your identity provider.



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

Go back to Pandora FMS documentation index