



SAML Single Sign-On avec Pandora FMS



From:

<https://pandorafms.com/manual/!current/>

Permanent link:

https://pandorafms.com/manual/!current/fr/documentation/pandorafms/technical_annexes/12_saml

2024/06/10 14:36



SAML Single Sign-On avec Pandora FMS

SAML Single Sign-On avec Pandora FMS

SAML est une norme ouverte d'authentification et d'autorisation basée sur XML. Pandora FMS peut fonctionner comme un fournisseur de services avec votre fournisseur d'identité SAML interne.

Les administrateurs s'authentifient toujours contre la base de données locale.

Configuration de Pandora FMS

Vous devrez aller vers Management → Setup → Setup → Authentication et sélectionner SAML dans Authentication method.

The screenshot displays the Pandora FMS web interface. The top navigation bar includes the Pandora FMS logo, the text 'Pandora FMS the Flexible Monitoring System', a search bar with the placeholder 'Enter keywords', and several utility icons. Below the navigation bar, there are two tabs: 'Operation' and 'Management'. The left sidebar menu is expanded to show the 'Setup' section, with 'Authentication' selected. The main content area is titled 'Setup Authentication' and contains the following configuration options:

- Authentication method:** A dropdown menu with 'SAML' selected.
- Fallback to local authentication:** A checkbox that is currently unchecked.
- Automatically create remote users:** A checkbox that is currently unchecked.
- SimpleSAML path:** A text input field with an information icon.
- SAML source:** A text input field with an information icon.
- SAML user id attribute:** A text input field.
- SAML mail attribute:** A text input field with an information icon.
- SAML group name attribute:** A text input field with an information icon.
- Simple attribute / Multivalue attribute:** A toggle switch that is currently turned off.

Configuration du fournisseur de services

Pour configurer le fournisseur de services, téléchargez [SimpleSamlphp](#) et l'installez dans

/opt/simplesamlphp/.

Configurez un *endpoint* pour gérer les authentifications dans /simplesaml :

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

Ajoutez votre SP à 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',  
    ],
```

Enregistrez les métadonnées de l'IdP :

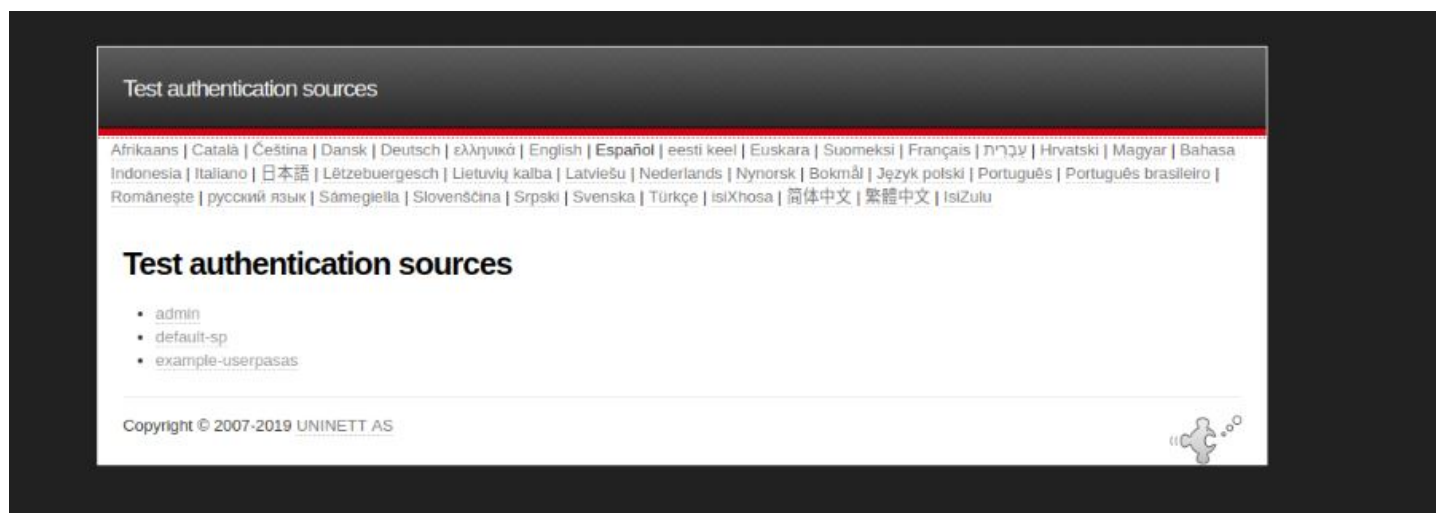
```
$metadata['http://172.16.0.3:8080/simplesaml/saml2/idp/metadata.php'] = array(  
    'name' => array(  
        'en' => 'Test IdP',  
    ),  
    'description' => 'Test IdP',  
    'SingleSignOnService' =>  
'http://172.16.0.3:8080/simplesaml/saml2/idp/SSOService.php',  
    'SingleLogoutService'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

Il est recommandé d'utiliser la validation de certificat avec `certFingerprint` direct au lieu de `certFingerprint`.

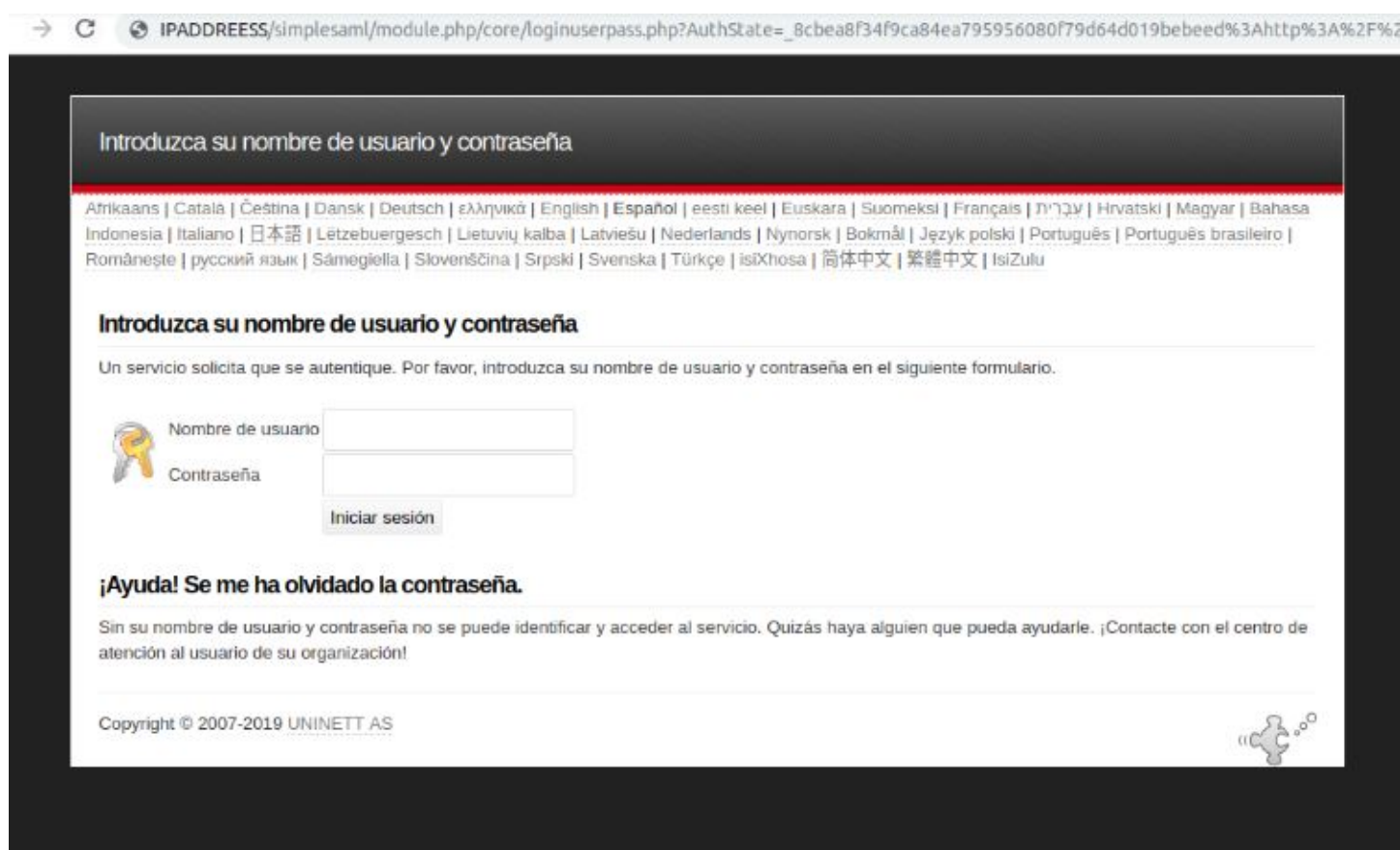
Vous devez vous assurer que le fichier `/opt/simplesamlphp/lib/_autoload.php` existe.

Une fois que vous avez installé `simplesamlphp`, vérifiez si le login fonctionne directement dans le `saml`. Pour ce faire, accédez à l'adresse IP suivante et sélectionnez la source d'authentification.

```
http:///simplesaml/module.php/core/authenticate.php
```



Un écran de connexion apparaîtra comme le suivant où un utilisateur et un mot de passe saml que vous avez créés seront entrés.



Si le login est correct, un écran récapitulatif apparaîtra avec tous les attributs de l'utilisateur.

Le guide est également disponible sur [SimpleSAMLphp Service Provider QuickStart](#).

Configurer votre fournisseur d'identité

Pour que les utilisateurs de SAML soient générés correctement dans Pandora FMS, il est nécessaire de définir dans chacun d'eux les attributs d'identification suivants qui apparaissent dans les

paramètres SAML :

Configuration » Authentication

Authentication method: SAML

Fallback to local authentication

Automatically create remote users

SimpleSAML path

SAML source

SAML user id attribute

SAML mail attribute

SAML group name attribute

Simple attribute / Multivalue attribute

Profile attribute

Tag attribute

Double authentication

Session timeout (mins)

- Fallback to local authentication> Si elle est désactivée, elle ne permet pas à un utilisateur qui n'existe pas dans SAML de se connecter (à l'exception des utilisateurs administrateurs de l'outil). Dans le cas où l'authentification contre SAML échoue et que cette option est désactivée, elle ne sera pas consultée dans la base de données du serveur.
- Automatically create remote users> Crée automatiquement les utilisateurs lors de leur première connexion à l'aide de SAML dans l'outil. S'il est désactivé, il doit être créé manuellement à l'avance.
- SimpleSAML path> Configure le chemin vers le dossier où se trouve le répertoire simplesaml.php.
- SAML Source> Nom de la source SAML contre laquelle nous souhaitons faire des demandes. Le nom doit correspondre à la source que vous avez sélectionnée dans :

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

- SAML user id attribute> Le champ récupéré à partir de SAML qui sera utilisé comme nom d'utilisateur (par exemple uid).
- SAML mail attribute> Le champ récupéré à partir de SAML qui sera utilisé comme nom d'utilisateur (par exemple email).
- SAML group name attribute> Le champ récupéré à partir de SAML qui sera utilisé comme groupe utilisateur (par exemple group1PersonAffiliation).
- Profile attribute> Le champ récupéré de SAML qui sera utilisé comme profil de groupe de l'utilisateur (par exemple urn:profile_example:Operator Read).
- Simple attribute / Multivalue attribute> Option qui vous permet de sélectionner si vous voulez utiliser un attribut simple pour les champs Profil et Tag dans Pandora FMS ou un attribut multi-valeur.

Si vous choisissez Simple attribute, deux nouveaux champs appelés Profile attribute et Tag attribute apparaîtront, où les noms des attributs SAML seront sélectionnés pour correspondre au nom du Profil et Tag dans Pandora FMS lors de sa création.

Lorsque vous sélectionnez Multivalue attribute vous devez utiliser un attribut qui suit ce format :

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

Une fois l'attribut dans le SAML créé et sélectionné de cette manière avec la configuration dans Pandora FMS, les paramètres suivants seront indiqués :

Simple attribute / Multivalue attribute

SAML profiles and tag attribute

SAML profile and tags prefix

- SAML profiles and tag attribute> Nom de l'attribut multivaleur.
- SAML profile and tags prefix> Préfixe qui précède la clé de rôle et la balise dans la valeur de l'attribut. Si c'est urn:artica:role: et urn:artica:tag:, il faut configurer le préfixe urn:artica.

Ouverture de session


Vous devrez naviguer dans la console Pandora FMS et cliquer sur *Login*. Vous serez redirigé vers le fournisseur d'identité.

Enter your username and password

[English](#) | [Bokmål](#) | [Nynorsk](#) | [Sámegiella](#) | [Dansk](#) | [Deutsch](#) | [Svenska](#) | [Suomeksi](#) | [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](#)

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.




Username

Password

Help! I don't remember my password.

Too bad! - Without your username and password you cannot authenticate yourself for access to the service. There may be someone that can help you. Consult the help desk at your organization!

Copyright © 2007-2014 Feide RnD



Après une connexion réussie, vous serez redirigé vers la console Pandora FMS.



[Retour à l'index de documentation Pandora FMS.](#)