Pandora FMS での SAML シングルサインオン

Pandora FMS での SAML シングルサインオン

Pandora FMS ドキュメント一覧に戻る

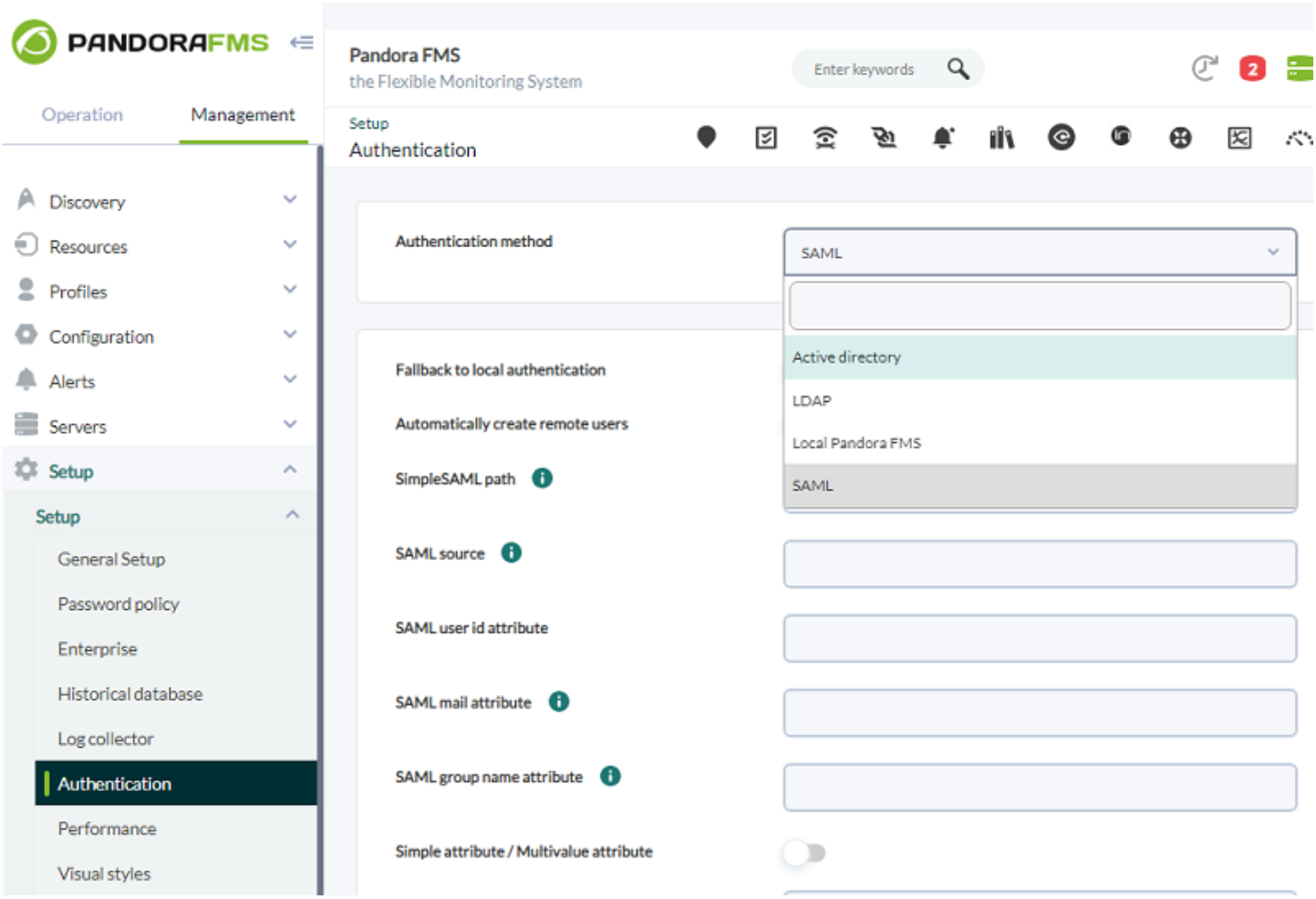
Pandora FMS での SAML シングルサインオン

SAML は、XML をベースにした、認証のためのオープンな標準規格です。Pandora FMS は、内部の SAML IdP(ID プロバイダ) と共に、SP (サービスプロバイダ) として動作します。

管理者は常にローカルのデータベースで認証されます。

Pandora FMS の設定

管理(Management) → セットアップ(Setup) → セットアップ(Setup) → 認証(Authentication) へ行き、認証方法(Authentication method) で SAML を選択します。



サービスプロバイダ設定

サービスプロバイダの設定をするには、最初に SimpleSamlphp をダウンロードし、/opt/simplesamlphp/ にインストールします。

/simplesaml の認証管理のために、*endpoint* を設定します。

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

authsources /opt/simplesamlphp/config/authsources.php に SP を追加します。

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

IdP メタデータを登録します。

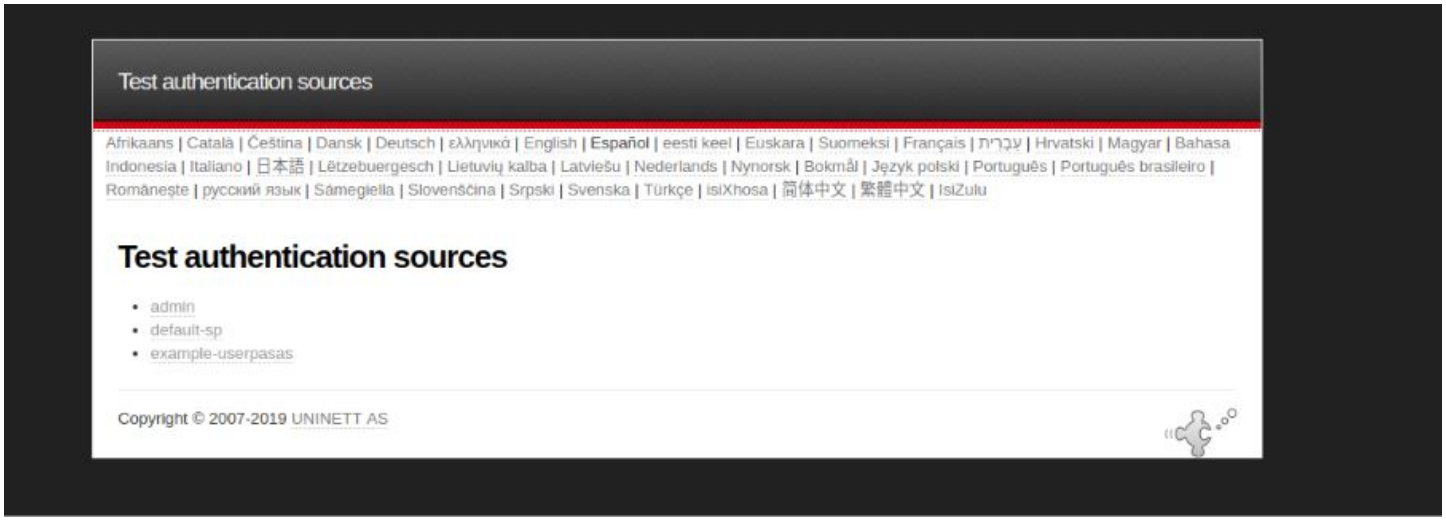
```
$metadata['http://172.16.0.3:8080/simplesaml/saml2/idp/metadata.php'] = array(
       'name' => array(
           'en' => 'Test IdP',
       ),
       'description' => 'Test IdP',
       'SingleSignOnService' =>
'http://172.16.0.3:8080/simplesaml/saml2/idp/SSOService.php',
       'SingleLogoutService'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

certFingerprint の代わりに、直接認証を使用した認証の検証を使用することをお勧めします。

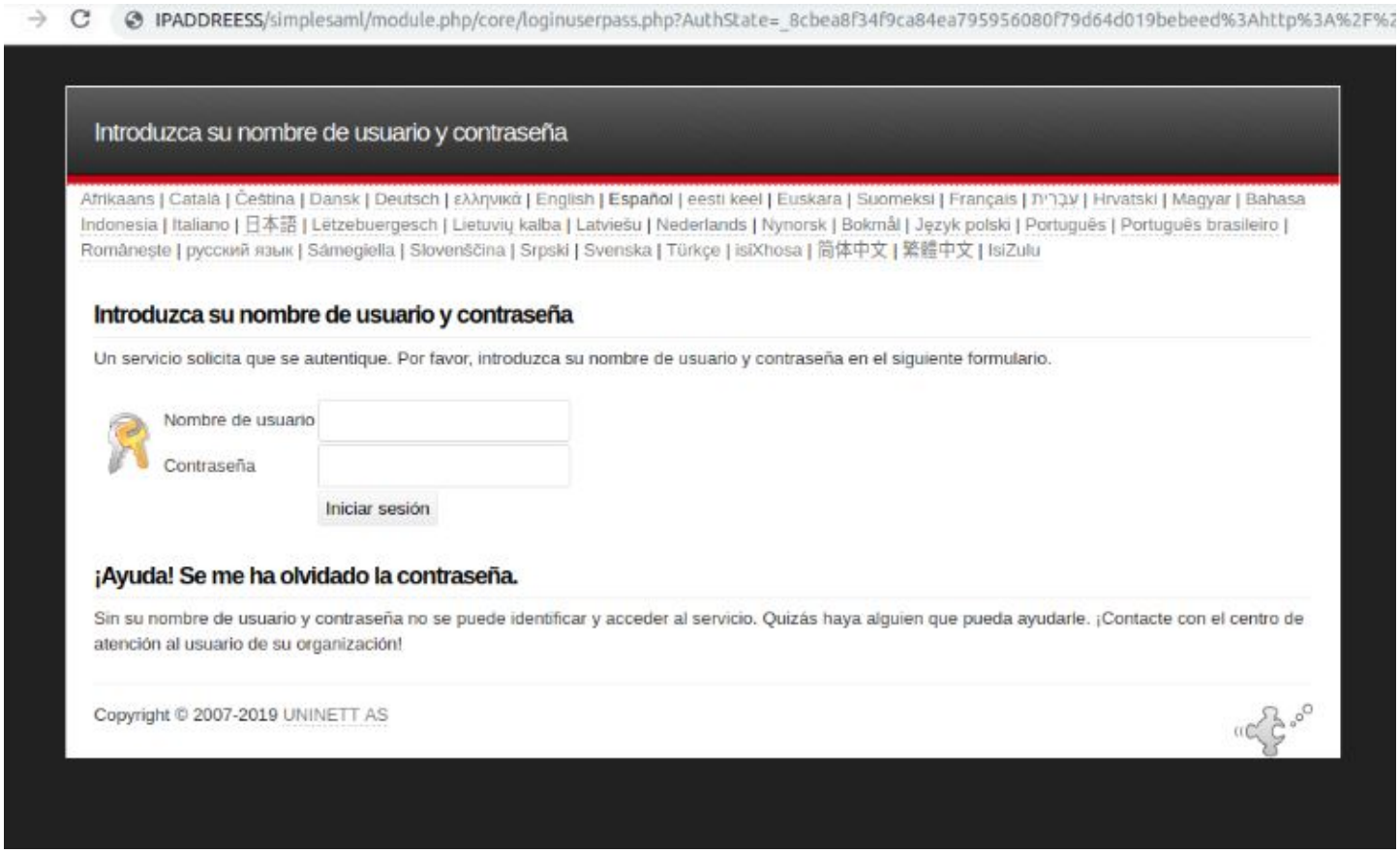
/opt/simplesamlphp/lib/_autoload.php ファイルが存在することを確認します。

simplesamlphp をインストールしたらsaml でのログインが正しく動作するかを確認します。それには、以下にアクセスし認証元を選択します。

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



次のようなログイン画面が表示されるので、saml ユーザとパスワードを入力します。

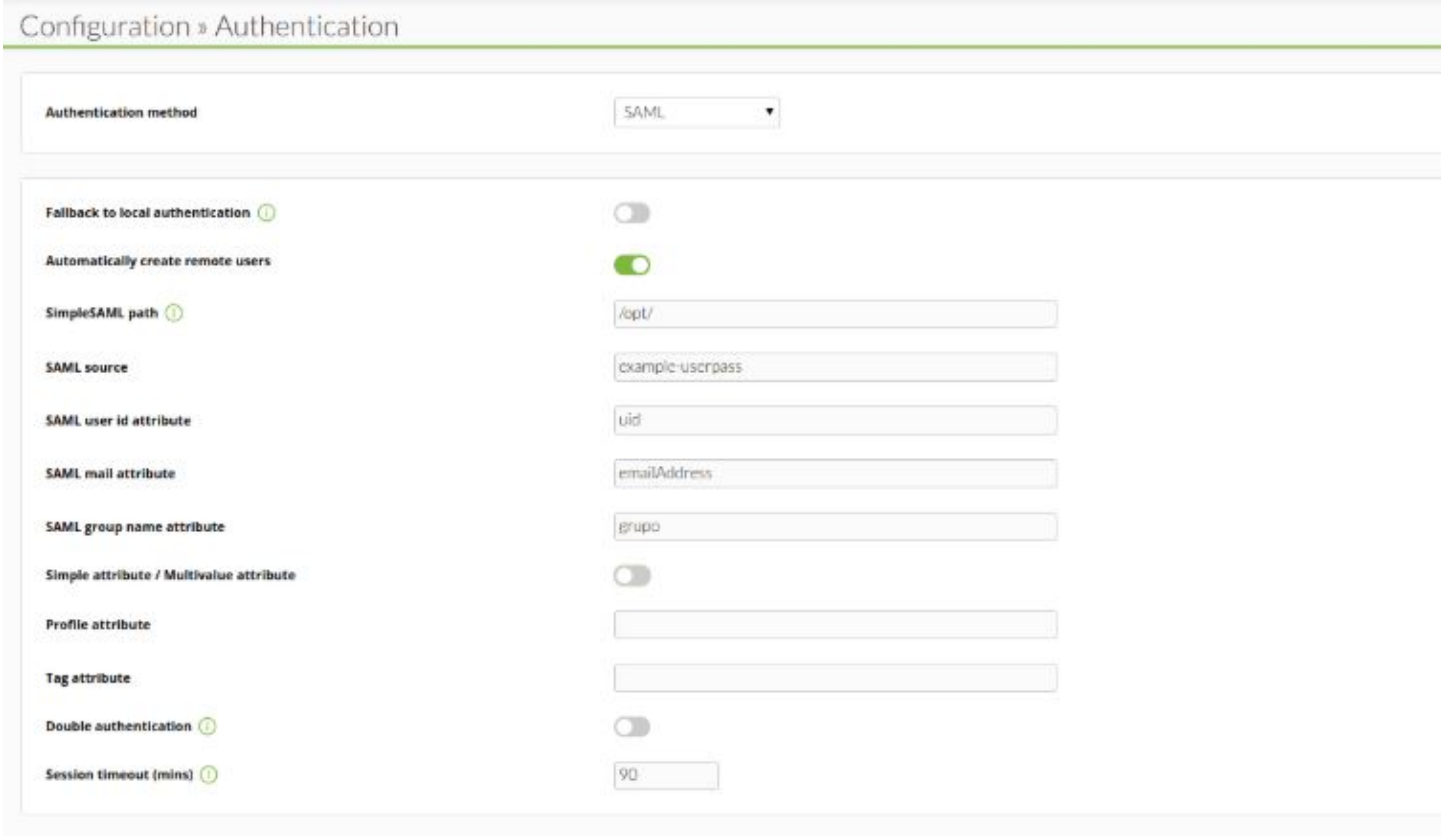


正しくログインできると、すべてのユーザ属性を含む概要画面が表示されます。

こちらのガイドも参考にしてください。SimpleSAMLphp Service Provider QuickStart.

IDプロバイダの設定

SAML ユーザが Pandora FMS で正しく生成されるためには、SAML 設定に表示される次の識別属性をすべてのユーザに定義する必要があります。



- **ローカル認証へのフォールバック**(Failback to local authentication): 無効にすると、saml に存在しないユーザはログインできなくなります(管理者ユーザを除く)。saml に対する認証が失敗した際、このオプションが無効になっているとサーバのデータベース上のアカウントはチェックされません。
- **リモートユーザの**自動作成(Automatically create remote users): saml を使用した初回ログイン時に、ユーザを自動的に作成します。無効にする場合は、事前に手動でユーザを作成しておく必要があります。
- SimpleSAML パス(SimpleSAML path): simplesamlphp がインストールされているディレクトリのパスです。
- SAML ソース(SAML Source): クエリが送られる SAML ソースの名前です。名前は以下で選択したソースにマッチする必要があります。

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

- SAML ユーザ ID 属性(SAML user id attribute): ユーザ名として利用される SAML フィールドです。(例: uid)
- SAML メール属性(SAML mail attribute): ユーザのメールとして使われる SAML フィールドです。(例: email)
- SAML グループ名属性(SAML group name attribute): ユーザグループとして使われる SAML フィールドです。(例: group1PersionAffiliation)
- 単一属性/複数属性(Simple attribute / Multivalue attribute): ユーザグループのプロファイルとして使われる SAML フィールドです。(例: nowiki>urn:profile_example:Operator Read)

単一属性の利用を選択した場合は、プロファイル属性(Profile attribute) および タグ属性(Tag attribute)が表示されます。そこで、Pandora FMS のプロファイルおよびタグにマッチする SAML 属性を選択します。

複数属性を選択したときは、以下のフォーマットで属性を指定します。

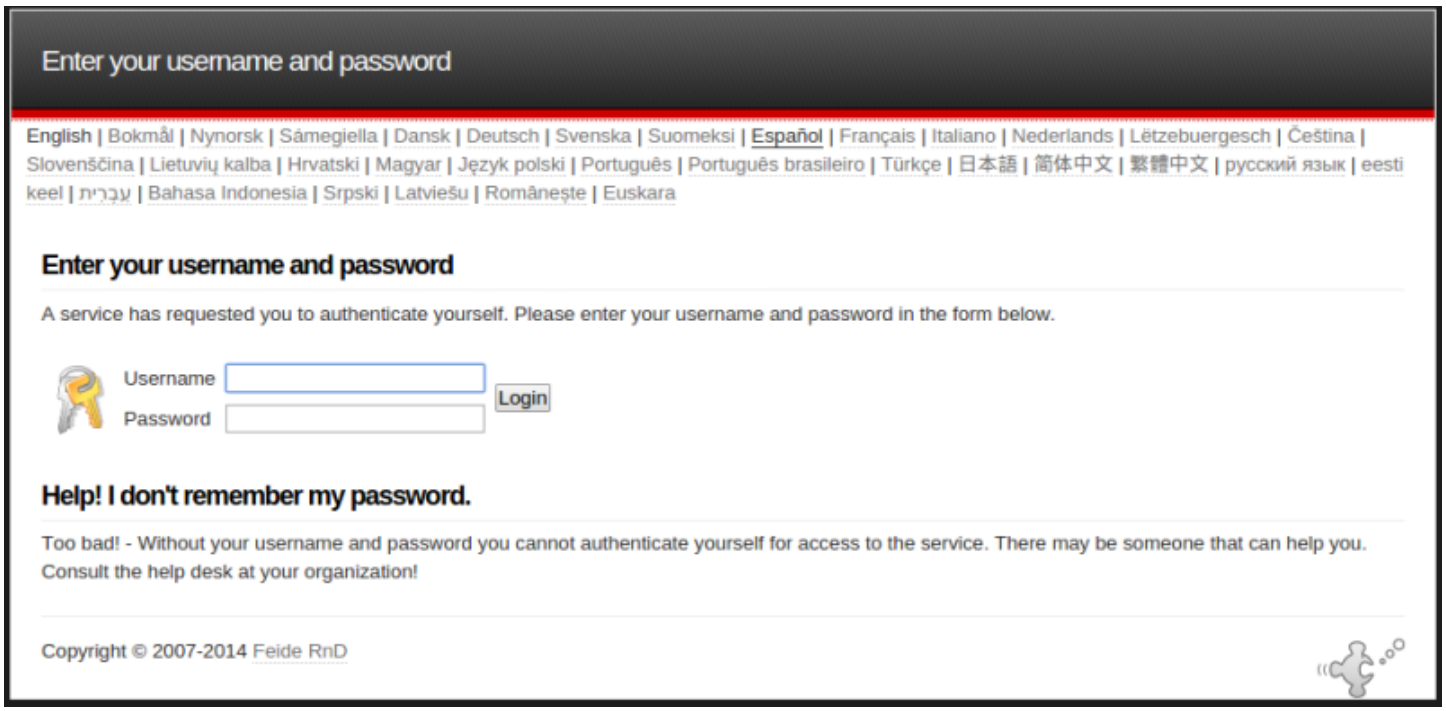
```
<Attribute Name="MULTIVALUE_ATTRIBUTE">
<AttributeValue>PREFIX:role:rolename</AttributeValue>
<AttributeValue>PREFIX:tag:tagname</AttributeValue>
</Attribute>
```

属性を SAML で作成し、Pandora FMS の設定を行うと、次のパラメータが表示されます。

- SAML プロファイルおよびタグ属性: 複数属性の名前。
- SAML プロファイルおよびタグプレフィックス(SAML profile and tags prefix): 値の属性の役割およびタグキーの前につくプレフィックス。urn:artica:role:<rolename> および urn:artica:tag:<tagname> の場合。urn:artica プレフィックスを設定する必要があります。

ログイン

Pandora FMS コンソールへ行き、*ログイン* ボタンをクリックします。ID プロバイダへリダイレクトされます。



ログインに成功すると、Pandora FMS コンソールにリダイレクトされ戻ってきます。