SAML Single Sign-On con Pandora FMS

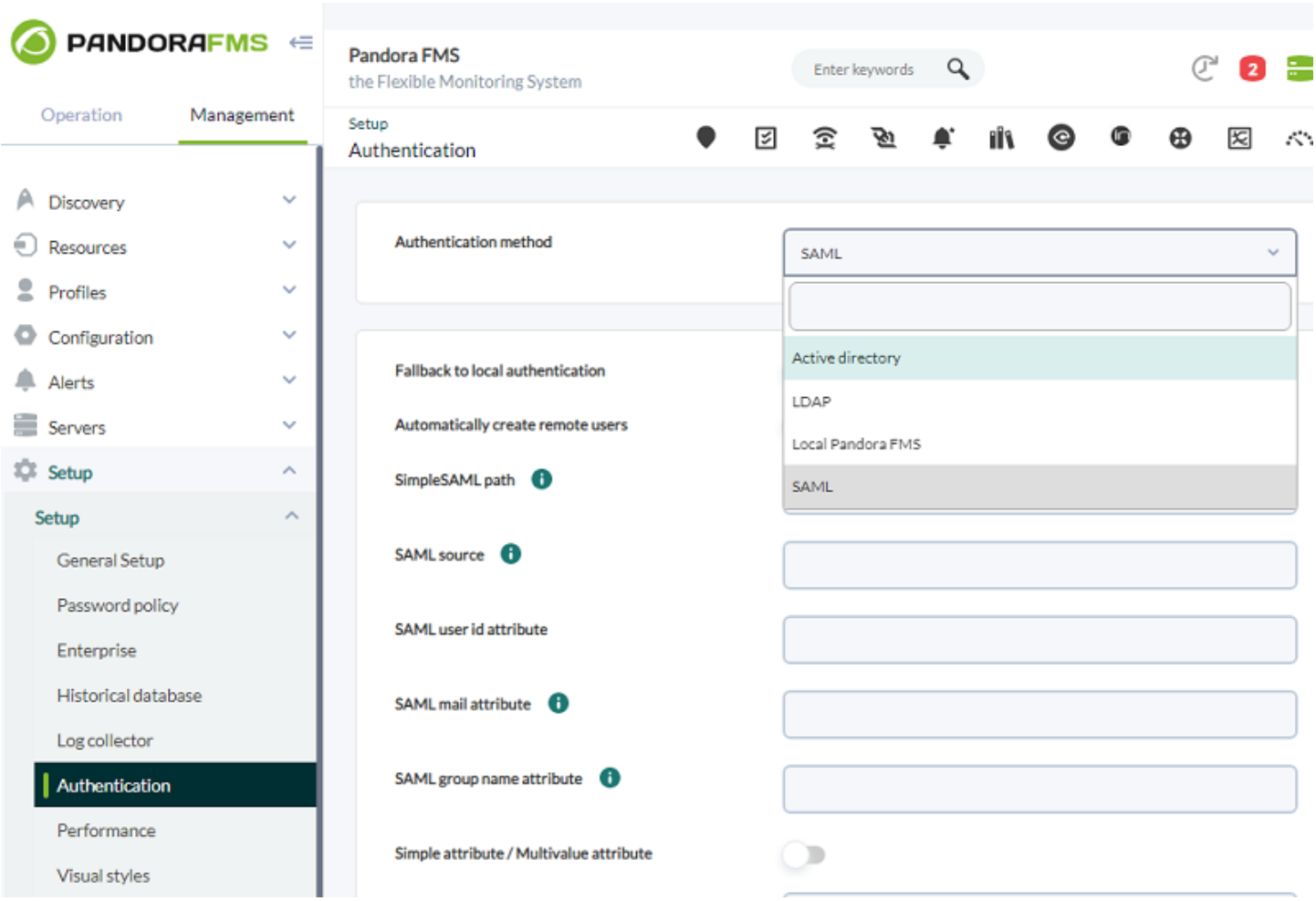
SAML Single Sign-On con Pandora FMS

SAML es un estándar abierto de autenticación y autorización basado en XML. Pandora FMS puede funcionar como un proveedor de servicios con su proveedor de identidades SAML interno.

Los administradores siempre se autentican contra la base de datos local.

Configurando Pandora FMS

Será necesario ir a Management → Setup → Setup → Authentication y seleccione SAML bajo Authentication method.



Configurando el proveedor de servicios

Para configurar el proveedor de servicios habrá que descargar SimpleSamlphp e instalarlo en `/opt/simplesamlphp/`.

Será necesario configurar un *endpoint* para gestionar las autentificaciones en `/simplesaml`:

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

Tendrá que agregar su SP en `/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',
   ],
```

Habrá que registrar los metadatos del IdP:

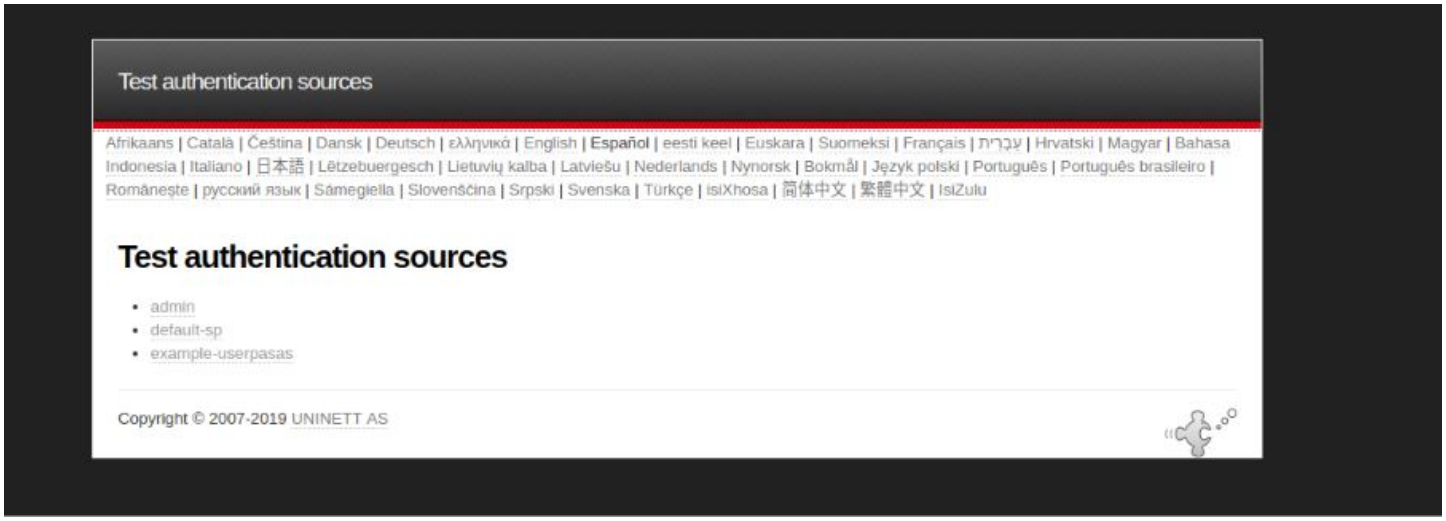
```
$metadata['http://172.16.0.3:8080/simplesaml/saml2/idp/metadata.php'] = array(
       'name' => array(
           'en' => 'Test IdP',
       ),
       'description' => 'Test IdP',
       'SingleSignOnService' =>
'http://172.16.0.3:8080/simplesaml/saml2/idp/SSOService.php',
       'SingleLogoutService'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

Se recomienda utilizar la validación de certificado con
certificado directo en vez de certFingerprint.

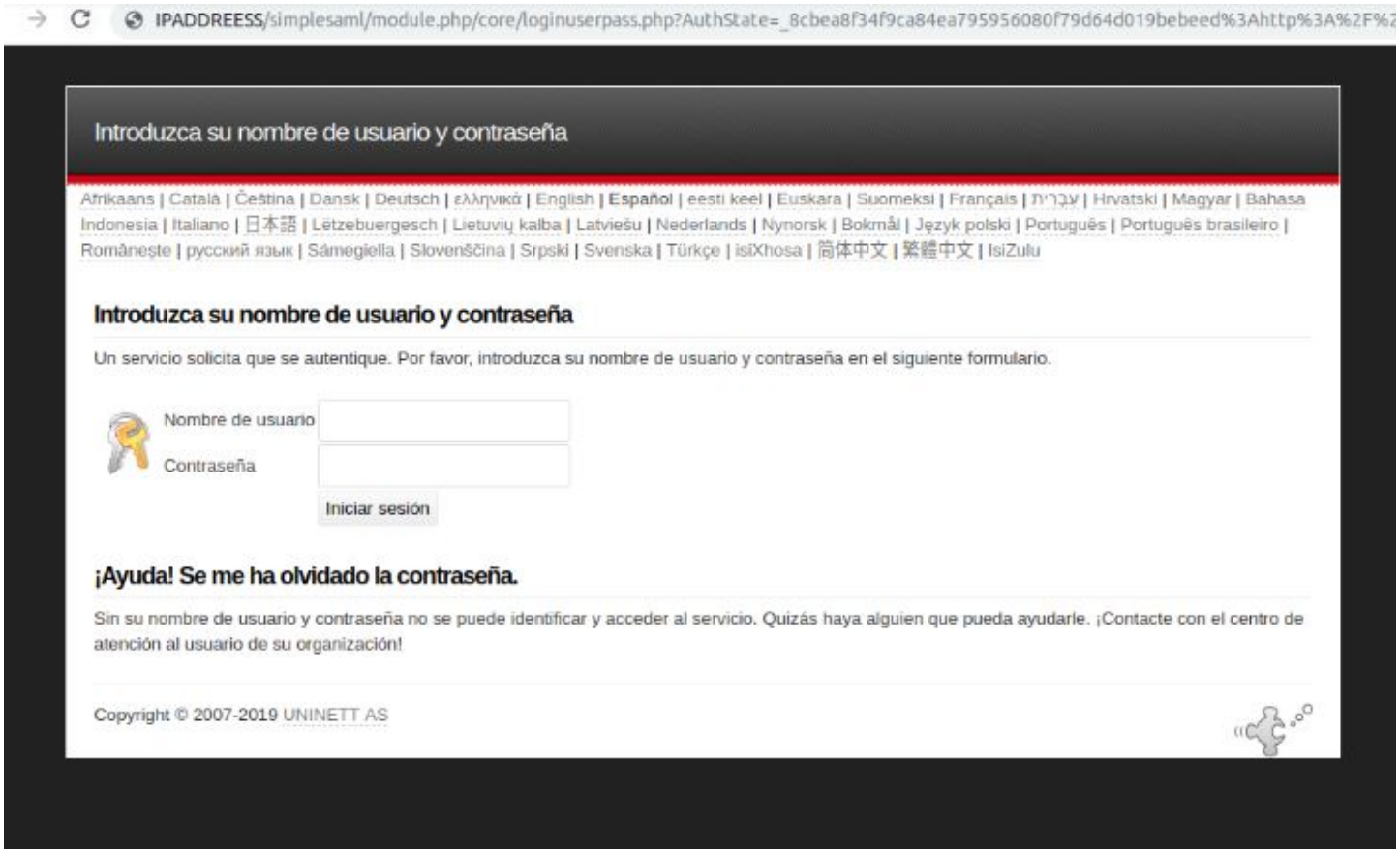
Será necesario asegurarse de que el fichero `/opt/simplesamlphp/lib/_autoload.php` existe.

Una vez instalado simplesamlphp se puede comprobar si funciona el *login* directamente en el saml. Para ello se accederá a la siguiente dirección IP y se seleccionará la fuente de autenticación.

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



Aparecerá una pantalla de *login* como la siguiente donde se introducirá un usuario y contraseña de saml que se haya creado.



Si el *login* es correcto aparecerá una pantalla resumen con todos los atributos del usuario.

Tiene también disponible la guía en SimpleSAMLphp Service Provider QuickStart.

Configurando su proveedor de identidades

Para que se generen los usuarios de SAML correctamente en Pandora FMS es necesario definir en cada uno de ellos los siguientes atributos identificativos que aparecen en la configuración de

SAML:

- Failback to local authentication: Si está desactivada no permitirá iniciar sesión a ningún usuario que no exista en SAML (exceptuando usuarios tipo superadmin). En el caso de que falle la autenticación contra SAML y esté esta opción deshabilitada no consultará en la base de datos del servidor.
- Automatically create remote users: Creará automáticamente los usuarios cuando inicie sesión por primera vez mediante SAML en la herramienta. En caso de estar desactivado debe crearse manualmente con anterioridad.
- SimpleSAML path: Configura la ruta a la carpeta donde se encuentra el directorio `simplesamlphp`.
- SAML Source: Nombre de la fuente SAML contra la cual se han de realizar las peticiones. El nombre debe coincidir con la fuente que se haya seleccionado en:

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

- SAML user id attribute: El campo recuperado de SAML que se utilizará como nombre de usuario (p.e. uid).
- SAML mail attribute: El campo recuperado de SAML que se utilizará como email de usuario (p.e. email).
- SAML group name attribute: El campo recuperado de SAML que se utilizará como grupo del usuario (p.e. group1PersonAffiliation).
- Profile attribute: El campo recuperado de SAML que se utilizará como perfil sobre grupo del usuario (p.e. urn:profile_example:Operator Read).
- Simple attribute / Multivalue attribute: Opción que permite seleccionar si se ha de utilizar un atributo simple para los campos de Perfil y Tag en Pandora FMS o un atributo multivalor.

En el caso de elegir Simple attribute aparecerán dos nuevos campos llamados Profile attribute y Tag attribute donde se seleccionarán los nombres de los atributos de SAML que coincidirán con el nombre del Perfil y Tag en Pandora FMS al crearse.

Cuando se seleccionan Multivalue attribute se tiene que utilizar un atributo que siga este formato:

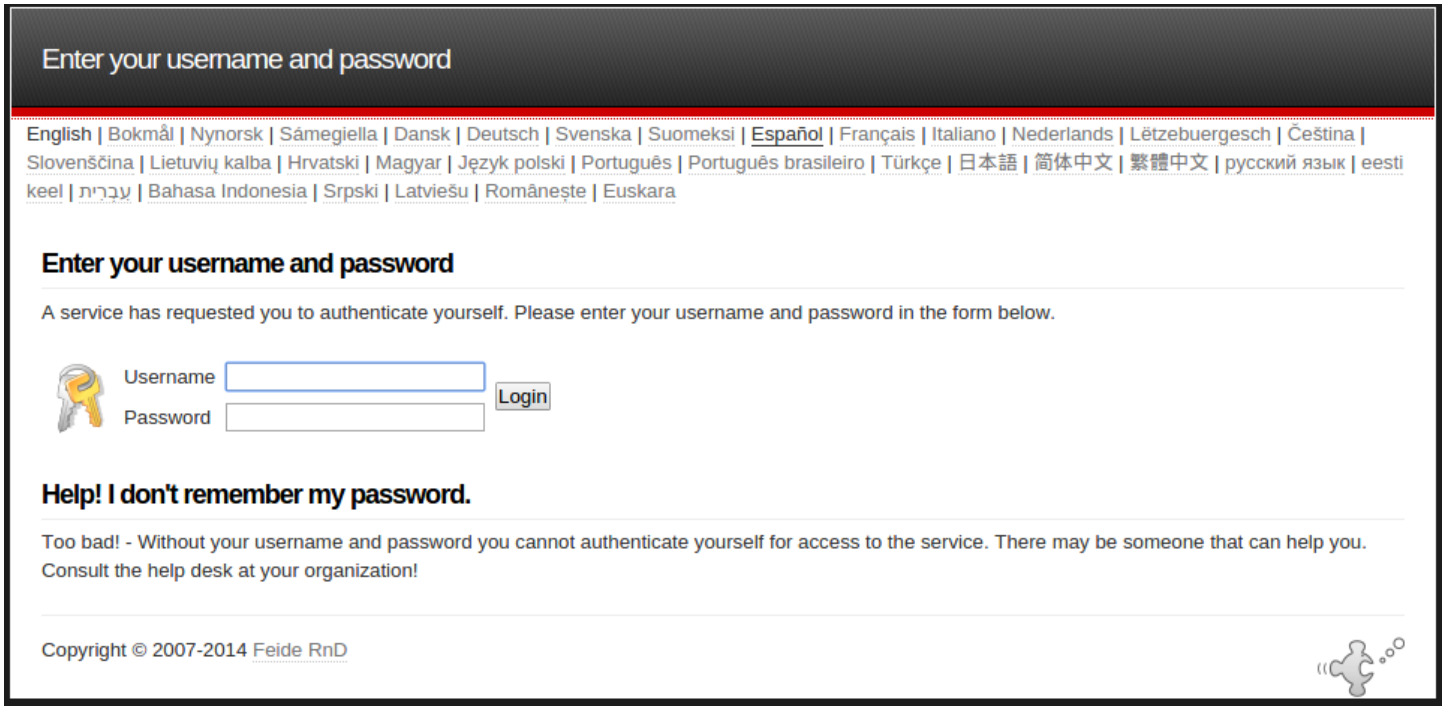
```
<Attribute Name="MULTIVALUE_ATTRIBUTE">
<AttributeValue>PREFIX:role:rolename</AttributeValue>
<AttributeValue>PREFIX:tag:tagname</AttributeValue>
</Attribute>
```

Una vez se tenga el atributo en el SAML creado y seleccionado de esa forma con la configuración en Pandora FMS, se indicarán los siguientes parámetros:

- SAML profiles and tag attribute: Nombre del atributo multivalor.
- SAML profile and tags prefix: Prefijo que irá antes de la clave *role* y *tag* en el valor del atributo. En el caso de que sea `urn:pfms:role:< rolename >` y `urn:pfms:tag:` habría que configurar el prefijo `urn:pfms`.

Inicio de sesión

Será necesario navegar en la Consola de Pandora FMS y hacer clic en el botón de *Login*. Se redirigirá al proveedor de identidades.



Después de un inicio de sesión correcto se redirigirá de vuelta a la Consola de Pandora FMS.

Volver al Índice de Documentación Pandora FMS