



SAML Single Sign-On con Pandora FMS



From:

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

Permanent link:

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

2025/05/12 09:57



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.

Se deben realizar varios pasos antes de poder utilizar SAML en Pandora FMS.

Tener [operativo un servidor SAML](#).

[Configurar los parámetros en Pandora FMS](#).

Si se piensa utilizar [Azure con SAML](#) se debe configurar dicho servidor.

Instalación de SimpleSAMLphp 2.0

Se debe descargar SimpleSAMLphp versión 2.3.2 desde su repositorio oficial:

<https://github.com/simplesamlphp/simplesamlphp/releases/tag/v2.3.2>

y luego ser *subido* al Pandora FMS server. Si el PFMS server tiene acceso a internet y se tiene instalado wget se puede utilizar directamente la siguiente instrucción en un directorio que cuente con espacio y derechos de escritura suficientes:

```
wget
https://github.com/simplesamlphp/simplesamlphp/releases/download/v2.3.2/simplesamlphp-2.3.2-full.tar.gz
```

Se descomprime el fichero descargado con:

```
tar -xvf simplesamlphp-2.3.2-full.tar.gz
```

Se debe mover la carpeta a su ubicación final:

```
mv simplesamlphp-2.3.2 /opt/simplesamlphp
```

Para compartir acceso con Pandora FMS se debe crear el siguiente enlace simbólico:

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

SimpleSAMLphp basa su configuración en el fichero `config.php`, con la ubicación final establecida anteriormente se ha de renombrar la plantilla que trae por defecto:

```
mv /opt/simplesamlphp/config/config.php.dist  
/opt/simplesamlphp/config/config.php
```

Así se tendrá la ruta completa del fichero de configuración en:

```
/opt/simplesamlphp/config/config.php
```

Con el editor de texto favorito se deben editar los siguientes valores (nótese que se debe cambiar `pandora.local` por la URL de la Consola web PFMS y conservar la coma al final de línea ya que forman parte de bloques de instrucciones):

```
/opt/simplesamlphp/config/config.php
```

```
'baseurlpath' => 'https://pandora.local/simplesamlphp/',  
'auth.adminpassword' => '123pandora',
```

Se deben guardar los cambios del fichero y salir a la línea de comandos.

Si aparece algún error de permisos por cache se debe aplicar:

```
mkdir /var/cache/simplesamlphp && chown apache:apache  
/var/cache/simplesamlphp
```

De esta manera se tendrá a SimpleSAMLphp en funcionamiento y deberá mostrar la página de inicio en la URL `https://pandora.local/simplesamlphp/` (se debe cambiar `pandora.local` por la URL de la Consola web PFMS).

Dado el caso que se conecte por HTTP en vez de HTTPS la autenticación fallará hasta que el servidor web Apache sea configurado para que *escuche* por el puerto seguro 443.

Welcome

This is the front page of the SimpleSAMLphp authentication software. There's not much to see here.

If you are the administrator of this installation, please refer to the [SimpleSAMLphp documentation](#) for how to configure and interact with the software.

© 2007-2024 [SimpleSAMLphp](#)



Para acceder a la administración de SimpleSAMLphp primero se debe cambiar el nombre al fichero `authsources.php.dist`:

```
mv /opt/simplesamlphp/config/authsources.php.dist  
/opt/simplesamlphp/config/authsources.php
```

Se accede mediante la URL `https://pandora.local/simplesamlphp/admin/` (se debe cambiar `pandora.local` por la URL de la Consola web PFMS):

Indique su nombre de usuario y clave de acceso

Un servicio solicita que se autentique. Esto significa que debe indicar su nombre de usuario y su clave de acceso en el siguiente formulario.

Nombre de usuario

Clave de acceso

¡Socorro! Se me ha olvidado mi clave de acceso.

¡Muy mal! - Sin su nombre de usuario y su clave de acceso usted no se puede identificar y acceder al servicio. A lo mejor hay alguien que puede ayudarle. !P&ocute;ngase en contacto con el centro de ayuda de su universidad!

Configuración de Pandora FMS con SAML

Menú Management → Setup → Setup → Authentication.

Los siguientes valores son comunes:

Authentication

Authentication method	SAML
Fallback to local authentication	<input type="checkbox"/>
Automatically create remote users	<input type="checkbox"/>
Advanced Config SAML	<input type="checkbox"/>
Simple attribute / Multivalue attribute	<input type="checkbox"/>
Profile attribute	<input type="text"/>
Tag attribute	<input type="text"/>
SAML group name attribute	<input type="text"/>
SimpleSAML path	/opt/
SAML source	default-sp
SAML user id attribute	<input type="text"/>
SAML mail attribute	<input type="text"/>

Algunos campos notables:

- Atributo de nombre de grupo SAML: Campo SAML donde buscar el nombre del grupo (mientras auto crear usuarios remotos esté activado)
- Ruta de SimpleSAML: Directorio donde se encuentra la carpeta simplesamlphp.
- SAML de origen: Nombre authsource, por ejemplo: example-userpass.
- Atributo de correo SAML: Campo SAML donde buscar el correo electrónico del usuario (mientras auto crear usuarios remotos esté activado)

Antes de configurar cualquier servicio de terceros con SAML se recomienda **probar y comprobar localmente** la instalación realizada de SimpleSAMLphp.

Configuración de Azure con SAML

En servicios de Azure® se debe acceder a la sección Extra ID:

Servicios de Azure



Recursos

Reciente Favorito

Nombre

Tipo

Última consulta



No se ha visto ningún recurso recientemente

Mostrar todos los recursos

Acceder luego a Aplicaciones empresariales:

Inicio >

Default Directory | Información general ...

+ Agregar ▾ ⚙ Administrar inquilinos 📄 Novedades

📘 Información general

Características en versión preliminar

🔧 Diagnosticar y solucionar problemas

✓ Administrar

- 👤 Usuarios
- 👥 Grupos
- 📱 External Identities
- 👤 Roles y administradores
- 📁 Unidades administrativas
- 🔗 Asociados del administrador delegado
- 📱 Aplicaciones empresariales** ☆
- 📱 Dispositivos
- 📁 Registros de aplicaciones

📘 Azure Active Directory ahora es Microsoft Entra ID. [Más info](#)

Información general Supervisión Propiedades Re

🔍 Buscar en el inquilino

Información básica

Nombre	Default Directory
Id. del inquilino	a94116d3-1c12-4b82-a38c-c4f42i
Dominio principal	dani96cthotmail.onmicrosoft.com
Licencia	Microsoft Entra ID gratis

Alertas

📘 Azure AD ahora es Microsoft Entra ID
Microsoft Entra ID es el nuevo nombre de Azure Active Directory. No es necesario que realice ninguna acción.

Se crea una nueva aplicación (o se utiliza una existente):

iones empresariales > Aplicaciones empresariales

presariales | Todas las aplicaciones ...

<< + Nueva aplicación  Actualizar  Descargar (exportar) |  Información de versión pre

Vea, filtre y busque aplicaciones en su organización que estén configuradas para usar su inquilino de M

La lista de aplicaciones que mantiene su organización está en [registros de aplicaciones](#).

Tipo de aplicación == **Aplicaciones empresari**

Se encontró 1 aplicación

Nombre	↑↓ Id. de objeto	Id. de aplicación
P Pandora		

Se accede a inicio de sesión único:

Microsoft Azure Actualización

Inicio > Default Directory | Aplicaciones empresariales > Aplicaciones empresariales | Todas las aplic

Pandora | Información general

Aplicación empresarial

- Información general
- Plan de implementación
- Diagnosticar y solucionar problemas
- Administrar
 - Propiedades
 - Propietarios
 - Roles y administradores
 - Usuarios y grupos
 - Inicio de sesión único**
 - Aprovisionamiento
 - Proxy de la aplicación
 - Autoservicio
 - Atributos de seguridad personalizados
- Seguridad

Propiedades

P Nombre ⓘ
Pandora

Id. de aplicación ⓘ
4fcbb445-db72-4cd2-856b-6...

Id. de objeto ⓘ
5ea4e764-4bff-4e6a-b1ff-49d...

Getting Started

- 1. Asignar usuarios y grupos**
Proporcionar a usuarios y grupos específicos acceso a las aplicaciones
[Asignar usuarios y grupos](#)
- 5. Autoservicio**

Se edita la configuración básica de SAML:

de sesión basado en SAML ...

◊ << [↑](#) Cargar el archivo de metadatos [↶](#) Cambiar el modo de inicio de sesión único [☰](#) Test esta aplicación | [🗨](#) ¿Tiene algún comentario?

Configuración del inicio de sesión único con SAML

Una implementación de SSO basada en protocolos de federación mejora la seguridad, la confiabilidad y las experiencias del usuario final, y además, es más fácil de implementar. Elija el inicio de sesión único de SAML siempre que sea posible para las aplicaciones existentes que no usen OpenID Connect u OAuth. [Más información.](#)

Leer [guía de configuración](#) para obtener ayuda para integrar Pandora.

1

Configuración básica de SAML

Identificador (id. de entidad)	saml-pandora
Dirección URL de respuesta (URL del Servicio de consumidor de aserciones)	https://pandora.local/simplesamlphp/
URL de inicio de sesión	<i>Opcional</i>
Estado de la retransmisión (opcional)	<i>Opcional</i>
Dirección URL de cierre de sesión (opcional)	https://pandora.local/pandora_console/index.php?bye=bye

Editar

Editar la configuración

2

Atributos y reclamaciones

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Grupo	user.department
Perfil	user.jobtitle
Identificador de usuario único	user.userprincipalname

Editar

3

Certificados SAML

Se rellenan los siguientes campos, con el ID para la aplicación, la dirección del SimpleSAMLphp instalado (se debe cambiar `pandora.local` por la URL de la Consola web PFMS) y la dirección donde Azure® tendrá que redirigir cuando se cierre la sesión:

Configuración básica de SAML



Guardar | ¿Tiene algún comentario?

Id. único que identifica la aplicación en el id. de Microsoft Entra. Este valor debe ser único en todas las aplicaciones del inquilino de Microsoft Entra. El identificador predeterminado será el público de la respuesta SAML para el SSO iniciado por el IDP.

<input type="text" value="saml-pandora"/>	Predeterm...
Agregar identificador	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Dirección URL de respuesta (URL del Servicio de consumidor de aserciones) * ⓘ

La URL de respuesta es el lugar donde la aplicación espera recibir el token de autenticación. Esto también se denomina "Servicio de consumidor de aserciones" (ACS) en SAML.

<input type="text" value="https://pandora.local/simplesamlphp/"/>	Índi...	Predeterm...
Agregar dirección URL de respuesta	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Dirección URL de inicio de sesión (opcional)

La dirección URL de inicio de sesión se usa si quiere realizar el inicio de sesión único iniciado por el proveedor de servicios. Este valor es la dirección URL de la página de inicio de sesión de la aplicación. Este campo no es necesario si quiere realizar el inicio de sesión único iniciado por el proveedor de identidades.

<input type="text" value="Escriba una dirección URL de inicio de sesión"/>	<input checked="" type="checkbox"/>
--	-------------------------------------

Estado de la retransmisión (opcional) ⓘ

El parámetro Estado de retransmisión indica a la aplicación dónde redirigir a los usuarios una vez completada la autenticación. El valor suele ser una dirección URL o una ruta de dirección URL que lleva a los usuarios a una ubicación específica de la aplicación.

<input type="text" value="Escriba un estado de retransmisión"/>

Dirección URL de cierre de sesión (opcional)

Esta dirección URL se usa para devolver la respuesta de cierre de sesión SAML a la aplicación.

<input type="text" value="https://pandora.local/pandora_console/index.php?bye=bye"/>	<input checked="" type="checkbox"/>
--	-------------------------------------

Descargar el fichero XML con metadatos de federación el cual se utilizará más adelante:

3

Certificados SAML

Certificado de firma de tokens

Estado	Activo	 Editar
Huella digital	00D21F06CBF569DF35CA7C7E2F8A7A060CF8047D	
Expiración	26/8/2027, 10:53:08	
Correo electrónico de notificación	dani_96ct@hotmail.com	
Dirección URL de metadatos de federación de aplicación	<input type="text" value="https://login.microsoftonline.com/a94116d3-1c12..."/>	
Certificado (Base64)	Descargar	
Certificado (sin procesar)	Descargar	
XML de metadatos de federación	Descargar	

Certificados de verificación (opcional)

Obligatorio	No	 Editar
Activo	0	
Expirado	0	

4

Configurar Pandora

Y por último se debe guardar el ID que de el paso anterior y la URL del identificador extra:

4

Configurar Pandora

Tendrá que configurar la aplicación para vincularla con el id. de Microsoft Entra.

Dirección URL de inicio de sesión	<input type="text" value="https://login.microsoftonline.com/a94116d3-1c12..."/>	
Identificador de Microsoft Entra	<input type="text" value="https://sts.windows.net/a94116d3-1c12-4b82-a38..."/>	
URL de cierre de sesión	<input type="text" value="https://login.microsoftonline.com/a94116d3-1c12..."/>	

Configuración en SimpleSAMLphp

Se debe editar el fichero `/opt/simplesamlphp/config/authsources.php` con los siguientes valores:

```
<?php

$config = [
    /*
     * When multiple authentication sources are defined, you can specify one to use by default
     * in order to authenticate users. In order to do that, you just need to name it "default"
     * here. That authentication source will be used by default then when a user reaches the
     * SimpleSAMLphp installation from the web browser, without passing through the API.
     *
     * If you already have named your auth source with a different name, you don't need to change
     * it in order to use it as a default. Just create an alias by the end of this file:
     *
     * $config['default'] = &$config['your_auth_source'];
     */

    // This is a authentication source which handles admin authentication.
    'admin' => [
        // The default is to use core:AdminPassword, but it can be replaced with
        // any authentication source.

        'core:AdminPassword',
    ],

    // An authentication source which can authenticate against SAML 2.0 IdPs.
    'default-sp' => [
        'saml:SP',

        // The entity ID of this SP.
        'entityID' => 'saml-pandora',

        // The entity ID of the IdP this SP should contact.
        // Can be NULL/unset, in which case the user will be shown a list of available IdPs.
        'idp' => 'https://sts.windows.net/a94116d3-1c12- [REDACTED]',

        // The URL to the discovery service.
        // Can be NULL/unset, in which case a builtin discovery service will be used.
        'discoURL' => null,
    ],
];
```

Y por la página web de SimpleSAMLphp al menú de Federación y luego a la sección Herramientas para la conversión de XML a PHP:

[Configuración](#)[Test](#)[Federación](#)[Log out](#)

Hosted entities

default-sp

EntityID: saml-pandora

Type: **SAML 2.0 SP metadata**

Trusted entities

SAML 2.0 IdP metadata

<https://sts.windows.net/a94116d3-1c12-4b82-a38c-c4f42ab6c771/>

Herramientas

[Conversor de XML a metadatos de SimpleSAMLphp](#)

Look up metadata for entity:

SAML 2.0 IdP metadata ▾

EntityID

Search

Se debe cambiar el nombre de saml20-idp-remote.php.dist con:

```
mv /opt/simplesamlphp/metadata/saml20-idp-remote.php.dist  
/opt/simplesamlphp/metadata/saml20-idp-remote.php
```

Se copia el contenido del XML descargado anteriormente, se pega y se procesa; esto generará un texto de configuración para PHP el cual se copia y pega dentro del fichero /opt/simplesamlphp/config/authsources.php reemplazando todo su contenido.

Si todo está correcto se procede a realizar una prueba:

SimpleSAMLphp

[Configuración](#)
[Test](#)
[Federación](#)
[Log out](#)

Test Authentication Sources

[admin](#)
[default-sp](#)

Obteniendo el siguiente resultado:

SimpleSAMLphp

 español ▼

[Configuración](#)
[Test](#)
[Federación](#)
[Log out](#)

Hola, esta es la página de estado de SimpleSAMLphp. Desde aquí puede ver si su sesión ha caducado, cuanto queda hasta que lo haga y todos los atributos existentes en su sesión.

Su sesión será valida durante 28695 segundos.

Atributos

http://schemas.microsoft.com/identity/claims/tenantid	a94116d3-1c12-4b82-a38c-c4f42ab6c771
http://schemas.microsoft.com/identity/claims/objectidentifier	c756e802-3cd8-48fb-8116-f4fda7b5c61c
http://schemas.microsoft.com/identity/claims/displayname	Dani Cebrian
http://schemas.microsoft.com/identity/claims/identityprovider	live.com
http://schemas.microsoft.com/claims/authnmethodsreferences	http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password http://schemas.microsoft.com/claims/multipleauthn http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/unspecified
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givennameDani	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Cebrian

El correo electrónico e identificador de usuario se puede sacar de los atributos que devuelve Azure® en la prueba realizada anteriormente:

Atributos

http://schemas.microsoft.com/identity/claims/tenantid	a94116d3-██████████-a38c-c4f42ab6c771		
http://schemas.microsoft.com/identity/claims/objectidentifier	c756e802-3cd8-48fb-██████████-b5c61c		
http://schemas.microsoft.com/identity/claims/displayname	Dan		
http://schemas.microsoft.com/identity/claims/identityprovider	live.com		
http://schemas.microsoft.com/claims/authnmethodsreferences	http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password http://schemas.microsoft.com/claims/multipleauthn http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/unspeified		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Dan		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	C		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	██████████@hotmail.com		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	dan██████████.com#EXT#@dan██████████.onmicrosoft.com		
	<table border="1"> <tr> <td>Grupo</td> <td>All</td> </tr> </table>	Grupo	All
Grupo	All		
	<table border="1"> <tr> <td>Perfil</td> <td>Pandora Administrator</td> </tr> </table>	Perfil	Pandora Administrator
Perfil	Pandora Administrator		

Authentication

Authentication method

SAML



Fallback to local authentication



Automatically create remote users



Advanced Config SAML



Simple attribute / Multivalue attribute



Profile attribute

Perfil

Tag attribute

SAML group name attribute



Grupo

SimpleSAML path



/opt/

SAML source



default-sp

SAML user id attribute

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

SAML mail attribute



http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Double authentication



Control of timeout session



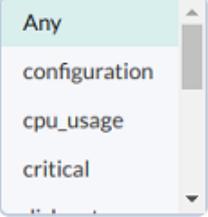
Check activity



Para la configuración avanzada se puede profundizar el *mapeo* de propiedades o seleccionar una por defecto en caso de no hacer coincidencia con ninguna:

SAML

Profiles selected	Groups selected	Tags selected	No hierarchy	Default	saml Attributes	OP
Pandora Administrator	Applications, Databases	configuration	No	No	Perfil: Pandora Administrator, Grupo: All	

Profiles	Groups	Tags	No hierarchy	Default	saml Attributes	OP
Chief Operator 		 <ul style="list-style-type: none">Anyconfigurationcpu_usagecritical	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

[Volver al índice de documentación de Pandora FMS](#)