SAML Single Sign-On con Pandora FMS

SAML Single Sign-On con Pandora FMS

SAML es un estándar abierto de autentificación 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/simplesa
mlphp-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
```

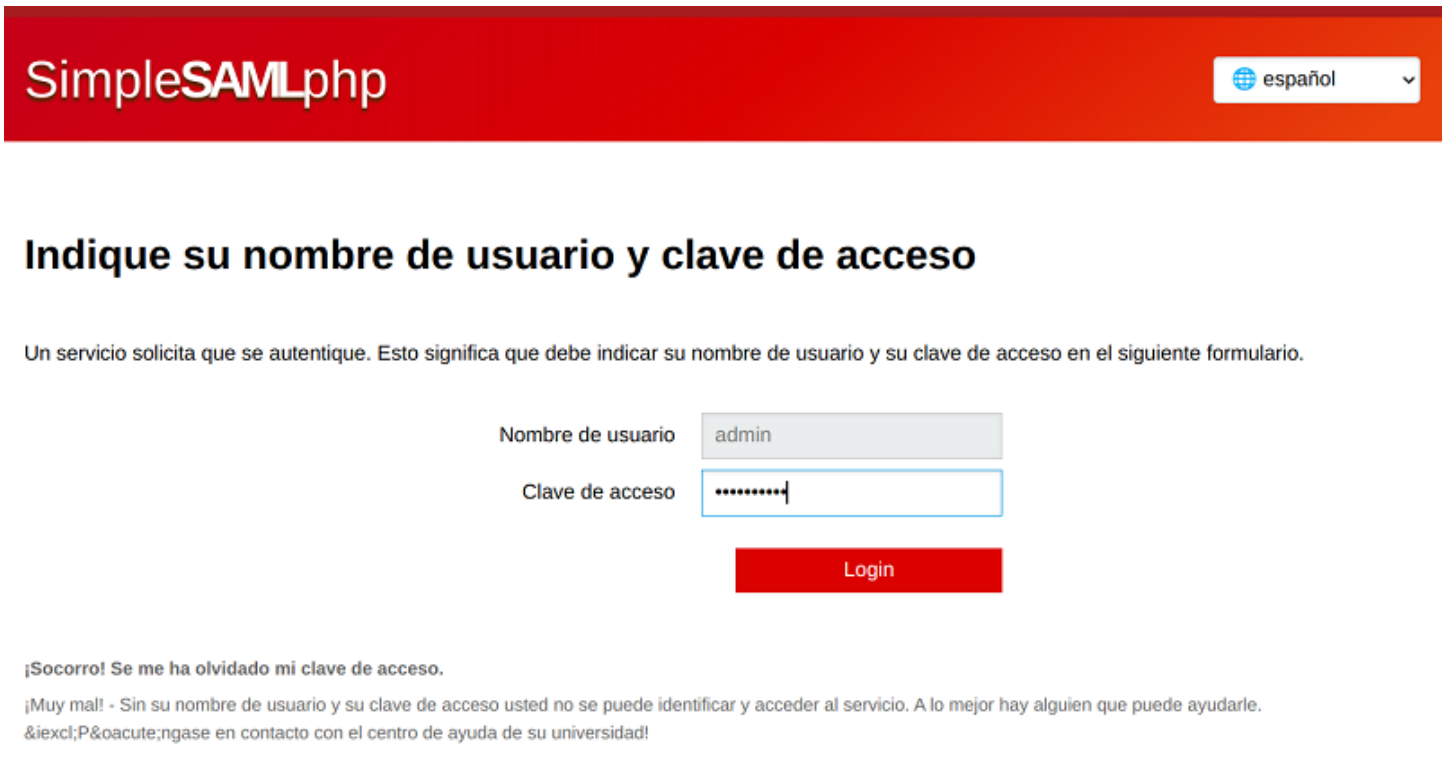
De esta manera se tendrá a SimpleSAMLphp en funcionamiento y deberá mostrar la página de inicio en la URL `https://pandora.local/simplesamlphp/` (se debe cambiar `pandora.local` por la URL de la Consola web PFMS).

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.

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
```

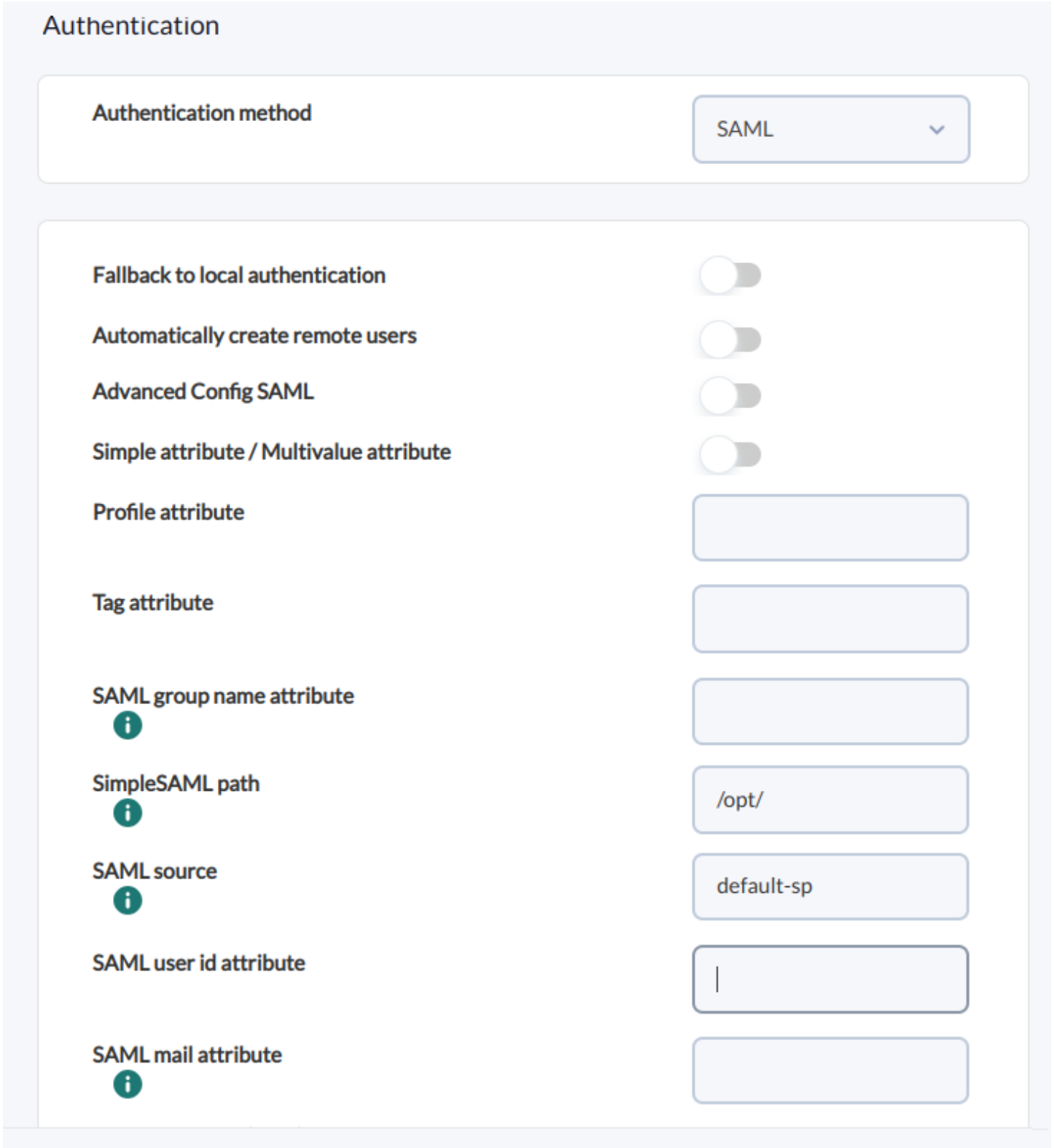
Se accede mediante la URL `https://pandora.local/simplesamlphp/admin/` (se debe cambiar `pandora.local` por la URL de la Consola web PFMS):



Configuración de Pandora FMS con SAML

Menú Management → Setup → Setup → Authentication.

Los siguientes valores son comunes:



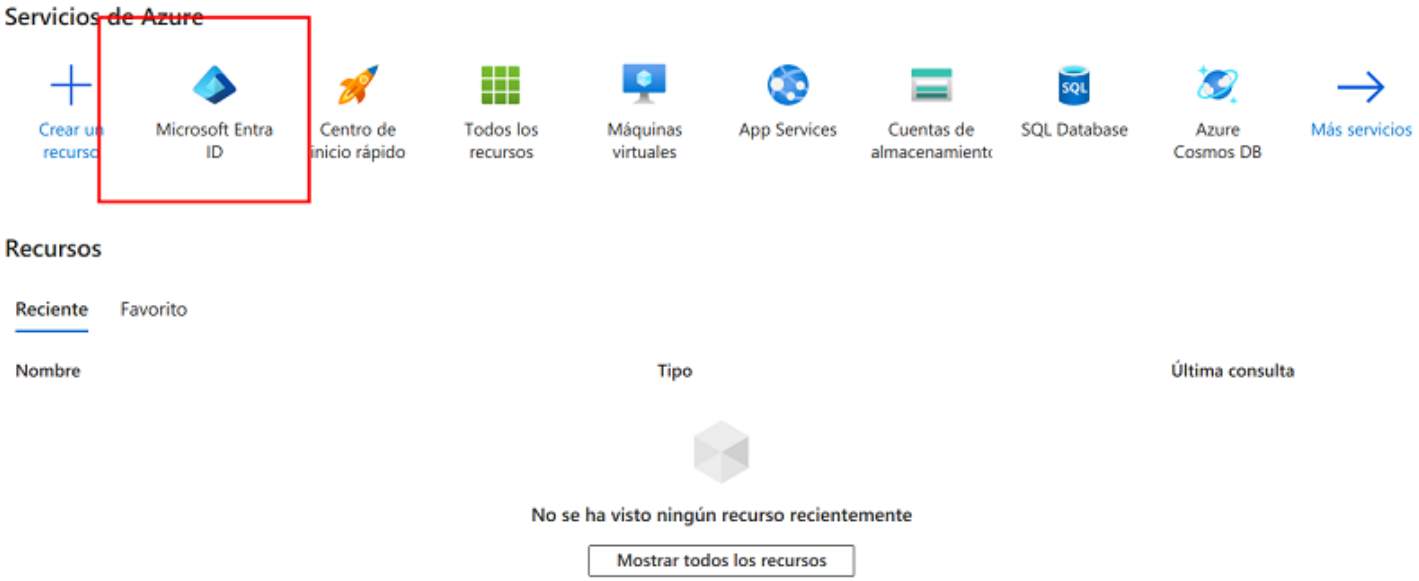
Algunos campos notables:

- 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)

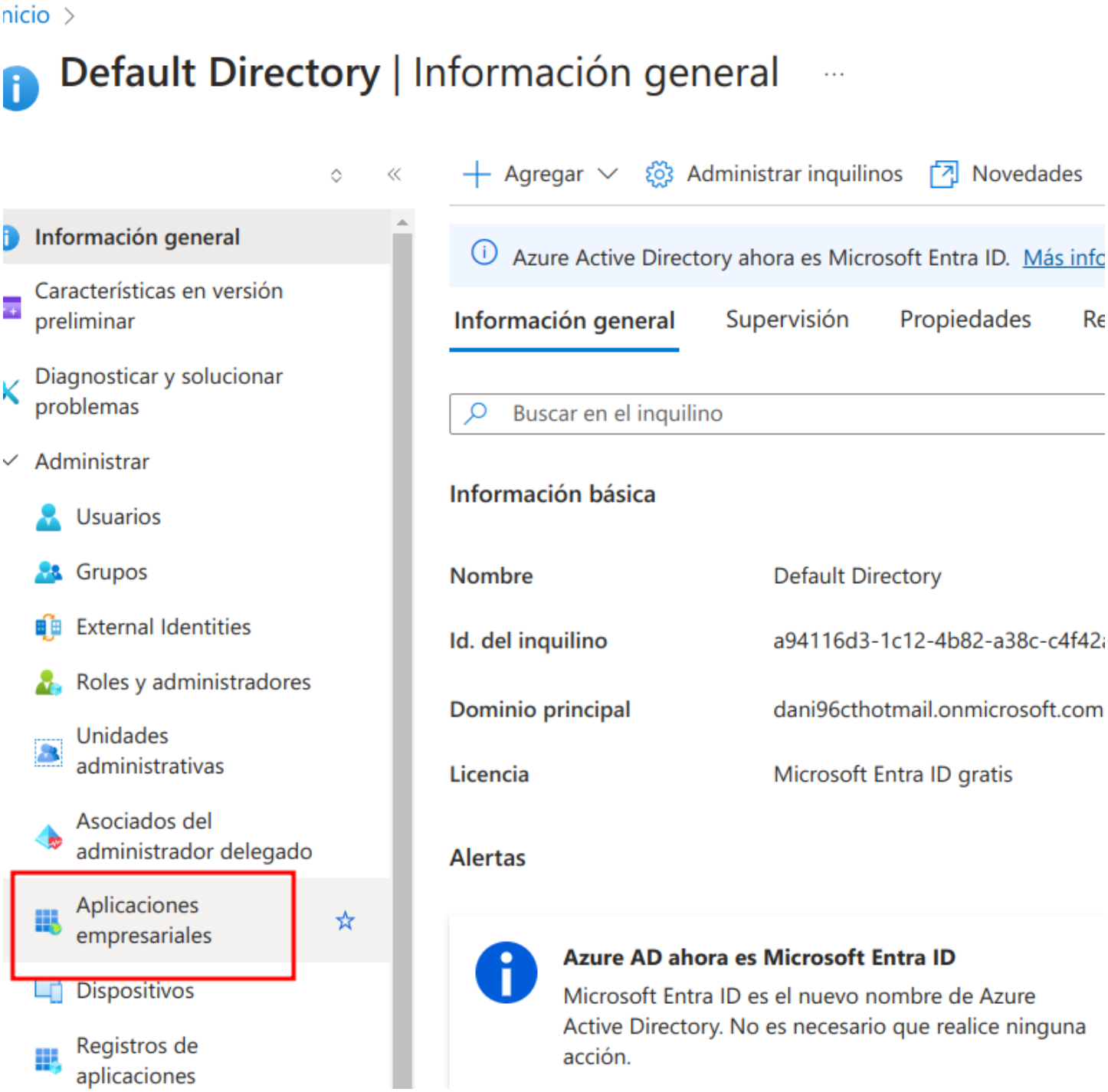
Antes de configurar cualquier servicio de terceros con SAML se recomienda probar y comprobar localmente la instalación realizada de SimpleSAMLphp.

Configuración de Azure con SAML

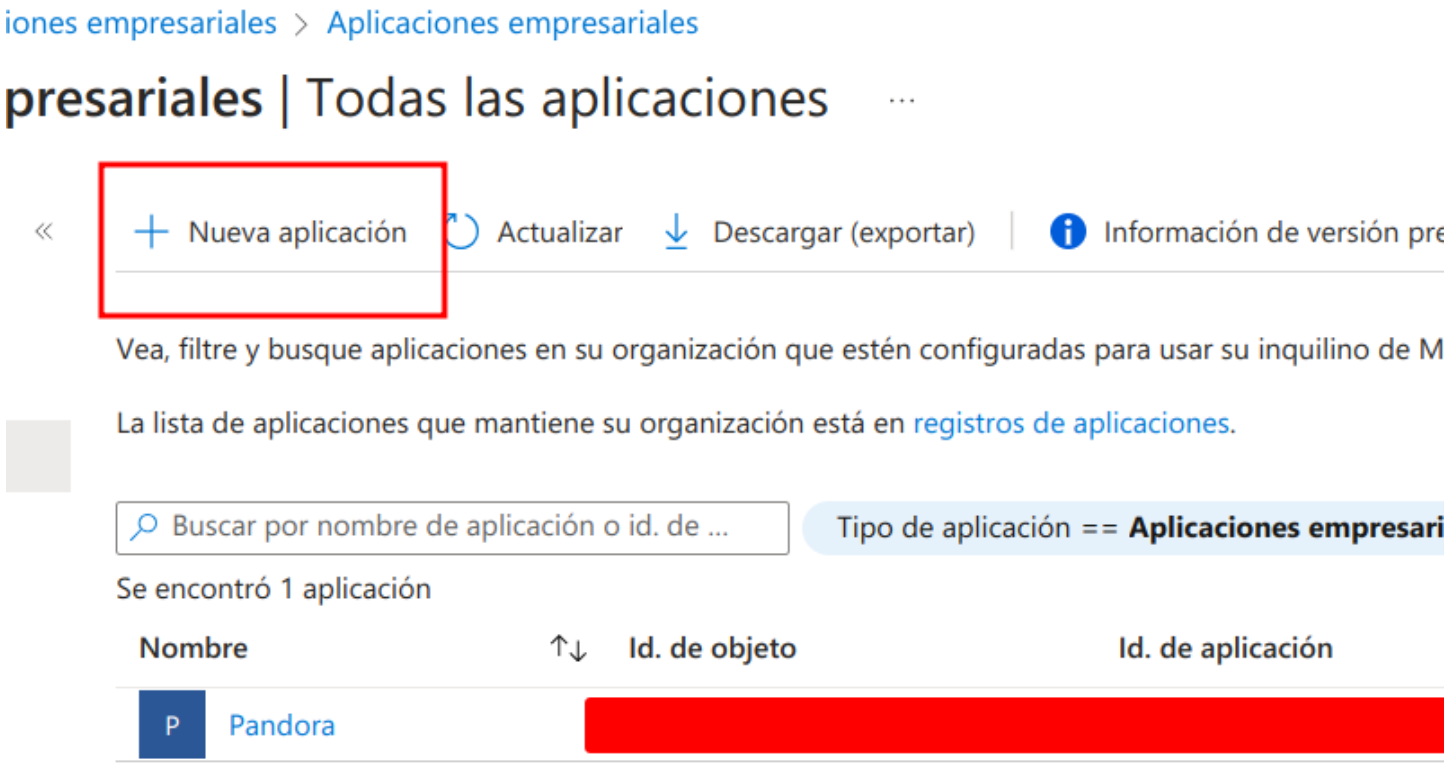
En servicios de Azure® se debe acceder a la sección Extra ID:



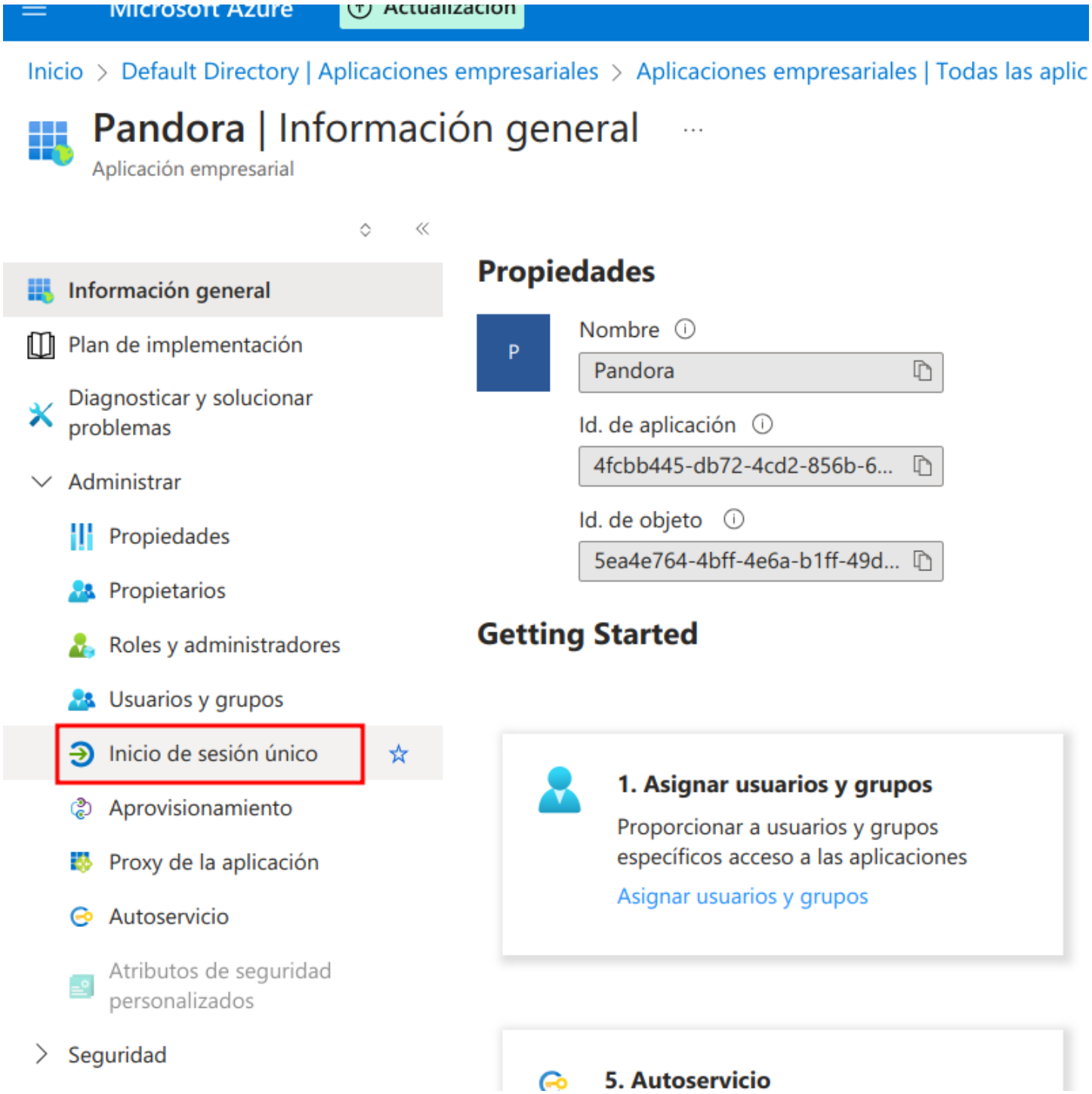
Acceder luego a Aplicaciones empresariales:



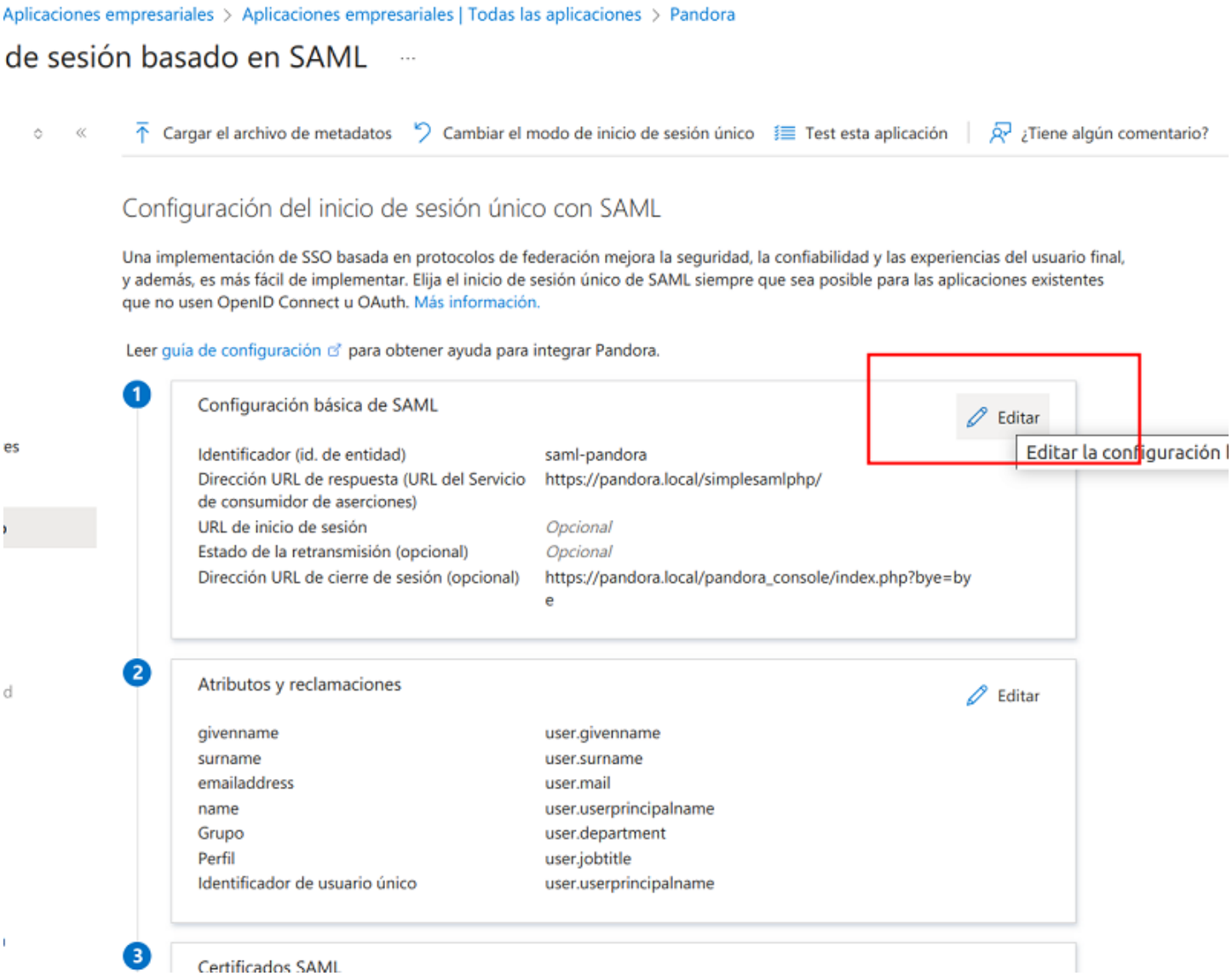
Se crea una nueva aplicación (o se utiliza una existente):



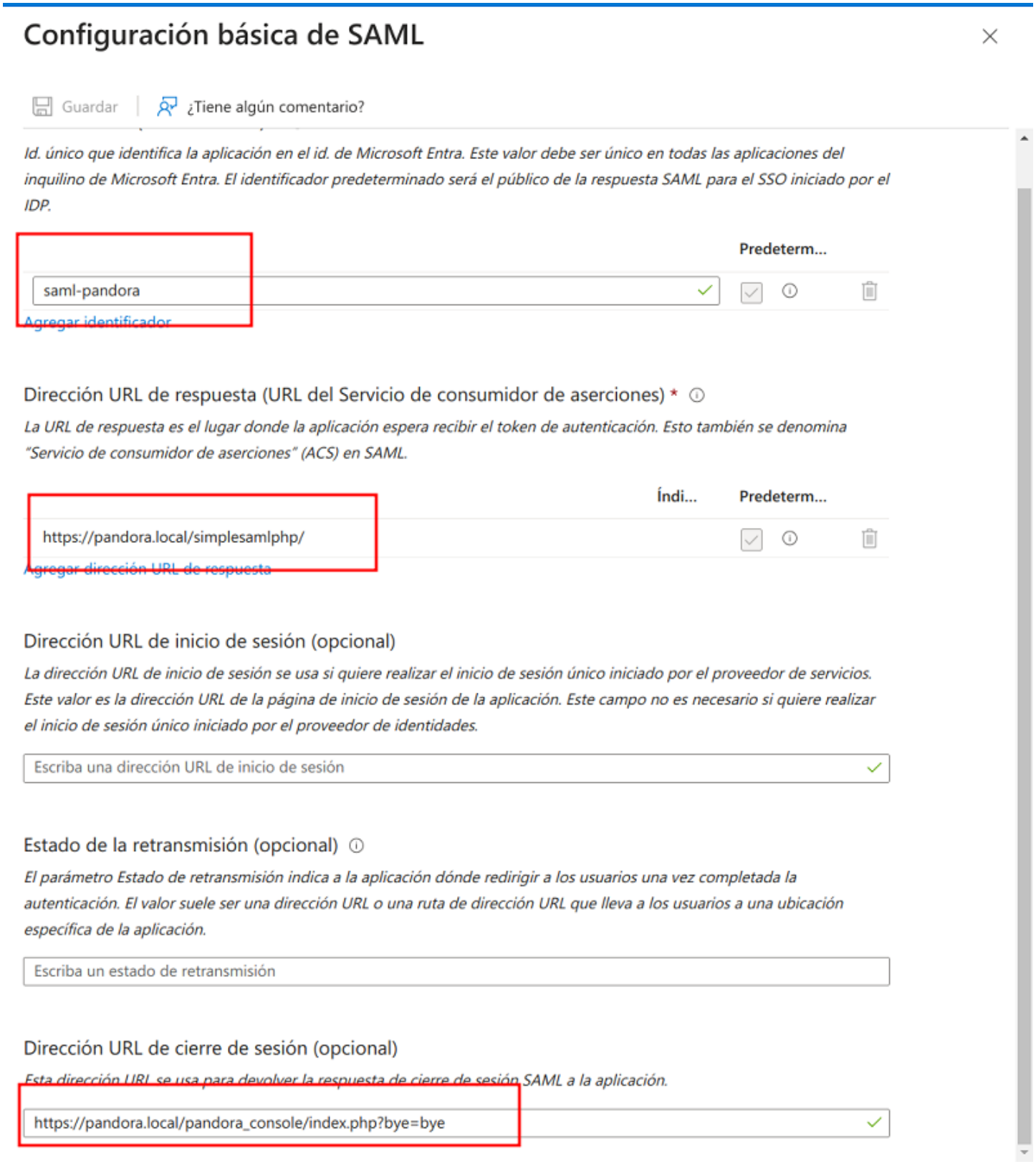
Se accede a inicio de sesión único:



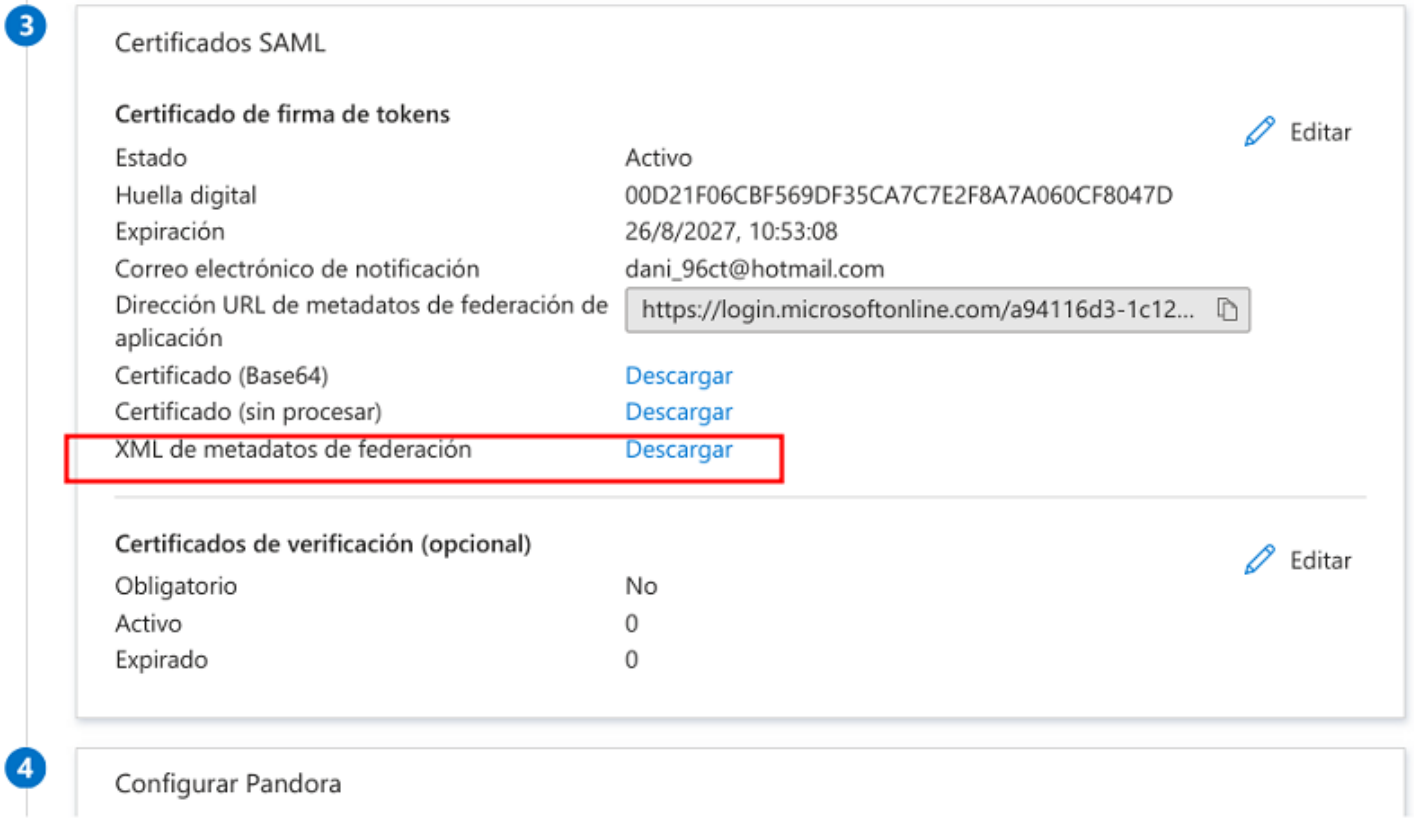
Se edita la configuración básica de SAML:



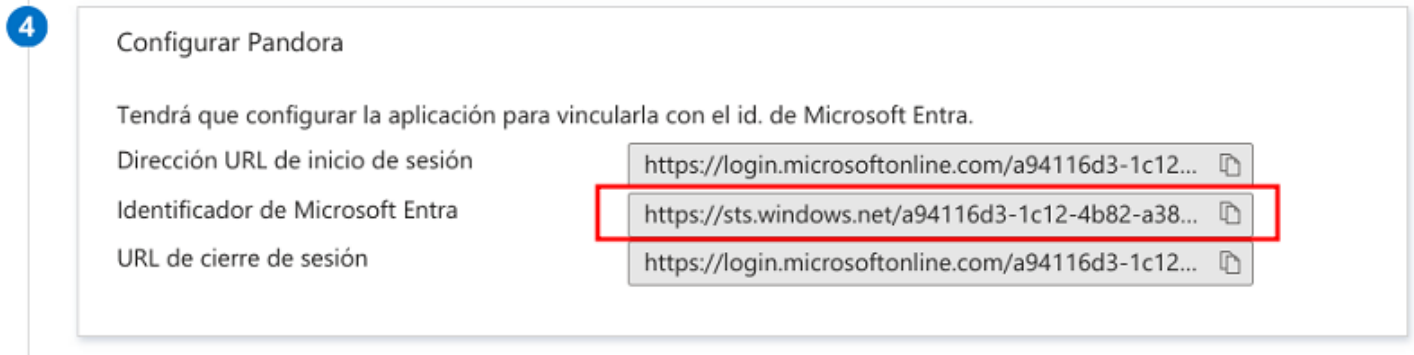
Se rellenan los siguientes campos, con el ID para la aplicación, la dirección del SimpleSAMLphp instalado (se debe cambiar `pandora.local` por la URL de la Consola web PFMS) y la dirección donde Azure® tendrá que redirigir cuando se cierre la sesión:



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



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

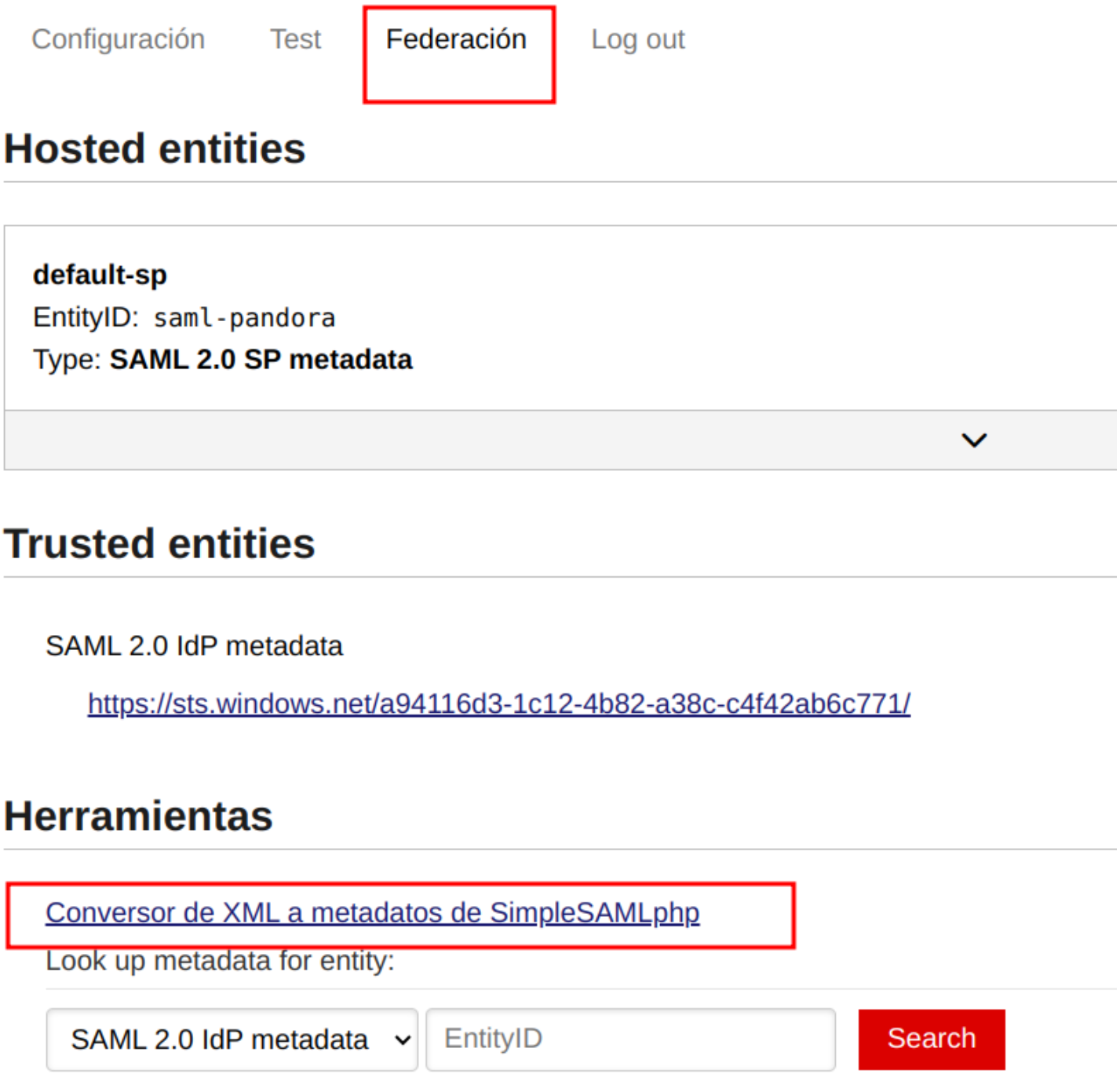


Configuración en SimpleSAMLphp

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

```php
<?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:



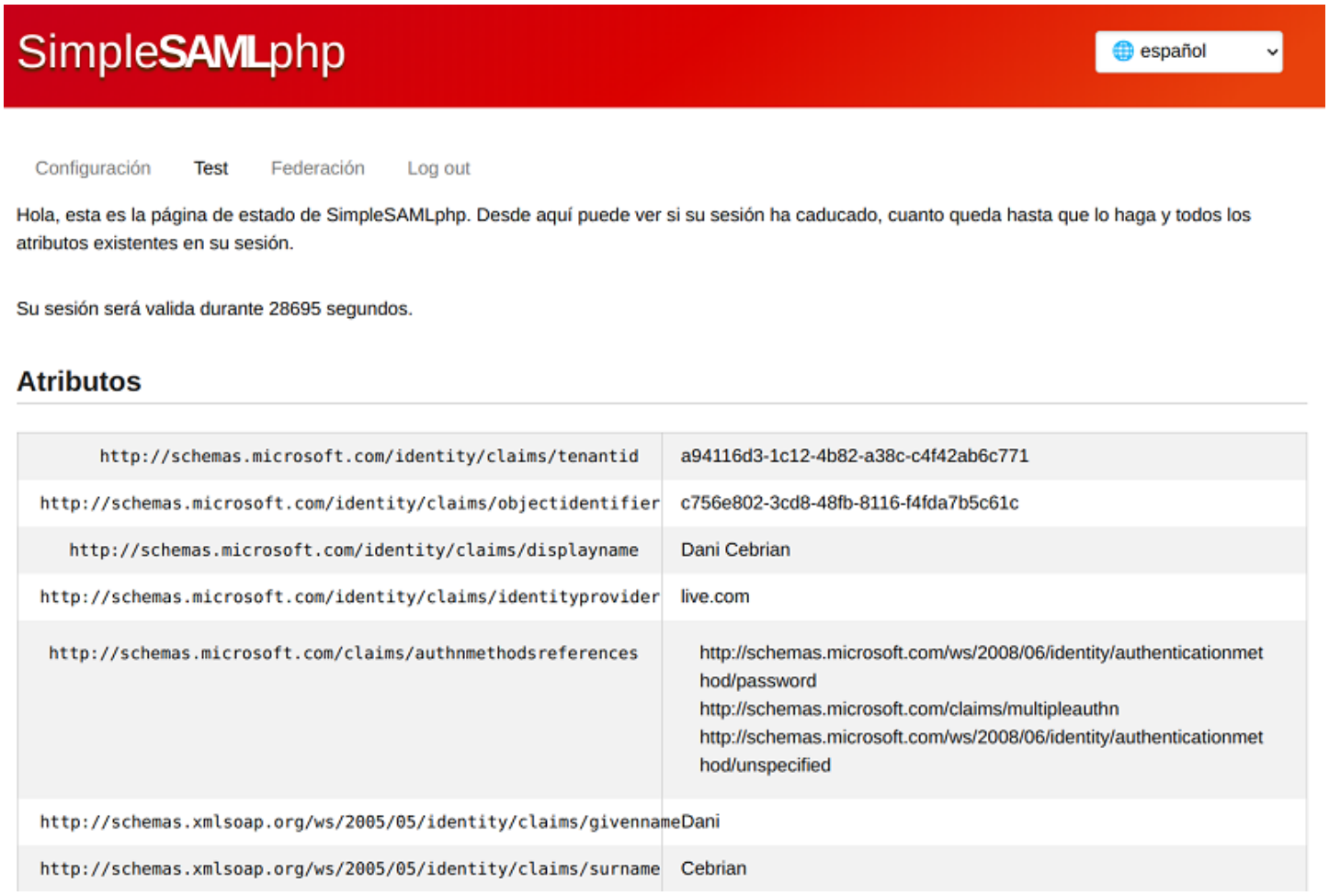
Se debe cambiar el nombre de `saml20-idp-remote.php.dist` con:

```
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:

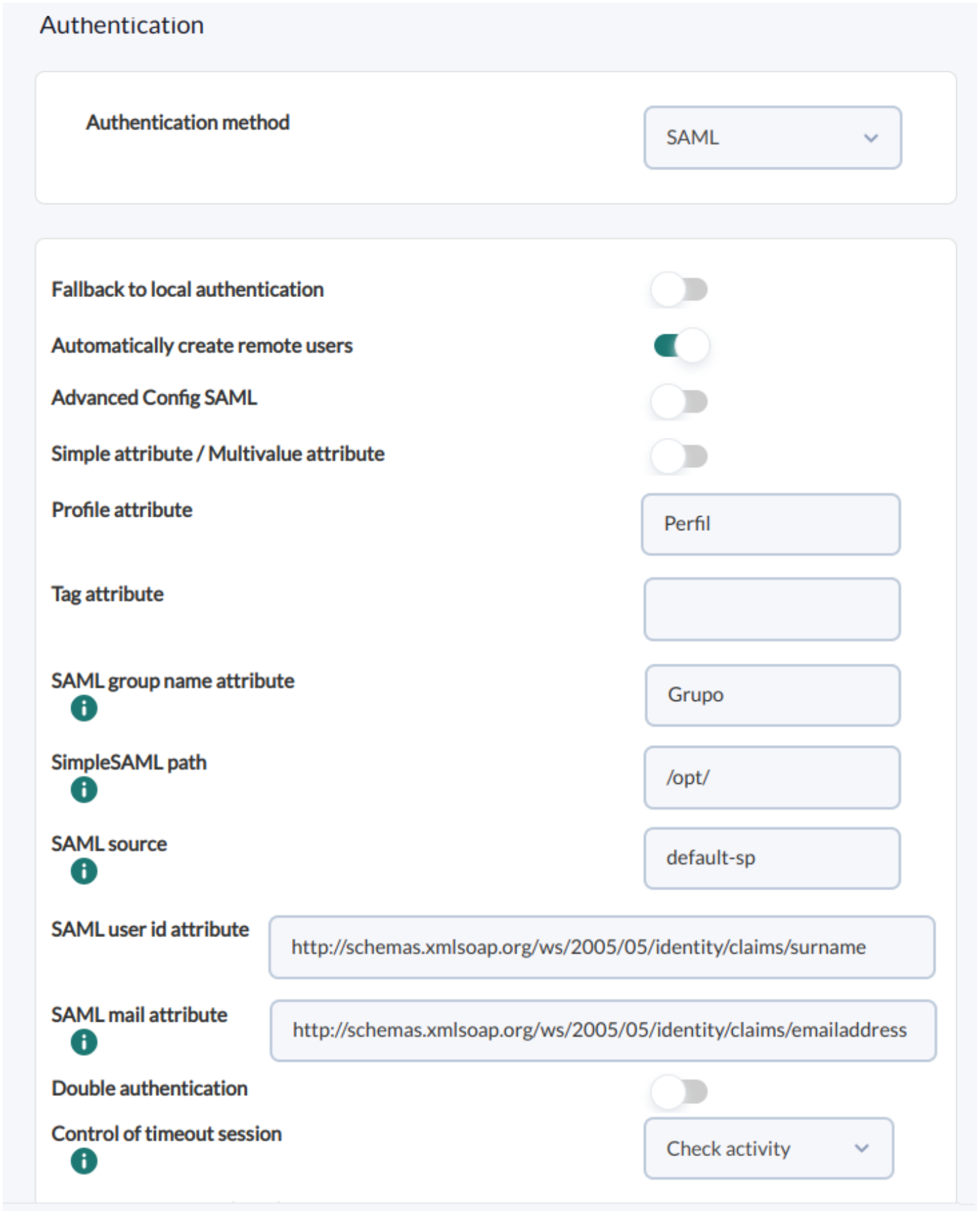
Obteniendo el siguiente resultado:



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[redacted]a38c-c4f42ab6c771
http://schemas.microsoft.com/identity/claims/objectidentifier	c756e802-3cd8-48fb-[redacted]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/unspecified
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/emailaddre[redacted]	@hotmail.com
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	dan[redacted].com#EXT#@dan[redacted].onmicrosoft.com
Grupo	All
Perfil	Pandora Administrator



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	× Applications	Any configuration cpu_usage critical				

Volver al índice de documentación de Pandora FMS