

## **SimpleSAML - Configuración como Proveedor de Identidad**

## Prerrequisitos

- Tener instalado simpleSAML. Las instrucciones de como hacerlo se pueden encontrar en:

<https://docs.google.com/document/d/1sunCjRxcoHMkxoEsrXRKELwXqWA360cCmvRzC77uhXU>

## Configuración

Para el presente ejemplo se realizará la configuración del Proveedor de Identidades (Idp) con Método de Autenticación contra Base de Datos Mysql

1. Habilitar la funcionalidad Proveedor de Identidades (Idp)

Abrir el archivo de configuración de simpleSAML:

```
nano /var/simplesamlphp/config/config.php
```

Habilitar el soporte para SAML 2.0 y Shibboleth 1.3 en la sección:

```
'enable.saml20-idp' => true,  
'enable.shib13-idp' => true,
```

2. Crear la fuente de autenticación

Abrir el archivo de fuentes de autenticación de simpleSAML:

```
nano /var/simplesamlphp/config/authsources.php
```

- Modificar la sección de ejemplo de fuente de autenticación example-sql:

```
/*  
'example-sql' => array(  
    'sqlauth:SQL',  
    'dsn' => 'pgsql:host=sql.example.org;port=5432;dbname=simplesaml',  
    'username' => 'simplesaml',
```

```
'password' => 'secretpassword',  
'query' => 'SELECT uid, givenName, email, eduPersonPrincipalName FROM users  
WHERE uid = :username AND password = SHA2(CONCAT((SELECT salt FROM  
users WHERE uid = :username), :password),256);',  
,  
*/
```

Quitar los simbolos de comentarios de inicio (/\*) y de fin (\*/)

Editar el nombre de la fuente de autenticación (example-sql) por un nombre adecuado para la aplicación

```
IdpUD => array(  

```

Editar el dsn

```
'dsn' => 'mysql:host=10.20.0.38;port=3306;dbname=dbms'
```

Editar nombre de usuario para conectarse a la base de datos Mysql,

```
'username' => 'miusuario',
```

Editar nombre la contraseña para conectarse a la base de datos Mysql,

```
'password' => 'mipassl',
```

Editar la consulta para rescatar nombres de usuario y contraseñas de una tabla de la base de datos mysql

```
'query' => 'SELECT id_usuario, clave FROM tablaUsuario WHERE usuario =  
:username AND clave = :password',
```

al final queda así:

```
IdpUD => array(  
'sqlauth:SQL',  
'dsn' => 'mysql:host=10.20.0.38;port=3306;dbname=dbms',  
'username' => 'usuarioDBMysql',  
'password' => 'passDBMysql',
```

```
'query' => 'SELECT usuario, clave FROM usuarios WHERE usuario = :username  
AND clave = 'query' => 'SELECT id_usuario, clave FROM tablaUsuario WHERE  
usuario = :username AND clave = :password',  
)
```

### 3. Crear certificados autofirmados

Crear el directorio cert e ingresar a el

```
cd /var/simplesamlphp/  
mkdir cert  
cd cert
```

Crear los llave privada y el certificado autofirmado:

En la consola ejecutar el comando:

```
openssl req -newkey rsa:2048 -new -x509 -days 3652 -nodes -out server.crt -keyout server.pem
```

Los archivos server.crt (certificado) y server.pem (llave privada) son creados en el directorio cert.

- El certificado generado arriba tiene una validez de 10 años
- SimpleSAMLphp trabaja únicamente con certificados RSA, los certificados DSA no son soportados

### 4. Configurar el Proveedor de Identidad - IdP

Abrir el archivo de configuración del Idp

```
nano /var/simplesamlphp/metadata/saml20-idp-hosted.php
```

- Modificar los nombres las variables

```
'privatekey' => 'server.pem',  
'certificate' => 'server.crt',
```

Los nombres de privatekey y certificate deben coincidir con los nombres de los archivos generados en directorio cert para el Idp.

- Modificar la fuente de autenticación

```
'auth' => 'IdpUD',
```

Debe ser el mismo que se registró previamente en el archivo config/authsources.php

## Pruebas de funcionamiento

Seleccionar la pestaña autenticación

### Página de instalación de simpleSAMLphp

[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](#)

Bienvenido

Configuración

**Autenticación**

Federación

- [Probar las fuentes para la autenticación ya configuradas](#)

Entrar como administrador

Copyright © 2007-2014 Feide RnD



Seleccionar de la lista la fuente de autenticación creada, para esta caso es IdpUD

## Test authentication sources

[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](#)

## Test authentication sources

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

Copyright © 2007-2014 Feide RnD



## Ingresar nombre de usuario y contraseña

### Indique su nombre de usuario y clave de acceso

[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](#)

### 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

Login

### ¡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.  
¡Póngase en contacto con el centro de ayuda de su universidad!

Copyright © 2007-2014 Feide RnD



## Ejemplo de SAML 2.0 SP

[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](#)

## Ejemplo de SAML 2.0 SP

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.

### Atributos

cla_codigo	20152028024
cla_clave	aee00f0c2b384f25218f8844a470a7af8463c5a2

### Salir

[ [Salir](#) ]

### Sobre simpleSAMLphp

¡Eh! Esto del simpleSAMLphp está interesante, ¿dónde puedo averiguar más? Hay más información sobre simpleSAMLphp en el blog de I+D de Feide en [UNINETT](#).

Copyright © 2007-2014 Feide RnD



Para cerrar la sesión seleccionar el enlace [ Salir ].

Si existe error en la configuración se presenta la descripción del error

## Excepción no controlada

### Excepción no controlada

Se lanzó una excepción no controlada.

Por favor, si informa de este error, mantenga el tracking ID que permite encontrar su sesión en los registros de que dispone el administrador del sistema:

7a567ec231

### Información de depuración

La siguiente información de depuración puede ser de utilidad para el administrador del sistema o el centro de atención a usuarios:

SimpleSAML\_Error\_Error: UNHANDLEDEXCEPTION

```
Backtrace:  
0 /var/simplesamlphp/www/module.php:179 (N/A)  
Caused by: Exception: sqlauth:IdpUD: - Failed to execute query: SQLSTATE[42S22]: Column not found: 1054 Unknown column 'cla_codigos' in 'field list'  
Backtrace:  
3 /var/simplesamlphp/modules/sqlauth/lib/Auth/Source/SQL.php:139 (sspmod_sqlauth_Auth_Source_SQL::login)  
2 /var/simplesamlphp/modules/core/lib/Auth/UserPassBase.php:259 (sspmod_core_Auth_UserPassBase::handleLogin)  
1 /var/simplesamlphp/modules/core/www/loginuserpass.php:75 (require)  
0 /var/simplesamlphp/www/module.php:134 (N/A)
```

### Informar del error

Si lo desea, indique su dirección electrónica, para que los administradores puedan ponerse en contacto con usted y obtener datos adicionales de su problema

Correo-e:





**UNIVERSIDAD DISTRITAL  
FRANCISCO JOSÉ DE CALDAS**

### Universidad Distrital Francisco José de Caldas Oficina Asesora de Sistemas

*Este documento está bajo licencia de Creative Commons Reconocimiento 4.0 Internacional.*



Los nombres de programas, marcas, logotipos y citas de referencia son propiedad de sus respectivos autores y se consideran elementos conexos al documento sobre los cuales no aplican la licencia aquí declarada. Corresponde a los usuarios determinar claramente los derechos de autor que cobijan a cada uno de estos recursos.

Las ideas y expresiones contenidas en el documento corresponden a sus autores y no representan necesariamente la posición de la institución respecto a los temas tratados.