# My Project

## version 2.0.0

**Author Name**

February 06, 2017

# Contents


# Introducción

sysPass es un gestor de claves web escrito en PHP que permite la gestión centralizada de claves en un entorno multiusuario.

## Características

- Interfaz con Material Design Lite en HTML5 y Ajax
- Claves encriptadas con AES-256 CBC
- Multiusuario con gestión de usuarios, grupos y perfiles
- Gestión avanzada de perfiles con 29 niveles de acceso
- Autentificación con MySQL/MariaDB, OpenLDAP y Active Directory
- Notificaciones por email e in-app de actividad
- Enlaces públicos a cuentas sin necesidad de login
- Historial de cambios en cuentas
- Gestión de archivos asociados a cuentas con previsualización de imágenes
- Multilenguaje, con traducciones en Inglés, Catalán, Alemán, Polaco, Ruso, Francés y Holandés
- Enlace a Wiki externa e integración con API de DokuWiki
- Backup en formato portable y exportación en XML encriptado
- Registro de acciones y eventos con posibilidad de enviar a Syslog remoto en formato CEF
- Configurable y extensible mediante temas y plugins
- API para integración con otras aplicaciones
- Importación desde KeePass, KeePassX y CSV
- Instalación en un solo paso

## *Instalación*

### *Instalación Debian 8*

#### *Prerequisitos*

- Servidor Web (Apache/Nginx/Lighttpd) con SSL habilitado.
- MariaDB o MySQL >= 5
- PHP >= 5.6 <= 7.0
- **Módulos PHP**

    - mysql
    - mcrypt
    - Curl
    - Json
    - GD
    - ldap (opcional)
- Última versión de sysPass https://github.com/nuxsmin/sysPass/releases

### *Instalación*

Instalación de paquetes en Debian GNU/Linux:

```
apt-get install apache2 libapache2-mod-php5 php5 php5-curl php5-mysqlnd \
php5-curl php5-gd php5-json php5-mcrypt mysql-server
service apache2 restart
```

Opcional para habilitar LDAP:

```
apt-get install php5-ldap
service apache2 restart
```

### *Configuración de directorios y permisos*

Crear un directorio para la aplicación en la raíz del servidor web:

```
mkdir /var/www/html/syspass
```

Copiar y descomprimir el archivo sysPass en el directorio creado:

```
cp sysPass.tar.gz /var/www/html/syspass
cd /var/www/html/syspass
tar xzf syspass.tar.gz
```

Cambiar el propietario del directorio 'syspass/config'. Ha de coincidir con el usuario del servidor web:

```
chown www-data /var/www/html/syspass/config
chmod 750 /var/www/html/syspass/config
```

Crear y cambiar el propietario del directorio de copias de seguridad:

```
mkdir var/www/html/syspass/backup
chown www-data /var/www/html/syspass/backup
```

### *Configuración del entorno*

Abir un navegador y escribir la URL:

https://IP_O_NOMBRE_SERVIDOR/syspass/index.php

> ***Note***
>
> Seguir los pasos del instalador y tras la correcta finalización, ya es posible acceder a la aplicación

## *Instalación CentOS 7*

### *Prerequisitos*

- Servidor Web (Apache/Nginx/Lighttpd) con SSL habilitado.

- MariaDB o MySQL >= 5
- PHP >= 5.6 <= 7.0
- **Módulos PHP**
    - Mysql
    - mcrypt
    - ldap (opcional)
    - SimpleXML
    - Curl
    - Json
    - GD
    - PDO
- Última versión de sysPass https://github.com/nuxsmin/sysPass/releases

### *Instalación*

Instalación de paquetes

```
yum install httpd php-mysql php-pdo php-ldap php-gd php-pdo mariadb-server mariadb wget
```

Para iniciar y auto-iniciar el servidor web Apache:

```
systemctl enable httpd.service
systemctl start httpd.service
```

Para iniciar y auto-iniciar el servidor MariaDB:

```
systemctl enable mariadb.service
systemctl start mariadb.service
```

Necesitamos securizar el servidor MariaDB:

```
/usr/bin/mysql_secure_installation
```

### *Instalación del repositorio EPEL para módulo de encriptación*

Descargar e instalar el RPM para el repositorio de EPEL:

```
wget http://dl.fedoraproject.org/pub/epel/beta/7/x86_64/epel-release-7-0.2.noarch.rpm
yum install epel-release-7-0.2.noarch.rpm
yum install php-mcrypt
systemctl restart httpd.service
```

### *Habilitar los puertos en el firewall*

Añadir reglas en el firewall:

```
firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

### *Configuración de directorios y permisos*

Crear un directorio para la aplicación en la raíz del servidor web:

```
mkdir /var/www/html/syspass
```

Copiar y descomprimir el archivo sysPass en el directorio creado:

```
cp sysPass.tar.gz /var/www/html/syspass
cd /var/www/html/syspass
tar xzf syspass.tar.gz
```

Cambiar el propietario del directorio 'syspass/config'. Ha de coincidir con el usuario del servidor web:

```
chown apache /var/www/html/syspass/config
chmod 750 /var/www/html/syspass/config
```

Crear y cambiar el propietario del directorio de copias de seguridad:

```
mkdir var/www/html/syspass/backup
chown apache /var/www/html/syspass/backup
```

### *Modificando SELinux*

Para permitir a sysPass escribir su configuración y backups, tenemos dos opciones:

> ***Note***
>
> Elegir una de las dos opciones

- Cambiar el usuario y contexto de SELinux para hacer escribibles los directorios de config y backups:

```
chcon -R -t httpd_sys_rw_content_t /var/www/html/sysPass/config/
chcon -R -t httpd_sys_rw_content_t /var/www/html/sysPass/backup/
```

- Deshabilitar SELinux editando el archivo '/etc/sysconfig/selinux' y cambiar el valor de la variable "SELINUX" a "permissive" y reiniciar el sistema.

### *Configuración del entorno*

Abir un navegador y escribir la URL:

https://IP_O_NOMBRE_SERVIDOR/syspass/index.php

> ***Note***
>
> Seguir los pasos del instalador y tras la correcta finalización, ya es posible acceder a la aplicación

## *Instalación Gentoo*

### *Prerequisitos*

- Servidor Web (Apache/Nginx/Lighttpd) con SSL habilitado.
- MariaDB o MySQL >= 5
- PHP >= 5.6 <= 7.0
- **Módulos PHP**
    - mysql
    - pdo
    - mcrypt
    - ldap (opcional)
    - SimpleXML

    - Json
    - GD
    - intl
- Última versión de sysPass https://github.com/nuxsmin/sysPass/releases

### *Instalación de paquetes*

```
emerge --ask dev-db/mysql
emerge --ask www-servers/apache

PHP_TARGETS="php5-6"
USE="apache2 pdo curl simplexml xml zlib crypt gd intl json opcache"
emerge --ask dev-lang/php
```

Si se quiere habilitar LDAP es necesario compilar PHP con soporte para ldap:

```
PHP_TARGETS="php5-6"
USE="apache2 pdo curl ldap minimal simplexml xml zlib crypt gd intl json opcache"
emerge --ask dev-lang/php
```

En los siguientes enlaces hay disponible documentación más extensa de cómo instalar y configurar dichos paquetes:

https://wiki.gentoo.org/wiki/Apache

https://wiki.gentoo.org/wiki/PHP

https://wiki.gentoo.org/wiki/MySQL

### *Configuración de Apache*

Es necesario habilitar el módulo de PHP en Apache, por lo que editamos el archivo /etc/conf.d/apache2 y modificamos la variable APACHE2_OPTS añadiendo "-D PHP5":

```
APACHE2_OPTS="... -D PHP5"
```

Iniciamos y establecemos el auto-inicio de Apache:

```
rc-update add apached default
rc-service apache2 start
```

### *Configuración de MySQL*

Establecemos la clave de root de MySQL:

```
emerge --config dev-db/mysql
```

Iniciamos y establecemos el auto-inicio de MySQL:

```
rc-update add mysql default
rc-service mysql start
```

Securizamos la instalación de Mysql:

```
mysql_secure_installation
```

### *Configuración de directorios y permisos*

Crear un directorio para la aplicación en la raíz del servidor web:

```
mkdir /var/www/localhost/syspass
```

Copiar y descomprimir el archivo sysPass en el directorio creado:

```
cp sysPass.tar.gz /var/www/localhost/syspass
cd /var/www/localhost/syspass
tar xzf syspass.tar.gz
```

Cambiar el propietario del directorio 'syspass/config'. Ha de coincidir con el usuario del servidor web:

```
chown apache /var/www/localhost/syspass/config
chmod 750 /var/www/localhost/syspass/config
```

Crear y cambiar el propietario del directorio de copias de seguridad:

```
mkdir var/www/localhost/syspass/backup
chown apache /var/www/localhost/syspass/backup
```

### *Configuración del entorno*

Abir un navegador y escribir la URL:

https://IP_O_NOMBRE_SERVIDOR/syspass/index.php

> ***Note***
>
> Seguir los pasos del instalador y tras la correcta finalización, ya es posible acceder a la aplicación

### *Modo Hosting*

El modo hosting es para aquellas instalaciones que se ejecutan en un hosting externo en las que no es posible crear la base de datos ni el usuario de conexión a la misma.

> ***Note***
>
> **No se creará la base de datos (sí las tablas) ni el usuario de conexión**

Los pasos para realizar la instalación son los siguientes:

- Crear un usuario/clave en el panel del hosting.
- Crear la base de datos de sysPass (no crear tablas) y dar permisos al usuario anterior.
- Iniciar la instalación de sysPass (borrar el archivo "config/config.xml" si existe) y utilizar el usuario/clave creados como usuario de sysPass (los dos primeros campos).
- Indicar el usuario con permisos de administración de MySQL/MariaDB (puede ser el mismo de antes si tiene suficientes permisos), para realizar la creación de tablas en la base de datos de sysPass. Este usuario es sólo para la instalación y normalmente en los hostings suele ser el usuario/clave de gestión.
- Si hay conexión con la base de datos y los permisos son correctos, la instalación debe de finalizar correctamente.

> ***Note***
>
> En caso de errores, verificar el archivo de registro del servidor web.

## *Configuración*

### *Configuración de LDAP*

Para configurar un servidor de OpenLDAP correctamente, puedes seguir el siguiente artículo en https://wiki.debian.org/LDAP/OpenLDAPSetup en el que se describen los pasos para configurar un servidor totalmente operativo en distribuciones Debian y derivadas.

En OpenLDAP, para usar la característica de pertenecia a grupo, es necesario añadir un 'overlay' llamado 'membeof'. Es un módulo que añade un atributo interno a los usuarios que son miembros de un grupo.

Estos son los pasos para configurar el módulo:

- Crear un archivo 'ldap_memberof_add.ldif' con este contenido:

```
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib/ldap
olcModuleLoad: memberof
```

- Crear un archivo 'ldap_memberof_config.ldif' con este contenido:

```
dn: olcOverlay=memberof,olcDatabase={1}hdb,cn=config
objectClass: olcMemberOf
objectClass: olcOverlayConfig
objectClass: olcConfig
objectClass: top
olcOverlay: memberof
olcMemberOfDangling: ignore
olcMemberOfRefInt: TRUE
olcMemberOfGroupOC: groupOfNames
olcMemberOfMemberAD: member
olcMemberOfMemberOfAD: memberOf
```

- Modificar la configuración de LDAP con estos comandos:

```
ldapadd -D cn=admin,cn=config -w "password" -H ldapi:/// -f memberof_add.ldif
ldapadd -D cn=admin,cn=config -w "password" -H ldapi:/// -f memberof_config.ldif
```

### *Consejos*

- Comprobar que si el usuario 'admin' de sysPass coincide con el de LDAP, es necesario añadir este usuario al grupo de LDAP que tiene permisos de acceso a sysPass.
- El nombre y email de los usuarios de LDAP son obtenidos de los atributos 'displayname','fullname' y 'mail'.
- Es posible usar ldaps configurando la URI de conexión como 'ldaps:/ /mi_servidor_ldap'.
- Puedes instalar phpLDAPadmin para crear y administrar objetos de LDAP.

### *Enlaces*

- Wiki de LDAP en Debian: https://wiki.debian.org/LDAP/OpenLDAPSetup
- Configuración de 'memberof': http://www.cbjck.de/2012/05/enabling-the-memberof-overlay-for-openldap/

## *Aplicación*

sysPass es una aplicación que utiliza una base de datos MySQL/MariaDB para almacenar los datos de todos sus componentes excepto la configuración, que es almacenada en un archivo XML dentro del directorio "config".

### *Warning*

Es importante que el directorio "config" no sea accesible desde el servicio web, ya que puede revelar información importante.

### Encriptación

La encriptación de sysPass está basada en rijndael-256 en modo CBC mediante el uso del módulo mcrypt de PHP.

Los datos encriptados (hasta versión 2.0) son:

- Claves de las cuentas
- Datos de campos personalizados
- Exportación en formato XML de sysPass

Para hacer uso de la aplicación, por primera vez, es necesario conocer la clave maestra o la clave maestra temporal (ver Clave Maestra Temporal), ya que sólo se almacena un hash generado mediante Blowfish con un salt generado usando el generador de números aleatorios MCRYPT_DEV_URANDOM. Para la generación del hash en Blowfish se utiliza un coste de 7 para las iteraciones del algoritmo.

Tras hacer login con la clave maestra, ésta se almacena en los datos del usuario. Para su almacenamiento encriptado con rijndael-256 se utiliza una llave de 32 bytes generada con Blowfish usando la clave, el login del usuario y un salt generado con openssl_random_pseudo_bytes y almacenado en la configuración de sysPass bajo la etiqueta "passwordSalt".

En los siguientes inicios de sesión la clave maestra es recuperada desde los datos del usuario y desencriptada usando la clave, el login del usuario y el salt generado en la configuración de sysPass. Esta clave es almacenada en la sesión del usuario mediante la encriptación de la misma con una llave generada con Blowfish usando el ID de sesión de PHP y el salt de la aplicación.

#### Note

El ID de sesión de PHP es regenerado cada tiempo_máximo_sesion/2

En el caso de que la clave maestra sea cambiada se solicitará a todos los usuarios la nueva clave o una clave maestra temporal (ver Clave Maestra Temporal).

Si un usuario canbia su clave de acceso, en el siguiente login, se le solicitará la clave anterior para poder obtener la clave maestra. Si no es posible obtener la clave maestra, se le solicitará.

### Clave Maestra Temporal

Es posible generar una clave maestra temporal para su uso por los usuarios de la aplicación, así no es necesario conocer la clave maestra original.

Para la generación de la clave maestra temporal se utiliza la clave maestra original encriptada con rijndael-256 y una llave de 32 bytes generada usando openssl_random_pseudo_bytes cuyo hash Blowfish es almacenado en la tabla "config" de la base de datos.

#### Note

Para la comprobación de la clave maestra temporal **sólo** se utiliza el hash generado con Blowfish

### PKI

Para mejorar la seguridad de los datos enviados, se hace uso de PKI para la encriptación de las claves que son enviadas desde los formularios de la aplicación.

Las claves pública y privada son generadas en el directorio "config" de la aplicación.

### *Warning*

Tener en cuenta que el mayor riesgo de seguridad está en los propios usuarios, ya que una clave comprometida puede causar una brecha de seguridad.

Un servidor de sysPass comprometido puede ser peligroso si la base de datos está junto al servidor web, debido a que los datos de red pueden ser obtenidos por lo que las claves serían reveladas.

## *Autentificación*

Para la autentificación de sysPass es posible utilizar varios métodos:

- Base de datos MySQL/MariaDB (por defecto)
- Directorio LDAP (OpenLDAP, eDirectory, Active Directory, freeIPA, etc)

### *Note*

Si está activada la opción de LDAP, la autentificación con base de datos es utilizada cuando el servicio de LDAP no está accesible o el usuario no existe.

Para la autentificación con base de datos se comprueba un hash generado con Blowfish de la clave del usuario, por lo que la clave **nunca** se almacena.

Si se utiliza LDAP:

- Se almacena el hash de la clave del usuario generado con Blowfish para comprobarlo en caso de fallo del servicio de LDAP.
- No es posible editar el login, nombre e email del usuario.

## *Autorización*

Para la autorización de sysPass es posible utilizar varios métodos:

- Auth Basic (por defecto)
- Doble Factor 2FA (plugin Authenticator)

La autorización del tipo Auth Basic siempre es comprobada, por lo que si se reciben las cabeceras HTTP con los datos del usuario, se comprobará si el login del usuario de sysPass es igual al de Auth Basic.

La autorización 2FA mediante el plugin Authenticator es realizada mediante la generarión de un token OTP desde la aplicación Google Authenticator. Esta autorización es posible activarla desde las preferencias de cada usuario.

## *Permisos*

Los permisos en sysPass se establecen en los perfiles de los usuarios. Por defecto sólo se puede realizar una búsqueda de cuentas.

Existen 29 tipos de permisos:

- **Cuentas**
  - Crear - permite crear cuentas
  - Ver - permite ver los detalles de las cuentas [1]
  - Ver Clave - permite visualizar las clave de las cuentas [1]
  - Editar - permite modificar las cuentas y sus archivos [1]
  - Editar Clave - permite modificar las claves de las cuentas [1]
  - Eliminar - permite eliminar las cuentas [1]
  - Archivos - permite visualizar los archivos de las cuentas

- Compartir Enlace - permite crear enlaces públicos
- Privada - permite crear cuentas privadas
- Privada para Grupo - permite crear cuentas privadas sólo para el grupo principal
- Permisos - permite ver y modificar los permisos de las cuentas [1]
- Búsqueda Global - permite realizar una búsqueda en todas las cuentas excepto las privadas [2]

- **Gestión**
  - Usuarios - permite acceso total a la gestión de usuarios [3]
  - Grupos - permite acceso total a la gestión de grupos
  - Perfiles - permite acceso total a la gestión de perfiles
  - Categorías - permite acceso total a la gestión de categorías
  - Clientes - permite acceso total a la gestión de clientes
  - Campos Personalizados - permite acceso total a la gestión de campos personalizados
  - Autorizaciones API - permite acceso total a la gestión de autorizaciones API
  - Enlaces Públicos - permite acceso total a la gestión de enlaces públicos
  - Cuentas - permite acceso total a la gestión de cuentas
  - Archivos - permite acceso total a la gestión de archivos
  - Etiquetas - permite acceso total a la gestión de etiquetas
- **Configuración**
  - General - permite acceso total a la configuración del sitio, cuentas, wiki, ldap y correo
  - Encriptación - permite acceso total a la configuración de la clave maestra
  - Copia de Seguridad - permite acceso total a la realización de copias de seguridad [4]
  - Importación - permite acceso total a la importación de archivos XML y CSV
- **Otros**
  - Registro de Eventos - permite acceso total al registro de eventos

A nivel de usuario es posible establecer los siguientes permisos:

- Admin Aplicacion: permite acceso total a todos los módulos de la aplicación
- Admin Cuentas: permite acceso total a todas las cuentas excepto las privadas

## *ACL*

- Un usuario sólo puede visualizar o modificar las cuentas propias, de su grupo principal y las que tienen establecido el usuario o grupo secundario
- Un grupo puede contener varios usuarios, los cuales tendrán acceso a las cuentas de dicho grupo
- Una cuenta sólo puede ser modificada por los usuarios o grupos principales y los secundarios si está establecido el permiso de modificación en los accesos de la cuenta
- Las cuentas privadas sólo son accesibles por el propietario
- Las cuentas privadas para grupo sólo son accesibles por los usuarios el grupo principal

Notas

## *Búsqueda de Cuentas*

La búsqueda de cuentas realiza una consulta del texto introducido en los campos "nombre", "login", "url" y "notas".

Es posible fltrar los resultados mediante la selección de categoría, cliente o etiquetas.

El filtrado mediante etiquetas es acumulativo ("OR"), por lo que se incluirán las cuentas con las etiquetas seleccionadas.

Existen filtros especiales que son introducidos en el campo de texto:

| Filtro | Descripción |
|---|---|
| user:login | Devolver las cuentas a las que el usuario con login "login" tenga acceso |
| owner:login | Devolver las cuentas en las que "login" es propietario |
| maingroup:group_name | Devolver las cuentas con grupo principal "group_name" |
| group:group_name | Devolver las cuentas a las que el grupo con nombre "group_name" tenga acceso |
| file:file_name | Devolver las cuentas que contengan el archivo con nombre "file_name" |
| expired: | Devolver las cuentas con clave caducada |
| private: | Devolver las cuentas privadas del usuario actual |

## *API*

La API de sysPass utiliza JSON-RPC v2 para el intercambio de mensajes entre cliente-servidor.

La URL de acceso a la API es "https://servidor/sysPass/api.php".

### *Métodos*

#### *getAccountSearch*

Realiza una búsqueda de cuentas

| Parámetro | Descripción |
|---|---|
| text | Texto a buscar |
| count | Número de resultados a mostrar |
| categoryId | Id de categoría a filtrar |
| customerId | Id de cliente a filtrar |

#### *getAccountData*

Obtiene los detalles de una cuenta

| Parámetro | Descripción |
|---|---|
| id | Id de la cuenta |
| userPass | Clave del usuario asociado al token |

#### *getAccountPassword*

Obtiene la clave de una cuenta

| Parámetro | Descripción |
|---|---|
| id | Id de la cuenta |
| userPass | Clave del usuario asociado al token |
| details | Devolver detalles en la respuesta |

#### *addAccount*

Crea una cuenta

| Parámetro | Descripción |
|---|---|

| | |
|---|---|
| userPass | Clave del usuario asociado al token |
| name | Nombre de cuenta |
| categoryId | Id de categoría |
| customerId | Id de cliente |
| pass | Clave |
| login | Usuario de acceso |
| url | URL o IP de acceso |
| notes | Notas sobre la cuenta |

### *deleteAccount*

Elimina una cuenta

| Parámetro | Descripción |
|---|---|
| id | Id de la cuenta |

### *getCategories*

Realiza una búsqueda de categorías

| Parámetro | Descripción |
|---|---|
| name | Nombre a buscar |
| count | Número de resultados a mostrar |

### *addCategory*

Crea una categoría

| Parámetro | Descripción |
|---|---|
| name | Nombre de la categoría |
| description | Descripción |

### *deleteCategory*

Elimina una categoría

| Parámetro | Descripción |
|---|---|
| id | Id de la categoría |

### *getCustomers*

Realiza una búsqueda de clientes

| Parámetro | Descripción |
|---|---|
| name | Nombre a buscar |
| count | Número de resultados a mostrar |

---

1(1, 2, 3, 4, 5, 6) Sólo a las cuentas a las que el usuario y su grupo tienen acceso
2 En caso de no tener acceso a la cuenta, sólo es posible realizar una "Solicitud de Modificación"
3 Los usuarios "Admin Aplicación" no pueden ser modificados por otros usuarios
4 Sólo los usuarios "Admin Aplicación" pueden descargar archivos de copia de seguridad o XML

### *addCustomer*

Crea un cliente

| Parámetro | Descripción |
|---|---|
| name | Nombre del cliente |
| description | Descripción |

### *deleteCustomer*

Elimina un cliente

| Parámetro | Descripción |
|---|---|
| id | Id del cliente |

### *backup*

Realiza una copia de seguridad de la aplicación

## *Actualización*

Para la actualización de sysPass son necesarios los siguientes pasos:

1. Descargar la aplicación desde https://github.com/nuxsmin/sysPass/releases y descomprimir los archivos
2. Establecer el propietario y permisos del directorio de sysPass
3. Copiar los archivos ("config.xml", "key.pem" y "pubkey.pem") del directorio "config" de la versión actual a la nueva
4. Acceder desde un navegador a la aplicación

Si la aplicación requiere de actualización de la base de datos:

1. **Realizar una copia de seguridad de la base de datos**
2. Introducir el código de actualización que se encuentra en el archivo "config/config.xml" con la etiqueta "upgradeKey"

### *Note*

Tras la actualización, se mostrará un mensaje y en el registro de eventos se pueden revisar los detalles de la actualización

## *Preguntas Frecuentes*

### *¿Para qué sirve sysPass?*

sysPass un gestor de claves que permite almacenarlas de forma segura mediante encriptación de doble sentido con clave maestra. Las claves están asociadas a cuentas, las cuales tienen información detallada del propósito de la misma como: cliente, categoría, notas, archivos, etc.

La idea inicial era la de hacer accesible las claves de cuentas de acceso a servidores y servicios en un entorno multiusuario, de forma segura y que pudiera ser exportable a una memoria externa.

### *¿Dónde se puede instalar sysPass?*

La aplicación pueder ser instalada en cualquier sistema que disponga de Apache, PHP y MySQL.

### *¿Cómo se instala sysPass?*

Bajar la aplicación desde https://github.com/nuxsmin/sysPass/releases/latest y seguir los pasos de Instalación

## ¿Qué métodos de autentificación utiliza?

sysPass utiliza MySQL/MariaDB o LDAP como “backends” de autentificación.

En caso de utilizar LDAP, si no es posible conectar con el servidor de LDAP, se utilizará MySQL como “backend” utilizando los datos de acceso de la última sesión iniciada en LDAP.

Para más información ver: Autentificación

## ¿Para qué sirve la encriptación?

La encriptación de las claves en la base de datos permite que, en caso de que alguien tenga acceso a ésta o si se realiza una exportación de la misma, no sea legible sin la clave maestra.

Esta solución es muy conveniente para ejecutar la aplicación desde un pendrive, para casos en los que no es posible acceder al servidor donde se almacena la aplicación. ¿Qué tipo de encriptación utiliza?

El esquema de cifrado utilizado es rijndael-256 en modo CBC.

Para más información ver: Encriptación

## ¿Qué quiere decir “portable”?

Este término se refiere a aquellas aplicaciones que pueden ser ejecutadas sin realizar la instalación de componentes en el sistema operativo que la ejecuta.

Esta aplicación es posible hacerla “portable” mediante la instalación de apache, php y mysql en una unidad externa. Para ello, es posible utilizar cualquiera de los paquetes LAMP disponibles como WAMP, XAMPP, etc.

La herramienta de backup permite realizar una copia de todo el entorno (aplicación y base de datos), para poder instalarlo en la unidad externa. La encriptación de los datos de las cuentas, hace que la seguridad sea muy alta en caso de pérdida de la unidad extraíble.

## ¿Hay una clave maestra por cada cuenta/usuario?

La clave maestra es global para todas las cuentas y usuarios.

Cada vez que un usuario se dé de alta, cambie su clave personal o se reestablezca la clave maestra, será necesario que éste la introduzca en el siguiente inicio de sesión.

Cada vez que se produzca un cambio de clave maestra, los usuarios que tengan iniciada la sesión, sólo podrán visualizar las cuentas hasta que introduzca la nueva clave.

Para más información ver: Encriptación

## ¿Qué son los enlaces a Wiki?

Nos permiten enlazar las cuentas con un determinado patrón de nombre, a una Wiki externa que permita pasar el nombre de la cuenta como parámetro en la URL.

Hay dos tipos de enlaces, uno que enlaza con la página de búsqueda de la Wiki y pasa como parámetro el nombre del cliente, y otro, que enlaza directamente con la página de la cuenta.

## ¿Para qué sirven las categorías?

Las categorías tienen como objetivo el clasificar las cuentas para poder realizar búsquedas más precisas.

## ¿Para qué sirven los grupos de usuarios?

Estos grupos se utilizan para dar acceso a los usuarios a las cuentas que tengan dicho grupo como principal o secundario.

## ¿Para qué sirve el campo cliente?

Al igual que las categorías, es posible hacer búsquedas basadas en el cliente. Este campo se puede tratar de forma genérica como departamento, empresa, división, etc.

En futuras versiones se podrán asociar usuarios a clientes.

### *¿Existe un histórico de cuentas?*

Sí, cada vez que se realiza una modificación de una cuenta, se realiza una copia del estado anterior de la misma.

En los detalles de la cuenta se puede visualizar cada registro del histórico de una cuenta. Si la clave maestra con la que fue guardada la cuenta en dicho punto no conincide con la actual, no se podrá mostrar.

### *¿Para qué sirven los perfiles?*

Los perfiles son usados para definir las acciones que pueden realizar los usuarios.

Existen 29 niveles de acceso que pueden ser activados de forma conjunta, permitiendo así definir a qué partes de la aplicación pueden acceder los usuarios con dicho perfil.

### *¿Qué es el modo mantenimiento?*

Este modo se utiliza para impedir que los usuarios utilicen la aplicación en las ocasiones en las que se estén realizando operaciones sobre la Base de Datos, actualizaciones, etc.

El usuario que active el modo matenimiento será el único que puede utilizar la aplicación hasta el cierre de sesión. Después de ello es necesario desactivarlo en el archivo "config/config.xml" bajo la etiqueta "maintenance"

### *¿Puedo cambiar la Clave Maestra?*

Sí, para ello es necesario conocer la actual. Se recomienda realizar una copia de seguridad de la Base de Datos.

### *No recuerdo la Clave Maestra, ¿Puedo desencriptar las claves?*

No, no es posible visualizar una clave sin la Clave Maestra.

### *¿Funciona el backup en Windows?*

Sí, desde la versión 1.1 se utiliza la librería PHAR de PHP para realizar los backups.

### *El lenguaje no cambia*

Revisa las locales instaladas en tu sistema (servidor), porque sysPass usa el sistema de internacionalización GNU gettext.

Las locales deben de ser de la variante UTF-8.