# Cifrado de contraseñas

# Cifrado de contraseñas

Pandora FMS permite cifrar las contraseñas que se almacenan en la base de datos.

La clave de cifrado se genera a partir de una contraseña proporcionada por el usuario y no se guarda en la base de datos (*ni la contraseña ni la clave*), de modo que las contraseñas no se puedan recuperar de un volcado de la base de datos.

Una vez el usuario configura la contraseña, el cifrado funciona de forma transparente para el usuario.

Si se pierde la contraseña proporcionada por el usuario no podrá recuperar las contraseñas almacenadas en la base de datos de Pandora FMS. Guárdese en lugar seguro o hágase un respaldo (*backup*) de los ficheros `config.php` y `pandora_server.conf`.

## Detalles técnicos

Las contraseñas se cifran utilizando el cifrado Rijndael con bloques de 128 bits en modo ECB. Una clave de 256 bits se genera en el arranque a partir del MD5 de la contraseña configurada por el usuario.

## Configuración en una instalación nueva de Pandora FMS

Para habilitar el cifrado de claves, la contraseña se debe configurar tanto en el Servidor de Pandora FMS como en la Consola web.

Los pasos a seguir para el cifrado son los siguientes:

- Detener el servidor, tanto en Command Center (Metaconsola) como en los nodos.
- Actualizar los campos encryption_passphrase en `/etc/pandora/pandora_server.conf` y `/var/www/html/pandora_console/include/config.php`, tanto en Command Center (Metaconsola) como en los nodos.

```
$config["encryption_passphrase"]="your encryption passphrase";
```

- Lanzar el *script* de cifrado tanto en Command Center (Metaconsola) como en los nodos.

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

Se deberá reiniciar el servidor de Pandora FMS después de haber efectuado los cambios y haber lanzado el *script*.

## Cambiando la contraseña de cifrado

Es posible cambiar la contraseña de cifrado en caso de que se haya visto comprometida. Primero debe descifrar las contraseñas almacenadas en la base de datos:

```
/usr/bin/pandora_encrypt_db -d /etc/pandora/pandora_server.conf
```

A continuación, después de haber cambiado la contraseña de cifrado (como se describe en la sección para la configuración en una instalación nueva), se pueden cifrar de nuevo:

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

A partir de 7.0 NG 739 se incluye el gestor de credenciales seguro. Consulte la siguiente sección para finalizar correctamente este proceso.

Gestor de credenciales:

En caso de disponer de una base de datos cifrada, para poder seguir utilizando el gestor de credenciales sin perder datos *será necesario descifrar todo* menos la tabla tcredential_store.

Para ello ejecute los siguientes comandos:

```
/usr/bin/pandora_encrypt_db -d -c /etc/pandora/pandora_server.conf
```

Con lo que quedará descifrado.

Una vez descifrado, se volverá a cifrar de nuevo:

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

Si solo desea cifrar de cero, bastará con ejecutar el último comando.

## Quitando la contraseña de cifrado

Se recomienda mantener de manera cifrada toda contraseña almacenada en Pandora FMS.

- Detenga el servidor, tanto en Command Center (Metaconsola) como en los nodos.
- Lanzar el *script* de descifrado tanto en Command Center (Metaconsola) como en los nodos.

```
/usr/bin/pandora_encrypt_db -d /etc/pandora/pandora_server.conf
```

- Comentar encryption_passphrase en `/etc/pandora/pandora_server.conf` y `/var/www/html/pandora_console/include/config.php` tanto en Command Center (Metaconsola) como en los nodos.

```
# $config["encryption_passphrase"]="your encryption passphrase";
```

Se deberá reiniciar el servidor de Pandora FMS después de haber efectuado los cambios y haber lanzado el *script*.

Volver al índice de la documentación de Pandora FMS