

PANDORAFMS



Cifrado de contraseñas

20-09-2021





Cifrado de contraseñas

[Volver al Índice de Documentación Pandora FMS](#)

Cifrado de contraseñas en Pandora FMS

Pandora FMS permite cifrar las contraseñas que almacena 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 pierde la contraseña proporcionada por el usuario no podrá recuperar las contraseñas almacenadas en la base de datos de Pandora FMS. Guárdela en un lugar seguro o haga un 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. Los pasos a seguir para la encriptación son los siguientes:

- Detener el servidor, tanto en meta como en nodo.
- Actualizar los **encryption_passphrase** en */etc/pandora/pandora_server.conf* y */var/www/html/pandora_console/include/config.php* tanto en **nodo** como en **meta**.

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

- Lanzar el script de encriptado tanto en **nodo** como en **meta**.



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

No olvide reiniciar el servidor de Pandora FMS después de efectuar los cambios y lanzar el script.

Configuración en una instalación existente de Pandora FMS

Configure el cifrado de contraseñas siguiendo los pasos descritos para una instalación nueva. Desde este momento las nuevas contraseñas que se introduzcan en la consola de Pandora FMS se guardarán cifradas en la base de datos. Sin embargo, deberá cifrar las contraseñas ya existentes. Para ello siga los siguientes pasos:

- Detener el servidor tanto en **meta** como en **nodo**.
- Lanzar el script de descifrado tanto en **meta** como en **nodo**:

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

- Lanzar el script de encriptado tanto en **nodo** como en **meta**:

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

- Iniciar de nuevo el servidor de meta y de nodo.

El script no permitirá ejecutarse una segunda vez; de lo contrario se corromperían las contraseñas.



Es importante tener en cuenta que el parámetro **-e** será obligatorio añadirlo para descifrar solo las contraseñas antiguas. En caso de no añadir ese parámetro a bases de datos encriptadas anteriormente, se **perderán las contraseñas**.



Esta sección solo deberá tenerse en cuenta si se quiere actualizar de la versión 743 a la 744. Si este no es el caso, deberá realizarse el cifrado como si fuese nuevo.



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 7.0NG.739 se incluye el gestor de credenciales seguro.

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

Para ello ejecutamos los siguientes comandos:

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

Con lo que dejaremos todo descifrado.

Una vez descifrado, se volverá a encriptar de nuevo:

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

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

[Volver al Índice de Documentación Pandora FMS](#)



From:
<https://pandorafms.com/manual/> - **Pandora FMS Documentation**

Permanent link:
https://pandorafms.com/manual/es/documentation/07_technical_annexes/08_password_encryption

Last update: **2021/09/16 09:17**