Password encryption

Password encryption

Pandora FMS allows to encrypt the passwords stored in the database.

The encryption key is generated from a user-supplied password and is not stored in the database (*neither the password nor the key*), so that passwords cannot be recovered from a database dump.

Once the user sets the password, the encryption works transparently to the user.

If the password provided by the user is lost, you will not be able to recover the passwords stored in the Pandora FMS database. Save in a safe place or make a backup of the `config.php` and `pandora_server.conf` files.

Technical details

Passwords are encrypted using the Rijndael cipher with 128-bit blocks in ECB mode. A 256-bit key is generated at startup from the MD5 of the password set by the user.

Configuration in a new Pandora FMS installation

To enable key encryption, the password must be configured both in the Pandora FMS Server and in the Web Console.

The steps to follow for encryption are as follows:

- Stop the server, both in Command Center (Metaconsole) and in the nodes.
- Update the encryption_passphrase fields in `/etc/pandora/pandora_server.conf` and `/var/www/html/pandora_console/include/config.php`, both in Command Center (Metaconsole) and in nodes.

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

- Launch the encryption script both in Command Center (Metaconsole) and in the nodes.

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

The Pandora FMS server should be restarted after making the changes and launching the

script.

Changing the encryption password

It is possible to change the encryption password in case it has been compromised. You must first decrypt the passwords stored in the database:

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

Then, after having changed the encryption password (as described in the section for configuration in a new installation), you can encrypt it again:

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

From 7.0 NG 739 onwards, the secure credential manager is included. Please refer to the following section to finish this process correctly.

Credential store:

If you have an encrypted database, in order to continue using the credential manager without losing data *decrypt everything* except the tcredential_store table.

To do so, execute the following commands:

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

It will be deciphered.

Once decrypted, it will be re-encrypted again:

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

If you only want to encrypt from scratch, just execute the last command.

Removing the encryption password

It is recommended to keep every password stored in Pandora FMS encrypted.

- Stop the server, both in Command Center (Metaconsole) and in the nodes.

- Launch the decryption script both in Command Center (Metaconsole) and in the nodes.

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

- Comment encryption_passphrase in `/etc/pandora/pandora_server.conf` and `/var/www/html/pandora_console/include/config.php` both in Command Center (Metaconsole) and in nodes.

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

The Pandora FMS server should be restarted after making the changes and launching the script.

Back to Pandora FMS Documentation Index