Password encryption

Go back to Pandora FMS documentation index

Password encryption in Pandora FMS

Pandora FMS supports database-stored password encryption. The encryption key is generated from a user-provided password and is not stored in the database (neither the key nor the password) so that passwords cannot be recovered from a database dump. Once the password is configured, encryption is visible for the user.

If you lose the password given by the user, you will not be able to recover the password stored in Pandora FMS Database. Save this password in a safe place and make a backup of: *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 password MD5.

Configuration in a newly installed Pandora FMS

To enable password encryption, the password must be configured in both Pandora FMS Server and Pandora FMS Console. The steps for encryption are the following:

- Stop both Metaconsole and node servers.
- Update **encryption_passphrase** in /etc/pandora/pandora_server.conf and /var/www/html/pandora_console/include/config.php both in the **node** and **Metaconsole**.

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

- Launch the encryption script both in the **node** and **Metaconsole**.

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

Do not forget to restart the Pandora FMS Server after saving the changes.

Configuration in an existing Pandora FMS installation

Configure password encryption following the steps required for a newly installed Pandora FMS. At this point, any new passwords configured in the Pandora FMS Console will be stored in the database encrypted, but already existing passwords must be encrypted too. To that end, follow these steps:

- Stop both the **Metaconsole** and **node** servers.
- Launch the decryption script both in the **Metaconsole** as well as the **node**>

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

- Launch the encryption script both in the **node** and the **Metaconsole**>

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

- Restart the Metaconsole and node servers.

The script cannot be executed twice, otherwise passwords would get corrupted.

It is important to keep in mind that the **-e** parameter must be added to decrypt only old passwords. If that parameter is not added to previously encrypted databases, **passwords will be lost**.

This section is only relevant if you wish to update from version 743 to version 744. If that is not the case, encrypt it as if it were new.

Changing the encryption password

Changing the encryption password is possible in case it gets compromised. First, passwords stored within the database must be decrypted:

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

Then, after changing the encryption password (as described in the configuration in a newly installed Pandora FMS section), they can be encrypted again:

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

From 7.0NG.739 onwards, safe credential management is included.

In case of having an encrypted database available, to be able to keep using the credential manager without losing data, decrypt everything except for the table **tcredential_store**

For that purpose, execute the following commands:

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

Leave everything decrypted.

Once decrypted, encrypt it again:

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

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

Go back to Pandora FMS documentation index