New Feature: Improved On-Premise Password Security

Product - (٠) تعليقات - Ben Henley - 2015-09-14

If you're the system administrator for a Deskpro On-Premise installation, you'll naturally take the security of your helpdesk very seriously.

Deskpro uses a one-way hashing function to store all user, agent and admin account passwords. This means that the real passwords aren't ever stored in the database at all: just a mathematical 'fingerprint' that can be used to confirm the right password was entered, but can't be used to reconstruct it (short of spending decades crunching numbers on a supercomputer).

So even if some wrong-doers get hold of your database backups, they can't get anyone's password.

However, Deskpro can't use this hash technique to protect the passwords for your ticket email accounts. Your helpdesk has to provide the real password to your mail server or provider so it can download emails.

We've added a new option to the next version of Deskpro On-Premise which provides more security for your email account passwords.

In the new **Server > Encryption** section in the admin interface, you'll see an option to encrypt the stored passwords. The details are all explained there, but the up-shot is that this prevents anyone reading the passwords from the database or a backup.

Enable Encryption

To enable encryption, click the button below. This will generate a new secure key in a file on your se result in data loss because DeskPRO won't be able to read the encrypted data anymore. Therefore,

Note: After you enable encryption, you will need direct access to the filesystem to disable it again.

☐ I understand that if I lose the encryption key file (*data/encryption-key.bin*), that any encrypted dat
☐ I have prepared a secure method of backing up the key file.

Generate Key File & Enable Encryption →

On-Premise admins, update your helpdesk to the new version now to get this feature. (Cloud users, as always, don't have to worry about technical details like this - the way Cloud handles email access means it doesn't store your passwords).

For more information about the improved password security feature, see the Sysadmin manual.