conpal LAN Crypt
Multi Factor Authentication with
YubiKey Token

The YubiKey is a hardware authentication device manufactured by Yubico. Think of it as a tiny 'safe' that can store logon information securely and independently from any computer. It comes in various form factors ranging from a token big enough to be attached to a keyring to the smallest models that are so small they hardly protrude from a device once inserted in the USB port. YubiKey does not require a battery nor extra software to be installed on the host device. Just plug it into a USB port or use NFC and you're ready to go.

How can you enhance conpal LAN Crypt with MFA?

conpal LAN Crypt is a client-side encryption solution that provides file-level encryption. Its powerful key and policy management functionality supports data using different keys for business, personal and shared data. Keys assigned to a particular user are encrypted using standardized private key cryptography. Only a user in control of the private key can access those keys. Hence protection of the private key is paramount. The YubiKey token is an ideal solution for safekeeping private keys. When used, two separate authentication factors are required – knowledge and possession –thus strengthening the general level of security.

Enable Protection

1 Define what data to protect

In the conpal LAN Crypt Admin console, define what data to protect and which key to use. A single rule can be sufficient to get all your data encrypted. Define additional rules with different keys if you plan to share data in specified folders. That's all you need for now. If you are not happy with the result, you can always come back later and fine-tune the protected locations and keys to suit your needs.

2 Assign Keys to Users

Next, assign the policies and associated encryption keys to the users. Each user receives their own personal copy, encrypted with their own personal key. Personal keys are essential for protection against unauthorized access to data. For this reason, access to these keys must be particularly well secured. This ensures that only legitimate users can access encrypted data.

Enroll YubiKey Token

3 Enroll YubiKey Token

YubiKey tokens are a perfect option for keeping personal keys safe. In order to leverage this functionality in conpal LAN Crypt, the token must first be registered and provisioned. Options include either central management, where tokens are provisioned with the personal keys directly by the issuing authority (e.g. PKI), or a self-service option, in which the user transfers their previously issued personal key to the YubiKey token for better protection.

Activate Multi Factor Authentication

4 Windows and Mac

Once initialized, the use of the YubiKey token is straightforward. Plug the token into your system and you're all set. No need to install additional software or make any changes to your configuration. Once connected, conpal LAN Crypt will automatically detect the token and make use of it for decryption of the user's profile and encryption keys.

5 Multi Factor Authentication

Access to the personal key from now on requires two factors. First the user has to hold the physical YubiKey token. Secondly, he also needs to know the tokens' end user PIN. This PIN is required to access the personal key. Once the PIN has been provided successfully, conpal LAN Crypt can perform private key operations and decrypt the user's keys. The use of YubiKey token adds two factors to the conpal LAN Crypt authentication – knowledge and possession.