Confidentiality and Data Protection 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.

Admin

YubiKey enrollment

conpal LAN Crypt leverages public key cryptography to secure encryption profiles on a per-user base. For that purpose, each user requires a certificate along with the public/private key pair assigned. The system is flexible in regards of the origin of the certificates as well as the storage location of the user's private key.

Certificates can be imported from any external Certification Authority, generate by the conpal LAN Crypt administration as self-signed certificates, or created on the YubiKey token itself. As for the private key, one option is to import the key to a safe location provided by the endpoint system itself. Another option is having the private key stored on a YubiKey token. If the key pair was generated on the token itself, this takes care of the key storage. If the key pair was generated by an external system, the user's private key needs to be imported to the token. Once the private key is available on the YubiKey token, the token can be used to unlock the user's conpal LAN Crypt profile and activate encryption.

Client

YubiKey Client Software

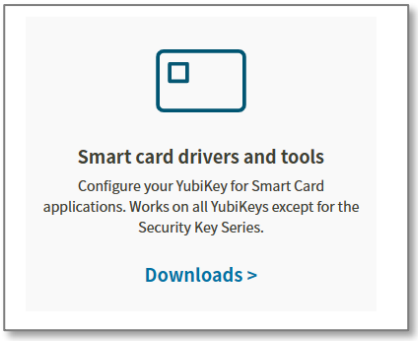
Centrally Managed token
If the YubiKey token is enrolled centrally or the keys have been created on the token itself, the token is ready for use by the end-user. Support for YubiKey PIV token is already built-in into Windows and Mac clients. There is no need to install any additional software to enable use of the token in conpal LAN Crypt. Just plug in the token to a USB port on the endpoint when prompted. Please keep on reading the conpal LAN Crypt client section below.

User Managed token
YubiKey token may be handed out to the end user without the private key provisioned. In that case, the user's private key needs to be imported to the YubiKey before it can be used to log on to the conpal LAN Crypt client. This requires some software from YubiKey to be installed on the system. Please follow the steps below to import a user's private key into the YubiKey token.

Note:
Installation instructions apply to both Windows and macOS devices.

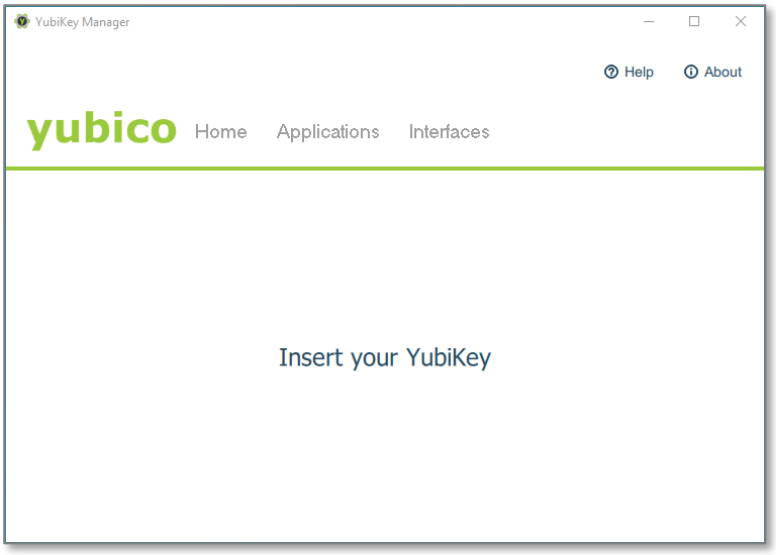
Install YubiKey Smart Card driver

The YubiKey Smart Card driver enables certificate enrollment for users and administrators, allows managing the YubiKey smart Card PIN, and supports smart card authentication on Windows. It is required by the YubiKey Manager software to manage the token.



Install YubiKey Manager

The YubiKey Manager includes both a graphical user interface and a command line tool to create PIN Unlock Keys (PUK)s on YubiKey devices for customers that require the use of a PUK. It is also used to import the user's private key into the token.
Launch the YubiKey Manager an insert the token to a local USB port.

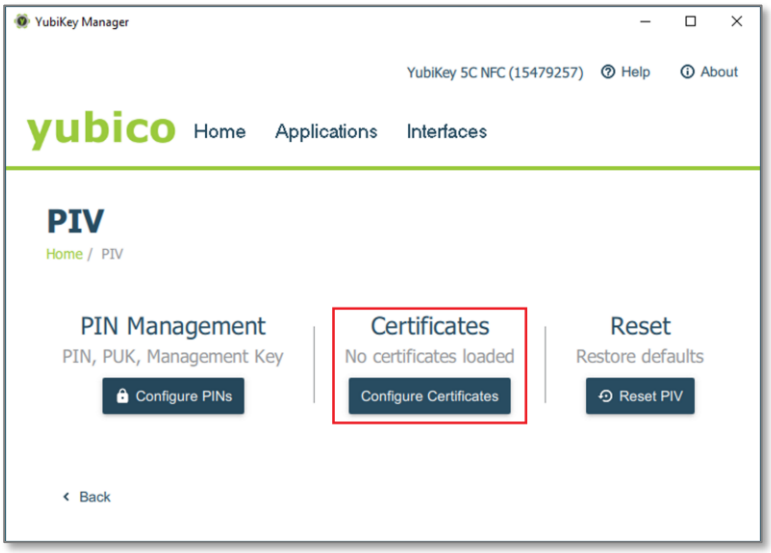


Import user key

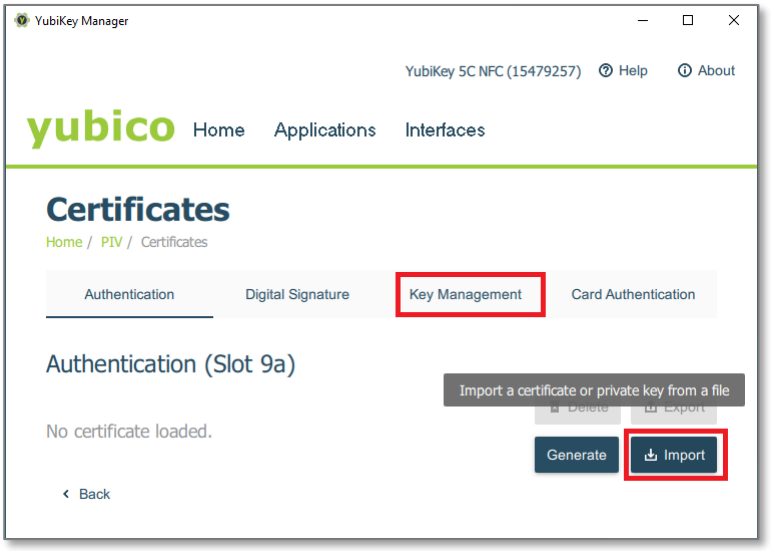
Next step is the key import. With this operation, the token is essentially 'personalized' and is tied to a particular user. Launch the YubiKey Manager and insert the token.

Navigate to the '**PIV**' option in the '**Applications**' menu to bring up the dialog with the smart card related options.

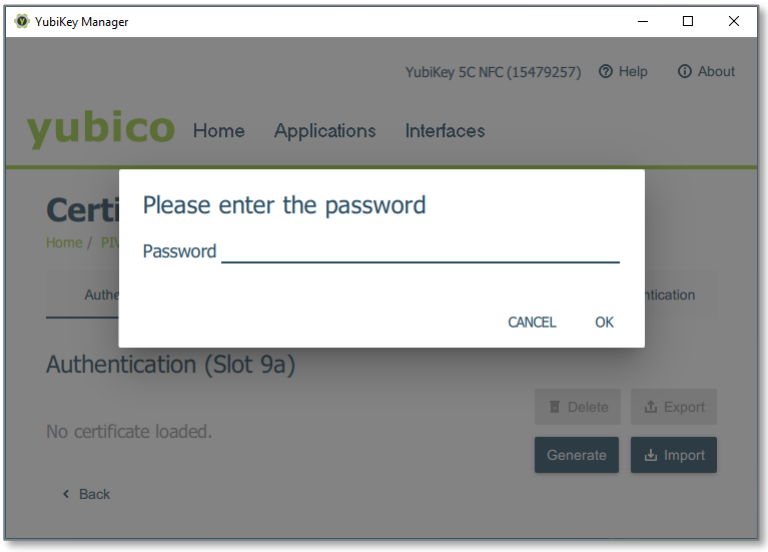
In the PIV dialog, select '**Certificates**' to get to the import page.



The YubiKey token supports four slots for storing private keys. Each slot has specific characteristics. It is important to choose the right one. For keys to be used with conpal LAN Crypt, the '**Key Management**' slot has to be used. Select '**Import**' to start the operation.



Upon import, you will be asked to select the private key to be imported. Select the **p12 file** that you want to import. This will typically be the p12 that has been provided to you by your conpal LAN Crypt admin. You will have to authenticate to the YubiKey token (i.e. present the token's PIN and management key) in order to be able to import the key.



After the import operation has completed successfully, you will be prompted with the confirmation dialog. It will give you details about the key just imported which you can use to verify.

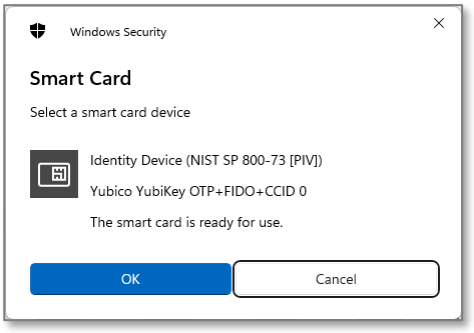
All set and done - the token can now be used in conpal LAN Crypt.

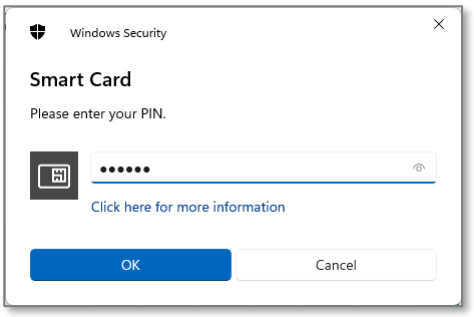
conpal LAN Crypt client authentication

The user's private key is necessary to unwrap/decrypt the profile that has been assigned to the user in the conpal LAN Crypt administration. Upon loading of a user's encryption profile, the conpal LAN Crypt client needs access to the user's private key. Depending on the storage location of the private key, the user may be prompted for a specific action. In the case of a YubiKey token, the user will have to plug in the token and authenticate to the token with his private PIN whenever a policy is loaded or updated. This is always the case when the user logs on to the system. But it can actually happen anytime in case a policy update has been triggered by the conpal LAN Crypt administrator.

Insert token and present PIN

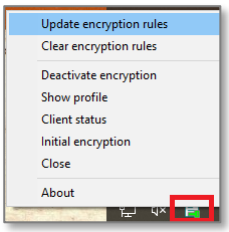
Right-click on the conpal LAN Crypt icon in the System Tray and select 'Update encryption rules'





Verify policy (optional)

Check the conpal LAN Crypt icon in the System Tray to check if the encryption profile has been loaded successfully. A green key indicates that everything is OK, indicating that the conpal LAN Crypt client has been able to successfully decrypt the user's profile using the private key stored on his YubiKey token.



Known Limitations

There are no known limitations. All YubiKey series 5 token are supported.