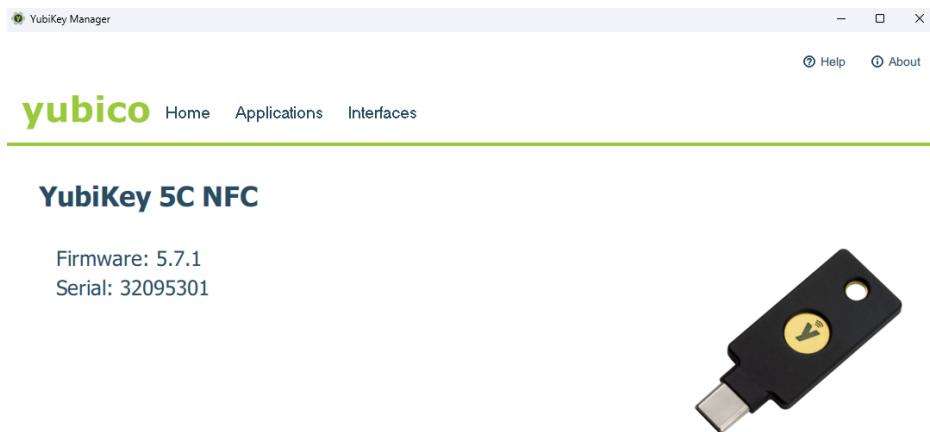


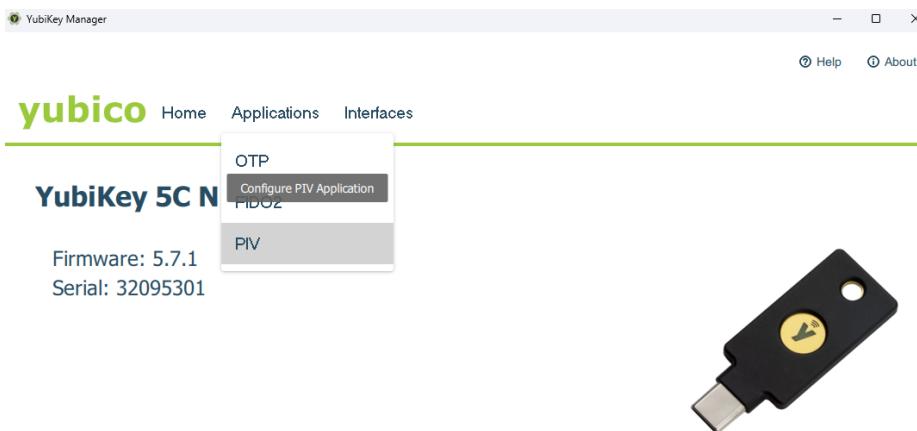
Création et configuration d'une yubikey pour la connexion VPN et VM

Brancher la yubikey au pc

Lancer yubikey manager



Cliquer sur PIV



Vous devriez arrivez sur cette page

The screenshot shows the YubiKey Manager interface for the PIV application. At the top, it displays "YubiKey Manager" and "YubiKey 5C NFC (32095301) Help About". Below that is the yubico logo and navigation links for Home, Applications, and Interfaces. The main content area is titled "PIV" and shows three sections: "PIN Management" (PIN, PUK, Management Key), "Certificates" (No certificates loaded), and "Reset" (Restore defaults). Under "PIN Management", there is a button labeled "Configure PINs". Under "Reset", there is a button labeled "Reset PIV". At the bottom left, there is a "Back" link.

Cliquez sur « RESET PIV » pour reset la configuration de la clé

The screenshot shows the YubiKey Manager interface with a confirmation dialog box overlaid. The dialog box is titled "Reset PIV?" and contains the message: "This will delete all PIV data, and restore all PINs to the default values. This action cannot be undone!". It has two buttons at the bottom: "NO" and "YES". Behind the dialog, the PIV configuration page is visible, showing the same three sections: PIN Management, Certificates, and Reset. The "Reset" section has a "Reset PIV" button. A "Back" link is also present at the bottom left.

Aller sur PIN management, puis changer le code PUK

The screenshot shows the YubiKey Manager application window. At the top, it displays "YubiKey Manager" and the device identifier "YubiKey 5C NFC (32095301)". Below the header, there's a navigation bar with links for "Home", "Applications", and "Interfaces". The main content area is titled "Change PUK" and includes a breadcrumb trail: "Home / PIV / Configure PINs / PUK". There are three input fields: "Current PUK" (containing "12345678"), "New PUK" (containing "*****"), and "Confirm new PUK" (containing "*****"). To the right of the "Current PUK" field is a checkbox labeled "Use default". Below the input fields are two buttons: "< Back" on the left and "✓ Change PUK" on the right.

Cliquez sur USE DEFAULT puis renseigner une code PUK

-8 caractères

-Majuscule, minuscule, chiffres, lettres

-Pas de caractères spéciaux (@, &, #, !, etc...)

This screenshot shows the same "Change PUK" page as the previous one, but with a notable difference: the "Use default" checkbox next to the "Current PUK" field is now checked. The other fields ("New PUK" and "Confirm new PUK") remain the same as in the first screenshot. The "Finish and change the PUK" button at the bottom has become active and is highlighted in blue.

Après cela, renseigner le code PUK dans Bitwarden à l'utilisateur

Nouveau Identifiant

Détails de l'élément

Nom de l'élément (requis)
yubikey - Henry Vu

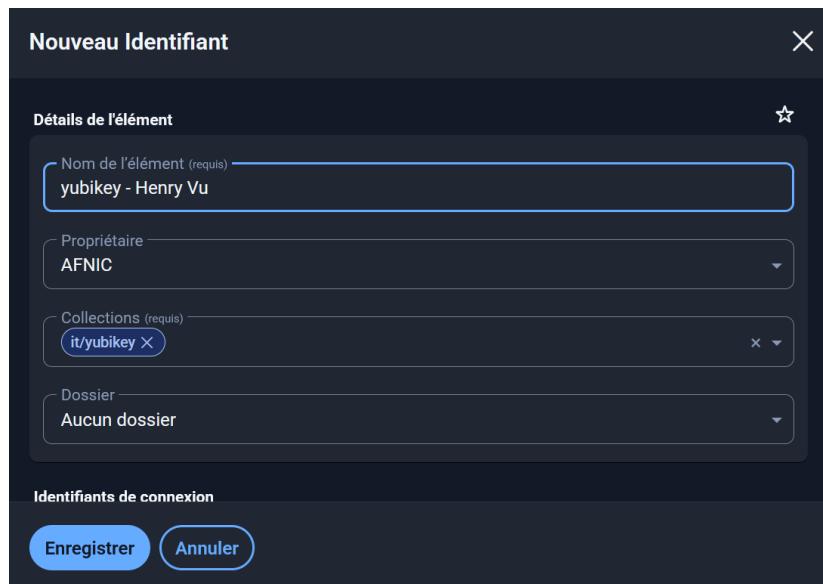
Propriétaire
AFNIC

Collections (requis)
[it/yubikey X](#)

Dossier
Aucun dossier

Identifiants de connexion

Enregistrer Annuler



Nouveau Identifiant

Identifiants de connexion

Nom d'utilisateur
PUK

Mot de passe
••••••••

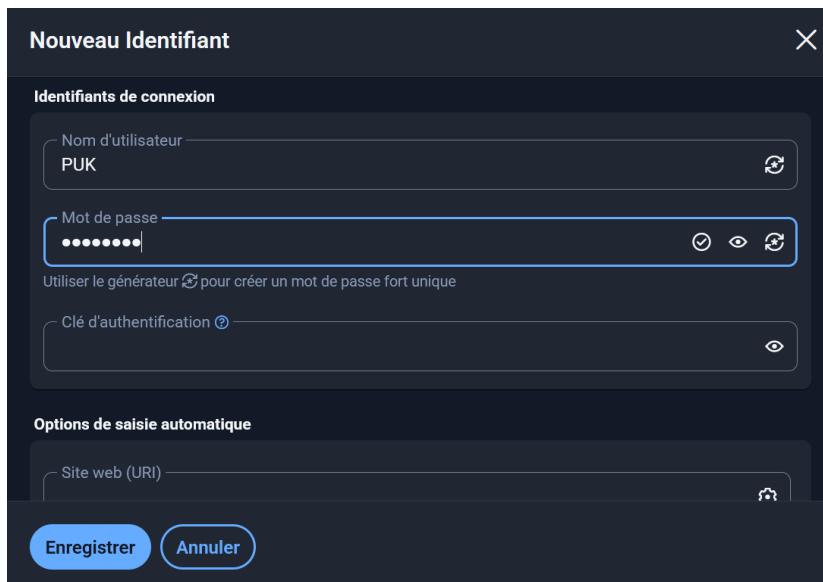
Utiliser le générateur  pour créer un mot de passe fort unique

Clé d'authentification 

Options de saisie automatique

Site web (URI)

Enregistrer Annuler



Nouveau Identifiant

+ Ajouter le site web

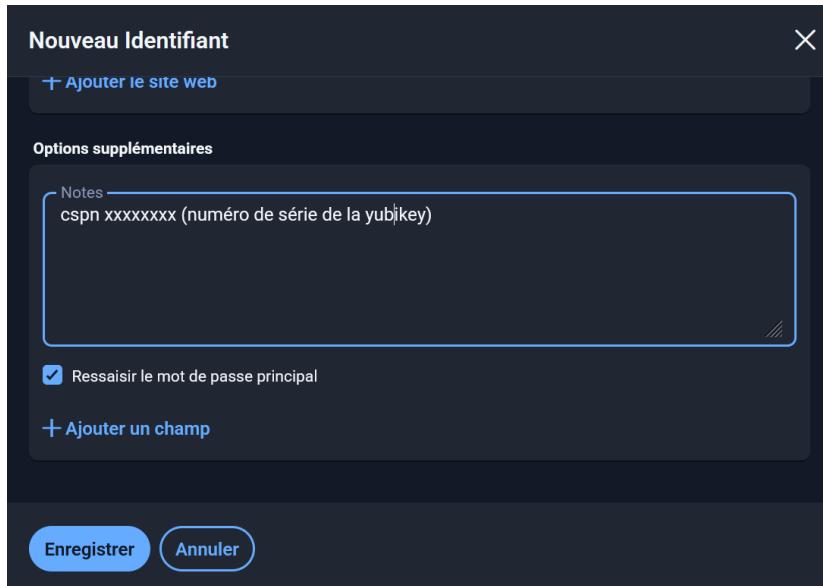
Options supplémentaires

Notes
cspn xxxxxxxx (numéro de série de la yubikey)

Ressaisir le mot de passe principal

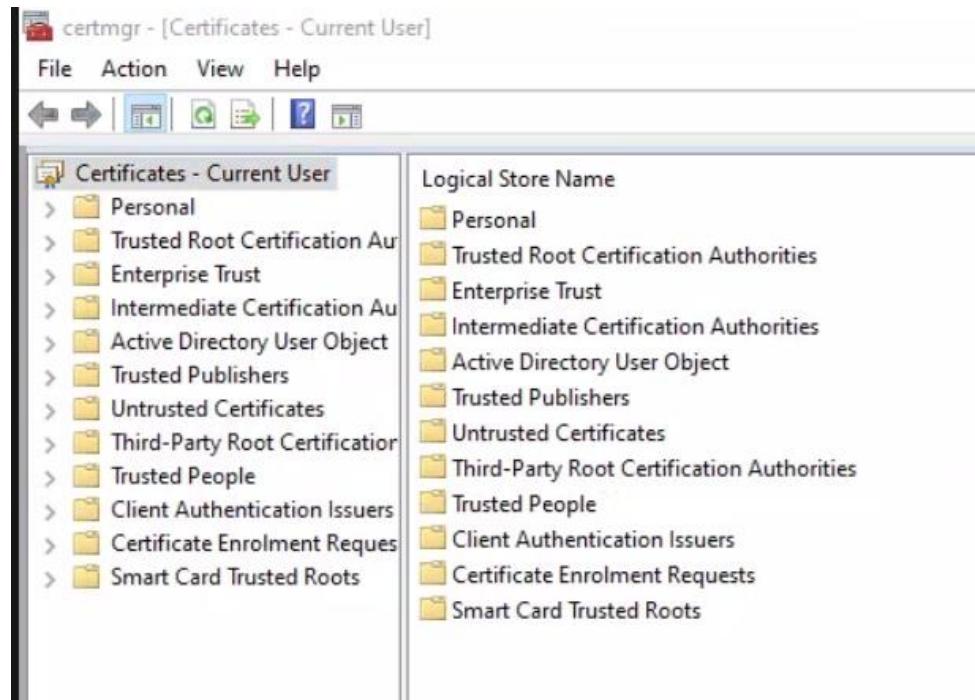
+ Ajouter un champ

Enregistrer Annuler

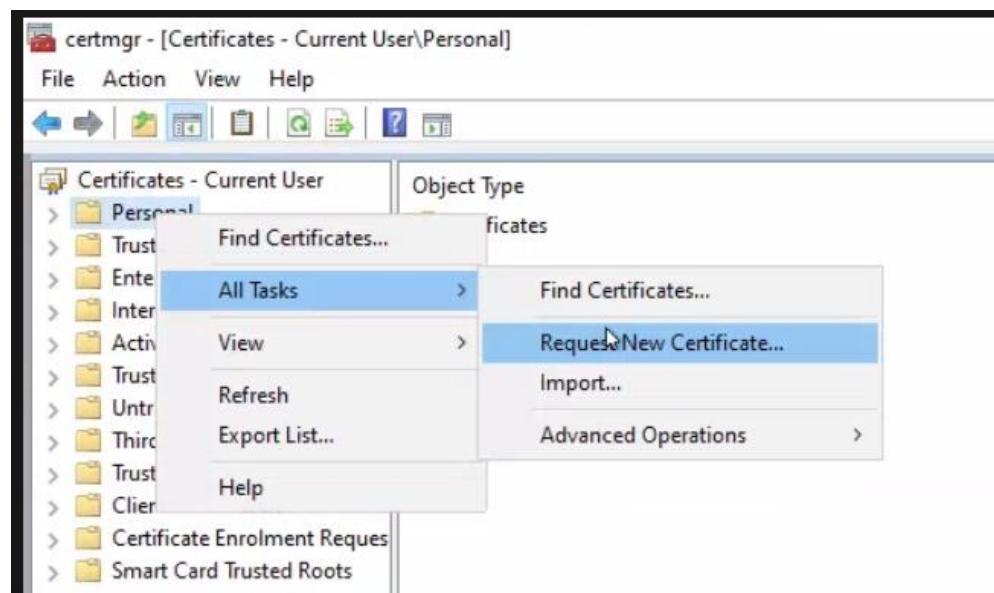


Se connecter en tant que dlg.nom depuis sa VM

Aller sur le certmgr.msc



Clic droit sur Personnel, puis All Task, puis Request New Certificate.





Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network

You have credentials that can be used to verify your right to obtain the certificate

[Next](#) [Cancel](#)



Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

Configured by you

Add New

Category	Policy
Configured by your administrator	Active Directory Enrollment Policy
Configured by you	(Empty)

[Next](#) [Cancel](#)

Sélectionner le certificat correspondant à être éligible à donner des certificats



Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

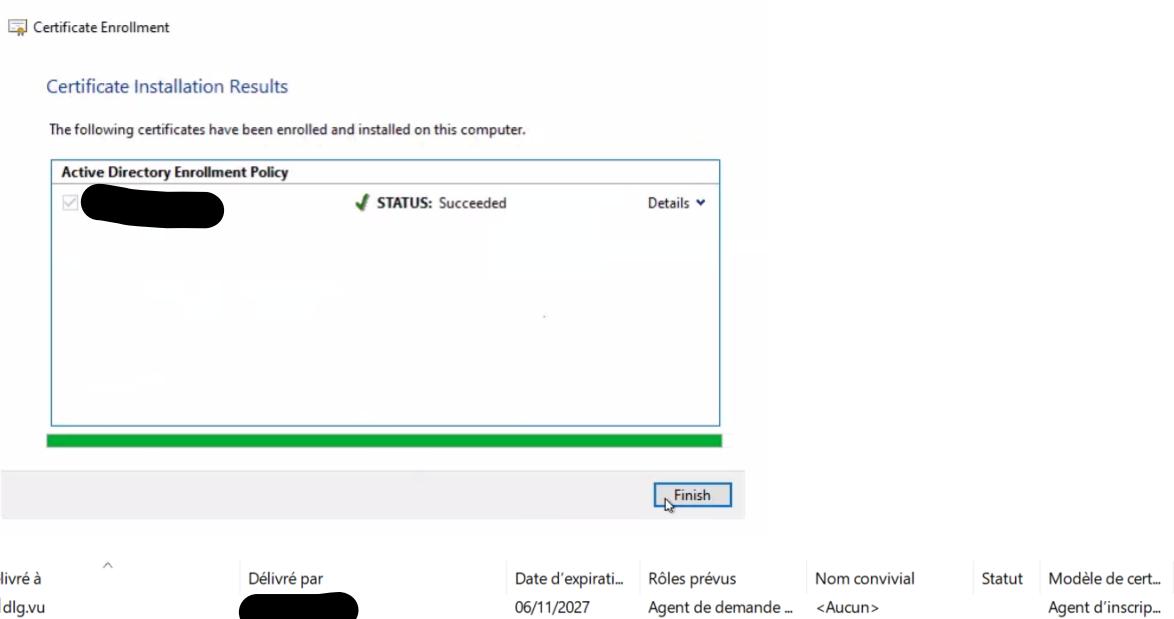
Template	Status	Action
[Redacted]	STATUS: Available	Details

Note: More information is required to enroll for this certificate. Click here to configure settings.

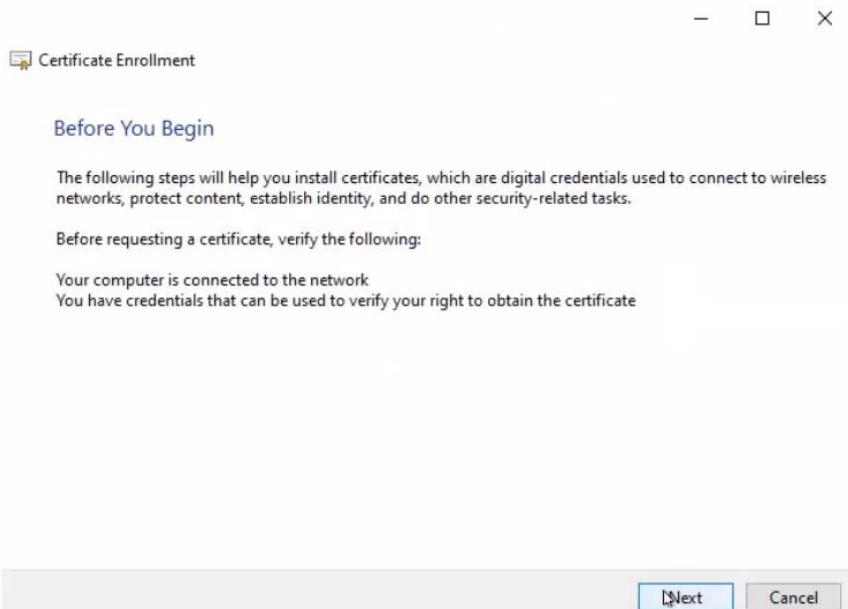
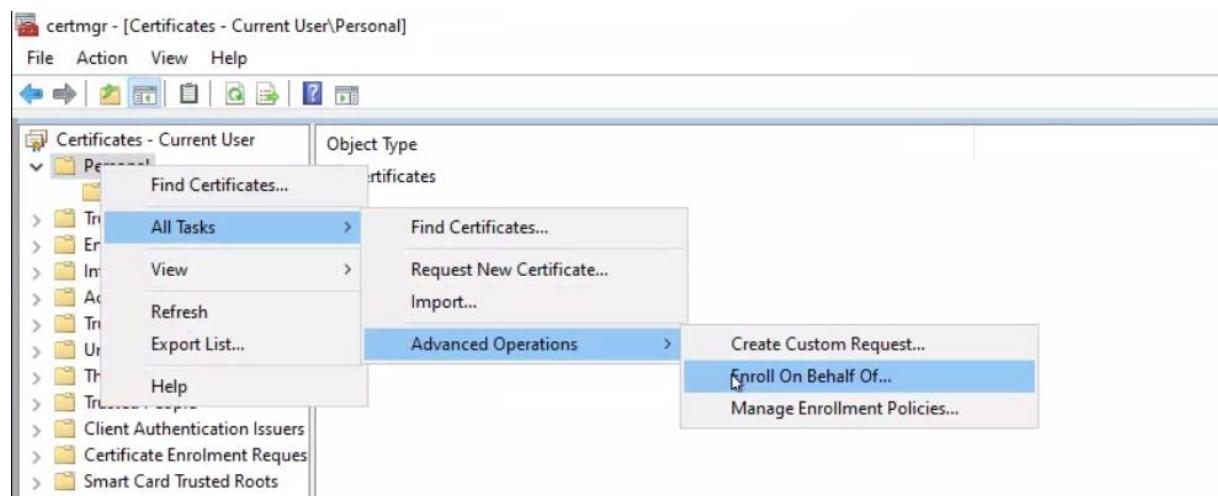
Show all templates

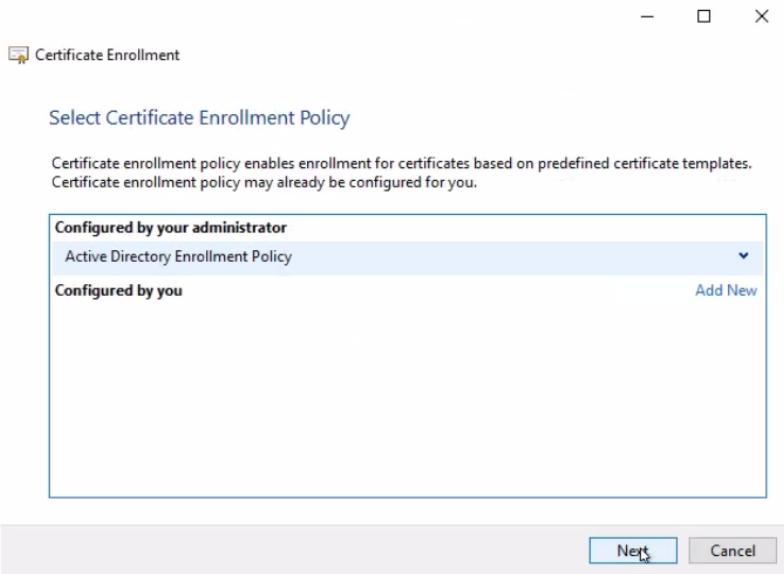
Template	Status	Action
[Redacted]	STATUS: Available	Details

[Enroll](#) [Cancel](#)

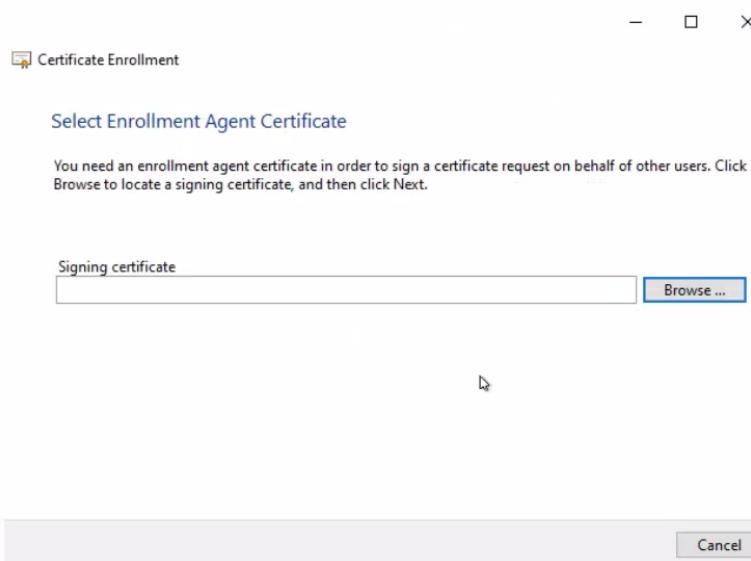


Maintenant pour configurer une yubikey utilisateur, sélectionner, All Task, Advanced Options et Enroll on Behalf Of...

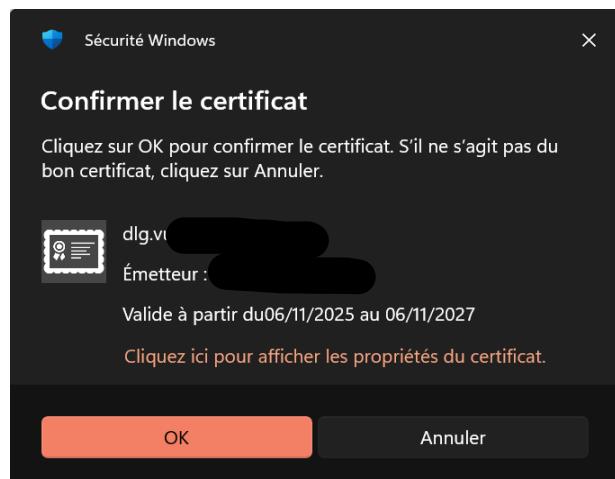




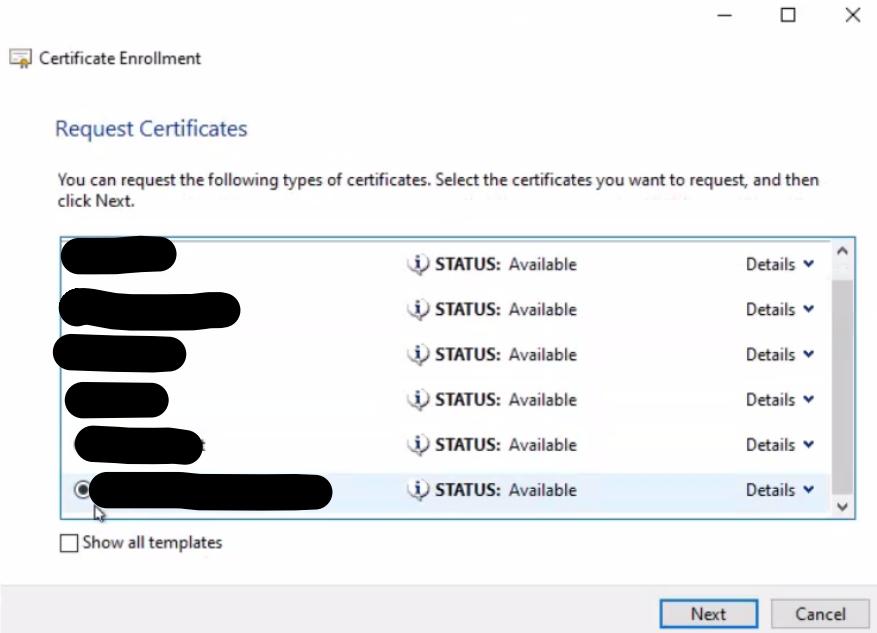
Cliquez sur Browse



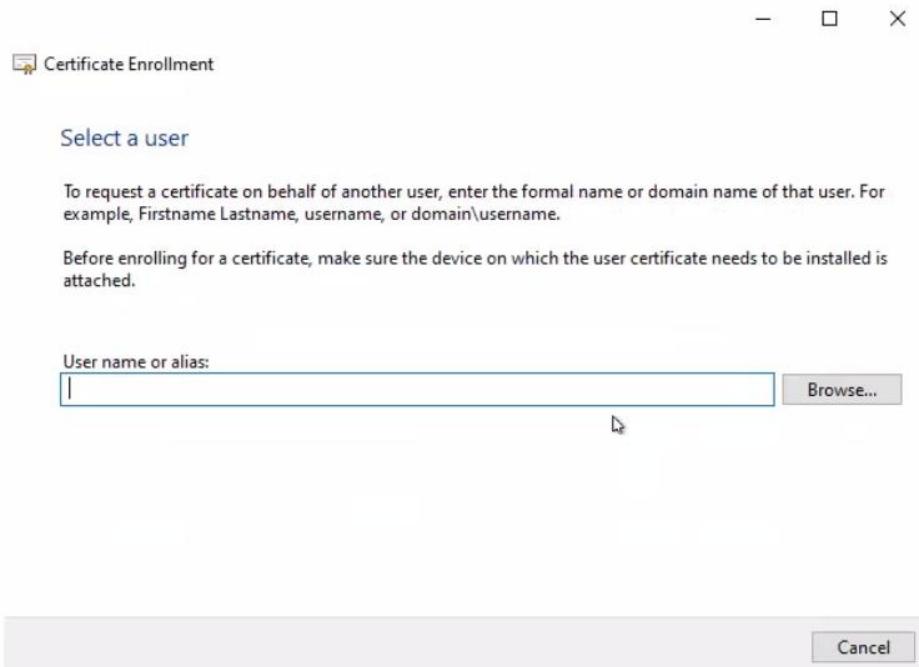
Confirmer le certificat fait précédemment



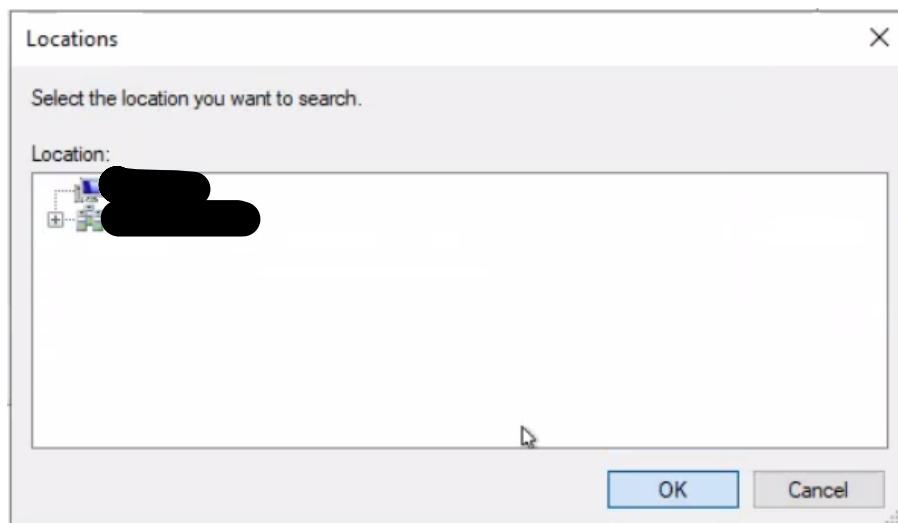
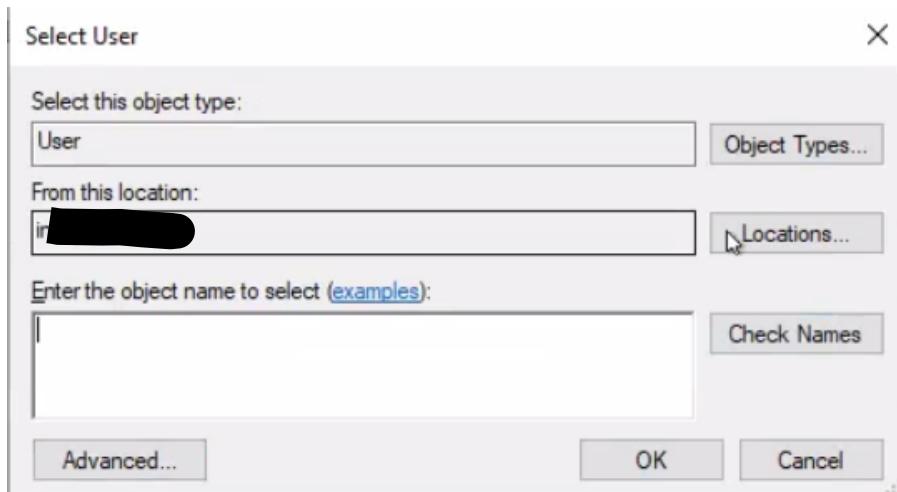
Sélectionner le certificat correspondant



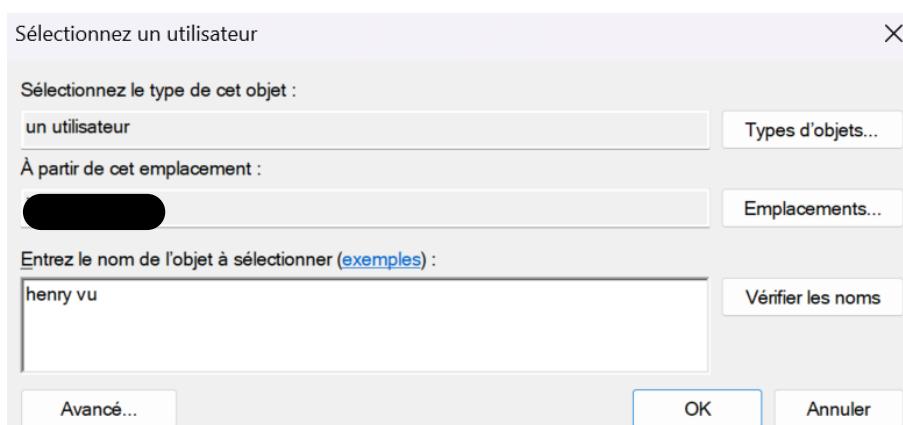
Cliquez sur Browse pour sélectionner l'utilisateur en question



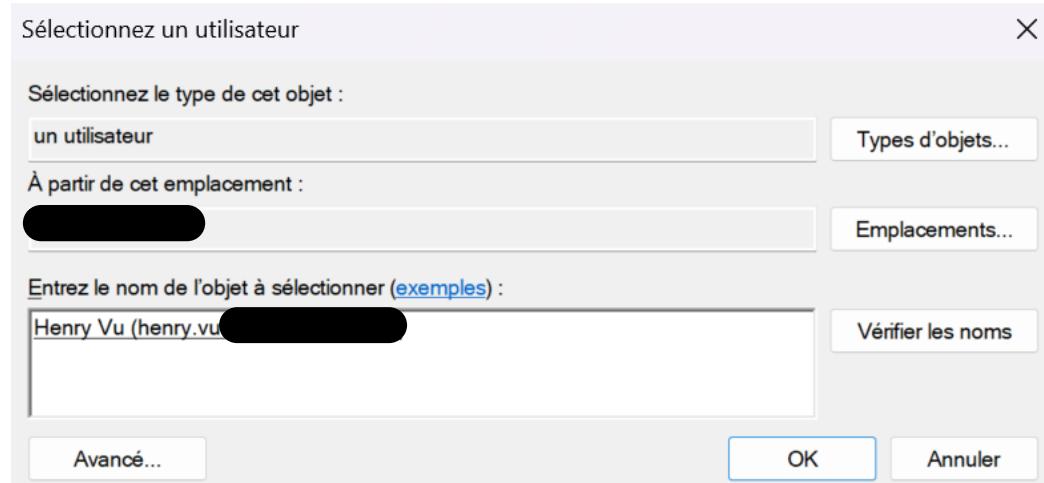
Aller sur locations puis sélectionner le domaine



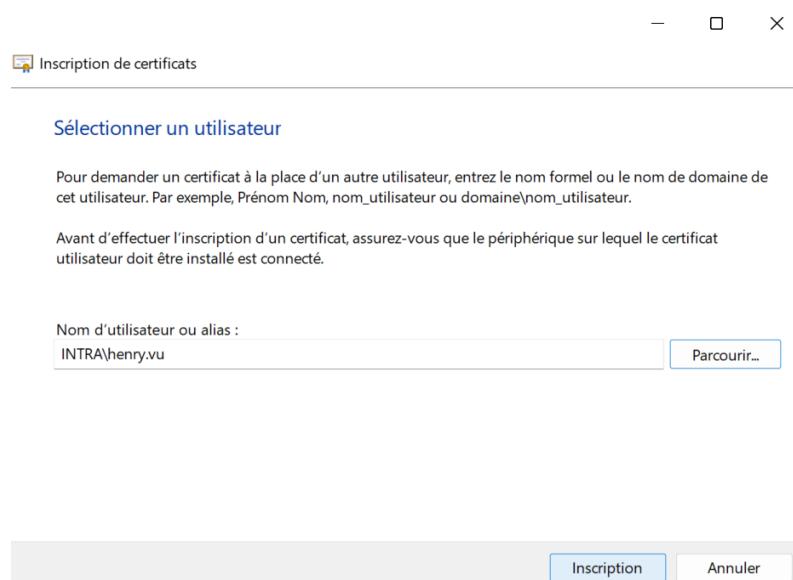
Entrer le nom de l'utilisateur



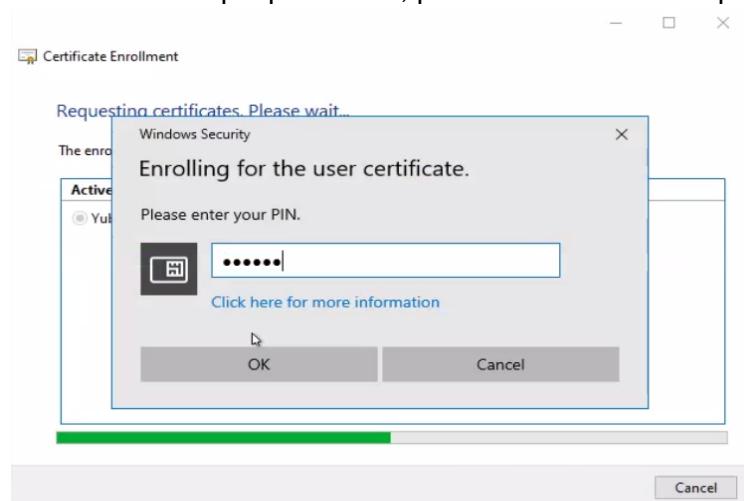
Cliquez sur vérifier les noms



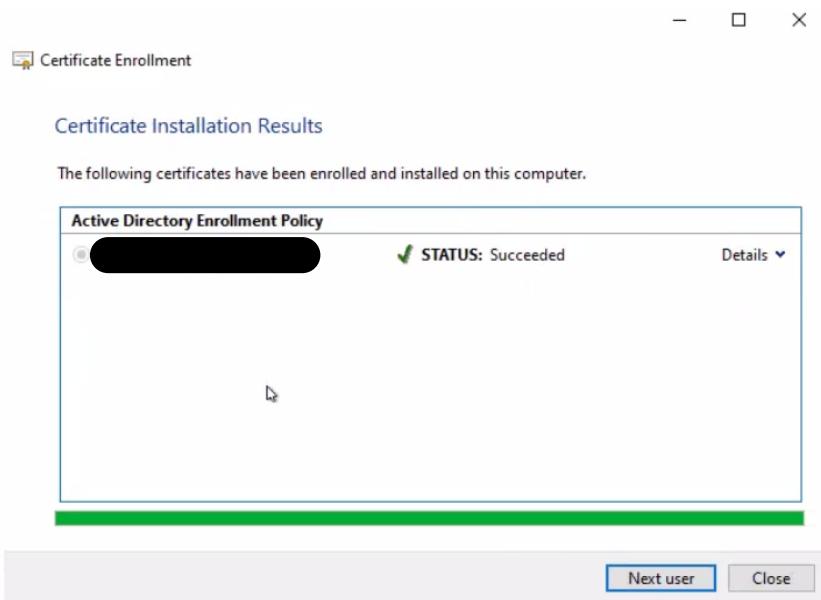
Cliquez sur inscription pour implanter le certificat sur la yubikey



Rentrer le code pin par défaut, puis toucher la clé lorsqu'elle clignote



Une fois fini, cliquez sur close ou Next User s'il y a d'autre utilisateur demander



Maintenant la clé prête, il ne manque plus que le code pin que l'utilisateur doit personnaliser soi même

Aller sur le yubikey manager et sur PIV

A screenshot of a web-based Yubico PIV application. The header includes the Yubico logo and navigation links for Home, Applications, and Interfaces. Below the header is a "Configure PIV Application" button. The main content area has a large "PIV" heading with a cursor icon pointing towards it. Below the heading is a breadcrumb trail: "Home / PIV".

Changer le code PIN

A screenshot of a web-based Yubico PIN configuration page. The header includes the Yubico logo and navigation links for Home, Applications, and Interfaces. Below the header is a "Configure PINs" section with a breadcrumb trail: "Home / PIV / Configure PINs". The main content area displays three sections: "PIN" (3 retries left, Change PIN button), "PUK" (PIN Unlock Key, Change PUK button), and "Management Key" (Protected by PIN, Change Management Key button).

Sélectionner Use default, le code pin prédéfini et rentrer 2 fois le code PIN personnalisé

- 8 caractères
- Majuscule, minuscule, chiffres, lettres
- Pas de caractères spéciaux

yubico Home Applications Interfaces

Change PIN

Home / PIV / Configure PINs / PIN

Current PIN

New PIN

Confirm new PIN

Désactiver les fonctionnalités NFC puis enregistrer

yubico Home Applications Interfaces

Interfaces

Home / Interfaces

USB Disable all

OTP FIDO2

FIDO U2F PIV

OATH

NFC Enable all

OTP FIDO2

FIDO U2F PIV

OATH