

FICHE 1 – PRÉREQUIS

RAPPEL SUR LE CODE PIN ET LE CODE PUK D'UNE YUBIKEY AVEC L'AUTHENTIFICATION SMARTCARD/PIV¹

L'objectif principal du code PIN est d'authentifier l'utilisateur afin qu'il puisse utiliser la clé privée contenue dans la clé de sécurité à des fins de signature et déchiffrement. La norme spécifie qu'il s'agit d'une valeur de 6 à 8 octets, chaque octet étant un numéro ASCII ('0' à '9', soit 0x30 à 0x39 en ASCII). Cependant, la YubiKey permet d'utiliser n'importe quel caractère ASCII pour le code PIN.



Attention ! Un nombre de tentative limité (8 tentatives par défaut) est défini pour saisir le code PIN. Après un certain nombre d'échecs d'authentification répété, l'accès à l'authentification SmartCard/PIV sera verrouillé et seule une réinitialisation à l'aide du code PUK permettra de débloquer la situation.

Le code PUK est utilisé pour débloquer le code PIN. La norme spécifie que le code PUK doit être une valeur de 8 octets, chaque octet pouvant être n'importe quel caractère ASCII. Cependant, la YubiKey accepte un code PUK de 6 à 8 caractères. **Le code PUK est lui-même soumis à un nombre de tentative limité. En cas d'échecs répétés, il ne sera plus possible d'accéder aux options de réinitialisation de la clé .**

CHANGEMENT DU CODE PUK ET DU CODE PIN PIV SUR LA YUBIKEY



Attention ! Le code PUK et le code PIN par défaut liés à l'authentification SmartCard/PIV sur la Yubikey doivent être **obligatoirement** changés pour éviter le blocage de la clé lors de la mise en œuvre de la nouvelle authentification.

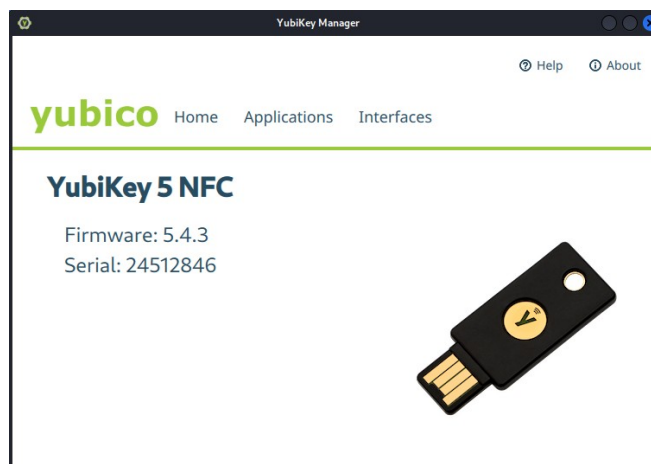
Plusieurs méthodes sont envisageables pour effectuer ce changement dont une par déploiement d'une GPO (Stratégie de groupe Microsoft). Dans le cas présent, nous passerons par l'outil Yubikey Manager.

URL de téléchargement de l'application Yubikey Manager :

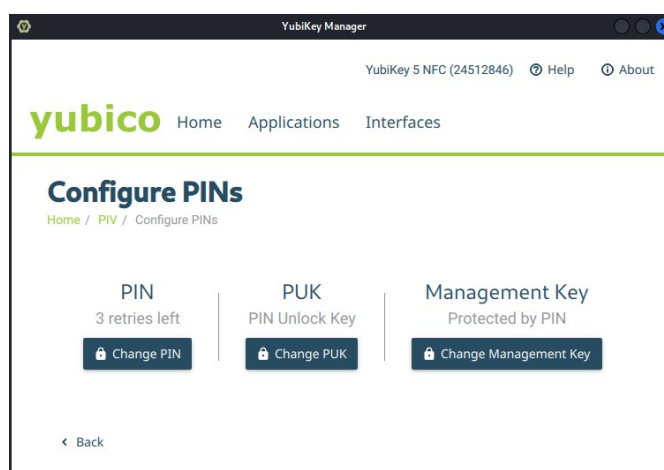
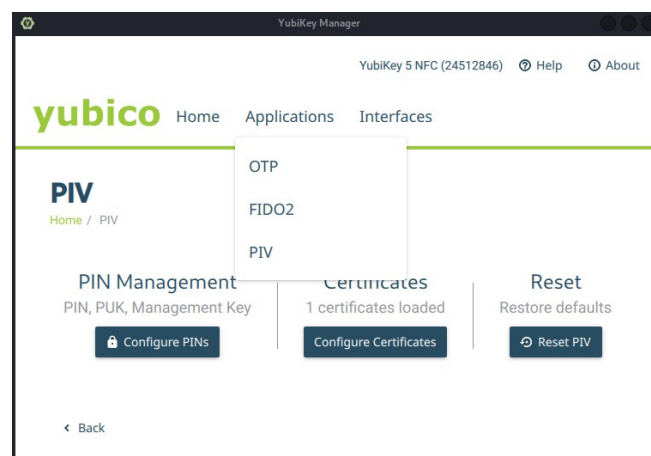
<https://www.yubico.com/support/download/yubikey-manager/>

Lancer l'application et insérer la clé de sécurité dans le port USB

1 <https://docs.yubico.com/yesdk/users-manual/application-piv/pin-puk-mgmt-key.html>



Cliquer sur le menu Application > PIV puis sur Configure PINs



Cliquer ensuite sur Change PUK

Modifier le code PUK par défaut 12345678 par celui de votre choix (ex : 23456789). **Attention ! Veiller à ne pas perdre ce code !**

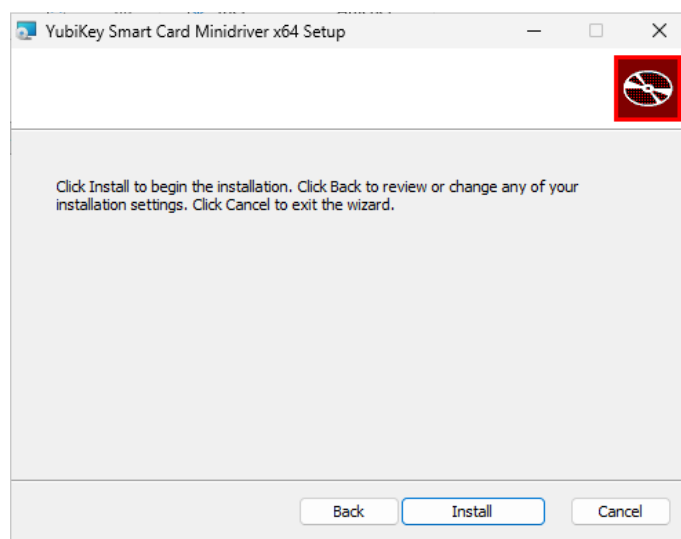
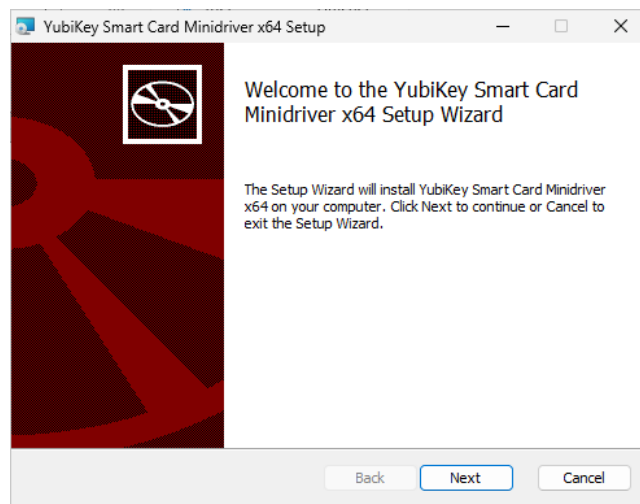
Modifier ensuite le code PIN par défaut 123456 par celui de votre choix (ex : 234567).

INSTALLATION DU MINIDRIVER YUBIKEY SMART CARD

Il est nécessaire d'installer ce pilote sur tous les postes clients et tous les serveurs (Windows 11 ou Windows Server) sur lesquels vous souhaitez implémenter ce type d'authentification.

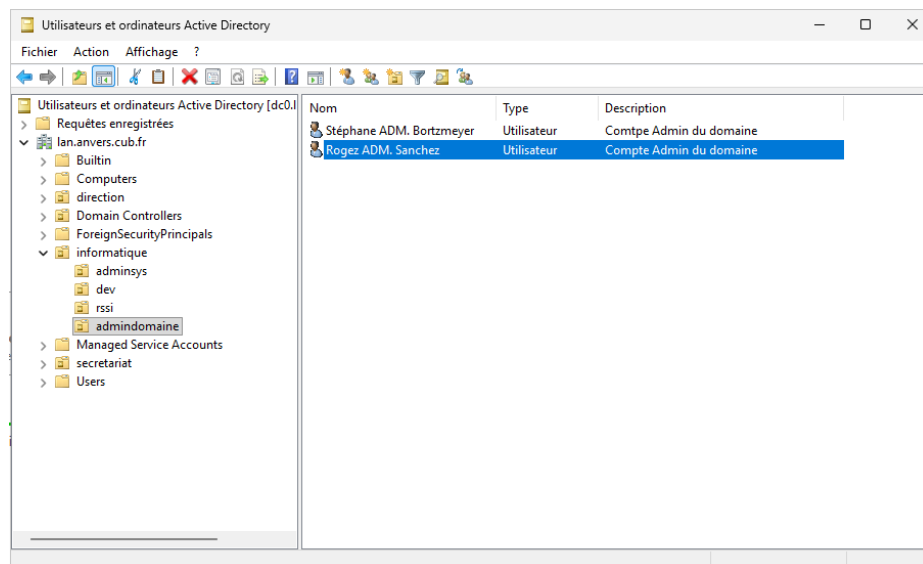
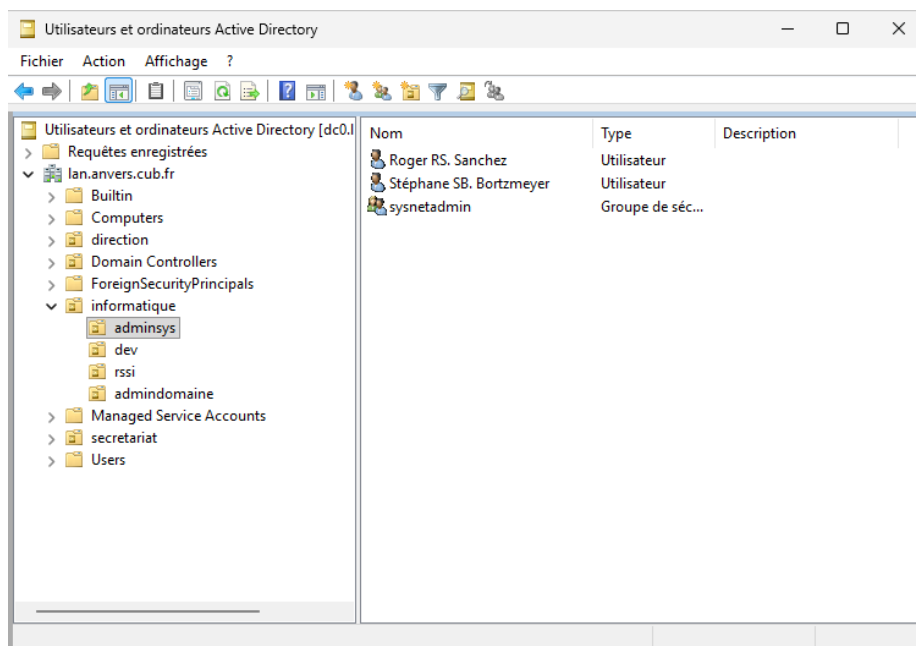
URL de téléchargement du driver :

<https://www.yubico.com/support/download/smart-card-drivers-tools/>



CONFIGURATION DU SERVEUR CONTRÔLEUR DE DOMAINE WINDOWS SERVER ET DE L'ENVIRONNEMENT MICROSOFT

Le serveur Windows doit disposer du rôle AD/DS contrôleur de domaine. Dans l'annuaire Active Directory, il est préférable de disposer de plusieurs unités d'organisation avec différents comptes et groupes.



Les clients et serveurs mobilisés dans ce contexte doivent également être intégrés au domaine.