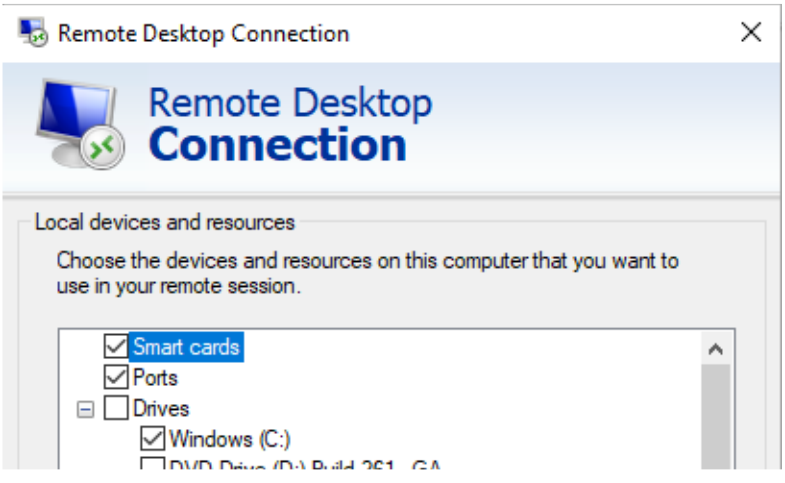
Configuring a YubiKey with a Smart Card Account

1. Pre-Installation Checklist:

• Ensure your smart card account (SC-JHEDID) is a local administrator on your workstation.

• Your workstation must be Windows, on the Hopkins network and joined to the WIN domain.

• Verify you have enabled "Smart cards" for resource redirection within RDP if you plan to remote connect to workstations and servers with your YubiKey:



2. Install the YubiKey Manager

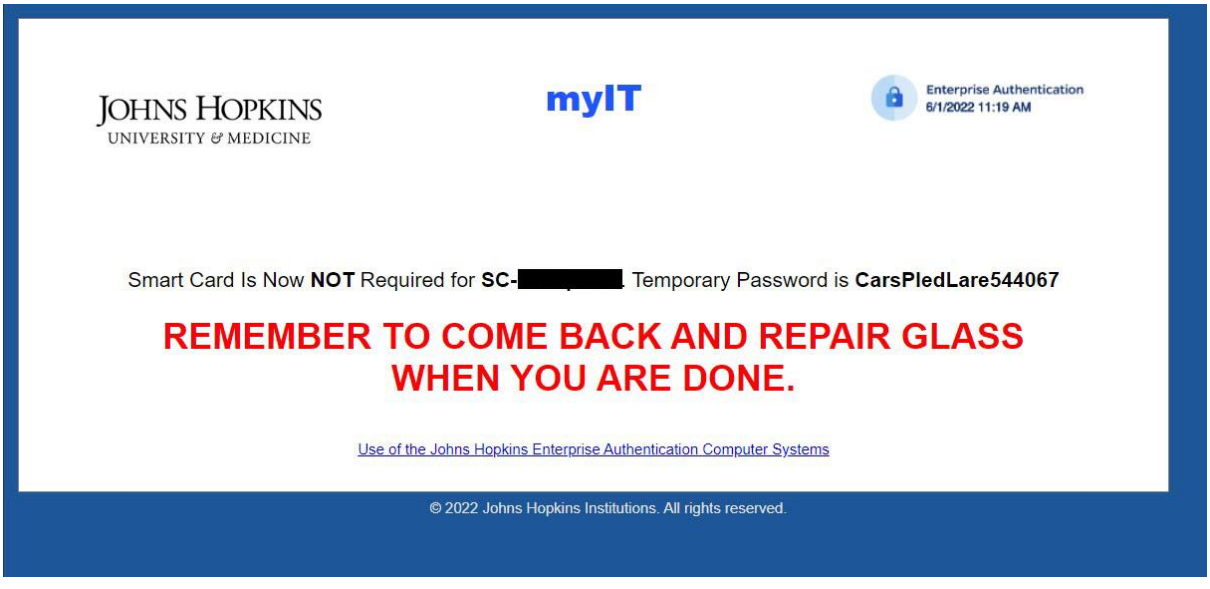
Download and install the YubiKey Manager onto your workstation.

3. Break Glass on your Smart Card Account

Login to the myIT site and break glass. Provide the reason "Configuring YubiKey" and click **Break Glass**.

4. Copy your Temporary Password

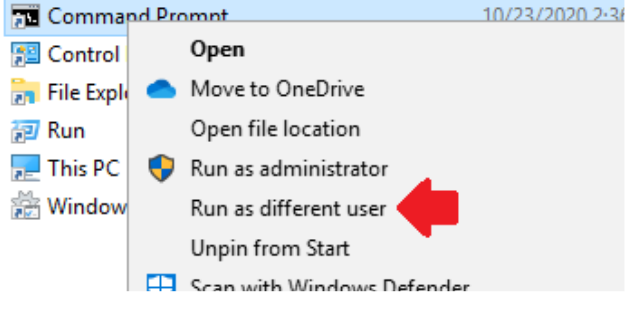
The myIT site will generate a temporary password. You will need this password later.



5. Run Command Prompt as different user

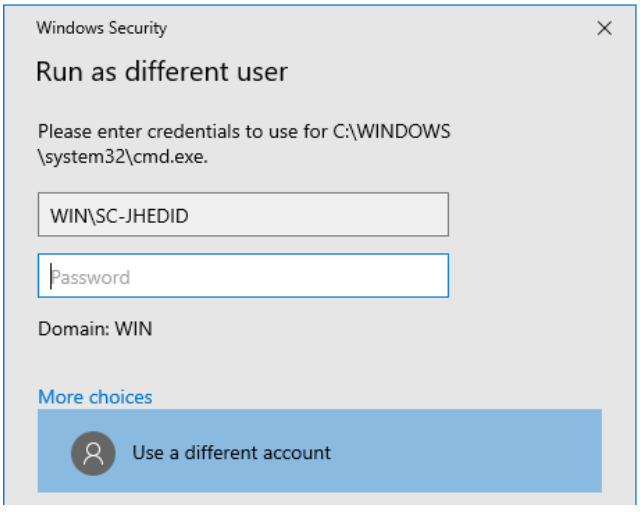
Use the Windows search box and type **cmd.exe** > right click the application > select **Open file location**. Once you locate the application, hold down the **Shift button and right click** simultaneously on the application.

Select **Run as a different user**.



6. Authenticate with your Smart Card Account

Select **More choices** and **Use a different account**. Authenticate with your smart card account and its broken glass password from step 4.



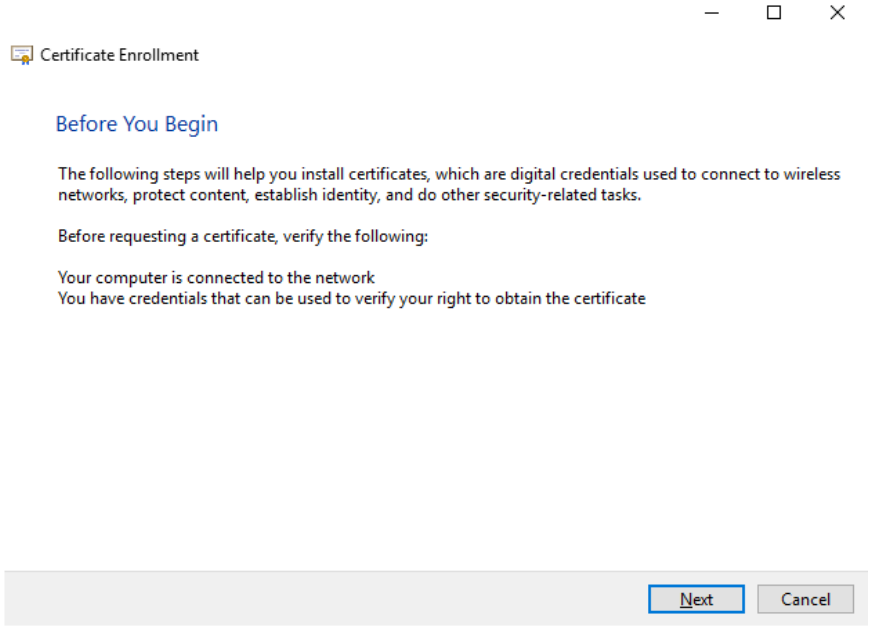
7. Request a Smart Card Certificate

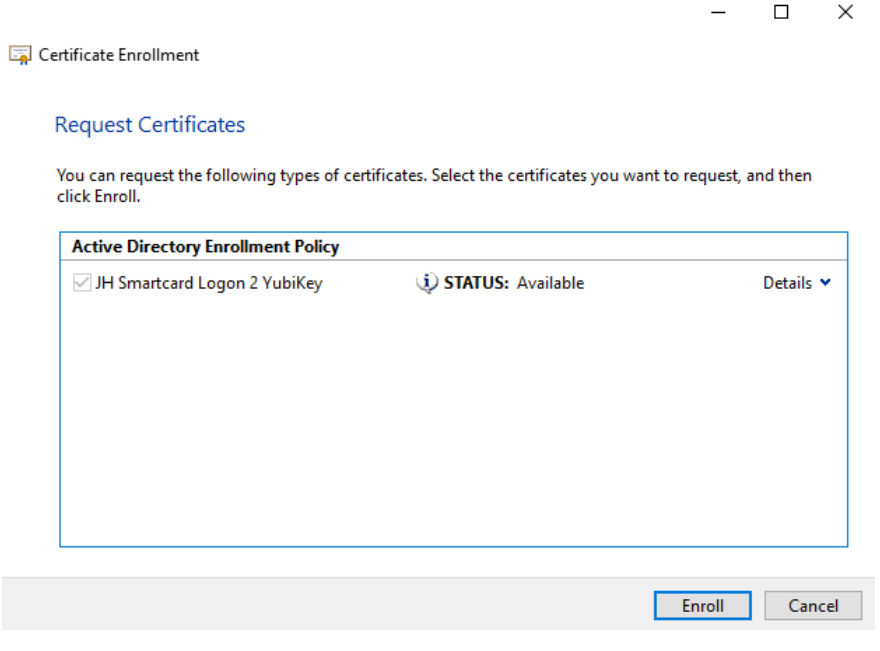
At the command prompt, type the following to enroll your smart card certificate:

```
C:\>certreq -enroll "JH Smartcard Logon 2 Yubikey"
```

8. Enroll your Smart Card Certificate

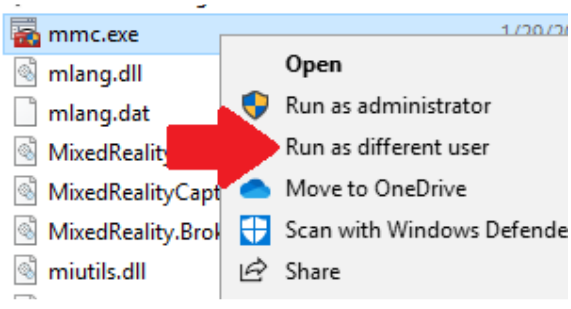
You will receive a certificate enrollment popup. Click **Next** and **Enroll** at the bottom of the popup to finish.



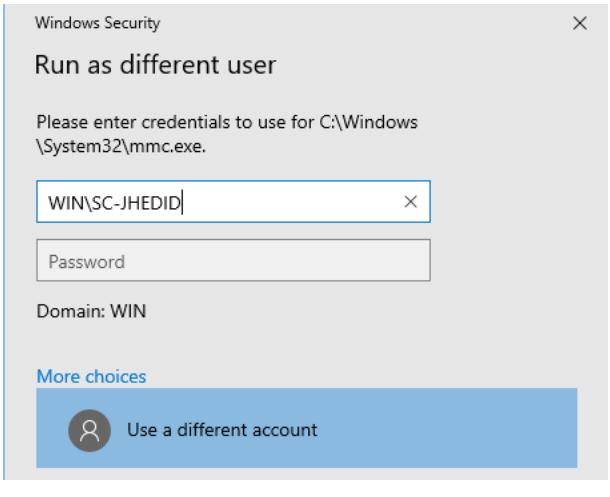


9. Export your Smart Card Certificate

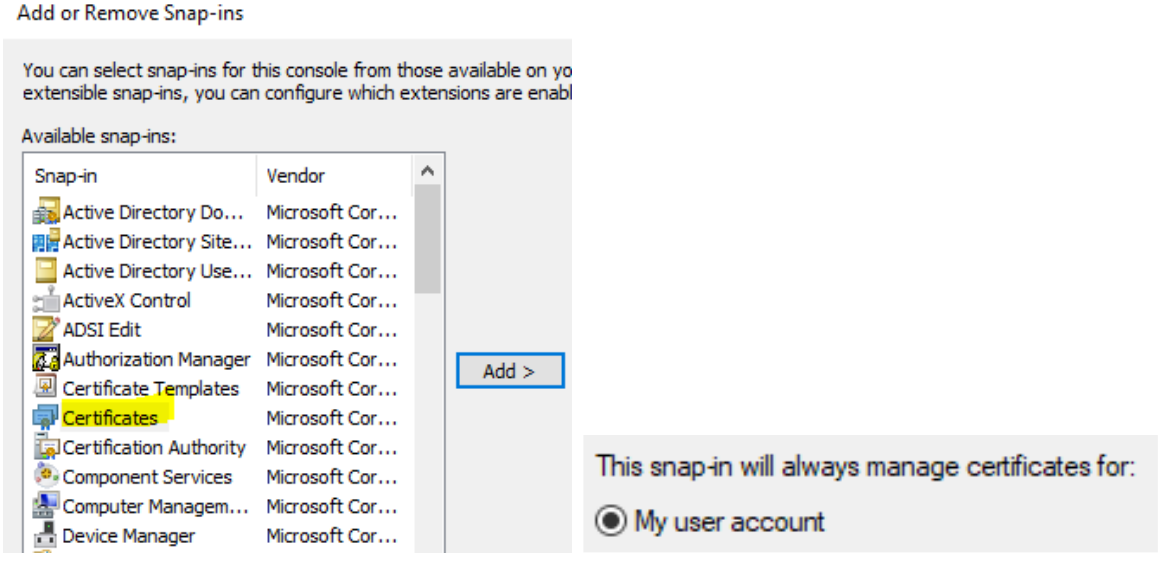
Use the Windows search box and type **mmc.exe** > right click the application > select **Open file location**. Once you locate the application, holding down the **Shift button and right click** simultaneously on the application. Select **Run as a different user**.



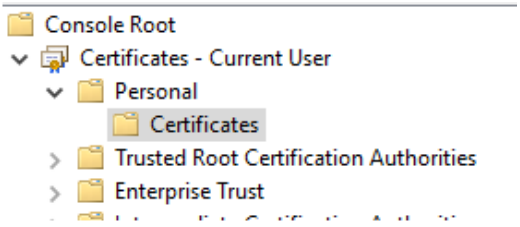
Select **More choices** and **Use a different account**. Authenticate with your smart card account and its broken glass password from step 4.



Go to '**File**' > '**Add/Remove Snap-ins**' and add certificates for your '**User Account**'. Click **OK.**

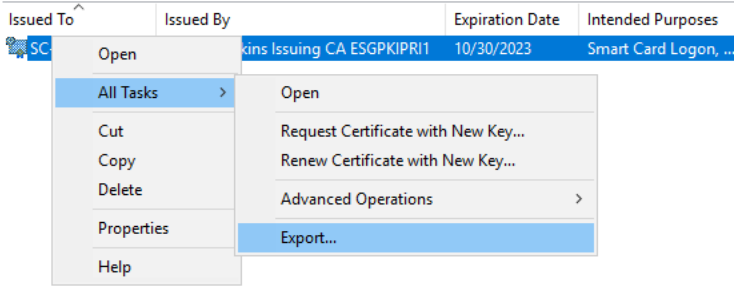


Once the certificates snap-in is loaded, locate your smart card certificate by expanding **Certificates–Current User** > **Personal** > **Certificates**. Your certificate will appear in the right side window.

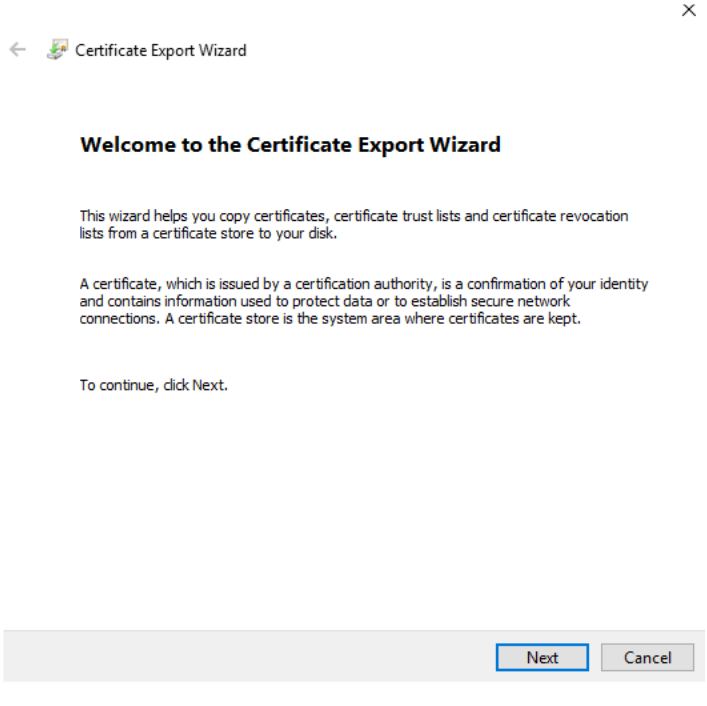


Note: If you appear to have multiple certificates, the correct one to use will have an expiration date of exactly two years from the day you created it.

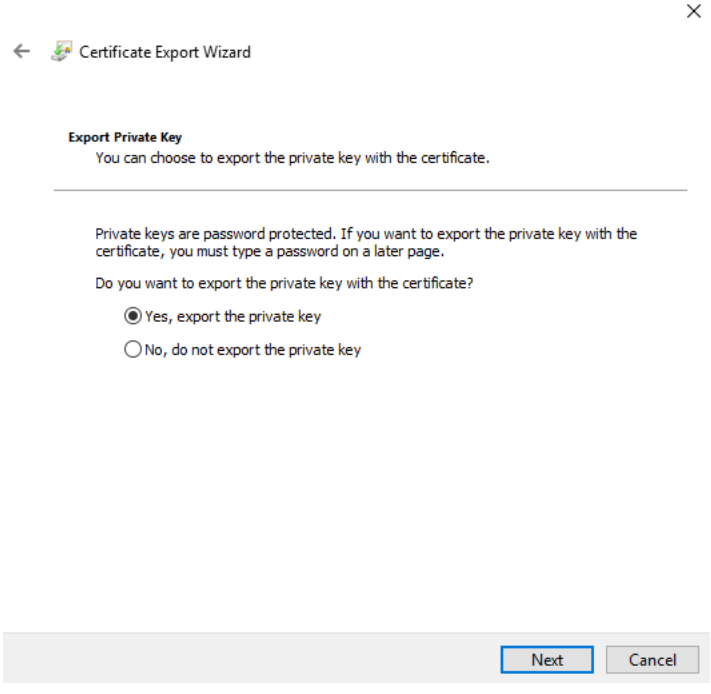
Right Click your certificate and select **All Tasks**. Click **Export...**



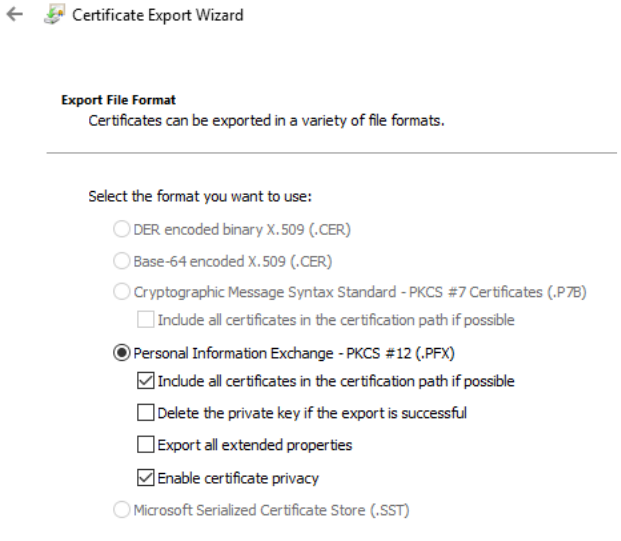
The Certificate Export Wizard will appear. Click **Next.**



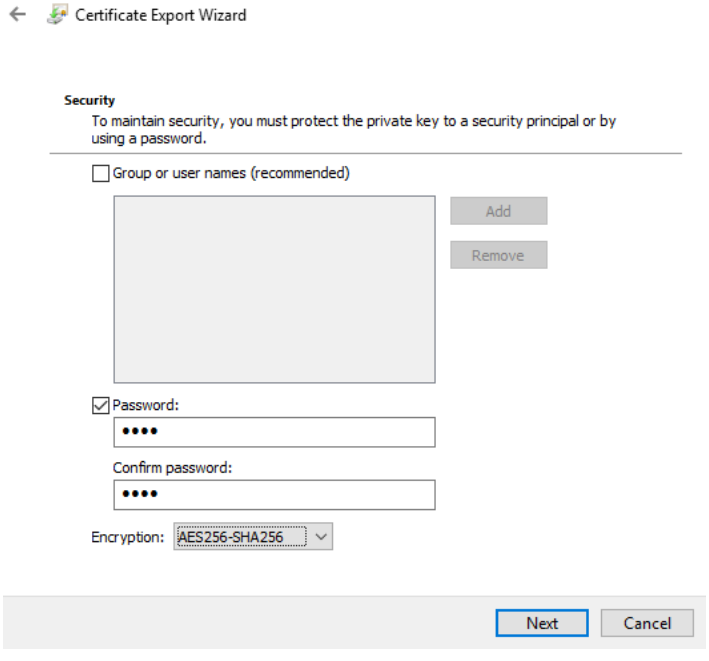
Verify **Yes, export the private key** is selected. Click **Next**.



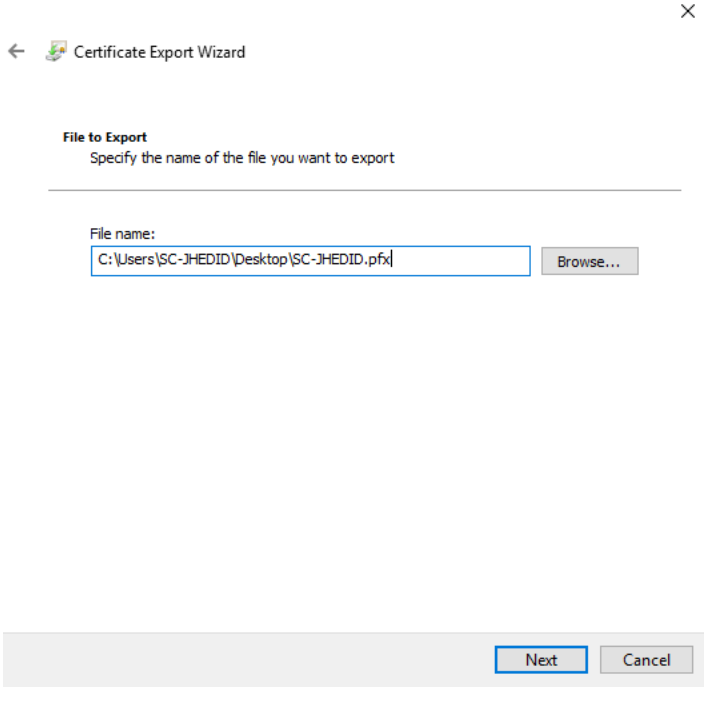
Ensure '**Personal Information Exchange'**, '**include all certificates in the certification path if possible'**, and '**Enable certificate privacy'** are selected. Click **Next**.



Create a password (less than 8 characters) to secure the certificate file and choose **AES256-SHA256** for encryption.

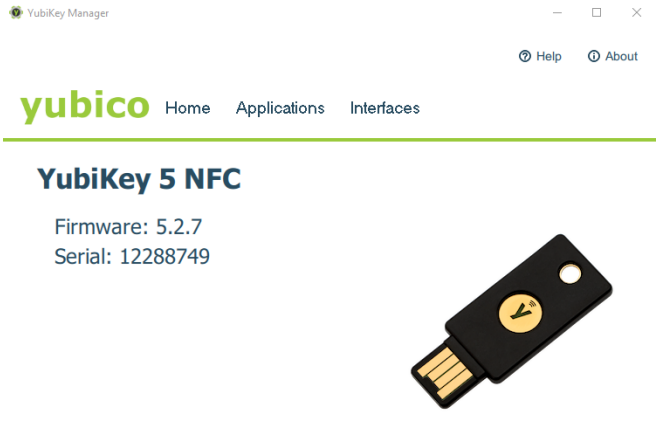


Save the .pfx file to an easily accessible location. Click **Next** and **Finish** to save.

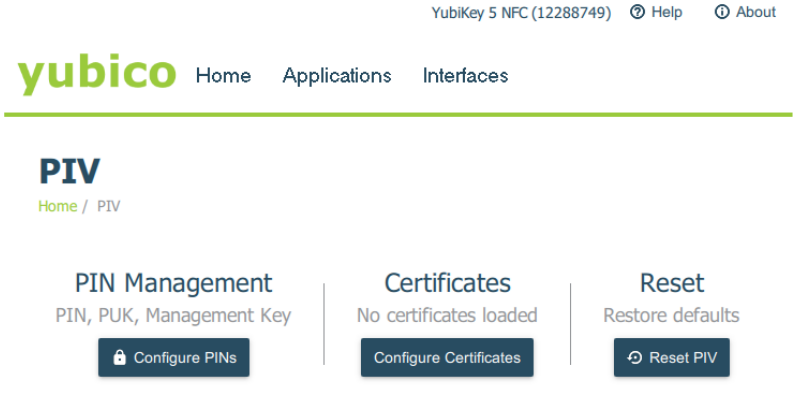


10. Import the Certificate to your YubiKey

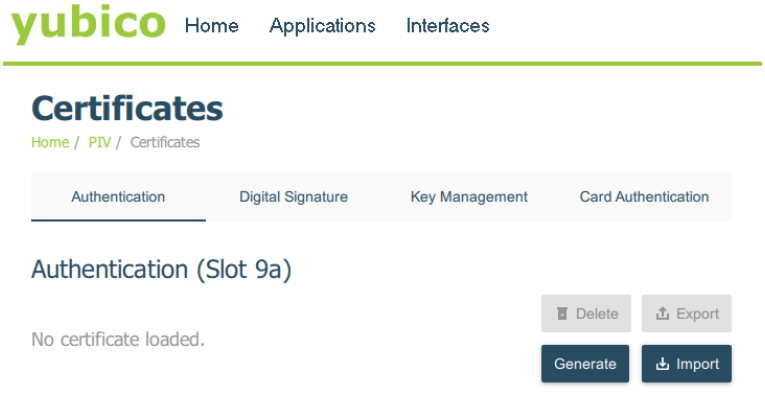
Insert your YubiKey into your workstation and launch the YubiKey Manager.



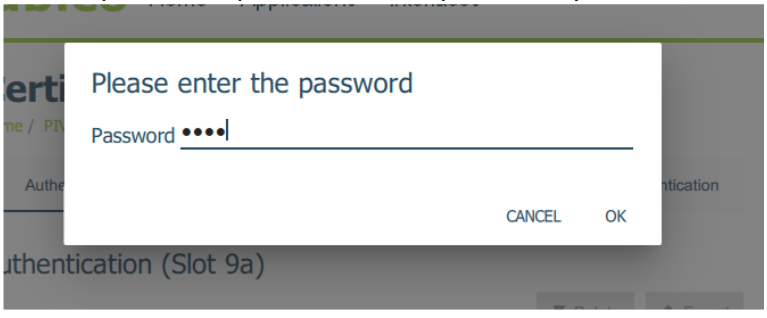
Click **Applications**, select **PIV**. Click **Configure Certificates**.



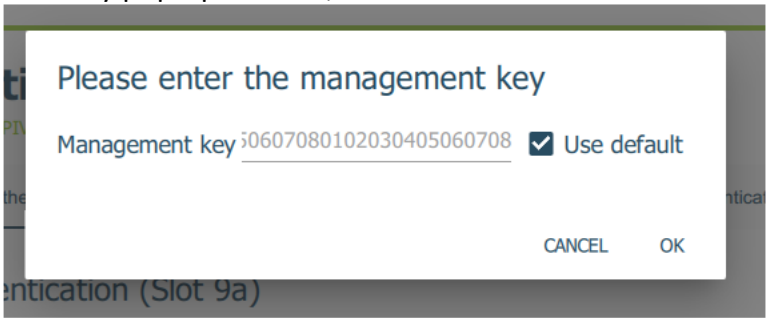
Ensure you are on the Authentication tab (slot 9a). Click **Import**.



Locate your .**pfx** file from Step 9 and import it with the password you created when it was saved.

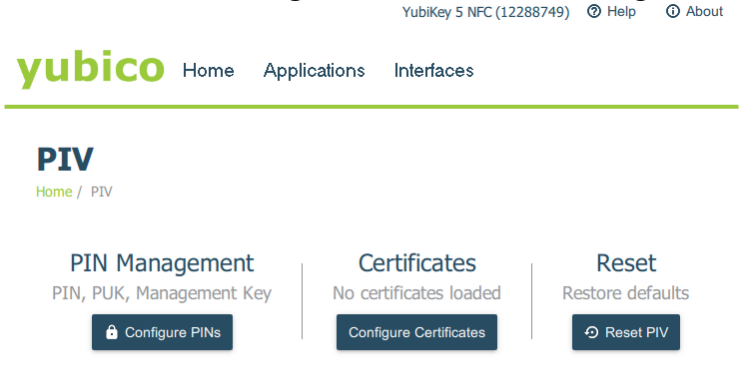


At the Management Key pop-up window, select the checkbox to **Use default** and click **OK**.

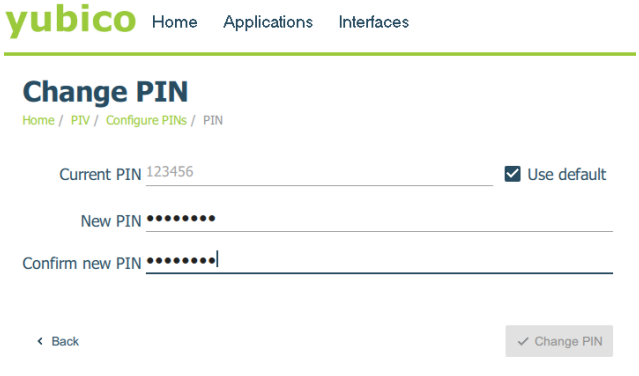


11. <u>Create a PIN for your YubiKey</u>

Click **Applications,** select **PIV**, and click **Configure PINs** under PIN Management**.**



Click **Change PIN.** Check the **Use default** option and create a PIN to use whenever you need to authenticate with your YubiKey. *Note: The PIN must be between 6 and 8 characters long and alphanumeric only.*



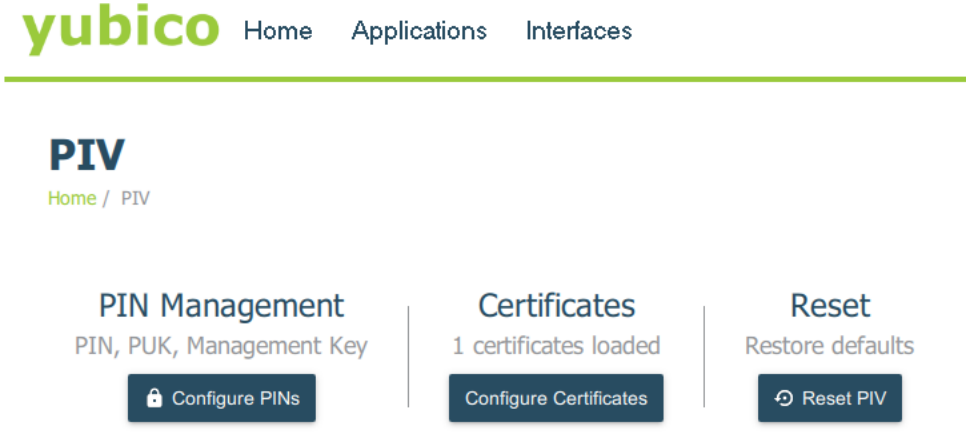
12. Using your YubiKey

Once you have set a PIN on your YubiKey, you must unplug it from your workstation and plug it back in. It needs to reinitialize within your Windows session.

Additionally, you must ensure your smart card account has sufficient privileges for accessing or administrating your systems. You will need to reach out to your LAN Administrator if you are unsure whether your smart card account has been granted sufficient privileges.

13. Managing your YubiKey

The PIV (Personal Identity Verification) section within the Applications menu allows you to manage the smart card aspect of your YubiKey.



The PIV section allows you to:

Reset your PIN, unlock your YubiKey, view the expiration of your certificate (Authentication Slot 9a), import a new certificate from our CA, and reset your YubiKey back to default.

Please visit our Admin MFA Resource Center for more information about smart cards at Hopkins.