yubico

# YubiKey PIV Manager User's Guide

## Using Active Directory Smart Card Login

YubiKey 4, YubiKey 4 Nano, YubiKey NEO, YubiKey NEO-n

## Copyright



## Trademarks



## Disclaimer



## Contact Information

**Yubico Inc**
420 Florence Street, Suite 200
Palo Alto, CA 94301
USA
yubi.co/contact

## Document Release Date

April 4, 2016

yubico

# Contents



# Introduction

Yubico changes the game for strong authentication, providing superior security with unmatched ease-of-use. Our core invention, the YubiKey, is a small USB and NFC device supporting multiple authentication and cryptographic protocols. With a simple touch, it protects access to computers, networks, and online services for the world's largest organizations.

Our innovative keys offer strong authentication via Yubico one-time passwords (OTP), FIDO Universal 2nd Factor (U2F), and smart card (PIV, OpenPGP, OATH) — all with a simple tap or touch of a button. YubiKeys protect access for everyone from individual home users to the world's largest organizations.

## PIV and YubiKeys

The YubiKey 4, YubiKey 4 Nano, YubiKey NEO, and YubiKey NEO-n support the Personal Identity and Verification Card (PIV) interface specified in the National Institute of Standards and Technology (NIST), SP 800-73 document, Cryptographic Algorithms and Key Sizes for PIV. This enables you to perform RSA or ECC sign and decrypt operations using a private key stored on the YubiKey. Your YubiKey acts as a smart card in this case, through common interfaces like PKCS#11.

For more information about the slots, see the Yubico website.

For more information about the PIV specifications, see the PIV standards on the NIST website.

This document covers only slot 9a (PIV authentication).

## YubiKey PIV Manager

After you download and install YubiKey PIV Manager, you can use it with one of the supported YubiKeys to request and import certificates for smart card login to log in to Microsoft Windows Active Directory domain environments. In addition, you can use the YubiKey PIV Manager for other tasks you perform with your YubiKeys, such as:

- Establishing an active connection to the Windows CA
- Setting a pin for the first time
- Changing the pin
- Resetting the PIV applet

This document describes the following topics:



## Getting Additional Help

For more information, and to get help with your YubiKeys, see:

- Support home page
- Documentation and FAQs
- Start a Support ticket

# Ensuring the YubiKey Has CCID Mode Enabled

Before you can use a YubiKey with the YubiKey PIV Manager, be sure you enable CCID mode using the YubiKey NEO Manager. Yubico ships YubiKey NEOs with U2F and OTP modes enabled, and CCID mode disabled by default.

**NOTE**: If CCID mode is already enabled on your YubiKey, skip this section.

**In this Chapter**



## Enabling CCID Mode for Your YubiKey NEO

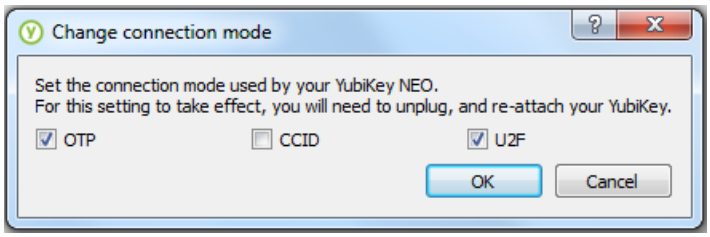
The following procedure applies to YubiKey NEOs only. If you have a YubiKey 4 or YubiKey 4 Nano, you can skip this section.

**To enable CCID mode using the YubiKey NEO Manager**

1. Download the latest version of YubiKey NEO Manager from the Yubico website.
2. Install and open YubiKey NEO Manager.
3. Insert your YubiKey NEO into a USB port of your computer.
4. Click **Change connection mode (OTP+U2F)**.

   **TIP**: If the button shows **Change connection mode (OTP+U2F+CCID)**, CCID mode has already been enabled for your YubiKey and you can skip this procedure.

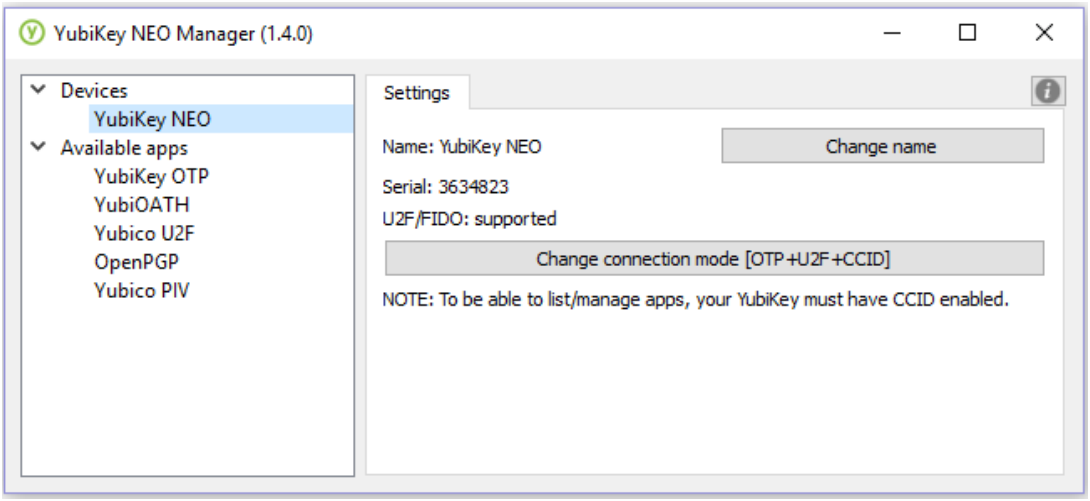
5. Select **CCID**.




6. Click **OK**, and remove your YubiKey NEO when prompted.

7. Insert your YubiKey NEO again into a USB port of your computer, and confirm that CCID is enabled (the **Change connection mode** button now shows **CCID,** and the installed CCID applets are now listed on the left side of the window).



# Using the YubiKey PIV Manager

Use YubiKey PIV Manager to set and change PINs and Personal Unlocking Keys (PUKs), request certificates from a Certification Authority, delete certificates, import certificates, and reset the PIV applet.

Through Group Policy, domain administrators have additional options, which enables them to customize the user experience with the YubiKey PIV Manager. For a full list of Group Policy options, see Using Group Policy Settings at the end of this document.

## Requirements

- Administrators: Distribute the YubiKey PIV Manager to the users in your domain environment.
- Users: Before running the YubiKey PIV Manager, establish an active domain connection to the Certification Authority. If you are a user within your corporate location, you probably already have an active domain connection. If you are connecting from outside your office location, you may need to be connected on the corporate VPN.

**In this Chapter**



## Downloading and Installing the YubiKey PIV Manager

Before you can request certificates from a Windows Certification Authority (CA), be sure you download and install the YubiKey PIV Manager, and then establish an active connection to the CA.

**To install YubiKey PIV Manager**

1. Download the latest version of YubiKey PIV Manager from the Yubico website.
2. Install and launch the YubiKey PIV Manager.
3. Open the installation wizard, and click **Next** to begin the installation process.
4. Follow the instructions on the installation wizard.

## Establishing an Active Connection to the Windows Certification Authority

To request certificates from a Windows Certification Authority (CA), establish an active connection to the CA on the same computer on which you installed the YubiKey PIV Manager.

**To establish an active connection to the CA**

1. Start YubiKey PIV Manager. Do one of the following.

   - Launch YubiKey PIV Manager from a laptop or desktop computer that is joined to the domain. The computer must have an active connection to the domain controller (connected on the local network, or connected over VPN).

   - Launch YubiKey PIV Manager over Remote Desktop Protocol (RDP) on any Windows computer that has an active connection to the domain. The source and destination computers must both be running the Windows operating system.
     **TIP**: If the **Do not allow smart card redirection** Group Policy object is set to **Enabled**, you cannot launch YubiKey PIV Manager over RDP. For more information about this topic, see this Microsoft support article.

2. If you are connecting to a computer on the domain, insert the YubiKey into a USB port of your local Windows computer, and use Remote Desktop Connection (`mstsc.exe`) to connect your local computer to the domain computer.

## Setting a PIN for the First Time

If you have a YubiKey that was not previously set up with YubiKey PIV Manager, set a PIN the first time you open the YubiKey PIV Manager.

### Working with the Management Key

During device initialization, the YubiKey PIV Manager sets a new Management Key. By default, YubiKey PIV Manager cryptographically processes the PIN to generate a Management Key, and you cannot determine the Management Key after setting the PIN. For this reason, we recommend setting strong PIN complexity requirements at the Group Policy level.

If you choose not to follow this recommendation, or if you decide you need to know the Management Key, select the option to **Use a separate key** when setting the PIN. This allows you to manually set a new Management Key (must be exactly 48 alphanumeric characters), or use the built-in tool to generate a random Management Key. If you choose to do this, store the Management Key in a safe place. To learn more about the Management Key, see the Yubico developer's website.

**To set a PIN**

1. Choose a PIN.

   - The PIN is a password that you type when you are requesting certificates, logging into the domain using your YubiKey, and so on.
   - The PIN must be 4-8 characters in length.
   - If your administrator specified additional PIN complexity requirements using Group Policy, the PIN must be 6-8 characters in length, not include three or more consecutive characters that appear in the user's name, and must contain three of the four (numbers, capital letters, lowercase letters, and special characters).
   - Unless otherwise instructed by your administrator, keep the default setting, **Use PIN as key**. Alternatively, you can set the Management Key.

2. Type the new PIN, confirm it, and click **OK**.

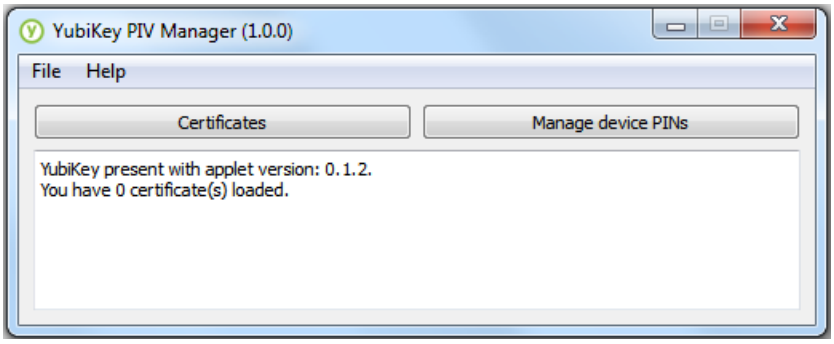
Now that the PIN is set, continue with the next sections, Requesting a Certificate for Smart Card Login from a Windows CA, or Importing an Existing Smart Card Login Certificate to the YubiKey.

## Requesting a Certificate for Smart Card Login from a Windows CA

Now that you have set a PIN, request a certificate from the Certification Authority.

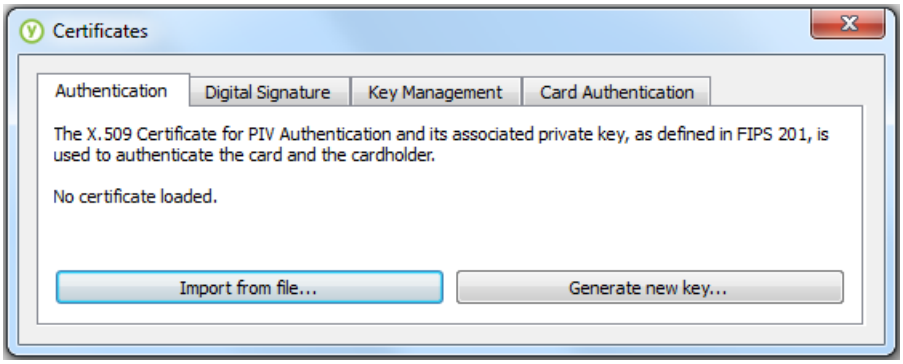
**To request a certificate for a smart card login**

1. Open YubiKey PIV Manager, and click **Certificates**:



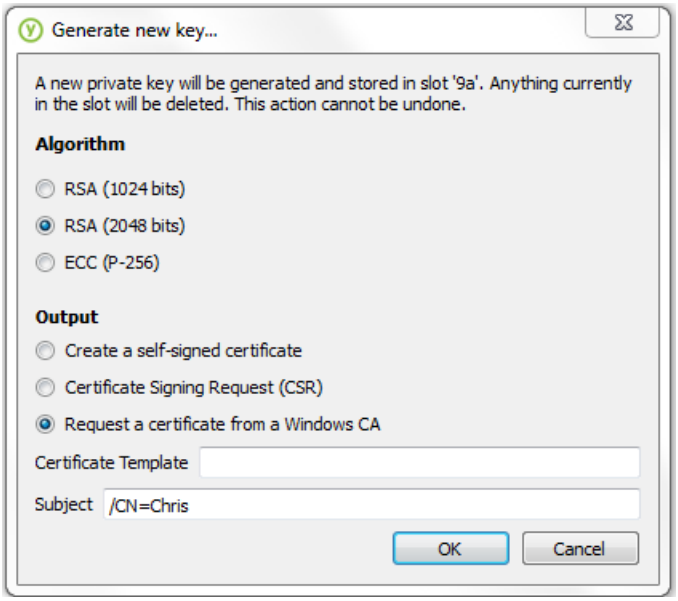

  

2. Click **Generate new key**.




3. Under **Output**, select **Request a certificate from a Windows CA**.

   - Depending on your organization, the **Certificate Template** field may already be completed. If not, type the name of the smart card login certificate provided by your administrator.
   - The **Subject** field should be automatically completed. If it is blank, get the value from your administrator and type it in the **Subject** field.
     **NOTE**: The Subject field will be pre-populated with the logged in user's common name. No changes are necessary.

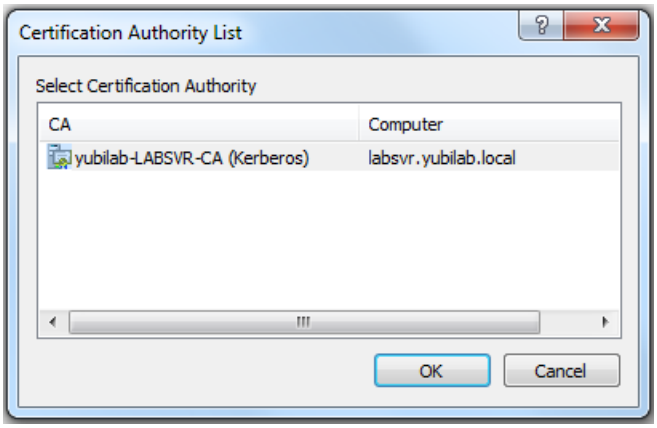



4. Click **OK** to continue the request, type your PIN when prompted, and click **OK** again.

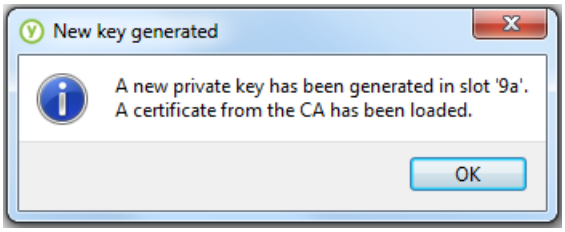
5. To confirm the Certification Authority, click **OK**.
   **TIP**: If there are multiple Certification Authorities to choose from, select the option provided by your

administrator.




6. Click **OK** to continue. When the certificate is successfully imported, the following dialog box appears:




7. Click **OK**. You can now exit YubiKey PIV Manager.

8. We recommend that you remove, and then again insert your YubiKey into a USB port of your computer.

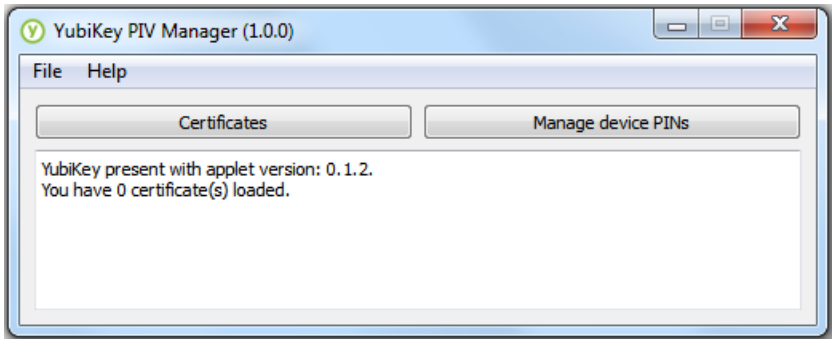
9. To verify that the certificate is working properly, log out of your domain account and then log back in, or connect over **Remote Desktop Protocol**.

## Importing an Existing Smart Card Login Certificate to the YubiKey

If you already have a smart card login certificate, import the `.pfx` file to your YubiKey. Make sure that the private keypair is on the certificate when you import the `.pfx` file.

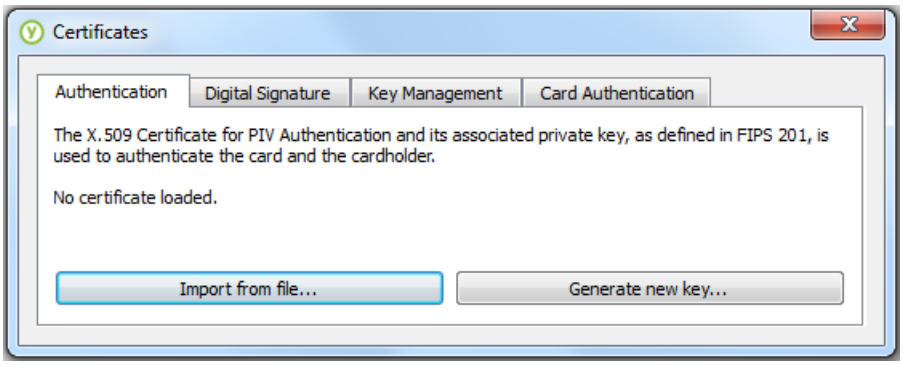
**To import an existing smart card login certificate to Your YubiKey**

1. Open YubiKey PIV Manager, and click **Certificates**:



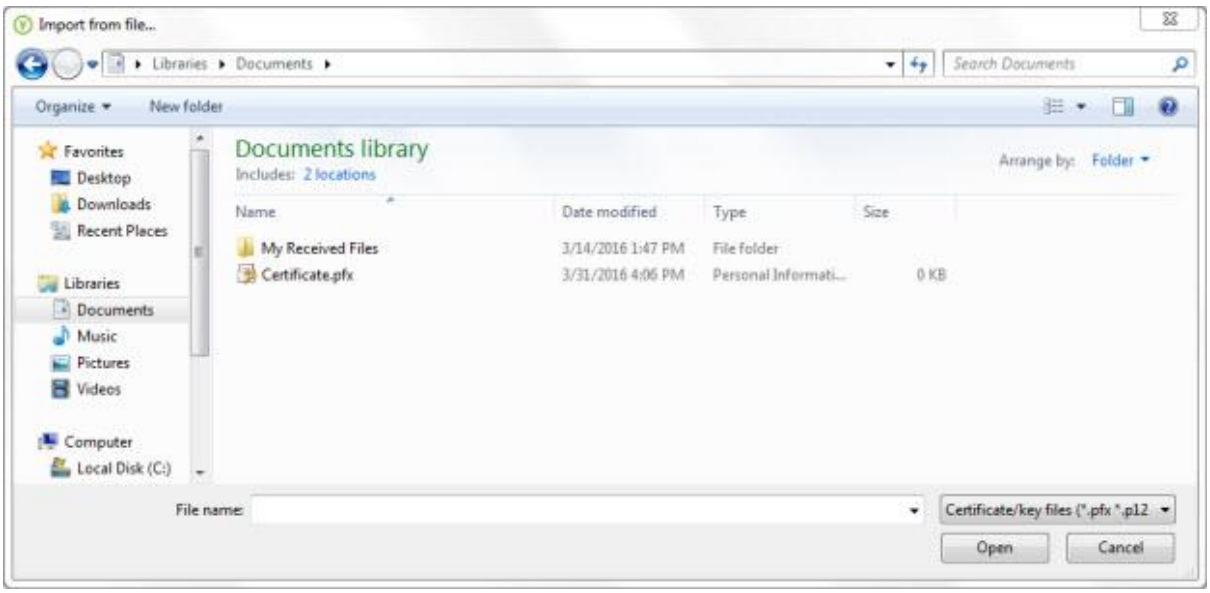
2. To import an existing certificate, click **Import from file**.




3. To overwrite the certificate currently stored in slot 9a, click **OK**.
   A message displays: `Anything currently in slot '9a' will be overwritten by the imported content. This action cannot be undone.`

4. To acknowledge the message stating that any certificates currently stored in slot 9a will be overwritten, click **OK**.

5. Browse to the certificate file that you want to import, and click **Open**.




6. To confirm the password that was set for the certificate, type the password and click **OK**.

   **NOTE**: A password was created when the certificate was created. If necessary, get the password from your administrator. Be sure you type that same password here. This field is *not* to confirm the PIN you set in a previous section of this document.

7. When you see a dialog box confirming that your certificate was successfully imported, click **OK**.

8. Before testing the smart card login certificate, remove and then again insert your YubiKey into a USB port of your computer.

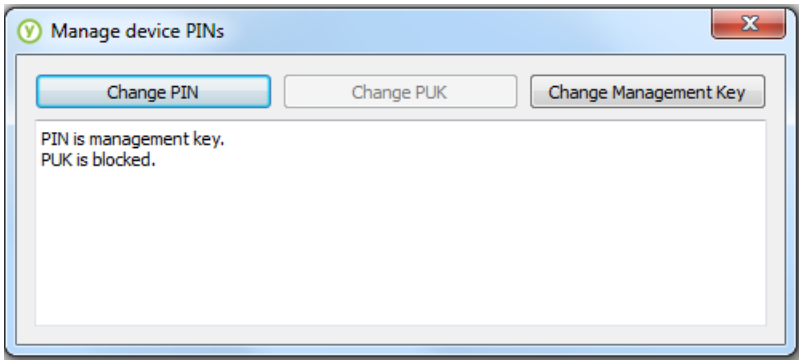
  

## Changing the PIN

You can change the PIN on the PIV applet at any time through the YubiKey PIV Manager.

**To change the PIN on the PIV applet**

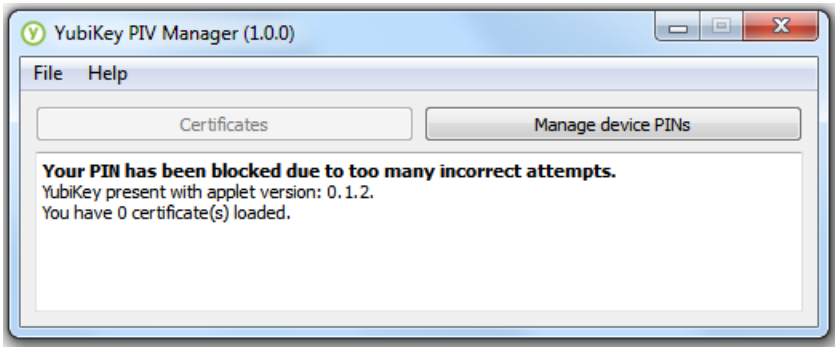
1. Open the YubiKey PIV Manager, and click **Manage device PINs**.
2. To change the PIN, click **Change PIN**.




3. Type the current PIN and the new PIN, and click **OK**.
4. To confirm the change, click **OK.**

## Resetting the PIV Applet When the PIN is Blocked

If you type an an incorrect PIN code three consecutive times, you will get locked out of the applet. Once this occurs, you cannot access previously loaded certificates. You must reset the PIV applet before you can make any changes or use the PIV applet. If this is the case, a message appears as follows:

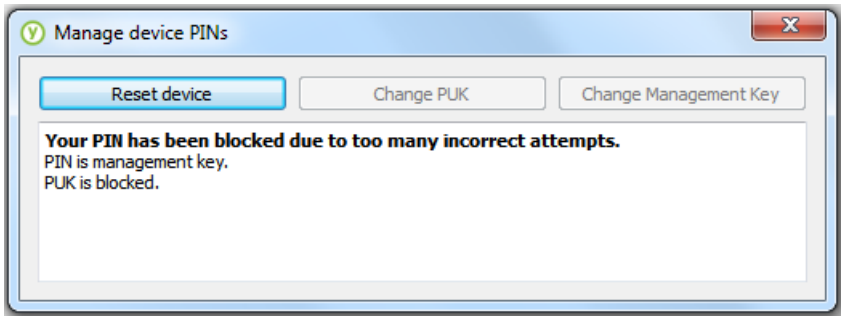


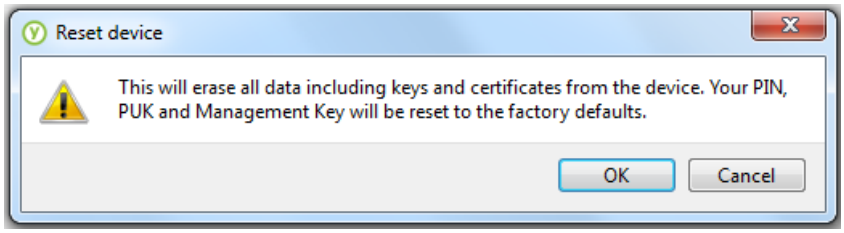
**To reset the PIV applet when the PIN is blocked**

1. Click Manage device PINs.

2. Click Reset device.




3. Click **OK** to reset the applet to factory defaults (erasing all data).




4. To confirm, click **OK**. After a few moments, you are prompted to initialize the device and set a new PIN.

   To read instructions about completing this process, return to the previous section, Setting a PIN for the First Time.

# Using Group Policy Settings for Domain Administrators

Through Group Policy, domain administrators have additional options, which enables them to customize the user experience with the YubiKey PIV Manager. For example, administrators can specify complexity requirements and PIN expirations, remove options from the YubiKey PIV Manager, and so on.

Group Policy settings are stored in the Windows Registry as follows:

`Computer\HKEY_CURRENT_USER\Software\Yubico\YubiKey PIV Manager`
or -

`Computer\HKEY_LOCAL_MACHINE\Software\Yubico\YubiKey PIV Manager`

## Group Policy settings

The following table describes the group policy options that administrators can use to customize the user experience with YubiKey PIV Manager.

| Name | Description | Key | Type | Key Type | Valid Options | Default Value |
|---|---|---|---|---|---|---|
| **algorithm** | The algorithm to use for key pair generation | algorithm | string | REG_SZ | RSA1024, RSA2048, ECC256 | RSA2048 |
| **card reader** | String to match against when looking for compatible YubiKey devices | card_reader | string | REG-SZ | [not restricted] | [none] |
| **Certreq Template** | Value to use in the `CertificateTemplate` parameter when calling `certreq.exe` | certreq_template | string | REG_SZ | [not restricted] | [none] |

| Name | Description | Key | Type | Key Type | Valid Options | Default Value |
|---|---|---|---|---|---|---|
| **Complex PIN/PUKs** | `True` to require complex PIN and PUK requirements, or `False` to maintain default complexity requirements | complex_pins | string | REG_SZ | True, False | False |
| **Enable Import** | When False, hide the Import from file button on the Certificates window | enable_import | string | REG_SZ | True, False | True |
| **PIN as Management Key** | When `True`, the Management Key is based on the PIN | pin_as_key | bool | REG_SZ | True, False | False |
| **PIN Expiration** | When entering a non-zero value, a timestamp is written when the PIN is changed, and the user must change the PIN after the specified number of days. Zero value = no PIN expiration. | pin_expiration | int | REG_DWORD | 0 or greater | 0 |
| **Displayed Output Formats** | Output formats available when generating a key | shown_outs | List of strings | REG_MULTI_SZ | PK, SSC, CSR, CA | SSC, CSR, CA |
| **Displayed Certificate Slots** | A list of the certificate slots to show in the YubiKey PIV Manager | shown_slots | list of strings | REG_MULTI_SZ | 9a, 9c, 9d, 9e | 9a, 9c, 9d, 9e |
| **Subject Distinguished Name (DN)** | Subject to use when generating a CSR or self-signed certificate | REG_SZ | string | REG_SZ | [not restricted] | /CN=%USERNAME% |