YubiKey Smart Card Deployment Guide

Best Practices and Basic Setup

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

Copyright

Trademarks

Disclaimer

Contact Information

Yubico Inc
530 Lytton Ave, Suite 301
Palo Alto, CA 94301
USA
yubi.co/contact

Document Release Date

Version 1.1
Oct 20, 2017

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 PIV specifications, see the PIV standards on the NIST website: (http://csrc.nist.gov/groups/SNS/piv/standards.html).

Microsoft Windows servers and clients have provided traditional smart card capabilities for years. But one thing was always missing, an efficient and cost-effective way to deploy this technology at scale. With new capabilities being provided by Yubico, much of the smart card complexity is eliminated, leaving the truly relevant technology that has stood the test of time - key-based Authentication backed by a Public Key Infrastructure (PKI).

A YubiKey paired with a specialized minidriver developed by Yubico and available natively in Windows 10, is changing the equation in the enterprise and promising scalable, manageable strong, key-based authentication throughout employee user populations.

The YubiKey Minidriver is a Windows driver, natively shipped with the Windows operating system (starting with Win 10 R3), for integrating the YubiKey into the Microsoft environment of clients, directories and management tools for key-based authentication. In this key-based solution, a YubiKey with PIV support is both a smart card and a smart card driver.

Using the simplest definition, a driver is a software component that lets the operating system and a device communicate with each other. This integration of YubiKey and the Microsoft tools enables end-users and administrators to manage certificates on YubiKeys with native Microsoft tools, and securely share those certificates via the Microsoft plumbing. The YubiKey Minidriver links all the Microsoft backend infrastructure (namely Active Directory) and management tools, including the all-important Certificate Authority, allowing the YubiKey to be use for smart card authentication without the need for costly hardware or middleware.

PIV Deployment

This document covers the basic steps required to set up an Active Directory domain environment for smart card authentication, including considerations before provisioning YubiKeys for smart card login. We recommend that a qualified domain administrator be placed in charge of the process and that you use these instructions as a guideline for deployment. Rather than cover the complexities inherent in a corporate environment (for example, an Enterprise Root Certification Authority, multiple Subordinate Certificate Authorities, Certificate Revocation Lists, and so on), these instructions cover only the basic topics.

The following topics are covered in this document:

Getting Additional Help

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

- Support home page
- Documentation and FAQs
- Start a Support ticket
  TIP: To assist in diagnosing issues, we recommend that you include a log file containing the issue observed. To enable the debug log file, add the following registry key. Log files will be created for each running process in C:\Logs.

  Key: HKLM\Software\Yubico\ykmd
  Value: DebugOn (DWORD) - to enable logging set value to 1.

- If you need assistance with Microsoft tools or products, contact Microsoft directly.

Feature list

On the Windows operating system, the Windows Inbox Smart Card Minidriver, msclmd.inf, enables base functionality for using PIV smart cards, such as YubiKeys, which have already been provisioned with at least one credential.

Windows Inbox Smart Card Minidriver (without YubiKey Minidriver)

- Use a single certificate of each type: Authentication, Signature, & Encryption (key management)
- Certificates using RSA 2048-bit keys

YubiKey Minidriver Feature Overview

The YubiKey Smart Card Minidriver (YubiKey Minidriver), ykmd.inf, provides additional features beyond the base Microsoft support: managing certificates and PINs on a YubiKey via the native Windows GUI and/or APIs and support for ECC cryptographic algorithms.

- Use *multiple* Authentication certificates
- Set / Change smartcard PIN via Windows GUI
- Unblock a blocked PIN
- Certificate Enrollment (add user certificate)
  - Auto-enrollment
  - MMC admin console on behalf of an end user
- Set policy for touch to allow private key use
- Import certificate chains for User Certificates
- Supported Key Algorithms
  - RSA 2048-bit keys
  - Elliptic Curve Cryptography (ECC) ECDH/ECDSA-P256 keys
  - Elliptic Curve Cryptography (ECC) ECDH/ECDSA-P384 keys

YubiKey Smart Card Minidriver Features

Use Multiple Authentication Credentials

All User Authentication Certificates on the YubiKey smart card are visible via the minidriver and are displayed for use by applications based on the certificate's Key Usage Extension and Extended Key Usage Extension.

Set / Change Smart Card PIN

- Provide the ability to set the smart card PIN during enrollment through the Windows interface.
- Provides the ability to Change the PIN directly through the Windows interface

Unblock a Blocked PIN

When a user enters their PIN incorrectly three times consecutively, the PIN is blocked and the smart card features are unusable until the PIN is unblocked.

If a PIN Unlock Key (PUK) was created for the device, the YubiKey Minidriver allows the PIN to be unblocked directly in the Windows interface by providing the PIN Unlock Key (PUK), in hexadecimal format.

IMPORTANT: Creation of a PUK is blocked by default in the minidriver. If you want to create a PUK for a YubiKey, follow instructions in the "YubiKey Smart Card Deployment Guide". If a PUK is not created and you forget your PIN, the device will need to be reset which permanently deletes all private keys and certificates, then new certificates and private keys must be created!

Certificate Enrollment (add user certificate)

The YubiKey Minidriver adds the following certificate deployment options:

- Auto-enrollment, enabling users to register their YubiKey directly through the Windows built-in certificate provisioning process
- Administrators enrolling on behalf of other users directly through the Microsoft MMC console of Windows Server

Set Policy for Touch to Allow Private Key Use

(YubiKey 4 devices on firmware version 4.3 and higher, YubiKey NEO not supported)

Set the policy to determine if touching the YubiKey's button is required to use the certificate's private key. This is an additional protection against use of a private key without explicit user intent. The policy is stored in the YubiKey's secure element during private key creation or import and cannot be changed. If a different policy is desired, a new certificate and private key must be created.

Touch Policy Options: Cached (for 15 seconds per touch), Never (No touch required) <default>

The default can be changed via a Windows registry entry and applies to all new certificate / private key pairs added to the YubiKey. If different policies are required per certificate, the registry entry must be changed prior to each certificates creation. See the YubiKey Smart Card Deployment Guide for additional information.

Import Certificate Chains for User Certificates

When User Certificates are added to a smart card via MS auto-enrollment or through Windows MMC, the intermediate certificate(s) and root certificate, aka certificate chain, are not added to the smart card.

If adding the complete certificate chain is required, the YubiKey Minidriver enables root and intermediate certificates to be imported through the MS Certutil command line utility.

Supported Key Algorithms

The YubiKey Minidriver supports the following algorithms for its certificate keys:

- RSA 2048-bit keys
- (ECC) ECDH/ECDSA-P256 keys
- (ECC) ECDH/ECDSA-P384 keys

Before You Begin

The YubiKey Minidriver is designed to function in a Windows Server and Client environment configured for smart card authentication. Ensuring your deployment is set up properly is a crucial element of the initial planning for the YubiKey Minidriver deployment.

System Requirements

Before performing the steps in this document, be sure your environment meets these requirements:

- The YubiKey Minidriver cannot be used simultaneously with the YubiKey PIV Manager for provisioning user Windows credentials. If your environment utilizes the YubiKey PIV Manager (such as environments using Mac OS and Linux in conjunction with Windows PCs), the YubiKey Minidriver should be prevented from being installed via Group or Domain Policy, and the PIV Manager should be used instead of the YubiKey Minidriver and native Windows components.
- For servers, install Microsoft Windows Server 2008 R2 or later (the examples shown in this document are from Windows Server 2016).
    - NOTE: YubiKey NEO and YubiKey NEO-n are not supported on Windows Server 2016 (certificate sizes using the default settings are too large). If you are using this version of Windows Server, be sure all of your users are using YubiKey 4 or YubiKey 4 Nano devices. For more information about compatibility, see the following table.
    - For clients, install Microsoft Windows 7 Pro/Enterprise/Ultimate or later (for YubiKeys to log in to Windows)
    - NOTE: Windows 10 (version 1607) users are no longer supported on Windows Server 2008 R2. Be sure you have moved these users to Windows Server 2012 R2 or later. For more information about compatibility, see the following table.

Windows Server Compatibility

	Server 2008 R2	Server 2012 R2	Server 2016
YubiKey NEO	Compatible	Compatible	Not Supported
YubiKey 4	Compatible	Compatible	Compatible

Windows Desktop Compatibility

	Windows 7	Windows 8 / 8.1	Windows 10+
Server 2008 R2	Compatible	Compatible	Not Supported
Server 2012 R2	Compatible	Compatible	Compatible
Server 2016	Compatible	Compatible	Compatible

- Set up a Microsoft Windows Active Directory domain environment.

- If you are using Remote Desktop Connection (RDP), install the YubiKey Minidriver on *both* the source and the destination computers.
- For Microsoft Windows Server 2008 R2 and up, it is recommended to use the Microsoft Key Storage Provider instead of the older Microsoft Credential Storage Provider. Microsoft Windows Server 2008 R2 may need the Microsoft Key Storage Provider installed before it is available.

Determining the Preferred Method of Enrollment

Before using the YubiKey Minidriver in implementing smart card authentication in an Active Directory domain environment, it is important to consider the method of user enrollment that you will use.

The three options using the YubiKey are:

- **User self-enrollment**: There are a few different ways of doing this. (1) Auto-enrollment can be set up in your domain, allowing you to utilize the built-in Windows functionality to request and load login certificates. (2) For situations where utilizing the native Windows smart card support is not ideal, such as deployments where MacOS and Linux PC are also using smart card authentication, self-enrollment can be accomplished by distributing the YubiKey PIV Manager and YubiKeys to enable users to request their own login certificates. For more information, download *YubiKey PIV Manager User's Guide* from the Yubico website.
- **Enrolling on behalf of other users**: By granting enrollment agent permissions to one or more users or groups, your administrators or help desk accounts with elevated permissions can enroll certificates on behalf of other users through the Microsoft Management Console.
- **Advanced enrollment**: Use the Yubico PIV command line tool to write custom command line scripts or build your own deployment application. For more information, download the *Yubico PIV Tool Command Line Guide* from the Yubico website.

NOTE: The first two options can be implemented concurrently to provide flexibility, but be sure to set up a separate certificate request template to cover each option.

Download all documentation from the Yubico website (https://www.yubico.com/support/documentation/).

Configuring a Certification Authority (CA) for Smart Card Authentication

In order to utilize the Smart Card functions in a Windows environment using the YubiKey Minidriver, a Certification Authority (CA) must first be stood up.

This chapter covers the basic configuration for setting up a new Certification Authority (CA) to a Windows Server (2008 R2 and above). These steps assume an Active Directory environment is already stood up and configured.

NOTE: If a Certification Authority already exists in your environment, skip this chapter and proceed to YubiKey Minidriver Installation.

In this Chapter

Certification Authority Prerequisites

IMPORTANT: The installation should be performed by an experienced system administrator. These instructions include steps for a basic configuration. For information about implementing advanced configurations, see this Microsoft Technet article (https://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx).

Before you create a Certification Authority (CA), be sure you set up a Microsoft Windows Active Directory domain environment.

Microsoft recommends that you do not deploy a Root Certification Authority (CA) on a Domain Controller. As an additional security measure, consider installing the Root CA on a standalone offline server, and use a Subordinate CA for all certificate signing. For more information, see the Microsoft documentation: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/server-certificate-deployment-overview

Creating a Certification Authority

If a Certification Authority already exists in your environment, skip this section and proceed to YubiKey Minidriver Installation.

Creating a Certification Authority:

1. Open Server Manager and choose **Add roles and features**, and click **Next**.
2. Select **Role-based or feature-based installation**, and click **Next**.
3. Select **Select a server from the server pool**.
4. From **Server Pool**, select the server on which you want to install the Certification Authority, and click **Next**.
5. Under **Server Roles**, select **Active Directory Certificate Services**, and click **Next**.
6. Click **Add Features**, and click **Next**.
7. Click **Next** again.
8. Select **Certification Authority**, and click **Next**.
9. Click **Install**. Allow several minutes for the process to complete.
10. Select **Configure Active Directory Certificate Services on the destination server**, and click **Next**.
11. Select **Certification Authority**, and click **Next**.
12. Choose **Enterprise CA**, and click **Next**.
13. Choose **Root CA**, and click **Next**.
14. Select **Create a new private key**, and click **Next**.
15. Select the **cryptographic provider**, **hash algorithm**, and **key length** for the private key, and click **Next**.
    NOTE: Changing the **cryptographic provider**, **hash algorithm**, and **key length** from the default values may increase the size of smart card login certificates beyond the available space on the YubiKey. Be sure the values you select are supported by the YubiKeys that you will use in your environment:

	Maximum supported certificate size	Supported key lengths (bits)	Supported hash algorithms	Encryption
YubiKey NEO	2048 bytes	RSA: 1024, 2048	SHA1, SHA256	RSA
YubiKey 4	3072 bytes	RSA: 1024, 2048 ECDSA: P256, P384	SHA1, SHA256, SHA384	RSA, ECDH

16. **Common name** and **Distinguished name** will be automatically populated. Confirm the values match the server name and domain name, and click **Next**.
17. Select the **validity period** for the Certification Authority certificate, and click **Next**.
    TIP: This period must be longer than what you set for the smart card login certificate template. Yubico recommends the default value of **5 years**.
18. Leave the Database locations to the default values and click **Next** again.
19. Verify all settings match the desired values, and click **Configure**.
20. When the process completes, exit the installation wizard by clicking **Close**.

YubiKey Minidriver Installation

There are multiple ways to install the YubiKey Minidriver in a Microsoft Windows environment. The YubiKey Minidriver is available to be downloaded directly from the Yubico website at https://www.yubico.com/support/knowledge-base/categories/downloads/.

The Minidriver must be installed on all machines where the YubiKey will be used as a smart card to access. These include servers which users remotely connect to, as well as the connecting PC.

Manual Install

The YubiKey Minidriver can be downloaded directly from the Yubico website and be distributed and installed manually by anyone with administrator rights on the computer. There are two versions of the YubiKey Minidriver; one for older versions of Windows (Windows 7 SP1, Windows 8.1, Windows Server 2008 R2 and Windows Server 2012 R2) and one for newer releases (Windows 10 and Windows Server 2016). Both versions are installed with the same process:

1. Download the YubiKey Minidriver, available at https://www.yubico.com/support/knowledge-base/categories/downloads/ as a ZIP file.
2. Extract the downloaded ZIP file to your preferred location.
3. Ensure no YubiKey is currently connected to your computer.
4. Locate and right-click on **ykmd.inf** and select **Install**.
5. Follow the prompts to install the driver. If prompted, restart your computer.

Setting Touch Policy

The YubiKey can be set to require a physical touch to confirm any cryptographic operations. This is an optional feature to increase security, ensuring that any authentication operation must be carried out in person. The YubiKey Minidriver sets the touch policy are set when a key is first imported or generated. Once set for a key on the YubiKey, the policies cannot be changed.

By default, the touch policy for keys imported/generated through the minidriver is created with the default setting of the touch policy disabled.

To alter the policy behavior, the registry must be configured prior to setting up keys, either on the station enrolling the keys or pushed out to all machines using Group Policy Objects.

Key: **HKLM\Software\Yubico\ykmd**

Value: **NewKeyTouchPolicy** (DWORD) - sets the touch policy on new keys generated/imported through the minidriver. Accepted values are:

- **1 <Never>** - Default policy of never requiring a user touch
- **2 <Always>** - Policy is set to require a user touch to confirm each and every cryptographic operation. Yubico does not recommend using this setting, as some Windows services, such as login, may require multiple cryptographic operations in a short time span.
- **3 <Cached>** - Policy is set to require physical touch once, then allow for cryptographic operations in a small time window afterwards. For using the physical touch option with Windows Smart Card Logon, this option is required.

Setting PIN Unblock Code (PUK) Policy

When a YubiKey is used with the YubiKey Minidriver for the first time, the YubiKey Minidriver checks to ensure default values are not being used for the management key and the PIN Unblock Code (PUK). If the default values are in use, the YubiKey Minidriver will upgrade the Management key to a protected value and block the PUK. A blocked PUK will prevent the PIN Unblock function from being active.

The YubiKey Minidriver supports unlocking a blocked PIN using the built-in Windows UI. To enable this function, you need to enable the **Allow Integrated Unblock screen to be displayed at the time of logon** in Windows Group Policy. This configuration setting is located in: **Computer Configuration->Administrative Templates->Windows Components->Smart Card**

To allow the PUK to remain unblocked, a registry key must be set on the system the YubiKey is first programmed on. This can either be an enrollment station or pushed out using Group Policies to all systems. When this option is enabled, it is critical you use the YubiKey PIV tool to change the PUK before the YubiKey is used.

The PUK policy can be set in the registry using the entry:

Key: **HKEY_LOCAL_MACHINE\Yubico\ykmd**

Value: **BlockPUKOnMGMUpgrade** (DWORD) - setting it to 0 disables the PUK lock feature, any other value enables it.

For information on using the YubiKey PIV tools for setting the PUK, refer to Yubico documentation at: https://developers.yubico.com/yubico-piv-tool/

Preparing the Certification Authority for Smart Card Login with a YubiKey

Before smart card login certificates can be requested and loaded to YubiKeys, several steps need to be completed, including creating smart card login templates and publishing the templates in the Certification Authority.

The examples in this section use Microsoft Windows Server 2012 R2. If you are using a different version of Windows Server, modify the steps to suit your environment.

In this Chapter

Creating a Smart Card Login Template for User Self-Enrollment

It is important to create a smart card login certificate template in the CA before distributing YubiKeys to your users who will enroll themselves. These topics are described:

Creating a Smart Card Login Template for User Self-Enrollment

1. Right-click the Windows Start button and select **Run**.
2. Type `certtmpl.msc` and press Enter.
3. Click **Certificate Templates**, locate and right-click **Smartcard Logon**, and select **Duplicate Template**.
4. Select the General tab, and make the following changes as needed:
   a. For **Template display name / Template name**, we recommend that you choose a short name without spaces such as YubiKey or YubicoSC.
   b. For **Validity period**, ensure the timeframe you specify does not exceed the restrictions for your Certification Authority.
   c. Ensure the option to **Publish certificate in Active Directory** is selected.
5. Select the Compatibility tab, and make the following changes as needed:
   a. Select the operating system where the **Certification Authority** resides.
   b. For **Certificate recipient**, select the oldest Windows operating system in your domain environment.
6. Select the Request Handling tab, and make the following changes as needed:
   a. For **Purpose**, select **Signature and encryption**.
   b. Ensure the option for **Include symmetric algorithms allowed by the subject** is selected.
   c. Ensure the option for **Renew with the same key** is selected. This option may be disabled if Windows 7 and below are included in the Compatibility settings.
   d. **Check the option** for **automatic renewal of smart card certificates, use the existing key if a new key cannot be created**.
   e. Check the option for Prompt the user during enrollment.
7. On the Cryptography tab, make the following changes, as needed:
   a. Provider category: Select **Key Storage Provider** from the dropdown.
   b. Algorithm name: Select either **RSA**, **ECDH_P256**, or **ECDH_P384** from the dropdown. Note: ECDH_P521 is not supported.
      - Note that if an ECDH algorithm is selected, the client Windows systems need to have Elliptic Curve Cryptography (ECC) Certificate Login support added using Group Policy or by editing the registry. See the following section for instructions.
   c. Minimum key size: If you selected **RSA** in the previous step, enter `2048`. If you selected **ECDH_P256** or **ECDH_P384** in the previous step, this field automatically populated.
   d. Select the option for **Requests must use one of the following providers**.
   e. Under **Providers**, select **Microsoft Smart Card Key Storage Provider**.
   f. For **Request hash,** click the arrow and select **SHA256** from the list displayed.
8. On the Security tab, make the following changes, as needed:
   a. Group or user names: Confirm the domain group you want to allow access to the template is listed. If not, click **Add**, enter the name of the group, and then click **OK**.
   b. Permissions for [group name]:

   If users will be auto-enrolling using the built-in Windows functionality, ensure the options are checked for **Read**, **Enroll**, and **Autoenroll**.

9. Click **Apply**, and then click **OK** to close the template properties window.
10. Close the Certificate Templates window.

Adding the Template to the Certification Authority

1. Right-click the Windows Start button and select **Run**.
2. Type `certsrv.msc` and press Enter.
3. Click **Certification Authority**, double-click your server, double-click **Certificate Templates**, right-click on the white space within the center pane, select **New** and then select **Certificate Template to Issue**.
4. Locate and select the recently created self-enrollment template, and then click **OK**.
5. Allow Active Directory to update. Depending on environment, it could take up to eight hours for the template to publish to Active Directory.

Editing Group Policy to Enable Auto-Enrollment

1. Right-click the Windows Start button and select **Run**.
2. Type `gpmc.msc` and press Enter.
3. Navigate to the AD forest and Domain containing your server, double-click your server and double-click Group Policy Objects.
4. Right-click on the group policy you want to edit, and then select **Edit**.
5. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.
6. Right-click **Certificate Services Client - Certificate Enrollment Policy** and select **Properties**.
7. Click the arrow for Configuration Model and select **Enabled**.
8. Click **OK**.
9. Right-click **Certificate Services Client - Auto-Enrollment** and select **Properties**.
10. Click the arrow for Configuration Model and select **Enabled**.
11. Select the checkbox for **Renew expired certificates, update pending certificates, and remove revoked certificates**.
12. Select the checkbox for **Update certificates that use certificate templates**.
13. Click **OK**.
14. Expand **User Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies**.
15. Right-click **Certificate Services Client - Certificate Enrollment Policy** and select **Properties**.
16. Click the arrow for Configuration Model and select **Enabled**.
17. Click **OK**.
18. Right-click **Certificate Services Client - Auto-Enrollment Policy** and select **Properties**.
19. Click the arrow for Configuration Model and select **Enabled**.
20. Select the checkbox for **Renew expired certificates, update pending certificates, and remove revoked certificates**.
21. Select the checkbox for **Update certificates that use certificate templates**.
22. Click **OK.**
23. Allow Active Directory to update. Depending on your environment, it could take up to eight hours for the template to publish to Active Directory.

Using Auto-Enrollment to Enroll Users

With Auto-Enrollment enabled on the Windows Server and local systems via Group Policy, the user's experience is straightforward. This section describes the steps your users will need to follow to auto-enroll their YubiKey for Login.

User Auto-Enrollment Workflow

1. Log into a user account. A Certificate Enrollment notification appears above the System Tray.
2. Click the Certificate Enrollment notification to open the Certificate Enrollment wizard. If the popup has disappeared (or didn't initially appear) click the arrow in the System Tray to expand the list of options and click on the certificate icon.
3. On the initial screen, click **Next**.
4. Select the appropriate certificate template and click **Enroll**. If multiple certificate templates are listed, assuming the template was set up properly, "**STATUS:** Enrollment required" should appear next to the correct template.
5. Enter your YubiKey PIN and then click **OK**. If a custom PIN has not been set, enter the default PIN:
   123456.
6. Windows enrolls the YubiKey for Windows login. The process may take several seconds, depending on the network connection to the server running the Certification Authority. Once completed, click **Finish**.

Setting the PIN

Once a YubiKey is registered, the user's PIN should be changed if the default value (123456) is still set. Once the user has logged into his account, he can change the PIN of a YubiKey connected to his system as follows:

1. Use **Ctrl+Alt+Del** to enter the lock screen.
2. Select **Change a Password** from the options presented.
3. The user is prompted to enter the current PIN, as well as the new PIN.
4. Press Enter to commit the new PIN.

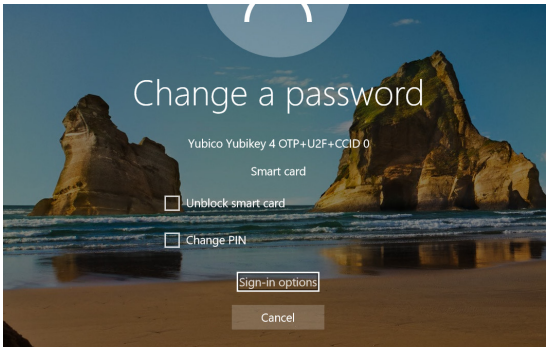
PIN Unblock

By default, the user PIN is blocked when three consecutive incorrect PINs have been entered. The PIN Unblock Code (PUK) is used for unblocking the User PIN. If both the PIN and the PUK are blocked, the YubiKey must be reset, which deletes any loaded certificates and returns the YubiKey to a factory default state. By default, the PUK is blocked by the YubiKey Minidriver. To enable the PUK, see the section, Setting PIN Unblock Code (PUK) Policy.

Windows 7, Windows Server 2008, and Windows Server 2008 R2 require the PIN unblock code (PUK) to be typed in as hexadecimal digits. This means that if your PUK is 12345678, to unlock a pin through the Windows UI, you must type the ASCII hex-encoded bytes of the PUK string (in this case, the unlock code would be 3132333435363738). Refer to an ASCII chart (for example, www.asciitable.com) to encode a PUK in hexadecimal.

To unblock the user PIN:

1. With the YubiKey inserted, attempt to log in at the Windows login screen. When the PIN is blocked, the "change a password" screen is displayed. The following screenshot is an example using Windows 10.



2. Select the checkbox for **Unblock smart card**.
3. In the Response field, enter the PUK code in hexadecimal format. For example, the default value of 12345678 in hexadecimal format is 3132333435363738. Refer to your favorite ASCII to hex converter, if necessary.
4. In the **New PIN** and **Confirm PIN** fields, enter a new, properly formatted PIN, and then press Enter.
5. Remove and then reinsert the YubiKey, and test the new PIN to verify you can access the account.

Note: To enable this function, the "**Allow Integrated Unblock screen to be displayed at the time of logon**" Group Policy Object must be set. This setting is located in:

Computer Configuration > **Administrative Templates** > **Windows Components** > **Smart Card**

Creating a Smart Card Login Template for Enrolling on Behalf of Other Users

In order for administrators and privileged help desk users to enroll YubiKeys for other users, the CA must be set up to do so. This section provides instructions on setting up a CA to support an Enrollment Agent to allow for the Enroll on Behalf functionality.

These topics are described:

- Creating an Enrollment Agent Enabled Smart Card Certificate Template
- Adding the Template to the Certification Authority
- Specifying the Permissions for the Enrollment Agents and Publishing the Certificate Template
- Creating an Enrollment Agent
- Using an Enrollment Agent to Enroll on Behalf of
- Generating and Importing User Certificates as a .pfx file

To create an enrollment agent enabled smart card certificate template

1. Right-click the Windows Start button and select **Run**.
2. Type `certtmpl.msc` and press Enter.
3. Click **Certificate Templates**, locate and right-click **Smartcard Logon**, and select **Duplicate Template**.
4. Select the General tab, and make the following changes, as needed:
    a. For Template display name / Template name, we recommend that you choose a short name without spaces such as YubiKey or YubicoSC.
    b. For Validity period, ensure the timeframe you specify does not exceed the restrictions for your Certification Authority.
    c. Ensure the option to **Publish certificate in Active Directory** is selected.
5. Select the Compatibility tab, and make the following changes as needed:
    a. Select the operating system where the **Certification Authority** resides.
    b. For **Certificate recipient** select the oldest Windows operating system in your domain environment.
6. Select the Request Handling tab, and make the following changes as needed:
    a. For **Purpose,** select **Signature and encryption**.
    b. Ensure the option to **Include symmetric algorithms allowed by the subject** is selected.
    c. Ensure the option to **Renew with the same key** is selected. This option may be disabled if Windows 7 and below are included in the Compatibility settings.
    d. Ensure the option **For automatic renewal of smart card certificates, use the existing key if a new key cannot be created** is selected.
    e. Ensure this option to **Prompt the user during enrollment** is checked.
7. On the Cryptography tab, make the following changes, as needed:
    a. For **Provider category**, click the arrow and select **Key Storage Provider** from the dropdown.
    b. For **Algorithm name**, select either **RSA**, **ECDH_P256**, or **ECDH_P384** from the list displayed. Note: ECDH_P521 is not supported.
        i. Note that if an ECDH algorithm is selected, the client Windows machines need to have Elliptic Curve Cryptography (ECC) Certificate Login support added using Group Policy or by editing the registry. See the following section for instructions.
    c. For **Minimum key size**, if you selected **RSA** in the previous step, enter `2048`. If you selected **ECDH_P256** or **ECDH_P384** in the previous step, this field is automatically populated.
    d. Select the option for **Requests must use one of the following providers**:.
    e. For **Under Providers**, select **Microsoft Smart Card Key Storage Provider**.
    f. Click the arrow for **Request hash** and select **SHA256** from the list displayed.
8. On the Security tab, make the following changes, as needed:
    a. For **Group or user names**: Confirm **Authenticated Users** is listed. If is not, click **Add**, enter the name of the group, and then click **OK**.
    b. For **Permissions for Authenticated Users**, be sure the option for **Read** is checked.
    c. For **any administrator, group or user who needs to create certificates for others**, be sure the option for **Read** and **Enroll** is checked.
9. On the Issuance Requirements tab, make the following changes, as needed:
    a. Be sure the option is selected for **This number of authorized signatures**, and enter 1.
    b. For **Policy type required in signature**, Select **Application policy**.
    c. For **Application policy**, select **Certificate Request Agent**.
10. Click **OK** to close the template properties window.
11. Close the Certificate Templates MMC Snap-in.

To add the template to the Certification Authority

1. Right-click the Windows Start button and select **Run**.
2. Type `certsrv.msc` and press Enter.
3. Click **Certification Authority**, double-click your server, double-click **Certificate Templates**, right-click on the white space within the center pane, select **New**, and then select **Certificate Template to Issue**.
4. Locate and select the enroll-on-behalf-of template you just created, and then click OK.
5. Allow Active Directory to update. Depending on environment, it could take up to eight hours for the template to publish to Active Directory.

To specify the permissions for the enrollment agents and publish the certificate template

1. Right-click the Windows Start button and select **Run**.
2. Type `certtmpl.msc` and press Enter.
3. Right-click the **Enrollment Agent** template, and then click **Properties**.
4. On the **Security** tab, make sure the user or group designated as an Enrollment Agent has **Read** and **Enroll** permissions on the template, and then click **OK**.
5. In the **Certificate Authority** window, right-click the **Certificate Templates** folder, and select **New**, and then select **Certificate Template to Issue**
6. Select the **Enrollment Agent** template, and click **OK**. The Enrollment Agent certificate automatically saves to the user's default file save location.

To create an enrollment agent

1. Right-click the Windows Start button and select **Run**.
2. Type `certmgr.msc` and press Enter.
3. Under Console Root, click to expand **Certificates - Current User**.
4. Click to expand **Personal**.
5. Click to select **Certificates.**
6. Right-click on the white space within the center pane, select **All Tasks**, and then select **Request New Certificate…**
7. Click **Next**.
8. Select **Active Directory Enrollment Policy** and then click **Next**.
9. Locate and select the Enrollment Agent template, and then click **Enroll**.

To use an enrollment agent to “Enroll on Behalf of”

1. Right-click the Windows Start button and select **Run**.
2. Type `certmgr.msc` and press Enter.
3. Under Console Root, click to expand **Certificates - Current User**.
4. Click to expand **Personal**.
5. Right-click on the white space within the right pane, select **All Tasks**, select **Advanced Operations**, and then select **Enroll on Behalf of**.
6. Select Active Directory Enrollment Policy and then click **Next**.
7. Click **Browse**, choose your enrollment agent certificate from the Security Pop-up screen, and then click **Next.**
8. Locate and select the smart card template you created for enroll on behalf of, and then click **Next**.
9. Click **Browse**, select the user you want to enroll, and then click **OK**.
10. In the User name or Alias field, verify you have the correct user, and then click **Enroll**.
11. Enter the PIN for the Smart Card and then click **OK**. The YubiKey with be loaded with a certificate for the selected user. It is recommended that users change their PIN once the certificate is loaded.

Generating and importing user certificates as a .pfx file

In environments where the user certificates cannot be generated on the YubiKey, they can be generated on a Windows PC as a .pfx file and imported to a YubiKey for use.

To use an enrollment agent to generate a .pfx file for import

1. Right-click the Windows Start button and select **Run**.
2. Type `mmc` and press Enter.
3. Add a Certificates snap-in for My User account.
4. In the console tree, expand the Personal store, and then click Certificates.
5. On the Action menu, point to All Tasks, point to Advanced Operations, and then click Enroll on behalf of to open the Certificate Enrollment wizard. Click Next.
6. Browse to the Enrollment Agent certificate that you will use to sign the certificate request that you are processing. Click Next.
7. Select the type of certificate that you want to enroll for. When you are ready to request a certificate, click Enroll.
8. After the Certificate Renewal Wizard has successfully finished, click Close.

Exporting a certificate with Private Key

1. On the workstation where you enrolled the smart card certificates, choose **Start,** choose **Run**, and then in the Open box, type `MMC`. Choose **OK.**
2. On the Console page, on the File menu, select Add/Remove Snap in.
3. On the Add/Remove Snap-in dialog box, choose **Add**. The Add Standalone Snap-in page appears. Select **Certificates** and then choose **Add**.
4. On the Certificates snap-in page, select **My user account**, and then choose **Finish**. On the Add or Remove Snap-in page, choose Close, and then on the Add/Remove Snap-in page, choose OK.
5. On the Console page, in the navigation pane, expand **Certificates - Current User** – and then expand **Personal.** In the navigation pane, select **Certificates**.
6. In the details pane, locate the certification authority certificate that was issued for the Smart Card template. This file should have the name of your Smart card user. **Right-click** this certificate, select **All Tasks**, and then choose **Export**.
7. The Welcome to the Certificate Wizard dialog box appears. Choose **Next** to continue.
8. On the Export Private Key page, select **Yes**, export the private key. Choose **Next**.
9. On the Export File Format page, make sure that you select Personal Information Exchange – PKCS #12(.PFX). Make sure that you select the Enable strong protection box. Choose **Next.**
10. On the Password page, supply a password, and then choose **Next**.
11. On the File to Export page, type the path and filename of the .pfx file. For example, C:\usercert.pfx. Choose **Next**.
12. Choose Finish. On the Certificate Export Wizard page, choose **OK** to confirm that the export was successful.
13. Repeat steps 7 through 12. For each user certificate to export.

Importing a .pfx file using the YubiKey PIV Manager

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 (along with its associated private key), click **OK**.
4. To acknowledge the message stating that any certificates currently stored in slot 9a will be overwritten, click **OK**.
5. Browse to the .pfx file you want to import (created in steps 7-12 of the previous section), and click **Open**.
6. To confirm the password that was set for the certificate, type the password and click **OK**. (see step 10 of the previous section)
7. Click **OK**.

Adding Support for Elliptic Curve Cryptography (ECC) Certificate Login

By default, ECC certificates are not supported for domain login in Active Directory. In order to allow ECC certificates for domain login, a GPO must be set. This can be done either through Group Policy or by editing the registry on the local system (in the case of a system where Group Policy is not managed by the domain). These topics are described:

Adding ECC Through a Group Policy Object

1. Right-click the Windows Start button and select **Run**.
2. Type `gpmc.msc` and press Enter.
3. Navigate to the AD forest and Domain containing your server, double-click your server and double-click Group Policy Objects.
4. Right-click on the group policy you want to edit, and then select **Edit**.
5. Expand **Computer Configuration > Policies > Administrative Templates > Windows Components > Smart Card.**
6. Right-click on **Allow ECC certificates to be used for logon and authentication** and select **Edit**.
7. On the Edit window select **Enabled**.
8. Click **OK**.
9. Allow Active Directory to update. Depending on environment, it could take up to eight hours for the template to publish to Active Directory.

Adding ECC Through the Local Registry

In the event a machine cannot be managed via Group Policy, support for ECC Certificates can be done via the local registry.

1. Right-click the Windows Start button and select **Run**.
2. Type `regedit` and press Enter.
3. Expand **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Policies** > **Microsoft** > **Windows** > **SmartCardCredentialProvider** (Note: It is possible that SmartCardCredentialProvider doesn't currently exist. If that is the case, right-click Windows and select **New** > **Key** and name it SmartCardCredentialProvider).
4. With SmartCardCredentialProvider highlighted, open the **Edit** menu and select **New** > **DWORD (32-bit) Value**.
5. Name the new object EnumerateECCCerts.
6. Right-click on EnumerateECCCerts and select **Modify…**
7. Set the Value data to 1 and click **OK**.
8. Close Registry Editor.

Changing the Behavior for Your Domain When You Remove the Smart Card

When a user logs into the domain account using a smart card, by default, the user can remove the smart card at any point with no change to the login status.

For security reasons, you may want to enforce a different behavior. In Group Policy, you can specify that Windows locks the user account, or logs out the user if the smart card is removed at any point while the user is logged in to the account.

Important: If you are planning to implement additional functions of the YubiKey NEO (that is, U2F protocol or one or both of the configuration slots) and your Group Policy specifies that Windows locks the user's workstation or logs the user out, this temporarily disconnects the smart card from the operating system and locks the workstation or logs out the user account. This is the expected behavior for USB and smart card combination devices. This does not apply to the YubiKey 4, YubiKey 4 Nano, or YubiKey 4C.

In this Chapter

Editing Group Policy to Lock the User's Workstation when a Smart Card is Removed

1. Right-click the Windows Start button and select **Run**.
2. Type `gpmc.msc` and press Enter.
3. Right-click on the group policy you want to edit, and then select **Edit**.
4. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
5. On the left pane, locate and right-click **Interactive Logon: Smart card removal behavior**, and select **Properties**.
6. Click **Local Security Setting**, and set it to Lock Workstation or Force Logoff, depending on your requirements.
7. Click **Apply**, and then click **OK**.

Adding a Key to the Windows Registry to Delay the Smart Card Removal Policy Service

When using the YubiKey NEO with other functions (such as U2F), the YubiKey will act as if the smart card has been ejected, locking Windows. To prevent this from occurring, the registry can be modified to delay the Smart Card Removal Policy Service.

1. Right-click the Windows Start button and select **Run**.
2. Type `regedit` and press Enter.
3. Right-click on the group policy you want to edit, and then select **Edit**.
4. Expand **Computer Configuration** > **Preferences** > **Windows Settings**.
5. Right-click **Registry,** and select **New** > **Registry Item**.
6. Set the following fields as indicated:

   Action: `Update`
   Hive: `HKEY_LOCAL_MACHINE`
   Key Path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SCPolicySvc`
   Value name: `DelayedAutoStart`
   Value type: `REG_DWORD`
   Value data: `1`

7. Click **OK**.

Working with Enterprise Root Certificates

For a standard forest, Windows can manage the trust chain for the YubiKey smart card authentication automatically. However, in situations where there may not be a direct connection between the Windows computer and the server with the Certification Authority, loading the Root Certificate on a YubiKey can bridge the gap for the initial registration. Common situations covered are: including systems on a multi-forest domain, users logging onto domain accounts from non-domain systems, or deployments adding new systems to a domain using a smart card for authentication.

Adding an Enterprise Root Certificate to the YubiKey

1. Right-click the Windows Start button and select **Windows PowerShell (admin)** or **Command Prompt (Administrator)**, depending on your Windows build.
2. Type in the following command and press Enter:
   ```
   certutil -scroots update
   ```
3. When prompted for your Windows Security PIN, enter the PIN for your smart card and then press Enter.
4. To verify both the smart card certificate and the root certificate are loaded to the smart card, type in the following command and then press Enter:
   ```
   certutil -scinfo
   ```

You are prompted to enter your smart card PIN several times. Enter it each time it is requested.

Manually deleting certificates

To delete certificates from a certificate chain manually, including a Base CSP container and associated key/certificate on the YubiKey 4 or YubiKey NEO through the YubiKey Minidriver, use the `certutil` command line program. To list the current containers on the card, use the command:

```
certutil -key -csp "Microsoft Base Smart Card Crypto Provider"
```

This returns a list of container names and key types. To remove a container cleanly, use the following command while running with elevated permissions as administrator:

```
certutil -delkey -csp "Microsoft Base Smart Card Crypto Provider" "<container name>"
```


Next Steps

This section helps you determine the next steps in your YubiKey smart card deployment process using the YubiKey Minidriver.

User Self Enrollment

If auto-enrollment has been set up in your environment, your users should be prompted to register a smart card the next time they log into their accounts.

Enrollment on Behalf of Other Users

The YubiKey Smart Card Minidriver allows for an admin or user with elevated permissions to enroll on behalf of other users. This is useful for deployments where the YubiKeys need to be provisioned from a central location, or replacement YubiKeys need to be generated for users who have locked their PIN.

Protecting Microsoft Cloud Environment with a YubiKey

Microsoft has built an impressive collection of integrated cloud service capabilities that span infrastructure, platforms and applications. Many of these services can also be secured with your YubiKey through Active Directory Federation Services (AD FS). While the steps to do so are outside the scope of this document, interested parties can learn more at: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-additional-authentication-methods-for-ad-fs

Troubleshooting

Working with the YubiKey and the YubiKey Minidriver, there are a number of options to help troubleshoot issues with the YubiKey. As Yubico receives more feedback from customers, this section will be updated with common questions and fixes.

YubiKey Smart Card Specifications

There are storage limitations to consider when loading multiple certificates to the YubiKey:

YubiKey 4

- The YubiKey 4 has a maximum certificate size of 3052 bytes in DER format. Up to twelve (12) certificates can be stored concurrently.
- The YubiKey 4 has 15,260 bytes available for storing Certificate Chain Certificates (root and intermediate certificates).
- The firmware doesn't report how much space allocated to the smart card applet is currently in use.

YubiKey NEO

- The YubiKey NEO has a maximum certificate size of 2024 bytes in DER format. Up to four (4) certificates can be stored concurrently.
- The YubiKey NEO has 10120 bytes available for storing Certificate Chain Certificates (root and intermediate certificates).
- Since the YubiKey Minidriver prioritizes assigning slots for keys by smart card usage, it will place the first two authentication keys in slots 9a and 9d during enrollment. This driver is designed for the YubiKey 4 which has additional retired slots available for general purpose (82-90), so it will attempt to place a third exchange key in slot 82. This will fail on the YubiKey NEO (maximum of two certificates). For details, refer to https://developers.yubico.com/PIV/Introduction/Certificate_slots.html.

Basic Troubleshooting

- If I YubiKey is connected to a computer when installing the YubiKey Minidriver, Windows may continue to use the native generic smart card minidriver. The YubiKey Minidriver can be set as the default driver by following these steps:
    - Connect your YubiKey to your computer
    - Open up **Device Manager**
    - Locate the YubiKey smart card entry - it will be labeled **Identity Device (NIST SP 800-73 [PIV])**. Right click the entry and select **Update driver**.
    - In the window which opens, select **Search automatically for updated driver software**
    - A list of drivers will be displayed. Select **YubiKey Minidriver**
- The YubiKey NEO, when trying to enroll a certificate larger than the supported maximum key size of 2048 bits may freeze unexpectedly. For larger certificates, it is recommended to use the YubiKey 4 hardware.
- When attempting to import a certificate into the YubiKey 4 when the card has reached its maximum storage of 12 certificates, the certutil program may show an inconsistent number of certificates.
  Use the following command to list the keys seen by the YubiKey Minidriver along with their associated container names:

  ```
  certutil -key -csp "Microsoft Base Smart Card Crypto Provider"
  ```

  Use the following command to delete a specific key:

  ```
  certutil -delkey -csp "Microsoft Base Smart Card Crypto Provider" "<container name>"
  ```

- Due to a limitation with the legacy CSP, the Microsoft Base Smart Card Crypto Provider will not see any ECC certificates or keys. To view ECC certificate and key information, use the Smart Card Key Storage Provider:
  `certutil -csp "Microsoft Smart Card Key Storage Provider"`

  We recommend you use the "Microsoft Smart Card Key Storage Provider" for better security and functionality.

- The Microsoft Smart Card Key Storage Provider does not support importing ECC keys and certificates through the certutil program. This is a limitation of the certutil program.
- Windows 7 may not be able to verify code integrity of the YubiKey Minidriver DLL (ykmd.dll) due to the SHA256 signature of Yubico's code signing certificate. If you see a "Bad Image" warning when running certutil or see error 3002 in the Microsoft Windows CodeIntegrity Operational log, apply update KB3033929 to resolve this issue.

Advanced Troubleshooting

When the YubiKey is not seen as a smart card on the host Window PC, Administrators can try the following troubleshooting steps to resolve the issue.

Details and Configuration

- If working with a YubiKey with existing keys, the minidriver will automatically create containers for slots containing RSA and ECC keys with corresponding valid certificates if the keys/certs have been manually through other tools.
- PIN and touch policy are set when a key is imported or generated and cannot be changed after it is configured on the device. By default, the PIN and touch policy for imported/generated keys through the minidriver are created using the default settings according to YKPIV_PINPOLICY_ONCE (1) and YKPIV_TOUCHPOLICY_DEFAULT (0). The PIN policy cannot be modified. To alter the touch policy behavior, the following registry entry must be configured prior to setting up keys. Note, changing these settings is most commonly done using an enrollment machine where multiple YubiKeys will be configured.

  Key: **HKLM\Software\Yubico\ykmd**

  Value: **NewKeyTouchPolicy** (DWORD) - sets the touch policy on new keys generated/imported through the minidriver. Accepted values are the numeric value of the touch policy definition from ykpiv.h

- Blocked PUK: The Minidriver will automatically block an unsafe PUK. It is, however, not possible for the Minidriver to know the value of the new PUK. If the Minidriver detects that you are using a default MGM key, and have not modified your YubiKey via the PIV Manager or equivalent tool, when it protects your MGM key it will also block your PUK.
  If you are confident that you have changed your PUK to a safe value, or if you want to discontinue this behavior you can control this functionality via the following registry value:

  Key: **HKEY_LOCAL_MACHINE\Yubico\ykmd**

  Value: **BlockPUKOnMGMUpgrade** (DWORD) - 0 turns off the PUK block feature, any other value enables it

Logging

For issues not resolved by this guide, it is recommended to enter a support ticket at https://www.yubico.com/support/get-support/ . To assist in the diagnostics of issues, it is recommended to include a log file containing the issue observed.

To enable the debug log file, add the following registry key and log files will be created per running process in C:\Logs.

Key: **HKLM\Software\Yubico\ykmd**

Value: **DebugOn** (DWORD) - to enable logging set value to 1.

Uninstalling the YubiKey Minidriver

Should you determine that you prefer to utilize the inbox generic class minidriver provided by Microsoft (msclmd.inf) to access the YubiKey PIV functions instead of the YubiKey Minidriver, follow the instructions below to uninstall the YubiKey Minidriver.

1. Open Command Prompt as Administrator or PowerShell as Admin
2. Change directory to [OS drive letter]:\Windows\System32\DriverStore\FileRepository
3. Type cd ykmd and press Tab, and then press Enter. The current path should look similar to the following:
   C:\Windows\System32\DriverStore\FileRepository\ykmd.inf_amd64_1e4c7d5bdb6914f9

4. Type the following command and press Enter:
   ```
   rundll32 setupapi.dll,InstallHinfSection DefaultUninstall 4 .\\ykmd.inf
   ```

If you want to also delete the driver and other related files from your computer, delete the entire YubiKey Minidriver directory in C:\Windows\System32\DriverStore\FileRepository\ (using the example in step 3, the directory name is ykmd.inf_amd64_1e4c7d5bdb6914f9).

To prevent the YubiKey Minidriver from being reinstalled after removal, it can be blocked via the Windows Group Policy. This configuration setting is located in:

1. Right-click the Windows Start button and select **Run**.
2. Type `gpmc.msc` and press Enter.
3. Navigate to the AD forest and Domain containing your server, double-click your server and double-click Group Policy Objects.
4. Right-click on the group policy you want to edit, and then select **Edit**.
5. Expand **Computer Configuration -> Administrative Templates -> System -> Device Installation -> Device Installation Restrictions**
6. Right-click **Prevent installation of the of devices that match any of these device IDs** and select **Edit**.
7. Click the option **Enabled**.
8. Under Options, click **Show**
9. Enter the Hardware ID. This can be found via Device Manager:
   a. Click on **Smart Cards -> YubiKey Smart Card**
   b. Right click on the **YubiKey Smart Card** and select **Properties**.
   c. Open the Details tab, and the Drop down to Hardware ids
   d. The SCFILTER\CID_ID# value for the YubiKey will be displayed. Note the YubiKey 4 and YubiKey NEO have different hardware IDs.
10. Click **OK**.

