YubiKey Smart Card Minidriver User Guide

Yubico

May 14, 2025

CONTENTS

CHAPTER

ONE

INTRODUCTION

As a tool to deploy smart cards across an environment consisting of multiple domains with multiple user identities stored on a single YubiKey, the YubiKey Smart Card Minidriver (YKMD) enables management of the YubiKey smart card functionality based on the US Federal Government Personal Identity Verification (PIV) standard (for details on this functionality, see the YubiKey Technical Manual).

Microsoft Windows supports traditional PIV smart cards for user authentication, allowing the YubiKey to be utilized as a strong authentication solution. The YubiKey Minidriver extends the support of the YubiKey on Windows from just authentication to allowing Windows to load and directly manage certificates on it. This enables an easy to use, easy to deploy, scalable implementation of strong multi-factor authentication across an entire organization utilizing the native Windows tools and the YubiKey.

The YKMD allows for the use of native Windows services to enroll YubiKeys as smart cards, both directly by individual users and by administrators enrolling YubiKeys as smart cards on behalf of other users.

The YKMD is a small, lightweight driver that builds on top of the Windows Inbox Smart Card Minidriver (Windows Minidriver). On the Windows operating system, the Windows Minidriver provides basic functionality for using PIV smart cards that have already been provisioned with at least one certificate. However, the Windows Minidriver cannot be used to provision certificates or manage PINs. Unlike this and other native Microsoft tools or legacy Yubico tools, the YKMD accomplishes this by enabling Windows to write directly to the PIV module, utilize the native CertUtil command suite, and add extended functionality when using the YubiKey as a smart card. See *YKMD Features*.

Note: For Mac OS and Linux environments in conjunction with Windows PCs, use the YubiKey Manager / ykman instead of the YubiKey Minidriver and native Windows components.

Note: Provisioning credentials on the YubiKey using the Windows certificate enrollment dialogs (enabled by the YubkiKey Minidriver) **in parallel with** other tools such as the YubiKey Manager or Yubico Authenticator is not recommended. See the YubiKey Manager (ykman) CLI and GUI Guide.

This guide covers the installation of the YKMD on user PCs, as well as instructions for users enrolling YubiKeys as smart cards directly.

CHAPTER

TWO

YKMD FEATURES

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

The YubiKey Minidriver 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. This includes:

Certificate Enrollment Options
The YKMD adds the following certificate enrollment/deployment options:

- **Auto-enrollment**, enabling users to register their YubiKey directly through the Windows built-in certificate provisioning process.
- **Enrollment-on-behalf-of**: enabling administrators to enroll on behalf of other users through the Microsoft Management Console (MMC) on Windows Server.
- Automatic re-enrollment

Import certificate chains for user certificates
When User Certificates are added to a smart card via Microsoft auto-enrollment or through Windows MMC, the intermediate certificates and root certificate (also known as the certificate chain) are not added to the smart card. If adding the complete certificate chain is required, the YKMD enables root and intermediate certificates to be imported through the Microsoft `Certutil.exe` command line utility.

Support for multiple authentication certificates/credentials on a single YubiKey.
Use the YKMD to view all user authentication certificates on the smart card. They are displayed for use by applications based on the certificates' Key Usage Extension and Extended Key Usage Extension.

Certificate Key Algorithms Support
Elliptic-Curve (ECC) (Windows 10 and Windows 11)

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

We also support 3k/4k and Ed25519/(X25519); however, since the release of Minidriver 4.6.3.252 and the 5.7 firmware on YubiKeys, please note that while Ed25519 certificates will be listed, the private key cannot be used due to limitations of the Windows BaseCSP, which does not support this algorithm.

Set and change smartcard PIN via Windows GUI.
This feature provides the ability to set and change the PIN directly through the Windows interface (press Ctrl + Alt + Del > [Change a password]) without the need to install any additional third-party applications.

Unblock a blocked PIN
Utilize the Integrated Unblocking Screen.

Set policy for touch
This allows private key use.

Note: For information on how to use these features, see our Support article, Deploying the YubiKey Minidriver to Workstations and Servers.

CHAPTER

THREE

YKMD INSTALLATION

The YKMD must be installed on all machines where the YubiKey is used as a smart card for access. These include servers to which users remotely connect, as well as the connecting PC. The YKMD can be downloaded directly from the Yubico website at Smart card drivers and tools. Scroll down the page to **YubiKey Smart Card Minidriver (Windows)**.

Note: The YKMD is no longer available through Microsoft Windows Update.

When installing the YKMD, there are two options.

MSI installer
: Using either the Windows GUI or Command line

  We recommend using the MSI installer through the Windows command line for local installations and remote computers and Servers. See *Automated Installation*.

  If the MSI installers are blocked, use the CAB installation method.

CAB file
: For large enterprise deployments, Yubico recommends using the CAB file in conjunction with a Group Policy Object Endpoint Configuration utility. This allows installing on to domain-connected machines. See *Automated Installation*.

  Yubico recommends using any software management platform already in place to deploy the YKMD to an enterprise environment.

  To deploy the YKMD with specific settings, such as with legacy_nodes and silent_install, requires an `.mst` file to enable these options in addition to the GPO.

For information on setting up a Windows Certification Authority for smart card authentication or enabling enroll on behalf of permissions for administrators, see the *Manual Installation*.

When using existing keys, the YKMD updates YubiKeys PIV containers to allow Windows to access credentials already present on the YubiKey for slots containing RSA and ECC keys with corresponding valid certificates if the keys and certificates are added manually through other tools. This function is blocked if the management key is manually changed using another tool.

Note: We recommend **not** provisioning credentials on the YubiKey using the Windows certificate enrollment dialogs (enabled by the YubkiKey Minidriver) in parallel with other tools such as the YubiKey Manager or Yubico Authenticator. If your environment uses Mac OS and Linux in conjunction with Windows PCs, use the YubiKey Manager instead of the YubiKey Minidriver and native Windows components. See the YubiKey Manager (ykman) CLI and GUI Guide.

CHAPTER

FOUR

MANUAL INSTALLATION

The YubiKey Minidriver can be downloaded directly from the Yubico website and distributed and installed manually by anyone with administrator rights on the computer. The YubiKey Minidriver software is available both as an MSI installer for 32 and 64 bit systems, and as a CAB file.

4.1 MSI File Install

The MSI Installer is the preferred method of manually installing the YubiKey Minidriver.

Note: The MSI installer automatically looks for and uninstalls previously installed YubiKey Smart Card driver versions from CAB, Windows Update, and an earlier Windows installer package.

1. Download the YubiKey Minidriver, available as an `.msi` file:
   a. Go to Windows Smart Card Applications and Tools.
   b. Scroll down the page to **YubiKey Smart Card Minidriver (Windows)**.
   c. Select the 32 or 64 bit installer as appropriate for the environment it is installed on.
2. Locate and double-click on **YubiKey-Minidriver MSI** Windows Installer.
3. Follow the prompts to install the driver. If prompted, restart your computer.

4.1.1 Command Line MSI Install

The YubiKey Minidriver MSI can also be installed via command line interface (CLI) using the `msiexec` command.

In the following examples, the version number, `4.6.3.252`, is an example. The actual number changes as downloads are updated.

Basic
The basic CLI install command is:

```
msiexec /i YubiKey-Minidriver-4.6.3.252-x64.msi
```

Unattended
To install in unattended mode with no user interaction required, include the `/passive` flag:

```
msiexec /i YubiKey-Minidriver-4.6.3.252-x64.msi /passive
```

Quiet
To install in quiet mode with no user interaction or dialog, use the `/quiet` flag:

```
msiexec /i YubiKey-Minidriver-4.6.3.252-x64.msi /quiet
```

Remote

When deploying the YubiKey Minidriver to remote servers where the YubiKey cannot be physically inserted:

Installing the MSI with the `Legacy Node` option enabled on servers prevents the "Smart Card Logon Over RDP Fails with `Requested Key Container is not Available`" error.

Create a legacy node for loading the YubiKey Minidriver. To do this, install the YubiKey Minidriver with the `INSTALL_LEGACY_NODE=1` option set:

```
msiexec /i YubiKey-Minidriver-4.6.3.252-x64.msi INSTALL_LEGACY_NODE=1 /quiet
```

4.2 CAB File Install

Installing the YubiKey Minidriver via CAB file is suggested in cases where installing via the MSI installer is prohibited. We recommend removing previous version(s) of the YubiKey Minidriver prior to installing the latest version via the CAB file.

Note: Earlier versions of the YubiKey Minidriver are **not** automatically removed when installing via the CAB file.

---

1. Download the CAB file for the YubiKey Minidriver:
   a. Go to Smart card drivers and tools.
   b. Scroll down the page to **YubiKey Smart Card Minidriver (Windows)**.
2. Extract the downloaded CAB file to your preferred location.

   This can simply be done via the CLI using the `Expand` command. For example, to extract the contents to the `C:\ykmd` directory, use the command:

   ```
   expand.exe yubikey-minidriver-4.6.3.252.cab -F:* C:\ykmd
   ```

   The version number, `4.6.3.252`, is an example. The actual number changes as downloads are updated.
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.

CHAPTER

FIVE

AUTOMATED INSTALLATION

This section provides configuration requirements and guidance for deploying YKMD in an enterprise environment. The steps provided allow YKMD to be pushed out to all workstations from a central repository, without requiring administrative rights on the local workstation.

There are two ways to automate installing YKMD:

Method 1
: Auto-install using a Startup Script. This is recommended for most environments. Create a startup script that can be pushed out via Group Policy Object (GPO). This automatically installs YKMD on ALL devices in the computer object OU that the GPO is linked to.

Method 2
: End user install using Device Manager. This is recommended when YKMD needs to be available to a large number of users but only installed on an as-needed basis: Create a registry entry on all client workstations with a GPO setting allowing standard users to update the inbox drivers to YKMD, without requiring an admin to physically touch or access the machine for the install. This way, the users can insert the YubiKey, launch the Device Manager, and automatically update the smart card driver to the latest version of YKMD.

Note: The version number shown below (4.6.3.252) is only an example. The actual number changes as downloads are updated.

5.1 Installing via Group Policy Object

For large deployments, YKMD can be centrally installed via Group Policy Objects. By leveraging a PowerShell script for the necessary commands and a shared network drive accessible from every client station to distribute the YKMD files, an Administrator can automate the installation. When creating an installation script, an Administrator needs to ensure they define registry entries for the PUK Policy, the Touch Policy and the Debug Log Policy, as well as installing the INF file directly.

5.2 Preparing the Deployment Environment

The process for deploying the YKMD `.cab` file requires every endpoint to be connected to the enterprise GPO domain and to have access to a shared directory. For machines where this is not an option, such as those on isolated networks, YKMD needs to be installed manually.

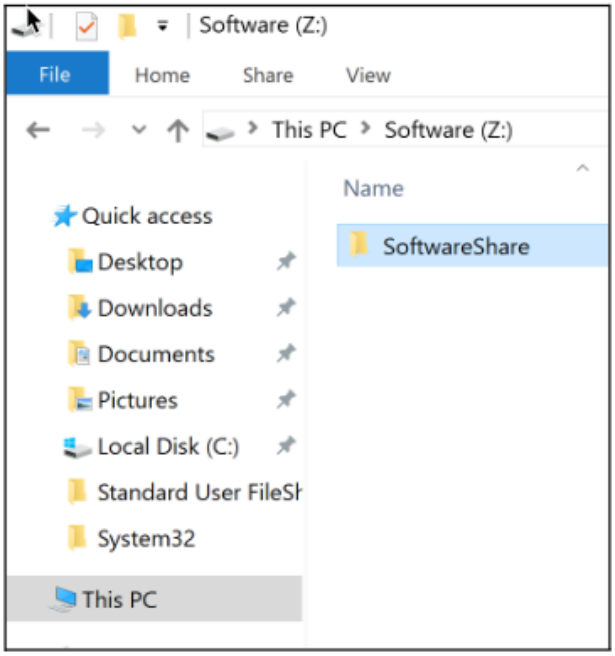
5.3 Creating the Driver Store

The first step to deploying YKMD is creating a network shared directory for the YKMD `.cab` file. If you already have a network share for driver software, we recommend using the existing location. If not, you need to create a shared network folder, which is accessible with read and execute permissions for all users.

For this example, we create a new folder in the `Z:\` drive.

1. Open File Explorer and browse to `Z:\`.
2. Create a new folder, such as: **SoftwareShare**.

   For example:

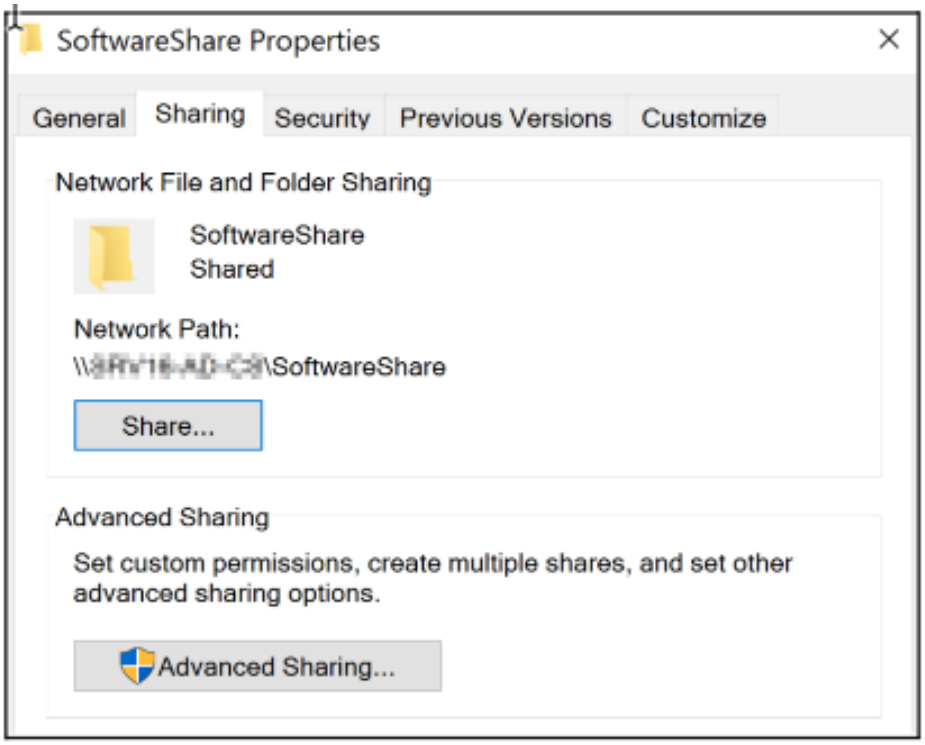


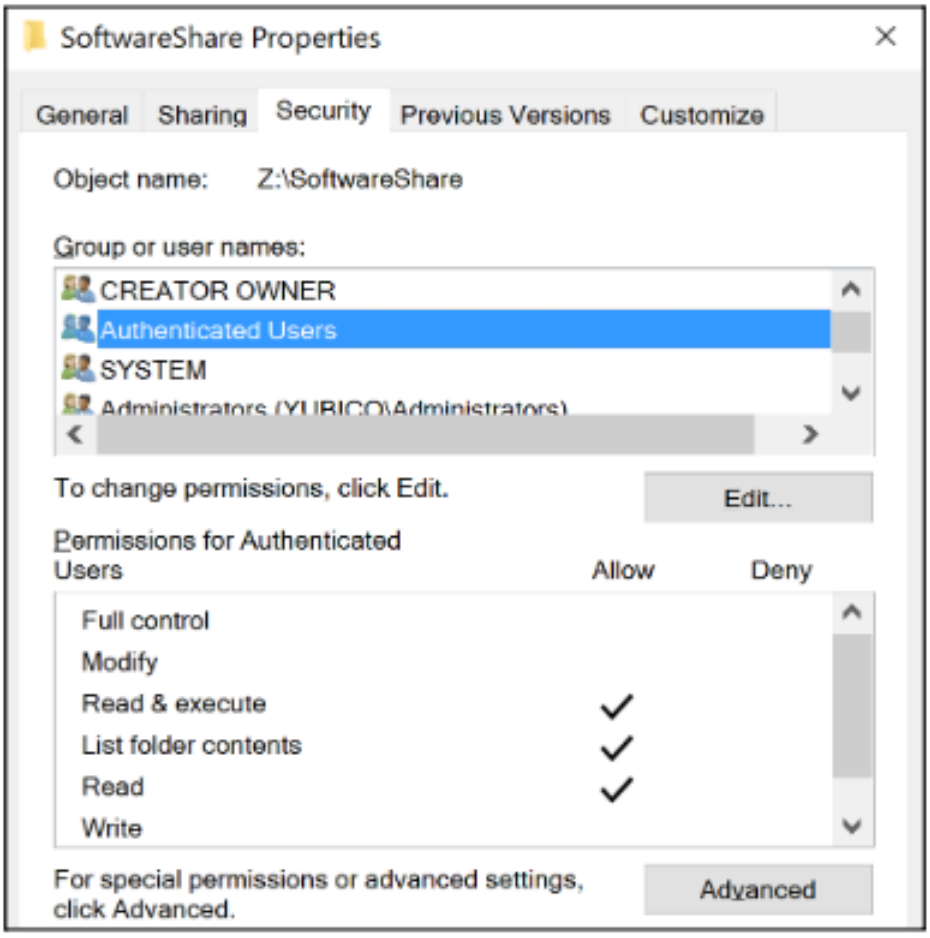
3. Inside this folder, create another folder, for example named **YKMD**. You can build this file structure per your standard naming convention.
4. Ensure the read, write, execute permissions on the folder are set as follows:
   - Read / Execute for **Everyone** or **Authenticated Users**
   - Read / Write / Execute for **Administrators**

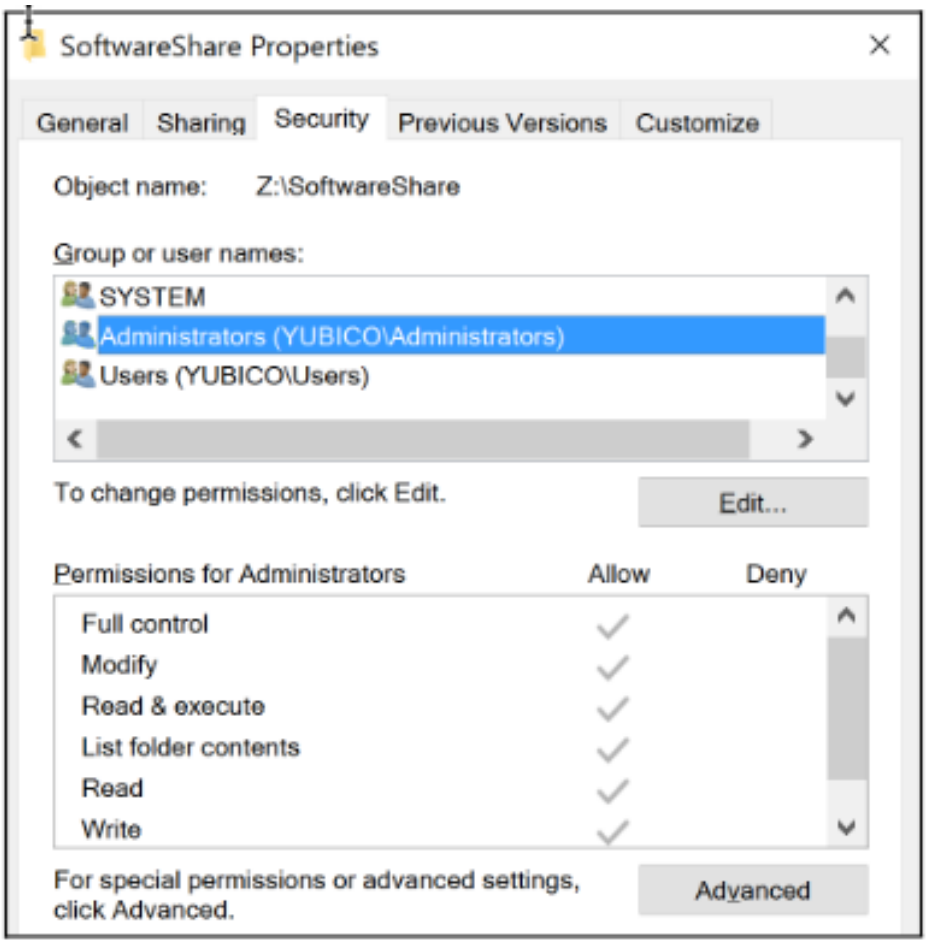
   Share network path.

   Authenticated users permissions settings

   Administrators permission settings


SoftwareShare Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
SoftwareShare
Shared
Network Path:
\\[redacted]\SoftwareShare
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...


SoftwareShare Properties
General
Sharing
Security
Previous Versions
Customize
Object name: Z:\SoftwareShare
Group or user names:
CREATOR OWNER
Authenticated Users
SYSTEM
Administrators (YUBICO\Administrators)
To change permissions, click Edit.
Edit...
Permissions for Authenticated Users
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced


SoftwareShare Properties
General
Sharing
Security
Previous Versions
Customize
Object name: Z:\SoftwareShare
Group or user names:
SYSTEM
Administrators (YUBICO\Administrators)
Users (YUBICO\Users)
To change permissions, click Edit.
Edit...
Permissions for Administrators
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced

5.4 Method 1 - Auto-Install via Startup Script

This process creates a PowerShell script for installing YKMD. This script is run with elevated permissions via GPO. It deploys YKMD upon startup, and continues to do so until the GPO object is disabled or removed.

5.4.1 Create the Minidriver Zip File

The PowerShell script deploys YKMD to the client machines as a zip file. Download the latest version of the YKMD and add it to a zip file named `YKMD.zip`.

5.4.2 Create the PowerShell Script

The PowerShell script used for the install script connects an endpoint to the shared network folder created previously. See *Creating the Driver Store*.

1. Copy the YKMD components to a local directory on the machine and install YKMD.
2. Create a PowerShell script with all the following items.

   Define the environmental variables at the start of the script.

```
$server="Server"
$shared_folder = "shared"
$temp = "$env:windir\temp"
$YKMD = "YubiKey-Minidriver-4.6.3.252.cab.sha256"
$DriverPath = "$env:windir\System32\DriverStore\FileRepository"
$destination = "YKMD"
$fullpath = $temp+"\"+$destination
$logdir = "$temp\logs";
$logfile = "yubikey.log"
$logfullpath = $logdir+"\"+$logfile;
New-Item $logdir -ItemType Directory -force;
Start-Transcript -Path $logfullpath -force;
copy-item "\\$server\$shared_folder\YKMD.zip" -Destination $temp -force;
Expand-Archive -Path "$temp\YKMD.zip" -DestinationPath $fullpath -force;
cmd.exe /c expand $fullpath\$YKMD -F:* $fullpath | Out-Null
Get-ChildItem $fullpath -Recurse -Filter "*inf" | ForEach-Object { PNPUtil.exe /add-
↪driver $_.FullName /install }
rundll32.exe setupapi.dll,InstallHinfSection Yubico64_61_Install 132 $fullpath\YKMD.
↪inf

# Remove the comment ``#`` from next line to create the device node or leave the␣
↪comment to let Windows handle creating the device node when the YubiKey is␣
↪inserted.
#cmd.exe /c DrvInst.exe "5" "2" "$DriverPath\YKMD.inf_amd64_24989c5c4b9230ad\YKMD.
↪inf" "0" "4e6904753" "0000000000000238" "WinSta0\Default"

Get-Service -Name "Scardsvr" | Set-Service -StartupType Automatic
Stop-Transcript
```

   Where -

   - `YKMD.zip` is copied to a shared folder which users have read permissions to replace the server with name of server that hosts the `YKMD.zip`.

- `folder_name` is replaced with name of shared folder on the network.
- `temp` sets the folder location.
- `YKMD` adds file_name. The version number, `4.6.3.252`, is an example. The actual number changes as downloads are updated.
- `DriverPath` adds driver path to the environment variable.
- `folder_name` replaces the folder name of destination.
- `Start-Transcript` starts recording logs. This doesn't work if the script is run remotely.
- `copy-item` downloads YKMD from the shared folder and install.
- `Get-ChildItem` installs the `.inf` driver.
- `rundll32.exe` imports the registry keys.
- `Get-Service` enables the Smart Card Service.
- `Stop-Transcript` stops logging.

3. Save this PowerShell script (`.ps1`) on the Windows Server for deployment.

5.4.3 Configure the GPO

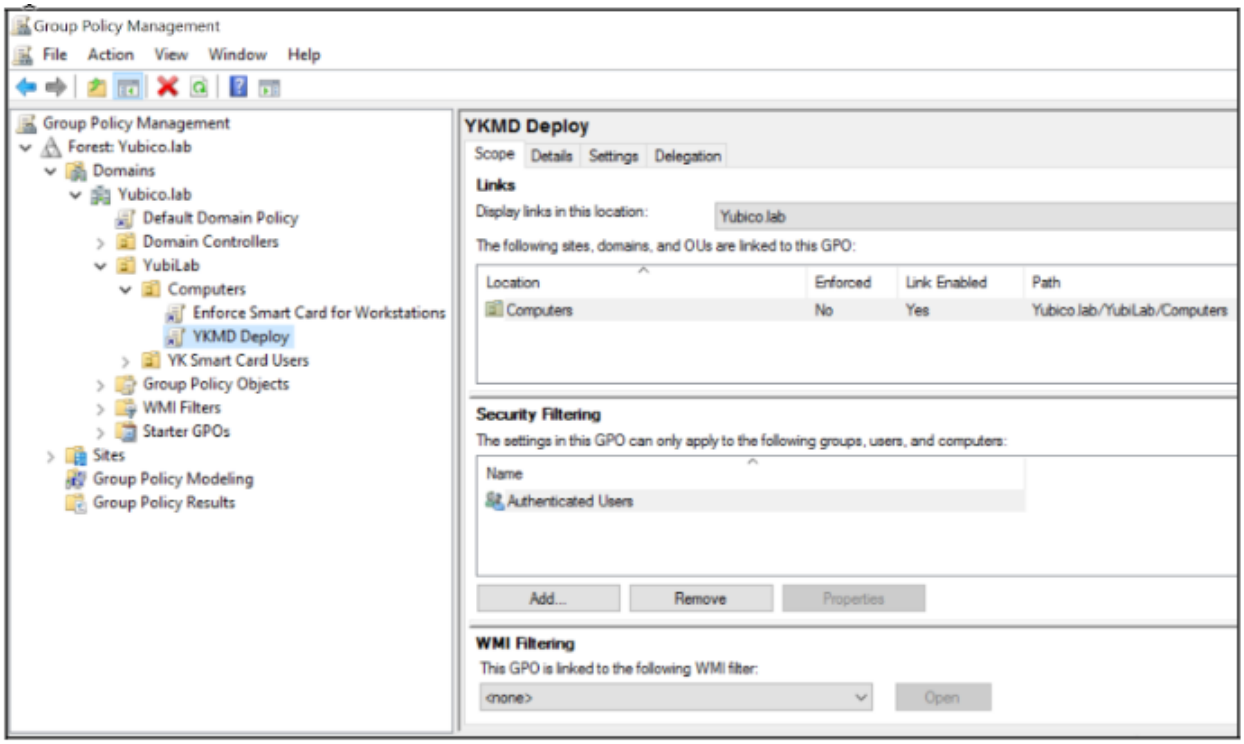
After the installation PowerShell script file is created, create the Group Policy Object to run the script. To do this, create a new GPO and link it to the location of the computer objects which require YubiKey Minidriver.

1. Click **Start > Run > gpmc.msc**.
2. Navigate to your domain and locate the OU for the computer objects.
3. Right-click and select **Create a GPO in this domain and Link it here**.
4. Create a descriptive name for this GPO, such as: **YKMD Deploy**.

   Example:

5.4.4 Edit YKMD Deploy GPO

1. Right-click the new YKMD Deploy GPO and select **Edit**.
2. Expand **Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown)**.
3. Right-click **Startup** and select **Properties**.
   a. Select **Add** then **Browse**.
   b. Using another file explorer window, browse to your startup script (`.ps1`), then copy and paste the file into the **File name** field.
   c. Select the file, then select **Open**.
   d. With the script in the **Script Name** field, select **OK**.
4. Select **OK** once more to complete the GPO configuration.

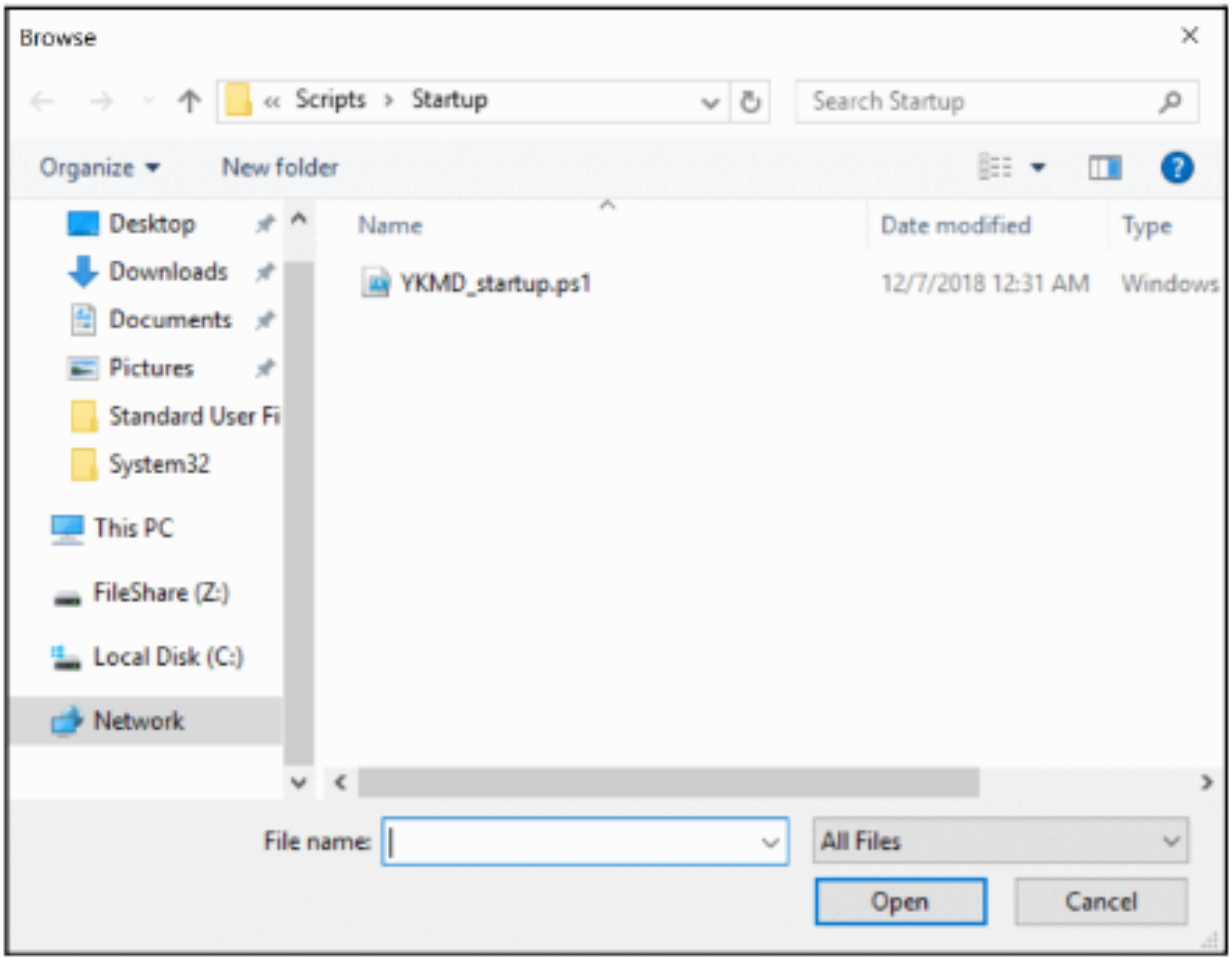


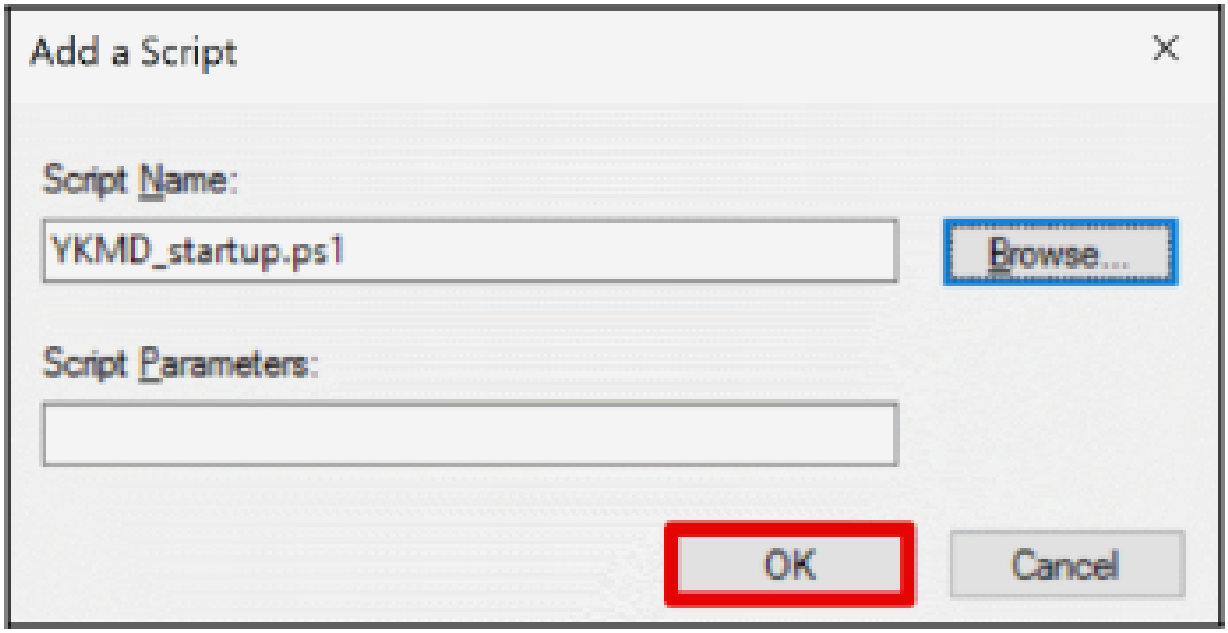
5.5 Method 2 - Standard User Install (Manual Update)

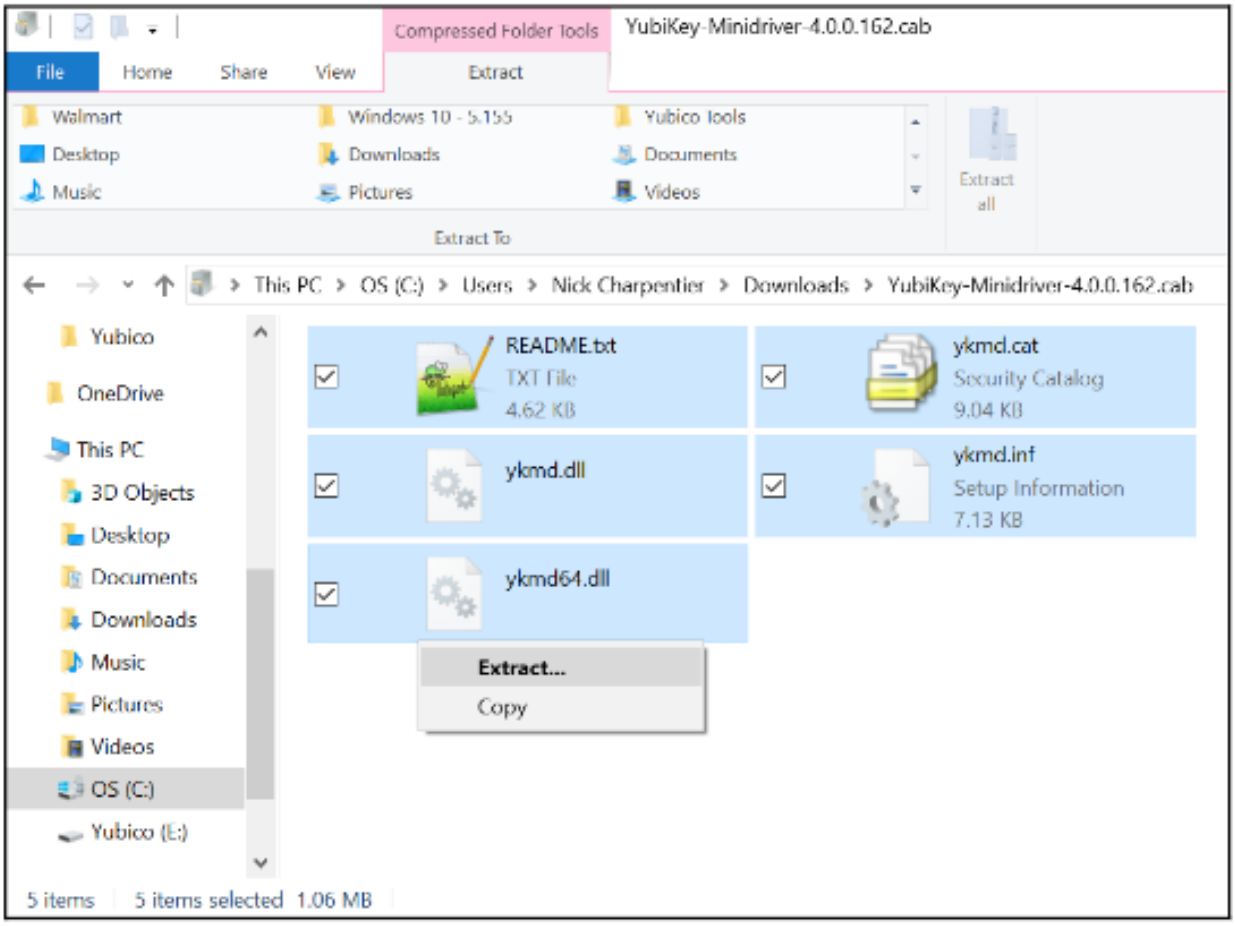
This process configures endpoints to make YKMD available to install when the standard user is ready. This does not install YKMD until the user requests it via the Device Manager.

5.5.1 Preparing YKMD for Distribution

1. Download YKMD from the Yubico Support site.
   a. See Windows Smart Card Applications and Tools
   b. Scroll down the page to **YubiKey Smart Card Minidriver (Windows)**.
   c. Download the latest release of the YubiKey Minidriver.
2. Extract the downloaded contents:
   a. Browse to your downloads directory.
   b. Double click the YKMD `.cab` file to open and view the contents.
   c. Select **All**.
   d. Right-click > **Extract**.
   e. Select either a local directory or extract directly to the fileshare created in previously. See *Creating the Driver Store*.


Browse
Scripts › Startup
Search Startup
Organize
New folder
Desktop
Downloads
Documents
Pictures
Standard User Fi
System32
This PC
FileShare (Z:)
Local Disk (C:)
Network
Name
Date modified
Type
YKMD_startup.ps1
12/7/2018 12:31 AM
Windows
File name:
All Files
Open
Cancel


Add a Script
Script Name:
YKMD_startup.ps1
Browse...
Script Parameters:
OK
Cancel


Compressed Folder Tools
YubiKey-Minidriver-4.0.0.162.cab
File
Home
Share
View
Extract
Walmart
Windows 10 - 5.155
Yubico Tools
Desktop
Downloads
Documents
Music
Pictures
Videos
Extract all
Extract To
This PC > OS (C:) > Users > Nick Charpentier > Downloads > YubiKey-Minidriver-4.0.0.162.cab
Yubico
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
OS (C:)
Yubico (E:)
README.txt
TXT File
4.62 KB
ykmd.cat
Security Catalog
9.04 KB
ykmd.dll
ykmd.inf
Setup Information
7.13 KB
ykmd64.dll
Extract...
Copy
5 items
5 items selected 1.06 MB

5.5.2 Configure the GPO

Confirm that the file share is configured and accessible to all client workstations, and that YKMD is extracted to that directory. Once this is accomplished, proceed to configure the GPO.

The Group Policy Object handles two things:

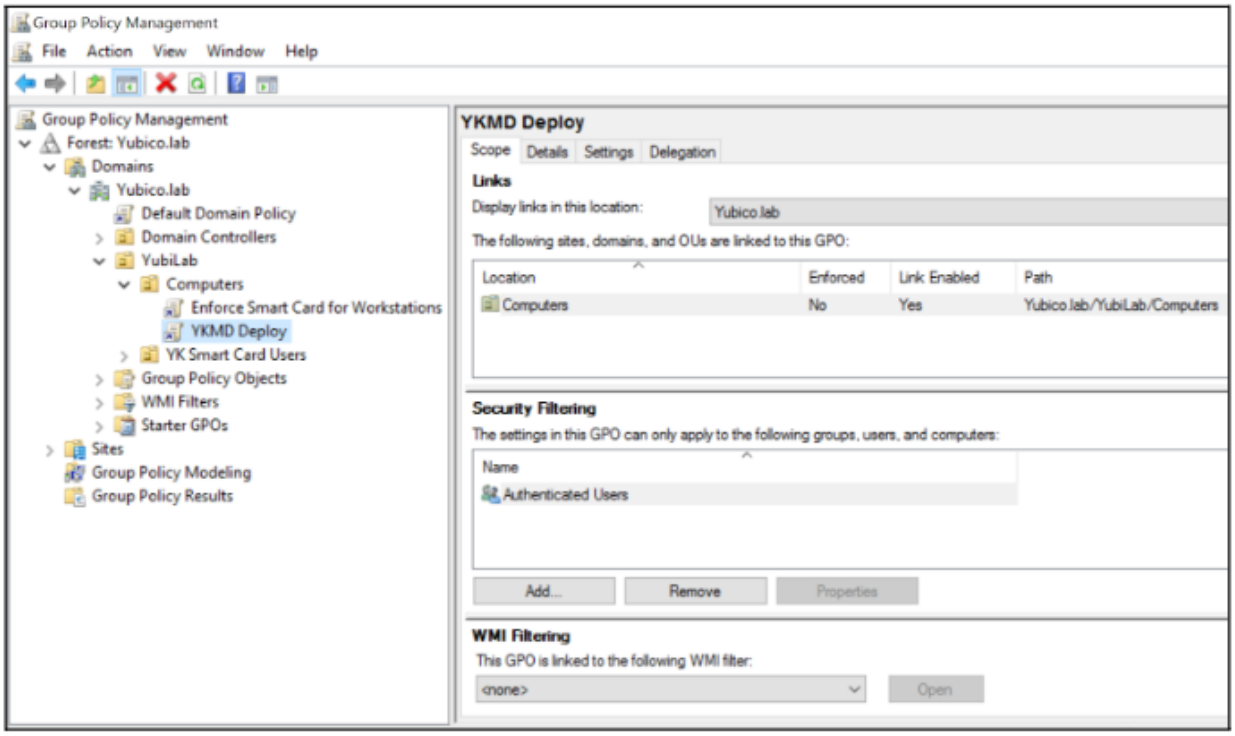
- Making the client workstations aware of the location of YKMD. This is accomplished via an updated Registry setting.
- Allowing standard users to install YKMD without requiring admin privileges. This is accomplished via whitelisting the GUID of YKMD.

5.5.2.1 Create a new GPO

In the location of the computer objects that require YKMD, create a new GPO and link it.

1. Click **Start > Run > gpmc.msc**.
2. Navigate to your Domain and locate the OU for the computer objects.
3. Right-click and select **Create a GPO in this domain and Link it here**.
4. Create a descriptive name for this GPO, such as: **YKMD Deploy**.

   For example:



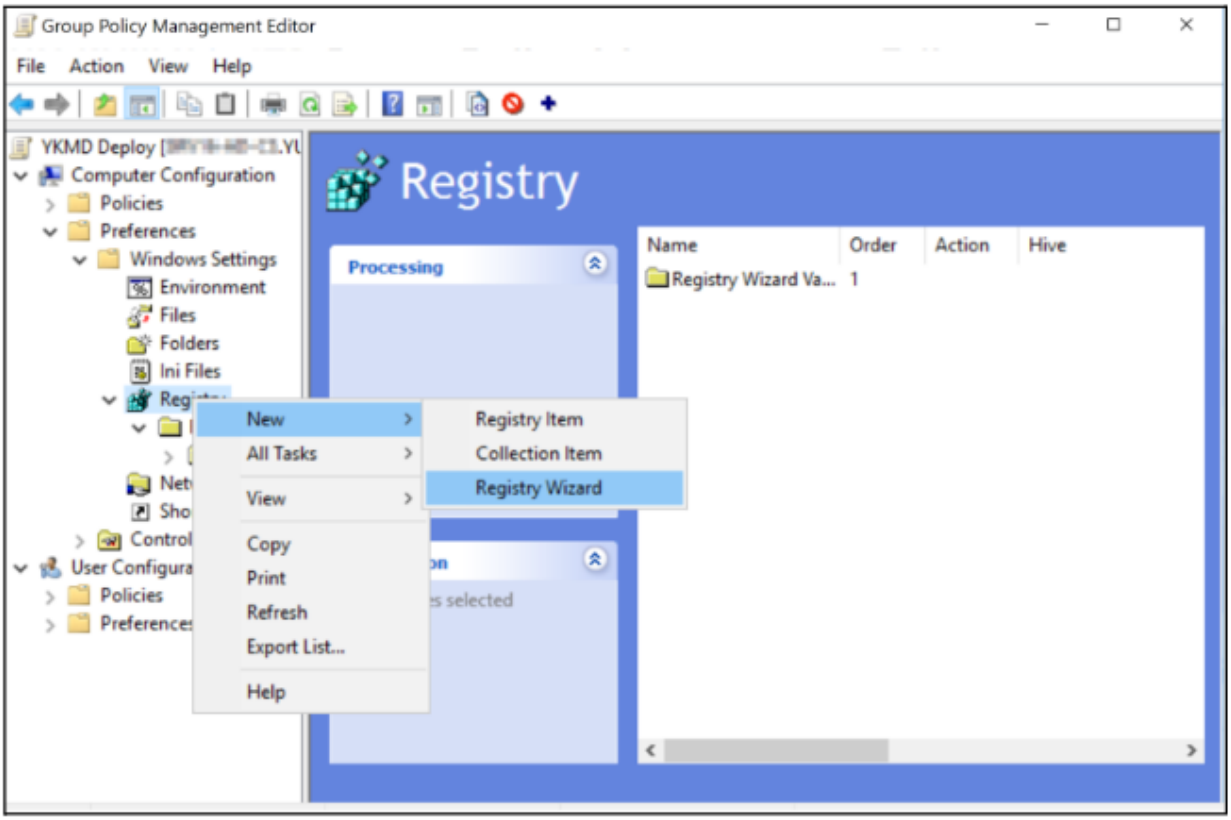
5. Edit this GPO to complete the configuration. Complete the steps in the following sections.

5.5.3 Client Registry Setting

5.5.3.1 Update device path

Update the existing **Device Path** registry setting to reference the newly created driver store.

1. Right-click the new YKMD Deploy GPO and select **Edit**.
2. Expand **Computer Configuration > Preferences > Windows Settings > Registry**.
3. Right-click **Registry** and select **New > Registry Wizard**.



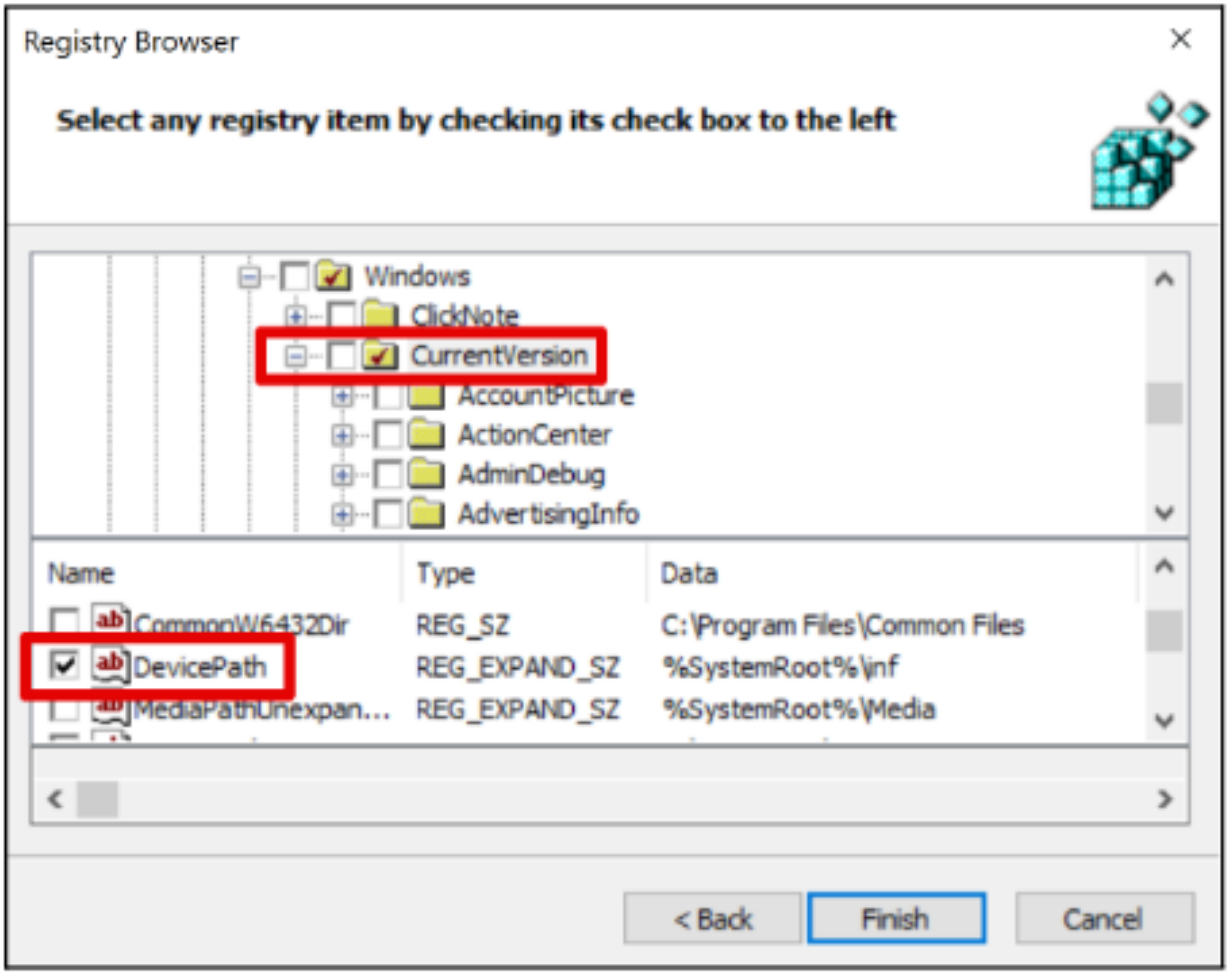
5.5.3.2 Create new Registry

The Registry wizard walks you through creating the new Registry setting for your client machines.

1. When the registry browser comes up, browse to **Another Computer** or use the **Local Computer** since this registry setting should be the same on both. For this example, we are using **Local Computer**.
2. Select **Local Computer**, then click **Next**.
3. Browse to: **HKLM > Software > Microsoft > Windows > CurrentVersion**.
4. From the **CurrentVersion** panel, in the bottom window, scroll down and select **DevicePath**.

   For example:

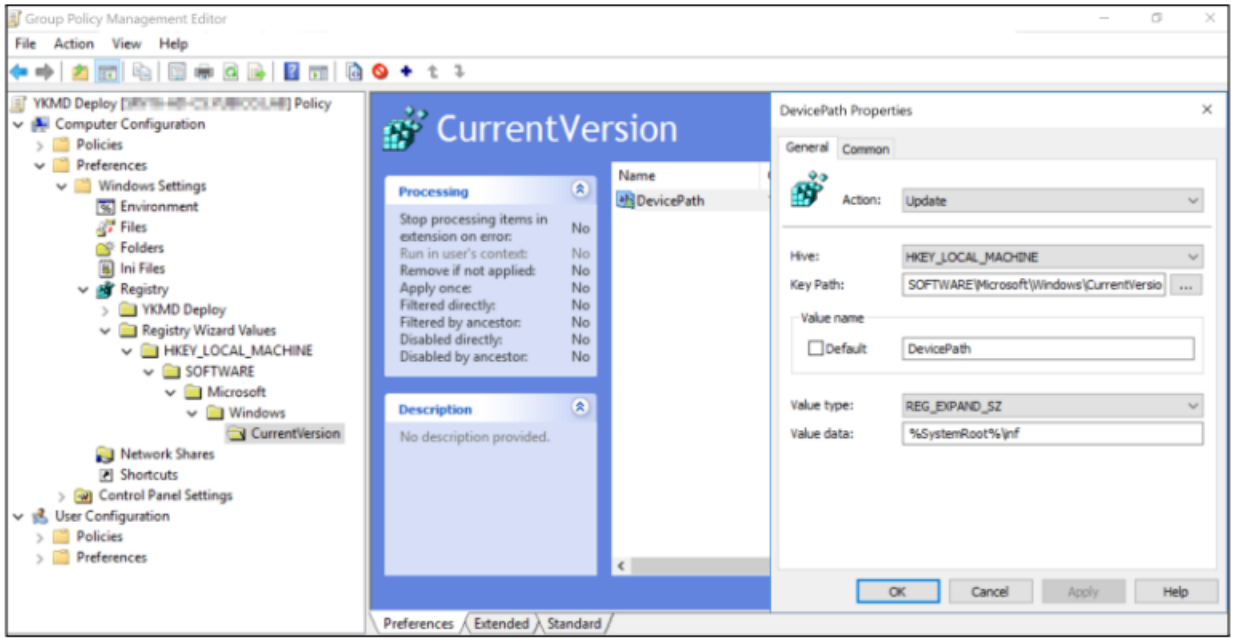
5. Click **Finish**.


Registry Browser
Select any registry item by checking its check box to the left
Windows
ClickNote
CurrentVersion
AccountPicture
ActionCenter
AdminDebug
AdvertisingInfo
Name
Type
Data
CommonW6432Dir
REG_SZ
C:\Program Files\Common Files
DevicePath
REG_EXPAND_SZ
%SystemRoot%\inf
MediaPathUnexpan...
REG_EXPAND_SZ
%SystemRoot%\Media
< Back
Finish
Cancel

5.5.3.3 Update New Registry

Update this new Registry value to append the newly created file share to its search locations. You can append any number of fileshare locations, just separate them with a semicolon.

1. Select the **Registry Wizard Values** created in *Create new Registry* and rename it to something more descriptive. For example, **YKMD Deploy**.
2. Fully expand the new registry value.
3. Double-click the **Device Path** so you can edit the contents.



4. Update the last field, **Value Data**.

   To update, add the following to the existing value:

   ```
   ;\\<servername>\<filepath>\<driverstore>
   ```

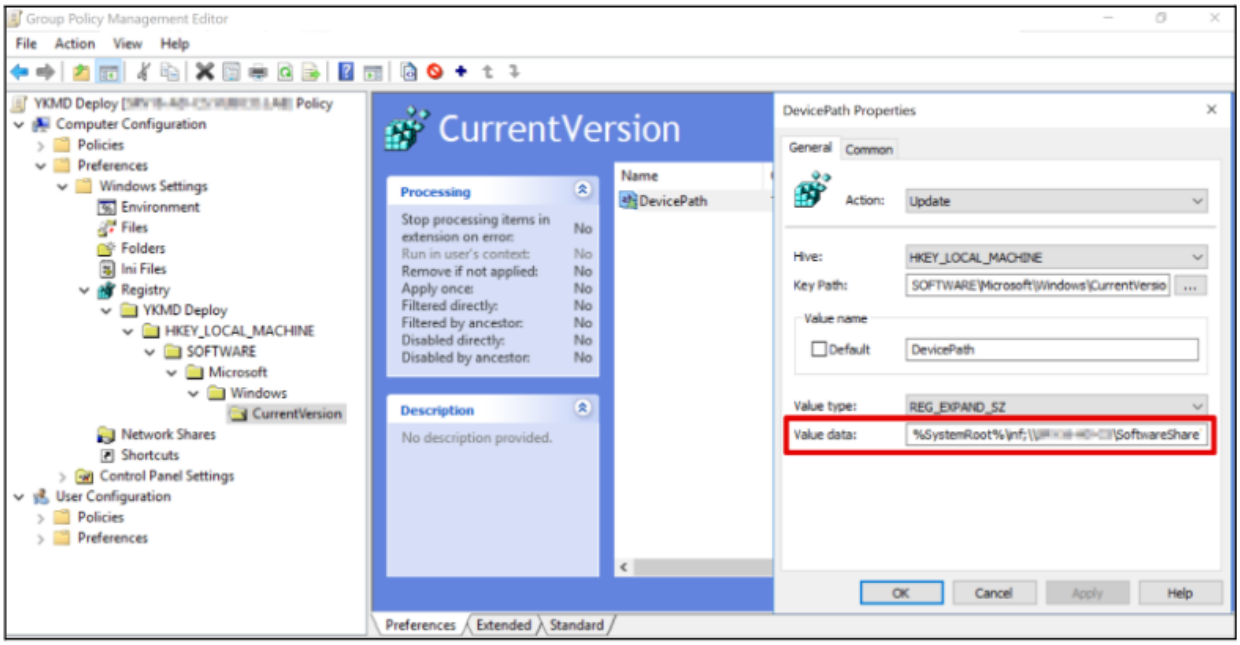
   Note the semicolon at the beginning of the string.

   For example:

   ```
   %SystemRoot%\inf;\\<servername>\SoftwareShare\YKMD
   ```

   The final value should resemble the following:

5. Click **Apply**. Then click **OK** to save your settings.



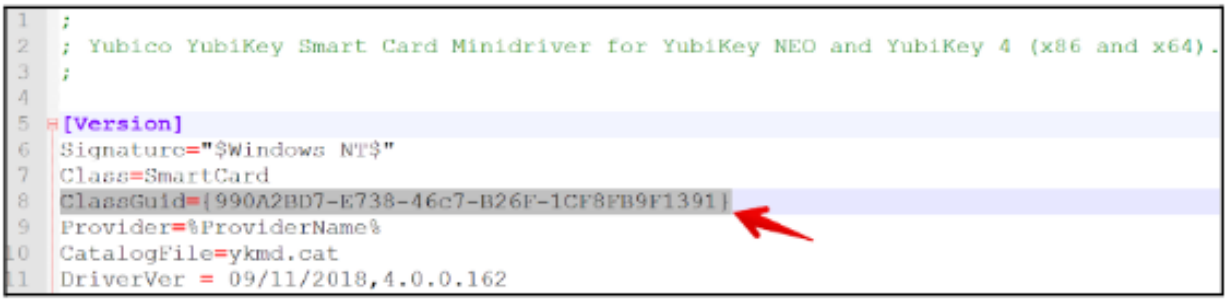
5.5.4 Whitelisting the YKMD GUID

This step allows a silent install that does not require the user to elevate to an admin account.

5.5.4.1 Locate the GUID of YKMD

1. Browse to the extracted contents of the YKMD `.cab` file.
2. Select the file `YKMD.inf`, right-click and open with a text editor.
3. Find the line `ClassGuid=`.

   For example:



4. Copy and paste the full content of that line after the =.

   For example:

   `ClassGuid={990A2BD7-E738-46c7-B26F-1CF8FB9F1391}`

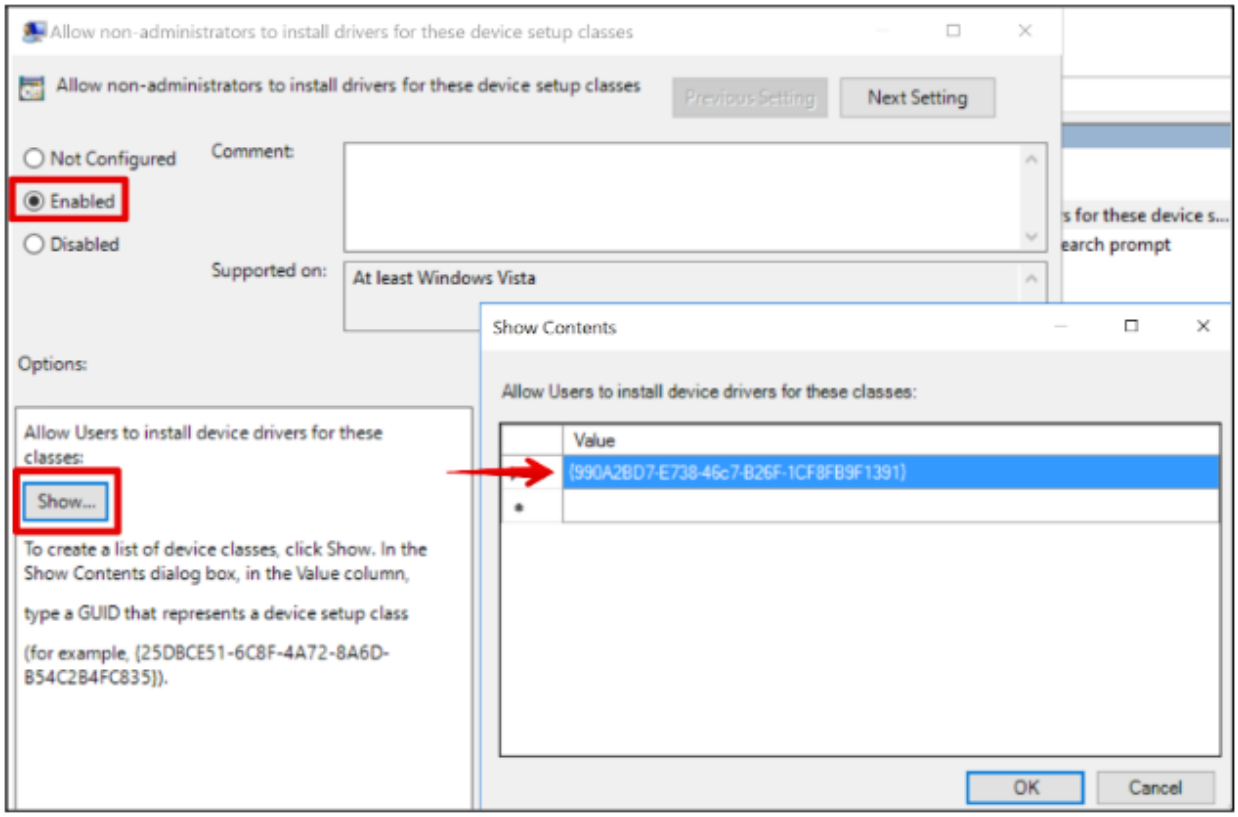
   The GUID: `{990A2BD7-E738-46c7-B26F-1CF8FB9F1391}` brackets included, is what we are whitelisting.

5.5.4.2 Enable and Configure Group Policy

Enable and configure the Group Policy with the updated GUID value:

1. Select the Group Policy **YKMD Deploy** created earlier. See *Configure the GPO*.
2. Browse to: **HKLM > Policies > System > Driver Installation**.
3. Select **Allow non-administrators to install drivers for these device setup classes**.
4. Right-click, and select **Edit**.
    a. Select **Enabled**.
    b. Under Options on the bottom left, select **Show**.
    c. Add the GUID Value from *Locate the GUID of YKMD* into the next open line. If you have not used this before, this is the first line.

       For example:



    d. Select **OK > Apply > OK**.

5.6 Completing the Installation

Confirm the following installation steps are completed.

1. Creation of a network file share to host and distribute YKMD.
2. Download and extraction of YKMD.
3. GPO created and applied to the computer objects which require YKMD.
4. GPO configured based on Method 1 or Method 2 below:

   Method 1
   Push the PowerShell script file to auto-install YKMD.

   Method 2

   a. Client-side registry update.

   b. Whitelist of YKMD GUID for installation by non-admin users.

Important: If any of the above is not completed, review the instructions in this chapter, before proceeding.

5.6.1 Issue a Group Policy Update

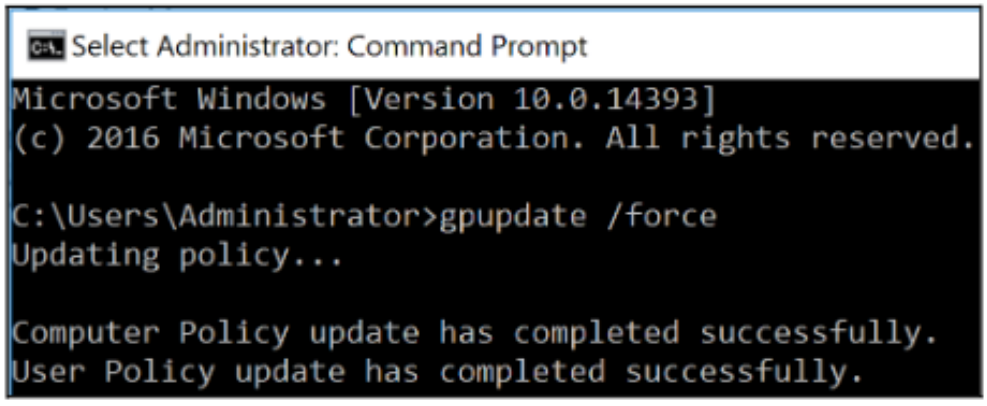
This can be issued as soon as Method 1 or Method 2 tasks are completed. **The version numbers shown are examples**. The actual number changes as YKMD is updated.

1. Refresh the Group Policy for all clients and publish the new changes.

   From the command line, issue the command:

   `gpupdate /force`

   For example:



2. If the client computer does not have YKMD installed:

   Method 1
   The end-user must reboot their computer. YKMD is installed during the next reboot.

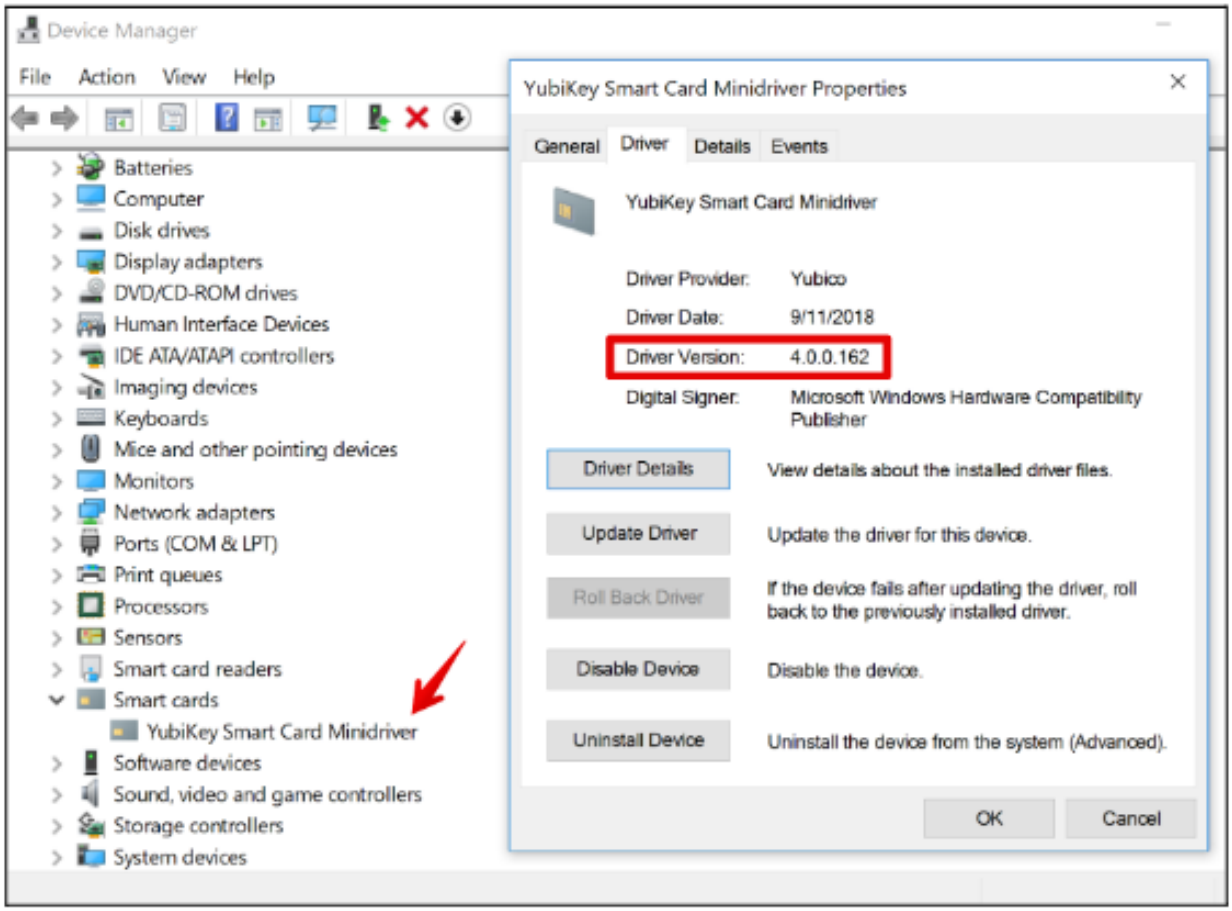
   Method 2
   The end-user updates YKMD through the Device Manager.

   a. Launch the **Device Manager**.

b. Select YKMD.

c. Select **Update > Search automatically for updated driver software**.

3. Confirm YKMD is successfully installed. Open **Device Manager**.



CHAPTER

SIX

VERIFYING INSTALLATION

6.1 Verify Installation Using Powershell

The following is a PowerShell script that can be used to verify proper installation of the YKMD.

Note: Running the script requires elevation.

1. Run the PowerShell command:

```
Get-WindowsDriver -Online
```

2. Enter the ProviderName, ClassName, and Version at the prompts.

```
$_.ProviderName
$_.ClassName
$_.Version
```

Where

- ProviderName, enter `Yubico`
- ClassName, enter `SmartCard`
- Version, enter *

CHAPTER

SEVEN

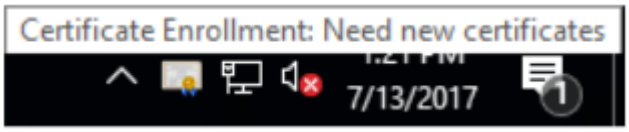
SELF-ENROLLING YUBIKEYS ON WINDOWS

There are two methods for enrolling the YubiKey as a smart card for the Windows environment. This chapter covers the self-enrollment process, where a user enrolls their YubiKey directly to their domain-connected Windows PC. The other method allows for an administrator to enroll a YubiKey to another user directly.

If your environment has been set up to allow auto-enrollment, the process is straightforward. This section describes the steps you need to complete to enroll your YubiKey for Login.

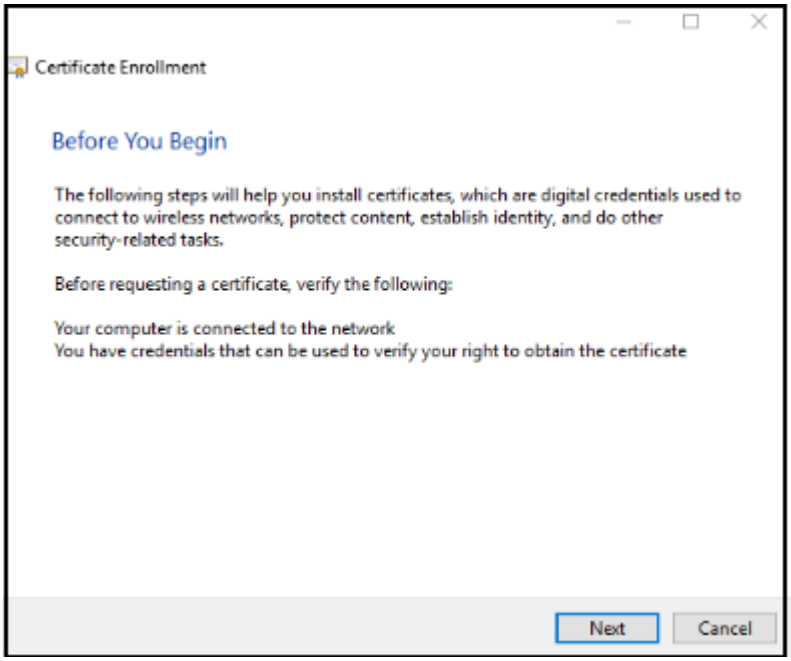
With Auto-Enrollment enabled on the Windows Server and local machines via Group Policy, the end user experience is straightforward.

1. Log into a user account. A Certificate Enrollment popup appears above the System Tray.

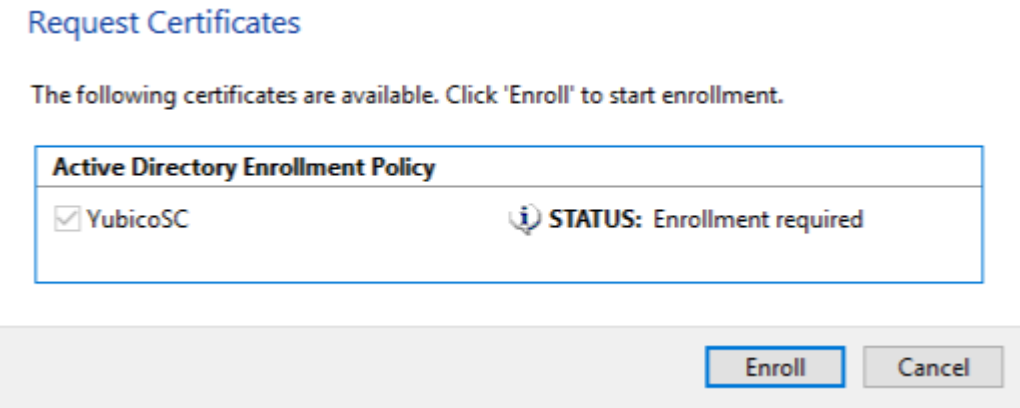


2. Click the Certificate Enrollment popup to open the Certificate Enrollment wizard. If the popup has disappeared (or did not initially appear) click the **arrow** in the System Tray to expand the list of options and click the **certificate** icon.

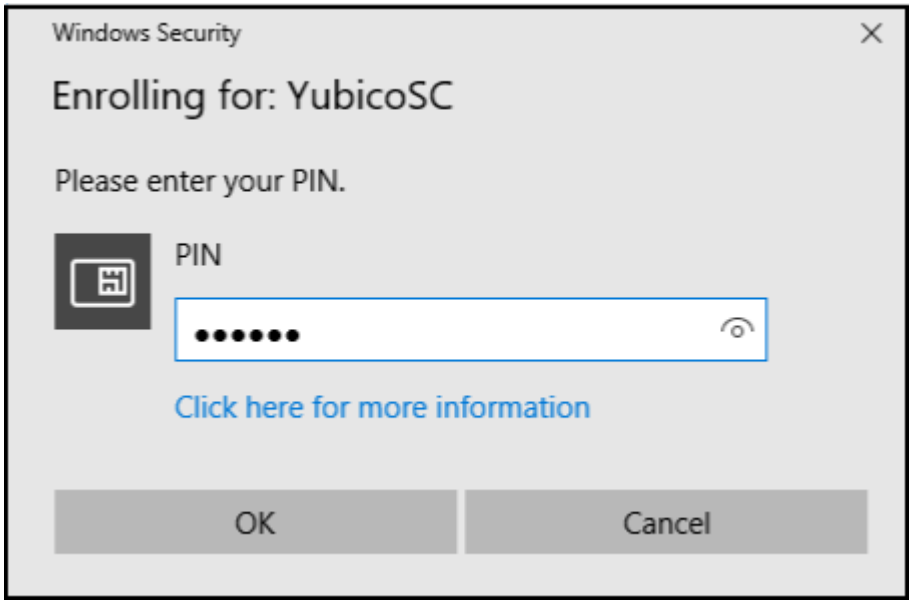
3. On the opening dialog, click **Next**.



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** appears next to the correct template.



5. Enter for PIN for your YubiKey and then click **OK**. If a PIN has not been set, enter the default PIN, `123456`.



6. Windows Auto-Enrolls the YubiKey for Windows Login. The process can take several seconds, depending on the network connection to the server running the Certification Authority. When it is completed, click **Finish**.

CHAPTER

EIGHT

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.

8.1 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
```

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

8.2 Manually Delete Certificates

To delete certificates from a certificate chain manually, including a Base CSP container and associated key and 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>"
```

CHAPTER

NINE

SETTING PIN UNBLOCK CODE (PUK)

When a YubiKey is used with the YubiKey Smart Card Minidriver (YubiKey Minidriver) for the first time, the YubiKey Minidriver checks to ensure that the Management Key and the PIN Unblock Code (PUK) have been changed from the default values.

If they have not been changed from the default value, the YubiKey Minidriver upgrades the Management Key to a protected non-default value and blocks the PUK so that the PIN remains blocked. A blocked PUK prevents the PIN Unblock function from being active.

9.1 Set or Change Smart Card PIN

The steps in this section use the YubiKey Manager (GUI) to enable:

- Setting the smart card PIN during enrollment through the Windows interface.
- Changing the PIN directly through the Windows interface.

1. To prevent the PUK from being blocked, configure the local registry prior to setting up YubiKeys.

   Key
   `HKLM\\Software\\Yubico\\ykmd`

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

2. The YubiKey Minidriver supports unlocking a blocked PIN using the built-in Windows UI. To enable this function, 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

3. For the PUK to remain unblocked, use either the YubiKey Manager, the Yubico PIV Tool, or Yubico Authenticator to set a non-default PUK prior to using the Windows interface to load or access certificates stored on the YubiKey.

   When the YubiKey Minidriver first accesses the YubiKey, it checks if the PUK is set to the default value. For PUKs with user supplied values, this causes the retry counter to decrement by one. This can be reset by entering the correct PUK via the Windows interface, but requires changing the PIV PIN.

4. Setting the PUK can be accomplished in YubiKey Manager by navigating to:

   Applications > PIV > Configure PINs > Change PUK

To use the command-line version of YubiKey Manager (ykman), see the *YubiKey Manager (ykman) CLI and GUI Guide*, section ykman piv access change-puk.

To manage the FIDO2 PIN, see the Yubico Authenticator User Guide, section PIN Protection.

To use Yubico PIV tool, refer to the documentation on Yubico PIV Tool.

9.2 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: You cannot create a PUK with the YubiKey Minidriver.

To create a PUK for a YubiKey, follow the instructions for *Setting PIN Unblock Code (PUK)* using either the YubiKey Manager, the Yubico PIV Tool, or Yubico Authenticator.

If you do not create a PUK and you forget your PIN, recovery requires that you reset the device. Resetting the device:

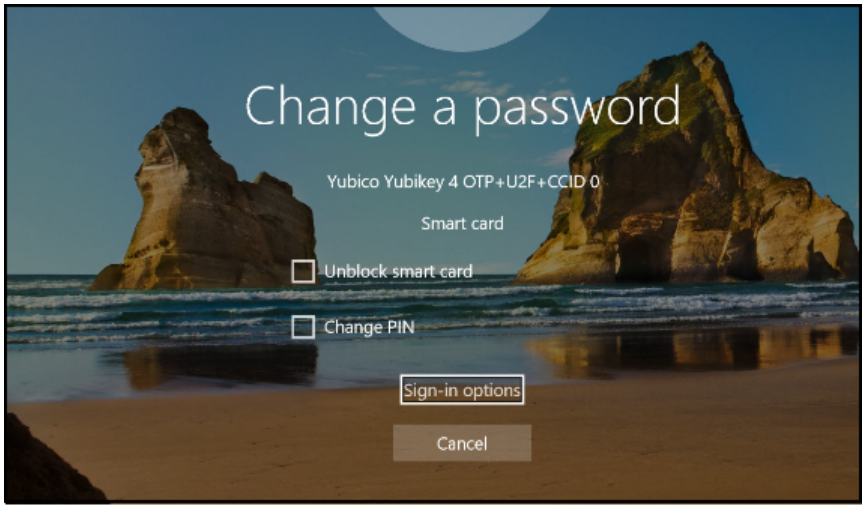
- Permanently deletes all private keys and certificates.
- Requires new certificates and private keys!

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. To use the PUK, the administrator must have the PUK enabled when the key and certificate were loaded on the YubiKey. If both the PIN and the PUK are blocked, the YubiKey must be reset, which deletes any loaded certificates and returns the PIN and PUK to default values (`123456` and `12345678`, respectively).

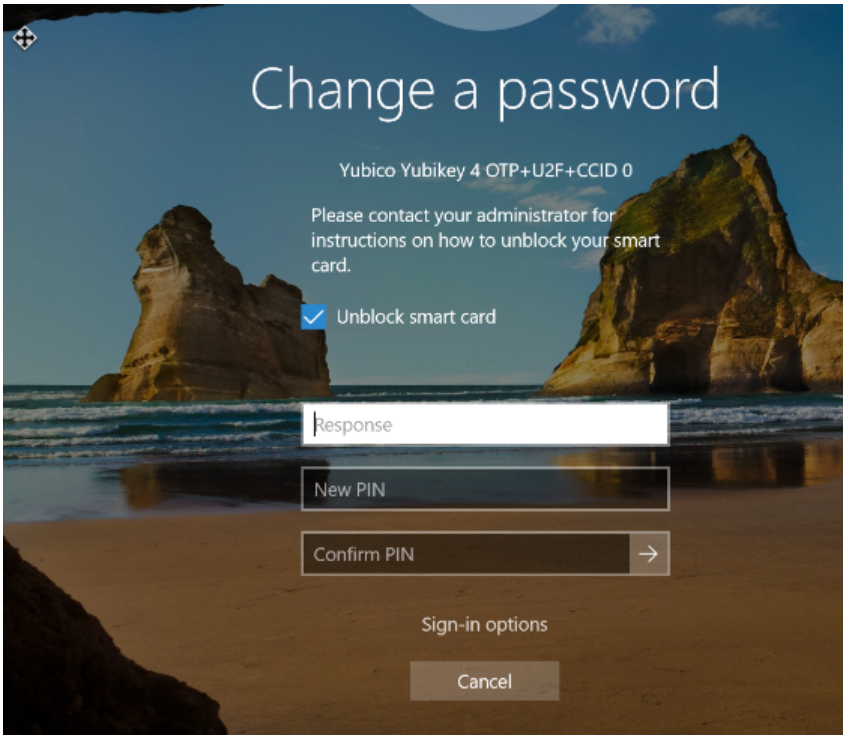
Note: Both Windows Server 2008 and Windows Server 2008 R2 require the PIN unblock code (PUK) to be typed in as hexidecimal digits. This means that if your PUK is `12345678`, to unlock a pin through the Windows UI, you must type the ASCII hex-encoded bytes of the PUK string (in this case, the unlock code would be `3132333435363738`). Refer to an ASCII chart (for example, www.asciitable.com) to encode a PUK in hexidecimal. This does not apply to later versions of Windows.

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 following screen appears (example in Windows 10).



2. Check the checkbox next to **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`.
4. In the **New PIN** and **Confirm PIN** fields, enter a new, properly formatted PIN, and then press **Enter**.
5. Remove the YubiKey, reinsert, and test the new PIN to confirm you can access the account.

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

Computer Configuration > Administrative Templates > Windows Components > Smart Card

CHAPTER

TEN

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 Smart Card Minidriver (YubiKey Minidriver) sets the touch policy when a key is first imported or generated. Once set for a key on the YubiKey, the policies cannot be changed.

Note: The touch policy setting can influence the user experience. Consider the potential impacts before adjusting this configuration.

10.1 Set Policy for Touch to Allow Private Key Use

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.

By default, the touch policy for keys imported/generated through the YubiKey Minidriver, is created with the touch policy default setting: `disabled`.

10.2 Touch Policy Options

To alter the policy behavior, configure the registry 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 YubiKey Minidriver. Accepted values are:

- `1 <Never>` - (No touch required) 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>` - (for 15 seconds per touch) 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.

Note: Due to OS limitations, there is no visual prompt on the screen when touch is required in this scenario. Microsoft's minidriver specification that YubiKey Minidriver is based off of has no concept of touch requirement.

Change the default through a Windows registry entry and apply it to all new certificate and private key pairs added to the YubiKey. If different policies are required per certificate, change the registry entry prior to creating each certificate.

CHAPTER

ELEVEN

CONFIGURE THE MINIDRIVER REGISTRY

The YubiKey Smart Card Minidriver can be configured for non-default behavior through the registry keys.

To configure the YubiKey Minidriver registry entries:

1. As administrator, open the Registry Editor.
2. Create the key: `HKEY_LOCAL_MACHINE\SOFTWARE\Yubico\ykmd`.
3. Refer to the table below to add key value(s) as applicable.
4. Close the registry editor and reboot the machine.

11.1 YubiKey Minidriver Registry Key Reference

Important: Always thoroughly test configuration prior to implementation. Furthermore, to mitigate risks, we recommend that all testing be conducted in a controlled test environment. Finally, note that unless you use the latest version, not all of the settings are necessarily available in your YubiKey Minidriver. You should therefore use the latest version.

Value	Type	Data	Description
AutoFingerprint	DWORD	1 (0)	Controls the biometric authentication dialog for the YubiKey Bio Multi-protocol Edition. Default `1`. The YubiKey Minidriver immediately asks for fingerprint verification if a fingerprint is enrolled on the device AND is not blocked.
BlockPUKOnMGMUpgrade	DWORD	0 (1)	Controls availability of PUK when the YubiKey is configured with known values. Default `1`. The YubiKey Minidriver restricts PUK access when the YubiKey value, is at factory value, `12345678`. Set to `0`, the PUK functionality is not restricted, regardless if the YubiKey factory value is unchanged. Note: Allowing unblock (PUK) with a known factory value can be a concern.

continues on next page

Table 1 – continued from previous page

Value	Type	Data	Description
DebugOn	DWORD	0 (1)	(Optional) Activates creating a debug log. To enable, set value to `1`. The registry key value triggers generating a debug log major security that is saved to: `C:\Logs`
DebugVerbosity	DWORD	0 (1-3)	Applies only when DebugOn is non-zero. Sets logging level used by the YubiKey Minidriver and its dependencies. Valid values are (0) - none to (3) - APDU level verbosity.
ExternalPinCache Policy	DWORD	2 (1-4)	This setting overrides the *PIN_CACHE_POLICY_TYPE* ` for the external PIN_ID in the YubiKey Minidriver. This setting controls how the YUbiKey Bio PIN (fingerprint) is cached. Default is 0 (PinCacheNormal). This key accepts any valid `PIN_CACHE_POLICY_TYPE` numeric value. See https: //learn.microsoft.com/en-us/windows-hardware/drivers/smartcard/ card-pin-operations#-pin_cache_policy_type for more information.
ManageCSPCache	DWORD	1 (0)	Determines if by clearing its cached data, the container map synchronization check compels the BaseCSP to retrieve the container map and certificate details from the YubiKey Minidriver. When disabled, `0`, this feature prevents certain card modifications from being reflected in the BaseCSP. Note: Deactivating, `0`, this feature can enhance the certificate enumeration performance.
NewKeyTouch Policy	DWORD	1 (2,3)	Enables the touch policy for PIV. Setting is optional. Default `1`, touch input is not mandatory for PIV operations. Set to `2`, touch input is enforced at all times (similar to FIDO2). Set to `3`, touch input activated, with cache touch input for a limited duration with less frequent requirements. Note: While improving security, configuring touch for PIV may have an adverse effect on usability. Note also that this configuration does not impact already configured YubiKeys (the setting must be present at the time of enrollment).
PinCacheTimeout	DWORD	60	If either `UserPinCachePolicy` or `ExternalPinCachePolicy` is set to 'timed' (1), this setting sets the number of seconds for which the BaseCSP caches the PIN. This is only a recommendation to the BaseCSP and is not implemented by the Minidriver.

continues on next page

Table 1 – continued from previous page

Value	Type	Data	Description
ProtectManagement	DWORD	1 (0)	Governs the creation and storage of the PIV card management key within a secure object to enable write access for PIV functionality. Default 1. The YubiKey Minidriver generates a new card management key and stores it in a PIN-protected object (in the YubiKey PIV application) when the factory value is present during PIN entry (such as during enrollment). Set to 0. Disables feature. Third party solutions (such as CMS products), while managing YubiKeys may optionally disable this setting and assume ownership of this feature and dependant processes (suchas enrollment).
RefreshDeviceKeys	DWORD	1 (0)	Controls the behavior of container map synchronization that happens based on the timeout defined by RefreshWindow. Default, 1, The YubiKey Minidriver (YKMD) checks that the container map stored in the mscmap PIV object matches the container map in the SCardCache. Additionally, the YKMD enumerates all keys and certificates in the PIV application the and then updates map accordingly. Set to 0, disables feature. This can improve performance, especially over RDP. However, certificates enrolled outside of the YubiKey Minidriver might not be present in the container map as reported to theBaseCSP(!)
RefreshWindow	DWORD	300	Sets the time interval (in seconds) for how often the YubiKey Minidriver (YKMD) synchronizes the container map reported to the BaseCSP. By default the YubiKey Minidriver (YKMD) performs synchronization when the time difference between the last call from the BaseCSP and current time exceeds 300 seconds. During synchronization the YKMD: 1. Clears the BaseCSP cache (depending on setting of ManageCSPCache). 2. Enumerates the certificates and keys in the PIV application (depending on setting of RefreshDeviceKeys). 3. Ensures the currently cached container map contains the same information as the on-card container map and the list of newly enumerated certificates. Note: Setting a higher value than default may have a positive impact on performance without using the heavier-handed settings of RefreshDeviceKeys and ManageCSPCache

continues on next page

Table 1 – continued from previous page

Value	Type	Data	Description
SupportAlwaysPin	DWORD	1 (0)	Enables and disables support for the `Always Prompt PIN_ID` in the YubiKey Minidriver. The `Always Prompt PIN_ID`, `PIN_CACHE_POLICY_TYPE` is set to `PinCacheAlwaysPrompt` and is assigned as the PIN for key containers that map to PIV slots that have the `PIN_ALWAYS` pin policy in the YubiKey PIV application (such as, slot 9c) in devices that support slot metadata (YubiKey 5.2.7+).
UserPinCache Policy	DWORD	0 (1-4)	This setting overrides the `PIN_CACHE_POLICY_TYPE` for the user PIN_ID in the YubiKey Minidriver. Default is 0 (PinCacheNormal). This key accepts any valid `PIN_CACHE_POLICY_TYPE` numeric value. See https://learn.microsoft.com/en-us/windows-hardware/drivers/smartcard/card-pin-operations#-pin_cache_policy_type for more information.

CHAPTER

TWELVE

LOGGING MINIDRIVER BEHAVIOR

Should errors occur in the use of the YubiKey as a PIV Smart Card with YKMD, error logging can be enabled on the local computer using the registry. Once enabled, log files are created per running process in `C:\Logs`. See Smart Card Basic Troubleshooting for additional troubleshooting steps.

- Key: `HKEY_LOCAL_MACHINE\SOFTWARE\Yubico\ykmd`
- Value: `DebugOn` (DWORD) - `1` enables error logging.

Note: Refer to *Configure the Minidriver Registry* for additional registry settings.

CHAPTER

THIRTEEN

UNINSTALL THE YUBIKEY MINIDRIVER

13.1 YubiKey Minidriver Installed using MSI

If the YubiKey Smart Card Mindriver (YubiKey Minidriver) was installed using the MSI, Yubico recommends using the Program and Features Interface to remove it.

1. Use **Windows+R** to display the run terminal window, enter `appwiz.cpl` and click **OK**.
2. The Programs and Features window opens. Scroll down and locate the entry for the **YubiKey Smart Card Minidriver**.
3. Right click on the YubiKey Minidriver entry and select **Uninstall**.

13.2 Manual Uninstall

Manual install is run in a terminal.

1. Open **Command Prompt as Administrator** or **PowerShell as Admin**.
2. Run: `%windir%\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. If multiple versions of the YubiKey Minidriver have been installed, each has its own separate directory. Repeat this and the following steps for each installation directory.
5. Type the following command and press **Enter**:

```
rundll32 setupapi.dll,InstallHinfSection DefaultUninstall 4 .\\ykmd.inf
```

6. If you want to also delete the driver and other related files from your computer:

   Delete the entire YubiKey Minidriver directory in `%windir%\System32\DriverStore\FileRepository\`

   From the example in step 3, the directory name is `ykmd.inf_amd64_1e4c7d5bdb6914f9`.

   To do delete the driver and related files:

   a. The Admin needs to take ownership of the directory use the `takeown` command. For example, using the directory from step 3, the command is:

```
TAKEOWN /F ykmd.inf_amd64_1e4c7d5bdb6914f9 /R /A
```

b. Following taking ownership of the directory, grant full control access to the directory and the files within with the `icalcs` command.

   For example, using the directory from step 3, the command is:

```
ICACLS ykmd.inf_amd64_1e4c7d5bdb6914f9 /grant Administrator:F /T
```

c. After the ownership and access is set, the files can be deleted as normal.

13.3 Preventing Reinstallation after Removal

To prevent the YubiKey Minidriver from being reinstalled after removal, blocked it via the Windows Group Policy.

These are steps for Windows 10. Steps for Windows 11 are slightly different.

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 **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**.

   The `SCFILTER\CID_ID#` value for the YubiKey is displayed. Note that YubiKey 4, YubiKey 5, and YubiKey NEO have different hardware IDs.
10. Click **OK**.

CHAPTER

FOURTEEN

COPYRIGHT

14.1 Trademarks

Yubico and YubiKey are registered trademarks of Yubico AB. All other trademarks are the property of their respective owners.

14.2 Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

14.3 Contact Information

Yubico AB
Gävlegatan 22
113 30 Stockholm
Sweden

More options for getting touch with us are available on the Contact page of Yubico's website.

14.4 Document Updated

2025-05-14 23:30:11 UTC