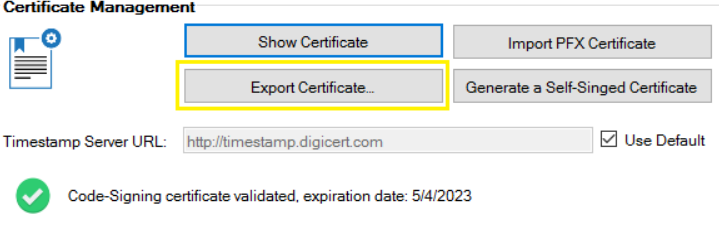# Certificate and GPO Deployment Guide

Document Versions:

Date	Version	Description
September, 30, 2018	1.0	Initial Release

|	
Certificate Management Show Certificate Import PFX Certificate Export Certificate... Generate a Self-Singed Certificate Timestamp Server URL: http://timestamp.digicert.com ☑ Use Default ✅ Code-Signing certificate validated, expiration date: 5/4/2023	For clients to **install third-party updates**, they must **trust** the **code-signing certificate**. **Click** the "**Export Certificate…**" button to export the certificate to a (**.CER**) file.
Save As ✕ ← → ∨ ↑ 🖳 > This PC > Desktop ∨ ↻ Search Desktop 🔍 Organize ▼ New folder 🖥 This PC Name Date modified Type 🖥 Desktop 📁 Client Logs 4/5/2018 9:03 PM Shortcut 📄 Documents 📁 Server Logs 1/11/2017 7:03 AM Shortcut ⬇ Downloads ♪ Music File name: PatchMyPC-CodeSigningCertificate Save as type: Certificates (*.cer) ∧ Hide Folders Save Cancel	In the "**Save As**" dialog, give your certificate a name and click the Save button.
Certificate Export Successful ✕ ℹ The certificate has been exported. Please ensure this certificate is added to the "Trusted Root Certification Authorities" and "Trusted Publishers" certificate store on clients. You can learn more at https://patchmypc.net/documentation OK	Click **OK** on the **Certificate Export Successful** dialog.
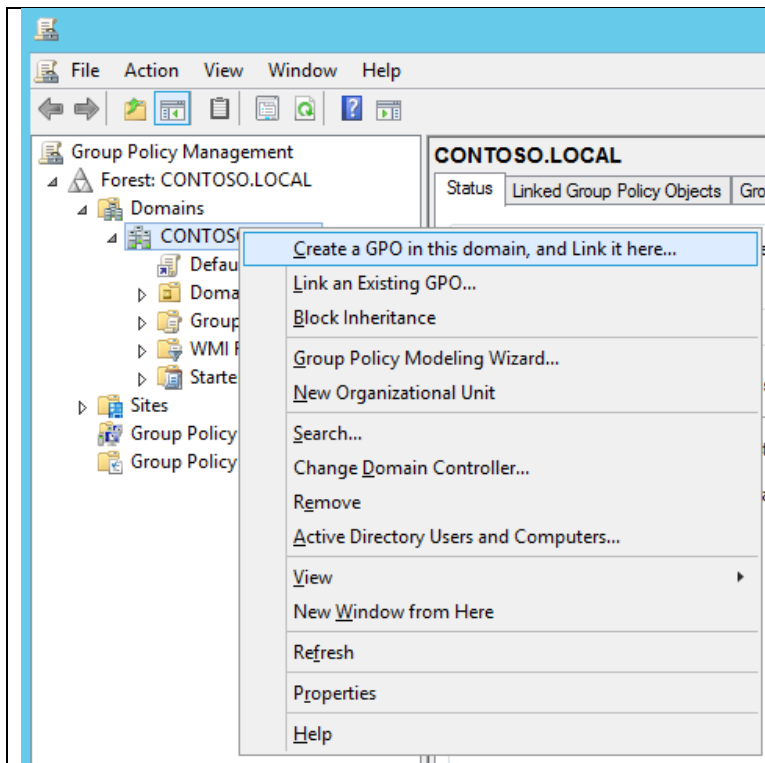
Next, we will **distribute** the **exported certificate** to clients to ensure **they trust updates** published using the **code-signing certificate exported**.

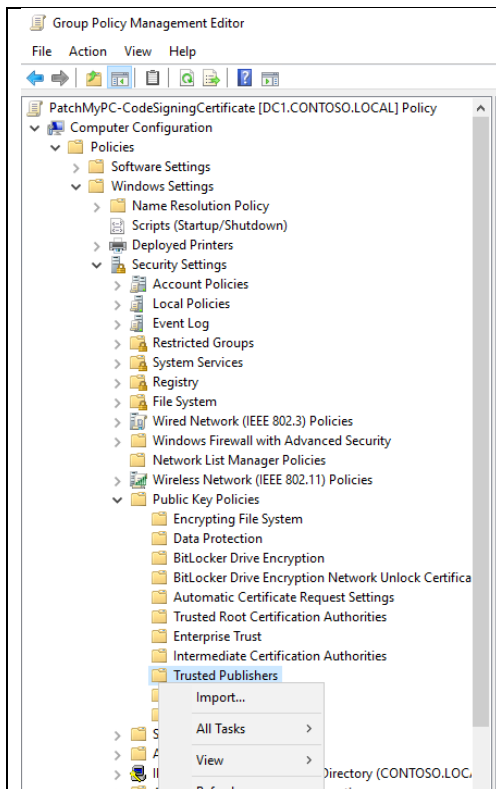You can either **create** a new GPO or **edit** an existing GPO.

To create a new GPO, **right-click** the Domain and choose "**Create a GPO in this domain, and Link it here….**".
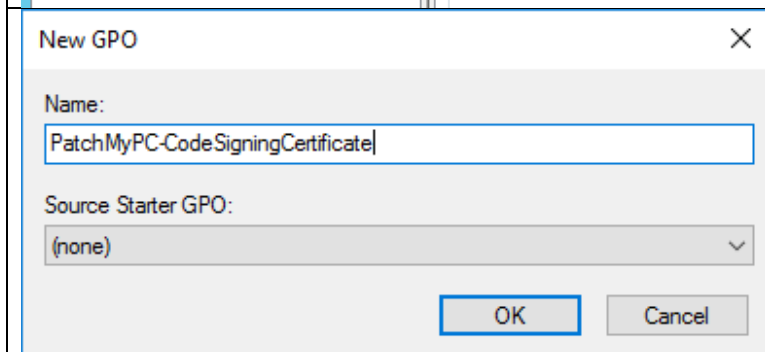
If you **choose** to create a **new GPO**, give it a name and click **OK**
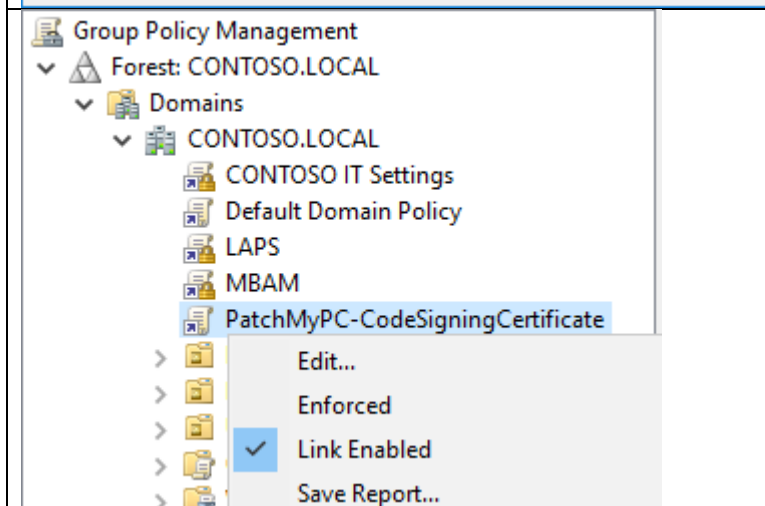
Right-click the newly created GPO or the existing GPO and click **Edit…**
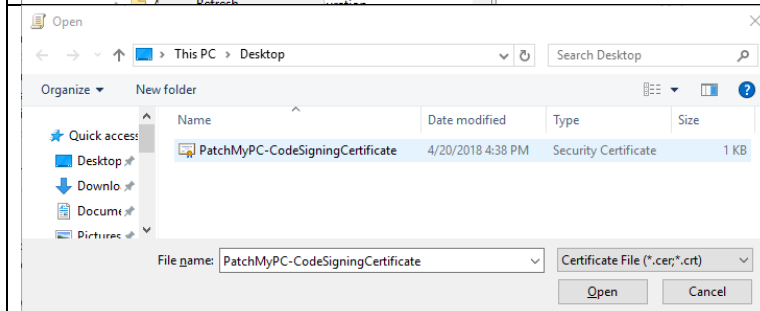
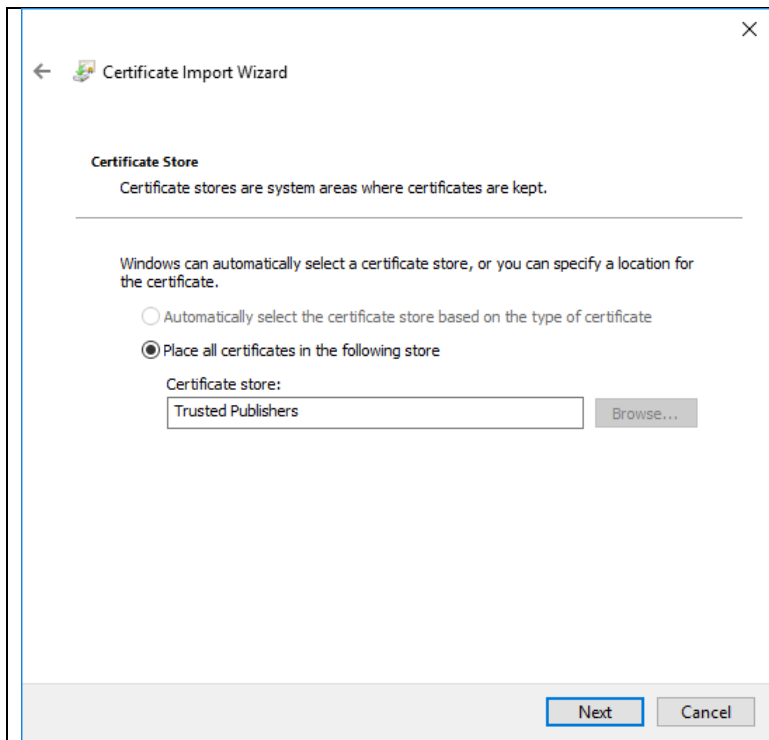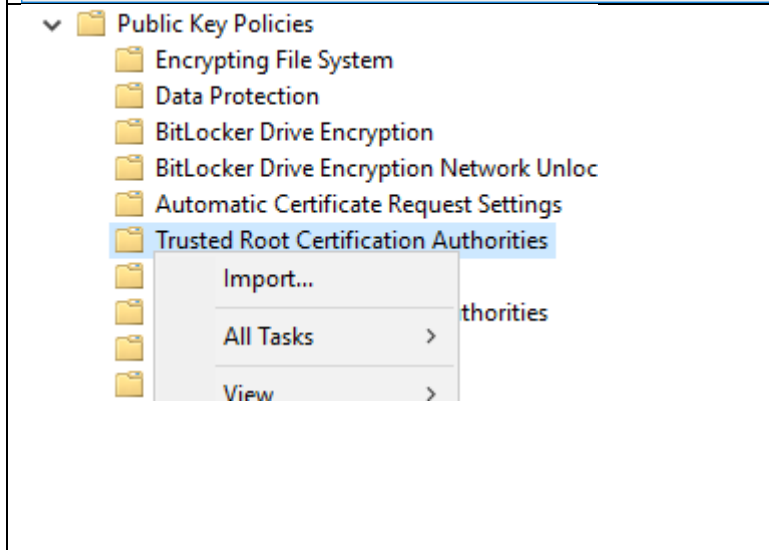|	
	In the "**Group Policy Management Editor**" navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**. Right Click "**Trusted Publishers**" and Click **Import** Click **Next** on the "**Welcome to the Certificate Import Wizard**" Click **Browse** in the "**Certificate Import Wizard**"
	In the **Open** dialog, select the **.CER** file that was **exported** and click **Open**

|	
Certificate Import Wizard screenshot showing the Certificate Store step with "Place all certificates in the following store" selected and "Trusted Publishers" in the Certificate store field	Click **Next** on the "**Certificate Import Wizard**" then click Finish on the "**Completing the Certificate Import Wizard**" Click **OK** on the "The import was successful." **MessageBox**.
Public Key Policies tree showing Encrypting File System, Data Protection, BitLocker Drive Encryption, BitLocker Drive Encryption Network Unloc, Automatic Certificate Request Settings, Trusted Root Certification Authorities with context menu showing Import..., All Tasks, View	If you used a **self-signed** certificate, you *MUST* also import the **exported .CER file** to the "**Trusted Root Certificate Authorities**" certificate store in **addition** to the "**Trusted Publishers**" **Right-click** the "**Trusted Root Certificate Authorities**" and click **Import…** and **repeat** the same steps used to import the .CER file into the "**Trusted Publishers**" certificate store.
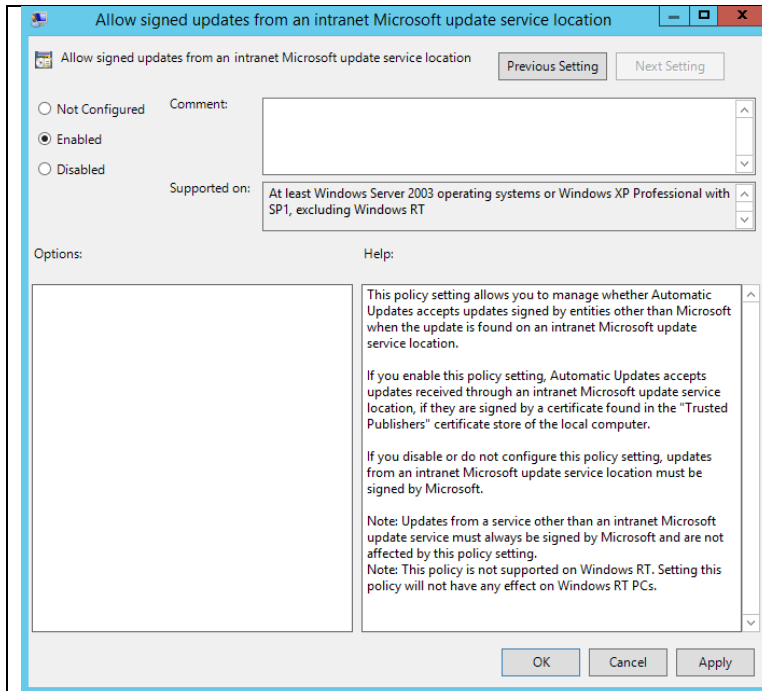
Within the same group policy object, Navigate to **Computer Configuration > Administrative Templates > Windows Components > Windows Update.**

Click the "**Allow signed updates from an intranet Microsoft update service location**" policy.

Click "**Enabled**".

Click the **OK** Button.

This **policy is required** by clients to **allow** third-party updates to be **installed**.
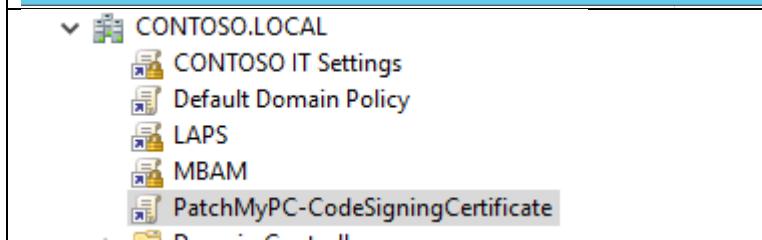
We have now **completed** the **certificate** and **Group Policy pre-requisites** for publishing updates on the **server** and **client** side.