GYTPOL Validator

Client Deploy via GPO using Task Scheduler

Doc: GYT-TEC-009
Release: 02
Date: 28th June 2022

Total pages:	9

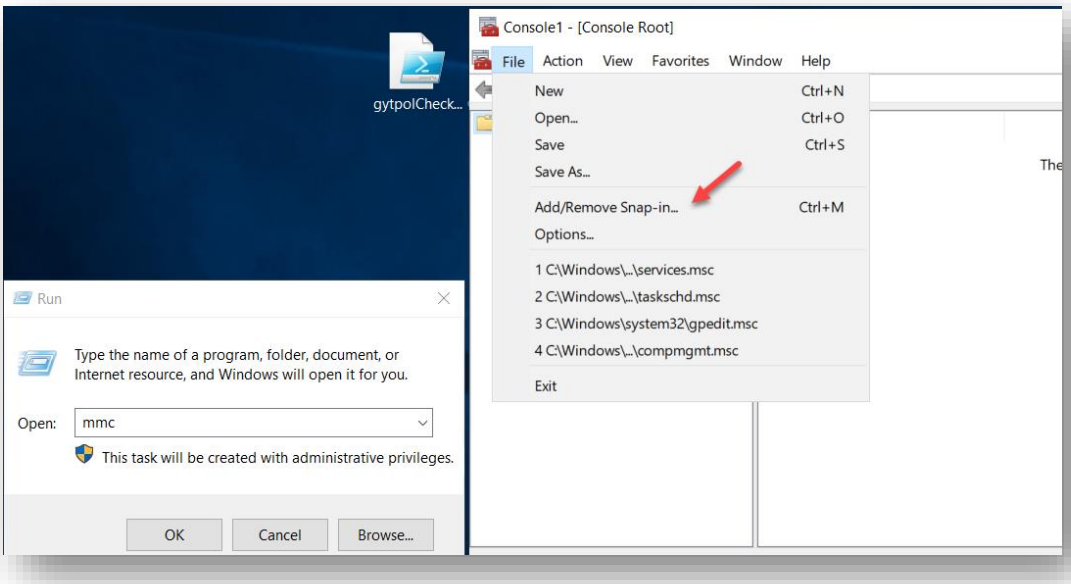
Doc. Title:	GYTPOL Validator Client Deploy via GPO using Task Scheduler

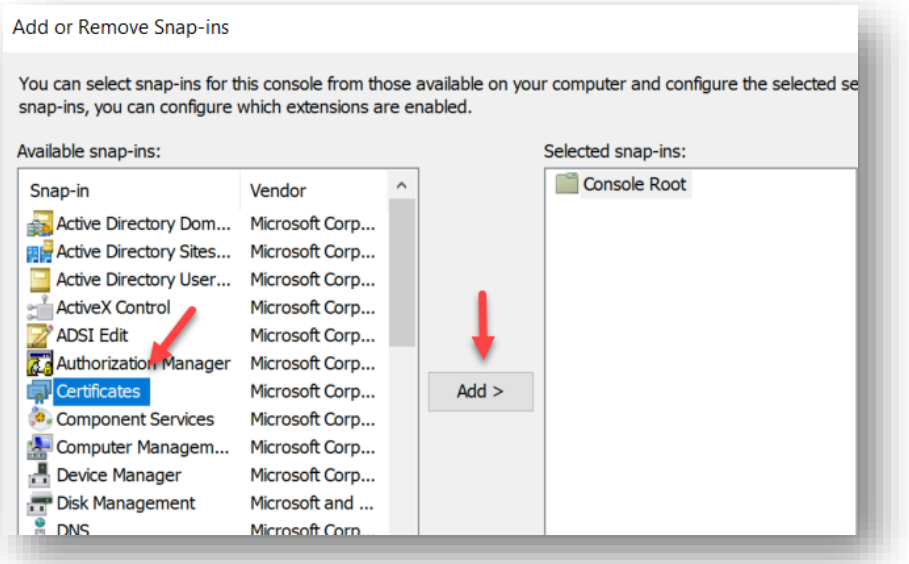
Doc. No.:	GYT-TEC-009	**Classification:**	Confidential
Revision:	02	**Restriction:**	GYTPOL and approved recipients
Date:	28th June 2022	**Customer:**	

Owner:	Mark Zuk	**Reviewers/ Approvers:**	Matthew Album Gilad Raz Tal Kollender
Author:	Mark Zuk		

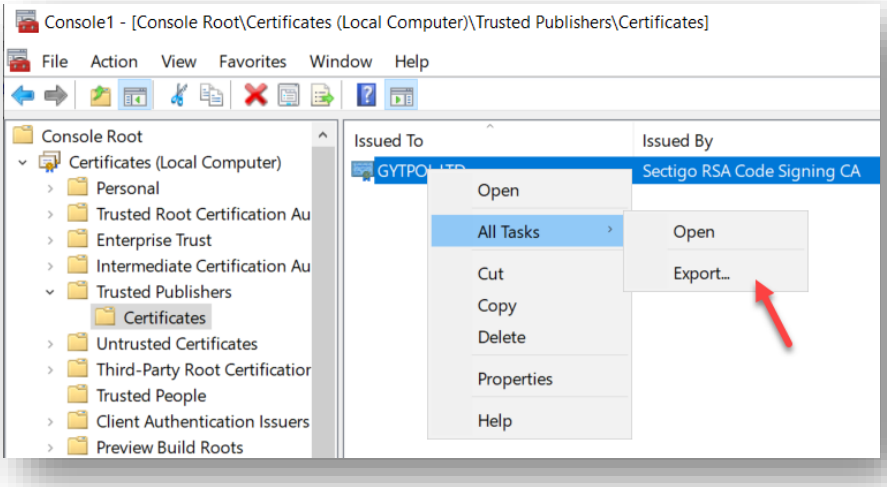
Export GYTPOL certificate

1. Install gytpolClient_x64.msi manually from an elevated CMD.
    a. Please follow this user guide to see manual installation steps.
2. Once GYTPOL client is installed, please open **mmc** from Run and add **Certificates Snap-in** using the file menu.





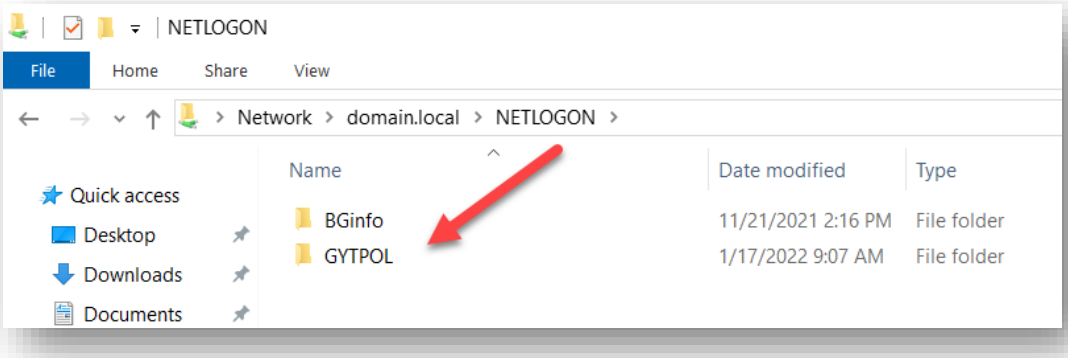
3. When you click Add > → choose Computer Account and click Next.
4. Choose Local Computer and click Finish.
5. Click OK on the Add or Remove Snap-ins window.
6. In the Certificates console, browse to Trusted Publishers → Certificates and look for GYTPOL LTD.
7. Right click GYTPOL LTD → All Tasks → Export



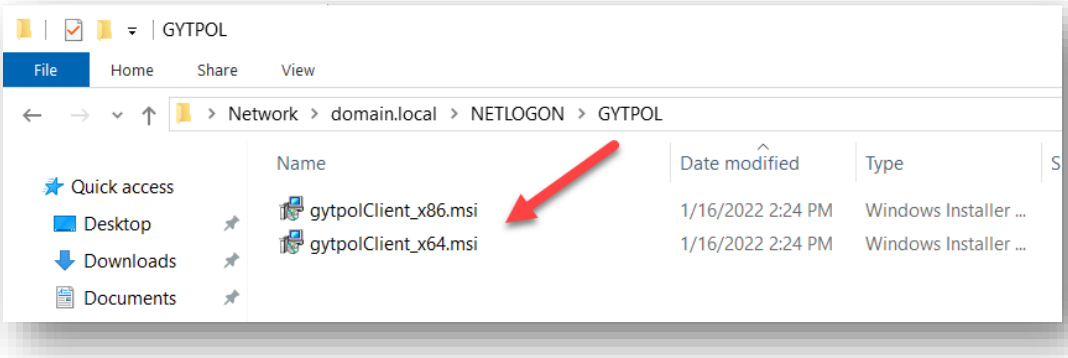
8. Follow the Export Wizard with its defaults and save the file somewhere in your network. We will import it to our GPO created in the next steps, so keep in mind it should be accessible to your Domain Controller.

Creating the GPO

1. Create a folder named **gytpol** under your domains NETLOGON folder.
   - Replace *domain.local* with your domain name

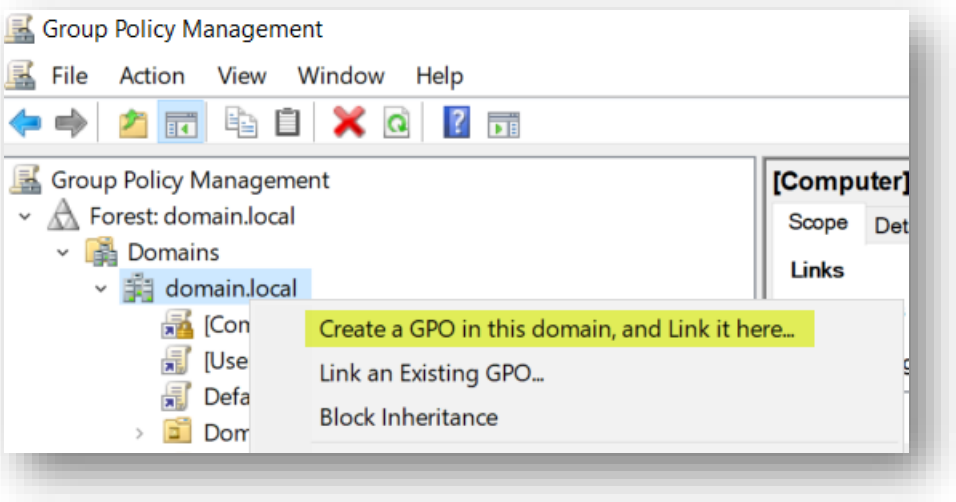


2. Copy the **MSI files only** from GYTPOLs Client zip file into that folder

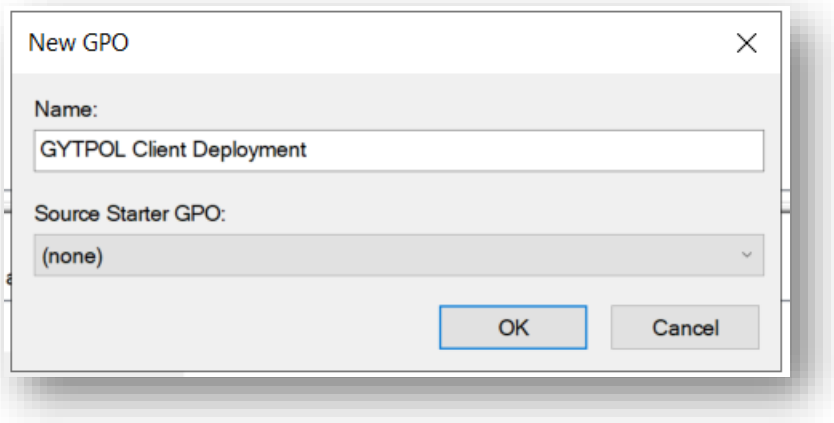


3. Copy the **gytpolClient_GPO.ps1** script sent you by the GYTPOL team under that folder (if not sent, please contact **support@gytpol.com**)

4. Go to your Group Policy Management Console (GPMC) → Forest → Domains → *yourDomainName* → Right click and select "**Create a GPO in this domain, and link it here…**"

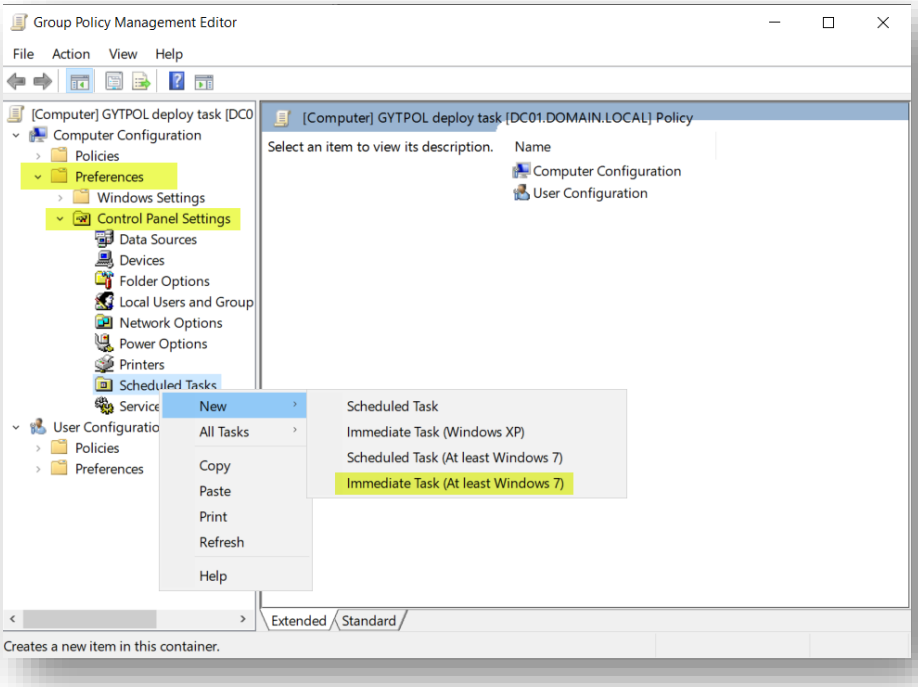


5. Name the GPO as ***GYTPOL Client Deployment*** (or any relevant name) → OK



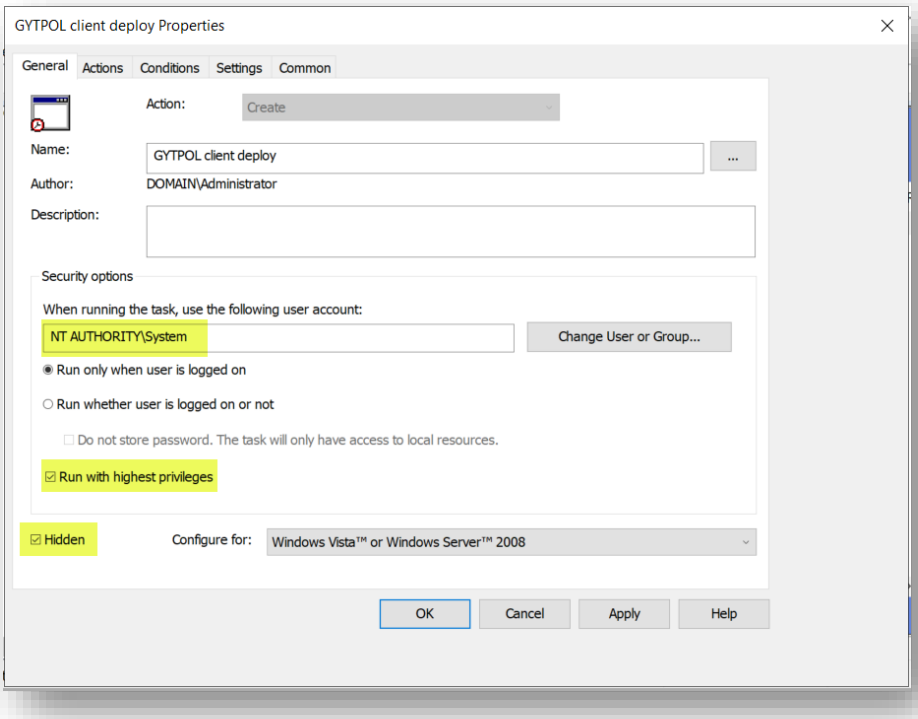
6. Right click the policy you created → Edit

7. Go to **Computer Configuration → Preferences → Control Panel Settings → Scheduled Tasks → New → Immediate Task (At least Windows 7)**



Task Properties:

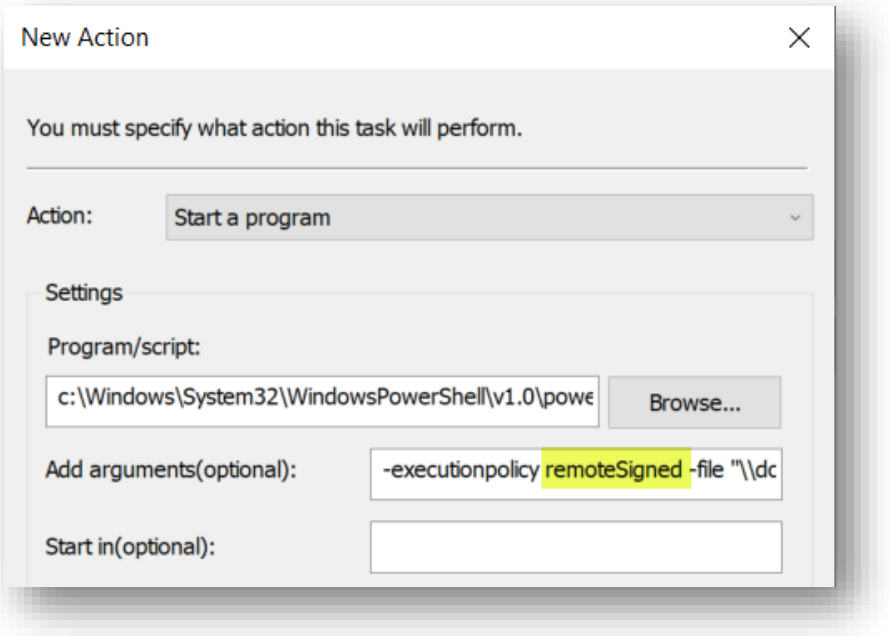
a. **General tab**: Name the task "*GYTPOL Client deploy*", run it under **NT AUTHORITY\SYSTEM**, check **Run with highest privileges** and select the **Hidden** check boxes.



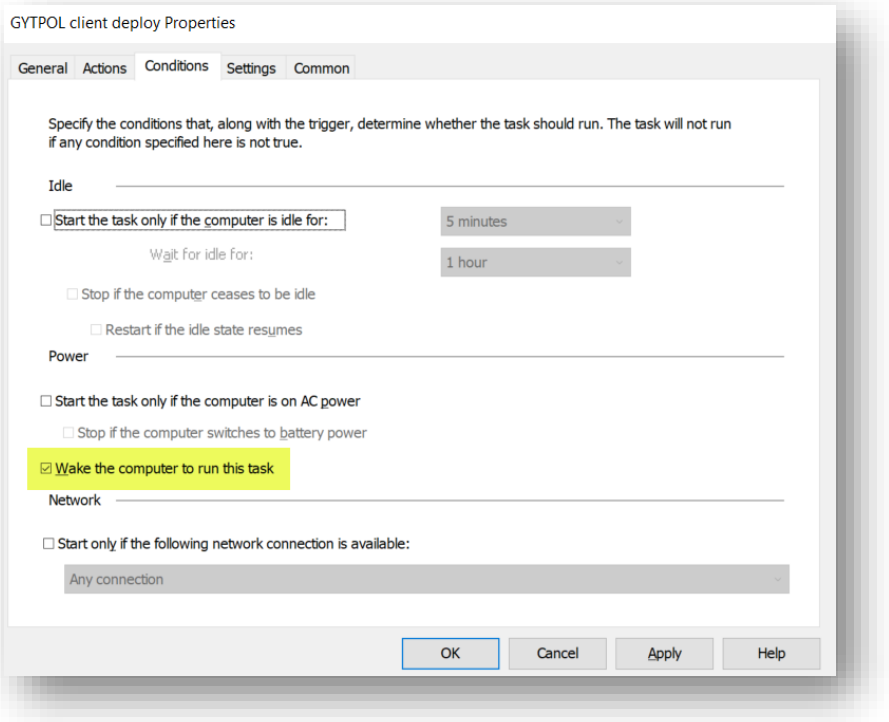
b. **Actions tab:** click New.

i. Under **Settings** → **Program/Settings** → enter the following: *c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe*

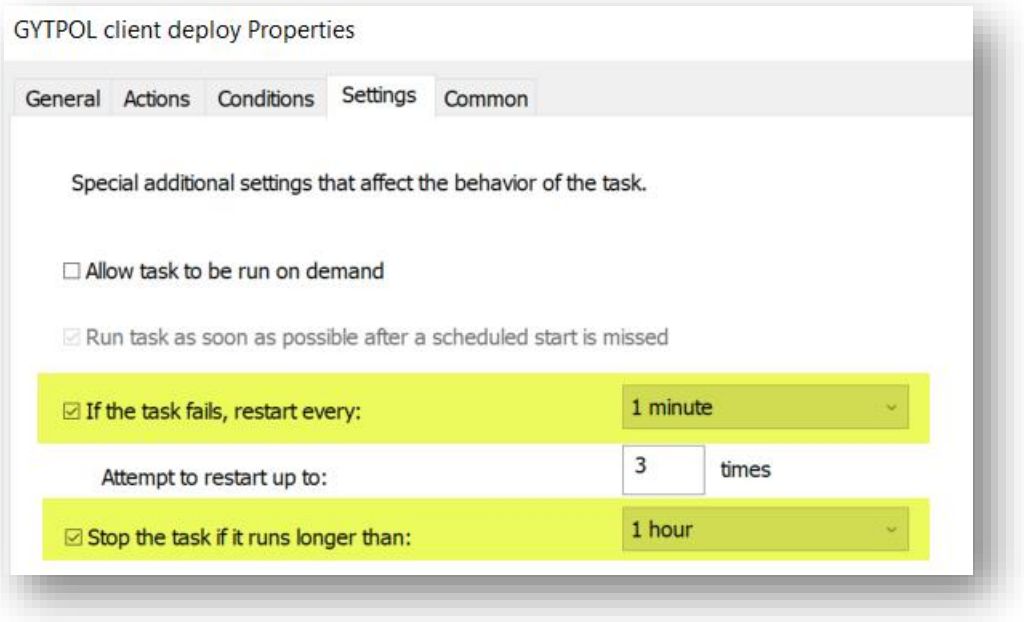
ii. **Add arguments (optional):** *-executionpolicy* ***remoteSigned*** *-file* *"\\yourDomainName\netlogon\gytpol\gytpolClient_GPO.ps1"*



c. **Conditions tab:** check **Wake the computer to run this task**



d. **Settings tab:** Set the options as shown

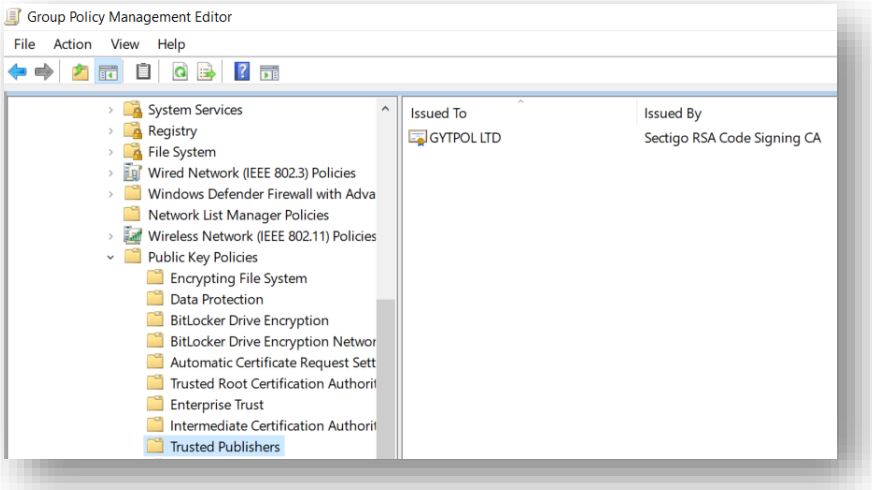


e. **Common tab:** leave default settings

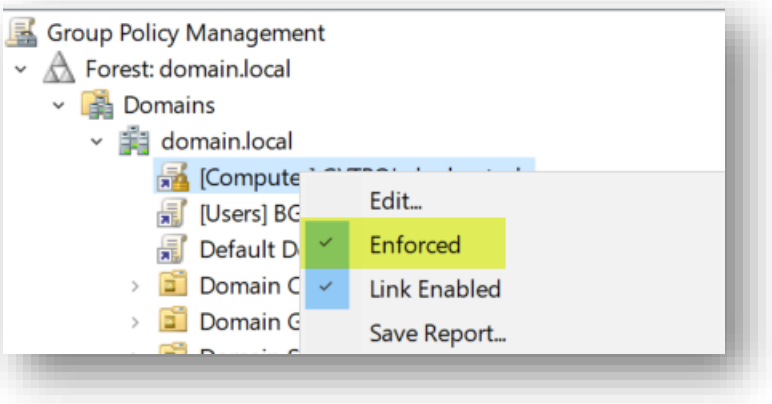
8. Click **OK** to close the task scheduler properties

Adding the Certificate to our GPO

1. Browse to **Computer Configuration → Policies → Windows Settings → Security Settings → Public Key Policies → Trusted Publishers**
2. R. click on Trusted Publishers → Import
3. Browse to the location where the exported certificate is stored and import it to the Certificate Import Wizard
4. Follow the Wizard with its defaults and the certificate will be shown in the Trusted Publishers folder in GPMC:



Close the GPO window and go back to the Group Policy Management Console (GPMC) → right click on the **GYTPOL Client Deployment** object → click **Enforced** and make sure this is what you see:



Once the GPO is refreshed on the PC/Server it will run the task and you should start seeing new devices added to the Dashboard.

- You can manually test the policy by running ***gpupdate /force*** from an elevated Command Prompt and check if Powershell.exe executes and msiexec.exe is also running.