

Certificate and GPO Deployment Guide

Document Versions:

Date	Version	Description
September, 30, 2018	1.0	Initial Release

Certificate Management	For clients to install third-party
Show Certificate Import PFX Certificate	updates, they must trust the
Export Certificate Generate a Self-Singed Certificate	code-signing certificate. Click the
Timestamp Server URL: http://timestamp.digicert.com	"Export Certificate" button to export the certificate to a (.CER)
	tile.
E Save As X	In the "Save As" dialog, give your
\leftarrow \rightarrow \checkmark \bigstar This PC \rightarrow Desktop \checkmark \circlearrowright Search Desktop $ ho$	certificate a name and click the
Organize 🔻 New folder 🗄 👻 📀	Save button.
Image: Server Logs Name Date modified Type Image: Desktop Image: Client Logs 4/5/2018 9:03 PM Shortcut Image: Downloads Image: Server Logs 1/11/2017 7:03 AM Shortcut Image: Downloads Image: Server Logs Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: PatchMyPC-CodeSigningCertificate Image: Server Logs Image: Server Logs Image: File name: File name: File name: File name: File name: File name: File name	
Certificate Export Successful X 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	Click OK on the Certificate Export Successful dialog.
ОК	

<u>.</u>	Next, we will distribute the
📓 File Action View Window Help	exported certificate to clients to
(=	ensure they trust updates
Group Policy Management	published using the code-signing
A Forest: CONTOSO.LOCAL Status Linked Group Policy Objects Grou	certificate exported.
Create a GPO in this domain, and Link it here	You can either create a new GPO
Doma Link an Existing GPO	or edit an existing GPO.
WMI Crows Deline World	
Starte New Organizational Unit S	To create a new GPO, right-click
Group Policy Search	the Domain and choose "Create
Group Policy Change Domain Controller	a GPO in this domain, and Link it
Remove a	here".
Active Directory Users and Computers	
⊻iew	
New <u>W</u> indow from Here	
Refresh	
P <u>r</u> operties	
Help	
New GPO X	If you choose to create a new
Nama	GPO, give it a name and click OK
Patch MvPC-Code Signing Certificate	
Source Starter GPO:	
(none) ~	
OK Cancel	
🛃 Group Policy Management	Right-click the newly created
✓ ▲ Forest: CONTOSO.LOCAL	GPO or the existing GPO and click
✓ Ii Domains	Edit
V 🚔 CONTOSO.LOCAL	
CONTOSO IT Settings	
Default Domain Policy	
INDAIN INDAIN INDAIN INDAIN INDAIN INDAIN	
> 1 Enforced	
> 📑 🗹 Link Enabled	
Save Report	

Group Policy Management Editor	In the "Group Policy
File Action View Help	Managament Editor" povigata to
	Wanagement Editor havigate to
PatchMyPC-CodeSigningCertificate [DC1.CONTOSO.LOCAL] Policy	Computer Configuration >
Computer Configuration	Policias > Windows Sattings >
> Software Settings	Policies > Windows Settings >
🗸 🚞 Windows Settings	Security Settings > Public Key
> 🔛 Name Resolution Policy	Delicios
Scripts (Startup/Shutdown)	Policies.
✓ ➡ Security Settings	
> 📑 Account Policies	
> 🗿 Local Policies	Right Click "Trusted Publishers"
> 🗿 Event Log	and Click Import
> System Services	
> 🔁 Registry	
> 📑 File System	Click Next on the "Malcome to
initial interval with Advanced Security	Click wext on the welcome to
Network List Manager Policies	the Certificate Import Wizard"
> 🚂 Wireless Network (IEEE 802.11) Policies	•
Public Key Policies Encounting File System	
Data Protection	Click Browse in the "Certificate
BitLocker Drive Encryption	
BitLocker Drive Encryption Network Unlock Certifica	Import Wizard"
Trusted Root Certification Authorities	
Enterprise Trust	
Intermediate Certification Authorities	
Trusted Publishers	
import	
> 🖺 S All Tasks >	
> A View >	
S S I Directory (CONTOSOLOC)	
📓 Open X	In the Open dialog, select the
← → ∽ ↑ 🔄 > This PC > Desktop 🗸 🗸 Search Desktop 🔎	CEP file that was experted and
Organize 🔻 New folder 🛛 👘 👻 🔲 2	.Cer me that was exported and
A Name Date modified Type Size	click Open
Aure Date mounted type Date mounted type	
Desktop * PatchMyPC-CodeSigningCertificate 4/20/2018 4:38 PM Security Certificate 1 KB	
🕹 Downlo 🖈	
🗎 Docume 🖈	
E Pictures 🖉 💆	
File name: PatchMyPC-CodeSigningCertificate Certificate File (*.cer;*.crt)	
<u>O</u> pen Cancel	
h.	

 Certificate Import Wizard Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Publishers Browse 	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 .
Next Cancel Public Key Policies Encrypting File System Data Protection BitLocker Drive Encryption BitLocker Drive Encryption Network Unloc Automatic Certificate Request Settings Trusted Root Certification Authorities 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.

Allow signed updates from an intranet Microsoft update service location	Within the same group policy
Allow signed updates from an intranet Microsoft update service location Previous Setting Next Setting	object, Navigate to Computer
Net Configured Comment:	Configuration > Administrative
○ Disabled ✓	remplates > windows
Supported on: At least Windows Server 2003 operating systems or Windows XP Professional with SP1, excluding Windows RT	Components > Windows Update.
Options: Help:	Click the "Allow signed updates
This policy setting allows you to manage whether Automatic	from an intranet Microsoft
when the update is found on an intranet Microsoft update service location	undate service location" policy
If you enable this policy setting. Automatic Updates accepts	
updates received through an intranet Microsoft update service location, if they are signed by a certificate found in the "Trusted	
Publishers" certificate store of the local computer.	Click "Enabled".
If you disable or do not configure this policy setting, updates from an intranet Microsoft update service location must be	
signed by Microsoft.	Click the OK Button.
Note: Updates from a service other than an intranet Microsoft update service must always be signed by Microsoft and are not	
affected by this policy setting. Note: This policy is not supported on Windows RT. Setting this	This policy is required by clients
policy will not have any effect on Windows RT PCs.	to allow third-party undates to
	to allow till d-party updates to
OK Cancel Apply	be installed.
V 🚔 CONTOSO.LOCAL	We have now completed the
🚘 CONTOSO IT Settings	certificate and Group Policy pre-
📓 Default Domain Policy	requisites for nublishing undates
	an the converticed eligent side
MBAM	on the server and client side.
PatchMyPC-CodeSigningCertificate	