

Getting Started - Basic

Patch My PC Docs - Basic

Documentation for the Basic subscription and integrating Microsoft's System Center Updates Publisher with Configuration Manager

Patch My PC offers a Basic subscription where customers can leverage our catalogue within [System Center Updates Publisher](#) (SCUP). With the Basic subscription, the only publishing method available is with SCUP and not with the [Patch My PC Publisher](#).

This document will detail the step-by-step instructions on setting up SCUP with Configuration Manager using our catalogue. It will cover:

- Installing SCUP
- Connecting SCUP to WSUS and Configuration Manager
- Creating a code signing certificate, show example deployment method of the certificate using GPO, and configuring other needed GPO settings
- Importing the Patch My PC third party updates catalogue
- Deploying the updates with Configuration Manager

For more information about SCUP, please see [System Center Updates Publisher | Microsoft Docs](#).


You can request a quote for the Basic subscription from here: [Basic Subscription](#).

Installation

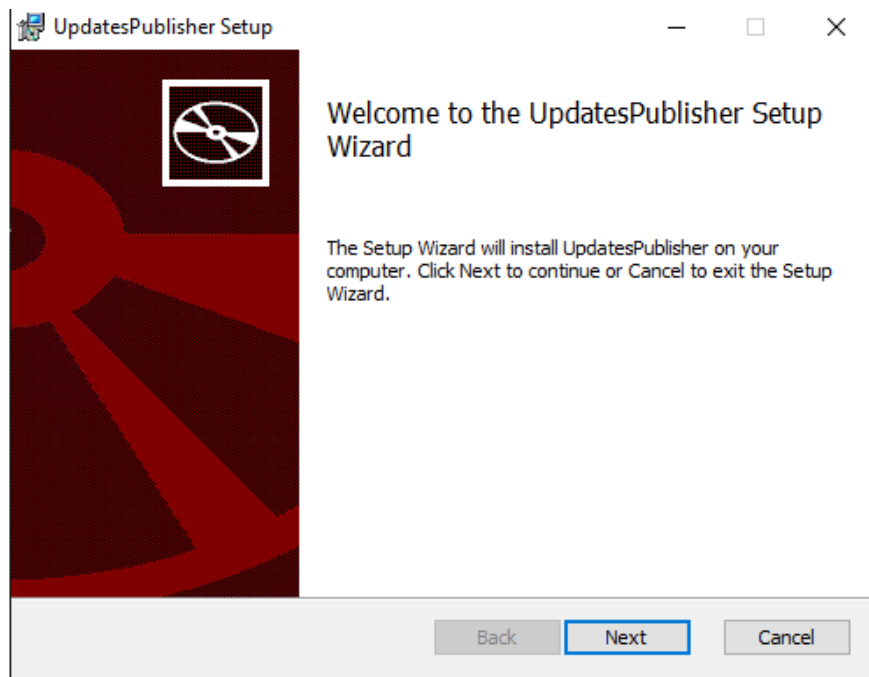
This section will detail the step-by-step instructions on setting up SCUP with Configuration Manager using our catalogue.

Before starting the installation, decide where you are going to install SCUP. You can either install it on your top most WSUS/Software Update Point server in Configuration Manager, or you can install it on a remote machine and configure SCUP to point to the remote WSUS server.

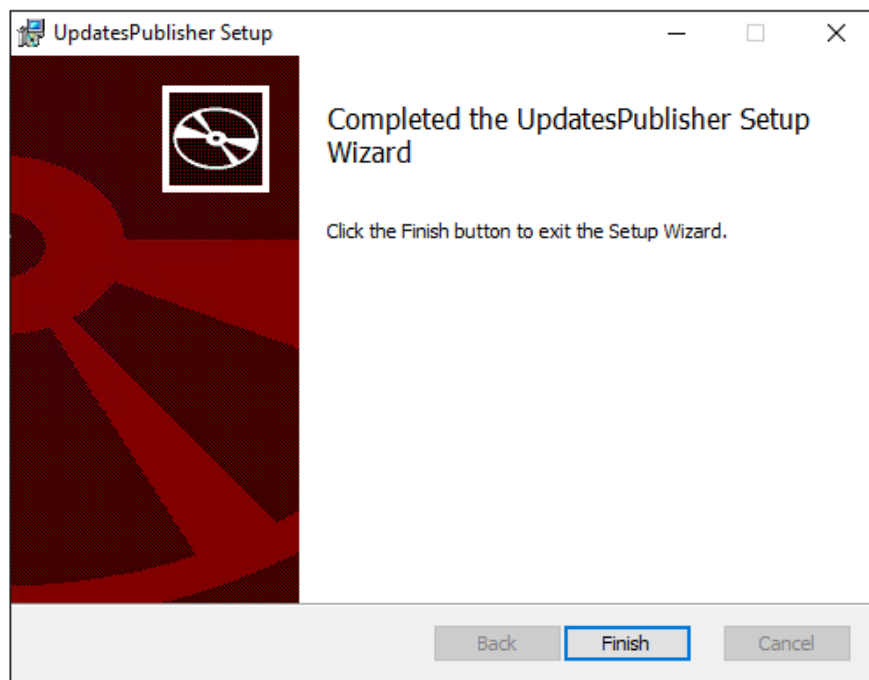
Once decided, download the installer for [SCUP from Microsoft](#), start the installation and complete the wizard to finish installation.

 For information about SCUP's prerequisites and requirements, read more on [Install Updates Publisher | Microsoft docs](#)

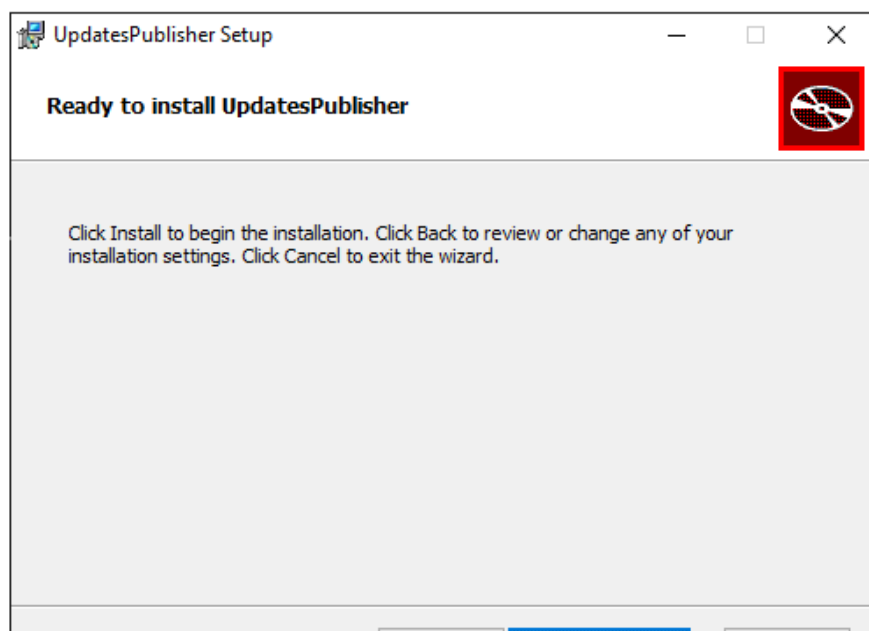
1



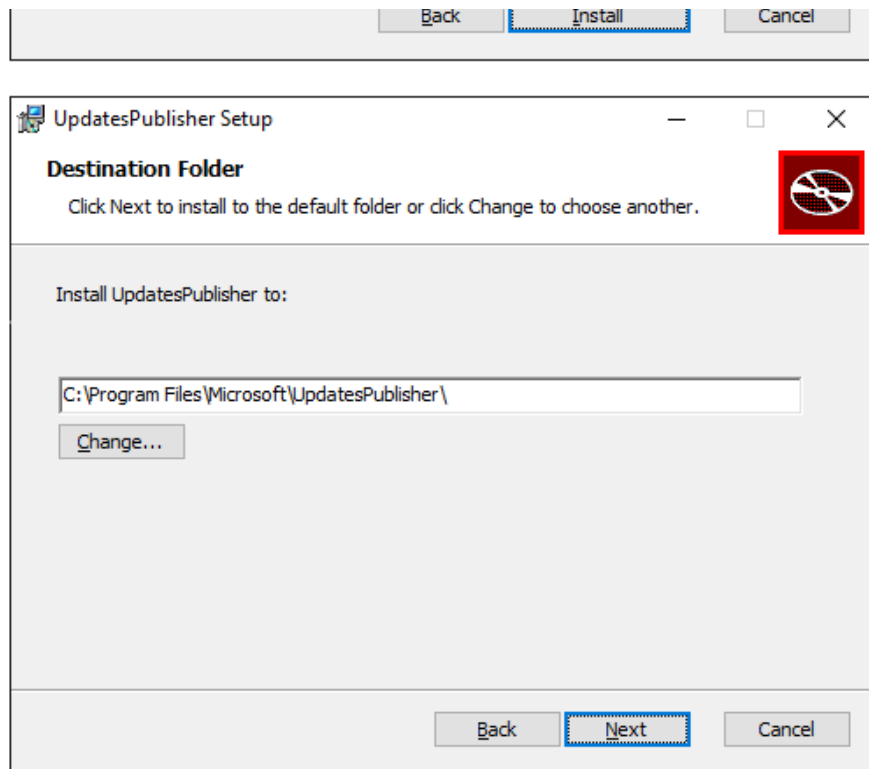
2



3

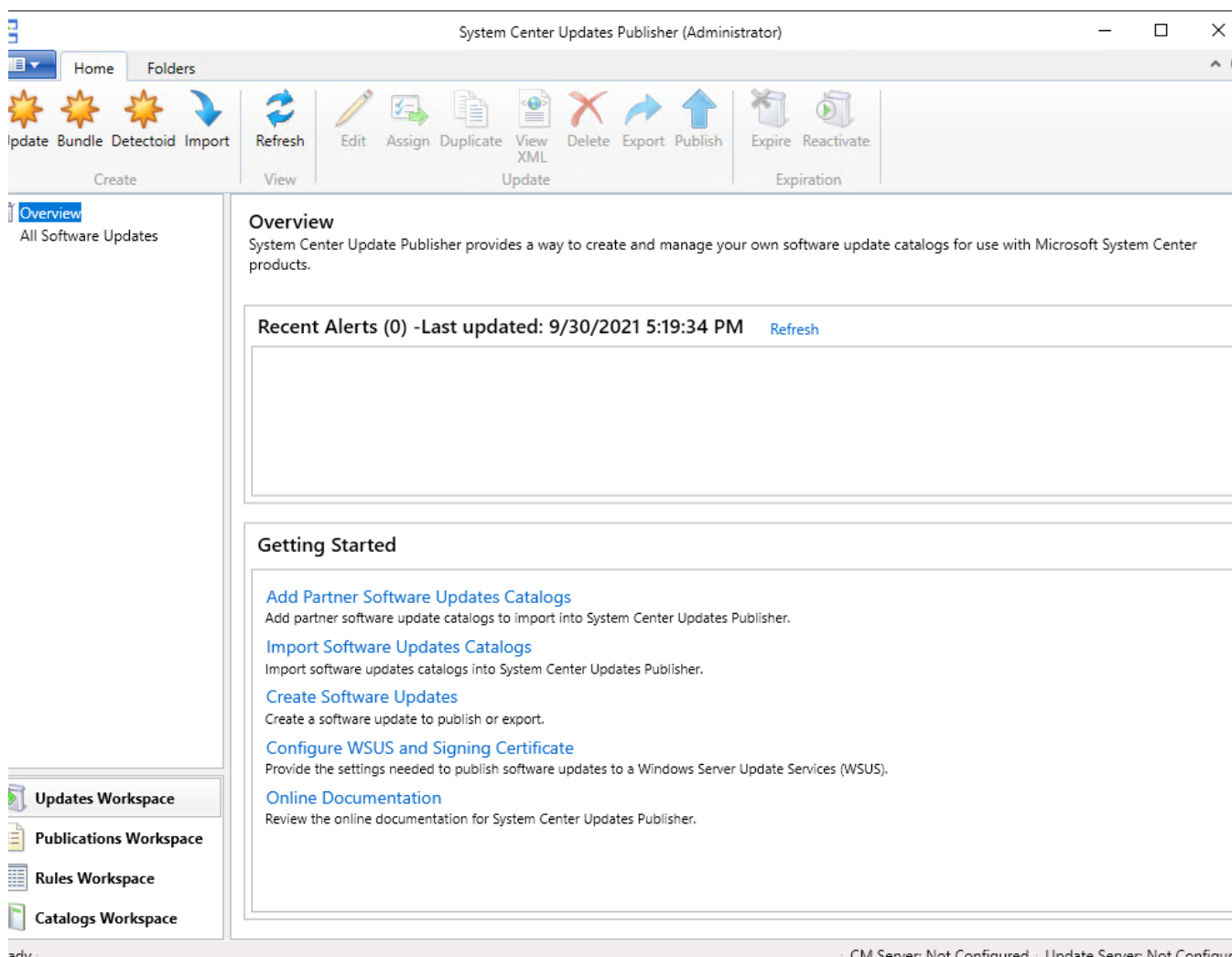


4



SCUP installation wizard

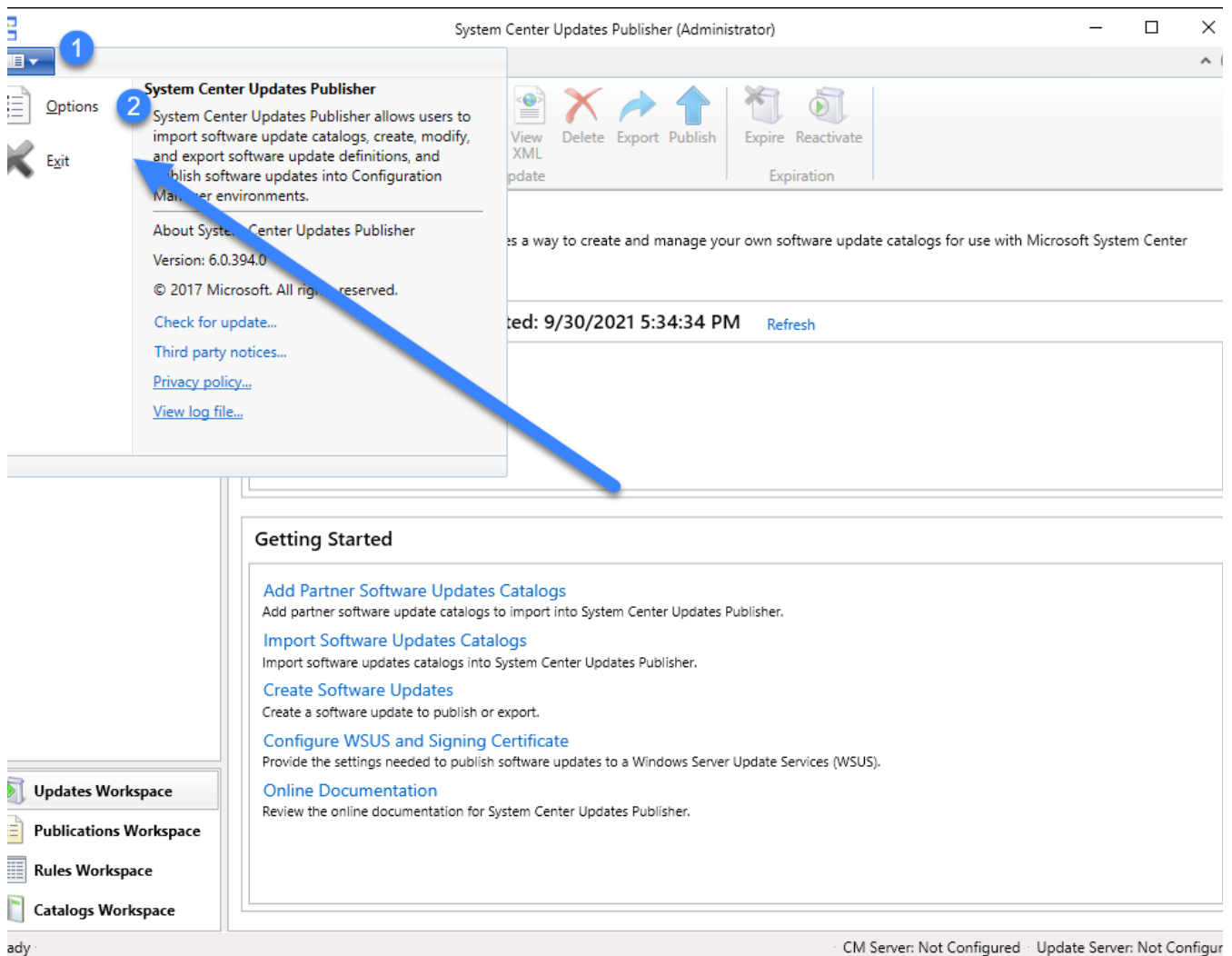
From the Start Menu, launch Updates Publisher and by default this is what SCUP looks like with no catalogues imported:



Connecting to WSUS and Configuration Manager

This section will detail how to connect SCUP to WSUS and Configuration Manager.

Within the top left menu, click on **Options**.



Updates Publisher - Options menu

While in the Update Server section, connect to your WSUS server. If you still SCUP on your top level WSUS/Software Update Point then you can choose **Connect to a local update server**, otherwise if you installed SCUP remotely then choose **Connect to a remote update server** and enter the connection details.

Click **Test Connection** to verify.

- i** If you receive a warning after testing connection advising the test connection succeeded but 'the signing certificate is not in the Trusted Publishers store, ...' - this is normal and will be addressed in the **Code Signing Certificate** section.

System Center Updates Publisher Options

Options

- Update Server**
- ConfigMgr Server
- Proxy Settings
- Trusted Publishers
- Advanced
- Authoring
- Updates
- Logging

☒ **Enable publishing to an update server**

Settings

Configure the update server to use for publishing. WSUS Administrators group rights are required on the update server for you to successfully publish software updates.

☒ **Connect to a local update server**
☐ **Connect to a remote update server:**

☐ **Use SSL when communicating with the updates server**

Name:

Port:

Test Connection

Signing Certificate

The signing certificate is used to digitally sign the content you want to publish to the update server. Browse to an existing signing certificate and choose Create, or leave File empty and choose Create to have the update server generate a self-signing certificate.

File:

Browse... **Create** **Remove**

Last recorded update server certificate

Certificate issuer: CN=PMP1 Intermediate CA, DC=contoso1, DC=local
 Expiration date: 13/05/2026 07:08:09

OK **Cancel**

Updates Publisher - Update Server menu

Change to the ConfigMgr Server section and connect to your Configuration Manager site or Central Administration Site host name. Again, if this server is localhost to where you have installed SCUP, choose **Connect to a local Configuration Manager server**, other choose the other option and enter the host name of your site server.

Click **Test Connection** to verify.

System Center Updates Publisher Options

Options

- Update Server
- ConfigMgr Server**
- Proxy Settings
- Trusted Publishers
- Advanced

☒ **Enable Configuration Manager integration**

Settings

Enter the Configuration Manager Central Site or Central Administration Site (CAS) that is used to check whether update content should be provided during publication.

☒ **Connect to a local Configuration Manager server**
☐ **Connect to a remote Configuration Manager server:**

Name:

Authoring

Updates

Logging

Test Connection

Automatic publishing settings

Specify the threshold values that control whether software updates published with the Automatic setting are published with full content. During publishing, these values are checked against the Configuration Manager site to determine if the update content should be included. If both requirements are not met, the software update content will not be downloaded and included.

Requested client count threshold: 1

Package source size threshold (MB): 0

OK Cancel

Updates Publisher - ConfigMgr Server menu

Code Signing Certificate

This section will discuss the certificate requirements for third party patching and SCUP.

A code signing certificate is required to sign the third party updates before they can be published. The same code signing certificate must be trusted by the devices you intend to deploy third party updates to.

You can either generate a self-signed certificate from the WSUS server, or you can import a previously issued certificate from an internal or public Certificate Authority.

Self-signed Certificate

To generate a self-signed certificate, first start by setting the following registry key on your WSUS server:

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	Software\Microsoft\Update Services\Server\Setup
Value Name	EnableSelfSignedCertificates
Value Type	REG_DWORD
Enabled Value	1
Disabled Value	0

i This is required because from 2012 R2 onwards Microsoft removed the ability to generate self-signed certificates in the UI, read more about that here: [WSUS no longer issues self-signed certificates | Microsoft Docs](#).

The above registry change is a suggested workaround by the same article.

Navigate back to the Update Server section from the Options menu and click **Create** under the **Signing Certificate** section to issue a new self-signed code signing certificate for WSUS. After doing this, you should see certificate details at the bottom.

System Center Updates Publisher Options

Options

Update Server

ConfigMgr Server

Proxy Settings

Trusted Publishers

Advanced

Authoring

Updates

Logging

☒ Enable publishing to an update server

Settings

Configure the update server to use for publishing. WSUS Administrators group rights are required on the update server for you to successfully publish software updates.

☒ Connect to a local update server

☐ Connect to a remote update server:

☐ Use SSL when communicating with the updates server

Name: localhost

Port: 8530

Test Connection

Signing Certificate

The signing certificate is used to digitally sign the content you want to publish to the update server. Browse to an existing signing certificate and choose Create, or leave File empty and choose Create to have the update server generate a self-signing certificate.

File:

Browse... Create Remove

Last recorded update server certificate

Certificate issuer: CN=WSUS Publishers Self-signed

Expiration date: 9/30/2026 7:59:59 AM

OK Cancel

Updates Publisher - Update Server menu

Verify you can see the newly issued self-signed code signing certificate in the **certlm.msc** (Local Computer Certificates store) under the WSUS store.

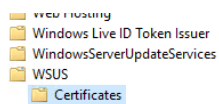
certlm - [Certificates - Local Computer\WSUS\Certificates]

File Edit Action View Help

Certificates - Local Computer

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Client Authentication Issuers
- Preview Build Roots
- Test Roots
- AAD Token Issuer
- MSIEHistoryJournal
- Remote Desktop
- Smart Card Trusted Roots
- SMS
- Trusted Devices
- Wah History

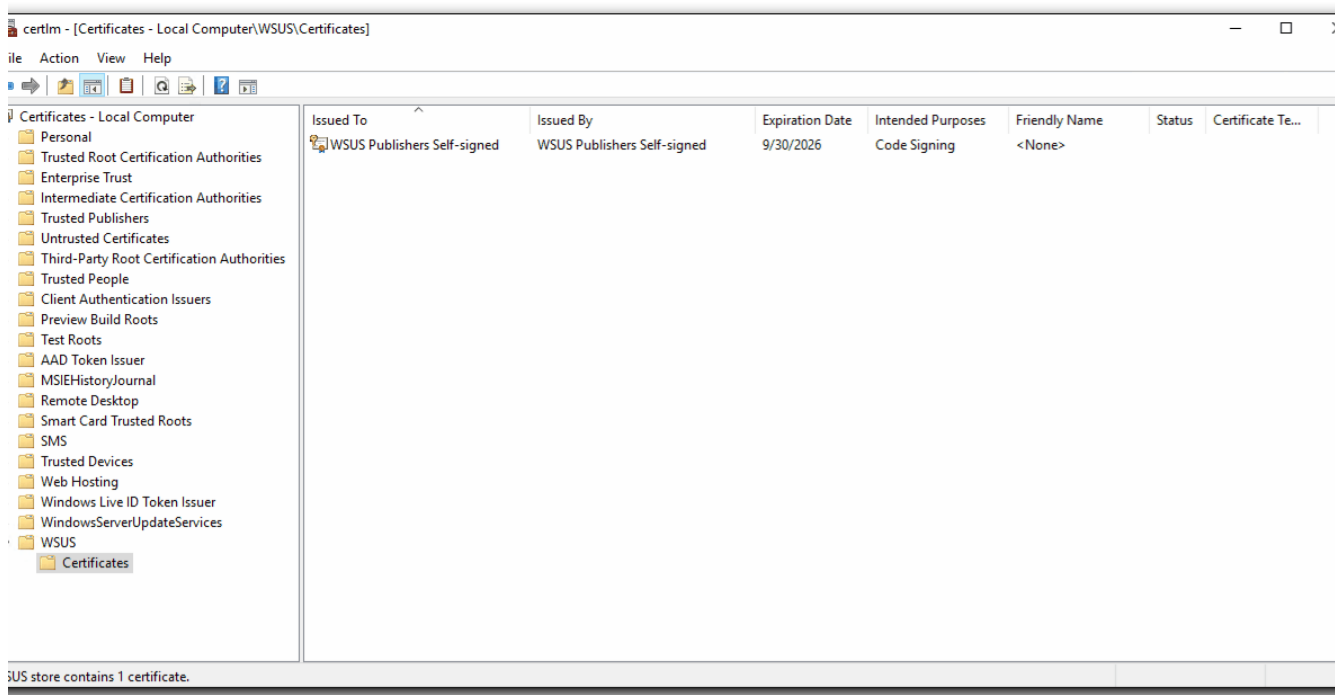
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
WSUS Publishers Self-signed	WSUS Publishers Self-signed	9/30/2026	Code Signing	<None>		



JS store contains 1 certificate.

Local Computer Certificate WSUS Store

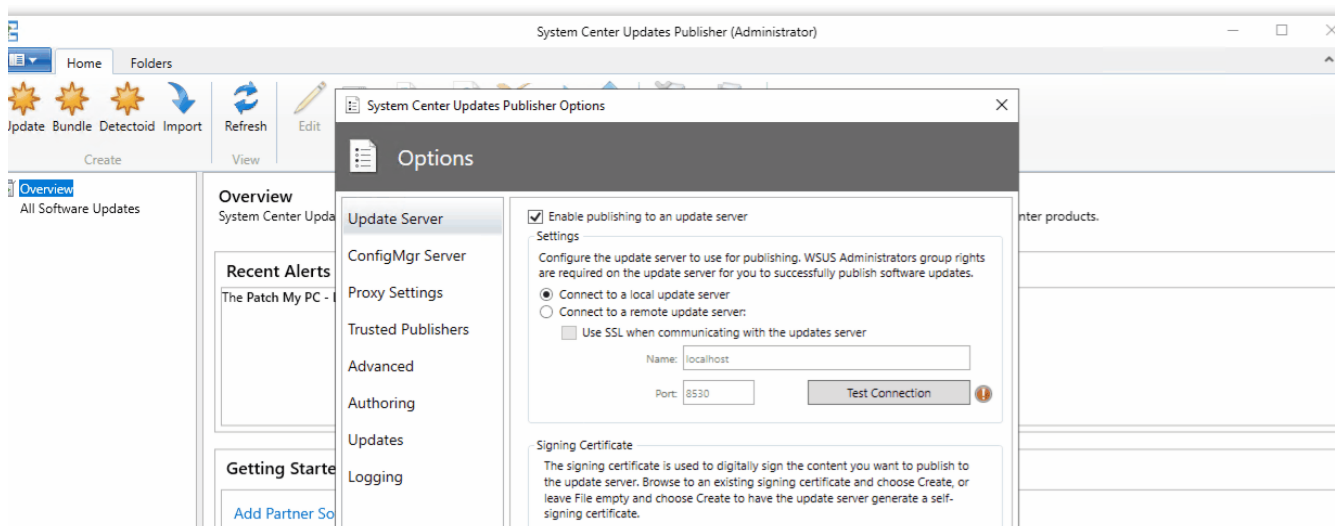
Since this certificate is self-signed, it must be trusted by the WSUS server itself and also stored in the Trusted Publisher store. Right click on the certificate, and copy and paste it to the **Trusted Publishers** and **Trusted Root Certification Authorities** stores.

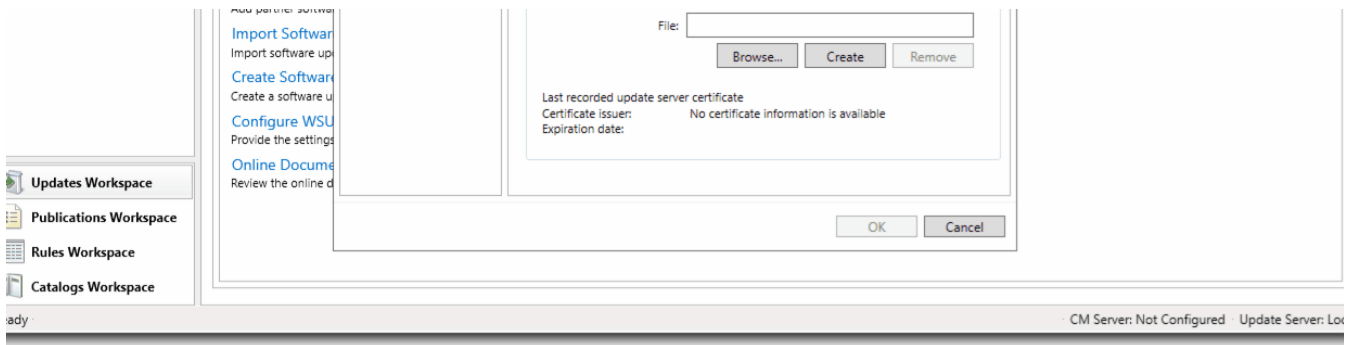


Copying certificate to Trusted Root Certification Authorities and Trusted Publishers stores

PKI Certificate

Navigate back to the Update Server section from the Options menu and click **Browse...** to choose your code signing certificate. If the certificate is protected by a password, you must then click **Create** to complete importing the certificate for the password prompt.

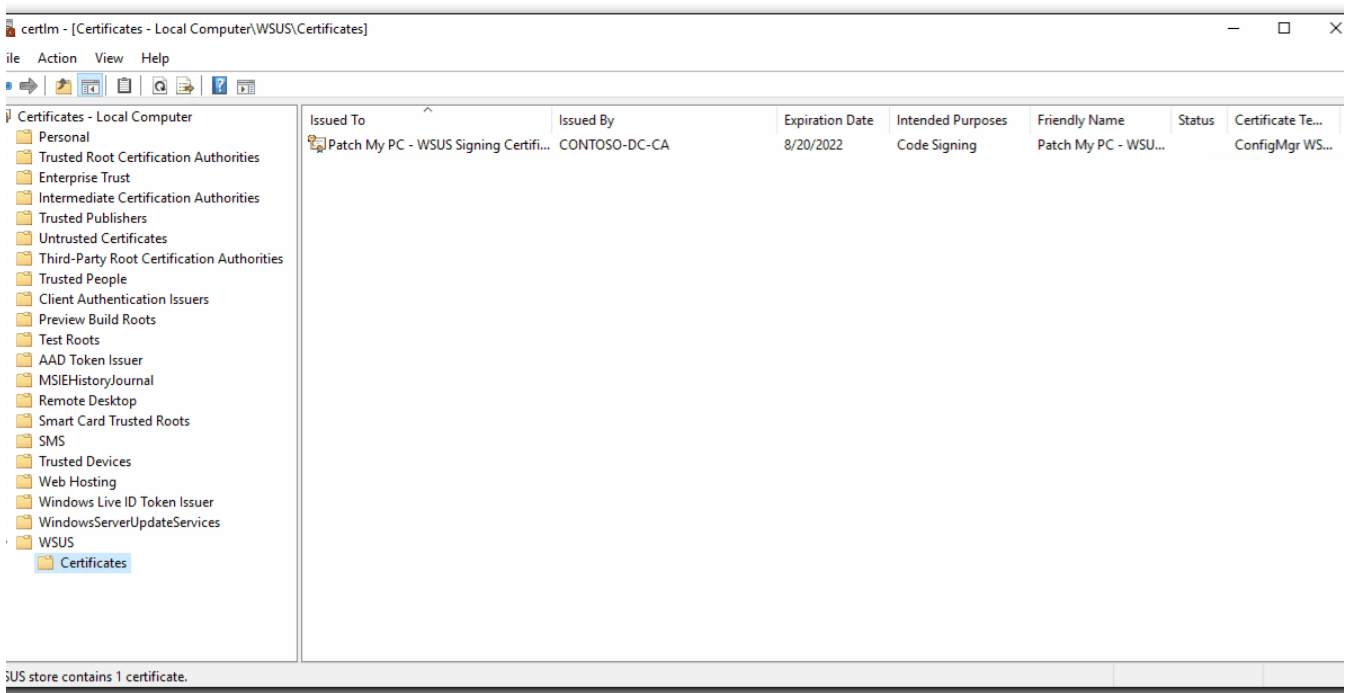




Updates Publisher - Importing .pfx and entering password

Verify you can see the newly imported code signing certificate in the **certlm.msc** (Local Computer Certificates store) under the WSUS store. You should copy the certificate to the **Trusted Publishers** store. You also need to ensure the certificate's Root CA certificate is in the server's **Trusted Root Certification Authorities** store so the server trusts it.

i If your code signing certificate is not trusted, source the issuer's certificate chain certificates and install them in the **Trusted Root Certification Authorities** store.



Copying certificate to Trusted Publishers and ensuring it is trusted

Deploying the Code Signing Certificate

This section will detail the certificate requirements for your endpoints, and also provide an example method of deploying your code signing certificate using Group Policy.

A requirement of the Windows Update Agent for the target systems you intend to deploy third party updates to is ensure the software update .cab files be signed by a trusted code signing certificate.

Up to this point you have configured SCUP to sign third party updates so that they're published to WSUS using your desired code signing certificate. The next requirement is to ensure your devices trust **the same code signing certificate**.

If you used a self-signed code signing certificate, distribute the certificate to your devices in their **Trusted Publishers** and **Trusted Root Certification Authorities** store.

If you used a code signing certificate issued from an internal or public CA, distribute the certificate to your devices in the **Trusted Publishers** store. Also ensure your devices trust the certificate chain.

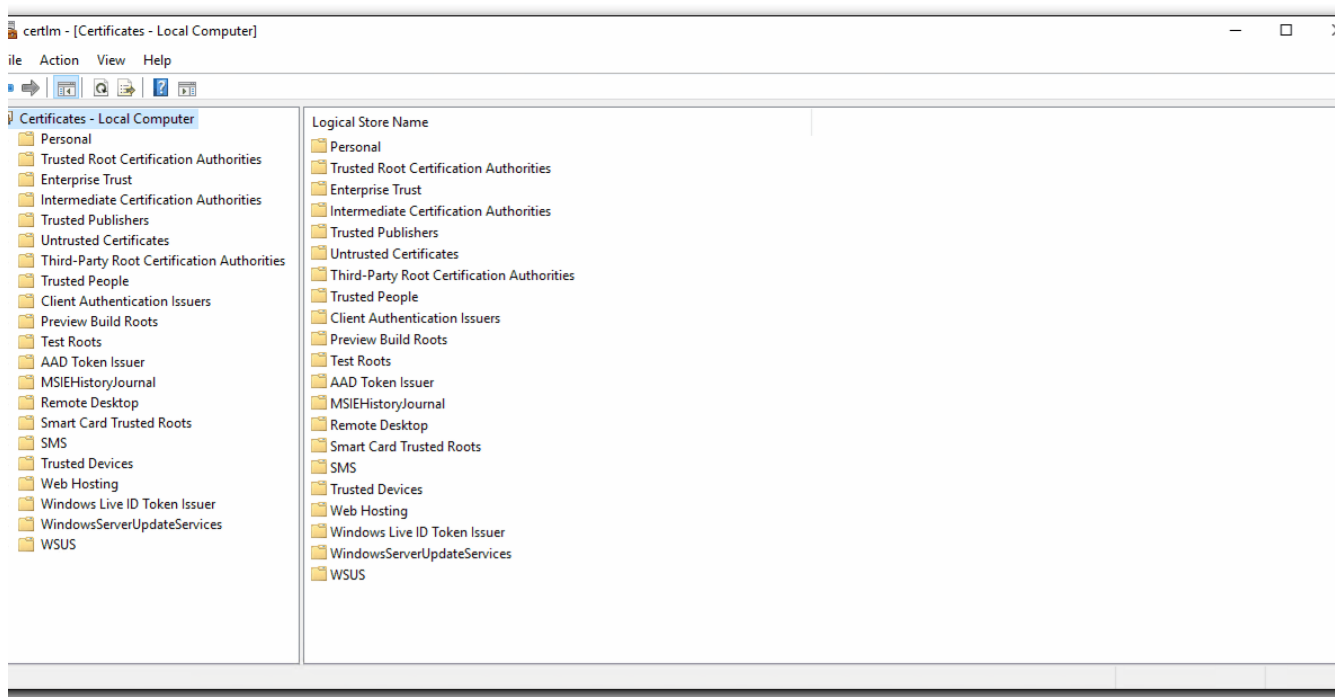
Group Policy

This section will detail how to deploy your code signing certificate to your endpoint using Microsoft Active Directory Group Policy.

Ensure you have your code signing certificate to hand as a file (e.g. .cer or .crt). If you generated a self-signed certificate, you can export the certificate from the Local Machine Certificates snap in (certlm.msc).



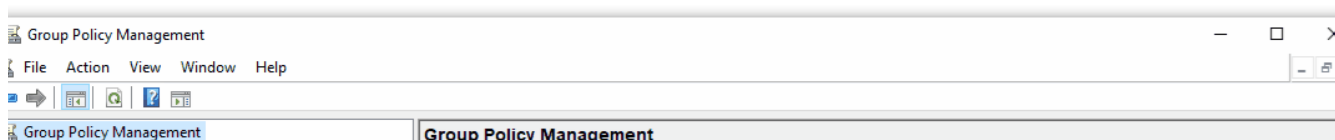
Exporting or distributing the private key with the certificate is not recommended.

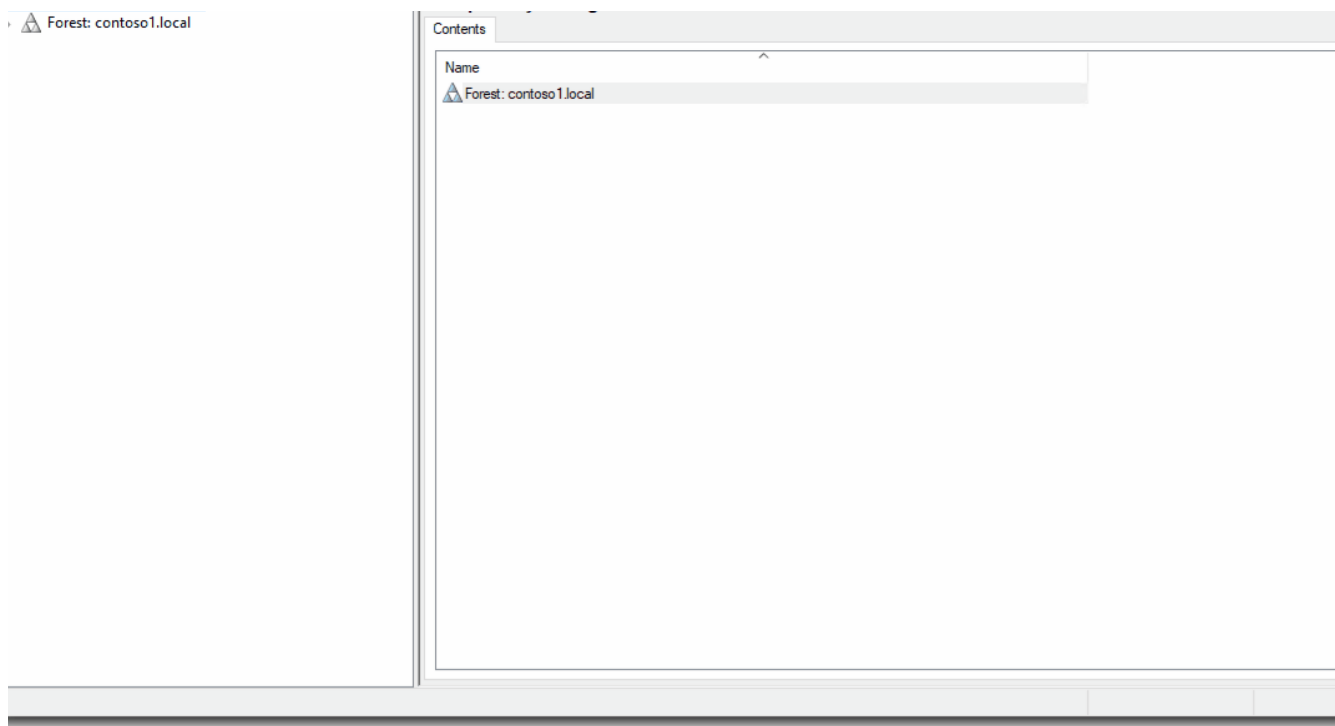


Export code signing certificate from the Local Machine Certificates snap-in

Create or use an existing Group Policy Object and link it so it is targeting the endpoints you intend to deliver third party software updates to.

Under **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**, import your code signing certificate to the **Trusted Publishers** store. If you used a self-signed certificate, also import it into the **Trusted Root Certification Authorities** store.





Create GPO to deploy code signing certificate

Allow signed updates from an intranet Microsoft update service location

The devices you intend to deliver third party software updates to should be configured to [Allow signed updates from an intranet Microsoft update service location](#). This can be achieved using Group Policy. The location of this policy is in **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update**.

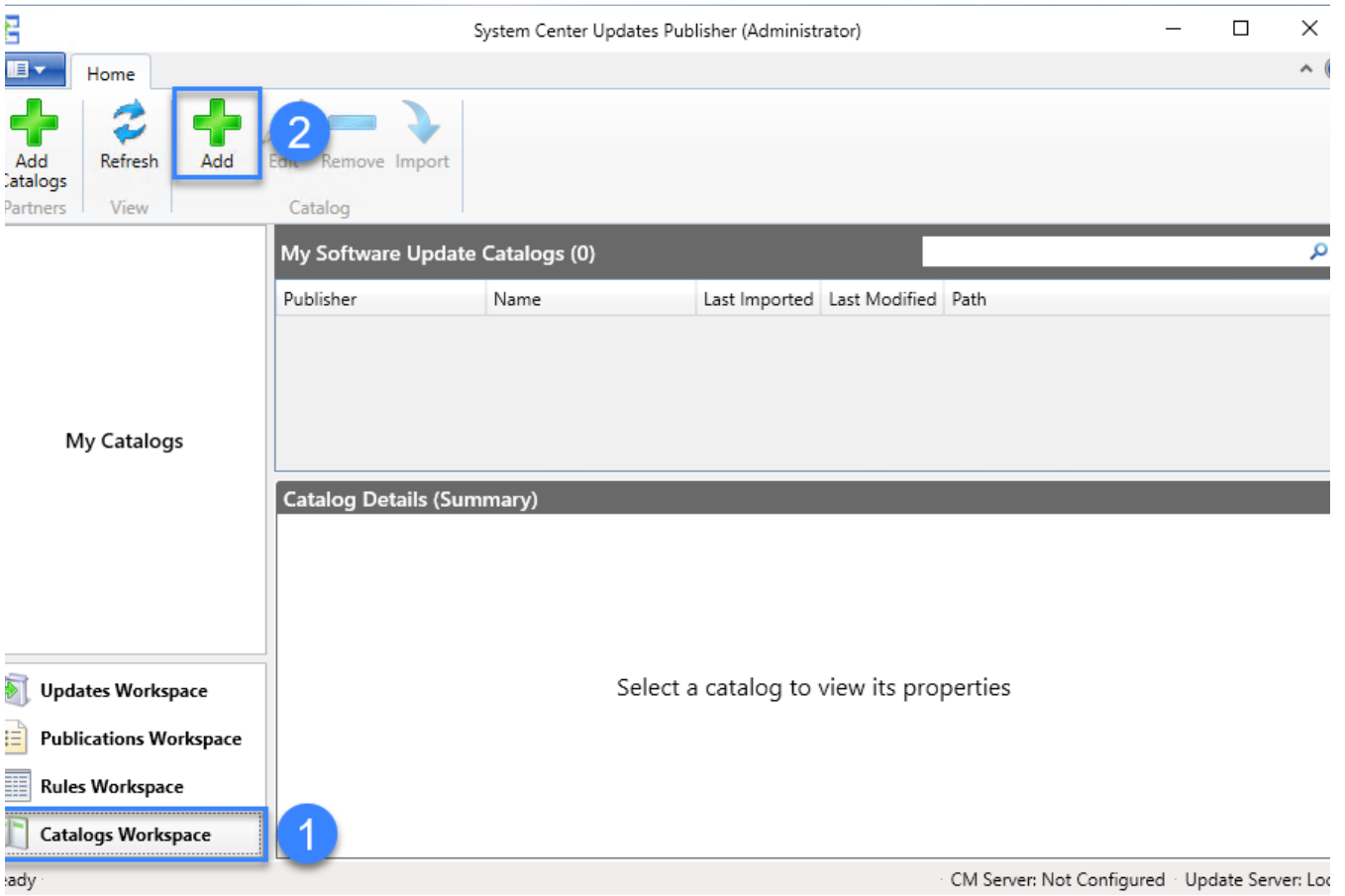
Ultimately, it configures the following registry value on the device:

Registry Hive	HKEY_LOCAL_MACHINE
Registry Path	Software\Policies\Microsoft\Windows\WindowsUpdate
Value Name	AcceptTrustedPublisherCerts
Value Type	REG_DWORD
Enabled Value	1

Adding the Catalog

This section will detail how to configure SCUP to utilise the Patch My PC catalogue. You must complete Installation and Configuration before continuing.

Open SCUP and navigate to the **Catalogs Workspace**, and from the ribbon at the top, click **Add** (not Add Catalogs).



System Center Updates Publisher (Administrator)

Home

Add Catalogs Refresh Add Edit Remove Import

Partners View Catalog

My Catalogs

My Software Update Catalogs (0)

Publisher	Name	Last Imported	Last Modified	Path
-----------	------	---------------	---------------	------

Catalog Details (Summary)

Select a catalog to view its properties

Updates Workspace Publications Workspace Rules Workspace Catalogs Workspace

CM Server: Not Configured · Update Server: Loc

Updates Publisher - Add new catalog

At the **Add Software Update Catalog** window, enter the catalogue path, publisher, name, and description.

The catalogue path will be the following URL, replacing <YOURLICENSEID> with your license ID issued to you after purchase.

1 https://patchmypc.com/scupcatalog/apis/subscriber_download.php?id=<YOURLICENSEID>

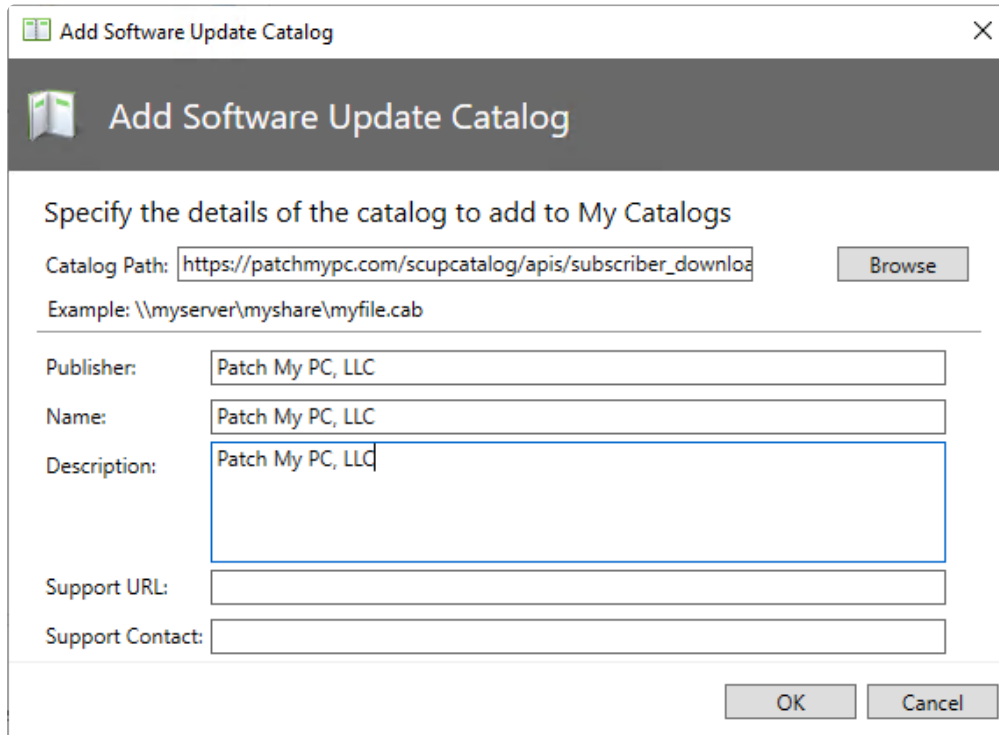
 If you do not yet have a license ID, please [request a quote](#) to purchase our basic subscription.

As for publisher, name, and description, you can for example enter **Patch My PC, LLC**.

After you've defined these fields, click **OK**, after which point you will see the Patch My PC catalog listed as a

catalog in the Catalogs Workspace.

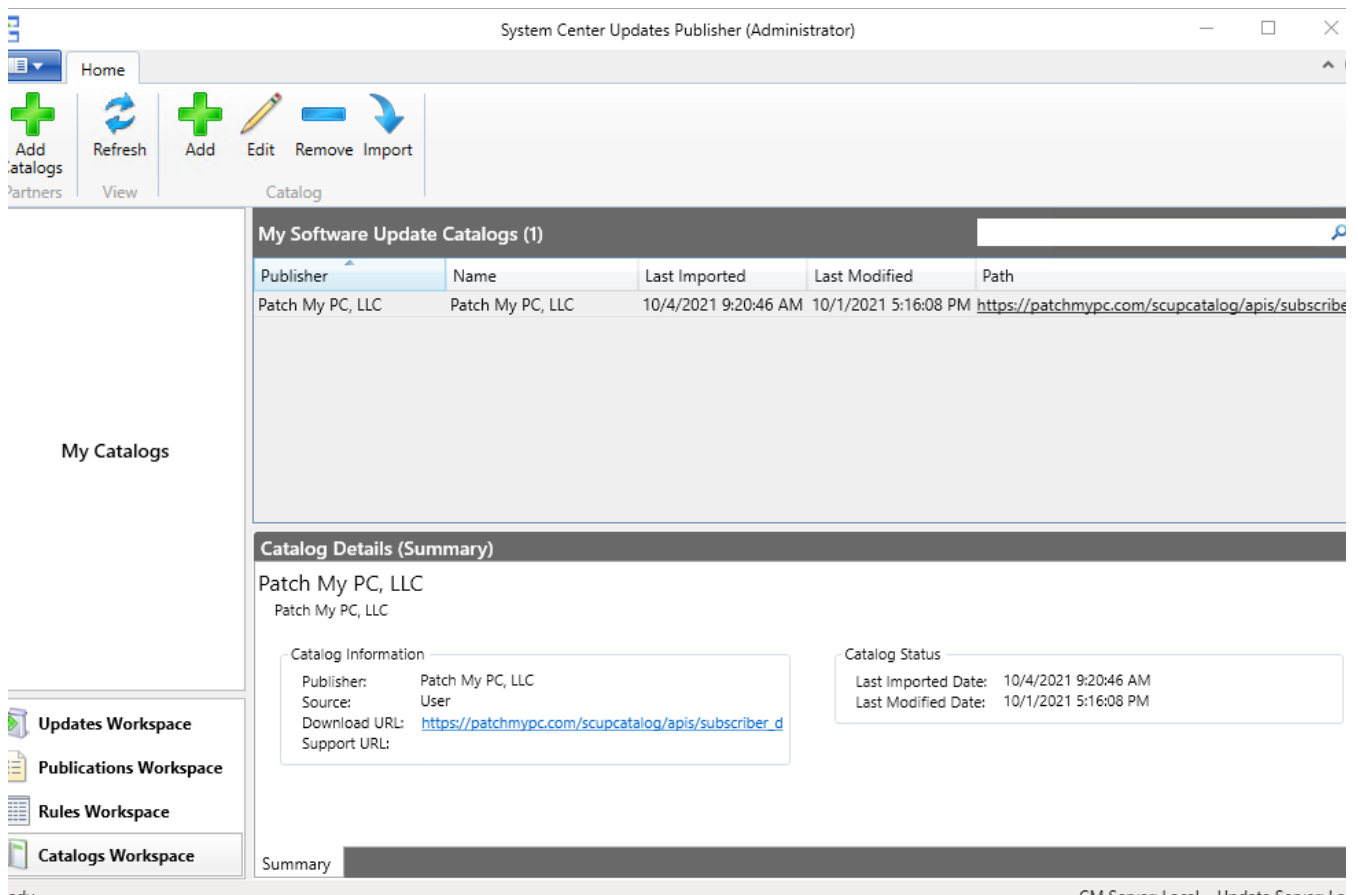
- i** If you receive any errors while importing or downloading the catalog, the **UpdatesPublisher.log** file located in your user's **%temp%** directory will be useful for troubleshooting possible connectivity failures to **patchmypc.com**.



The dialog box is titled "Add Software Update Catalog". It contains the following fields and controls:

- Catalog Path:** A text box containing "https://patchmypc.com/scupcatalog/apis/subscriber_download" and a "Browse" button.
- Example:** The text "\\myserver\myshare\myfile.cab".
- Publisher:** A text box containing "Patch My PC, LLC".
- Name:** A text box containing "Patch My PC, LLC".
- Description:** A text box containing "Patch My PC, LLC".
- Support URL:** An empty text box.
- Support Contact:** An empty text box.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Updates Publisher - Add Software Update Catalog



The screenshot shows the "System Center Updates Publisher (Administrator)" application. The interface includes a top navigation bar with "Home", "Partners", and "View" tabs. Below this is a ribbon with icons for "Add catalogs", "Refresh", "Add", "Edit", "Remove", and "Import". The main content area is divided into two sections:

- My Software Update Catalogs (1):** A table with the following data:

Publisher	Name	Last Imported	Last Modified	Path
Patch My PC, LLC	Patch My PC, LLC	10/4/2021 9:20:46 AM	10/1/2021 5:16:08 PM	https://patchmypc.com/scupcatalog/apis/subscriber_d
- Catalog Details (Summary):** A section for "Patch My PC, LLC" showing details:
 - Catalog Information:**
 - Publisher: Patch My PC, LLC
 - Source: User
 - Download URL: https://patchmypc.com/scupcatalog/apis/subscriber_d
 - Support URL:
 - Catalog Status:**
 - Last Imported Date: 10/4/2021 9:20:46 AM
 - Last Modified Date: 10/1/2021 5:16:08 PM

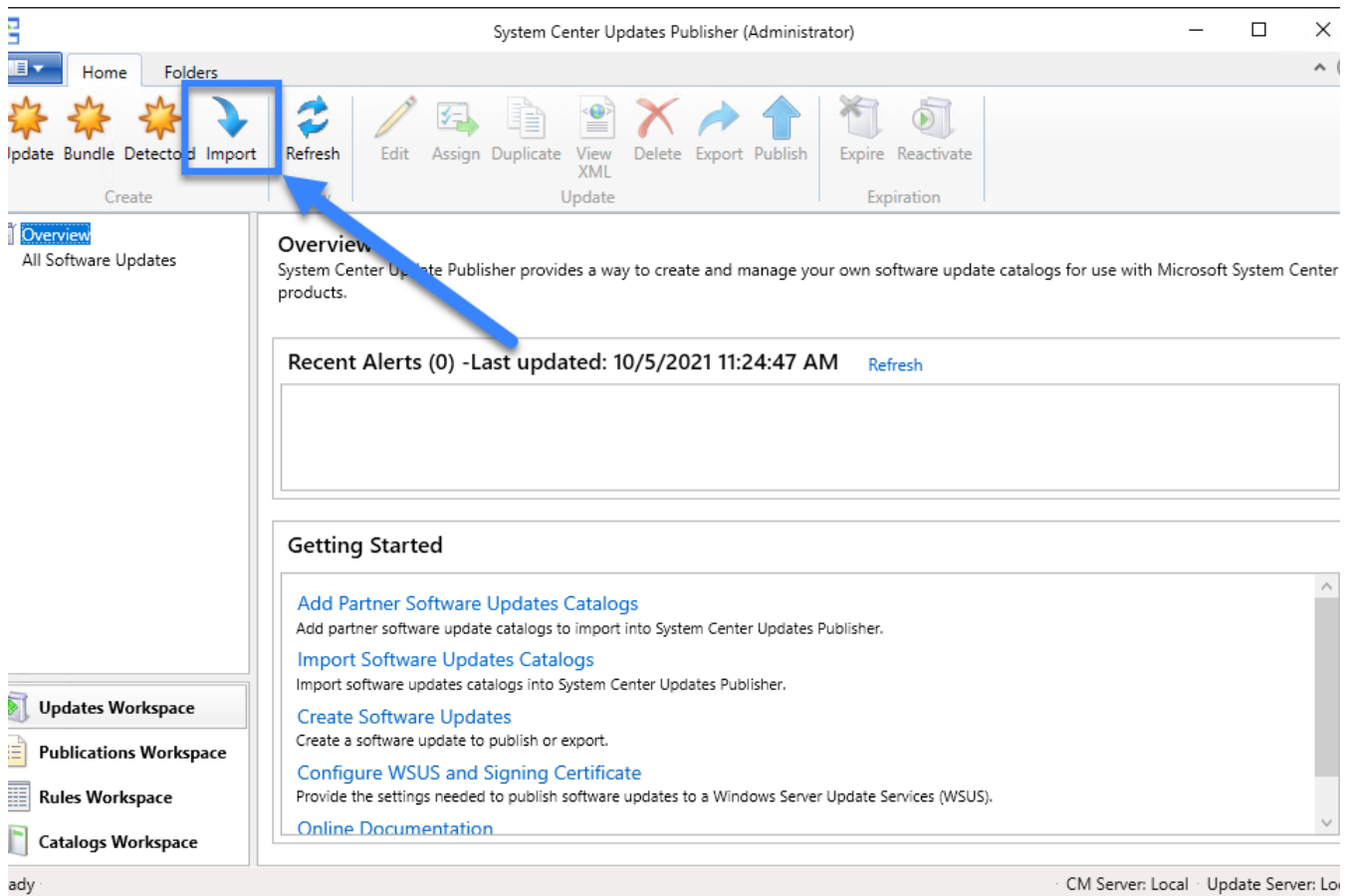
The left sidebar shows the "Updates Workspace" and "Catalogs Workspace" tabs.

Importing the Catalog

This section will detail how to import the Patch My Pc catalog for the first time into SCUP.

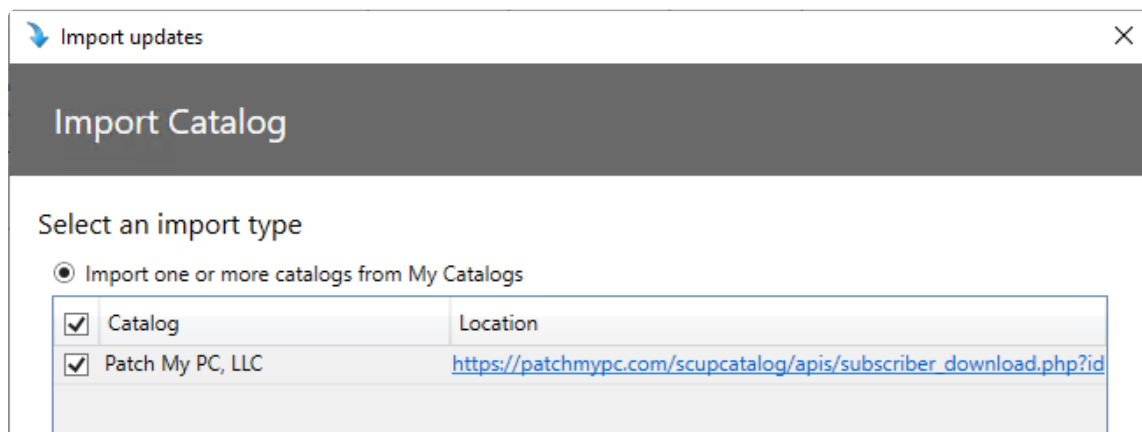
Before we can publish updates to WSUS and therefore Configuration Manager, we first need to import the updates into SCUP.

Open SCUP and within the default Updates Workspace, click **Import** from the ribbon.



Updates Publisher - Import catalog

Select the Patch My PC catalog from the list added from the previous step, and click **Next**.



Updates Publisher - Import catalog

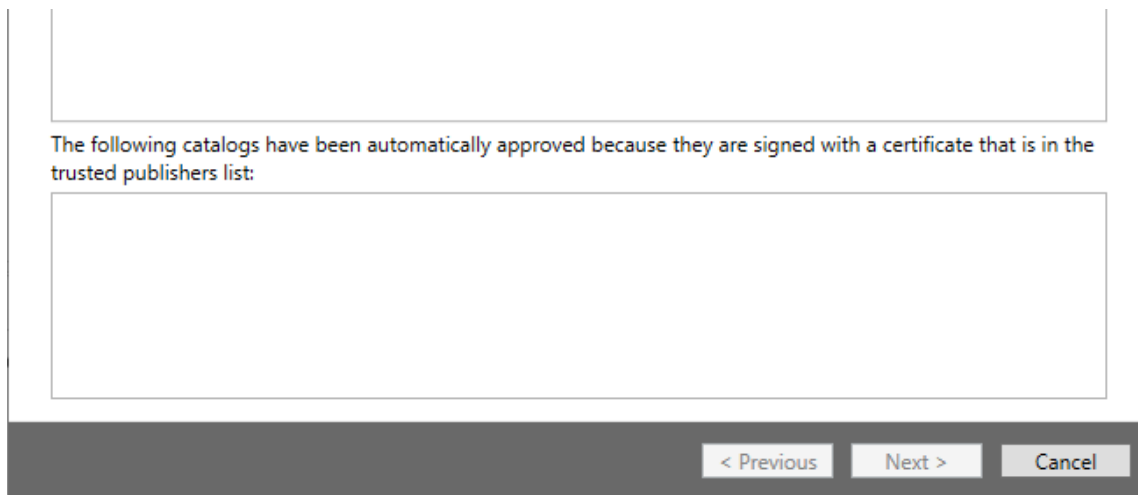
i If you receive any errors while importing or downloading the catalog, the **UpdatesPublisher.log** file located in your user's **%temp%** directory will be useful for troubleshooting possible connectivity failures to **patchmypc.com**.

! If you receive an error while importing the catalogue and UpdatesPublisher.log indicates error "**The request was aborted: Could not create SSL/TLS secure channel.**", check out this KB article:

[How to Resolve Download Errors During PatchMyPC SCUP Catalog Download – Exception Message: The request was aborted: Could not create SSL/TLS secure channel -2146233079](#)

At the next dialogue you will need to decide if you want to trust the code signing certificate used to sign our approve as a one-off by clicking on **Approve**, or always approving it by selecting **Always Approve**. You can validate the certificate by clicking on **View certificate**.

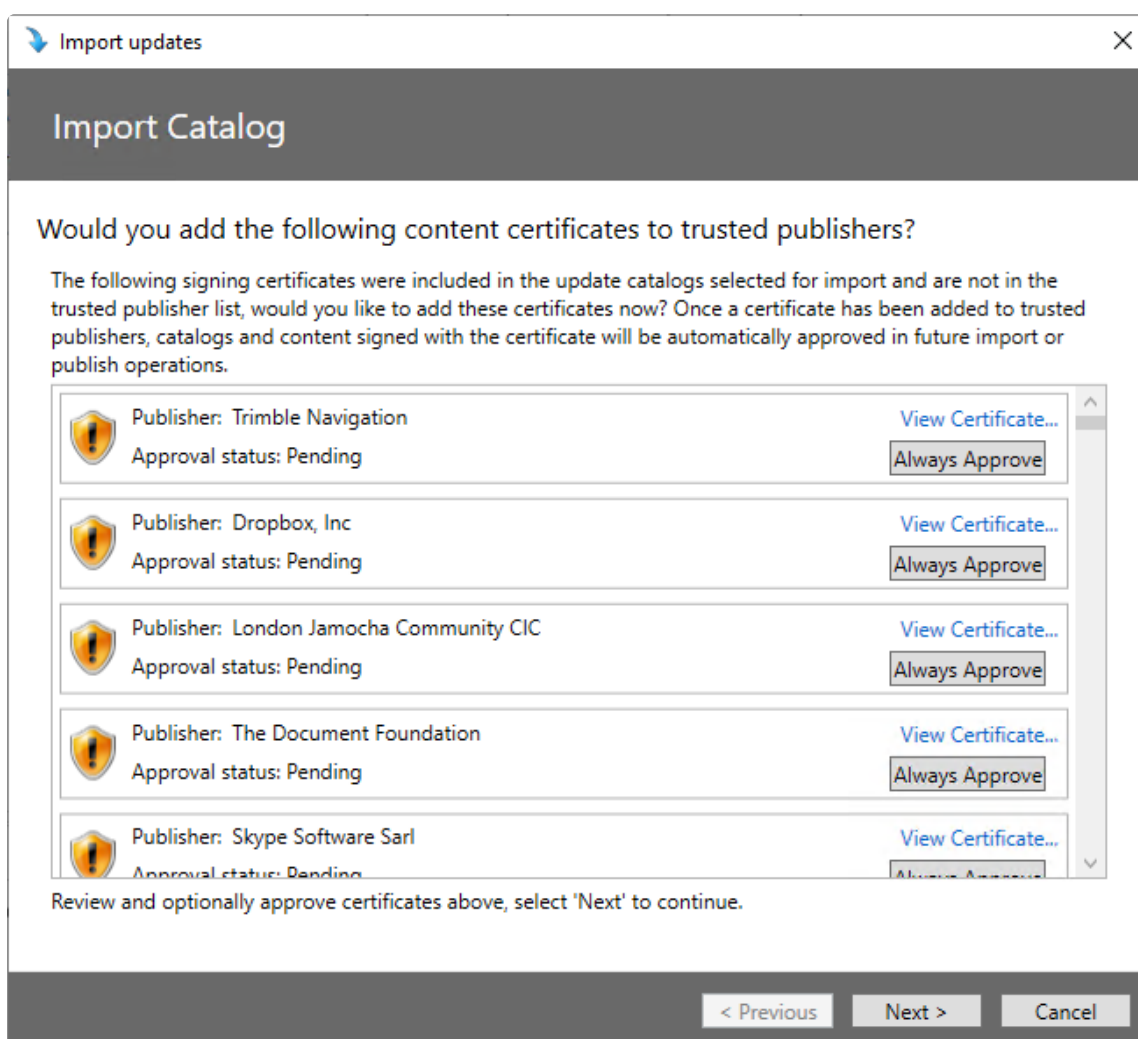
Click **Next** to progress.



Updates Publisher - Import catalog

At the next dialogue you can review and individually **Always Approve** certain third party product code signing certificates used to sign their installers (if any), or you can do a bulk one-time approval for all by clicking on **Next**. SCUP will then begin importing all updates into SCUP (not WSUS/ConfigMgr).

- i** If you receive any errors while importing or downloading the catalog, the **UpdatesPublisher.log** file located in your user's **%temp%** directory will be useful for troubleshooting possible connectivity failures to **patchmypc.com**.



Once complete, you will see the Patch My PC category on the left-hand side containing all updates in the catalog.

The screenshot shows the 'System Center Updates Publisher (Administrator)' window. The left sidebar contains a tree view with 'Overview', 'All Software Updates', 'Patch My PC', and 'SCUP Updates' (selected). The main pane displays a table of updates under the heading 'All Patch My PC SCUP Updates software updates (585)'. The table has columns: Name, Update Type, Classification, Severity, Article ID, Bulletin ID, and CVE ID. Below the table is an 'Update Details' section. The bottom status bar shows 'CM Server: Local' and 'Update Server: Local'.

Name	Update Type	Classification	Severity	Article ID	Bulletin ID	CVE ID
1Password 7.7.819 (User)	Update	Update	Moderate	PMPC-2021-0	PMPC-2021-0	
7-Zip 19.00 (EXE-x64)	Update	Update	Moderate	7Z-19.00-EXE	7Z-19.00-EXE	
7-Zip 19.00 (EXE-x86)	Update	Update	Moderate	7Z-19.00-EXE	7Z-19.00-EXE	
7-Zip 19.00 (MSI-x64)	Update	Update	Moderate	7Z-19.00-MSI	7Z-19.00-MSI	
7-Zip 19.00 (MSI-x86)	Update	Update	Moderate	7Z-19.00-MSI	7Z-19.00-MSI	
8x8 Work 7.11.4.3 (MSI-x64)	Update	Update	Moderate	PMPC-2021-0	PMPC-2021-0	
Adobe Acrobat DC Update 15.006.30527	Update	Security	Critical	APSB20-48	APSB20-48	CVE-2020-9
Adobe Acrobat DC Update 17.011.30202	Update	Security	Critical	PMPC-2021-0	PMPC-2021-0	CVE-2021-3
Adobe Acrobat DC Update 20.004.30015	Update	Security	Critical	PMPC-2021-0	PMPC-2021-0	CVE-2021-3
Adobe Acrobat DC Update 21.007.20095	Update	Update	Moderate	PMPC-2021-0	PMPC-2021-0	
Adobe Acrobat Reader DC - MUI Update 15.006.30	Update	Security	Critical	APSB20-48	APSB20-48	CVE-2020-9
Adobe Acrobat Reader DC - MUI Update 17.011.30	Update	Security	Critical	PMPC-2021-0	PMPC-2021-0	CVE-2021-3
Adobe Acrobat Reader DC - MUI Update 20.004.30	Update	Security	Critical	PMPC-2021-0	PMPC-2021-0	CVE-2021-3

Updates Publisher - Patch My PC updates

Updating the Catalog

The section will detail the process to update the catalogue in SCUP.

In order to publish newer releases/versions of third party updates into your environment, you need to update the Patch My PC catalogue in SCUP. This section will detail the process to update SCUP with the latest Patch My PC catalogue.

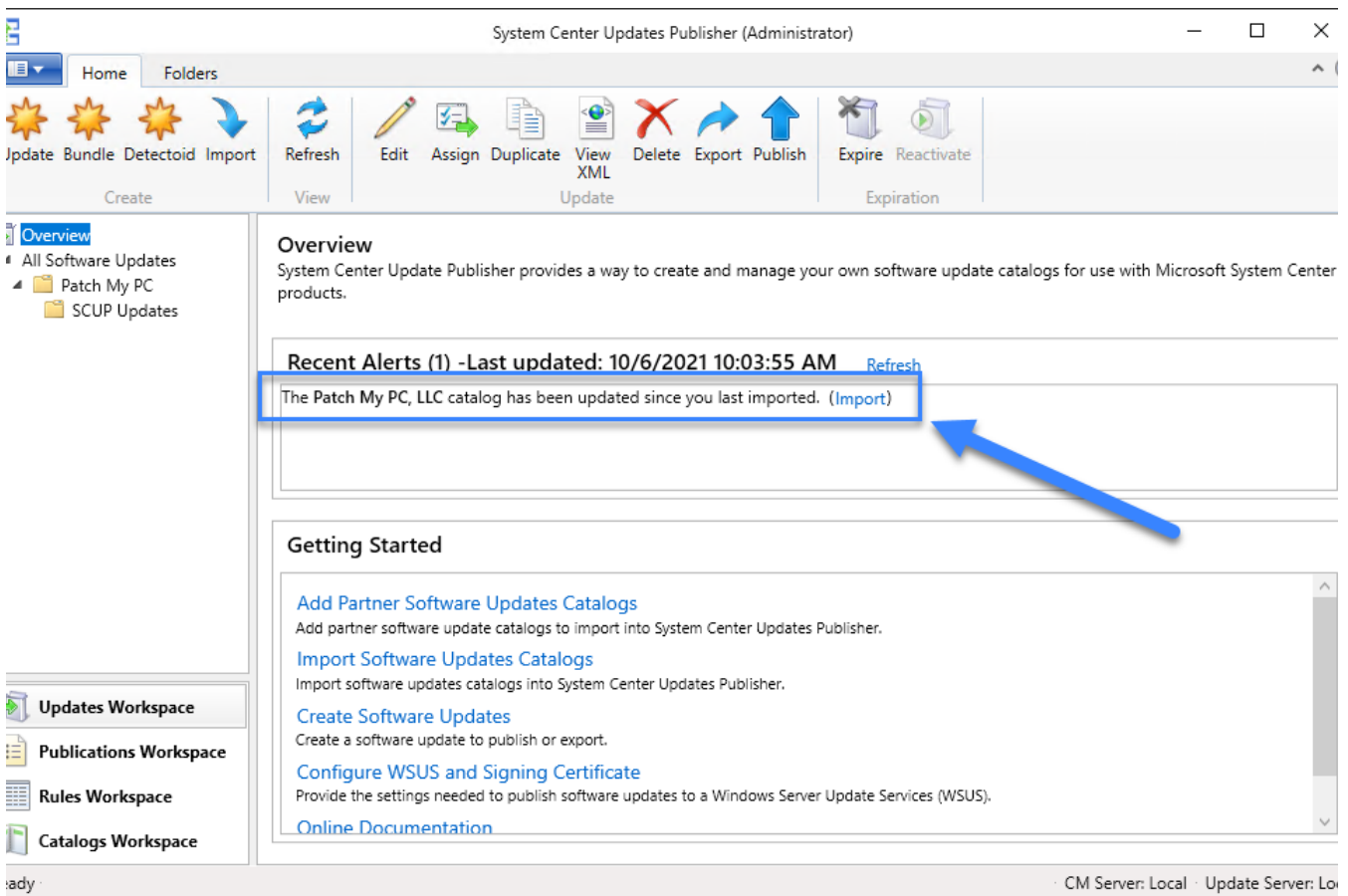
We typically update our catalogue atleast once a day, usually excluding weekends. See more information about this in our FAQ: [What is the Turnaround Time for Third-Party Software Updates to be Added to the Catalog?](#)

You can also subscribe to an email newsletter or RSS feed to be informed when we do update our catalog.

<https://patchmypc.com/category/catalog-updates/feed>

If a new catalogue has been released, upon opening SCUP you will be notified if a newer version of our catalogue is available.

i To catalogue comparison process is logged in **UpdatesPublisher.log**. This file is located in your user's **%temp%** directory.



Updates Publisher - New catalogue update available

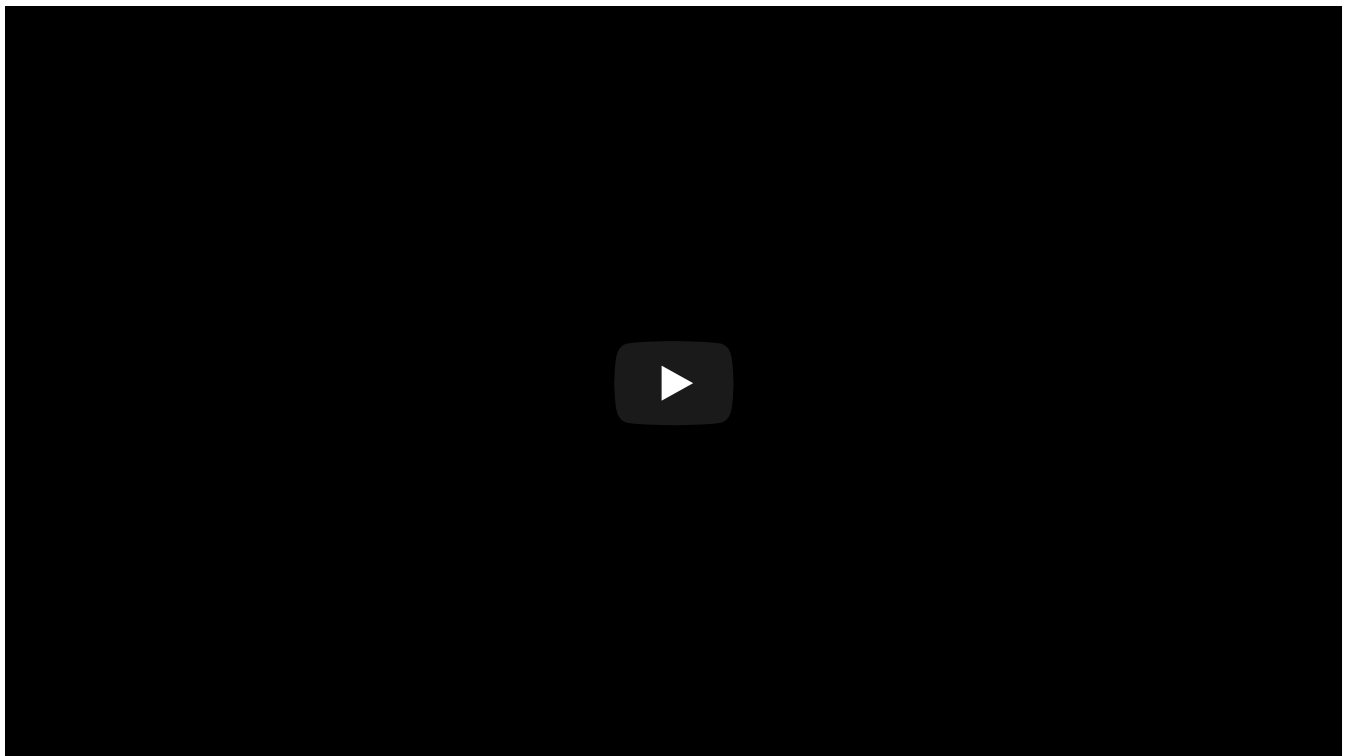
Clicking on **Import** will bring up **Import Catalog** wizard. Complete this wizard using the same process as detailed in the previous **Importing the Catalog** section to update SCUP with the new Patch My PC catalog.

i If you receive any errors while importing or downloading the catalog, the **UpdatesPublisher.log** file located in your user's **%temp%** directory will be useful for troubleshooting possible connectivity failures to **patchmypc.com**.

Removing Expired Updates

This section will detail the process for removing expired updates from SCUP.


The below video will show you how to clean up and correctly handle expired updates in SCUP.




Publishing Updates

This section will detail publishing updates from SCUP into WSUS and Configuration Manager.

At this point, you should have the Patch My PC catalog imported and see third party updates in the SCUP console.

-  Ensure you have connected SCUP to WSUS and Configuration Manager.
In the bottom right-hand corner of the SCUP console, it should **not** read "Not Configured" for **CM Server** and **Update Server**.
To configure the connection to WSUS and Configuration Manager, follow the steps in the [Connecting to WSUS and Configuration Manager](#) section of this document.

In order to publish updates to WSUS, you can select one or more updates and select **Publish** via either right clicking or via the ribbon along the top. Complete the wizard by choosing to publish with **Full Content**. You will be asked to verify and trust the certificate (if any) used to sign the installer. You can choose between **Ask me every time** or **Always accept content signed by this publisher** to save your preference.

-  If you receive any errors while publishing updates, the **UpdatesPublisher.log** file located in your user's **%temp%** directory will be useful for troubleshooting.

System Center Updates Publisher (Administrator)

Home Folders

Update Bundle Detectoid Import Refresh Edit Assign Duplicate View XML Delete Export Publish Expire Reactivate

Overview
All Software Updates
Patch My PC
SCUP Updates

All Patch My PC SCUP Updates software updates (585)

Name	Update Type	Classification	Severity	Article ID	Bulletin ID	CVE ID
1Password 7.7.819 (User)	Update	Update	Moderate	PMPC-2021-0	PMPC-2021-0	
7-Zip 19.00 (EXE-x64)	Update	Update	Moderate	7Z-19.00-EXE	7Z-19.00-EXE	
7-Zip 19.00 (EXE-x86)	Update	Update	Moderate	7Z-19.00-EXE	7Z-19.00-EXE	
7-Zip 19.00 (MSI-x64)	Update	Update	Moderate	7Z-19.00-MSI	7Z-19.00-MSI	
7-Zip 19.00 (MSI-x86)	Update	Update	Moderate	7Z-19.00-MSI	7Z-19.00-MSI	
8x8 Work 7.11.4.3 (MSI-x64)	Update	Update	Moderate	PMPC-2021-0	PMPC-2021-0	
Adobe Acrobat DC Update 15.006.30527	Update	Security	Critical	APSB20-48	APSB20-48	CVE-2020-9
Adobe Acrobat DC Update 17.011.30202	Update	Security	Critical	PMPC-2021-0	PMPC-2021-0	CVE-2021-3
Adobe Acrobat DC Update 20.004.30015	Update	Security	Critical	PMPC-2021-0	PMPC-2021-0	CVE-2021-3
Adobe Acrobat DC Update 21.007.20095	Update	Update	Moderate	PMPC-2021-0	PMPC-2021-0	
Adobe Acrobat Reader DC - MUI Update 15.006.30	Update	Security	Critical	APSB20-48	APSB20-48	CVE-2020-9
Adobe Acrobat Reader DC - MUI Update 17.011.30	Update	Security	Critical	PMPC-2021-0	PMPC-2021-0	CVE-2021-3
Adobe Acrobat Reader DC - MUI Update 20.004.30	Update	Security	Critical	PMPC-2021-0	PMPC-2021-0	CVE-2021-3

Update Details
7-Zip 19.00 (MSI-x64)
Encryption strength for 7z archives was increased: the size of random initialization vector was increased from 64-bit to 128-bit, and the pseudo-random...

Update Status
Date modified: 3/17/2020 1:31:26 AM Date published: 10/5/2021 11:54:51 AM

Summary Installable Rules Installed Rules Supersedes Prerequisites

CM Server: Local Update Server: Local

Updates Publisher - Publishing an update

✓ At this point, the newly published update(s) will be in WSUS.

Next, in order to pull these updates in from WSUS to your Configuration Manager environment ready for deployment, you need to:

1. Synchronise your Software Update Point (SUP)
2. Enable the new Patch My PC vendor category on your SUP Products list
3. Sync the SUP once more to actually start pulling in the third party updates

Start off by starting a sync of your SUP by opening the Configuration Manager console. Navigate to the **Software Library**, expand the **Software Updates** folder, and either right click on **All Software Updates** and choose **Synchronize Software Updates**, or left click and choose to synchronise from the top ribbon.

Microsoft Endpoint Configuration Manager (Connected to P01 - Patch My PC 1)

Home Folder

Synchronize Software Updates Run Summarization Schedule Summarization Saved Searches Download Create Software Update Group Edit Membership Review License Publish Third-Party Software Update Content Deployment Move Properties

Software Library Overview Software Updates All Software Updates 556 items

Search

Icon	Title	Article ID	Required	Installed
	2017-05 Cumulative Update for Windows 10 for x64-based Systems (KB4019474)	4019474	0	0

2017-05 Cumulative Update for Windows 10 for x64-based Systems (KB4019474)	4019474	0	0
2017-06 Update for Windows 10 Version 1607 for x64-based Systems (KB3150513)	3150513	0	0
2017-06 Update for Windows 10 Version 1607 for x86-based Systems (KB3150513)	3150513	0	0
2017-06 Update for Windows Server 2016 for x64-based Systems (KB3150513)	3150513	0	0
2017-08 Update for Windows 10 Version 1511 for x64-based Systems (KB4035632)	4035632	0	0
2017-08 Update for Windows 10 Version 1511 for x86-based Systems (KB4035632)	4035632	0	0
2018-02 Cumulative Update for Windows 10 Version 1511 for x64-based Systems (KB4074591)	4074591	0	0
2018-02 Cumulative Update for Windows 10 Version 1511 for x86-based Systems (KB4074591)	4074591	0	0
2018-03 Cumulative Update for Windows 10 Version 1511 for x64-based Systems (KB4088779)	4088779	0	0
2018-03 Cumulative Update for Windows 10 Version 1511 for x86-based Systems (KB4088779)	4088779	0	0
2018-03 Cumulative Update for Windows Server 2016 (1709) for x64-based Systems (KB4090913)	4090913	0	0
2018-03 Cumulative Update for Windows Server Next for x64-based Systems (KB4087658)	4087658	0	0
2018-03 Update for Windows Server Next for x64-based Systems (KB4087657)	4087657	0	0
2018-04 Cumulative Update for Windows 10 Version 1511 for x64-based Systems (KB4093109)	4093109	0	0
2018-04 Cumulative Update for Windows 10 Version 1511 for x86-based Systems (KB4093109)	4093109	0	0

2017-05 Cumulative Update for Windows 10 for x64-based Systems (KB4019474)

Configuration Manager - Synchronise software updates with WSUS

⚠ Do not progress until the SUP sync is complete. You can monitor wsyncmgr.log for its progress.

Once the SUP sync is complete, enable the Patch My PC product category in your SUP's component properties in Configuration Manager. Do this by opening the Configuration Manager console, and navigate to **Administration**, **Sites**, right click on your site to **Configure Site Components**, and select **Software Update Point**.

Microsoft Endpoint Configuration Manager (Connected to P01 - Patch My PC 1)

Home | Hierarchy Settings | Saved Searches | Add Site System Roles | Create Site System Server | Create Secondary Site | Retry Secondary Site | Recover Secondary Site | Upgrade | Show Install Status | Refresh | Delete | Manage Content Library | Settings | Set Security Scopes | Properties

Administration > Overview > Site Configuration > Sites

Sites 1 items

Icon	Name	Type	Server Name	State	Site Code	Parent Site Code
	P01 - Patch My PC 1	Primary site	PMP1-CM01.contoso1.local	Site Active	P01	

Context menu options for P01 - Patch My PC 1:

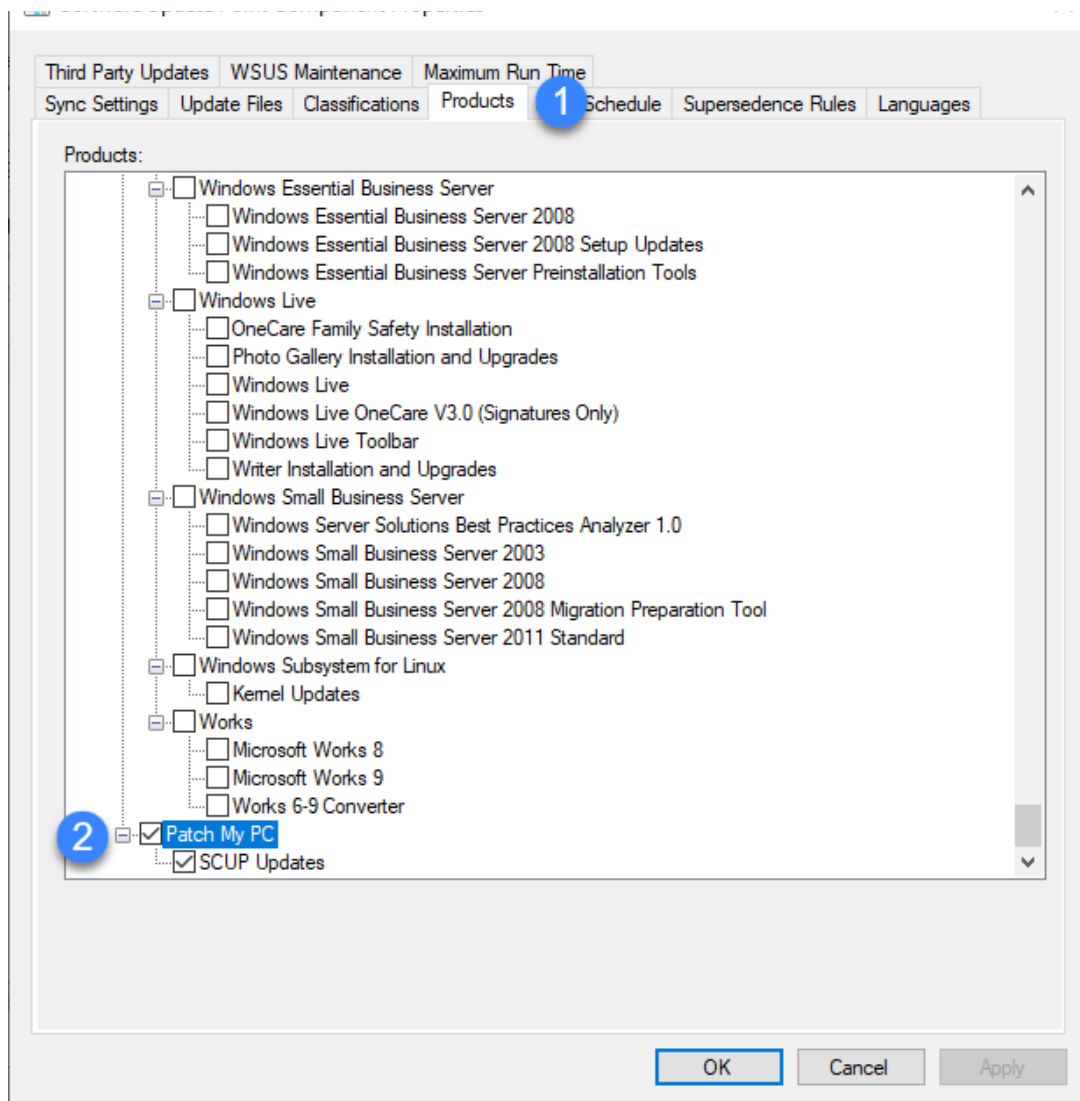
- Add Site System Roles
- Create Site System Server
- Create Secondary Site
- Retry Secondary Site
- Recover Secondary Site
- Upgrade
- Show Install Status
- Refresh
- Delete
- Manage Content Library
- Configure Site Components
- Client Installation Settings
- Site Maintenance
- Status Summarizers
- Status Filter Rules
- Set Security Scopes
- Properties

Sub-menu for Configure Site Components:

- Software Distribution
- Software Update Point
- Operating System Deployment
- Management Point
- Status Reporting
- Email Notification
- Collection Membership Evaluation

Configuration Manager - Configure SUP's component properties

Change to the **Products** tab, and scroll down to enable **Patch My PC**. Click **OK**.

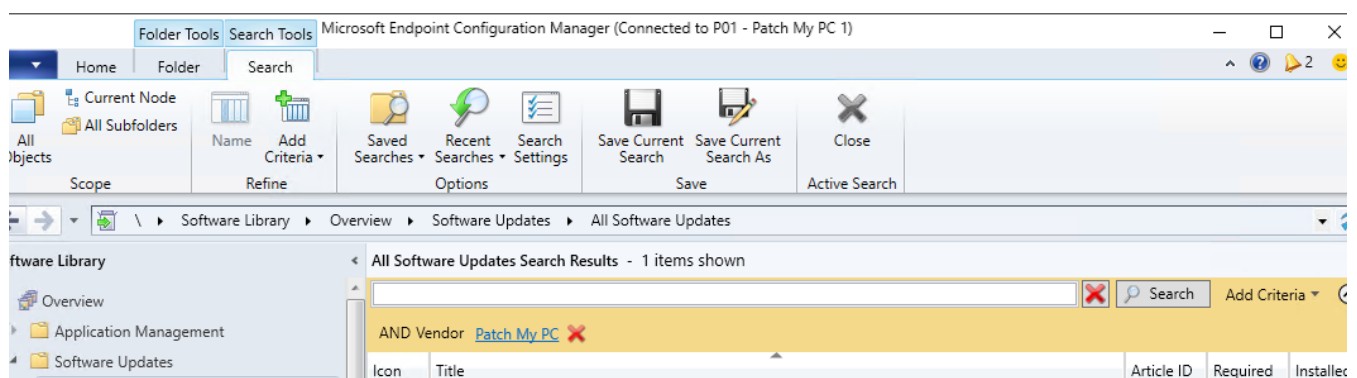


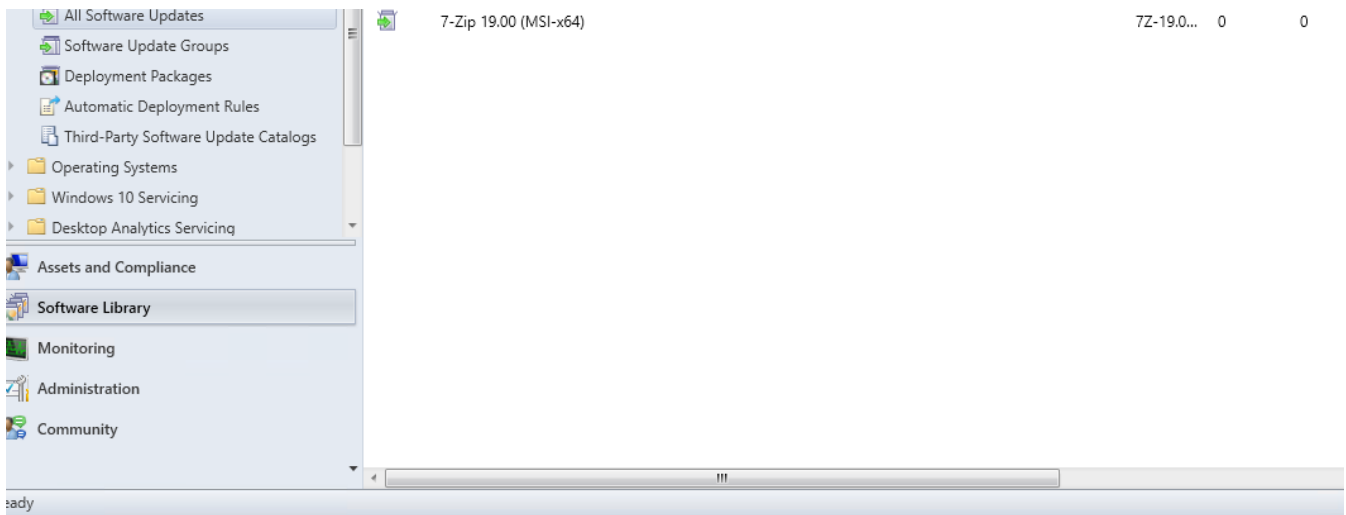
Configuration Manager - Enable Patch My PC vendor category

Finally, synchronise your SUP once more and wait until the sync is complete. Once the sync is complete, you should then see third party updates published from SCUP.

At this point, updates now showing up in Configuration Manager console are ready to deploy.

⚠ Ensure your devices trusted the code signing certificate used to sign the updates from SCUP. Refer back to the previous section [Code Signing Certificate](#) of this document for more details on this requirement, and also [Deploying the Code Signing Certificate](#) for an example on how to do this using Group Policy.





Configuration Manager - Showing third party updates in console

i Your SUP will need to synchronise each time you publish new updates to WSUS from SCUP.

Publishing Updates in Publication Groups

It is possible to create publication groups in SCUP and this enables you to logically group updates in SCUP before publishing. This is an alternative method to publishing updates individually or by multi-selecting and publishing.

For example, let's say we want to create a group of all updates released on a particular day or spanned across several days, and then bulk-publish that group and all its updates as Full Content.

In SCUP, sort the column **Date Modified** in descending order and multi-select all updates released on the date or timespan of your choice. Right click and choose **Assign**.

Name	Update Type	Classification	Severity	Article ID	Bulletin ID	CVE ID	Expired	Date Modified
Remote Desktop Manager Enterprise 2021.2.14.0	Update	Update	Moderate	PMPC-2021-1	PMPC-2021-1		No	10/5/2021
Remote Desktop Manager Free 2021.2.14.0	Update	Update	Moderate	PMPC-2021-1	PMPC-2021-1		No	10/5/2021
Paint.NET 4.3.2 (x86)	Update	Update	Moderate	PMPC-2021-1	PMPC-2021-1		No	10/5/2021
Paint.NET 4.3.2 (x64)	Update	Update	Moderate	PMPC-2021-1	PMPC-2021-1		No	10/5/2021
Opera 80.0.4170.16 (x86)	Update	Update	Important	PMPC-2021-1	PMPC-2021-1		No	10/5/2021
Opera 80.0.4170.16 (x64)	Update	Update	Important	PMPC-2021-1	PMPC-2021-1		No	10/5/2021
OpenVPN 2.5.22 (x64)	Update	Update	Moderate	PMPC-2021-1	PMPC-2021-1		No	10/5/2021
OBS Studio 27.1.3 (x64)	Update	Update	Moderate	PMPC-2021-1	PMPC-2021-1		No	10/5/2021
Mozilla Firefox ESR 78.15.0 (x86 it)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021
Mozilla Firefox ESR 78.15.0 (x64 it)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021
Mozilla Firefox 93.0.0 (x86 it)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021
Mozilla Firefox 93.0.0 (x64 it)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021
Mozilla Firefox ESR 78.15.0 (x86 ru)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021
Mozilla Firefox ESR 78.15.0 (x64 ru)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021
Mozilla Firefox 93.0.0 (x86 ru)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021
Mozilla Firefox 93.0.0 (x64 ru)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021
Mozilla Firefox ESR 78.15.0 (x86 da)	Update	Update	Critical	PMPC-2021-1	PMPC-2021-1	CVE-2021-384	No	10/5/2021

Update Details			
Severity:	Moderate	Package size:	171.90 MB
Bulletin ID:	PMPC-2021-10-05	Download URL:	https://cdn.devolution.net/download/...
Article ID:	PMPC-2021-10-05	Support URL:	https://remotedesktopmanager.com/support
CVE ID:		More Info URL:	https://remotedesktopmanager.com/release-notes

Updates Publisher - assign multiple updates to a group

Choose your publication type (e.g. **Full Content**) and name the publication group accordingly.

Assign updates to a publication

Assign Software Updates

Assign software updates to an existing or new publication

Assign software updates to a publication for group publishing and exporting. A software update can be associated with more than one publication. To publish or export a publication, use the Publication workspace.

Select the publication type for the selected software updates

Full Content

☐ Assign software updates to an existing publication

☒ Assign software updates to a new publication

2021-10 Week 1 Updates

OK Cancel

Updates Publisher - Assign updates to a publication

In the **Publications Workspace**, you will now see your new group. Right clicking on the group name in the left pane and choosing **Publish** will enable you to publish the entire group in bulk.

System Center Updates Publisher (Administrator)

Home Publication

Export Publish Refresh Automatic Full Content Metadata Only Remove

Publication View Publication Type Update

021-10 Week 1 Updates

2021-10 Week 1 Updates member updates (44)

Rename Delete Publish

Publish updates in the selected publication.

	Publish Option	Expired	Classification	Severity	Update Type	Date Modified	Date Published
Mozilla Firefox 93.0.0 (x64 da)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x64 es-ES)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x64 fr)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x64 it)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x64 nl)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x64 ru)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x86 da)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x86 de)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x86 en-GB)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x86 en-US)	Full Content	No	Security	Critical	Update	10/5/2021	
Mozilla Firefox 93.0.0 (x86 es-ES)	Full Content	No	Security	Critical	Update	10/5/2021	

Update Details

Updates Workspace

Publications Workspace

Deploying Updates

This section will detail how to deploy the newly published updates in Configuration Manager

The below video will show you how to deploy software updates in Configuration Manager for updates published by SCUP.

