## Publishing Service Setup Guide

### Document Versions:

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 07, 2018</td>
<td>1.0</td>
<td>Initial Release</td>
</tr>
<tr>
<td>July 08, 2018</td>
<td>1.1</td>
<td>New Features Included</td>
</tr>
<tr>
<td>September 30, 2018</td>
<td>1.2</td>
<td>New Features Included</td>
</tr>
<tr>
<td>February 14, 2019</td>
<td>1.3</td>
<td>New Features Included</td>
</tr>
<tr>
<td>April 10, 2019</td>
<td>1.4</td>
<td>New Features Included</td>
</tr>
<tr>
<td>July 12, 2019</td>
<td>1.5</td>
<td>Application Feature Included</td>
</tr>
<tr>
<td>February 07, 2020</td>
<td>1.6</td>
<td>New Features Included</td>
</tr>
<tr>
<td>March 03, 2020</td>
<td>1.7</td>
<td>User Interface Changes</td>
</tr>
</tbody>
</table>
**System Requirements:**

- Must be installed on top-most WSUS/SUP
- Microsoft .NET Framework 4.5
- Supported Operating Systems
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- If using WSUS 3.0 SP2 (Server 2008/2008 R2), you should install [KB2938066](https://support.microsoft.com/en-us/help/2938066) on all WSUS servers in your environment.

**Download** the latest MSI installer of the publishing service using the following URL:

https://patchmypc.com/publishing-service-download

Start the installation by **double-clicking** the downloaded MSI.

**Note:** Depending on user account control settings, you may need to run an elevated command prompt and launch the MSI from the command prompt.

Click **Next** in the **Welcome Wizard**

Click **Next** in the **Installation Folder Dialog**

**Optionally,** you can change the installation folder by clicking **Browse**...

Click **Install** on the **Ready to Install** dialog.

**Note:** if user-account control is enabled, you will receive a prompt “Do you want to allow this app to make changes to your device?” Click **Yes** on this prompt to allow installation.
If you are configuring the product for Microsoft Intune Win32 application publishing only, you should review our separate installation guide for Microsoft Intune.

For a Configuration Manager setup, leave the checkbox Enable Microsoft Intune standalone mode un-checked.

Leave the “Launch Patch My PC Publishing Service” checked then click Finish.

Note: if user-account control is enabled, you will receive a prompt “Do you want to allow this app to make changes to your device?” Click Yes on this prompt to allow installation.

If you already purchased a license or have a 30-day full trial, paste your catalog URL and click the Validate URL button.

Access to https://patchmypc.com is required. If required, configure a web proxy in the Advanced tab first. For activation errors, please review Troubleshooting License Activation Issues.
If you want to configure the publishing service in **public trial mode**, click the “Use Trial Mode” checkbox.

Click **Yes** on the prompt to enable trial catalog mode.

When the **public trial mode** is enabled, the “Updates” “ConfigMgr Apps” and “Intune Apps” tab will filter to only show products available from the **public trial catalog**.

**Note:** If you need all products for evaluation purposes, please **submit the full-trial request form**.

To publish software updates to WSUS, a WSUS signing certificate (Code-Signing) must be configured.

The certificate can be **self-signed** or issued by a third-party or even internal certificate authority.

**Certificate Option 1 - SCCM Managed:**

If you are running **SCCM 1806** or newer, you can enable the option for “**Configuration Manager manages the certificate**”. If enabled, SCCM will automatically generate the signing certificate during the next software update point sync. You can monitor `wscyncmrg.log` to see it created.

You will need to **reopen** the publishing service after SCCM creates the certificate for the certificate validation.

**Note:** if your software update point is remote from the site server, **WSUS needs to be configured in HTTPS**.

**Certificate Option 2 - Self-Signed:**

To use a self-signed certificate, Click the “**Generate a Self-Signed Certificate**” button, then click “**OK**”.

---

Patch My PC – Publishing Service Setup Guide
Certificate Option 3 - PKI:

If you want to use a publicly created code-signing certificate, Click the “Import PFX Certificate” button and follow any password prompts.

Note: We have a detailed PFX certificate guide available [here](#).

The catalog status image should show a green checkbox and display the code-signing certificate’s expiration date.

We use DigiCert for timestamping published third-party software updates.

If you want to use a different timestamping server, you can un-check Use Default and enter your desired timestamping HTTP Server URL.

For clients to install third-party updates, they must trust the code-signing certificate.

If you enabled the option Configuration Manager manages the certificate from the previous step, your SCCM clients would automatically trust the WSUS signing certificate.

If you aren’t on SCCM 1806+ or can’t enable this option due to HTTPS requirements if your SUP is remote from the site server, you need to follow our supplemental guide [here](#) for deploying the WSUS signing certificate and trusted third-party update using GPO.
For clients to install third-party updates, they must also have a policy enabled to trust third-party updates.

If you are running SCCM 1802+, set the client setting to “Enable third party updates = Yes”.

If you aren’t on SCCM 1802+, you need to follow our supplemental guide for deploying the GPO.

Click the Update tab to enable products for software update publishing.

Arrows can be used to expand or collapse products.

Database Search can be used to scan SCCM products already installed product and enable detected products.

Search can be used to find products and vendors by name

Note: when the trial mode is enabled, you will only see a subset of products.

If using the scan SCCM feature, you need to provide the SCCM database server name and database name.

Click Query to start the search then choose the products you want to enable for publishing by clicking Enable Selected Products or Cancel.

You can also click the Export button if you want to export the list of detected products to a CSV.

Note: this requested the user to have db_datareader rights in SQL to the SCCM database.
You can configure **scanning of products** for software updates or applications to automatically enable before any synchronization based on the product(s) being detected on a certain number of devices in Configuration Manager based on hardware inventory.

Auto-enabling detected products is helpful when new products are added to the catalog, and you don’t want to enable products within the publisher manually.

You can **right-click “All Products” or specific “Vendor/Product”** and toggle between **Metadata** and **Full Content**.

**Full Content** – publishes the full content of the update to WSUS. Full-content includes metadata and the update binaries and is **required to download and deploy the update in WSUS/SCCM**.

**Metadata only** – publish only the metadata; update binaries are not published.

**Metadata only** allows you to view the compliance details in SCCM/WSUS for the update, but you will be unable to deploy unless it’s **re-published with full-content**.
**Auto Kill:** application processes will be auto-closed before the update installs.

**Skip Update:** skip an update if the app is running, will retry at next software update deployment and eval cycle.

**Pre/Post Scripts:** run your own custom pre/post scripts for a product.

**Command Lines:** add custom command lines when needed.

**Republish Update(s):** see [When, Why, and How to Republish Update(s)]

For a detailed description of each right-click option, please see [Custom Options Available for Third-Party Updates and Applications]

For the [Enterprise Plus] subscription, you can enable the option to create SCCM applications in the ConfigMgr Apps tab.

These applications can be deployed using existing SCCM deployment methods like collection deployments and task sequences.
If you enable the option **Automatically create applications**, you will need to click the **Options** button to configure additional options required for application creation.

**SMS Provider Server:** The server name of your SMS Provider.

**Source Folder (UNC):** The network path used for application source files. The service will create a subfolder named `Applications` in the root of the path defined. Application content will be created in a `<Vendor>`\ `<Product>`\ `<ID>` structure.

**Application Creation Options:** Application attributes that you can configurable.

**Content Distribution Options:** Options for automatic content distribution.

**Detection Method:** The application’s detection method uses a PowerShell script. The script is signed using the WSUS Signing Certificate by default. The **PowerShell execution** must allow **AllSigned** scripts.

Optionally, you can **automatically enable products** in the **Applications** tab that you previously enabled in the **Updates** tab by clicking the **Copy icon**.

You can also choose whether you want to copy any **custom right-click options** enabled in the Update Rules products by using the Yes or No dialog prompt.

You can review the following **supplemental video guide** for enabling the base installation feature within the publishing service.
Click the **Sync Schedule** tab and adjust the schedule as needed.

The **scheduling time** is when the publishing service will download the latest catalog metadata and **auto-publish new updates** and **applications** for **enabled products**.

The **default schedule** is **Daily at 7 PM**

You can also configure the publishing service to **sync the SCCM software update point** if new third-party updates are published (Requires SUP to be co-located on the site server).

Optionally, you can enable **Notifications** in the **Alerts** tab.

To enable Email reports, click **Send Email Reports** and configure your SMTP sending options.

You can also paste a **Microsoft Teams webhook** to receive publishing alerts in a Microsoft Teams channel. See **Sending messages to connectors and webhooks** for more details.

We highly recommend enabling email reports, when emails are enabled, you will receive an email about any newly published updates **including Titles, Classification, Severity, CVE-ID’s, Catalog Expiration Details, and more**!

We recommend performing a **Test email** by clicking the **Test** button.

Click the **Apply** button to **save all changes**
**Modify Published Updates** performs various actions on published updates.

**Local Content Repository for Licensed Products** is used for products behind a paywall requiring a manual download. Please see this KB article for more details.

**SSRS Dashboard Reports** can be installed by clicking the Run Report Installer button.

**Standalone WSUS Mode**: This option should ONLY be used if you are deploying updates in WSUS and not using SCCM. When enabled, updates will be visible in the WSUS console.

In the About tab, you can view details about the publishing service.

You can disable the self-updates or opt-in to preview builds.

There are also a variety of helpful resources that are linked in the about tab including release notes, contact us, technical support email form, support forum, and request new products.
If you want to **start** the initial publishing of products, validate settings have been applied then click the Run Publishing Service Sync button in the **Sync Schedule** tab.

If **Run Now** is clicked, click OK on the “Run Now Successful” Message Box.

If you performed a **Run Now** Publishing, you could **monitor** the publishing process by clicking the Open PatchMyPC.log button in the **General Settings** tab.

Our log file uses a format compatible with **CMTrace.exe**.

We recommend setting **CMTrace.exe** as the **default log viewer**. It’s available in the SCCM Installation directory: `<InstallDir>\tools\cmtrace.exe`.

If you **enable email alerts** via SMTP, you will be sent an automated email whenever software updates or applications are **published**, **modified**, or **updated**.

When the first publishing operation is **completed**, we recommend that you run a “**Synchronize Software Updates**” on the SCCM site.

**Note:** You can monitor the software update point synchronization in the `wsyncmgr.log`.

---

**Patch My PC – Publishing Service Setup Guide**
Here is an example of the **wsyncmgr.log**.

You can verify the **synchronization is complete** when you see the line:

```
Sync time: 0d00h00m00s
```

Now that the **sync is complete**, you will need to **enable** the **Patch My PC** vendor in your software update point’s **Products tab**.

**Navigate** to the Administration Workspace > Site Configuration > Sites > Right-click your site > Configure Site Components > Click Software Update Point.

In the **Products tab**, enable the vendor named “Patch My PC” and **Click Apply** or **OK** to **Save** the settings.

If you run another “**Synchronize Software Updates**” on the SCCM site, the updates should **now be available** in the console after the sync is **complete**. You may need to click the **Refresh** button in the **All Software Updates** view.

**Note**: You can monitor the software update point synchronization in the **wsyncmgr.log**.

---

**Patch My PC – Publishing Service Setup Guide**
The setup of the publishing service is now **complete**!

Any newly released products meeting the criteria will be automatically published based on your **schedule**.

**Note:** If you are using **Automatic Deployment Rules** in SCCM. Filters:

- **Vendor** = Patch My PC
- **Superseded** = No
- **Classification** = Critical Updates, Security Updates, Updates

If you want to exclude specific products in your ADR, please refer to this guide **Filtering Specific Third-Party Products from ADRs**.

**Note:** Migration updates for Firefox to Firefox ESR or Java 6/7 to Java 8 are classified as “**Update Rollups**”.

If you want to receive email **notifications** regarding catalog updates, you can subscribe to our **update catalog newsletter**, and subscribe to our **RSS feed** that contains recent catalog updates.