



Patch My PC Microsoft Intune Setup Guide

Document Versions:

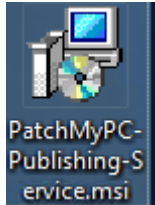
Date	Version	Description
February 07, 2020	1.0	Initial Release
March 03, 2020	1.1	User Interface Update

System Requirements:

- Microsoft .NET Framework 4.5
- Supported Operating Systems
 - Windows Server 2008
 - Windows Server 2008
 - Windows Server 2012
 - Windows Server 2012
 - Windows Server 2016
 - Windows Server 2019
 - Windows 10 (x64) – Microsoft Intune only

Prerequisites:

- When using Windows Server operating systems, WSUS should be installed and configured.
- If using Windows 10 client for Microsoft Intune only
 - Optional feature RSAT: Windows Server Updates Services Tools should be pre-installed



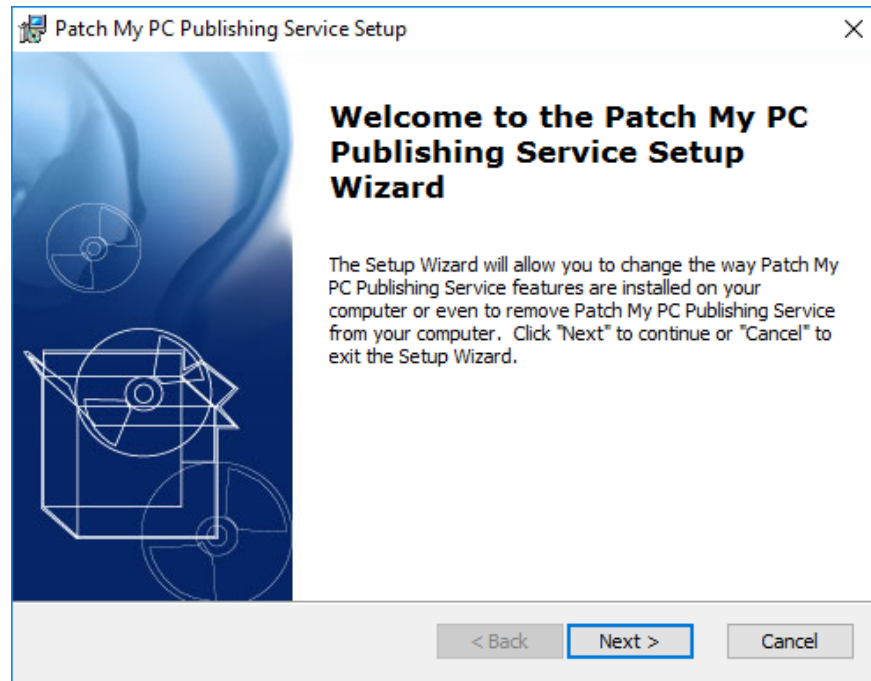
Download the latest **MSI installer** of the publishing service using the following URL:

<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.



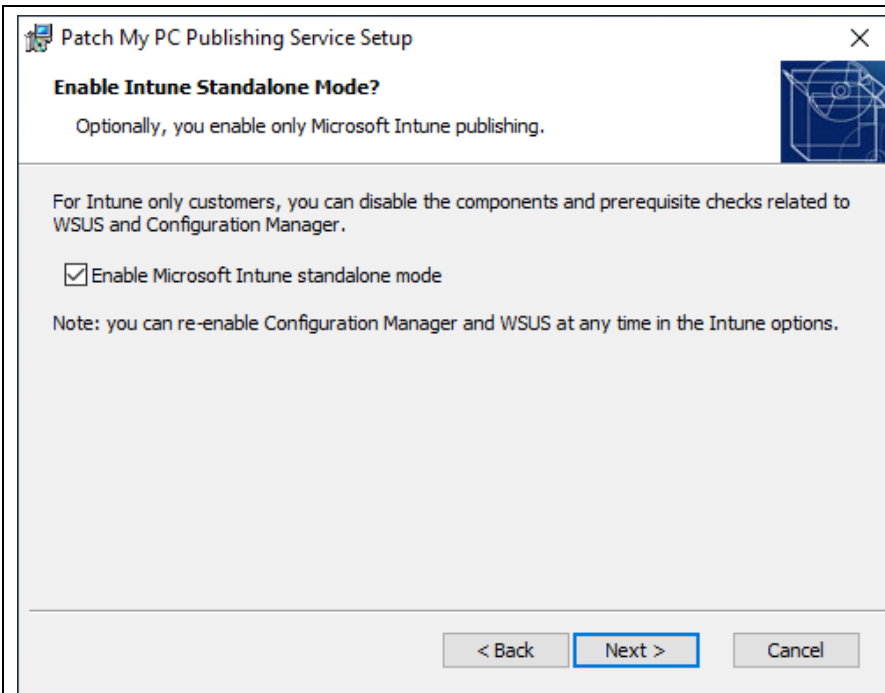
Click **Next** in the **Welcome Wizard**

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

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

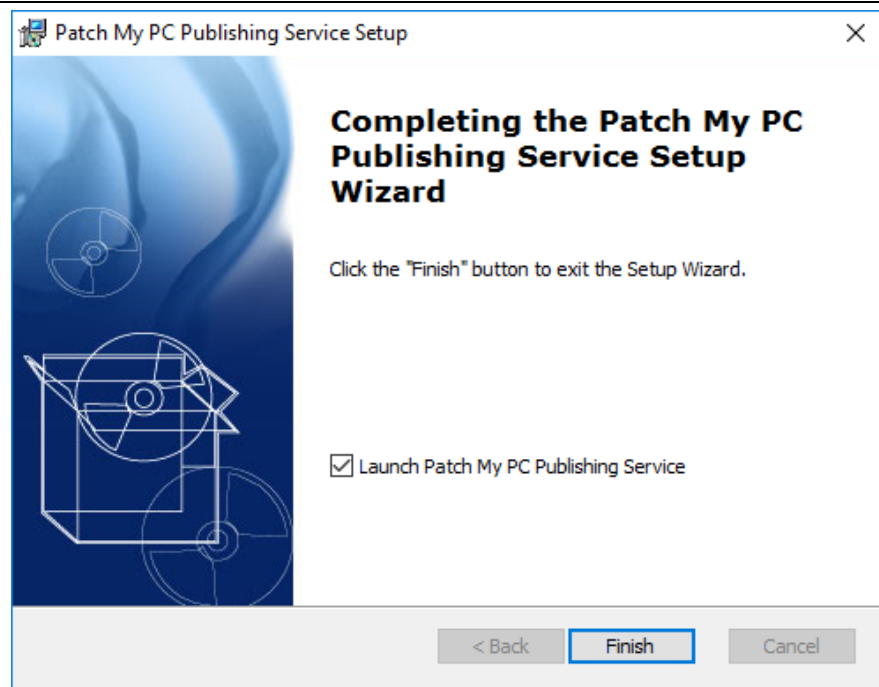
Click **Install** on the **Ready to Install** dialog.

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



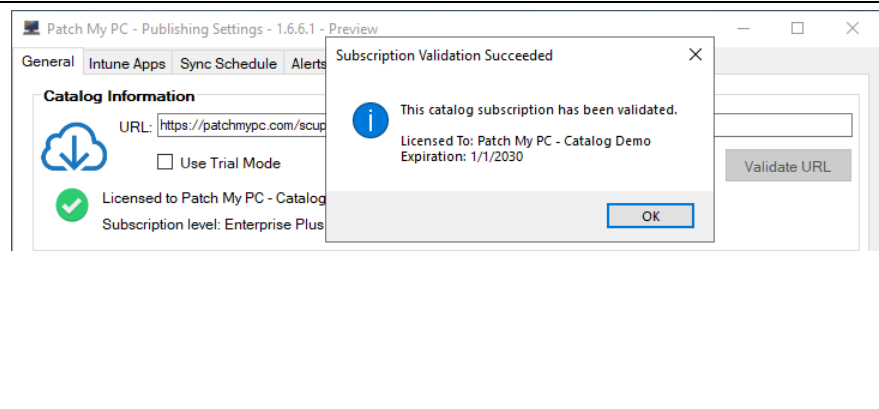
If you are configuring the product for **Intune Win32 application publishing only**, you can check **Enable Microsoft Intune standalone mode**

When this option is enabled, prerequisite checks related to WSUS and Configuration Manager are skipped.



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

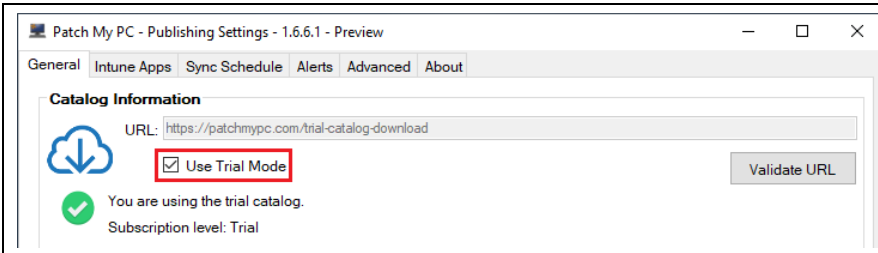
Note: if user-account control is enabled, you will receive a prompt “**Do you want to allow this app to make changes to your device?**” Click **Yes** on this prompt to allow installation



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

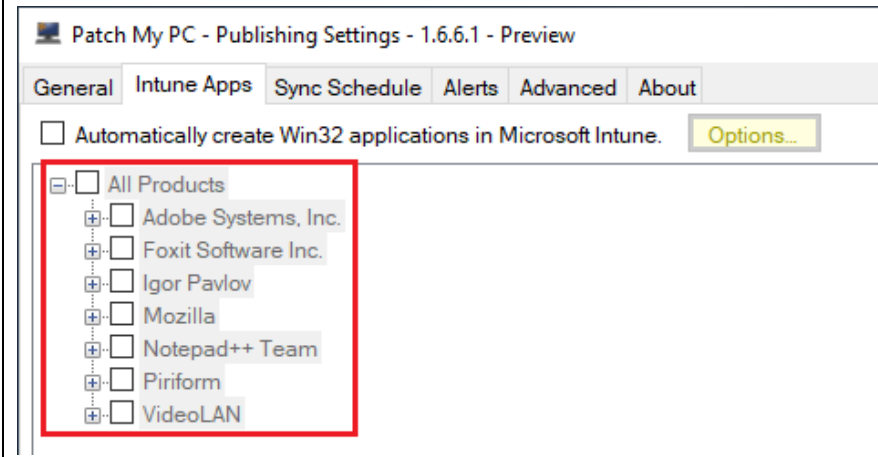
Access to <https://patchmypc.com> is required. If required, configure a web proxy in the **Advanced tab** first.

For activation errors, please review [Troubleshooting License Activation Issues](#)



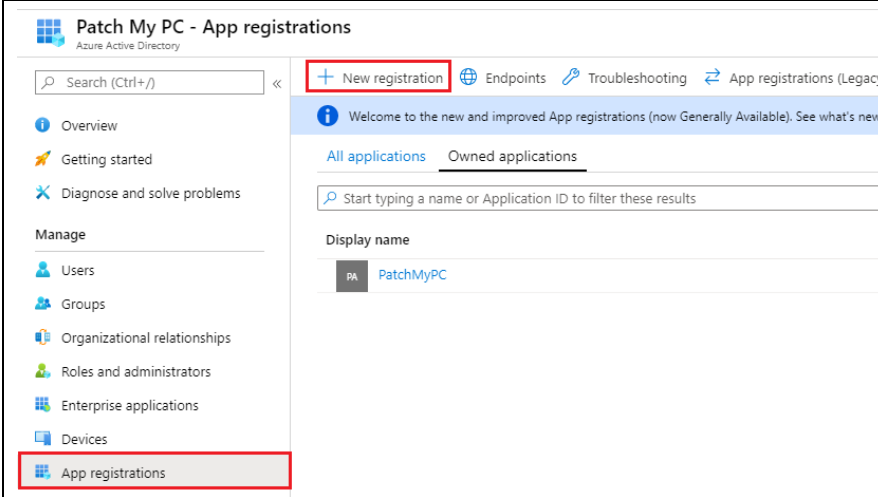
If you want to configure the publishing service in **public trial mode**, click the “**Use Trial Mode**” checkbox.

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



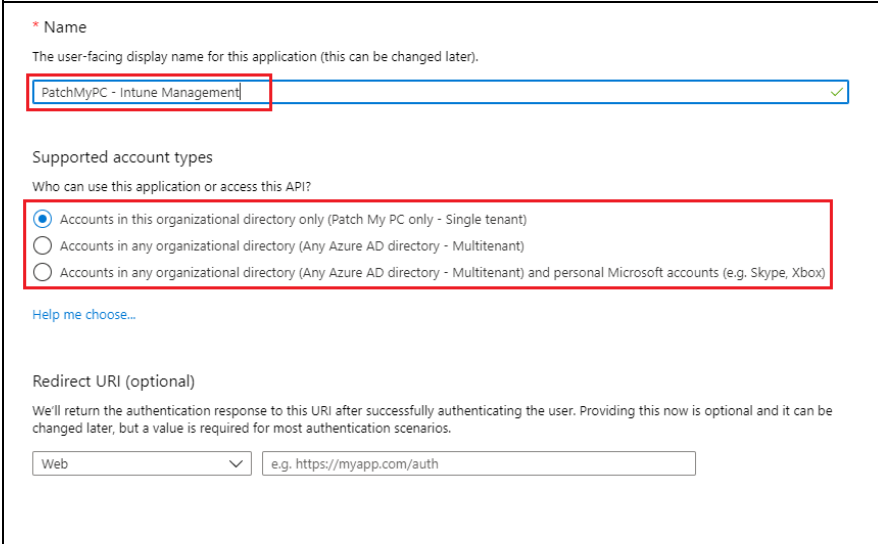
When the **public trial mode** is enabled, the “**Intune Apps**” tab will filter to only show subset products available in public trial mode.

Note: If you need additional applications for testing purposes, please **submit the full-trial request form**.



To delegate our service to have permissions to your Microsoft Intune tenant for application management, navigate to [Azure Ad App registrations](#).

Click **New registration**



Give your app registration a name such as “**PatchMyPC - Intune Management**”.

Configure the **account types** based on your tenant requirements. For this example, we will leave the default **Single tenant** option checked.

Please the Redirect URI default unless you have specific requirements for configuring the Redirect URI.

Click **Register**

<p>Manage</p> <ul style="list-style-type: none"> Branding Authentication Certificates & secrets Token configuration (preview) API permissions 	<p>Once created, navigate to the API permissions node.</p> <p>Next, we will need to delegate the required permissions for Intune application management.</p>																														
<p>Request API permissions</p> <p>< All APIs</p> <p>Microsoft Graph https://graph.microsoft.com/ Docs</p> <p>What type of permissions does your application require?</p> <div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid #ccc; padding: 5px; width: 45%;"> <p>Delegated permissions</p> <p>Your application needs to access the API as the signed-in user.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; width: 45%; background-color: #f9f9f9;"> <p>Application permissions</p> <p>Your application runs as a background service or daemon without a signed-in user.</p> </div> </div>	<p>In the API permissions node, click the button to Add a permission.</p> <p>In the right pane, choose Microsoft Graph and choose the option for Application permissions.</p>																														
<p>DeviceManagementApps (2)</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> DeviceManagementApps.Read.All Read Microsoft Intune apps <input checked="" type="checkbox"/> DeviceManagementApps.ReadWrite.All Read and write Microsoft Intune apps <p>Group (1)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Group.Create Create groups <input checked="" type="checkbox"/> Group.Read.All Read all groups 	<p>In the Permission dialog, you will need to enable the following permissions.</p> <p>Under the DeviceManagementApps toggle, enable:</p> <ul style="list-style-type: none"> - DeviceManagementApps.Read.All - DeviceManagementApps.ReadWrite.All <p>Under the Group toggle, enable:</p> <ul style="list-style-type: none"> - Group.Read.All <p>Click Add permissions</p>																														
<p>Configured permissions</p> <p>Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent</p> <p>+ Add a permission Grant admin consent for Patch My PC</p> <table border="1"> <thead> <tr> <th>API / Permissions name</th> <th>Type</th> <th>Description</th> <th>Admin Consent Requ...</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Microsoft Graph (4)</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>DeviceManagementApps.Read.All</td> <td>Application</td> <td>Read Microsoft Intune apps</td> <td>Yes</td> <td>⚠ Not granted for Patch ...</td> </tr> <tr> <td>DeviceManagementApps.ReadWrite.All</td> <td>Application</td> <td>Read and write Microsoft Intune apps</td> <td>Yes</td> <td>⚠ Not granted for Patch ...</td> </tr> <tr> <td>Group.Read.All</td> <td>Application</td> <td>Read all groups</td> <td>Yes</td> <td>⚠ Not granted for Patch ...</td> </tr> <tr> <td>User.Read</td> <td>Delegated</td> <td>Sign in and read user profile</td> <td>-</td> <td></td> </tr> </tbody> </table>	API / Permissions name	Type	Description	Admin Consent Requ...	Status	Microsoft Graph (4)					DeviceManagementApps.Read.All	Application	Read Microsoft Intune apps	Yes	⚠ Not granted for Patch ...	DeviceManagementApps.ReadWrite.All	Application	Read and write Microsoft Intune apps	Yes	⚠ Not granted for Patch ...	Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Patch ...	User.Read	Delegated	Sign in and read user profile	-		<p>To approve the new permissions click, Grant admin consent for <Org Name></p> <p>Choose Yes if prompted to consent for the required permissions.</p> <p>Note: To grant the permissions, you will need to be logged in to an Azure AD account with permissions to perform this task.</p>
API / Permissions name	Type	Description	Admin Consent Requ...	Status																											
Microsoft Graph (4)																															
DeviceManagementApps.Read.All	Application	Read Microsoft Intune apps	Yes	⚠ Not granted for Patch ...																											
DeviceManagementApps.ReadWrite.All	Application	Read and write Microsoft Intune apps	Yes	⚠ Not granted for Patch ...																											
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Patch ...																											
User.Read	Delegated	Sign in and read user profile	-																												

Add a client secret

Description

Expires

In 1 year
 In 2 years
 Never

Add **Cancel**

Click the **Certificates & secrets** node, and click **New client secret**.

Create a **Description name** and choose a **validity period** that meets your companies needs.

Click **Add**

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
PatchMyPC - Intune Management - Secret Key	12/31/2299	mdk3LFlywowif/D... <input type="button" value="Copy"/> <input type="button" value="Delete"/>

Click the button to **copy** the secret key.

Save the **key value** to a **secure location** for future use.

PatchMyPC - Intune Management

Search (Ctrl+/) <<

Overview | Quickstart | Manage | Branding | Authentication

Got a second? We would love your feedback on Microsoft identity platform (previ

Display name : PatchMyPC - Intune Management

Application (client) ID : **08e0d7af-5fe6-466f-ac30-97306ef7a397**

Directory (tenant) ID : b79783df-131e-

Object ID : b933a331-3d62-

Next, click the Overview node, and copy the **Application (client) ID** and save it to a secure location along with the **secret key value**.

Patch My PC - Publishing Settings - 1.6.6.1 - Preview

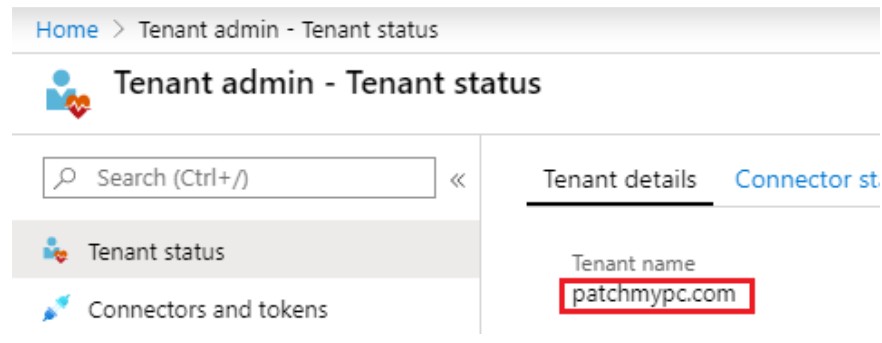
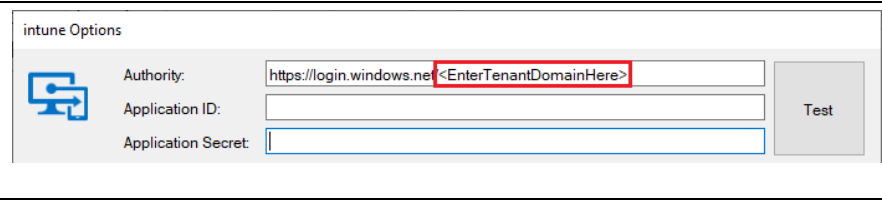
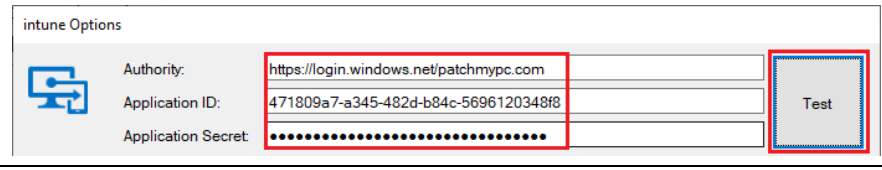
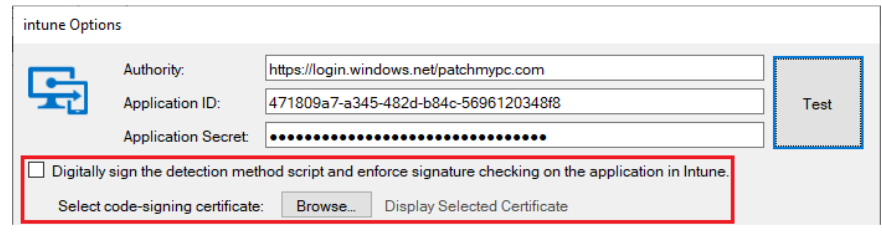
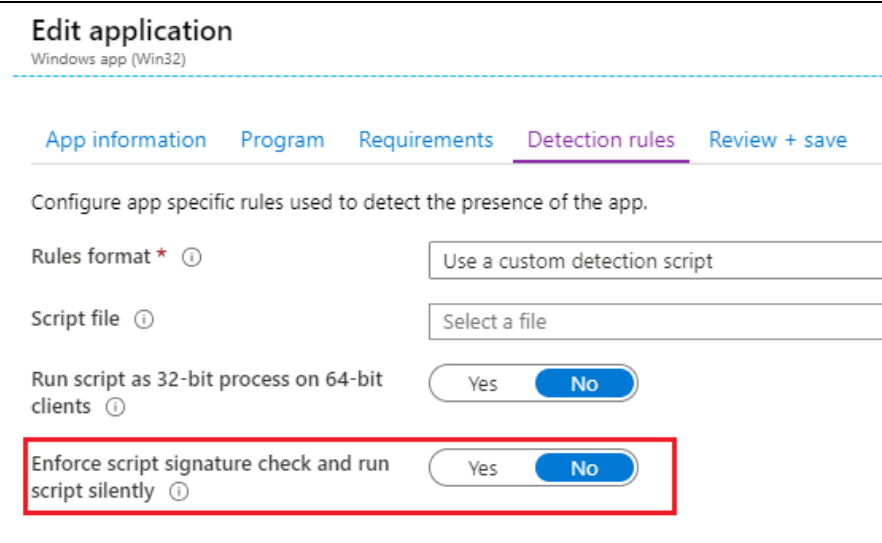
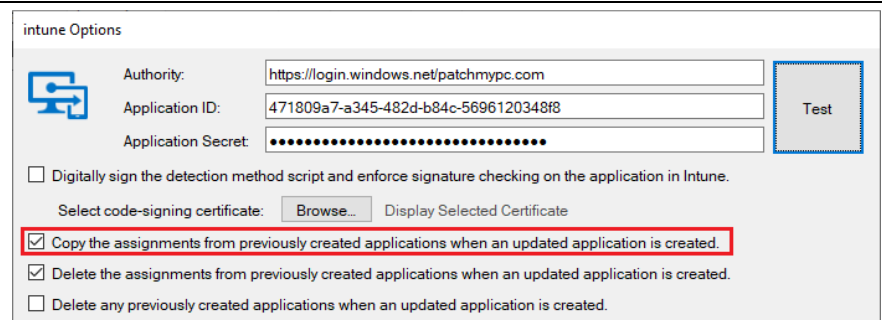
General | Intune Apps | Sync Schedule | Alerts | Advanced | About

Automatically create Win32 applications in Microsoft Intune.

- All Products
 - Adobe Systems, Inc.
 - Foxit Software Inc.
 - Igor Pavlov
 - Mozilla
 - Notepad++ Team
 - Piriform
 - VideoLAN

In the **Intune Apps** tab, click the checkbox **Automatically create Win32 application in Microsoft Intune.**

Next, click the **Options** button

	<p>Copy your Microsoft Intune tenant domain from the Tenant admin – Tenant status page.</p>
	<p>In the Authority URL textbox, replace <EnterTenantDomainHere> with your tenant domain name.</p>
	<p>Paste in the Application ID and Application Secret Key and click Test to validate we can successfully connect to your Intune tenant.</p>
	<p>By default, the PowerShell detection method scripts are not code-signed.</p> <p>Optionally, you can Browse to the local computer's personal certificate store and choose a code-signing certificate.</p>
	<p>If a code-signing certificate is not configured, the Win32 application in Microsoft Intune will configure the Detection Rules settings “Enforce script signature check and run script silently” = No</p> <p>If a certificate is selected, this setting will be Yes. If code-signing is enabled, clients will need to trust the certificate to install applications successfully.</p>
	<p>The option to “Copy the assignments from previously created applications when an update application is created.” will automatically deploy any new version of an application to the same group(s) from the previous version.</p>

Example: if Google Chrome 78 was created and assigned to an Azure AD Group and Google Chrome 79 is published later, it will be assigned to the same groups automatically.

intune Options

Authority:

Application ID:

Application Secret:

Digitally sign the detection method script and enforce signature checking on the application in Intune.

Select code-signing certificate: Display Selected Certificate

Copy the assignments from previously created applications when an updated application is created.

Delete the assignments from previously created applications when an updated application is created.

Delete any previously created applications when an updated application is created.

The option to **“Delete the assignments from previously created application when an updated application is created.”** will automatically remove any assignments for an older version of an application.

intune Options

Authority:

Application ID:

Application Secret:

Digitally sign the detection method script and enforce signature checking on the application in Intune.

Select code-signing certificate: Display Selected Certificate

Copy the assignments from previously created applications when an updated application is created.

Delete the assignments from previously created applications when an updated application is created.

Delete any previously created applications when an updated application is created.

The option to **“Delete any previously created applications when an updated application is created.”** will automatically delete any older versions of an application when a newer application is created.

intune Options

Authority:

Application ID:

Application Secret:

Digitally sign the detection method script and enforce signature checking on the application in Intune.

Select code-signing certificate: Display Selected Certificate

Copy the assignments from previously created applications when an updated application is created.

Delete the assignments from previously created applications when an updated application is created.

Delete any previously created applications when an updated application is created.

The **Run Intune Application Manager Utility** can be used to perform bulk deletion of **application assignments** or deletion of **applications** in Microsoft Intune.

Patch My PC - Publishing Settings - 1.6.5.1 - Preview

General Intune Apps Sync Schedule Alerts Advanced About

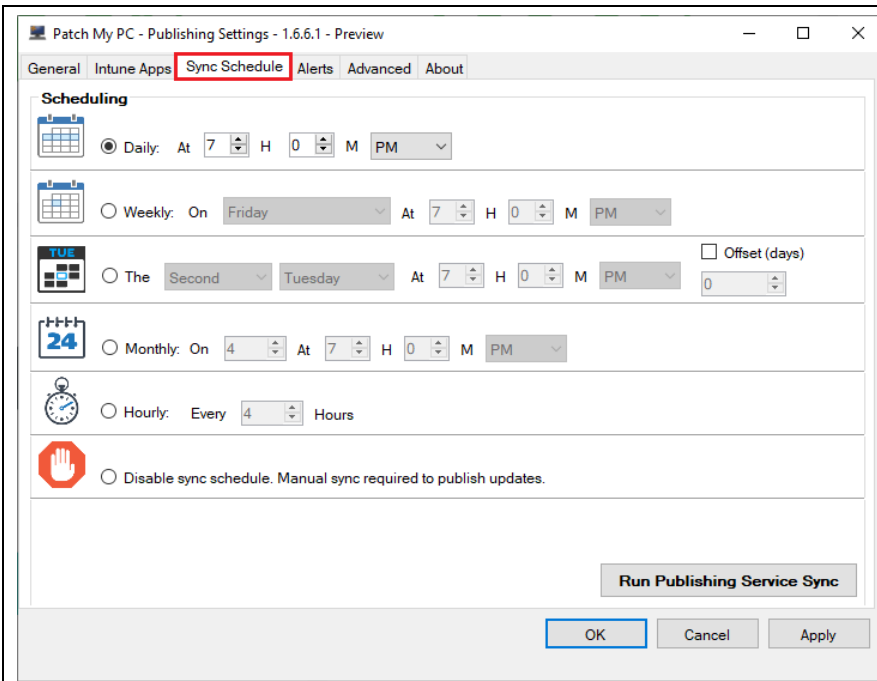
Automatically create Win32 applications in Microsoft Intune.

- Google, Inc.
 - Google Chrome (x86) (Full Content)
 - Google Chrome (x64) (Full Content)
 - Auto close application processes before installation – (Inactive)
 - Skip installation when the application is in use – (Inactive)
 - Add custom pre/post update installation scripts
 - Delete desktop shortcut(s) created by this application
 - Disable self-updater
 - Manage installation logging
 - Modify command line
 - Add MST transformation file
 - Manage assignments

In the **Intune Apps** tab, you can **enable products** for Win32 application publishing to Microsoft Intune.

Right-clicking All Products, Vendors, or Products will allow you to set custom options.

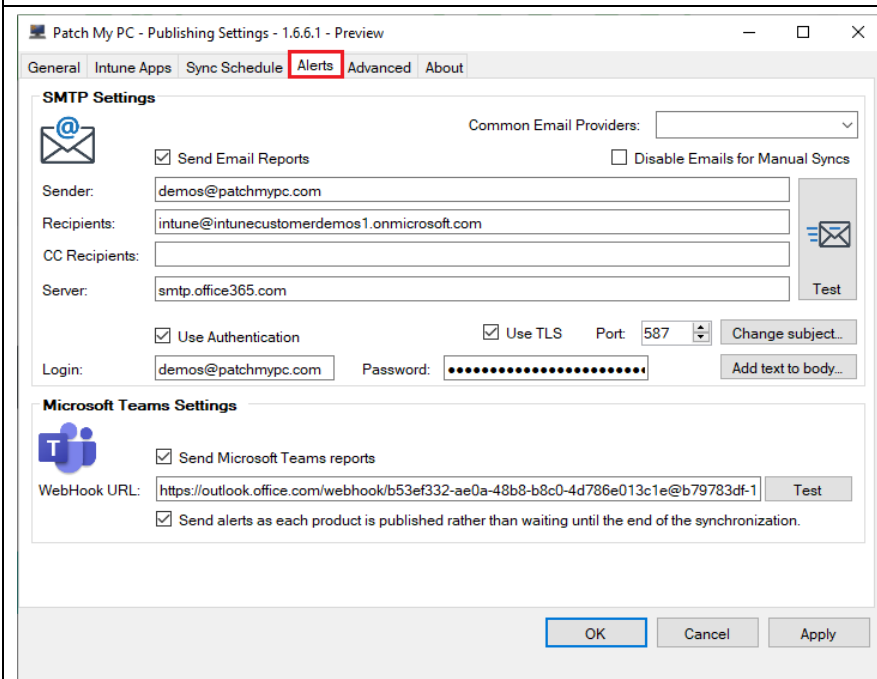
For a detailed description of each right-click option, please see [Custom Options Available for Third-Party Updates and Applications](#)



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 applications for enabled products to Microsoft Intune.**

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

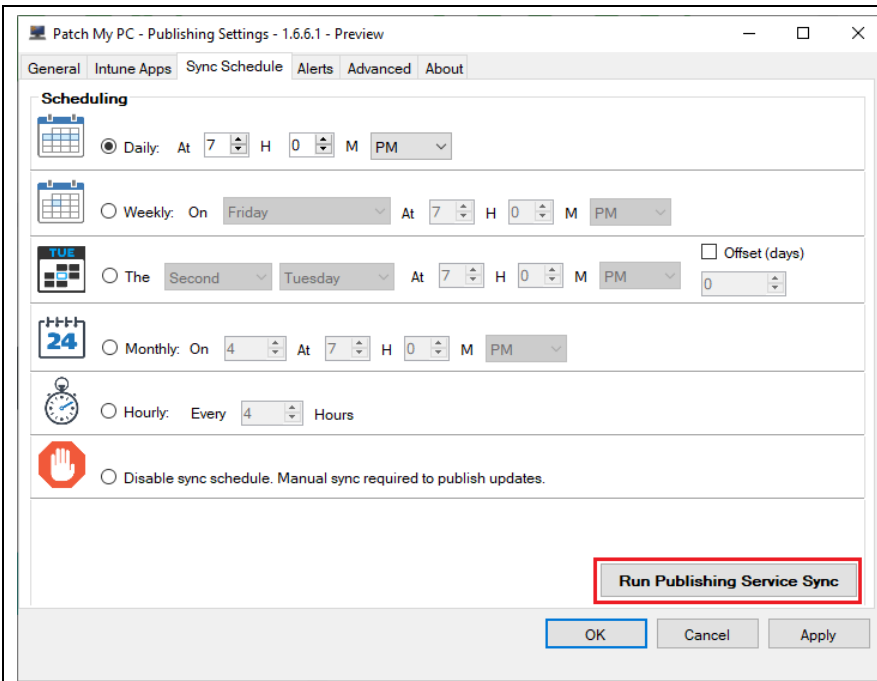


Optionally, you can enable **Notifications** in the **Alerts** tab.

To enable Email reports, configure your **SMTP sending options.**

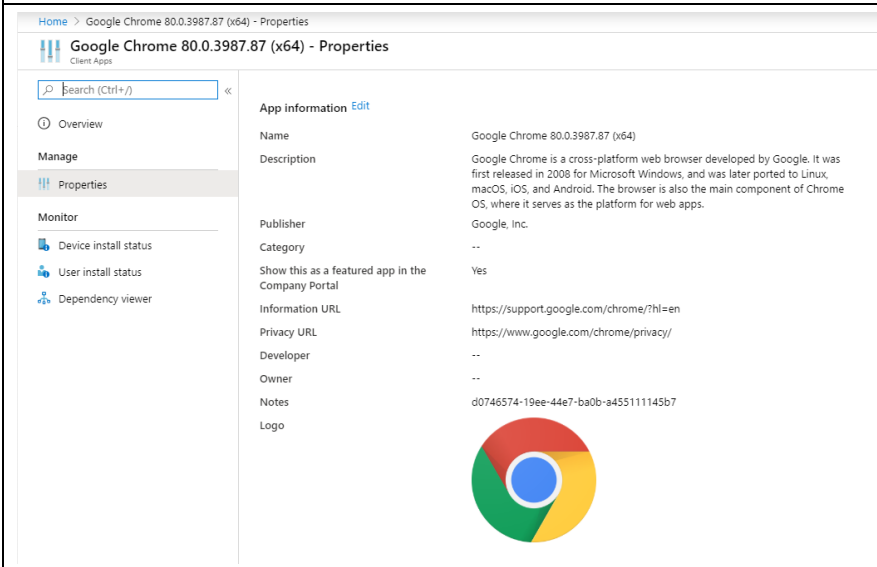
You can also paste a **Microsoft Teams webhook URL** to receive publishing alerts in a Microsoft Teams channel. See [Sending messages to connectors and webhooks](#) for more details.

We recommend enabling alerts to receive notifications published products including **Titles, Classification, Severity, CVE-ID's, Catalog Expiration Details, and more!**



If you want to **start the initial publishing of Win32 applications to Microsoft Intune** click the **Run Publishing Service Sync** button in the **Sync Schedule** tab

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



Once the **synchronization completes**, you should see all the selected applications automatically appear in Microsoft Intune.

These Win32 applications can now be [assigned to computers in Microsoft Intune](#).

Please see [What is Microsoft Intune app management?](#) for more details.