Deltek ProPricer

Connect For Office Deployment Guide

Contents

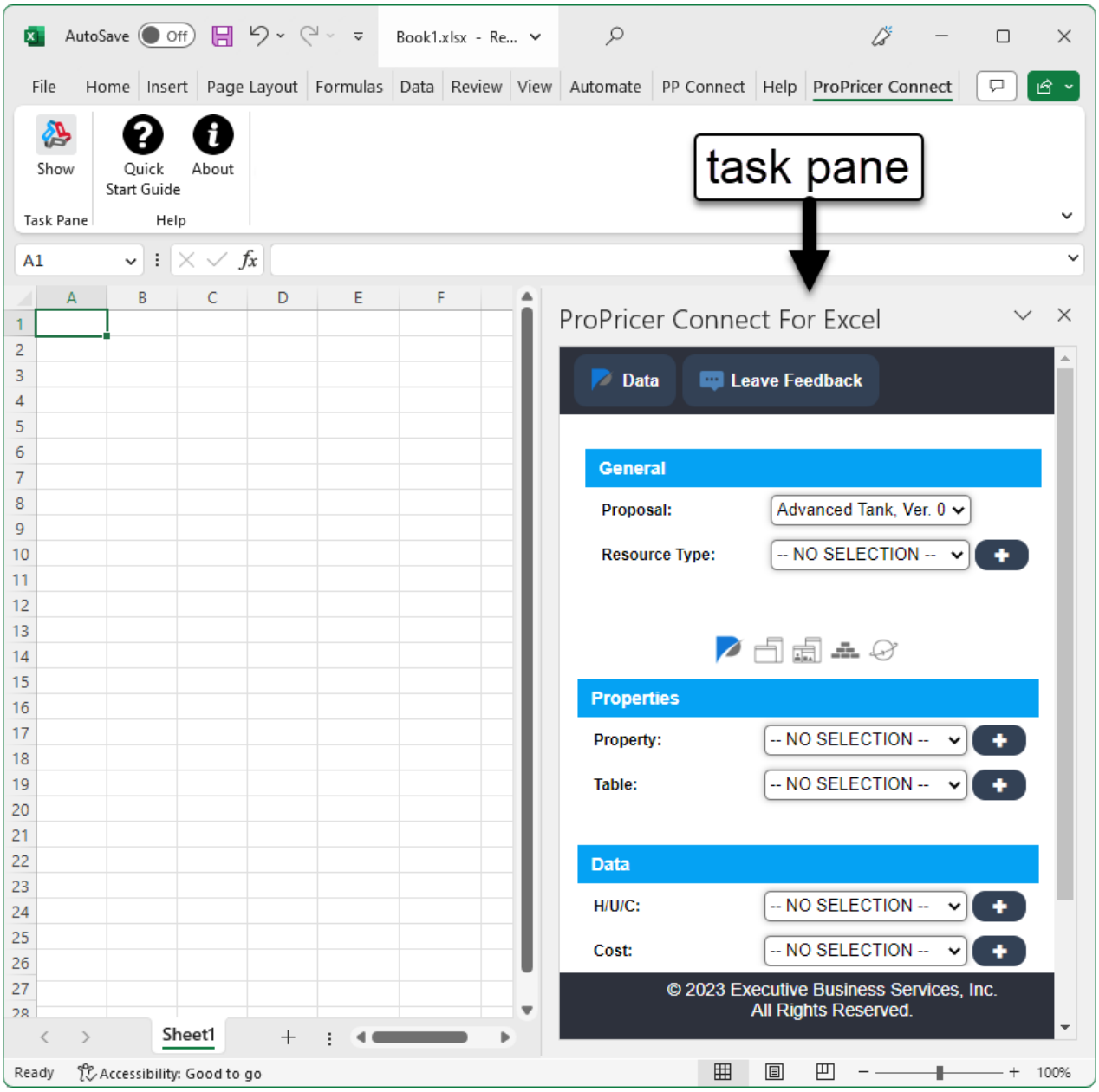
Introduction

ProPricer Connect for Office is a web add-in created on the Office Add-ins platform that lets you interact with Office documents from a web server. Office Web Add-ins can be deployed into any Office application, which provides the following advantages over add-ins built using VBA, COM, or VSTO:

- Cross-platform support: Office Add-ins run in Office on the web, Windows, Mac, and iPad.
- Centralized deployment and distribution: Administrators can centrally deploy Office Add-ins across an organization.
- Based on standard web technology: Standard web technology allows more versatility, better control, and improved web security.
- Ease of updates: Web apps can be easily updated without any user intervention.

In an Office application, the Connect for Office add-in appears in a task pane. The task pane can be repositioned or detached and moved to another monitor.

Depending on the deployment method you use, you can open the ProPricer ribbon from a new ribbon called ProPricer Connect, or you can launch the application with the My Add-ins button on the Insert ribbon.


AutoSave
Off
Book1.xlsx - Re...
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Automate
PP Connect
Help
ProPricer Connect
Show
Quick Start Guide
About
Task Pane
Help
task pane
A1
ProPricer Connect For Excel
Data
Leave Feedback
General
Proposal:
Advanced Tank, Ver. 0
Resource Type:
-- NO SELECTION --
Properties
Property:
-- NO SELECTION --
Table:
-- NO SELECTION --
Data
H/U/C:
-- NO SELECTION --
Cost:
-- NO SELECTION --
© 2023 Executive Business Services, Inc.
All Rights Reserved.
Sheet1
Ready
Accessibility: Good to go
100%

Set up

Considerations

An Office Add-in includes two basic components: an XML manifest file, and your own web application. The manifest defines various settings, including how the add-in integrates with Office client applications. The web application needs to be hosted on a web server like IIS, or Web App service in Microsoft Azure.

- The web application will serve both Connect for Word and Connect for Excel add-ins.
- The web application must have network access to ProPricer 9 Application Server.

Office requirements

For Word and Excel add-ins, users must have one of the following versions:

- Windows:
  - Microsoft 365 Business licenses (Business Basic, Business Standard, Business Premium) version 1704 or later
  - Office 365 Enterprise licenses (E1/E3/E5/F3)
  - Microsoft 365 Enterprise licenses (E3/E5/F3)
  - Microsoft Office 2016 (64-bit edition) or later.
- MacOS: Version 15.34 or later

Use one of the following methods to deploy Connect for Office application.

Method 1: IIS Web Server

Minimum requirements

- Microsoft Windows Server 2012 R2 (64 bits)
- Internet Information System 8.0
- SSL certificate

Deployment packages

The platform specific and framework-dependent package include only the application and its dependencies.

The .NET runtime is provided by ASP.NET Hosting Bundle. Deployment package includes a Windows x64 platform specific executable.

The zip packages are available in the Deltek Software Manager (DSM).

Install Connect for Office

Download and unzip the Connect for Office zip package to a folder where you want the site (for example, C:\inetpub\Connect for Office).

The zip packages are available in the Deltek Software Manager (DSM).

Prerequisites

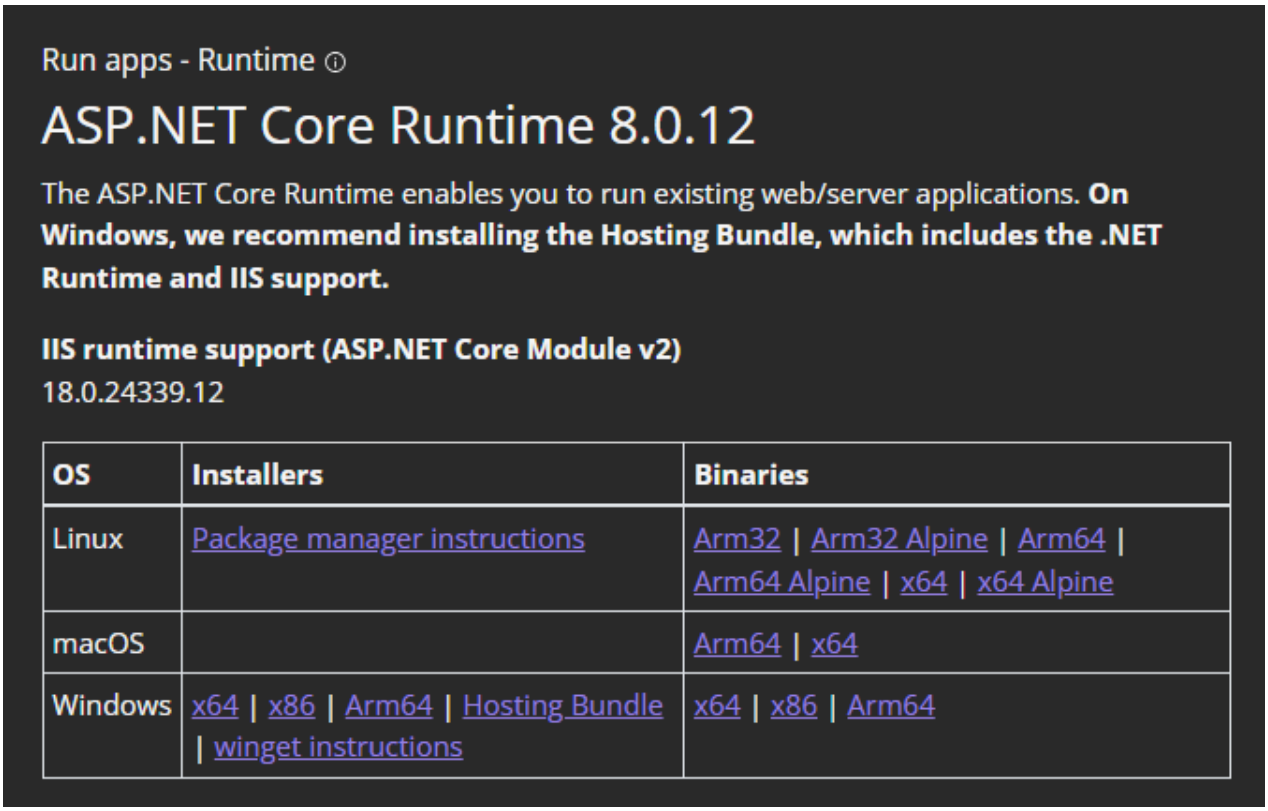
Enable Internet Information Service

1. Open Add Roles and Features.
2. In Roles, make sure Web Server (IIS) is enabled.
3. In Web Server, make sure the following are installed.
    1. Default Document
    2. Directory Browsing
    3. HTTP Errors
    4. Static Content
    5. HTTP Logging
    6. Static Content Compression
    7. Request Filtering
    8. IIS Management Console
4. Restart the server if required.

Install the .NET 8 Windows Server Hosting Bundle

Install the .NET 8 Hosting Bundle on the hosting system. The bundle installs the .NET 8 Runtime, .NET 8 Library, and the ASP.NET Core Module. The module allows ASP.NET Core apps to run behind IIS.

1. Go to the Download .NET 8.0 page.
2. Under Run apps - Runtime, download the installer using the Hosting Bundle link.



Run apps - Runtime ⓘ

ASP.NET Core Runtime 8.0.12

The ASP.NET Core Runtime enables you to run existing web/server applications. **On Windows, we recommend installing the Hosting Bundle, which includes the .NET Runtime and IIS support.**

IIS runtime support (ASP.NET Core Module v2)
18.0.24339.12

OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm32 Alpine | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS		Arm64 | x64
Windows	x64 | x86 | Arm64 | Hosting Bundle | winget instructions	x64 | x86 | Arm64

3. Run the installer on the server.
4. Restart the system or execute the following commands in a command shell:

```
net stop was /y
net start w3svc
```

Website set up

1. Open **Internet Information Service (IIS) Manager**.
2. Create the **PP9 Connect for Office** application pool. To create a new pool:
    - Right-click **Application Pools**, then select **Add Application Pool**.
    - In the **Name** field, enter a valid name like **Connect for Office App Pool**.
    - In the **.NET CLR version** field, select **No Managed Code**.
    - In the **Managed pipeline mode** field, select **Integrated**.
    - Select **Start application pool immediately**.
    - Click **OK** to create the application pool.
    - Right-click **Connect for Office App Pool**, then select **Advanced Settings**.
    - Set **Load User Profile** to **True**.

- Click **OK** to save the change.
- Right-click **Connect for Office App Pool**, then select **Recycle**.

3. Create the **ProPricer Connect for Office** website.
   - Right-click the **Sites** folder, then select **Add Website**.
   - In the **Site name** field, enter **Connect for Office**.
   - In the **Application pool** field, select the pool created in previous steps.
   - In the **Physical path** field, enter or select the path where the Connect for Office files are located. For example, C:\inetpub\Connect for Office.
   - In the **Type** field of the **Binding** section, select **https**.
   - In the **IP address** field, select **All Unassigned**.
   - In the **Port** field, enter a valid port number. Recommended to use https default port 443.

   Ensure the port is accessible to the end users.
4. In the **Host name** field, enter a domain.
5. Select the box **Require Server Name Indication**.
6. Select a valid SSL certificate for the domain.
7. Click **OK** to create the website.

Connect for Office requires a valid SSL certificate.

Configuration

To configure Connect for Web, use the configuration tool provided in the Configure folder in the target folder or edit appsettings.json.

The configuration tool is recommended.

Configuration Tool

1. Go to the folder where Connect for Office is installed
2. Open ConfigTool application from the Configure folder
    a. In the Host field enter your ProPricer Server hostname
    b. In the Port field enter the ProPricer Server port.
    c. In the Connection Name field select the name of the Database Connection you want to connect to.
    d. Optionally, add more connections clicking the Add button.
    e. In the Registration Key enter your Connect for Office license key.
3. Restart Website and Application Pool

Manual Configuration

To manually configure Connect for Office, edit appsettings.json in the target folder. Enter the ProPricer 9 Server name, port, and your Connect for Office key.

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft.AspNetCore": "Information"
    }
  },
  "AuthTokens": [
    {
      "Key": "Default",
      "Value": {
        "Host": "propricer9.mycompany.com",
        "Port": 8092,
```

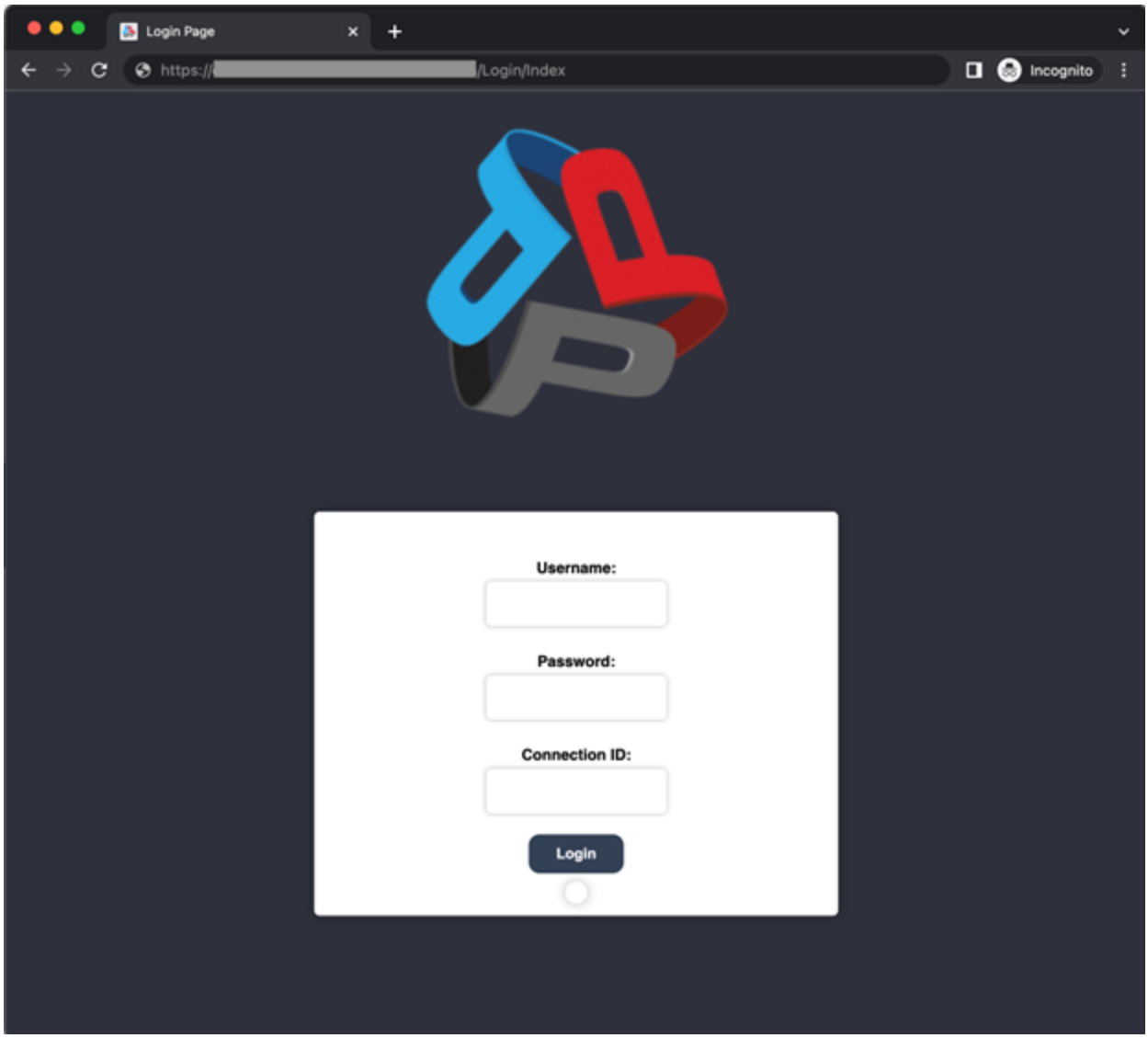
```
            "ConnectionName": "ProPricer_SQL"
        }
      }
    ],
    "Key": "XYZ11-0A6B61-CD0FGE-12345-ZW9W1A"
}
```

References

- Host ASP.NET Core on Windows with IIS. https://learn.microsoft.com/en-us/aspnet/core/host-and-deploy/iis/?view=aspnetcore-8.0

Test

1. Open your browser and go to https://<your-connect-for-office-hostname>/Login/Index. You should see a website like this.



2. Enter a valid ProPricer username and password. Enter a Connection ID matching the value configured in appsettings.json, default is “Default”. Click Login.

Common errors

500.119

A user in the application pool cannot read web.config. To fix this, assign permissions to the folder where the Connect for Web files are located (for example, C:\inetpub\Connect For Office).

ProPricer license activation error

For Windows workstation operating systems (for example, Windows 10), if you receive an error related to activating a ProPricer license, edit the website settings to run the site. Click Connect As, then select the same user in the application pool.

HTTP Error 503 – The service is unavailable

The service is unavailable when the application pool of the corresponding web application is stopped, disabled, or paused. It may also be unavailable when the given user identity of the application pool is invalid due to an expired password or is locked.

https://blogs.msdn.microsoft.com/webtopics/2010/02/17/a-not-so-common-root-cause-for-503-service-unavailable/

https://stackoverflow.com/questions/13322937/http-error-503-the-service-is-unavailable

Bad Request – Request header too long

“HTTP Error 400. The size of the request header is too long.”

While using Windows authentication, this error may appear instead of the Connect for Office application. It is the result of the user being a member of many Active Directory user groups.

To fix this:

1. Open Windows Registry Editor and go to:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters

2. Increase the settings for the MaxFieldLength and the MaxRequestBytes registry entries on the server so that the user's request headers do not exceed these values. For example:

"MaxRequestBytes"=dword:01000000

"MaxFieldLength"=dword:0000fffe

https://docs.microsoft.com/en-us/troubleshoot/iis/http-bad-request-response-kerberos

http://www.grouppolicy.biz/2013/06/how-to-configure-iis-to-support-large-ad-token-with-group-policy/

Maximum registration attempts exceeded

You will receive this error if the Connect for Office license is invalid when you try to connect to the ProPricer Server.

To fix this:

1. Make sure you have a valid key configured in the appsettings.json file.
2. Make sure the key hasn’t expired.
3. If the key is concurrent, make sure the key has been added in ProPricer Server Manager.

Firewall

Your firewall must allow inbound connections to the port you selected for the Connect for Office website (for example, 443) for your end users to use it.

Method 2: Web App on Azure

Minimum requirements

- Azure account with required permissions to create App Services.
- Windows App Service Plan with Production or Isolated plan depending on your workload.
- Optional: SSL certificate for custom domain (e.g. c4o.mycompany.com).

Download Connect for Office

Download and unzip the Connect for Office zip package.

The ZIP packages are available in the Deltek Software Manager (DSM).

Configuration Prerequisites

- ProPricer Server hostname and port.
- Connect for Office registration key.

App Service

1. In the Azure Portal, add a Web App (App Service).
2. Enter the Web App name.
3. Select the following settings:
    1. Publish: Code
    2. Runtime stack: .NET 8 (LTS)
    3. Operating System: Windows
    4. Region: Select the desired region
4. Click Next.
5. On the Monitoring tab, make sure Enable Application Insights is set to No.
6. Click Next.
7. On the Tags tab, create the desired tags.

8. Click Next.
9. Click Create.

Configuration

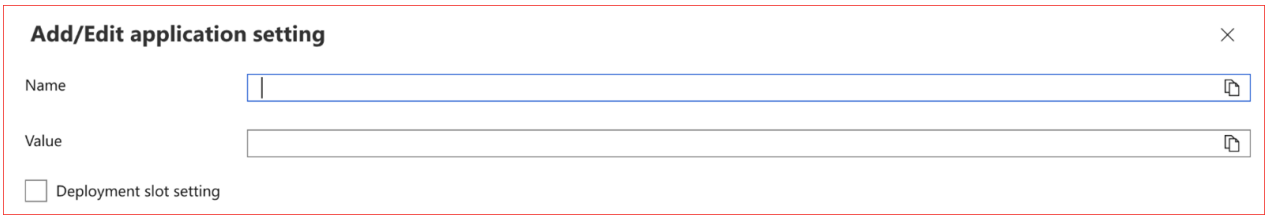
There are two methods for configuring Connect for Office:

- Manually edit appsettings.json in the target folder.
- Use the Configuration option in the Settings section of the App Service in the Azure Portal.

You can use either of these methods or a combination of both. The settings configured in the Azure Portal take precedence over the settings in the appsettings.json file. The recommendation is to use App Service Configuration.

To use App Service Configuration for Connect for Office:

1. In the App Service in the Azure Portal, go to the Settings section and select the Configuration option.
2. On the General Settings tab, click New application setting to create the following settings:



Name	Value	Example
AuthTokens:0:Key	The ID of the connection end users will use.	Default
AuthTokens:0:Value:ConnectionName	The ProPricer 9 Database Connection	ProPricer_SQL
AuthTokens:0:Value:Host	Your ProPricer 9 Application Server hostname	propricer9.mycompany.com
AuthTokens:0:Value:Port	Your ProPricer 9 Application Server port	8092
Key	Your Connect for Ofice registration key	XYZ11-0A6B61-CD0FGE-12345-ZW9W1A

3. Alternatively, click Advanced edit and use the following json:

```
{
  "name": "AuthTokens:0:Key",
  "value": "Default",
  "slotSetting": false
},
{
  "name": "AuthTokens:0:Value:ConnectionName",
```

```
  "value": "ProPricer_SQL",
  "slotSetting": false
},
{
  "name": "AuthTokens:0:Value:Host",
  "value": "propricer9.mycompany.com",
  "slotSetting": false
},
{
  "name": "AuthTokens:0:Value:Port",
  "value": "8092",
  "slotSetting": false
},
{
  "name": "Key",
  "value": "XYZ11-0A6B61-CD0FGE-12345-ZW9W1A",
  "slotSetting": false
},
```


4. On the General Settings tab, verify or adjust the following settings:
    - Stack: .NET
    - .NET Version: .NET 8
    - Platform: 64 Bit
    - Manage pipeline version: Integrated
    - FTP state: Disabled
    - HTTP version: 1.1
    - Web sockets: Off
    - Always on: On
    - ARR affinity: Off
    - HTTPS Only: On
    - Minimum TLS Version: 1.2

- Remote debugging: Off
- Client certificate mode: Ignore

5. Click Save.

Recommended TLS/SSL settings

Azure App Service is created with an SSL certificate by default to provide https and a subdomain, like connectforweb.azurewebsites.us.

In the App Service in the Azure Portal, you should verify that the following TLS/SSL settings were selected during configuration:

- HTTPS Only: On
- Minimum TLS Version: 1.2

Optionally, you can configure your own domain in this section, like mysite.mycompany.com.

Deploy ZIP file using ZipDeployUI

This ZIP file deployment uses the same Kudu service that powers continuous integration-based deployments.

1. Zip the folder. Select all files (not the parent folder), right-click, point to Send to, select Compress (zipped) folder, then name the ZIP file.

Deploy the ZIP file downloaded from the Deltek Software Manager (DSM) when all the settings are in the Configuration options of the App Service.

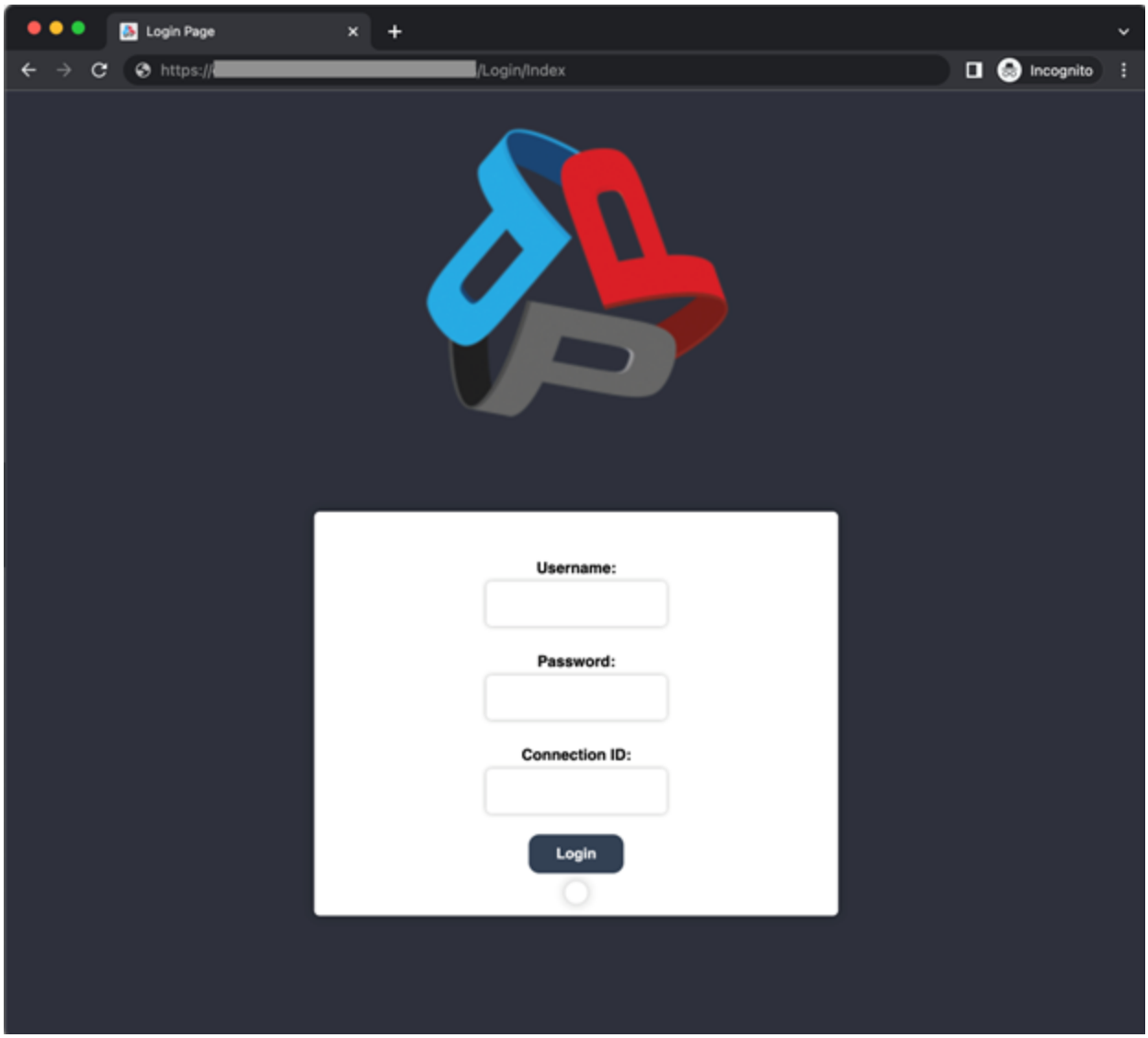
2. In the App Service options pane, select Advanced Tools, click Go, expand the Tools menu, then select Zip Push Deploy. Alternatively, in your browser, go to https://<app_name>.scm.azurewebsites.us/ZipDeployUI.
3. Upload the ZIP file by dragging it to the file explorer area on the web page.

When deployment is in progress, an icon in the top-right corner shows the progress percentage. The page also shows messages for the operation below the explorer area. When it is finished, the last deployment message should say Deployment successful.

Alternatively, use az webapp deployment source config-zip to deploy the ZIP file using Azure CLI, or the Publish-AzWebApp cmdlet to deploy the ZIP file using PowerShell.

Test

1. Open your browser and go to https://<your-connect-for-office-hostname>/Login/Index. You should see a website like this.



Enter a valid ProPricer username and password. Enter a Connection ID matching the value configured in AuthTokens:0:Key, default is “Default”. Click Login.

Common errors

Server Error in '/' Application. Could not load file or assembly

On the General Settings tab, make sure the .NET Version is .NET 8 and Platform is 64 Bit.

Virtual Network

Make sure Connect for Office has access to your ProPricer 9 Application Server. It is recommended that they are on the same Virtual Network (VNet).

Manifest configuration

The manifest file is an XML formatted document that describes the add-in behavior and security.
A manifest file is provided in the Connect for Office zip package for each of the supported Office applications.

Extract the zip package. The manifest files are inside the Word and Excel folders, accordingly.

NOTE: Do not modify anything other than what is described in this section.

Once you have successfully set up your web application, you will need the URL to access it. It could look like “https://c4o.mycompany.com”.

In the manifest file, run a Find/Replace to look for ~`remoteAppUrl` and replace all instances with your URL. For example, change the highlighted text:

```
<IconUrl DefaultValue="~remoteAppUrl/Images/PPMain_64.png" />
```

To your URL, like:

```
<IconUrl DefaultValue="https://c4o.mycompany.com/Images/PPMain_64.png" />
```

Repeat for all instances of ~remoteAppUrl.

Next, you will need to add the domain URL into the AppDomains section:

```
<AppDomains>
  <AppDomain>AppDomain1</AppDomain>
  <AppDomain>AppDomain2</AppDomain>
  <AppDomain>AppDomain3</AppDomain>
</AppDomains>
```

To your URL, like:

```
<AppDomains>
  <AppDomain>https://c4o.mycompany.com</AppDomain>
  <AppDomain>AppDomain2</AppDomain>
  <AppDomain>AppDomain3</AppDomain>
```

```
</AppDomains>
```

When you're done configuring the manifest file, save your changes. These changes to the manifest will tell the Office application where to look for specific resources and files on the web server.

Deployment

Deploying an add-in means you're pre-installing the add-in for a specific set of users in your organization. All management actions taken on a deployed add-in are fully controlled by the admin. It may take up to 24 hours after deployment for an add-in to show up for all users in the client application.

There are two deployment options provided by Microsoft:

- Microsoft 365 admin center: In a cloud deployment, you can distribute your add-in to users in your organization with the Microsoft 365 admin center. This is done through Integrated apps or Centralized Deployment.
- SharePoint catalog: In an on-premises environment, you can use a SharePoint catalog to distribute your add-in to users in your organization. A SharePoint app catalog is a special site collection that you can create to host Word, Excel, and PowerPoint add-ins. Because SharePoint catalogs don't support new add-in features implemented in the VersionOverrides node of the manifest, including add-in commands, we recommend that you use Centralized Deployment via the admin center if possible. Add-in commands deployed via a SharePoint catalog open in a task pane by default.

Microsoft 365 admin center (recommended)

The Microsoft 365 admin center makes it easy for an administrator to deploy Office Add-ins to users and groups in their organization. Add-ins deployed via the admin center are available to users in their Office applications right away, with no client configuration required. You can use Integrated apps to deploy internal add-ins as well as add-ins provided by ISVs. Integrated apps also show admins add-ins and other apps bundled together by same ISV, giving them exposure to the entire experience across the Microsoft 365 platform.

Summary

As an admin, you can:

- Deploy an Office Add-in for users in your organization.
- Manage how users can install and use Office add-ins.
- Upload custom Office add-ins for your organization.

Office Add-ins help you personalize your documents and streamline the way you access information on the web. They are supported in three desktop platforms: Windows, Mac, and Online Office apps. It's also supported in iOS and Android (mobile Outlook Add-ins only).

Add-ins also provide the following benefits:

- When your Office application starts, the add-in automatically downloads. If the add-in supports add-in commands, the add-in automatically appears in the ribbon of the application.
- Add-ins no longer appear for users if the admin turns off or deletes the add-in or removes users from Azure Active Directory or a group that the add-in is assigned to. You can learn how to perform these actions in the following section.

Assigning users

Admins can deploy an add-in to everyone or to specific users and groups. The right option for your organization depends on your configuration. However, Microsoft recommends making assignments by using groups. As an admin, you might find it easier to manage add-ins by using groups and controlling the membership of those groups rather than assigning individual users each time. In some situations, you might want to restrict access to a small set of users by making assignments to specific users by assigning users manually.

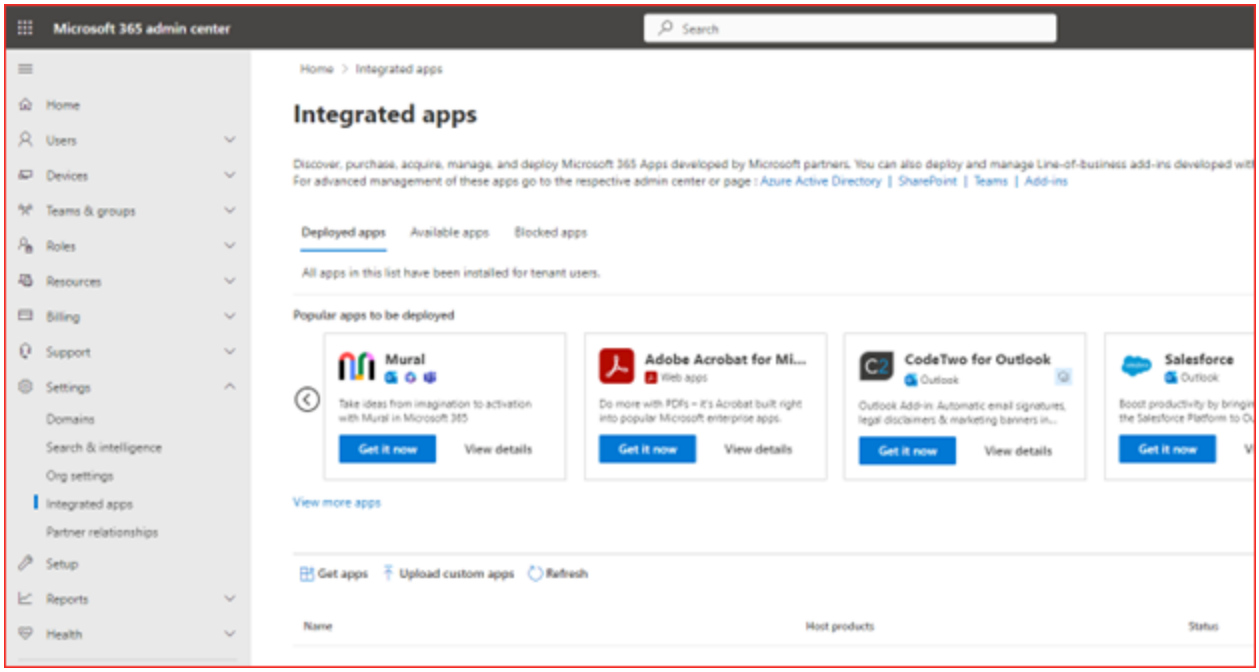
For more information please visit Microsoft “Manage Office add-ins” documentation on https://learn.microsoft.com/en-us/microsoft-365/admin/manage/office-addins?view=o365-worldwide

Steps for deployment

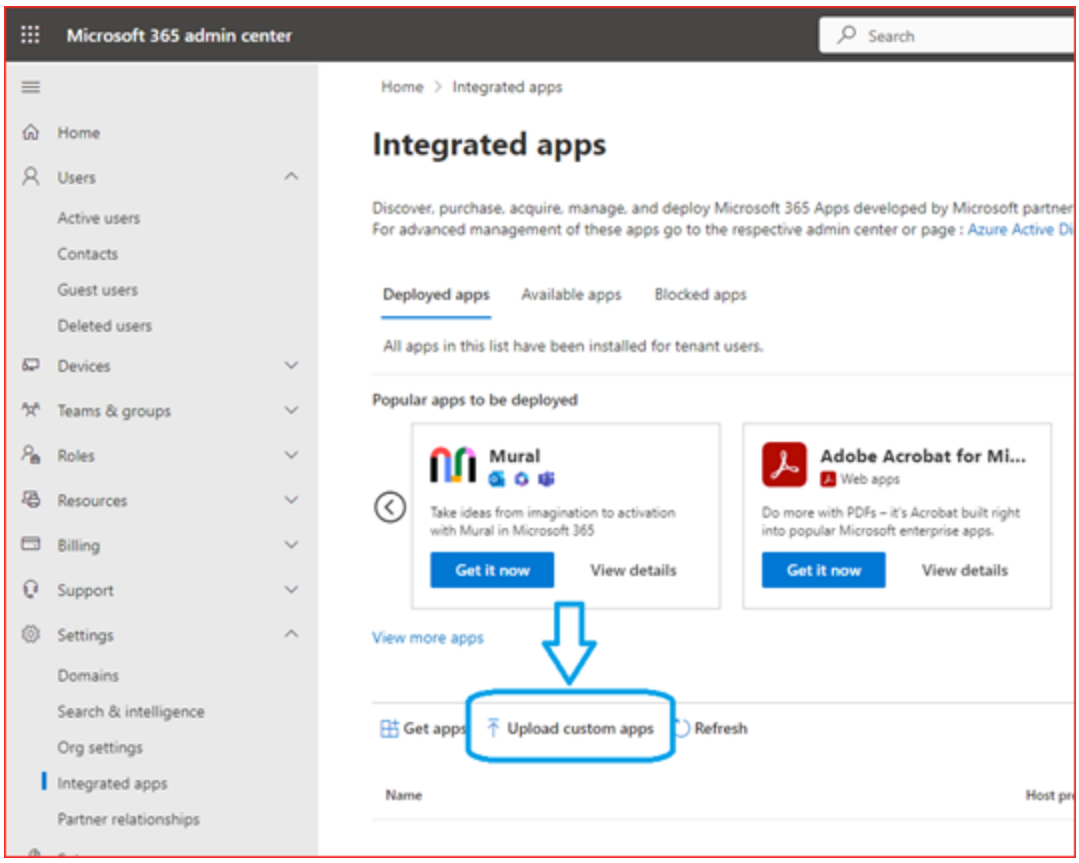
To deploy the manifest files for your office applications in the Microsoft 365 admin center, you will need to first log in with Administrator credentials and use the Integrated apps. Currently, Exchange admins, Global admins, and Azure Application admins can deploy add-ins from Integrated apps.

1. Open the Microsoft 365 admin center: https://admin.microsoft.com/Adminportal#/homepage.
2. In the admin center, in the left pane, expand Settings, then click Integrated apps.

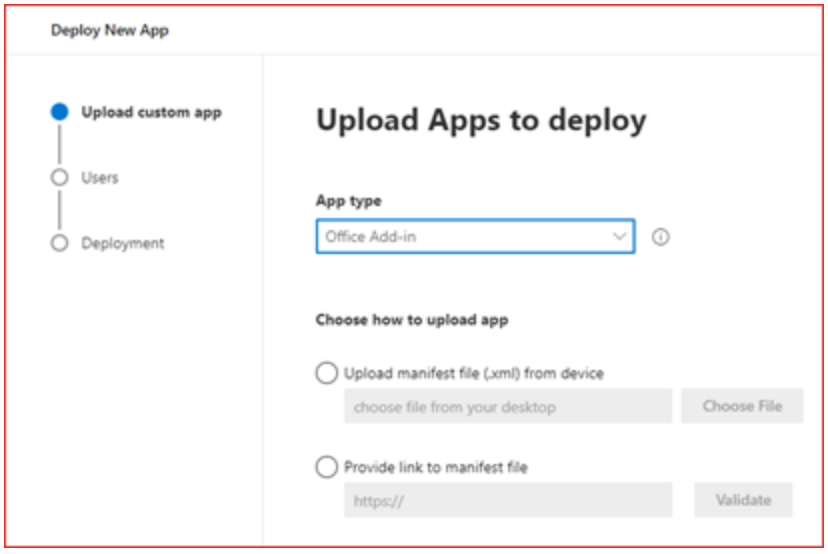
- If Settings does not show, click Show all to view all menu options.



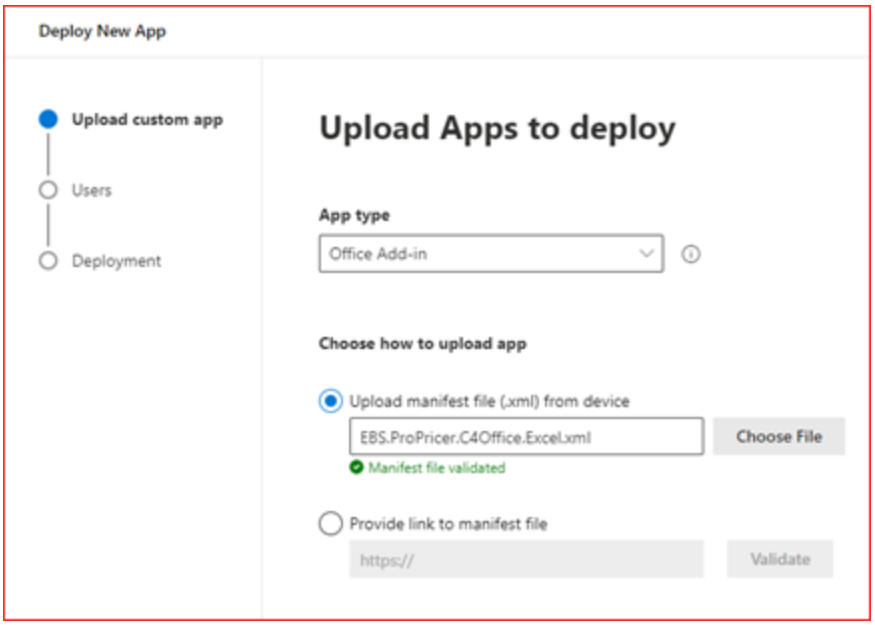
3. On the Integrated apps page, click the Upload custom apps.



4. In the dialog box that appears, change the App Type to Office Add-in.

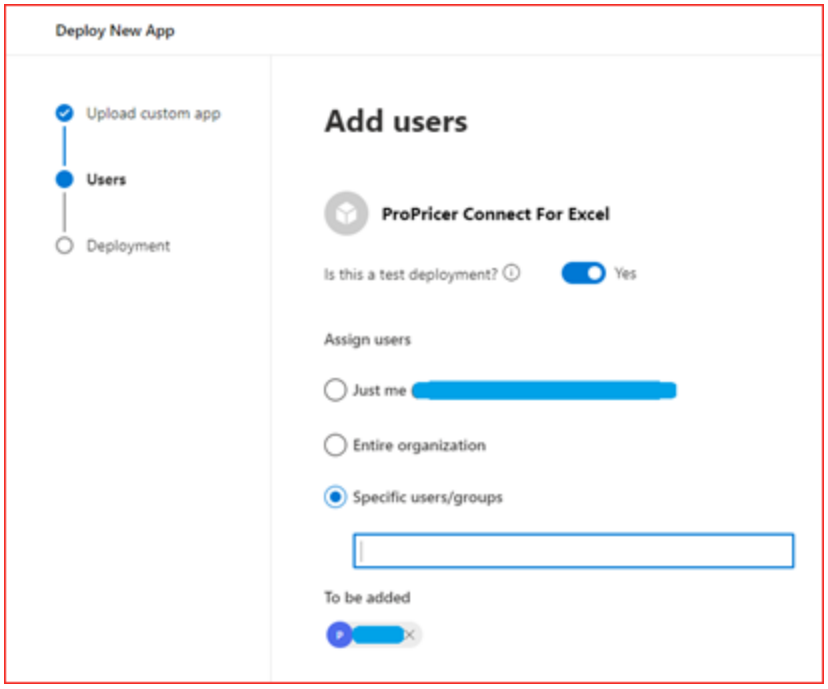


5. Upload the manifest file from your current device or from a link. When you upload the manifest file, it will be validated and any problems will be indicated. Click Next.



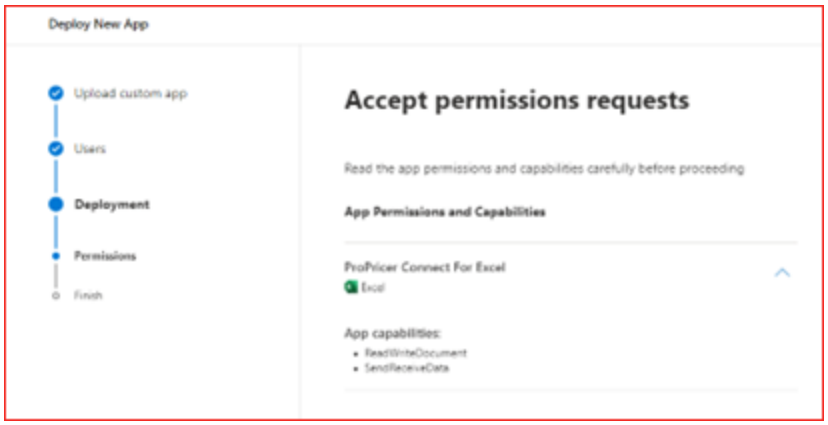
6. On the Add users page, the name of the manifest file appears. If you'd like to wait to deploy the Connect for Office to the entire organization, select the checkbox next to Is this a test deployment? then select one of the following options and click Next.
    - Just me: If you assign an add-in to just yourself, the add-in is assigned to only your account, which is ideal for testing the add-in.
    - Entire organization: This option assigns the add-in to every user in the organization. Use this option sparingly and only for add-ins that are truly universal to your organization.
    - Specific users/groups: If you assign an add-in to an individual user, and then deploy the add-in to a new user, you must first add the new user. If you assign an add-in to a group, users who are added to the group are automatically assigned the add-in. When a user is removed from a group, the user loses access to the add-in. In either case, no other action is required from the admin.

- Specific users/groups can be a Microsoft 365 group, a security group, or a distributed group.

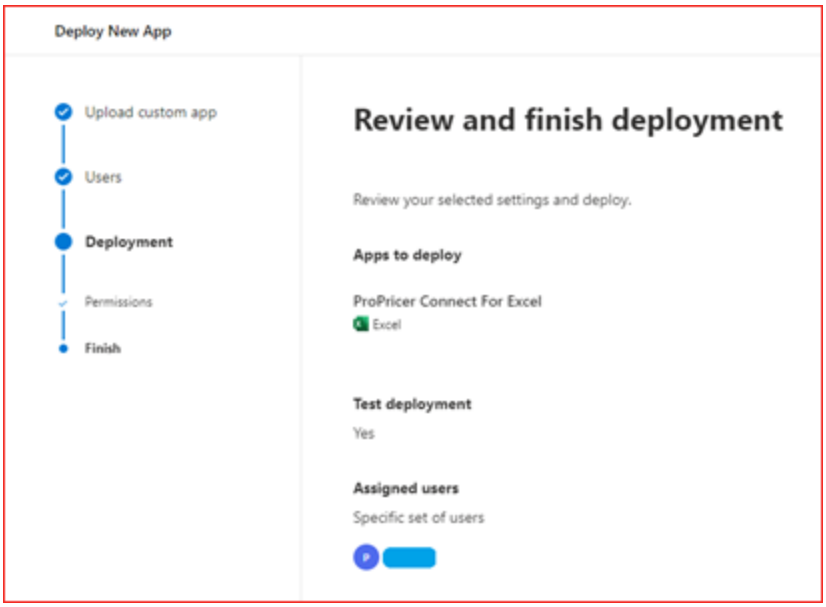


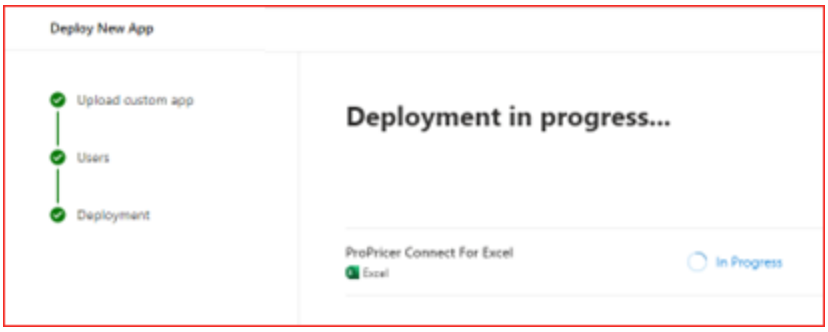
7. On the Accept permissions requests page, the permissions and capabilities of each app are listed. If an app needs consent, select Accept permissions, then click Next.

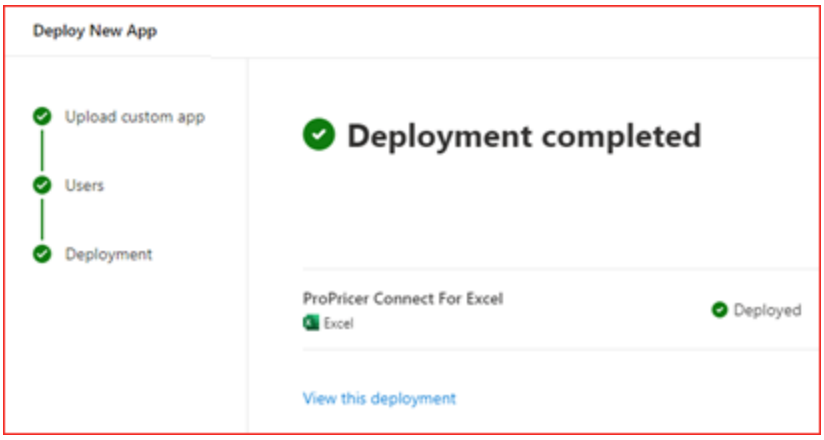
- Only a global administrator can give consent.



8. Review the deployment and then click Finish deployment.







- It can take up to 24 hours for an add-in to show up for client for all users.

9. You can view the deployment from the Overview tab by clicking View this deployment. In the Microsoft 365 admin center, you can see the status of each deployed app and the date you deployed the app.

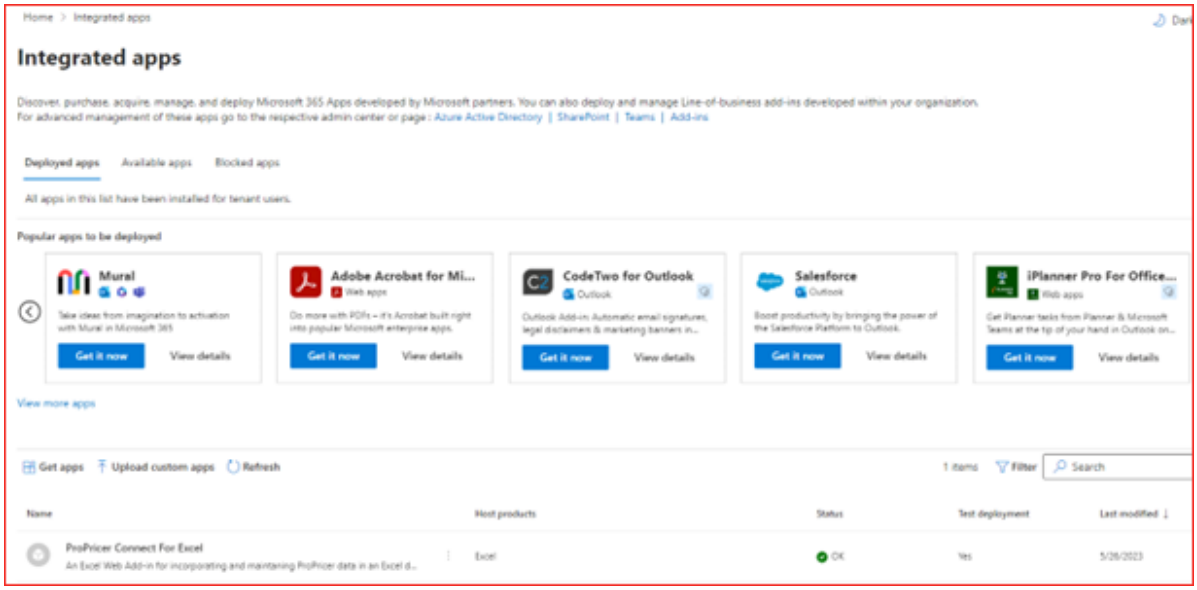
Client setup

When your deployment is complete, assigned users will be able to find Connect for Office in their respective Office applications. To set up Connect for Office in one of these applications, pleaase see the Connect for Office Quick Start Guide.

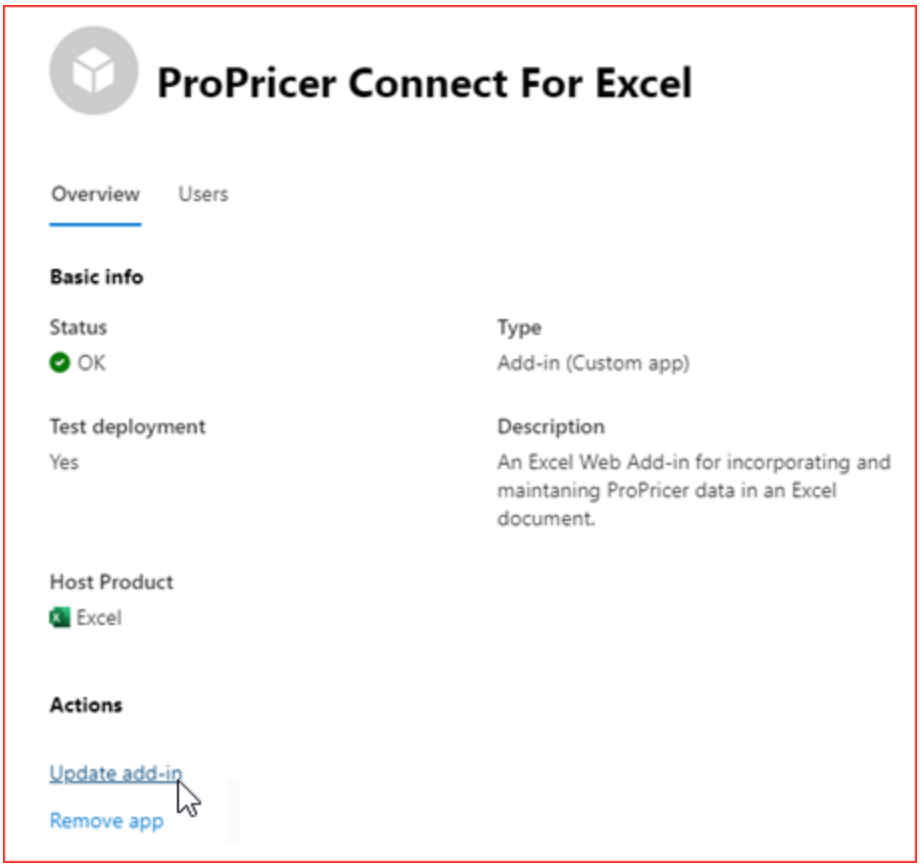
Update add-ins

To update your add-in, follow the steps:

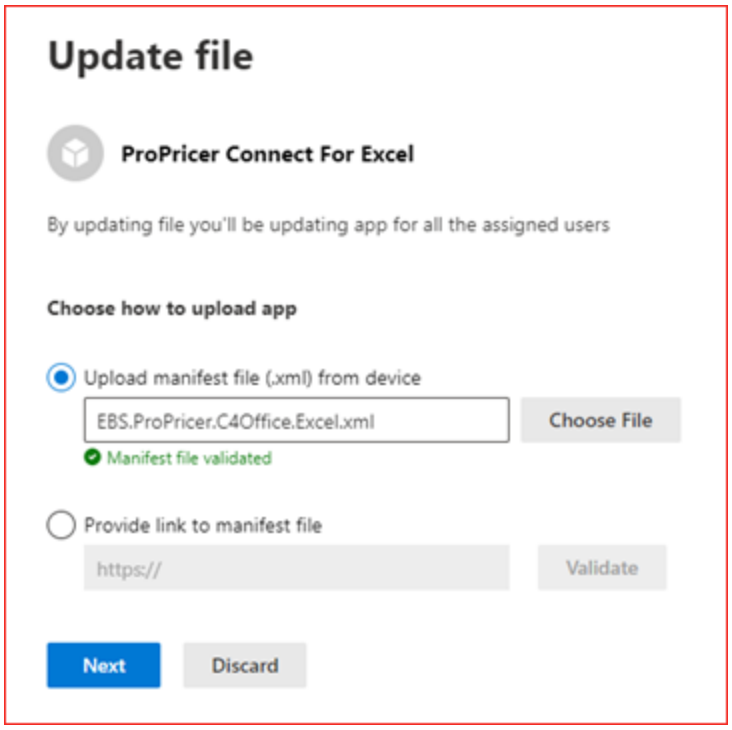
1. Access Microsoft 365 admin center. Then, in the left pane, expand Settings and click Integrated apps.
2. In the Deployed apps tab, you will see your add-ins listed. Select the one you want to update.



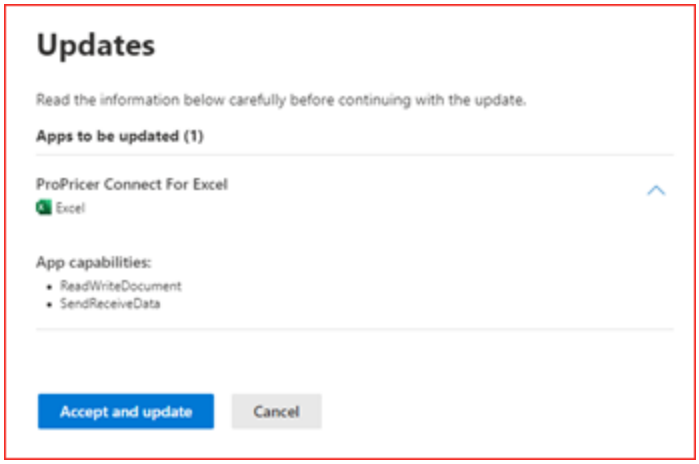
3. In the right-side pane, click Update add-in.



4. Upload the manifest file from your current device or from a link. When you upload the manifest file, it will be validated and any problems will be indicated. Click Next.

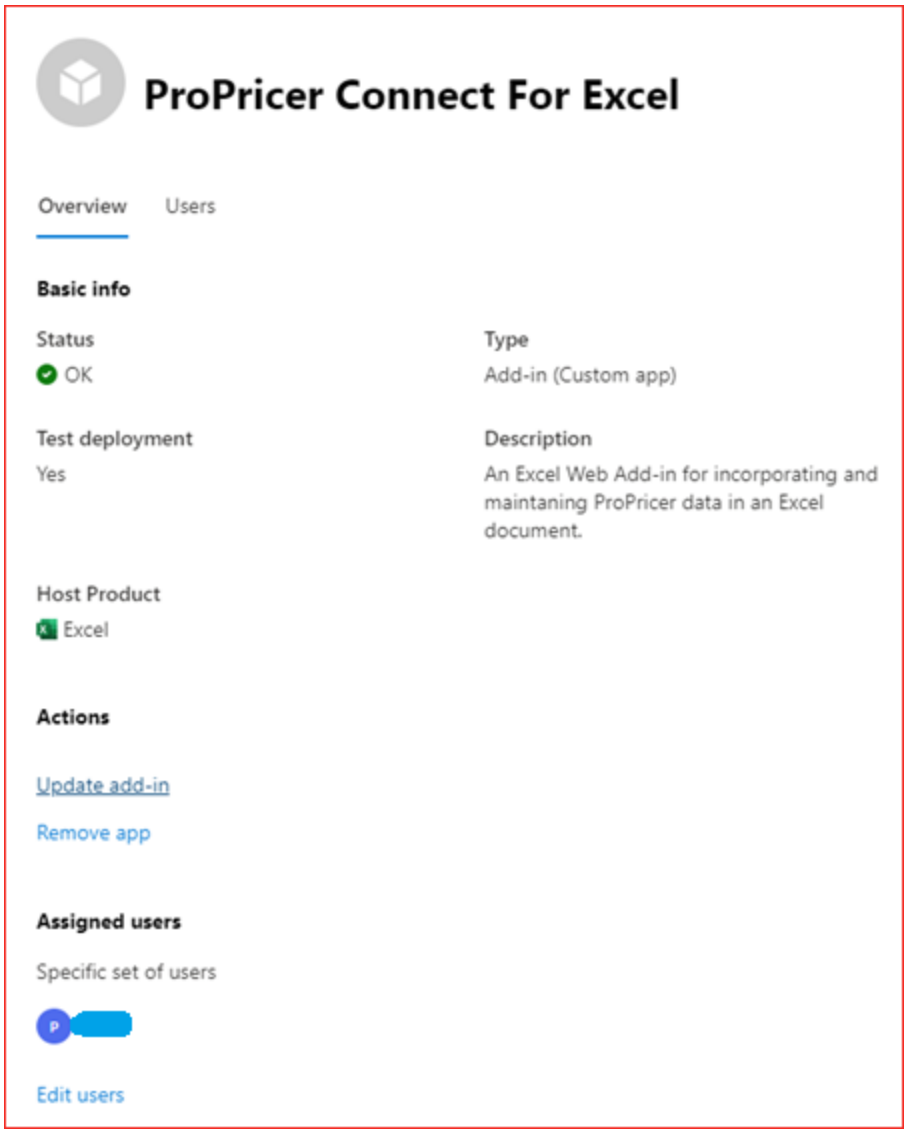


5. Review the update and click Accept and update.



Edit and delete add-ins

1. In the Add-in management pane, you can update, delete and edit the user's access.



Share Point

Summary

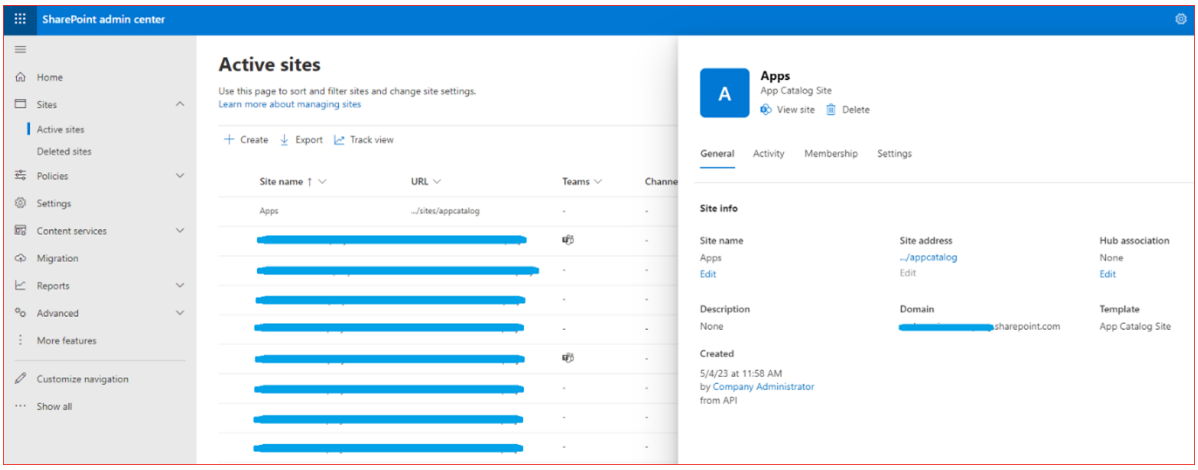
SharePoint is an available option for deploying the add-in to users in your organization, but in this version, this deployment limits certain non-important functionalities. However, it still has all the important Connect for Office features.

To access your SharePoint admin center, go to the SharePoint site which requires your tenant's name: https://TENANTNAME-admin.sharepoint.com/. Then, sign in with an account that has admin permissions for your organization.

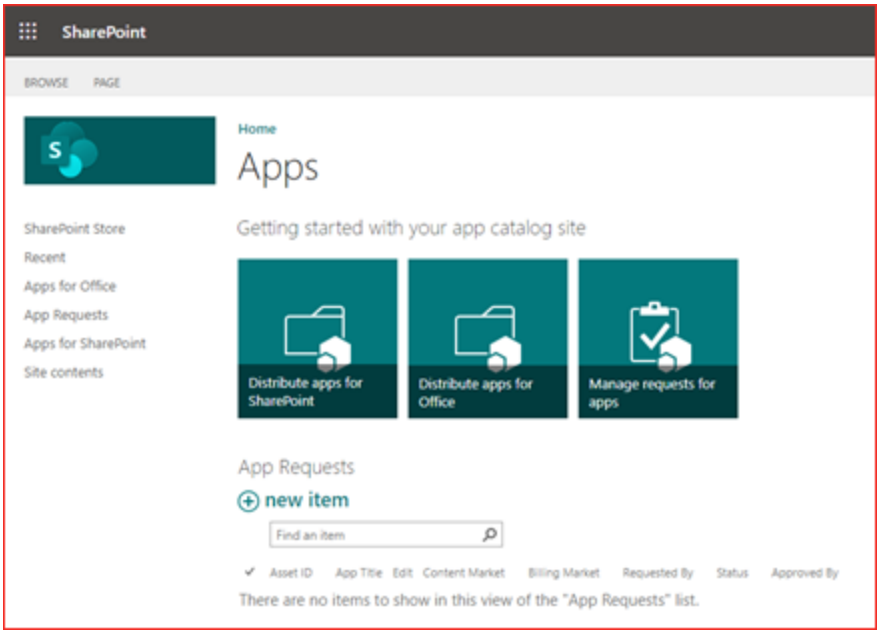
If you're using Microsoft 365, sign into the Microsoft 365 admin center, then go to the SharePoint admin center and open the More features page.

Steps for deployment

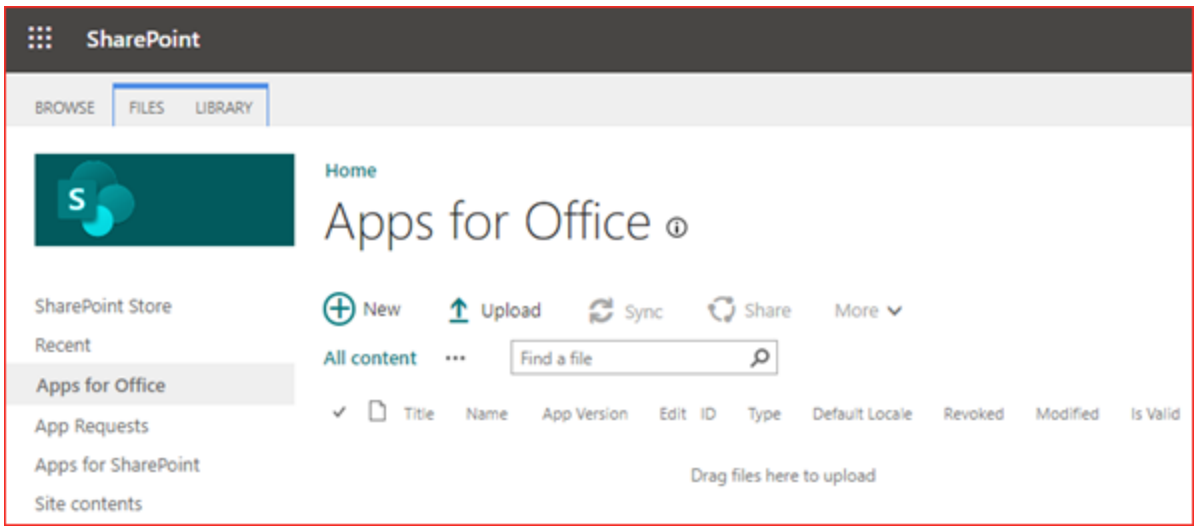
1. In your SharePoint admin center, go to the Active sites page, then on the Apps row, click the site address link or click Apps > View site in the right-side pane.



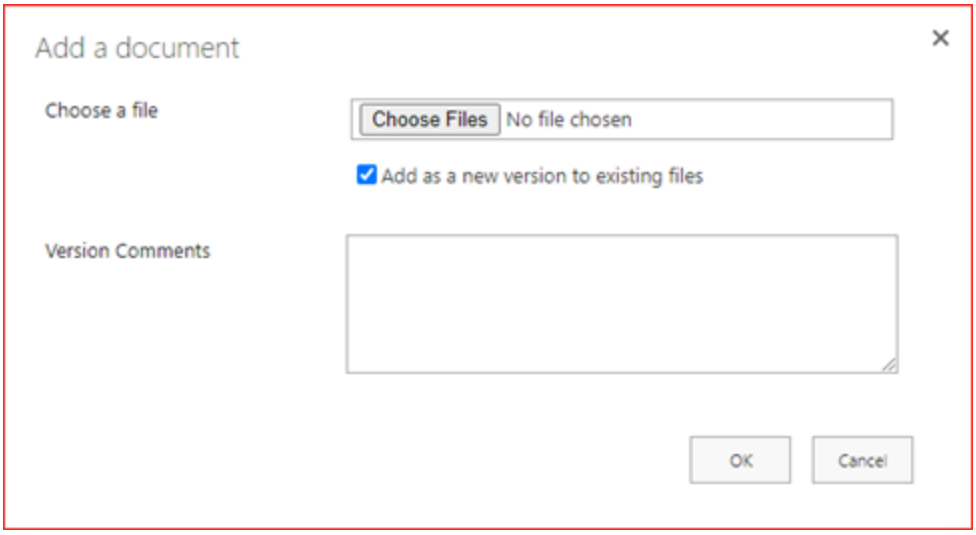
2. On the next page, click Distribute apps for Office.



3. On the Apps for Office page, click New.

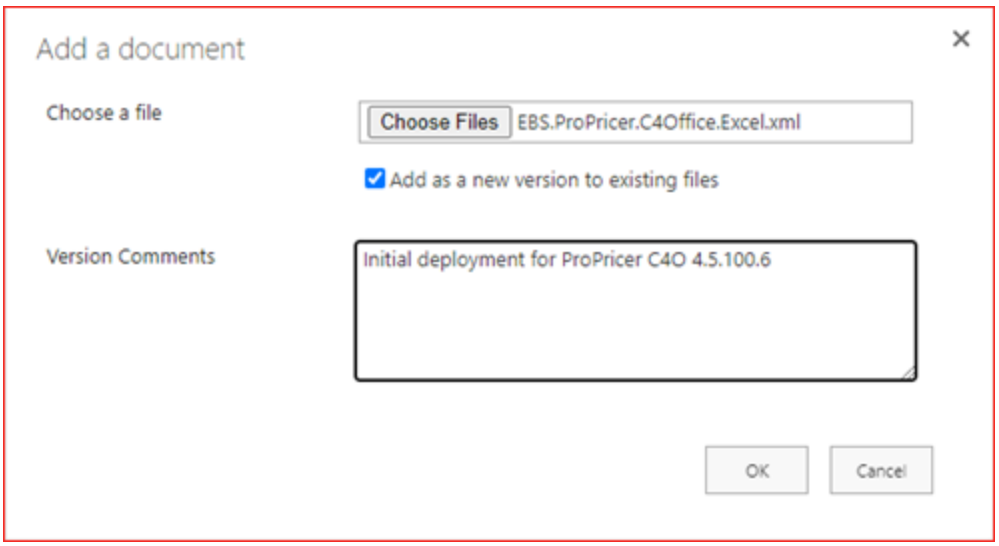


4. In the Add a document window, select Choose Files.

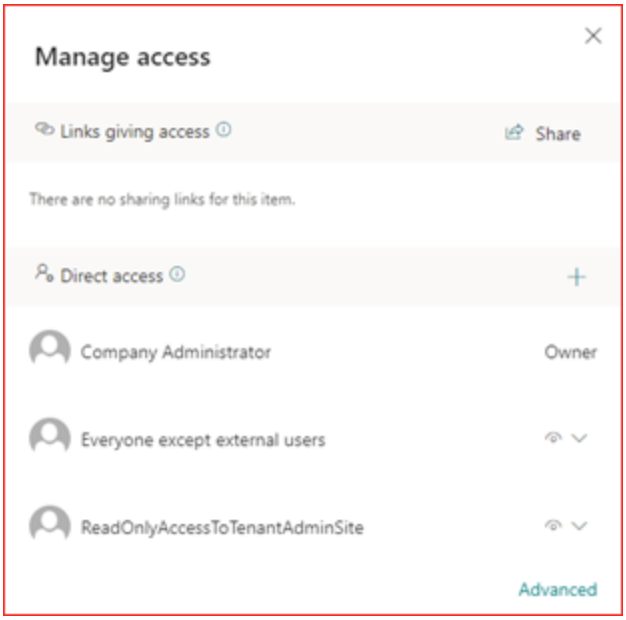


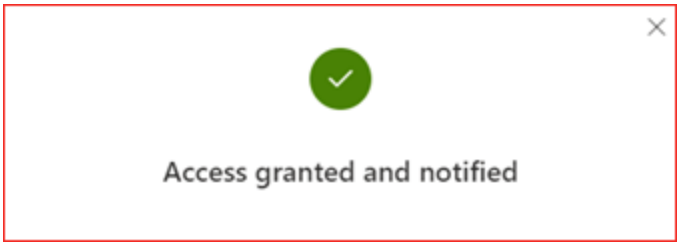
5. Select the manifest file and click Open.

6. In the Add a document window, click OK.



7. After uploading the file, click Apps for Office. Then, click the ellipsis button in the new manifest file and click Manage Access. In this section, you can add or remove permissions for groups or users.





8. Copy the link to your manifest file SharePoint location to distribute it to all users with access to the Add-in.

Steps for deployment with on-premises SharePoint Server

1. Open the Central Administration page.
2. In the left pane, click Apps.
3. On the Apps page, under App Management, click Manage App Catalog.
4. On the Manage App Catalog page, make sure you have the correct web application selected in the Web Application Selector.
5. Click the link under Site URL to open the app catalog site.
6. Click Distribute apps for Office.
7. In the Apps for Office page, click New.
8. In the Add a document dialog box, click Choose Files.
9. Select the manifest file and click Open.
10. In the Add a document dialog, click OK.

Client setup

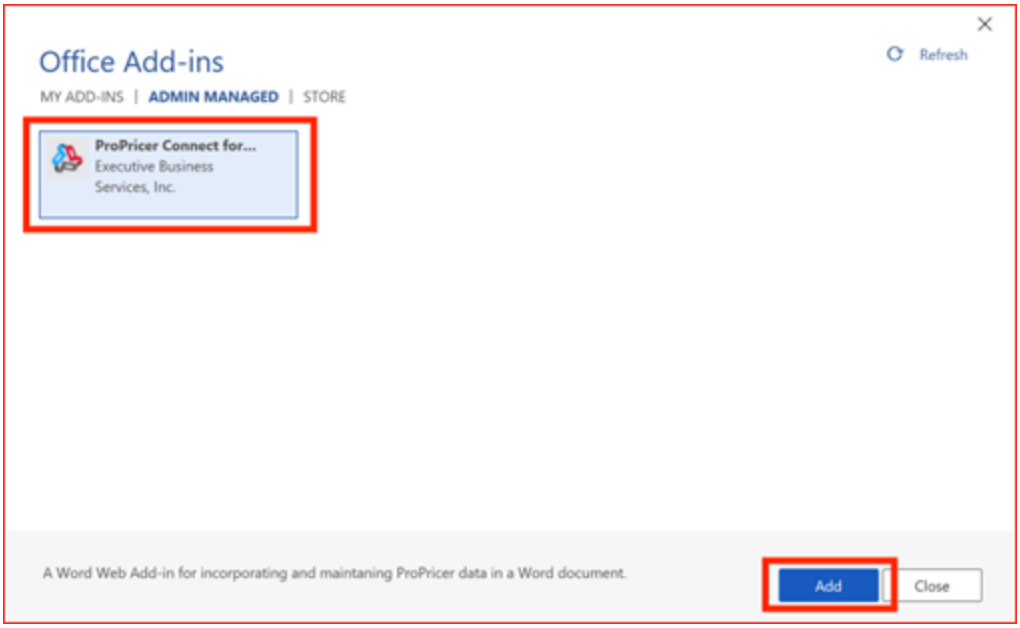
Complete the following steps to find Add-ins for online Office applications.

1. Open the online Office application (Excel, PowerPoint, or Word).
2. Create or open a document.
3. Click Insert > My Add-ins.
4. In the Office Add-ins dialog box, go to the MY ORGANIZATION tab. The Office Add-ins are listed.
5. Select an Office Add-in and click Add.

Complete the following steps to find Add-ins for desktop Office applications.

1. Open the desktop Office application (Excel, Word, or PowerPoint)
2. Go to File > Options > Trust Center > Trust Center Settings > Trusted Add-in Catalogs.
3. Enter the manifest file SharePoint location in the Catalog URL field and choose Add catalog. You'll need to use the shorter form of the URL. For example, if the URL of the SharePoint app catalog is https://<domain>/sites/<AddinCatalogSiteCollection>/AgaveCatalog enter https://<domain>/sites/<AddinCatalogSiteCollection>.
4. Restart the Office application.
5. Click Insert > Get Add-ins.

6. In the Office Add-ins dialog box, go to the MY ORGANIZATION tab. The Office Add-ins are listed.
7. Select a the ProPricer Connect for Word/Excel Add-in and Add.



Alternatively, an administrator can specify an app catalog on SharePoint by using Group Policy. The relevant policy settings are available in the Administrative Template files (ADMX/ADML) for Microsoft 365 Apps, Office LTSC 2021, Office 2019, and Office 2016 and be found under User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Security Settings\Trust Center\Trusted Catalogs.

For government clouds deployment please visit: https://learn.microsoft.com/en-us/office/dev/add-ins/publish/government-cloud-guidance