

# SharePoint Essentials Toolkit 2027 Release

Installation & Deployment Guide

*Last updated Oct 9th 2026*

## Contents

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| Contents .....                                                        | 2  |
| SharePoint Essentials Toolkit Overview .....                          | 7  |
| Minimum Requirements & Supported Environments .....                   | 8  |
| Supported Operating Systems.....                                      | 8  |
| Supported Virtualized Environments .....                              | 8  |
| Supported SharePoint Versions.....                                    | 8  |
| Software Requirements .....                                           | 8  |
| Minimum Hardware Requirements.....                                    | 9  |
| Supported Features: SharePoint Online vs SharePoint On-Premises ..... | 9  |
| Planning the Environment.....                                         | 10 |
| Network Diagram.....                                                  | 10 |
| Open Ports .....                                                      | 10 |
| Local Machine Permissions Required .....                              | 11 |
| SharePoint Permissions Required.....                                  | 11 |
| Data Privacy.....                                                     | 12 |
| Install SharePoint Essentials Toolkit.....                            | 13 |
| Download the Installer.....                                           | 13 |
| Pre-requisites.....                                                   | 13 |
| Silent installation of pre-requisites .....                           | 13 |
| Data & Installation Paths.....                                        | 13 |
| Silent Installation .....                                             | 14 |
| Steps for silent installation .....                                   | 15 |
| Installation Help Switches.....                                       | 15 |
| MSI Package .....                                                     | 16 |
| Troubleshooting Installation.....                                     | 17 |
| Managing Multiple Machine Installations .....                         | 18 |
| Pre-configure License Activation Key.....                             | 18 |
| Pre-configure Settings .....                                          | 18 |
| PowerShell – Update Settings .....                                    | 18 |
| PowerShell – Pre-populate License .....                               | 18 |
| Settings.json File Descriptions.....                                  | 20 |
| Export to Excel Report - Style Settings .....                         | 20 |

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| User Interface Settings .....                                                      | 20 |
| Application Identity .....                                                         | 21 |
| Performance Settings .....                                                         | 22 |
| Timeout Settings .....                                                             | 23 |
| Sync & Governance Settings .....                                                   | 23 |
| WebView2 / Browser Settings .....                                                  | 24 |
| Storage & Database Settings .....                                                  | 24 |
| Discovery Settings & Custom SharePoint Domains .....                               | 24 |
| Proxy Settings.....                                                                | 25 |
| Debug & Logging Settings.....                                                      | 25 |
| Pre-Flight Check Settings.....                                                     | 25 |
| Link Validation Settings .....                                                     | 25 |
| File & Folder Paths .....                                                          | 25 |
| Insights & ScoreCard Thresholds.....                                               | 26 |
| Export Settings .....                                                              | 28 |
| Enterprise Settings (Coming soon) – SPE Enterprise Manager parent application..... | 28 |
| Feature-Specific Settings.....                                                     | 28 |
| Analytics Feature Settings .....                                                   | 29 |
| Copy Feature Settings .....                                                        | 29 |
| Link Feature Settings.....                                                         | 29 |
| Permissions Feature Settings .....                                                 | 30 |
| Discovery Feature Settings .....                                                   | 31 |
| Search Feature Settings .....                                                      | 31 |
| Site Audit Feature Settings .....                                                  | 31 |
| Other Configuration Files .....                                                    | 32 |
| EmailSettings.json.....                                                            | 32 |
| ConnectionProfiles.json .....                                                      | 32 |
| AutoDiscoveryProfiles.json .....                                                   | 34 |
| Checking for Program Updates .....                                                 | 35 |
| Disable Checking for Program Updates .....                                         | 35 |
| Where are Credentials stored? .....                                                | 38 |
| Web Browser Authentication.....                                                    | 38 |
| Username and Password .....                                                        | 38 |

|                                                                                                                   |     |
|-------------------------------------------------------------------------------------------------------------------|-----|
| Certificate Authentication .....                                                                                  | 38  |
| Saving Credentials with Web Browser Authentication .....                                                          | 38  |
| How are Access Tokens Saved? .....                                                                                | 39  |
| Encryption - How is sensitive data stored? .....                                                                  | 40  |
| What data is encrypted by the SharePoint Essentials Toolkit? .....                                                | 40  |
| How is the data encrypted? .....                                                                                  | 40  |
| What else is encrypted? .....                                                                                     | 40  |
| License Activation .....                                                                                          | 41  |
| Online Activation .....                                                                                           | 41  |
| License Server Address - White List .....                                                                         | 42  |
| Offline Activation .....                                                                                          | 43  |
| Azure App Registration .....                                                                                      | 45  |
| SharePoint Essentials Toolkit App Registration in Azure Portal .....                                              | 45  |
| Azure App Registration Overview .....                                                                             | 45  |
| Azure Access Types Supported .....                                                                                | 45  |
| How does authentication work with Web Browser Authentication and Azure app registration? .....                    | 46  |
| Register the application .....                                                                                    | 47  |
| (Very Easy) Fully Automated using app wizard .....                                                                | 47  |
| (Easy) Partially Automated using a Link .....                                                                     | 61  |
| (Medium Effort (longest time)) Manual Registration using Azure Portal – (more control over API permissions) ..... | 70  |
| (Medium Effort) Manual Registration using PowerShell .....                                                        | 87  |
| Updating an Existing Azure App Registration for New Features .....                                                | 92  |
| API Permissions for CERTIFICATE Based Authentication (without User Activity Services) .....                       | 93  |
| API Permissions for DELEGATED Authentication (without User Activity Services) .....                               | 94  |
| API Permissions for USER ACTIVITY App Registration (CERTIFICATE) .....                                            | 95  |
| Configure Web Browser Authentication (WBA) to use Azure App Registration in SharePoint Essentials Toolkit .....   | 95  |
| Fully Automated – using app Wizard .....                                                                          | 97  |
| Partially Automated - Multitenant Setup – using URL .....                                                         | 97  |
| Manual Setup - Single Tenant Setup .....                                                                          | 98  |
| Test the Connection .....                                                                                         | 100 |
| Certificate based Authentication .....                                                                            | 102 |
| What is Azure App Registration Certificate-Based Authentication? .....                                            | 102 |

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| Benefits of setting up Certificate based authentication .....         | 102 |
| Drawbacks of Certificate based authentication .....                   | 102 |
| Using the Azure Key Vault.....                                        | 103 |
| Configure Certificate based authentication .....                      | 103 |
| Create the certificate .....                                          | 103 |
| Upload the certificate to Azure .....                                 | 103 |
| Setup Governance & User Activity Features.....                        | 106 |
| Supported Environments .....                                          | 106 |
| Unsupported Environments .....                                        | 106 |
| Required Microsoft 365 licenses .....                                 | 106 |
| Who can view User Activity? .....                                     | 106 |
| Setup & Configuration.....                                            | 106 |
| Pre-requisites .....                                                  | 106 |
| Add the connection for the Governance and User Activity services..... | 106 |
| Scheduled Jobs.....                                                   | 110 |
| PowerShell Support.....                                               | 111 |
| Sensitivity Labels and Microsoft 365 Archive .....                    | 112 |
| Reading Sensitivity Labels in Reports .....                           | 112 |
| What it does .....                                                    | 112 |
| How it works .....                                                    | 112 |
| Requirements .....                                                    | 112 |
| Good to know .....                                                    | 112 |
| Applying Sensitivity Labels in Bulk .....                             | 113 |
| What it does .....                                                    | 113 |
| How it works .....                                                    | 113 |
| Requirements .....                                                    | 113 |
| Step A — App registration .....                                       | 114 |
| Step B — Link the app to an Azure subscription .....                  | 114 |
| Step C — PDF support (optional) .....                                 | 115 |
| Step D — Toolkit connection.....                                      | 115 |
| Step E — Test with one file .....                                     | 115 |
| Label requirements .....                                              | 115 |
| Troubleshooting.....                                                  | 116 |

|                                |     |
|--------------------------------|-----|
| Cost control.....              | 116 |
| Microsoft 365 Archive .....    | 116 |
| What it does .....             | 116 |
| How it works .....             | 117 |
| Requirements .....             | 117 |
| Setup .....                    | 117 |
| What users should expect ..... | 118 |
| Troubleshooting.....           | 118 |
| Quick Reference .....          | 118 |
| Reference .....                | 119 |

## SharePoint Essentials Toolkit Overview

The SharePoint Essentials Toolkit is designed for SharePoint Site Collection Administrators and Site Owners. The product has many features to assist admins and Site Owners with SharePoint Administrative tasks.

# Minimum Requirements & Supported Environments

## Supported Operating Systems

- Microsoft Windows 10 (64-bit only)
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2025

## Supported Virtualized Environments

Below is a list of virtual machine solutions that have been tested, and work with, the SharePoint Essentials Toolkit. If you have a solution not listed below, you may contact us to verify it is a supported virtualized environment.

- Microsoft Hyper V
- Microsoft Azure Hypervisor
- Amazon Elastic Compute Cloud
- VMWare
- Citrix Workspace

## Supported SharePoint Versions

- SharePoint Online
- SharePoint Subscription Edition
- SharePoint Server 2019
- SharePoint Server 2016 (limited support)

---

*NOTE: For customers with SharePoint Server 2013 and older, or who need full SharePoint Server 2016 support, use SharePoint Essentials Toolkit 2019 (Classic). License included.*

---

## Software Requirements

The software pre-requisites are automatically installed by the application's installer. They can also be manually installed using links below.

- Microsoft .NET Core Desktop - .NET Desktop Runtime (x64)
  - <https://dotnet.microsoft.com/en-us/download/dotnet/>
- Microsoft WebView2
  - <https://developer.microsoft.com/en-us/microsoft-edge/webview2/>
- Microsoft Visual C++ Redistributable x64
  - [https://aka.ms/vs/17/release/vc\\_redist.x64.exe](https://aka.ms/vs/17/release/vc_redist.x64.exe)

## Minimum Hardware Requirements

- Processor Architecture: 64-bit Intel/AMD (32-bit and ARM64 are not supported)
- Processor Speed: Minimum Dual-Core 3GHz
- RAM: 8GB Minimum, 16GB or above recommended.
- Display: Resolution of 1366x768 or higher. We recommend monitor resolution of 1920x1080 or higher for optimal viewing.

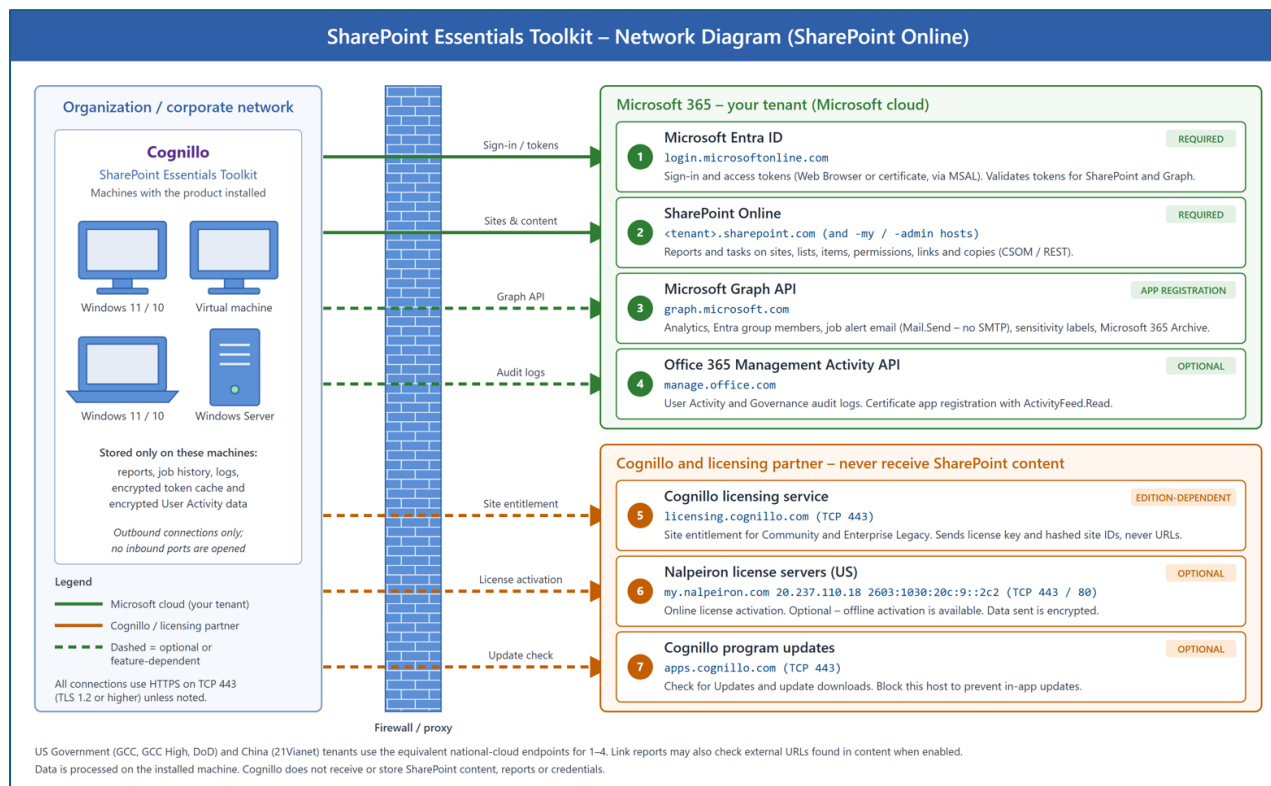
## Supported Features: SharePoint Online vs SharePoint On-Premises

Below features are **only available** in SharePoint Online

| Feature                          | SharePoint Online | SharePoint On-premises               |
|----------------------------------|-------------------|--------------------------------------|
| User Activity                    | Yes               | Not supported                        |
| Site & List Item Analytics       | Yes               | Not supported                        |
| Permissions Domain Group Members | Yes               | Not supported – Use SPE 2019 version |
| Governance                       | Yes               | Not supported                        |
|                                  |                   |                                      |

# Planning the Environment

## Network Diagram



## Open Ports

If using the online activation model (see below), the following must not be blocked:

|                                                                                                                                                                                 |                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <b>DNS</b>                                                                                                                                                                      | my.nalpeiron.com     |
| <b>IPv4</b>                                                                                                                                                                     | 20.237.110.18        |
| <b>IPv6</b>                                                                                                                                                                     | 2603:1030:20c:9::2c2 |
| <b>Port</b>                                                                                                                                                                     | 80 and 443*          |
| *All data sent to Nalpeiron is encrypted, regardless of http/https protocol.                                                                                                    |                      |
| NOTE: Nalpeiron license activation is optional.                                                                                                                                 |                      |
| NOTE: The Cognillo license server must also not be blocked (required for Community Edition license): licensing.cognillo.com, port 443. See License Server Address - White List. |                      |

For the in-app “Check for Updates” button to work, the following must not be blocked:

|             |                           |
|-------------|---------------------------|
| <b>DNS</b>  | https://apps.cognillo.com |
| <b>Port</b> | 443 only                  |

## Local Machine Permissions Required

Local machine - local admin rights required to install. Standard user on local machine to run the tool.

## SharePoint Permissions Required

We recommend the user to have Site Owner or Site Collection (SC) administrator rights to run all reports and management tasks.

Below is a breakdown of features and required permissions:

| Component / Feature                                               | Minimum Permissions Required                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Permission Reports                                                | Enumerate permissions level                                                                                                                                                                                                                                                        |
| Permission Reports + Sharing Link Details                         | **Enumerate permissions level                                                                                                                                                                                                                                                      |
| Permission Reports + Entra Domain Group Members                   | **Enumerate permissions level                                                                                                                                                                                                                                                      |
| Permission Changes                                                | Full control or SC Admin                                                                                                                                                                                                                                                           |
| Add/Remove Site Collection Admins                                 | SC Admin                                                                                                                                                                                                                                                                           |
| Remove User                                                       | Full control or SC Admin                                                                                                                                                                                                                                                           |
| Clone User                                                        | Full control or SC Admin                                                                                                                                                                                                                                                           |
| Orphaned Users Report                                             | Full control or SC Admin                                                                                                                                                                                                                                                           |
| Copy Lists                                                        | Full control or SC Admin                                                                                                                                                                                                                                                           |
| Link Reports                                                      | Read permission level                                                                                                                                                                                                                                                              |
| Link Find & Replace                                               | Edit permission level                                                                                                                                                                                                                                                              |
| Link Find & Replace + Preserve Author (Last Modified information) | SC Admin or Full Control<br>Needed to preserve last modified date and person. Prevents job from showing current user who ran job as last modified person for all changed files/items/pages. See <a href="#">How to Automatically Fix Links in SharePoint</a> for more information. |
| Site and Content Activity                                         | **Full control or SC Admin                                                                                                                                                                                                                                                         |
| Site, List and Item Inventory                                     | Read permission level at site, list and item level                                                                                                                                                                                                                                 |
| Content Type Inventory                                            | Read permission level at site and list level                                                                                                                                                                                                                                       |
| Content Search                                                    | Read permission level                                                                                                                                                                                                                                                              |
| Content Search & Replace                                          | Full control or SC Admin                                                                                                                                                                                                                                                           |
| User Activity Reports                                             | **Full control or SC Admin                                                                                                                                                                                                                                                         |
| Checked Out File Reports                                          | Read permission level                                                                                                                                                                                                                                                              |
| **Requires Azure App Registration                                 |                                                                                                                                                                                                                                                                                    |

## Data Privacy

The SharePoint Essentials Toolkit is installed on your network environment. Your data is not passed through Cognillo or other third parties. Data is processed locally on the installed machine. Cognillo does not have access to your organization's data.

For more information, see [Is our data private? Do you share PII \(Personally Identifiable Information\) with outside parties?](#)

NOTE: If using online license activation, users may provide an email address to associate with the license activation. This is optional and is not required, a machine name or other generic value can be used, it is strictly to assist customers in case they need to track down license use.

# Install SharePoint Essentials Toolkit

## Download the Installer

- [Download SharePoint Essentials Toolkit Full](#) (EXE)
- [Download SharePoint Essentials Toolkit Full](#) (MSI)

## Pre-requisites

- Installation should automatically install pre-requisites needed:
  - Microsoft NET Desktop Runtime (.NET Core)  
[Download link](#)
  - Microsoft Webview2 for browser authentication support  
[Download link](#)
  - Microsoft Visual C++ Redistributable  
[Download link](#)
- A local machine Administrator is required to install the application
- A local machine User can use the application (does not require local admin to run)

## Silent installation of pre-requisites

To silently install pre-requisites, you may use the commands below:

### WebView2 Runtime

MicrosoftEdgeWebview2Setup.exe /silent /install

### .NET 8 Desktop Runtime (x64)

windowsdesktop-runtime-8.x.x-win-x64.exe /install /quiet /norestart

### Visual C++ Redistributable

vc\_redist.x64.exe /install /quiet /norestart

**NOTE:** Microsoft Office and Adobe PDF are NOT required to be installed. However, the SharePoint Essentials Toolkit reports are in Excel format and would be easier for users to view if Excel is installed.

## Data & Installation Paths

The following directories are automatically created during installation.

- **Program binaries (default location)**
  - C:\Program Files\Cognillo\SharePoint Essentials Toolkit
  - This path can be changed during installation.
- **User data**
  - C:\Users\<username>\Documents\SharePoint Essentials Toolkit
  - Stores information such as reports, application logs and exported data.

- User data paths such as report paths, can be changed in the configuration file Settings.json (see below).
- **User settings file**
  - C:\Users\<username>\AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\Config\Settings.json
  - Stores information such as report file paths, and application level settings.
  - This path cannot be changed.
- **User system config data**
  - C:\Users\<username>\AppData\Roaming\Cognillo\SharePoint Essentials Toolkit
  - Stores information such as license cache, token cache (encrypted), webview2 data (for web browser authentication), installation and application update logs.
  - These paths are found in the Settings.json file and can be changed.
- **Governance & User Activity Data**
  - C:\Users\<username>\AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\Governance\User Activity Data\
  - Stores encrypted user activity data.
  - These paths are found in the Settings.json file and can be changed.

## Silent Installation

If you need to deploy the SharePoint Essentials Toolkit silently, this can be done using several command line switches/options, see below.

### MSI Silent Installation

`msiexec /I "C:\Install\SharePoint Essentials Toolkit.msi" /qn`

### Exe Silent Installation

`"C:\Install\SharePoint Essentials Toolkit.exe" /exenoui /qn`

### Run Elevated Command Prompt Window

*Be sure to execute the command prompt window elevated (Run as Administrator).*

### PowerShell

To use PowerShell, see example below which requires the & call operator:

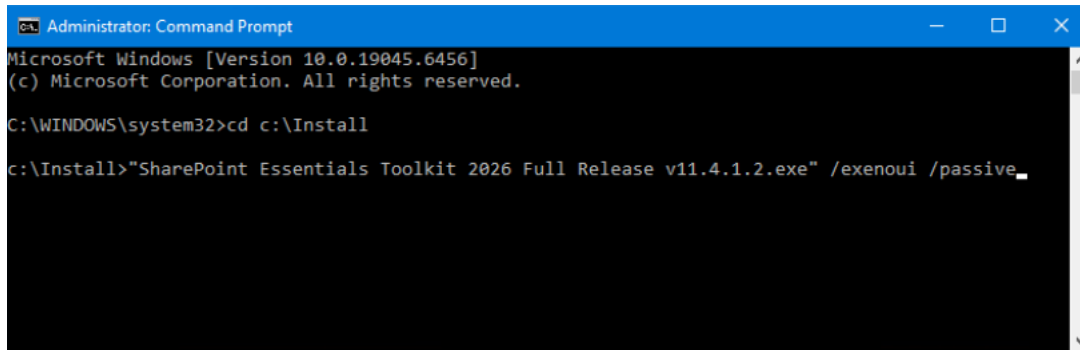
`& "C:\Path\SharePoint Essentials Toolkit 2027 Full Release v12.1.0.0.exe" /qn`

### Switch Options

- /qn - completely silent, no UI
- /qb - basic UI (progress bar only)
- /qn+ - silent but shows completion dialog
- /passive - unattended mode with progress bar
- /l\*v install.log - verbose logging

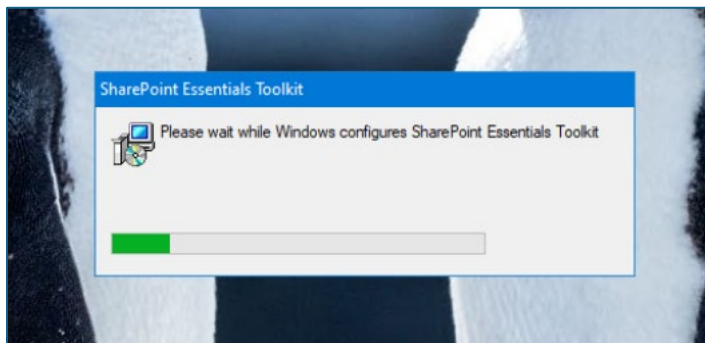
## Steps for silent installation

1. Download the SharePoint Essentials Toolkit, copy the path to the executable or MSI installation file.
2. Open the Command Prompt as a Local Administrator
3. Paste into the Command Prompt window by Right Clicking->Paste
4. Use one of the switches above to install the SharePoint Essentials Toolkit (example below)



5. Press Enter to execute silent installation

Below is a screenshot when using /exenoui /qb – which will install unattended but with a progress window:



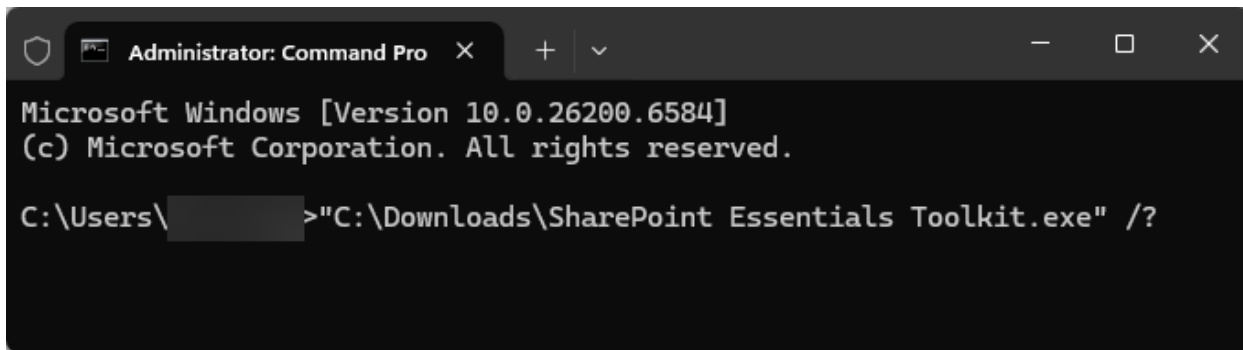
## Installation Help Switches

You can access all installation switches by using the /? Flags in a command prompt.

Right click the downloaded installation file and click 'Copy as path'

Click the Windows Start menu and open a Command Prompt, right click to paste.

Add /? To the end of the path like below:



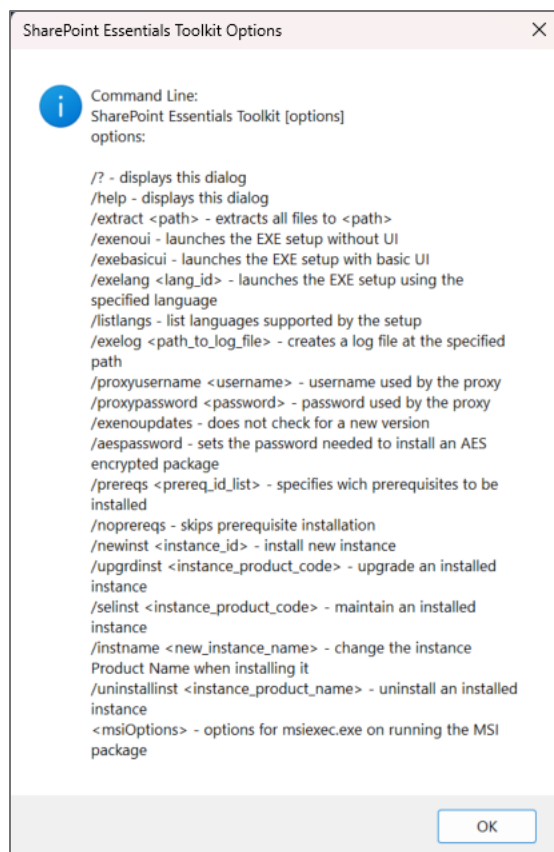
```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.26200.6584]
(c) Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>"C:\Downloads\SharePoint Essentials Toolkit.exe" /?

```

Press “Enter”, in a few moments the below dialog will appear.



## MSI Package

If you require the MSI package file, you can download the package using link below.

This is a permalink, which will always have the latest build:

- [Download SharePoint Essentials Toolkit Full](#) (MSI)

### Example Usage:

```

msiexec.exe /i "<Path>\SharePointEssentialsToolkitSetupMSI.msi" /passive
msiexec.exe /i "<Path>\SharePointEssentialsToolkitSetupMSI.msi" /quiet
msiexec.exe /i "<Path>\SharePointEssentialsToolkitSetupMSI.msi" /quiet SETUPEXEDIR=1

```

**NOTE:** “*SETUPEXEDIR=1*” may be required for the command line execution to work.

## Troubleshooting Installation

In the event you see installation errors. You can enable verbose logging by following steps below.

In the MSI Command Line field, specify the logging parameters,

For example: `/L*V "C:\package.log"`

This will create a verbose log file named "package.log" in the C: drive when the user launches the installation via the bootstrapper.

## Managing Multiple Machine Installations

If you need to pre-configure the license and settings for multiple machines that will have the SharePoint Essentials Toolkit installed, you may follow steps below to configure the settings and license information.

The steps below requires the use of a software packaging platform and/or PowerShell to write to values JSON files.

### Pre-configure License Activation Key

To pre-assign license keys for multiple users, you will need to open and write to the following entry POST-installation.

C:\Users\<username> \AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\License\License.json

NOTE: On older installations, it will be in the 'Local' application path (instead of 'Roaming').

### Pre-configure Settings

To pre-assign settings for multiple users, you will need to open and write to the following file POST-installation.

C:\Users\<username> \AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\Config\Settings.json

This is a standard JSON file. You can use PowerShell to open and write values to any of the properties within this file. See example below:

### PowerShell – Update Settings

Example PowerShell to modify the Settings.json values:

```
$path = "$env:APPDATA\Cognillo\SharePoint Essentials Toolkit\Config\Settings.json"
```

```
$settings = Get-Content $path -Raw | ConvertFrom-Json
```

```
$settings.MaxParallelSiteJobThreads = "3"
```

```
$settings.LargeJobThreshold = "50"
```

```
$settings.ExportStyle_Header_BackgroundHex = "#0078D4"
```

```
$settings | ConvertTo-Json -Depth 10 | Set-Content $path
```

### PowerShell – Pre-populate License

It is not recommended to attempt to modify values other than the LicenseEmail and LicenseCode.

```
param(
[Parameter(Mandatory=$true)]
[string]$LicenseEmail,
[Parameter(Mandatory=$true)]
[string]$LicenseCode
)

$path = "$env:APPDATA\Cognillo\SharePoint Essentials Toolkit\License\License.json"

$license = Get-Content $path -Raw | ConvertFrom-Json

$license.LicenseEmail = $LicenseEmail

$license.LicenseCode = $LicenseCode

$license | ConvertTo-Json -Depth 10 | Set-Content $path

Write-Host "License updated successfully"

Write-Host " Email: $LicenseEmail"

Write-Host " Code: $LicenseCode"
```

**Usage (PowerShell)**

```
.\Update-License.ps1 -LicenseEmail "customer@company.com" -LicenseCode
"123456789012345678"
```

## Settings.json File Descriptions

### Export to Excel Report - Style Settings

| Setting                          | Type    | Description                                                                |
|----------------------------------|---------|----------------------------------------------------------------------------|
| ExportStyle_Header_BackgroundHex | Color   | Background color for header rows in exported Excel files (ARGB hex format) |
| ExportStyle_Header_ForegroundHex | Color   | Text color for header rows in exported Excel files                         |
| ExportStyle_Group1_BackgroundHex | Color   | Background color for first-level grouping rows                             |
| ExportStyle_Group1_ForegroundHex | Color   | Text color for first-level grouping rows                                   |
| ExportStyle_Group2_BackgroundHex | Color   | Background color for second-level grouping rows                            |
| ExportStyle_Group2_ForegroundHex | Color   | Text color for second-level grouping rows                                  |
| ExportStyle_Group3_BackgroundHex | Color   | Background color for third-level grouping rows                             |
| ExportStyle_Group3_ForegroundHex | Color   | Text color for third-level grouping rows                                   |
| ExportStyle_Group4_BackgroundHex | Color   | Background color for fourth-level grouping rows                            |
| ExportStyle_Group4_ForegroundHex | Color   | Text color for fourth-level grouping rows                                  |
| ExportStyle_Group5_BackgroundHex | Color   | Background color for fifth-level grouping rows                             |
| ExportStyle_Group5_ForegroundHex | Color   | Text color for fifth-level grouping rows                                   |
| ExportExcelCellBorderColorHex    | Color   | Border color for Excel cells                                               |
| IsExportGroupHeadersBold         | Boolean | Makes group header text bold in exports                                    |
| IsExportShowGroupCount           | Boolean | Shows item count next to group headers                                     |

### User Interface Settings

| Setting                             | Type    | Description                                                                           |
|-------------------------------------|---------|---------------------------------------------------------------------------------------|
| ShowWizardTips                      | Boolean | Shows helpful wizard tip popups throughout the UI                                     |
| IsDetectExistingAppFocusOnStart     | Boolean | Detects if another instance is running and focuses it instead of opening a new window |
| IsMinimizeOnClose                   | Boolean | Minimizes to system tray instead of closing when clicking the X button                |
| LiveExplorerSortOrder               | Integer | Sort order for Live Explorer view (0=Default, 1=Alphabetical, etc.)                   |
| ExpandHomePageDirectoryOnStartup    | Integer | Controls auto-expansion of site directory on startup (0=None, 1=First level, etc.)    |
| MaxSitesToRenderListsInLiveExplorer | String  | Maximum number of sites to show lists for in Live Explorer (performance)              |

| Setting                            | Type    | Description                                                                                    |
|------------------------------------|---------|------------------------------------------------------------------------------------------------|
| MaxSitesToRenderListsInJobOptions  | String  | Maximum number of sites to show lists for in job options dialog                                |
| MaxRecordsToDisplayPerGridReport   | String  | Maximum rows to display in report grids (prevents UI slowdown)                                 |
| HomePageDeletionBehavior           | Integer | Behavior when deleting sites from home page (0=Recycle, 1=Permanent)                           |
| IsAlwaysShowSyncIcon               | Boolean | Always shows the sync icon in the UI                                                           |
| IsWizardHomeView                   | Boolean | Opens the home page in the task-based wizard view.                                             |
| StartPage                          | Integer | Page shown when the application starts. Stored as a number (default 1).                        |
| UiTheme                            | Integer | Color theme used by the application (0 = default).                                             |
| UiTextSize                         | Integer | Text size used in the user interface (0 = default).                                            |
| SiteDirectorySortOrder             | Integer | Sort order of sites in the site directory (0 = default).                                       |
| RecentTaskTitles                   | Array   | Titles of the most recently used wizard tasks, shown as shortcuts. Maintained automatically.   |
| RecentJobTemplates                 | Array   | Most recently used job templates. Maintained automatically.                                    |
| ExportToSharePointRecentSiteUrls   | Array   | Most recently used SharePoint site URLs for exporting to SharePoint. Maintained automatically. |
| HomeViewLayoutState                | Object  | Saved layout and panel states of the home view. Maintained automatically; do not edit.         |
| ReportColumnSelectionsByReportType | Object  | Saved column selections for each report type. Maintained automatically.                        |
| ReportGridLinesByReportType        | Object  | Saved grid line preference for each report type. Maintained automatically.                     |

## Application Identity

| Setting                      | Type    | Description                                                                                                                                |
|------------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------|
| SPEInstanceId                | GUID    | Unique identifier for this SPE installation instance. Used for telemetry, added password salt, and multi-instance detection.               |
| AutoDeactivateLicenseOnClose | Boolean | Automatically deactivates the license when the application closes, releasing the activation so the license can be used on another machine. |

## Performance Settings

| Setting                                 | Type    | Description                                                                                         |
|-----------------------------------------|---------|-----------------------------------------------------------------------------------------------------|
| LargeJobThreshold                       | String  | Number of items that triggers "large job" optimizations                                             |
| IsAutomaticallySettingJobPerformance    | Boolean | Auto-tunes job performance based on workload                                                        |
| UseCacheForCalculatingJobProgress       | Boolean | Uses cached data for progress calculations (faster but less accurate)                               |
| ExportListItemsBatchSize                | String  | Number of items to export to SharePoint per batch                                                   |
| ExportBatchThreadLimit                  | String  | Maximum concurrent export threads                                                                   |
| FetchItemsBatchSize                     | String  | Number of SharePoint items to fetch per request                                                     |
| ParseItemsBatchSize                     | String  | Number of items to parse in parallel                                                                |
| MaxParallelSiteJobThreads               | String  | Max concurrent site processing threads for regular jobs                                             |
| MaxParallelSiteJobThreads_Sync          | String  | Max concurrent threads for sync operations                                                          |
| ClientContextExecuteMaxConcurrentCalls  | String  | Max concurrent CSOM calls to SharePoint                                                             |
| ReportClearFromMemoryRowThreshold       | String  | Row count above which report data is cleared from memory to reduce memory use.                      |
| IntervalToSaveReportsToExcelMinutes     | String  | Interval, in minutes, at which report data is periodically saved to Excel during long-running jobs. |
| EnableSqliteReportStorage               | Boolean | Stores report data in a local SQLite database to reduce memory use with large reports.              |
| IsLazyingLoadField_CreatedBy            | Boolean | Loads the Created By field only when needed, which can speed up jobs.                               |
| IsLazyingLoadField_Editor               | Boolean | Loads the Modified By (Editor) field only when needed, which can speed up jobs.                     |
| IsLazyingLoadField_FileDetails          | Boolean | Loads file detail fields only when needed, which can speed up jobs.                                 |
| AlwaysExcludedFieldInternalNames        | Array   | Internal names of fields that are always excluded from reports (default: TaxKeyword).               |
| MaxSkippedItemLogEntriesPerJob          | String  | Maximum number of skipped-item entries logged for a single job.                                     |
| SiteAuditSyncIdleMinutesBeforeFullSpeed | String  | Minutes of inactivity before Site Audit synchronization runs at full speed.                         |
| MonitorJobIdleMinutesBeforeFullSpeed    | String  | Minutes of inactivity before monitor jobs run at full speed.                                        |

## Timeout Settings

| Setting                                 | Type   | Description                                                                   |
|-----------------------------------------|--------|-------------------------------------------------------------------------------|
| SiteConnectionTimeoutSeconds            | String | Timeout for site-level SharePoint operations                                  |
| ListConnectionTimeoutSeconds            | String | Timeout for list-level SharePoint operations                                  |
| ItemConnectionTimeoutSeconds            | String | Timeout for item-level SharePoint operations                                  |
| MaxItemProcessingTimeoutSeconds         | String | Maximum time allowed to process a single item before it's marked as timed out |
| ThrottlingMaxWaitTimeInLockStateSeconds | String | Max wait time when SharePoint throttles requests                              |
| ThrottlingBackoffWaitIntervalSeconds    | String | Base wait interval between retry attempts when throttled                      |
| ClientContextExecuteMaxRetryCount       | String | Number of retry attempts for failed SharePoint calls                          |

## Sync & Governance Settings

| Setting                                              | Type    | Description                                                                                                                                       |
|------------------------------------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| IsSyncSitesAtStartup                                 | Boolean | Syncs site data when application starts                                                                                                           |
| SyncHomePageDashboardHours                           | String  | How often to sync home page dashboard data (in hours)                                                                                             |
| HomePageDashboardBackupCount                         | String  | Number of dashboard backup files to retain                                                                                                        |
| EnableGovernanceDataCollectionService                | Boolean | Enables background governance data collection                                                                                                     |
| EnableGovernanceDataCollectionServiceHighPerformance | Boolean | Uses aggressive caching for governance (higher memory usage)                                                                                      |
| IncludeSyncJobsInJobHistory                          | Boolean | Includes sync operations in job history                                                                                                           |
| ExcludeInsightsSystemLists                           | Boolean | Excludes SharePoint system lists from insights                                                                                                    |
| ExcludeInsightsSystemSites                           | Boolean | Excludes system sites from insights                                                                                                               |
| EnableScheduledJobs                                  | Boolean | Enables the Scheduled Jobs feature.                                                                                                               |
| RunScheduledJobsAsSystem                             | Boolean | Runs scheduled jobs under the Windows SYSTEM account instead of the signed-in user.                                                               |
| ScheduledJobsTestMode                                | Boolean | Runs scheduled jobs in test mode. Intended for troubleshooting only.                                                                              |
| SharedScheduledJobsPath                              | String  | Folder where shared scheduled job definitions are stored (default: C:\ProgramData\Cognillo\SharePoint Essentials Toolkit\Shared Scheduled Jobs\). |
| PermissionChangeSnapshotRetentionDays                | String  | Number of days permission change snapshots are kept (default 30).                                                                                 |
| SharingLinkExpirationAdjustmentDays                  | String  | Number of days used when adjusting the expiration of sharing links (default 30).                                                                  |

## WebView2 / Browser Settings

| Setting                                 | Type    | Description                                                      |
|-----------------------------------------|---------|------------------------------------------------------------------|
| IsAutoSaveWebBrowserAuthCredentials     | Boolean | Automatically saves authentication cookies from browser          |
| WebView2UserAgent                       | String  | User agent string for WebView2 browser component                 |
| UseCustomWebView2UserAgent              | Boolean | Enables custom user agent string                                 |
| IsWebView2DPIAwareOverride              | Boolean | Overrides DPI awareness for WebView2 (fixes scaling issues)      |
| IsWebView2UseCustomFolderForEachProfile | Boolean | Uses separate browser profile folders per SharePoint environment |
| IsClearWBACacheAtJobAtStart             | Boolean | Clears Web Browser Authentication cache at job start             |

## Storage & Database Settings

| Setting                                  | Type    | Description                                                                 |
|------------------------------------------|---------|-----------------------------------------------------------------------------|
| EnableJobHistoryRealTimeDatabaseStorage  | Boolean | Saves job history to disk in real-time (prevents data loss on crash)        |
| MaxJobsInJobHistory                      | String  | Maximum number of jobs to keep in history                                   |
| AppStorageType                           | Integer | Storage backend type (0=File System, 1=CosmosDB) (Use 0, CosmosDB not used) |
| AzureCosmosDbStoragePrimaryKey_Encrypted | String  | Encrypted CosmosDB connection key (not in use)                              |
| SiteAuditsCosmosDBId                     | GUID    | CosmosDB database ID for site audit data (not in use)                       |
| AzureStorageAccountName                  | String  | Azure Storage account name for Migration API                                |
| AzureStorageAccountTempDataFolderPath    | String  | Local temp folder for Migration API operations                              |

## Discovery Settings & Custom SharePoint Domains

| Setting                          | Type   | Description                                   |
|----------------------------------|--------|-----------------------------------------------|
| MaxDiscoveryRecordsToFetch_Sites | String | Maximum sites to fetch during discovery       |
| CustomSPODomains                 | Array  | Custom SharePoint Online domains to recognize |

## Proxy Settings

| Setting              | Type    | Description                      |
|----------------------|---------|----------------------------------|
| ProxyServerPort      | String  | Proxy server port (0 = no proxy) |
| HasProxyServerConfig | Boolean | Indicates proxy is configured    |

## Debug & Logging Settings

| Setting                                     | Type    | Description                                                  |
|---------------------------------------------|---------|--------------------------------------------------------------|
| IsDebugModeEnabled                          | Boolean | Enables debug mode (verbose console output)                  |
| IsDebugMode                                 | Boolean | Legacy debug mode flag                                       |
| IsDebugModeEnhanced                         | Boolean | Extra-verbose debug logging                                  |
| IsDetailedLogging                           | Boolean | Detailed operation logging to files                          |
| DebugLogFilesDaysToKeepCount                | String  | Days to retain debug log files                               |
| DebugItemServiceStopNumberOfFieldsToLoadMax | String  | Max fields to load per item in debug mode                    |
| IsUsageLoggingEnabled                       | Boolean | Enables anonymous usage telemetry                            |
| DisableThreadingProblemsDetection           | Boolean | Disables threading issue detection (no longer used - ignore) |

## Pre-Flight Check Settings

| Setting                     | Type    | Description                                                                                                      |
|-----------------------------|---------|------------------------------------------------------------------------------------------------------------------|
| EnablePreFlightCheckService | Boolean | Validates job configuration before execution such as verifying user has access to sites in job before execution. |

## Link Validation Settings

| Setting                                | Type  | Description                                                        |
|----------------------------------------|-------|--------------------------------------------------------------------|
| LinkValidationSendAuthCookiesWhiteList | Array | Domains that receive auth cookies during link validation (* = all) |

## File & Folder Paths

| Setting            | Type   | Description                    |
|--------------------|--------|--------------------------------|
| FilePathSettings   | String | Location of this settings file |
| FilePathSiteAudits | String | Site audit data storage file   |

| Setting                                 | Type   | Description                                     |
|-----------------------------------------|--------|-------------------------------------------------|
| FilePathJobHistory                      | String | Job history index file                          |
| FilePathEmailSettings                   | String | Email notification configuration                |
| FilePathDebugLog                        | String | Debug log output file                           |
| FilePathLicense                         | String | License data file                               |
| FilePathSiteAuditTrends                 | String | Site trend data file                            |
| FilePathSharePointConnectionProfiles    | String | SharePoint connection profiles                  |
| FilePathSharePointAutoDiscoveryProfiles | String | Auto-discovery configurations                   |
| FilePathScheduledJobs                   | String | Scheduled jobs configuration                    |
| FolderPathConfig                        | String | Configuration files directory                   |
| FolderPathJobHistory                    | String | Job history data directory                      |
| FolderPathWebView2                      | String | WebView2 browser data directory                 |
| FolderPathLicense                       | String | License files directory                         |
| FolderPathGovernance                    | String | Governance data directory                       |
| FolderPathLogs                          | String | Application logs directory                      |
| FolderPathExports                       | String | Default export location                         |
| FolderPathReports                       | String | Default report location                         |
| FolderAccessTokenCache                  | String | OAuth token cache directory                     |
| FolderSessionCookieCache                | String | Session cookie cache directory                  |
| FolderPathJobTemplates                  | String | Job template files directory                    |
| FolderPathCustomViews                   | String | Custom grid view layouts directory              |
| FilePathMonitors                        | String | Monitors.json: stores monitor definitions.      |
| FolderPathMonitorRuns                   | String | Directory where monitor run results are stored. |

## Insights & ScoreCard Thresholds

| Setting                                                      | Type   | Description                                                         |
|--------------------------------------------------------------|--------|---------------------------------------------------------------------|
| ScoreCard_Threshold_SiteContentNotModifiedInLastDays         | String | Days since last modification used to flag stale site content.       |
| ScoreCard_Threshold_SiteContentNotModifiedInLastDays_Warning | String | Number of sites that triggers a warning.                            |
| ScoreCard_Threshold_SiteContentNotModifiedInLastDays_Error   | String | Number of sites that triggers an error.                             |
| ScoreCard_Threshold_SiteContentLowPageViewsCount             | String | Page view count below which site content is flagged as low traffic. |
| ScoreCard_Threshold_SiteContentLowPageViewsCount_Warning     | String | Number of sites that triggers a warning.                            |

| Setting                                                       | Type   | Description                                                      |
|---------------------------------------------------------------|--------|------------------------------------------------------------------|
| ScoreCard_Threshold_SiteContentLowPageViewsCount_Error        | String | Number of sites that triggers an error.                          |
| ScoreCard_Threshold_ListsContentNotModifiedInLastDays         | String | Days since last modification used to flag stale list content.    |
| ScoreCard_Threshold_ListsContentNotModifiedInLastDays_Warning | String | Number of lists that triggers a warning.                         |
| ScoreCard_Threshold_ListsContentNotModifiedInLastDays_Error   | String | Number of lists that triggers an error.                          |
| ScoreCard_Threshold_ListLargeItemsCount                       | String | Item count threshold for a “large list”.                         |
| ScoreCard_Threshold_ListLargeItemsCount_Warning               | String | Number of lists that triggers a warning.                         |
| ScoreCard_Threshold_ListLargeItemsCount_Error                 | String | Number of lists that triggers an error.                          |
| ScoreCard_Threshold_ListHasUniquePermissionsCount_Warning     | String | Number of items with unique permissions that triggers a warning. |
| ScoreCard_Threshold_ListHasUniquePermissionsCount_Error       | String | Number of items with unique permissions that triggers an error.  |
| ScoreCard_Threshold_SiteContentHighBrokenLinkCount            | String | Broken link count above which site content is flagged.           |
| ScoreCard_Threshold_SiteContentHighBrokenLinkCount_Warning    | String | Number of sites that triggers a warning.                         |
| ScoreCard_Threshold_SiteContentHighBrokenLinkCount_Error      | String | Number of sites that triggers an error.                          |
| ScoreCard_Threshold_SiteOpenToEveryoneCount_Warning           | String | Number of sites open to Everyone that triggers a warning.        |
| ScoreCard_Threshold_SiteOpenToEveryoneCount_Error             | String | Number of sites open to Everyone that triggers an error.         |
| ScoreCard_Threshold_ListOpenToEveryoneCount_Warning           | String | Number of lists open to Everyone that triggers a warning.        |
| ScoreCard_Threshold_ListOpenToEveryoneCount_Error             | String | Number of lists open to Everyone that triggers an error.         |
| ScoreCard_Threshold_ListLargeSizeMB                           | String | Size threshold, in MB, for a “large list”.                       |
| ScoreCard_Threshold_ListLargeSizeMB_Warning                   | String | Number of lists that triggers a warning.                         |
| ScoreCard_Threshold_ListLargeSizeMB_Error                     | String | Number of lists that triggers an error.                          |
| ScoreCard_Threshold_ListMajorVersionsCount                    | String | Major version count threshold.                                   |
| ScoreCard_Threshold_ListMajorVersionsCount_Warning            | String | Number of lists that triggers a warning.                         |

| Setting                                            | Type   | Description                                                                                                                                                                   |
|----------------------------------------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ScoreCard_Threshold_ListMajorVersionsCount_Error   | String | Number of lists that triggers an error.                                                                                                                                       |
| ScoreCard_Threshold_ListMinorVersionsCount         | String | Minor version count threshold.                                                                                                                                                |
| ScoreCard_Threshold_ListMinorVersionsCount_Warning | String | Number of lists that triggers a warning.                                                                                                                                      |
| ScoreCard_Threshold_ListMinorVersionsCount_Error   | String | Number of lists that triggers an error.                                                                                                                                       |
| EveryoneGroups                                     | Array  | Group names treated as “Everyone” for permission analysis (default: Everyone, Everyone except external users, All authenticated users, Domain Users, All Users, All Company). |
| EveryoneGroupsDefaultsVersion                      | String | Version of the built-in default Everyone group list. Tracks when the defaults were last updated.                                                                              |

## Export Settings

| Setting                  | Type    | Description                                         |
|--------------------------|---------|-----------------------------------------------------|
| ExportFileDateTimeFormat | Integer | Date format in export filenames (0=ISO, 1=US, etc.) |
| DefaultExportToExcelType | Integer | Default Excel format (0=XLSX, 1=XLS)                |
| JobDebounceTimeInSeconds | String  | Debounce time for rapid job triggers                |
| IsAutoCheckForUpdates    | Boolean | Automatically checks for application updates        |

## Enterprise Settings (Coming soon) – SPE Enterprise Manager parent application

| Setting                        | Type    | Description                                                 |
|--------------------------------|---------|-------------------------------------------------------------|
| IsManagedBySPEssentialsManager | Boolean | Indicates this instance is managed by SPE Manager           |
| TrendTrackingInterval          | Integer | Interval for tracking site trends (0=Daily, 1=Weekly, etc.) |

## Feature-Specific Settings

Each feature stores its own settings object in Settings.json. The FeatureItemsErrorPercentageThreshold value appears in every feature and sets the percentage of

item errors at which a job is treated as failed. Values shown as “String” are stored in quotation marks in the file.

## Analytics Feature Settings

| Setting                              | Type   | Description                                                                  |
|--------------------------------------|--------|------------------------------------------------------------------------------|
| TopSitesCount                        | String | Number of top sites shown in analytics (default 25).                         |
| LowSitesCount                        | String | Number of lowest-activity sites shown (default 5).                           |
| TopPagesCount                        | String | Number of top pages shown (default 25).                                      |
| LowPagesCount                        | String | Number of lowest-activity pages shown (default 5).                           |
| TopDocumentsCount                    | String | Number of top documents shown (default 25).                                  |
| LowDocumentsCount                    | String | Number of lowest-activity documents shown (default 5).                       |
| FeatureItemsErrorPercentageThreshold | String | Percentage of item errors at which the job is treated as failed (default 0). |

## Copy Feature Settings

| Setting                              | Type    | Description                                                                             |
|--------------------------------------|---------|-----------------------------------------------------------------------------------------|
| DefaultMaxFileSizeMB                 | String  | Maximum file size to copy, in MB (default 2000).                                        |
| ShowErrorForUsersNotFound            | Boolean | Shows an error when a user referenced by a copied item cannot be found (default false). |
| FeatureItemsErrorPercentageThreshold | String  | Percentage of item errors at which the job is treated as failed (default 0).            |

## Link Feature Settings

| Setting                                        | Type    | Description                                                                                                                           |
|------------------------------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------|
| IsHiddenWebPageLinksExcluded                   | Boolean | Excludes links in hidden web page content from results (default false).                                                               |
| LinkContentExclusions                          | Array   | URL path fragments excluded from link results, such as system images, catalogs, and service endpoints. Ships with 14 default entries. |
| ColumnRenameMappingCollection                  | Array   | Custom column name mappings for link reports (empty by default).                                                                      |
| IsExternalWebLinksForbiddenToTryWithWebRequest | Boolean | Skips checking external web links with a direct web request (default true).                                                           |
| ForceUseCookiesForLinkValidation               | Boolean | Always sends authentication cookies when validating links (default false).                                                            |
| SkipHtmlPageLinkValidation                     | Boolean | Skips link validation for HTML page links (default true).                                                                             |

| Setting                                                    | Type    | Description                                                                                      |
|------------------------------------------------------------|---------|--------------------------------------------------------------------------------------------------|
| LinkValidationTimeoutMilliseconds                          | String  | Timeout for each link check, in milliseconds (default 10000).                                    |
| IsLinkUrlDecodedForReport                                  | Boolean | Shows URL-decoded link addresses in reports (default true).                                      |
| IsForbiddenLinkTreatedAsValidLink                          | Boolean | Treats links that return a Forbidden response as valid instead of broken (default false).        |
| IsDisablePageLibraryMinorVersionsTemporarilyForFindReplace | Boolean | Temporarily turns off minor versions on page libraries while links are replaced (default false). |
| DefaultMaxFileSizeMB                                       | String  | Maximum file size scanned for links, in MB (default 20).                                         |
| MaxLinksPerItem                                            | String  | Maximum number of links reported per item (default 2000).                                        |
| MaxExcelCellLinksPerItem                                   | String  | Maximum number of links written to a single Excel cell (default 3000).                           |
| DefaultTimeout                                             | String  | Default timeout for link requests, in milliseconds (default 90000).                              |
| FeatureItemsErrorPercentageThreshold                       | String  | Percentage of item errors at which the job is treated as failed (default 5).                     |

## Permissions Feature Settings

| Setting                                  | Type    | Description                                                                                            |
|------------------------------------------|---------|--------------------------------------------------------------------------------------------------------|
| ColumnRenameMappingCollection            | Array   | Custom column name mappings for permission reports (empty by default).                                 |
| PermissionLevelDisplayType               | Integer | How permission levels are displayed in reports (default 0).                                            |
| AllowDuplicatePermissionLevelsWhenMerged | Boolean | Allows the same permission level to appear more than once when permissions are merged (default false). |
| ExclusionGroupsMembers                   | String  | Semicolon-separated list of groups whose members are not expanded in reports. Empty by default.        |
| ExclusionGroupMemberMaxThreshold         | String  | Groups with more members than this are not expanded (default 2000).                                    |
| PrivilegedPermissionLevelNames           | String  | Names of permission levels treated as privileged. Empty by default.                                    |
| FeatureItemsErrorPercentageThreshold     | String  | Percentage of item errors at which the job is treated as failed (default 5).                           |

## Discovery Feature Settings

| Setting                              | Type   | Description                                                                  |
|--------------------------------------|--------|------------------------------------------------------------------------------|
| FeatureItemsErrorPercentageThreshold | String | Percentage of item errors at which the job is treated as failed (default 0). |

## Search Feature Settings

| Setting                                                    | Type    | Description                                                                                    |
|------------------------------------------------------------|---------|------------------------------------------------------------------------------------------------|
| ColumnRenameMappingCollection                              | Array   | Custom column name mappings for search reports (empty by default).                             |
| DefaultMaxFileSizeMB                                       | String  | Maximum file size searched, in MB (default 500).                                               |
| MaxMatchesPerItem                                          | String  | Maximum number of matches reported per item (default 2000).                                    |
| MaxExcelCellMatchesPerItem                                 | String  | Maximum number of matches written to a single Excel cell (default 3000).                       |
| IsDisablePageLibraryMinorVersionsTemporarilyForFindReplace | Boolean | Temporarily turns off minor versions on page libraries while text is replaced (default false). |
| FeatureItemsErrorPercentageThreshold                       | String  | Percentage of item errors at which the job is treated as failed (default 5).                   |

## Site Audit Feature Settings

| Setting                              | Type    | Description                                                                  |
|--------------------------------------|---------|------------------------------------------------------------------------------|
| IncludeSharePointSystemLists         | Boolean | Includes SharePoint system lists in site audits (default false).             |
| FeatureItemsErrorPercentageThreshold | String  | Percentage of item errors at which the job is treated as failed (default 5). |

## Other Configuration Files

Along with Settings.json, the Config folder (%APPDATA%\Cognillo\SharePoint Essentials Toolkit\Config\) holds the files described below. The toolkit creates and updates these files itself. Edit them only when the toolkit is closed, and keep a backup before making changes.

### EmailSettings.json

EmailSettings.json stores the mail server settings the toolkit uses to send email, such as job alert emails. Passwords are stored encrypted.

| Setting                               | Type    | Description                                                                                               |
|---------------------------------------|---------|-----------------------------------------------------------------------------------------------------------|
| SendAsMailbox                         | String  | Mailbox address that email is sent from, for example a shared mailbox. Empty by default.                  |
| EmailAddress                          | String  | Email address of the account used to send email. Empty until email is configured.                         |
| Password                              | String  | Legacy password field. Leave empty; the SMTP password is stored in Smtplib.MailServer.Password.Encrypted. |
| Smtplib.SecurityProtocol              | Integer | Ignore, not required. Security protocol used for the SMTP connection (0 = default).                       |
| Smtplib.Server                        | String  | Ignore, not required. SMTP server host name (default smtp.office365.com).                                 |
| Smtplib.Port                          | String  | Ignore, not required. SMTP server port (default 587).                                                     |
| Smtplib.MailServer.Username           | String  | Ignore, not required. User name used to sign in to the SMTP server.                                       |
| Smtplib.MailServer.Password.Encrypted | String  | Ignore, not required. Encrypted password used to sign in to the SMTP server. Do not edit manually.        |
| MailServer.FromEmail                  | String  | Address that appears in the From field of outgoing email.                                                 |
| MailServer.FromDisplayName            | String  | Display name that appears in the From field (default "SharePoint Essentials Service").                    |
| IsSendEmailConfigured                 | Boolean | Indicates that email sending has been set up. Set by the toolkit when email settings are saved.           |

### ConnectionProfiles.json

ConnectionProfiles.json stores the connection profiles the toolkit uses to sign in to each SharePoint environment. Each entry in the ConnectionProfiles array is one profile. Passwords and certificate passwords are stored encrypted. Some settings, such as Username, TenantId, CertificatePath, and CertificatePassword\_Encrypted, are written only when they are used.

| Setting     | Type   | Description                  |
|-------------|--------|------------------------------|
| ProfileName | String | Display name of the profile. |

| Setting                                          | Type    | Description                                                                                                                                                         |
|--------------------------------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Id                                               | String  | Unique identifier (GUID) of the profile. Leave blank, it is auto populated.                                                                                         |
| SiteUrlMatchString                               | String  | URL prefix used to match sites to this profile, for example https://contoso.sharepoint.com/.                                                                        |
| TenantDomain                                     | String  | SharePoint tenant URL the profile connects to.                                                                                                                      |
| TenantId                                         | String  | Microsoft Entra tenant ID (GUID). Used with Azure App Registration and certificate authentication.                                                                  |
| IsEnabled                                        | Boolean | Turns the profile on or off.                                                                                                                                        |
| IsDefault                                        | Boolean | Marks the profile as the default profile.                                                                                                                           |
| CredentialType                                   | Integer | Authentication method used by the profile. Values seen in profile files: 1 = Web Browser Authentication, 2 = Certificate.                                           |
| Username                                         | String  | User name for the profile. Written only when a user name is stored.                                                                                                 |
| Password_Encrypted                               | String  | Encrypted password. Do not edit manually.                                                                                                                           |
| IsUsingAzureAppRegistration                      | Boolean | Signs in through your own Azure App Registration instead of the default sign-in.                                                                                    |
| IsAzureMultiTenantAppRegEnabled                  | Boolean | Signs in through a multi-tenant Azure app registration.                                                                                                             |
| IsEntraSingleSignOnEnabled                       | Boolean | Enables Microsoft Entra single sign-on for the profile.                                                                                                             |
| EntraEnterpriseAppId                             | String  | Application (client) ID of the Microsoft Entra app used for sign-in.                                                                                                |
| IsWebView2AllowSingleSignOnUsingOSPrimaryAccount | Boolean | Lets the embedded browser sign in automatically with the primary Windows account.                                                                                   |
| IsAutoDetectLoginPage                            | Boolean | Detects the sign-in page automatically during Web Browser Authentication.                                                                                           |
| CertificatePath                                  | String  | Full path to the certificate (.pfx) used for certificate authentication.                                                                                            |
| CertificatePassword_Encrypted                    | String  | Encrypted password of the certificate. Do not edit manually.                                                                                                        |
| AzureEnvironment                                 | Integer | Azure cloud environment of the tenant (0 = default).                                                                                                                |
| AzureHostingEnvironment                          | Object  | Sign-in endpoints for the Azure environment: EnvironmentType, Uri (default https://login.microsoftonline.com/), and GraphUri (default https://graph.microsoft.com). |
| mode                                             | Integer | Internal connection mode (0 = default).                                                                                                                             |
| CookieCollection                                 | Array   | Saved session cookies. Maintained automatically.                                                                                                                    |

## AutoDiscoveryProfiles.json

AutoDiscoveryProfiles.json stores profiles used to discover SharePoint sites automatically.

## Checking for Program Updates

The application can be updated using the following methods:

- Click “Check for Updates” from the application left navigation menu.
- Configured in Settings -> Automatically prompt user if an update is available. The tool will automatically check for updates and prompt you if you want to install them. This requires an internet connection.

The computer needs access to this path to get updates:

<https://apps.cognillo.com/appupdates/essentials/get-updates-spe.txt>

## Disable Checking for Program Updates

You can do this in several ways, listed below. There is no single command-line switch to disable the updater, but option 1 can be automated with a script that sets `IsAutoCheckForUpdates` to false in `Settings.json`.

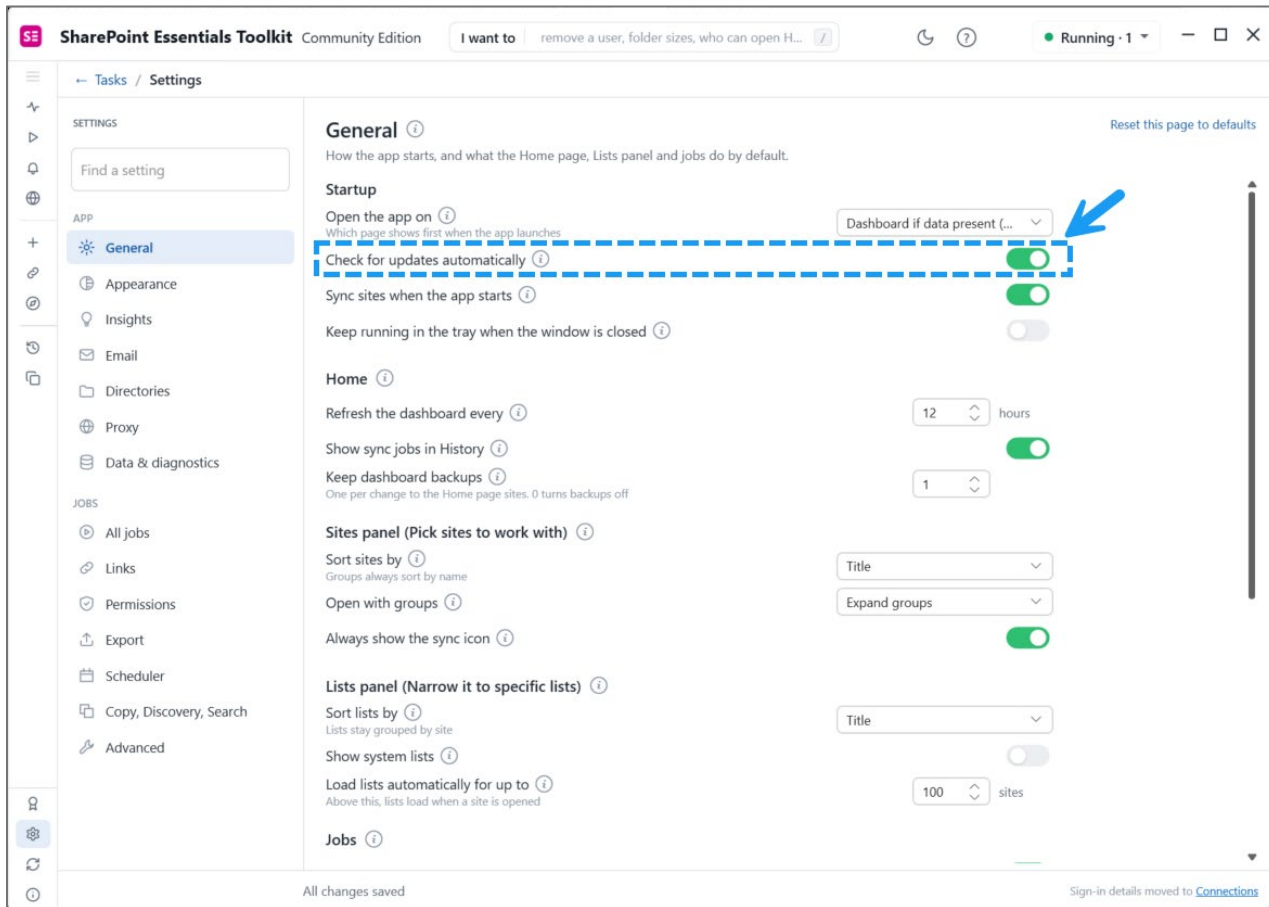
To disable Auto-Update check you have a few different options:

1. Pre-configure the `Settings.json` file. See this [section](#) for pushing settings to multiple machines.



```
{
  "SPEInstanceId": " ",
  "IsExportGroupHeadersBold": false,
  "IsAutomaticallySettingJobPerformance": true,
  "ExportListItemsBatchSize": "150",
  "ExportBatchThreadLimit": "20",
  "ExportFileDateTimeFormat": 0,
  "IsAutoCheckForUpdates": true,
  "EnableScheduledJobs": true,
  "EnableGovernanceDataCollectionService": true,
  "EnableGovernanceDataCollectionServiceHighPerformance": false,
  "IsMinimizeOnClose": false,
  "IsAutoSaveWebBrowserAuthCredentials": true,
  "WebView2UserAgent": "ISV|Cognillo|SharePointEssentialsToolkit/2025",
  "UseCustomWebView2UserAgent": false,
  "IsWebView2DPIAwareOverride": false,
  "EnableJobHistoryRealTimeDatabaseStorage": true,
  "AutoDeactivateLicenseOnClose": true,
  "IntervalToSaveReportsToExcelMinutes": "15",
  "IsUsageLoggingEnabled": false,
  "IsManagedBySPEssentialsManager": false,
  "MaxItemProcessingTimeoutSeconds": "900",
  "DefaultExportToExcelType": 1,
  "EnablePreFlightCheckService": true,
  "IsWebView2UseCustomFolderForEachProfile": true,
  "MaxDiscoveryRecordsToFetch_Sites": "10000",
  "LiveExplorerSortOrder": 1,
  "HomePageDeletionBehavior": 0,
  "MaxSitesToRenderListsInLiveExplorer": "100",
  "MaxSitesToRenderListsInJobOptions": "10",
  "ExpandHomePageDirectoryOnStartup": 0,
  "CustomSPODomains": [],
  "MaxRecordsToDisplayPerGridReport": "500000",
  "IsAutoCheckForUpdates": true
}
```

- Go to the Settings in the application and disable 'Automatically Check for Updates'.



- To block users from updating the software, it is necessary to block traffic to <https://apps.cognillo.com>.

The full path used to download the update is below:

<https://apps.cognillo.com/appupdates/essentials/SPEssentialsToolkitSetup.zip>

Users who subscribe to our automated email notifications for the update will also have this link:

<https://apps.cognillo.com/appupdates/essentials/SharePointEssentialsToolkitSetupMSI.zip>

Blocking (by DNS entry (redirect to invalid location) or firewall) ensures the user will not be able to update using links within the tool or manually from our website or email notifications.

**NOTE:** A tech savvy user could still manually modify the URL to use www instead of apps to bypass this. This also blocks our PDF user guides, which may reflect newer versions of the product, you would need to retain a copy of the PDF guides for your controlled release. Online material is not blocked.



## Where are Credentials stored?

### Web Browser Authentication

Credentials can be stored in the same way Microsoft Edge stores credentials.

The location of the Web Browser (WebView2 control) data is in the current user local app data folder:

C:\Users\<username>\AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\**WebView2**\

The location for access token cache ([encrypted](#)) when saving credentials, can be found here:

C:\Users\<username>\AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\**Token Cache**\

- To turn off saving of credentials, go to Settings > Jobs > Advanced > Embedded web browser and turn off 'Allow saving browser authentication credentials'.
- To clear stored credentials, go to My Connections within the tool, and click Sign in as a different user/Clear Cache.

---

*NOTE: Disabling the option to "Allow saving browser authentication credentials" will persist session data in WebView2 in order to prevent multiple prompts for users to authenticate. Session data will be cleared once the SharePoint Essentials Toolkit is closed and/or opened.*

---

To see how these credentials are stored, see the [Encryption](#) section.

To see how data such as web page data is stored and privacy options, see this [article](#) from Microsoft about WebView2.

### Username and Password

C:\Users\<username>\AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\Config\ConnectionProfiles.json

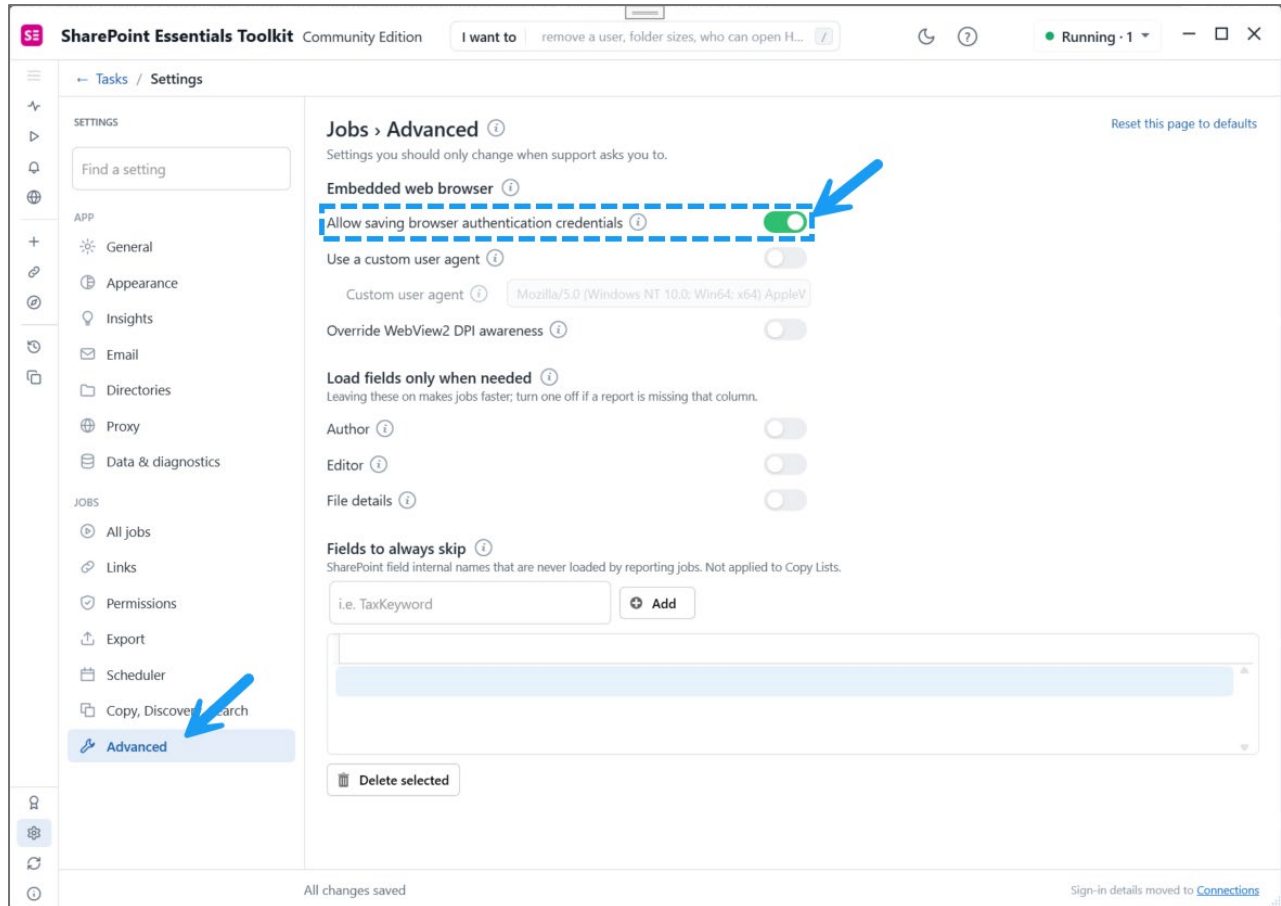
### Certificate Authentication

The certificate password is stored in

C:\Users\<username>\AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\Config\ConnectionProfiles.json

## Saving Credentials with Web Browser Authentication

To minimize authentication prompts, the SharePoint Essentials Toolkit has the option to save web browser access tokens. This option is enabled by default. To change this option, go to Settings > Jobs > Advanced > Embedded web browser > Allow saving browser authentication credentials.



## How are Access Tokens Saved?

Access tokens are saved to disk only when the option 'Allow saving browser authentication credentials' is enabled.

The storing and encryption logic is handled through MSAL ([Microsoft Authentication Library](#)) which is part of the Microsoft Identity platform. MSAL acquires, manages, caches, and refreshes tokens; it uses best practices for resilience. MSAL is used to encrypt access tokens using **Windows DPAPI**. Access tokens are encrypted on disk in this location:

C:\Users\<username>\AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\Token Cache\

NOTE: The MSAL cache is **production-ready, secure, and Microsoft-supported** - it's what Microsoft Teams, Office, Visual Studio, and other Microsoft apps use internally!

## Encryption - How is sensitive data stored?

### What data is encrypted by the SharePoint Essentials Toolkit?

- **Passwords** that are stored if using ‘**Username and Password**’ option in “My Connections” *Authentication Type*.
- **Access Tokens** are encrypted and stored to disk if ‘Allow saving browser authentication credentials’ is enabled in Settings page.
- **Governance and User Activity Data**
- For the physical location of above data, see [here](#)

### How is the data encrypted?

Data to be encrypted: is first encoded, then a passphrase is added programmatically, a salt value is then added for extra security, then this value is encrypted using AES (also known as Rijndael) encryption.

- AES-256-CBC with PKCS7 padding
- 128-bit IV size
- A 100K iteration count is used for encryption hardening (NIST recommended).
- Modern PBKDF2 – uses modern Rfc2898DeriveBytes with SHA-256 (not deprecated PasswordDeriveBytes).
- Random IV generation per encryption.
- Salt: Private composite string.
- Disposes sensitive information from memory when not needed.

Further, each installation of the SharePoint Essentials Toolkit (even if on the same machine) is configured with a unique GUID identifier. This unique GUID is hidden from the user interface. The GUID is added as an additional salt value to the encryption. Encrypted passwords also have local machine and user info added to the salt key. This has been done so that if another user gets access to the encrypted data file, they will not be able to view the data.

### What else is encrypted?

- **Communication** between the *SharePoint Essentials Toolkit* and *SharePoint Online* is encrypted using TLS 1.2 or higher (TLS 1.3 where both Windows and Microsoft 365 support it), see [here](#) for more information. For SharePoint on-premises, the SharePoint Essentials Toolkit will use the encryption required by the SharePoint on-premises environment.

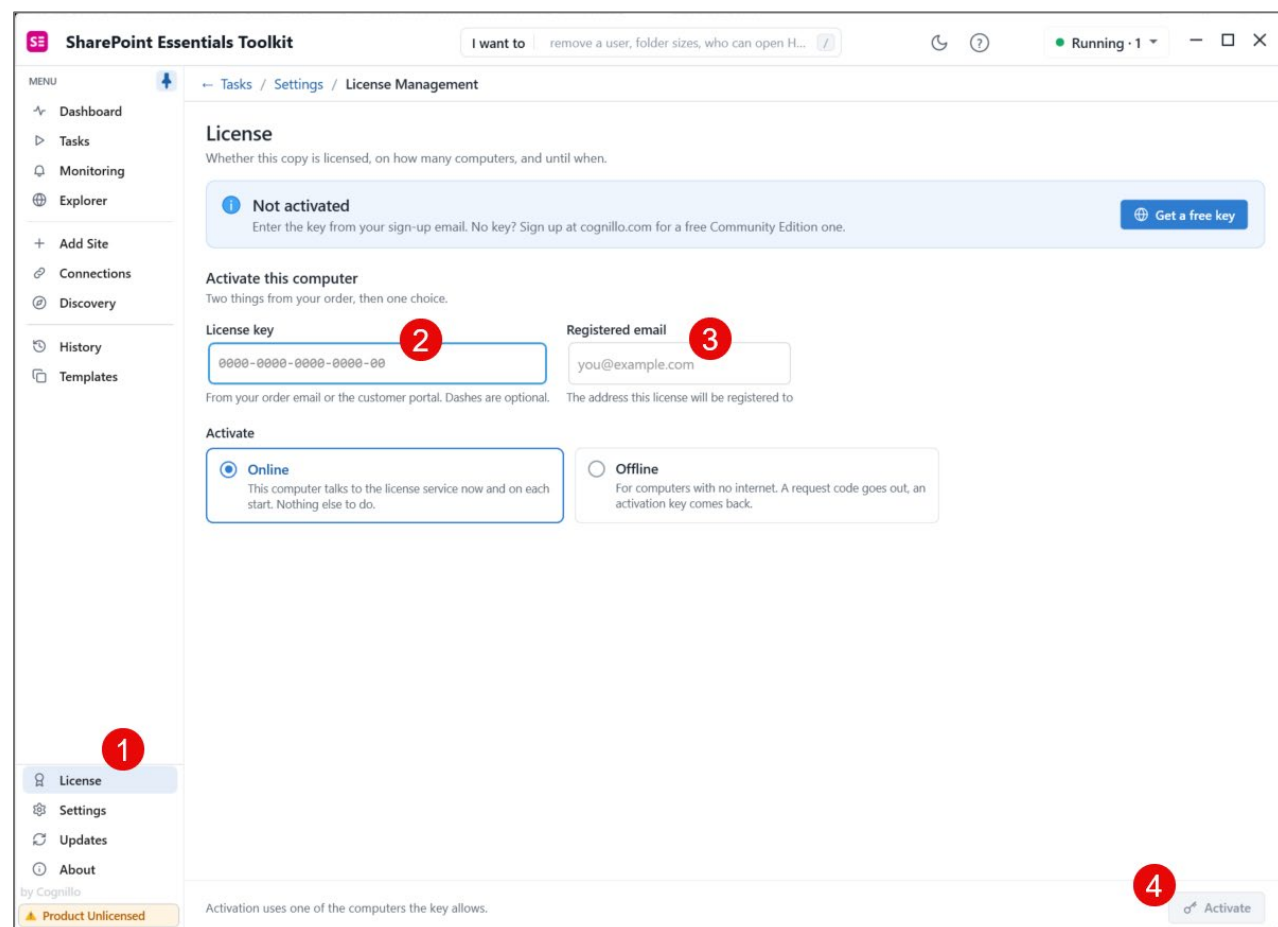
## License Activation

We offer 2 options for license activation, ONLINE and OFFLINE.

Below is a table that describes the 2 models:

| Model                                                   | Online                                                                                | Offline                                                                                                                                    |
|---------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Requires Internet Connection                            | Yes                                                                                   | No (only to SharePoint)                                                                                                                    |
| Requires contacting Cognillo for Offline Activation Key |                                                                                       |                                                                                                                                            |
| Features supported                                      | All                                                                                   | All                                                                                                                                        |
| App Updates                                             | Must have access to <a href="https://apps.cognillo.com">https://apps.cognillo.com</a> | Requires updates to be downloaded and installed manually (if <a href="https://apps.cognillo.com">https://apps.cognillo.com</a> is blocked) |

## Online Activation



The screenshot shows the 'SharePoint Essentials Toolkit' interface. The left sidebar (callout 1) contains a menu with 'License' selected. The main content area is titled 'License Management' and shows the 'License' section. A 'Not activated' message (callout 2) is displayed with a 'Get a free key' button. Below this, the 'Activate this computer' section has two input fields: 'License key' (callout 2) and 'Registered email' (callout 3). The 'Online' activation option is selected. At the bottom right, there is an 'Activate' button (callout 4).

Cognillo has partnered with **Nalpeiron** (<https://nalpeiron.com>) for license management. This helps us ensure the license activation servers are available with **99.9% uptime**.

Please note that only the license key and email address provided for activation are sent to Nalpeiron license servers. The email address can be of any value for activation, it is only used in the event you would like to deactivate a license and need to identify the machine it was installed on.

To begin ONLINE activation, see the steps below:

1. In SharePoint Essentials Toolkit, click License in the left navigation.
2. For Email, enter your email address. This email address will be associated with your license in our records.
  - The Email does not have to be your actual email, but it must be unique for each activation. Using your actual email is convenient if we need to look up your license (i.e. for support or if you need to have us deactivate a license for you).
3. License Activation Key:
  - NOTE: The email address used for the initial download should have received an email from Cognillo with the License Activation Key.
4. For License Activation Type, choose **Online**.
5. Click Activate. A confirmation popup should appear.
6. Verify the license information on the right side of the License page is correct. If anything is not correct, please contact Cognillo for support.

## License Server Address - White List

If online activation fails, ensure the required license servers are not blocked by a firewall and add below to the firewall allow list:

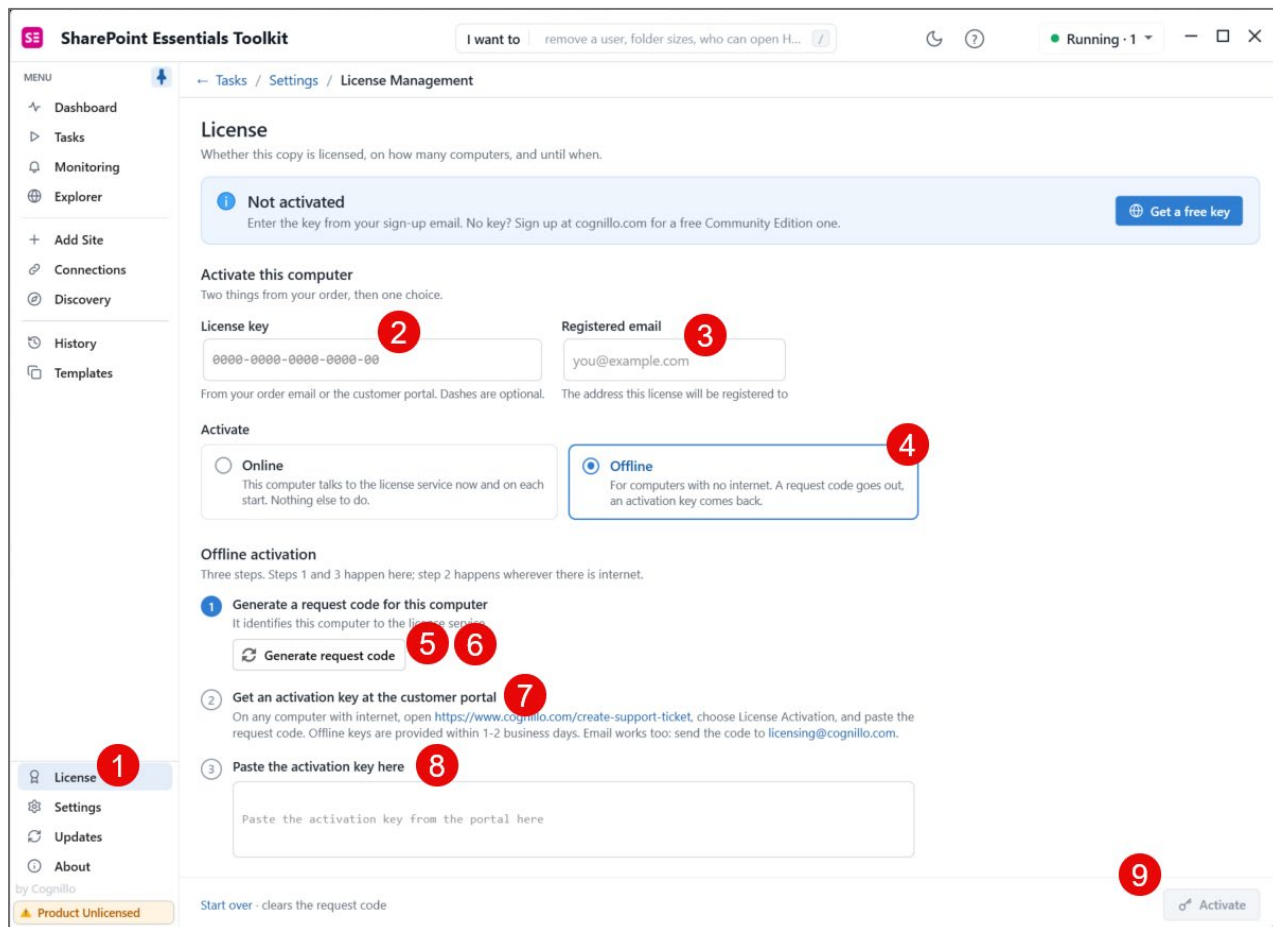
Ensure Cognillo license servers are whitelisted at this endpoint:

- DNS - licensing.cognillo.com
- Port – 443

Ensure Nalpeiron is whitelisted:

- DNS - my.nalpeiron.com
- IPv4 - 20.237.110.18
- IPv6 - 2603:1030:20c:9::2c2
- Ports - 80 and 443

## Offline Activation



The screenshot shows the 'SharePoint Essentials Toolkit' interface. The left navigation menu has 'License' highlighted (1). The main content area is titled 'License' and shows 'Not activated' status. It prompts the user to 'Activate this computer' by entering a 'License key' (2) and a 'Registered email' (3). Under the 'Activate' section, the 'Offline' option is selected (4). The 'Offline activation' section lists three steps: 1. 'Generate a request code for this computer' (5), which involves clicking the 'Generate request code' button (6). 2. 'Get an activation key at the customer portal' (7). 3. 'Paste the activation key here' (8), which involves pasting the key into the provided text box. A 'Start over' link is available below the text box. At the bottom right, there is an 'Activate' button (9).

1. In SharePoint Essentials Toolkit, click License in the left navigation.
2. Enter the product License Activation Key  
NOTE: The email address used for the initial download should have received an email from Cognillo with the License Activation Key.
3. For Email, enter your email address. This email address will be associated with your license in our records.
  - This value does not need to match our records for license activation to work. It is strictly used as a convenient way to look up your license (i.e. if you need to have us manually deactivate a license for you).
4. For License Activation Type, choose Offline.
5. Click **Generate request code**
6. A long random value should now appear in the request code text box. Copy the value in the text box using the **Copy** button.

**Offline activation**

Three steps. Steps 1 and 3 happen here; step 2 happens wherever there is internet.

✓ **Generate a request code for this computer**

It identifies this computer to the license service. Generated today at 16:50

[Regenerate](#) · [Save as file](#)

```
f725a1c24d91d70b9a939228ca78ba0cfdd5bbe7de7beca09be53108054b5272633179ef823a163efe680e32ddd  
db52bfcdcc09bb28e7f4ff128685dd045a43b4262c327b897fd86a392e71a84b9d50b0afdd7720fae36db2dade82
```

 Copy

- Click [Report a bug / Request feature / Get help](#) or email Cognillo at [support@cognillo.com](mailto:support@cognillo.com) or [licensing@cognillo.com](mailto:licensing@cognillo.com). In the support ticket or email, paste the request code we just copied. Cognillo support will respond with the corresponding Offline License Activation Key. At this point, your license has been activated with Cognillo, but not on your device.
- Copy and paste the key provided by Cognillo into the Activation Key field.
- Click Activate. A confirmation popup should appear.
- Verify the license information on the right side of the License page is correct. If anything is not correct, please contact Cognillo for support.

## Azure App Registration

**IMPORTANT:** These steps require a user to grant tenant-wide admin consent to SharePoint Essentials Toolkit. Elevated privileges in Azure are required to perform this step. Please refer to Microsoft's documentation for more details:

[Grant tenant-wide admin consent to an application - Microsoft Entra ID | Microsoft Learn](#)

## SharePoint Essentials Toolkit App Registration in Azure Portal

### Azure App Registration Overview

You can perform app registration using one of three ways:

1. **(Recommended and easiest) Fully Automated**  
Use the in-app 'Set up Azure app registration' wizard, which consents the shared app and can also create your own User Activity app registration and certificate
2. **Partially Automated (Multi-tenant Registration)**  
Use a shared multi-tenant app-registration from Cognillo
  - a. Use a simple [URL](#) to configure
3. **Manual App Registration (Single Tenant Registration)**  
Create an app registration unique for your tenant.
  - a. Use the Azure Portal (web browser)
  - b. Use the PowerShell script Setup-SPEAzure-OwnApp.ps1 (included in the Optional folder of the app download, or <https://apps.cognillo.com/appupdates/essentials/AzureAppRegistrationModernAuth.zip>)

For more information regarding single tenant vs multitenant app registration, see [here](#).

NOTE: The SharePoint Essentials Toolkit does not collect/store or process data in our tenant. Data is stored and processed locally on the user's machine.

### Azure Access Types Supported

The SharePoint Essentials Toolkit can authenticate users through their web browser (**Delegated authentication**) (default setup), or by using *Certificate based authentication* (**App-only authentication**).

**Delegated Authentication:** This will only give the current signed in user access to 'what they already have access to' in SharePoint. For example, the user will not be able to access SharePoint sites or content that they do not already have access to in SharePoint.

**Certificate-based Authentication:** This has the benefit of password-less authentication and may work better in some environments for scheduled jobs. However, it will provide ALL users who have access to the certificate and password, with the same SharePoint permissions (which are assigned to the certificate during App Registration).

For more information on delegated vs app-only access, see [here](#).

**NOTE:** The **Governance and User Activity features** in the tool *require a Certificate* to be configured in the My Connections section of the tool. This can be in addition to Delegated permissions so that users will by default only have access to what they do in SharePoint. See this [section](#) for more information.

## How does authentication work with Web Browser Authentication and Azure app registration?

The SharePoint Essentials Toolkit with Web Browser Authentication + Azure App Registration uses MSAL – Microsoft Authentication Library.

- **MSAL and Ephemeral Ports:**

The Microsoft Authentication Library (MSAL) for desktop applications leverages this behavior. When authenticating, MSAL initiates the process, opens the system browser for user interaction, and specifies localhost with a dynamically assigned port as the redirect URI. Azure AD then redirects the authentication token back to this localhost address and port, which the MSAL-enabled WPF application is listening on.

- **Loopback IP Redirect URIs (RFC 8252):**

The OAuth 2.0 for Native Apps specification (RFC 8252) explicitly allows for the use of loopback IP addresses (like localhost) with any port for redirection. This enables desktop applications to obtain an available ephemeral port from the operating system, open a socket on that port, and listen for the authentication response from Azure AD.

## Register the application

### (Very Easy) Fully Automated using app wizard

The in-app wizard performs the two one-time Azure steps that SharePoint Essentials Toolkit needs for a Microsoft 365 tenant, without opening the Azure portal:

- **Allow sign-in for your organization.** Grants tenant-wide consent to Cognillo's shared app, so everyone can sign in with their Microsoft account and never sees a "Need admin approval" prompt.
- **User Activity app registration.** Creates a certificate-based app in your tenant with Office 365 Management APIs › ActivityFeed.Read, uploads the certificate, grants admin consent, and saves a ready-to-use connection. This is what the User Activity reports and Monitoring read from.

Both connection profiles are written for you. Nothing has to be copied by hand.

**You need:** a Global Administrator account for the tenant. The wizard does not need a license, so the admin can run it on an non-activated install without taking up a user license.

**Time:** about five minutes.

---

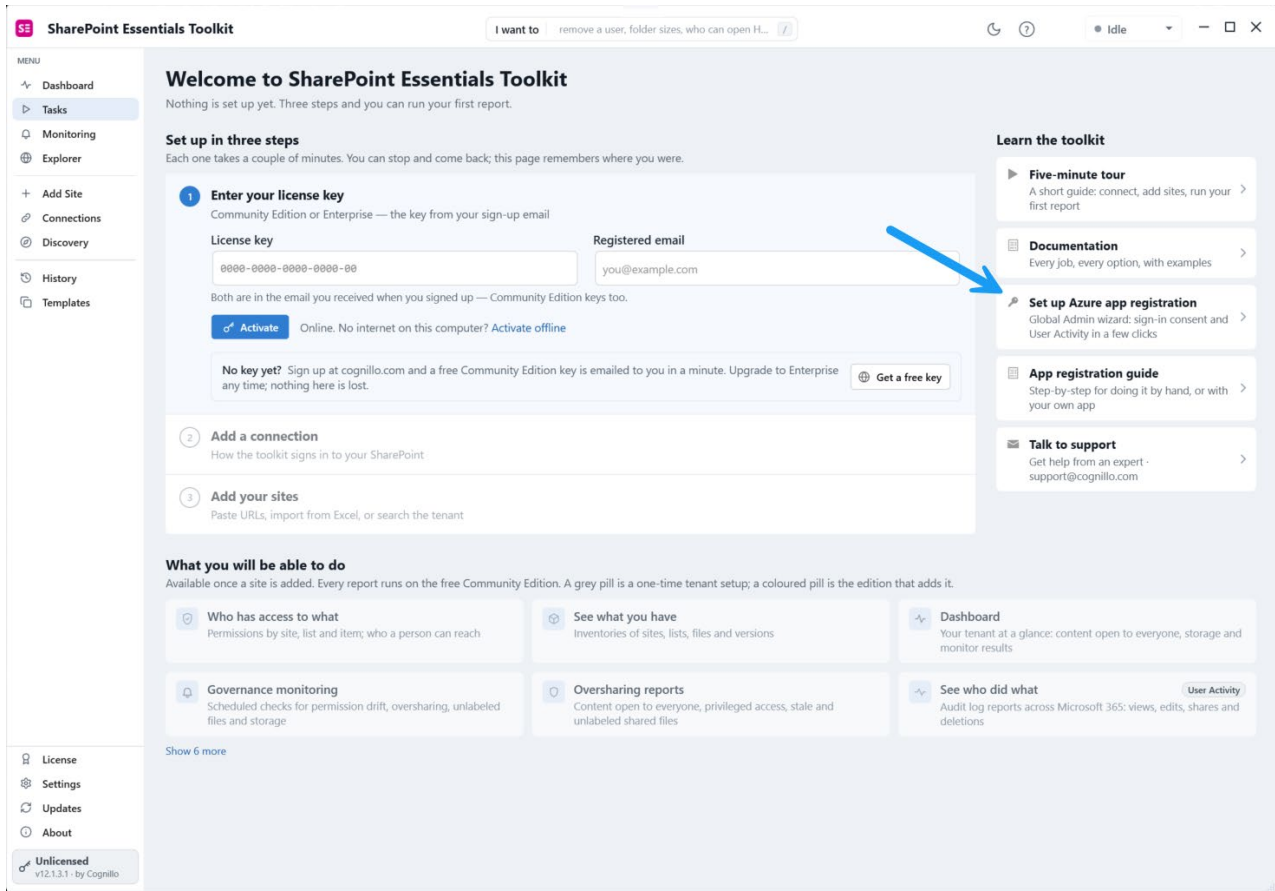
*NOTE: Not a Global Admin? Start the wizard anyway and choose **I'm not a Global Admin**. It gives you an email to send them. See "If you are not the Global Administrator" below.*

---

#### Step 1: Open the wizard

Any of the following opens it:

- **Home** › the **Set up Azure app registration** card under **Learn the toolkit**.
- **Connections** › the **Set up Azure app registration** link in **New connection** panel.



**SharePoint Essentials Toolkit**

I want to remove a user, folder sizes, who can open H...

**Welcome to SharePoint Essentials Toolkit**

Nothing is set up yet. Three steps and you can run your first report.

**Set up in three steps**

Each one takes a couple of minutes. You can stop and come back; this page remembers where you were.

**1 Enter your license key**

Community Edition or Enterprise — the key from your sign-up email

License key

Registered email

Both are in the email you received when you signed up — Community Edition keys too.

[Activate](#) Online. No internet on this computer? [Activate offline](#)

No key yet? Sign up at cognillo.com and a free Community Edition key is emailed to you in a minute. Upgrade to Enterprise any time; nothing here is lost. [Get a free key](#)

**2 Add a connection**

How the toolkit signs in to your SharePoint

**3 Add your sites**

Paste URLs, import from Excel, or search the tenant

**Learn the toolkit**

- Five-minute tour**  
A short guide: connect, add sites, run your first report
- Documentation**  
Every job, every option, with examples
- Set up Azure app registration**  
Global Admin wizard: sign-in consent and User Activity in a few clicks
- App registration guide**  
Step-by-step for doing it by hand, or with your own app
- Talk to support**  
Get help from an expert - support@cognillo.com

**What you will be able to do**

Available once a site is added. Every report runs on the free Community Edition. A grey pill is a one-time tenant setup; a coloured pill is the edition that adds it.

- Who has access to what**  
Permissions by site, list and item; who a person can reach
- See what you have**  
Inventories of sites, lists, files and versions
- Dashboard**  
Your tenant at a glance: content open to everyone, storage and monitor results
- Governance monitoring**  
Scheduled checks for permission drift, oversharing, unlabeled files and storage
- Oversharing reports**  
Content open to everyone, privileged access, stale and unlabeled shared files
- See who did what**  
Audit log reports across Microsoft 365: views, edits, shares and deletions

[Show 6 more](#)

**License**

**Settings**

**Updates**

**About**

**Unlicensed**  
v12.1.3.1 · by Cognillo

## Step 2: Confirm you are the Global Administrator

The first screen explains what the wizard will do. Click **I'm a Global Admin**.

 **Set up Azure app registration**

1 Allow sign-in — 2 User Activity — 3 Done

One-time setup for your Microsoft 365 tenant. Global Administrator required.

### What this does

This takes about five minutes and does two things in your Microsoft 365 tenant:

1. **Allow sign-in for everyone.** One click of Accept on Microsoft's consent page for Cognillo's shared app. After that, anyone in your organization can connect with their own account.
2. **Create the User Activity app registration (optional).** A small app of its own with a certificate, so the toolkit can collect who viewed and edited what. This is what Monitoring and the dashboard's activity figures run on.

Both steps need a Global Administrator of the tenant. Nothing is changed in SharePoint itself, and nothing here needs Azure PowerShell.

#### Cloud

Azure Public Cloud ▾

Leave on PublicCloud unless your tenant is in a sovereign cloud.

#### Tenant (optional)

contoso.onmicrosoft.com

Tenant id or \*.onmicrosoft.com domain. Only needed when the admin account belongs to more than one tenant.

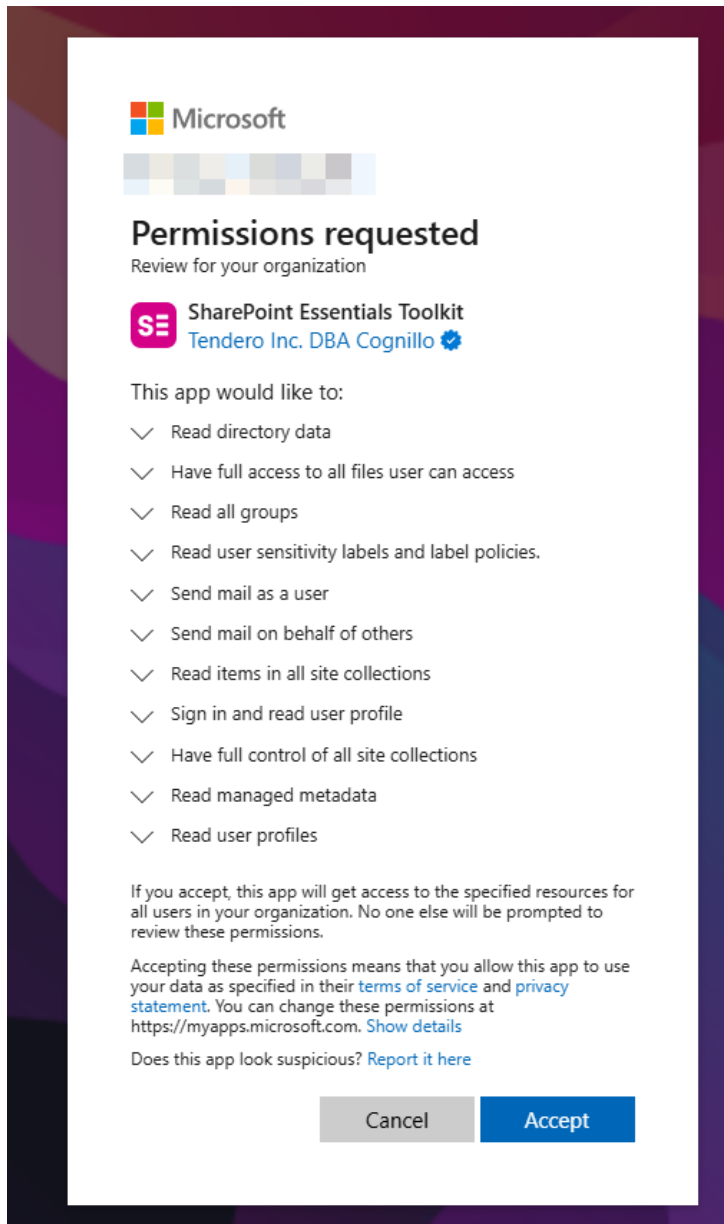
[I already have an app registration and certificate — open Connections](#)

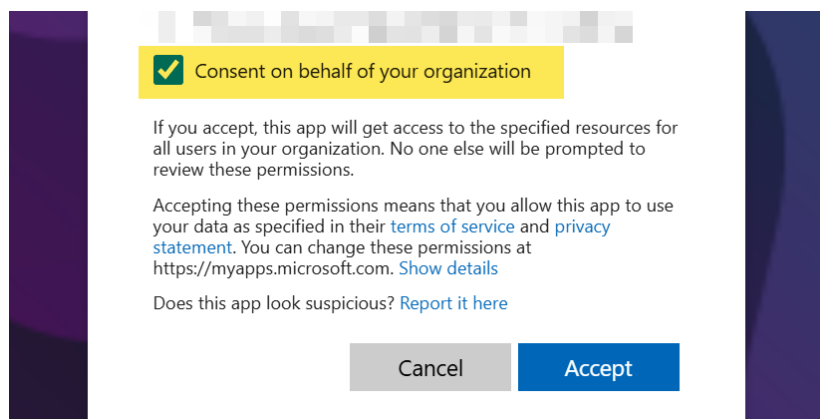
I'm not a Global AdminI'm a Global Admin — continue

### Step 3: Allow sign-in for your organization

1. Click **Open the consent page**. Your browser opens the Microsoft consent page for Cognillo's shared app.
2. Sign in as the Global Administrator.

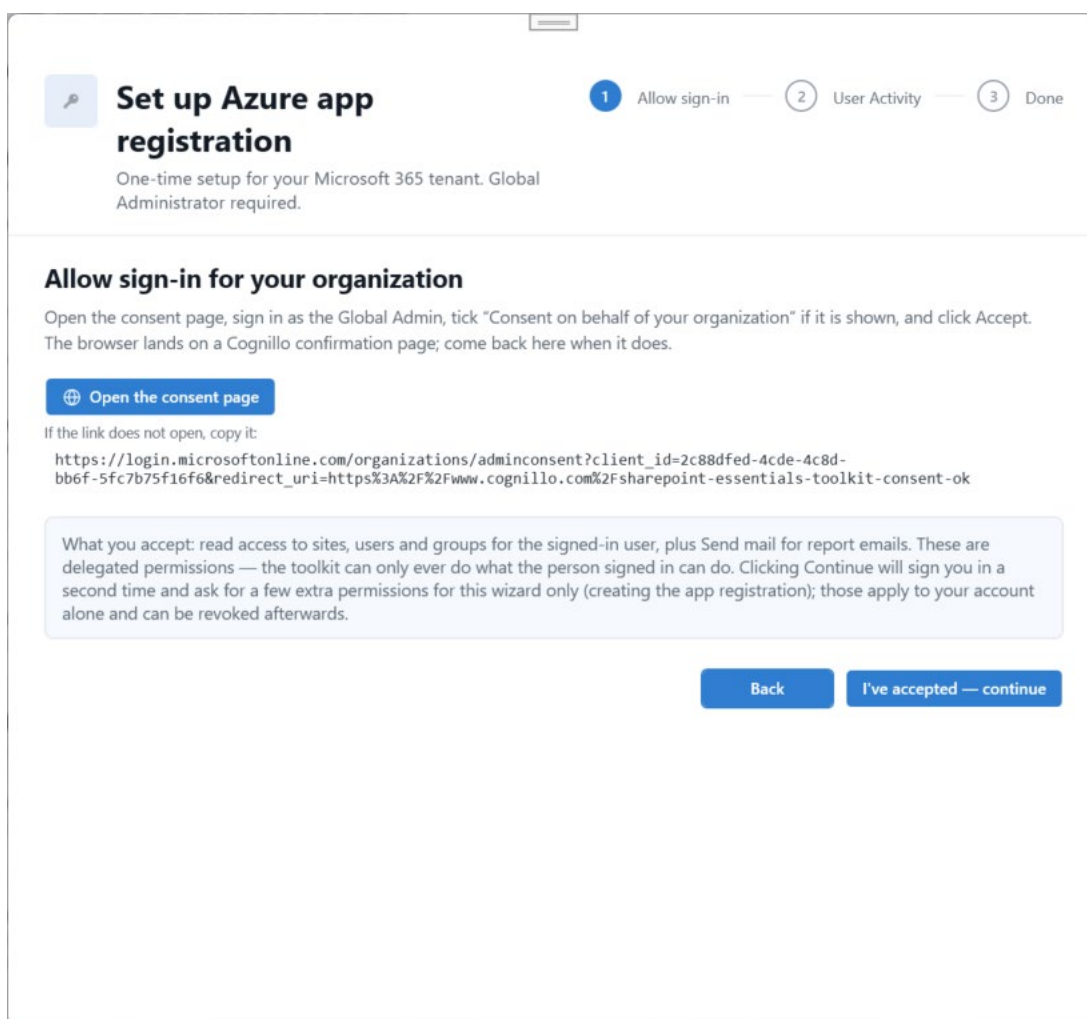
If a **Consent on behalf of your organization** checkbox is shown, tick it.





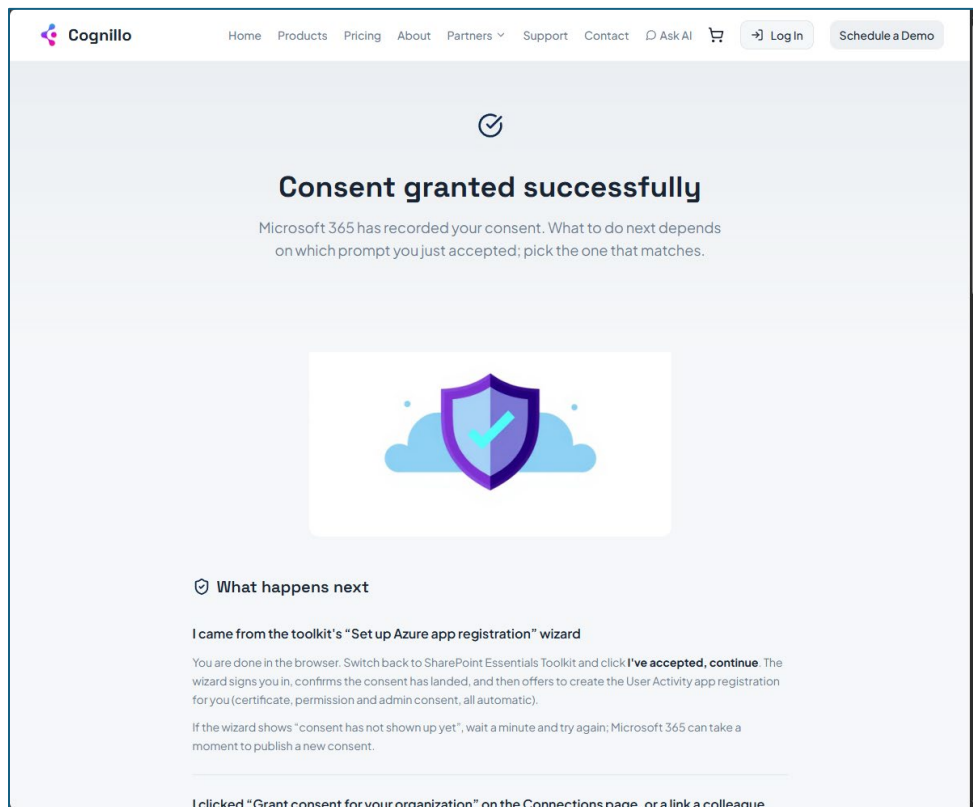
[Screenshot: Microsoft consent page with the “**Consent on behalf of your organization**” checkbox]

3. Click **Accept**. The browser lands on a Cognillo confirmation page.
4. Switch back to the toolkit and click **I’ve accepted, continue**.



If the browser does not open, hover the link under the button and use the copy icon, then paste it into a browser.

**What you are consenting to:** Delegated permissions only – read access to SharePoint sites, users and groups as the signed-in user, plus Send mail for emailing reports. The toolkit can never do more than the person signed in can do.



#### *Step 4: Sign in for the wizard*

A second browser sign-in opens. This one is for the wizard itself and asks for a few extra Microsoft Graph permissions (to create an app registration and grant consent). These apply to your account only; do not tick “consent on behalf of your organization” here. If you do, the wizard removes them from the tenant-wide grant when it closes.

 **One more sign-in, for the wizard itself**

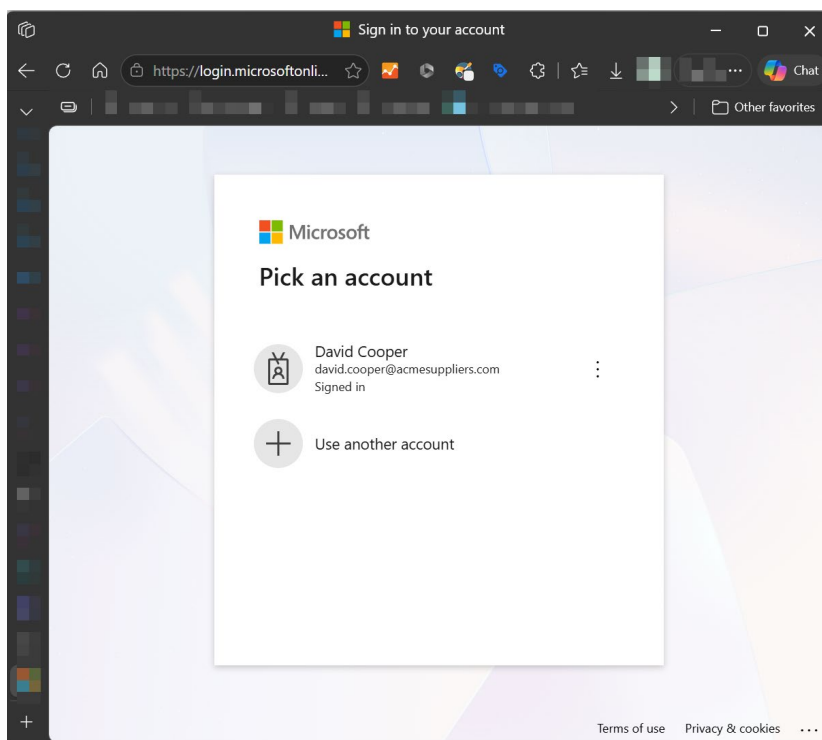
The sign-in you just completed granted consent for your organization. This one lets the wizard act as you in Microsoft Entra, which is **required to create the User Activity app registration** (the app, its certificate, its permission and admin consent). It also confirms the consent was recorded and fills in your SharePoint root site.

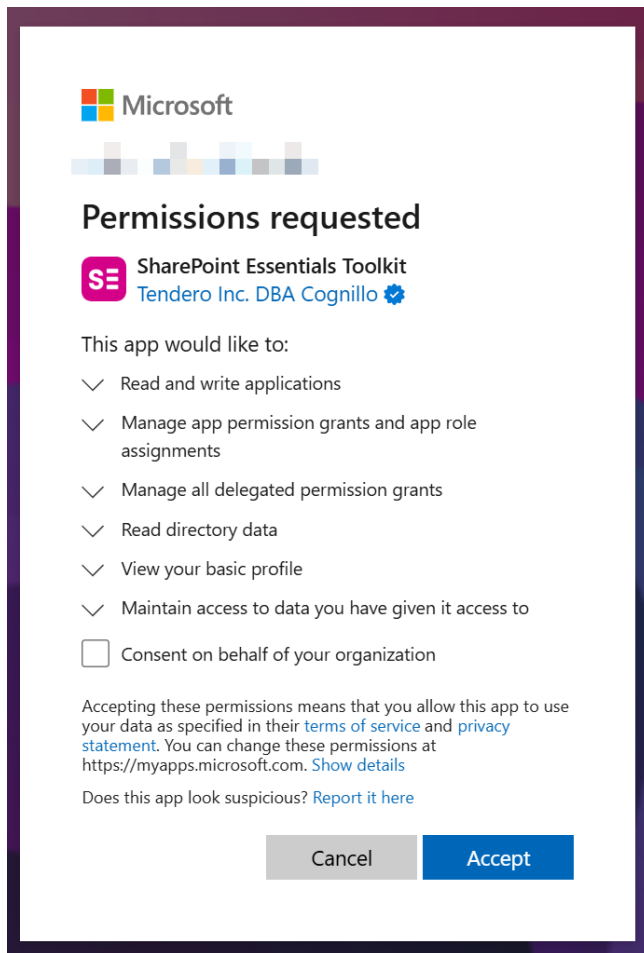
[Skip the sign-in — set up sites & content only, without User Activity](#)

[Show details](#)

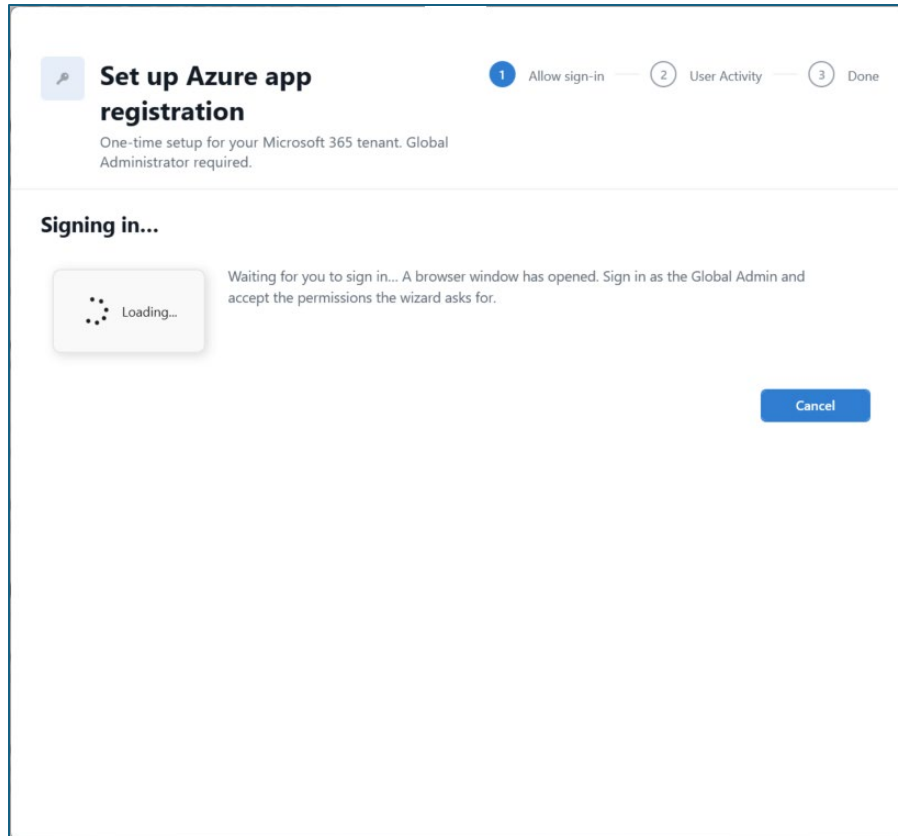
Not nowContinue to sign in

Sign in, accept, and return to the toolkit. The wizard gets ability to set up the **User Activity** app registration; confirms the organization consent has been recorded and works out your **SharePoint root site**. If you click 'Not now', you will need to manually input the tenant root site and User Activity setup and consent verification is skipped.





This second sign in is to give wizard temporary ability to create User Activity app registration, retrieve tenant URL and confirm everything works. You do **not** need to 'Consent on behalf of your organization', ticking this option will cause any hard but does nothing, the wizard removes its own permissions from the organization-wide grant when it closes.



### Step 5: *Create the User Activity app*

The wizard shows who you are signed in as and your tenant ID.

1. Check **SharePoint root site**. It is filled from your tenant's default domain; correct it if the guess is wrong. Use the root (<https://contoso.sharepoint.com>), not a site path and not the -admin address.



## Set up Azure app registration

One-time setup for your Microsoft 365 tenant. Global Administrator required.

✓ Allow sign-in
2 User Activity
3 Done

### User Activity app registration

Signed in as [chris.ang@cognillo.work](#) · tenant 21a7c3d8-c30f-431b-968a-69ab0f2fff44

✓ Your organization has consented to the shared app. Web Browser sign-in is ready.

Create it now? The wizard will register a single-tenant app in Microsoft Entra, generate a certificate, upload it, add Office 365 Management APIs › ActivityFeed.Read (application), grant admin consent, and save a ready-to-use connection in this toolkit. The certificate password is generated for you and stored encrypted with the connection.

**SharePoint root site**

Used to tie the connection to your tenant. Filled in from your tenant's default domain; change it if the guess is wrong.

**Names**

These are only labels; change them if your organization has a naming convention. The app can also be renamed in Microsoft Entra later.

**App registration name in Microsoft Entra**

Shown under App registrations and Enterprise applications. Also used for the certificate name and the .pfx file name. If an app with this name already exists, it is reused and a new certificate is added to it.

**Connection name in this toolkit (user activity)**

How the certificate connection is listed on the Connections page.

**Connection name in this toolkit (sites & content)**

A Web Browser sign-in connection through the shared app, added because this tenant has none yet. Reports and fixes run through it.

Skip for now
Create the User Activity app

- Under Names, change any of the three labels if your organization has a naming convention.

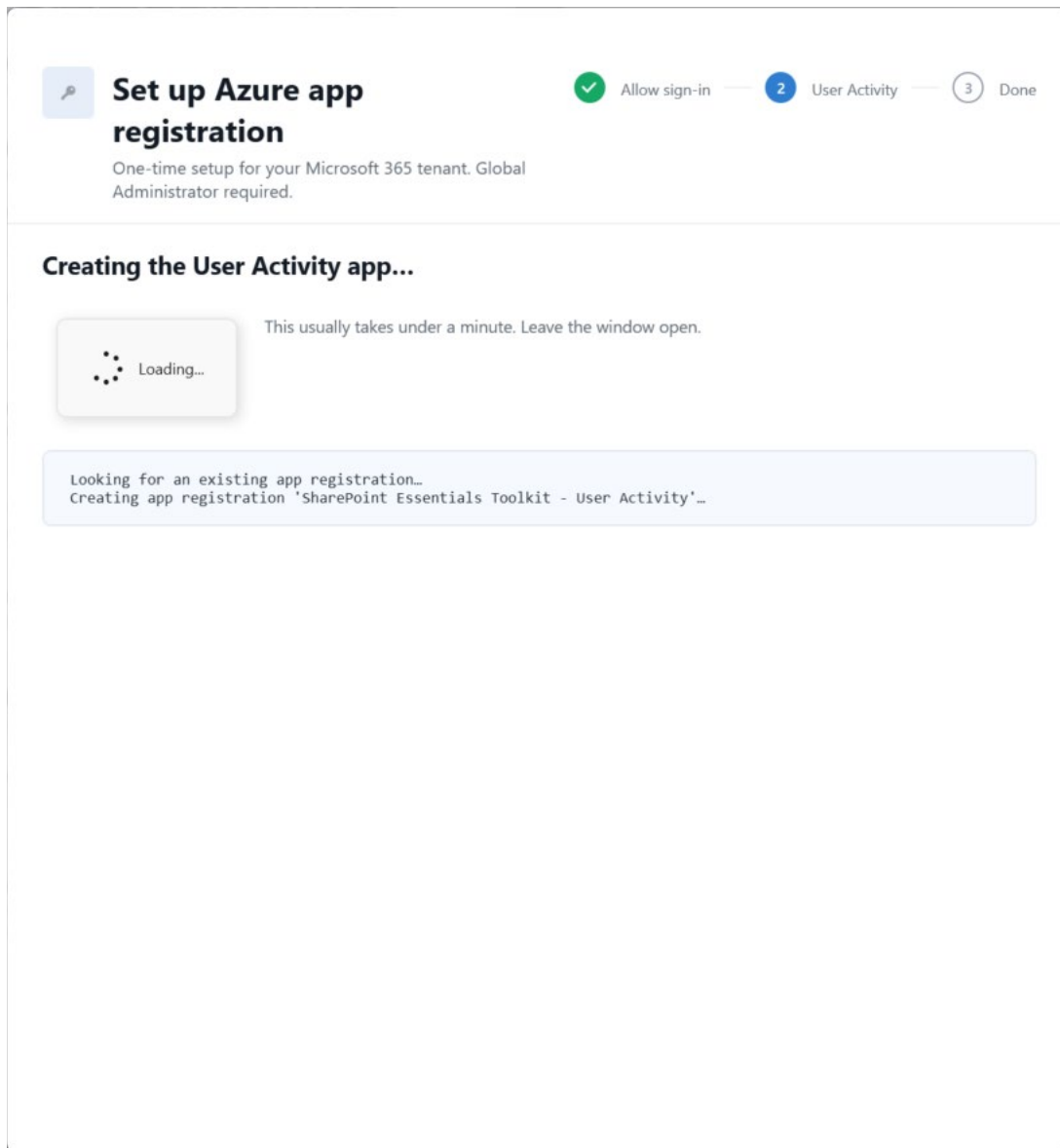
Defaults:

- App registration name in Microsoft Entra: SharePoint Essentials Toolkit - User Activity
- Connection name (user activity): Microsoft 365 user activity
- Connection name (sites & content): SharePoint sites & content (only shown when the tenant has no sites-and-content connection yet)

- Click **Create the User Activity app**.

Or click **Skip for now** to finish with sign-in consent only. You can run the wizard again later for the User Activity part.

The wizard then registers the app, creates and uploads a certificate, adds the permission, grants admin consent, saves the connections, and tests the certificate against Microsoft 365. This usually takes under a minute. Leave the window open.



---

**NOTE: Already have one?** If a User Activity connection for this tenant already exists in the toolkit, the wizard asks before continuing. The existing connection is disabled, not deleted, and can be re-enabled on the Connections page. If an app registration with the chosen name already exists in Microsoft Entra, it is reused and a new certificate is added alongside the existing ones; nothing is removed.

---

### Step 6: Review the summary

The **Setup complete** page shows:

- Consent status for both apps.
- The connections that were added.
- For the User Activity app: the app registration name, **App (client) ID** (with Copy), the certificate .pfx path (with **Show in folder**), the certificate expiry date, and the certificate password (hidden; click Show to reveal).

Keep a note of the certificate password only if you plan to use the same .pfx on another machine. On this machine it is already stored encrypted with the connection.

Click **Open Connections** to see the new profiles, or **Close**.

 **Set up Azure app registration**

One-time setup for your Microsoft 365 tenant. Global Administrator required.

✓ Allow sign-in — ✓ User Activity — 3 Done

### Setup complete

Admin consent granted for both apps.

A connection named SharePoint sites & content (Web Browser sign-in through the shared app) was added for your tenant.

#### Microsoft 365 user activity

The certificate signs in and the token carries ActivityFeed.Read.

|                      |                                                                                                                                                                                                                                                                              |                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| App registration     | SharePoint Essentials Toolkit - User Activity                                                                                                                                                                                                                                |                      |
| App (client) ID      | fc2661ef-1d2e-489b-8c68-                                                                                                                                                                  | <a href="#">Copy</a> |
| Certificate (.pfx)   | C:\Users\  \AppData\Roaming\Cognillo\SharePoint Essentials Toolkit\Governance\Certificates\SharePoint Essentials Toolkit - User Activity 20261009-1326.pfx <a href="#">Show in folder</a> |                      |
| Certificate expires  | 9 October 202                                                                                                                                                                             |                      |
| Certificate password | ..... <a href="#">Show / hide</a>                                                                                                                                                                                                                                            |                      |

Keep the .pfx and its password safe; you only need them again to use this connection on another machine. The password is already stored encrypted with the connection on this one. Put a reminder in your calendar a month before the certificate expires.

Open ConnectionsFinish

When you close, the toolkit offers to create the scheduled User Activity sync task and collects the first batch of activity.

### *What was created*

#### **In Microsoft Entra**

| Where                                                | What                                                                                                                                                                                                                |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enterprise applications</b>                       | <b>SharePoint Essentials Toolkit (Cognillo's shared app).</b> It does not appear under App registrations; it is registered in Cognillo's tenant. Its Permissions tab shows what was granted and lets you revoke it. |
| <b>App registrations and Enterprise applications</b> | <b>SharePoint Essentials Toolkit - User Activity (or your name),</b> with one certificate and the ActivityFeed.Read application permission, admin-consented. Branding shows the Cognillo logo and links.            |

#### **In the toolkit (Connections page)**

| Connection                            | Type                                                | Default                                        |
|---------------------------------------|-----------------------------------------------------|------------------------------------------------|
| <b>SharePoint sites &amp; content</b> | <b>Web Browser sign-in through the shared app</b>   | <b>Yes.</b> Reports and fixes run through it.  |
| <b>Microsoft 365 user activity</b>    | <b>Certificate sign-in to the User Activity app</b> | <b>No.</b> Used only for audit-log collection. |

#### **On this computer**

.pfx and .cer files in the toolkit's Governance\Certificates folder, named after the app and timestamped. The .pfx password is stored encrypted on the connection.

The certificate is valid for two years. Run the wizard again before it expires to add a new one; the old one keeps working until its date.

### *If you are not the Global Administrator*

1. Open the wizard and click **I'm not a Global Admin.**
2. Click **Copy to clipboard** and paste the text into an email to your admin. It contains the consent link for your tenant and the two ways to finish the User Activity part: run this wizard on their own machine, or run Setup-SPEAzure-SharedApp.ps1 from the toolkit download.
3. Once they confirm, Web Browser sign-in works for everyone. If they ran the wizard on their machine, ask them for the .pfx, its password and the **App (client) ID**, and add a User Activity connection with those on your Connections page.



## Set up Azure app registration

One-time setup for your Microsoft 365 tenant. Global Administrator required.

1

 Allow sign-in
 

2

 User Activity
 

3

 Done

### Hand this to a Global Administrator

Copy the text below into an email. It has the consent link for your tenant and the two ways the admin can finish the User Activity part — this wizard on their own machine, or the PowerShell script in the toolkit download.

No license is used. The admin can install the toolkit and run this wizard without activating it, so a single-user license is not taken up. Only the Test Connection task on the Connections page needs an activation; if they want to run it, they can activate and then hand the license back with Deactivate this computer on the License page.

Hi,

SharePoint Essentials Toolkit needs two one-time Azure steps that require a Global Administrator.

1. Allow sign-in for everyone (one click). Open this link, sign in, tick "Consent on behalf of your organization" if shown, and click Accept:  
[https://login.microsoftonline.com/organizations/adminconsent?client\\_id=2c88dfed-4cde-4c8d-bb6f-5fc7b75f16f6&redirect\\_uri=https%3A%2F%2Fwww.cognillo.com%2Fsharepoint-essentials-toolkit-consent-ok](https://login.microsoftonline.com/organizations/adminconsent?client_id=2c88dfed-4cde-4c8d-bb6f-5fc7b75f16f6&redirect_uri=https%3A%2F%2Fwww.cognillo.com%2Fsharepoint-essentials-toolkit-consent-ok)
2. Create the User Activity app registration (a certificate plus Office 365 Management APIs > ActivityFeed.Read). Either:
  - install SharePoint Essentials Toolkit and run Home > Set up Azure app registration, which does it in a few clicks, or
  - run Setup-SPEAzure-SharedApp.ps1 from the toolkit download (Optional folder) and send me the summary file and the .pfx it produces.

The wizard does not need a license: you can install the toolkit and run it without activating, so it will not take up a user license. If you also want to run Test Connection on the Connections page, activate first and then use Deactivate this computer on the license page to hand the license back.

Guide: <https://www.cognillo.com/help/set-up-azure-app-registration-sharepoint-essentials-toolkit>

Back

Copy to clipboard

Close

## Troubleshooting

| Message                                                                      | What to do                                                                                                                                                        |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "Your organization's consent ... has not shown up yet"                       | Consent can take a minute to appear. Click <b>Back</b> , then <b>I've accepted, continue</b> again. If you never clicked Accept, open the consent page and do so. |
| "That account cannot consent to the permissions the wizard needs"            | The account is not a Global Administrator. Sign in with one, or use <b>I'm not a Global Admin</b> .                                                               |
| "Microsoft Entra refused the request ... does not have enough privileges"    | Same cause, or the tenant blocks app creation. Run Setup-SPEAzure-SharedApp.ps1 from the toolkit download as a Global Admin instead.                              |
| "More than one app registration is named ..."                                | Rename or delete the duplicates in Microsoft Entra, then run the wizard again.                                                                                    |
| "The certificate signs in, but the token does not carry any permissions yet" | Admin consent is still propagating. The connection is saved and will work within a few minutes.                                                                   |

| Message                                             | What to do                                                                                              |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| "The logo and publisher links ... could not be set" | Cosmetic only. The connection is unaffected.                                                            |
| Certificate could not be uploaded                   | Upload the .cer from Governance\Certificates under the app's Certificates & secrets in Microsoft Entra. |

## (Easy) Partially Automated using a Link

Use this when you only need SharePoint Essentials Toolkit to sign in to SharePoint for reports and fixes, and do not need User Activity Services (audit-log based reports and Monitoring). It is a single browser step and does not create anything in your tenant's App registrations.

A Global Administrator opens one link, signs in and clicks **Accept**. That grants tenant-wide consent to Cognillo's shared app so everyone in your organization can use **Web Browser sign-in** without a "Need admin approval" prompt.

**You need:** a Global Administrator account for the tenant. No toolkit license is used; the admin does not even need the toolkit installed.

**Time:** about two minutes.

---

***NOTE: Want User Activity reports and Monitoring as well? Use the wizard instead; it does this step and the User Activity app registration in one pass. See "Fully Automated using app wizard" above. You can also do the link step now and run the wizard later; it will detect that consent is already granted and skip ahead.***

***NOTE: Automatic registration (using the link) supports Web Browser (delegated) sign-in for SharePoint sites & content. It does not support Certificate Based Authentication; a Certificate connection for SharePoint sites & content (for example, for scheduled jobs) requires your own app registration.***

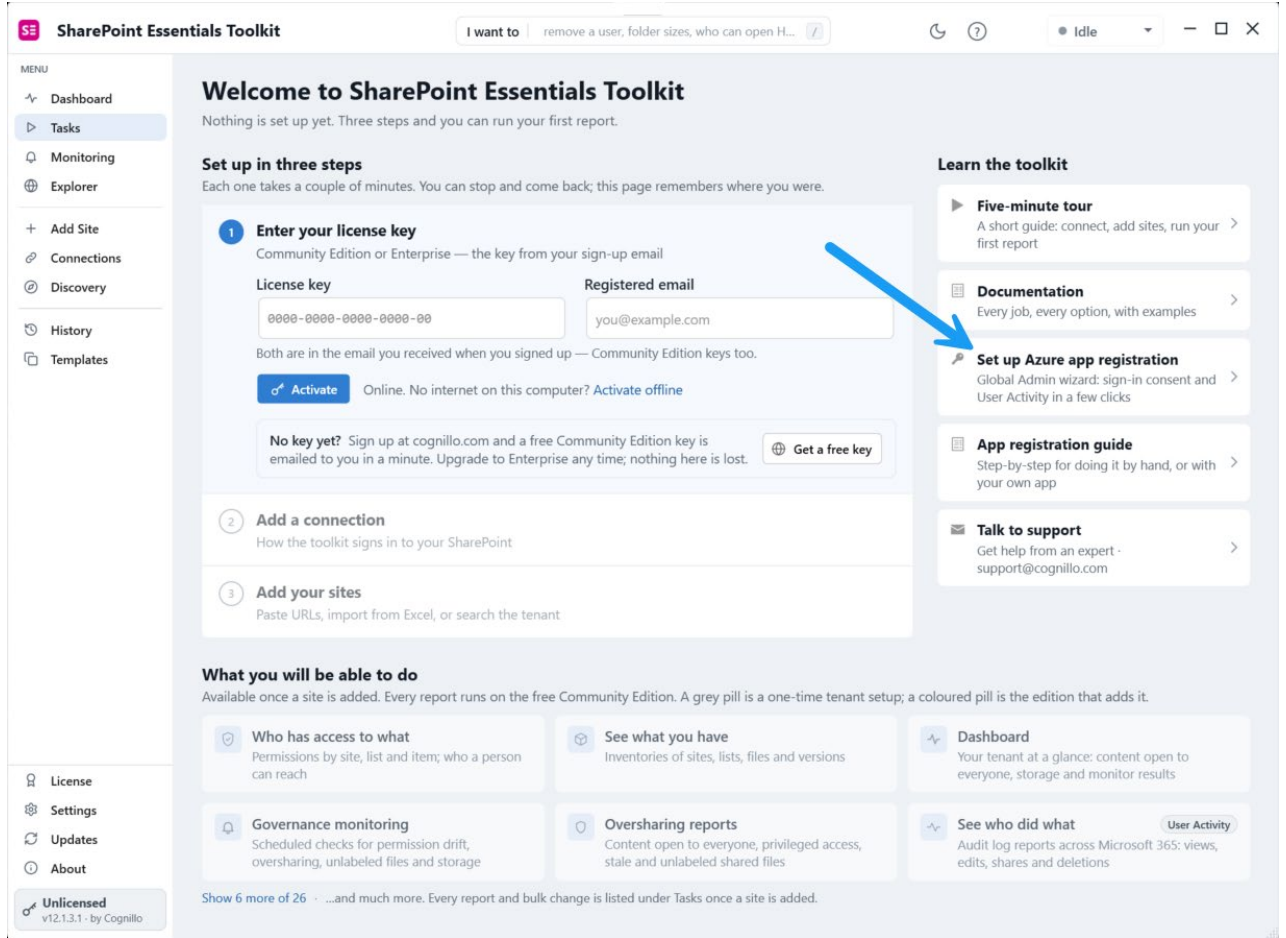
---

### Step 1: Get the consent link

The link is specific to your tenant. Either of these gives you the right one:

#### **From the toolkit (any user, no license needed)**

1. Open **Home > Set up Azure app registration** (or the same link on the **Connections page**).



**SharePoint Essentials Toolkit**

I want to remove a user, folder sizes, who can open H...

**Welcome to SharePoint Essentials Toolkit**

Nothing is set up yet. Three steps and you can run your first report.

**Set up in three steps**

Each one takes a couple of minutes. You can stop and come back; this page remembers where you were.

**1 Enter your license key**

Community Edition or Enterprise — the key from your sign-up email

License key  Registered email

Both are in the email you received when you signed up — Community Edition keys too.

[Activate](#) Online. No internet on this computer? [Activate offline](#)

No key yet? Sign up at [cognillo.com](#) and a free Community Edition key is emailed to you in a minute. Upgrade to Enterprise any time; nothing here is lost. [Get a free key](#)

**2 Add a connection**

How the toolkit signs in to your SharePoint

**3 Add your sites**

Paste URLs, import from Excel, or search the tenant

**Learn the toolkit**

- Five-minute tour**  
A short guide: connect, add sites, run your first report
- Documentation**  
Every job, every option, with examples
- Set up Azure app registration**  
Global Admin wizard: sign-in consent and User Activity in a few clicks
- App registration guide**  
Step-by-step for doing it by hand, or with your own app
- Talk to support**  
Get help from an expert - [support@cognillo.com](#)

**What you will be able to do**

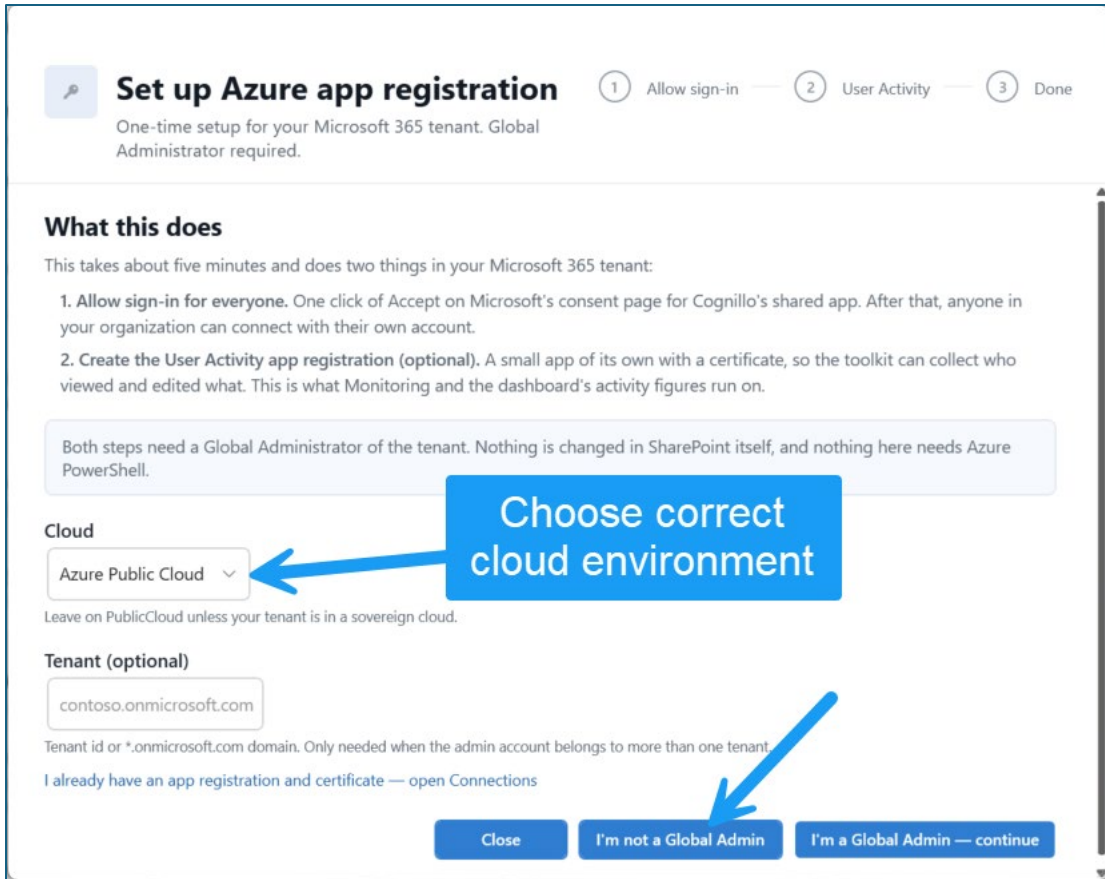
Available once a site is added. Every report runs on the free Community Edition. A grey pill is a one-time tenant setup; a coloured pill is the edition that adds it.

- Who has access to what**  
Permissions by site, list and item; who a person can reach
- See what you have**  
Inventories of sites, lists, files and versions
- Dashboard**  
Your tenant at a glance: content open to everyone, storage and monitor results
- Governance monitoring**  
Scheduled checks for permission drift, oversharing, unlabeled files and storage
- Oversharing reports**  
Content open to everyone, privileged access, stale and unlabeled shared files
- See who did what** User Activity  
Audit log reports across Microsoft 365: views, edits, shares and deletions

[Show 6 more of 26](#) ...and much more. Every report and bulk change is listed under Tasks once a site is added.

**Unlicensed**  
v12.1.3.1 · by Cognillo

2. Click **I'm not a Global Admin.**



**Set up Azure app registration** 1 Allow sign-in — 2 User Activity — 3 Done

One-time setup for your Microsoft 365 tenant. Global Administrator required.

### What this does

This takes about five minutes and does two things in your Microsoft 365 tenant:

1. **Allow sign-in for everyone.** One click of Accept on Microsoft's consent page for Cognillo's shared app. After that, anyone in your organization can connect with their own account.
2. **Create the User Activity app registration (optional).** A small app of its own with a certificate, so the toolkit can collect who viewed and edited what. This is what Monitoring and the dashboard's activity figures run on.

Both steps need a Global Administrator of the tenant. Nothing is changed in SharePoint itself, and nothing here needs Azure PowerShell.

**Cloud**

Azure Public Cloud ▾

Leave on PublicCloud unless your tenant is in a sovereign cloud.

**Tenant (optional)**

contoso.onmicrosoft.com

Tenant id or \*.onmicrosoft.com domain. Only needed when the admin account belongs to more than one tenant.

[I already have an app registration and certificate — open Connections](#)

Close I'm not a Global Admin I'm a Global Admin — continue

3. Click **Copy to clipboard**. The copied text is a ready-made email that contains the link as item 1. Keep item 1 and drop item 2 if you do not want the User Activity part.


**Set up Azure app registration**

1

 Allow sign-in
 

2

 User Activity
 

3

 Done

One-time setup for your Microsoft 365 tenant.  
Global Administrator required.

### Hand this to a Global Administrator

Copy the text below into an email. It has the consent link for your tenant and the two ways the admin can finish the User Activity part — this wizard on their own machine, or the PowerShell script in the toolkit download.

No license is used. The admin can install the toolkit and run this wizard without activating it, so a single-user license is not taken up. Only the Test Connection task on the Connections page needs an activation; if they want to run it, they can activate and then hand the license back with Deactivate this computer on the License page.

Hi,  
  
 SharePoint Essentials Toolkit needs two one-time Azure steps that require a Global Administrator.  
  
 1. Allow sign-in for everyone (one click). Open this link, sign in, tick "Consent on behalf of your organization" if shown, and click Accept:  
[https://login.microsoftonline.com/organizations/adminconsent?client\\_id=2c88dfed-4cde-4c8d-bb6f-5fc7b75f16f6&redirect\\_uri=https%3A%2F%2Fwww.cognillo.com%2Fsharepoint-essentials-toolkit-consent-ok](https://login.microsoftonline.com/organizations/adminconsent?client_id=2c88dfed-4cde-4c8d-bb6f-5fc7b75f16f6&redirect_uri=https%3A%2F%2Fwww.cognillo.com%2Fsharepoint-essentials-toolkit-consent-ok)  
  
 2. Create the User Activity app registration (a certificate plus Office 365 Management APIs > ActivityFeed.Read). Either:  
 - install SharePoint Essentials Toolkit and run Home > Set up Azure app registration, which does it in a few clicks, or  
 - run Setup-SPEAzure-SharedApp.ps1 from the toolkit download (Optional folder) and send me the summary file and the .pfx it produces.  
  
 The wizard does not need a license: you can install the toolkit and run it without activating, so it will not take up a user license. If you also want to run Test Connection on the Connections page, activate first and then use Deactivate this computer on the License page to hand the license back.

Back

Copy to clipboard

Close

## By hand

Use the link below. Replace organizations with your tenant's domain (for example contoso.onmicrosoft.com) or tenant ID, or leave organizations in place and Microsoft asks which tenant to use after sign-in:

[https://login.microsoftonline.com/organizations/adminconsent?client\\_id=2c88dfed-4cde-4c8d-bb6f-5fc7b75f16f6&redirect\\_uri=https://www.cognillo.com/sharepoint-essentials-toolkit-consent-ok](https://login.microsoftonline.com/organizations/adminconsent?client_id=2c88dfed-4cde-4c8d-bb6f-5fc7b75f16f6&redirect_uri=https://www.cognillo.com/sharepoint-essentials-toolkit-consent-ok)

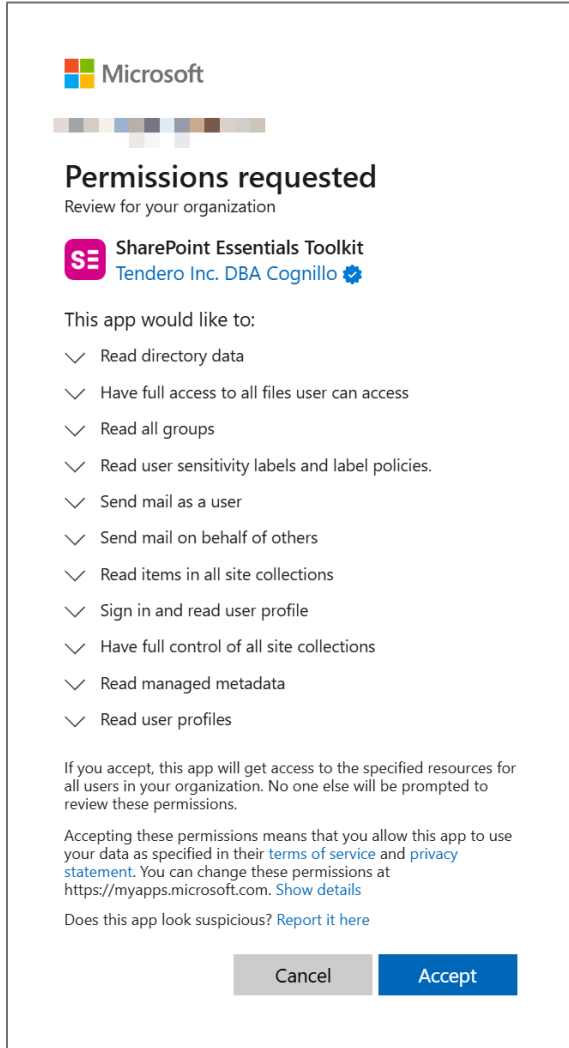
---

**NOTE: Government or sovereign clouds:** the host is different (login.microsoftonline.us for GCC High / DoD, login.chinacloudapi.cn for 21Vianet). Copy the link from the toolkit with the matching environment selected rather than building it by hand.

---

## Step 2: Grant consent (Global Administrator)

1. Open the link in a browser.
2. Sign in as the Global Administrator.
3. Read the permission list. If a **Consent on behalf of your organization** checkbox is shown, tick it.
4. Click **Accept**.



 Microsoft

 **SharePoint Essentials Toolkit**  
Tendero Inc. DBA Cognillo

Permissions requested  
Review for your organization

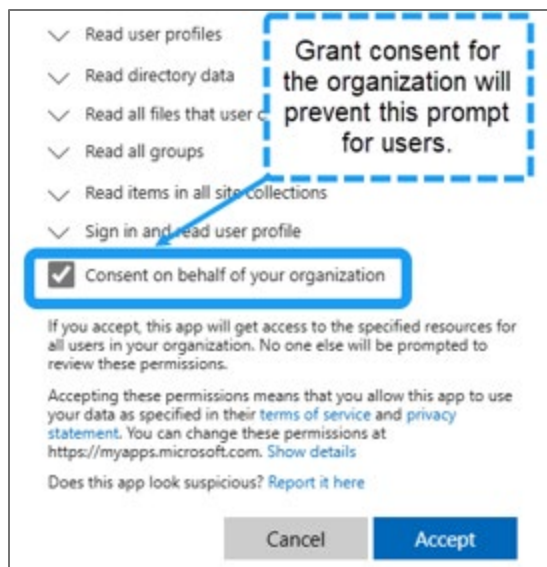
This app would like to:

- ✓ Read directory data
- ✓ Have full access to all files user can access
- ✓ Read all groups
- ✓ Read user sensitivity labels and label policies.
- ✓ Send mail as a user
- ✓ Send mail on behalf of others
- ✓ Read items in all site collections
- ✓ Sign in and read user profile
- ✓ Have full control of all site collections
- ✓ Read managed metadata
- ✓ Read user profiles

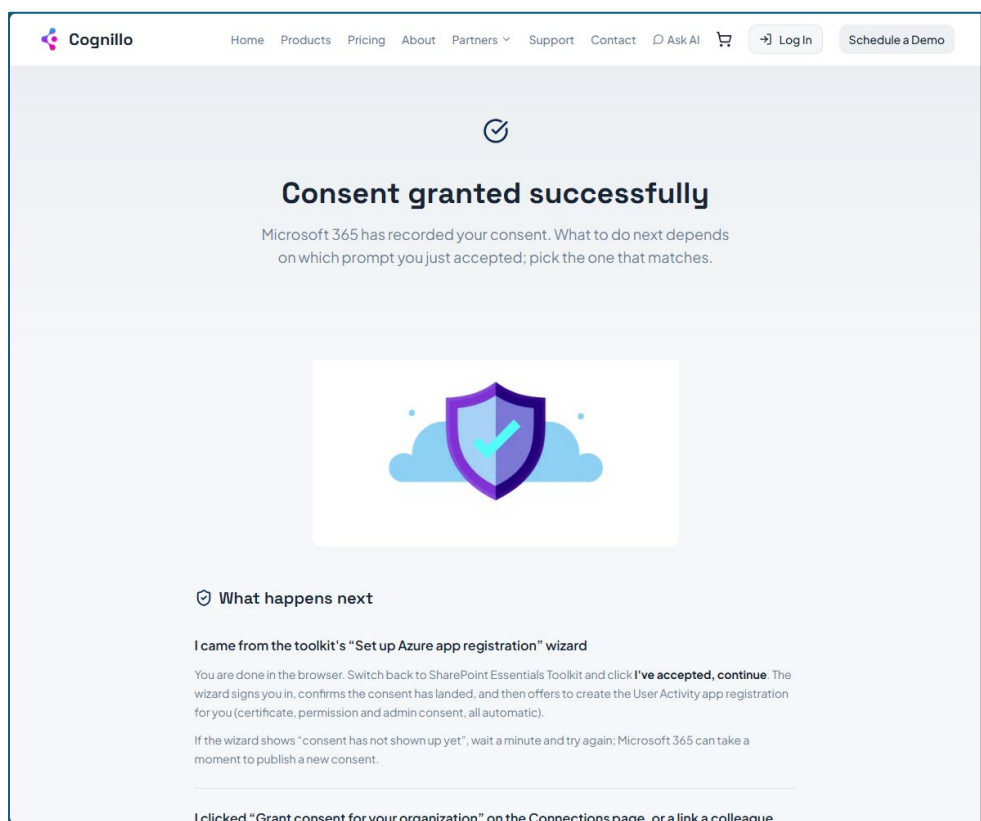
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their [terms of service](#) and [privacy statement](#). You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)



The browser lands on Cognillo's Consent granted successfully page. Nothing else is needed on the Microsoft side.



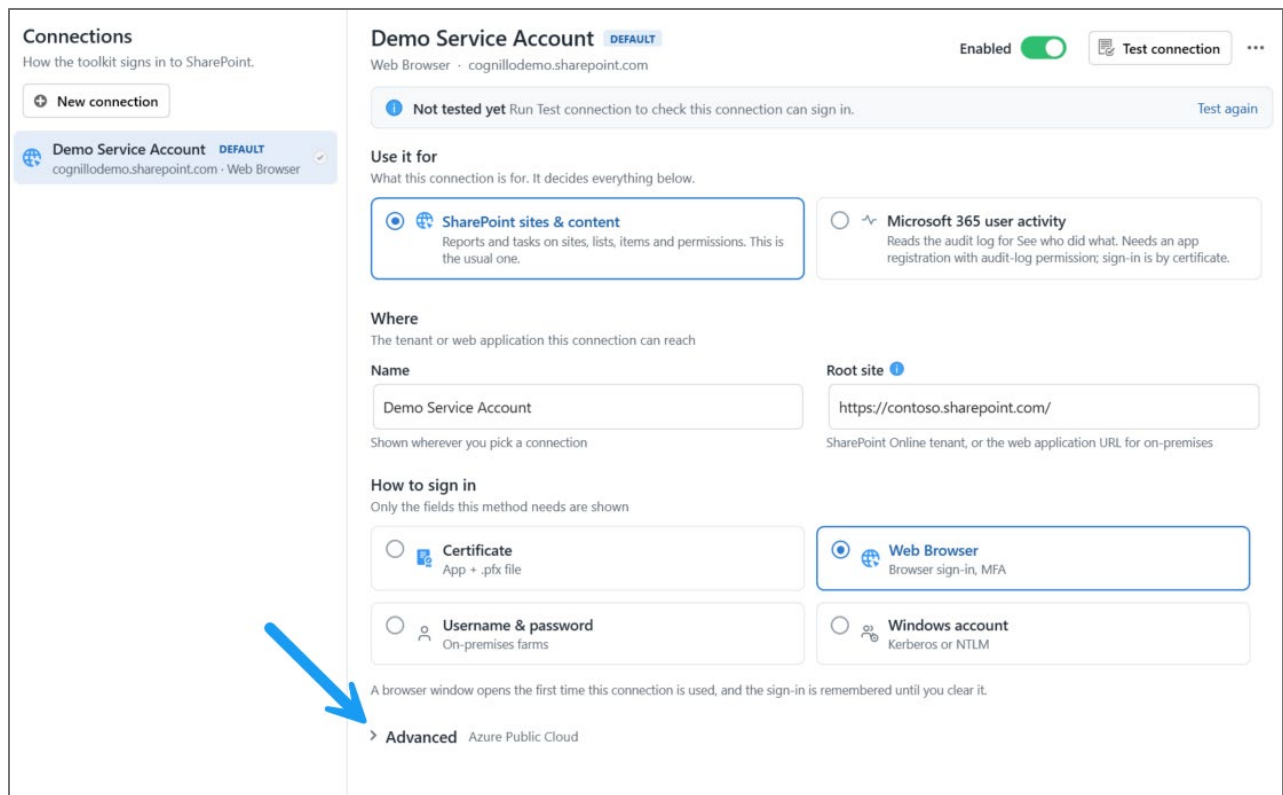
**What you are consenting to:** Delegated permissions only – read access to SharePoint sites, users and groups as the signed-in user, plus Send mail for emailing reports. Delegated means the toolkit acts as whoever is signed in and can never do more than that person can do in SharePoint.

Nothing is created under **App registrations**. The shared app is registered in Cognillo's tenant; your tenant gets a service principal entry under **Enterprise applications** named SharePoint Essentials Toolkit.

### Step 3: Add a connection in the toolkit

Each user who runs the toolkit does this once on their machine.

1. Open **Connections** and click **New connection**.
2. Give it a name, for example SharePoint sites & content.
3. Enter your SharePoint root site, for example <https://contoso.sharepoint.com> (the root, not a site path and not the -admin address).
4. Under **How to sign in**, choose **Web Browser**.
5. Click **Test connection**, sign in with your own Microsoft account when the browser window opens, and confirm it succeeds. (**Test connection** needs an activated license; saving does not.)
6. Save. If this is your first connection it becomes the default and every report and fix runs through it.



The screenshot shows the 'Connections' section on the left with a 'New connection' button. The main area is titled 'Demo Service Account' (DEFAULT) and shows it is 'Enabled'. A 'Test connection' button is visible. Below this, a message states 'Not tested yet Run Test connection to check this connection can sign in.' with a 'Test again' link.

**Use it for**  
What this connection is for. It decides everything below.

- ☒ **SharePoint sites & content**  
Reports and tasks on sites, lists, items and permissions. This is the usual one.
- ☐ **Microsoft 365 user activity**  
Reads the audit log for See who did what. Needs an app registration with audit-log permission; sign-in is by certificate.

**Where**  
The tenant or web application this connection can reach

**Name**  
Demo Service Account  
Shown wherever you pick a connection

**Root site**  
<https://contoso.sharepoint.com/>  
SharePoint Online tenant, or the web application URL for on-premises

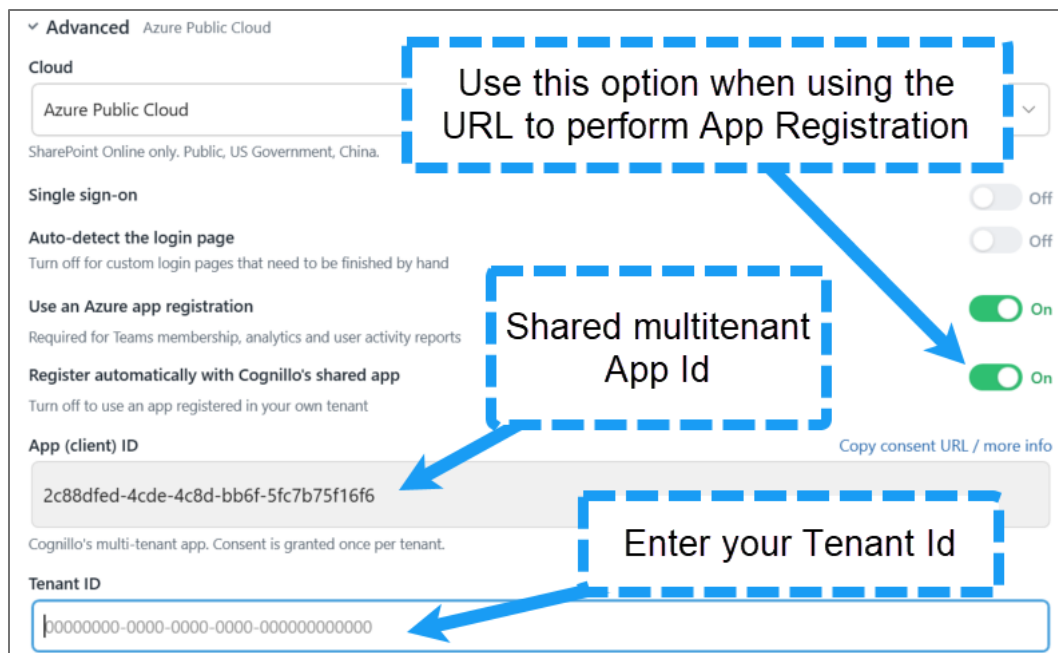
**How to sign in**  
Only the fields this method needs are shown

- ☐ **Certificate**  
App + .pfx file
- ☒ **Web Browser**  
Browser sign-in, MFA
- ☐ **Username & password**  
On-premises farms
- ☐ **Windows account**  
Kerberos or NTLM

A browser window opens the first time this connection is used, and the sign-in is remembered until you clear it.

**Advanced** Azure Public Cloud

If you expand **Advanced** and turn on **Use an Azure app registration**, keep **Register automatically with Cognillo's shared app** On and enter your **Tenant ID**:



Then add sites from Home or Sites as usual.

---

*NOTE: If a user still sees **Need admin approval** at sign-in, consent has not propagated yet or was granted in a different tenant. Wait a few minutes, and check the account's tenant matches the one the admin consented in.*

---

## What was created

### In Microsoft Entra

| Where                   | What                                                                                                                                                    |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enterprise applications | SharePoint Essentials Toolkit (Cognillo's shared app, application ID 2c88dfed-4cde-4c8d-bb6f-5fc7b75f16f6). Its Permissions tab lists what was granted. |
| App registrations       | Nothing.                                                                                                                                                |

### In the toolkit

Nothing is written automatically. Each user adds their own **Web Browser** connection (Step 3).

### What is not set up

User Activity Services. The toolkit shows User Activity Services is not configured on Monitoring, the Dashboard and in job options that depend on audit data. Those features stay off until a User Activity connection exists.

### Adding User Activity later

Run the wizard from **Home › Set up Azure app registration** as a Global Administrator, or run Setup-SPEAzure-SharedApp.ps1 from the toolkit download. Both recognize that sign-in consent is already granted and move straight to creating the User Activity app registration. See “Fully Automated using app wizard” or “Manual Registration using PowerShell”.

### Revoking consent

In Microsoft Entra, open **Enterprise applications › SharePoint Essentials Toolkit › Permissions** and revoke the grants, or delete the enterprise application. **Web Browser** sign-in then prompts for admin approval again. Rerun Step 2 to restore it.

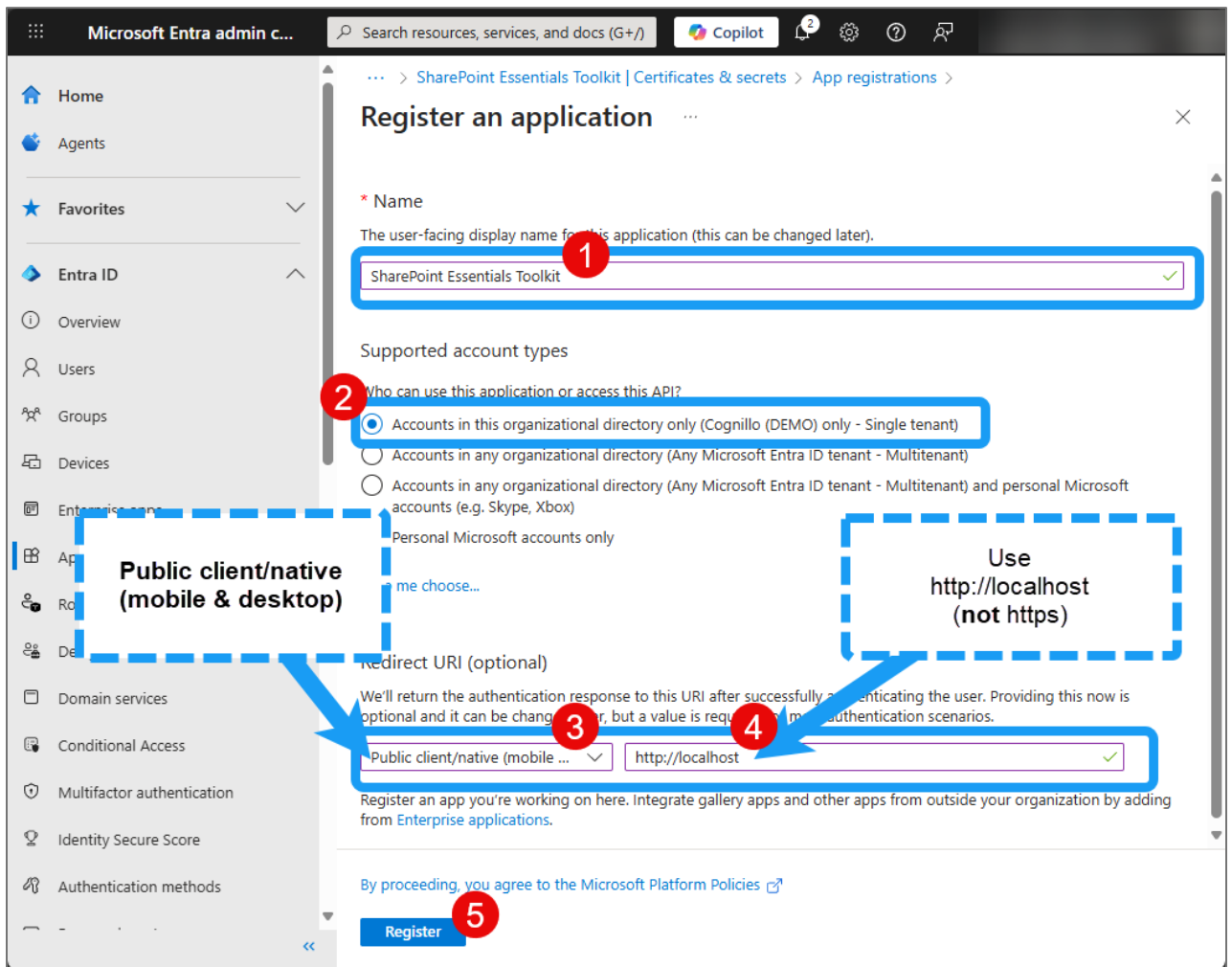
### Troubleshooting

| <b>Problem</b>                                                                                   | <b>What to do</b>                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>The consent page says the account is not authorized to consent</i>                            | <i>The account is not a Global Administrator (or a Privileged Role / Cloud Application Administrator). Sign in with one.</i>                                                                                               |
| <i>“AADSTS650052 ... needs access to a service that your organization has not subscribed to”</i> | <i>The tenant has no SharePoint Online or Exchange Online service plan behind the permission. Check the Microsoft 365 licensing on the tenant.</i>                                                                         |
| <i>“AADSTS90002 ... Tenant not found”</i>                                                        | <i>The domain in the link is wrong. Use the tenant’s .onmicrosoft.com domain, the tenant ID, or organizations.</i>                                                                                                         |
| <i>Users still get <b>Need admin approval</b></i>                                                | <i>Consent was granted in another tenant, or has not propagated yet. Confirm the enterprise application exists in the right tenant and wait a few minutes.</i>                                                             |
| <i>The redirect page does not load after Accept</i>                                              | <i>Consent was still recorded. Check <b>Enterprise applications</b> for SharePoint Essentials Toolkit; if it is there you are done.</i>                                                                                    |
| <i>Admin consent is blocked by policy for all apps</i>                                           | <i>A tenant admin can allow this one app from <b>Enterprise applications › Consent and permissions</b>, or grant it directly from the app’s <b>Permissions</b> tab with <b>Grant admin consent for &lt;tenant&gt;</b>.</i> |

## (Medium Effort (longest time)) Manual Registration using Azure Portal – (more control over API permissions)

Follow the steps below to create a unique app registration for the SharePoint Essentials Toolkit.

1. Navigate to <https://portal.azure.com>
2. Login
3. Go to Microsoft Entra ID
4. Under 'Manage', click 'App Registrations'.
5. Click 'New Registration'.
6. Enter a name for the app such as "SharePoint Essentials Toolkit".
7. Add <http://localhost> (not https) as a Redirect URI for "Public client/native (mobile & desktop)".



Microsoft Entra admin c...

Search resources, services, and docs (G+)

Copilot

SharePoint Essentials Toolkit | Certificates & secrets > App registrations >

### Register an application

\* Name

The user-facing display name for this application (this can be changed later).

SharePoint Essentials Toolkit

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Cognillo (DEMO) only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Public client/native (mobile & desktop) http://localhost

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

**Public client/native (mobile & desktop)**

**Use http://localhost (not https)**

### Application Redirect URI

The HTTP protocol is used (<http://localhost>) instead of HTTPS as the SharePoint Essentials Toolkit uses the local system browser to authenticate (i.e. such as Microsoft Edge or Google Chrome).

Reference can be found [here](#) (also see below).

## Redirect URIs

The redirect URIs to use in a desktop application depend on the flow you want to use.

Specify the redirect URI for your app by [configuring the platform settings](#) for the app in **App registrations** in the Microsoft Entra admin center.

- For apps that use [Web Authentication Manager \(WAM\)](#), redirect URIs need not be configured in MSAL, but they must be configured in the [app registration](#).
- For apps that use interactive authentication:
  - Apps that use embedded browsers: `https://login.microsoftonline.com/common/oauth2/nativeclient` (Note: If your app would pop up a window which typically contains no address bar, it is using the "embedded browser".)
  - Apps that use system browsers: `http://localhost` (Note: If your app would bring your system's default browser (such as Edge, Chrome, Firefox, and so on) to visit Microsoft login portal, it is using the "system browser".)

**Important**

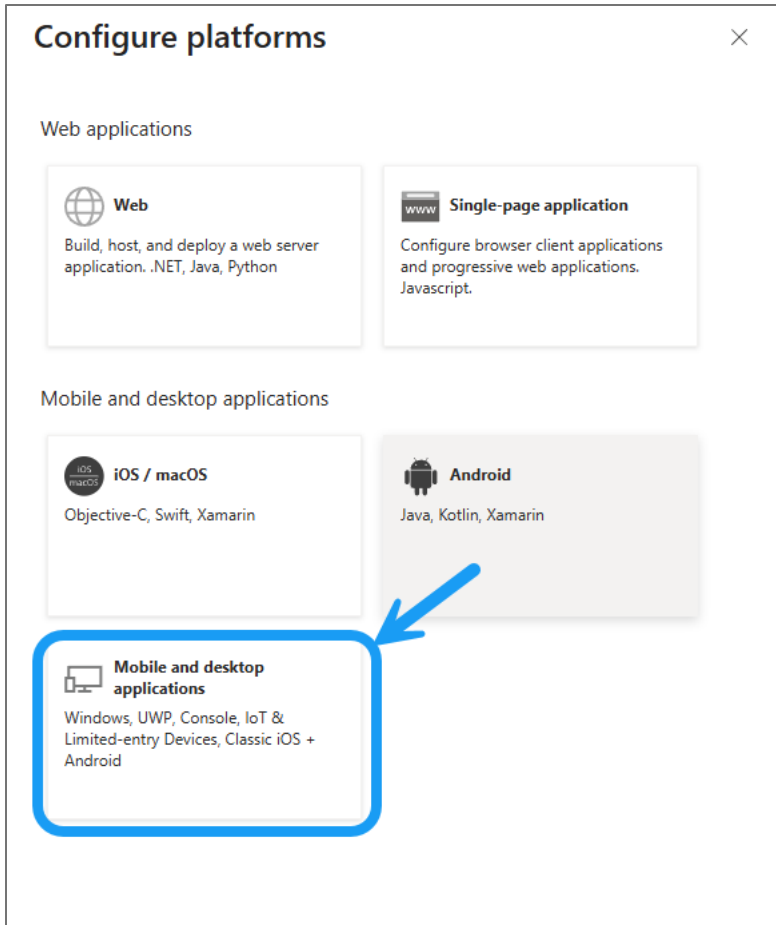
As a security best practice, we recommend explicitly setting `https://login.microsoftonline.com/common/oauth2/nativeclient` or `http://localhost` as the redirect URI. Some authentication libraries like MSAL.NET use a default value of `urn:ietf:wg:oauth:2.0:oob` when no other redirect URI is specified, which is not recommended. This default will be updated as a breaking change in the next major release.

For more information:

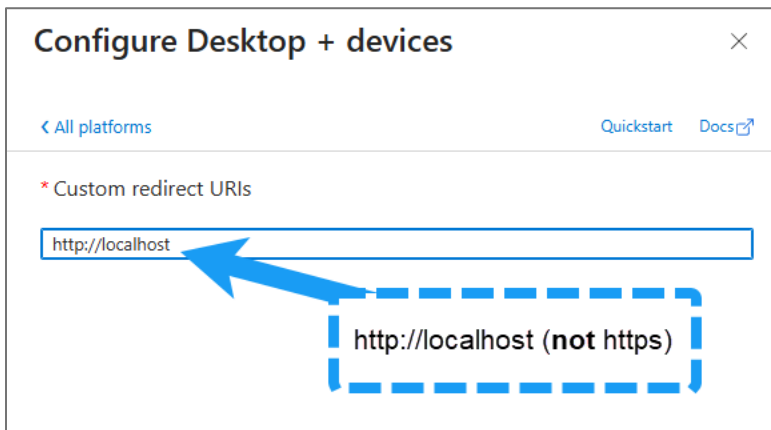
- [Quickstart: Register an app in the Microsoft identity platform - Microsoft identity platform | Microsoft Learn](#)

### *Configure the Registered Application*

1. In the **'Authentication'** tab, click **'Add a platform'**, and choose **"Mobile and desktop applications"**. You may skip to step 3 if you already see 'Mobile and desktop applications' in the page.



2. For the Custom redirect URIs, enter <http://localhost>  
See details [here](#) about the http vs https redirect URI.



3. Ensure the settings are configured as in the page below.

Home > App registrations > SharePoint Essentials Toolkit Test

## SharePoint Essentials Toolkit | Authentication

Search  Got feedback?

Overview  
Quickstart  
Integration assistant  
Diagnose and solve problems

Manage

- Branding & properties
- Authentication**
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- New support request

### Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

#### Mobile and desktop applications

##### Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) and the URI you send in the request to the login server should match one listed here. Also referred to as [Redirect URIs and their restrictions](#)

- ☐ <https://login.microsoftonline.com/common/oauth2/nativeclient>
- ☐ [https://login.live.com/oauth20\\_desktop.srf](https://login.live.com/oauth20_desktop.srf) (LiveSDK)
- ☐ [msal23680633-29c0-4bdf-8e65-8ec2a5f2994c//auth](https://login.live.com/oauth20_desktop.srf) (MSAL only)
- ☒ <http://localhost>

[Add URI](#)

**Automatically added by App Registration process**

**http://localhost (not https)**

### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Cognillo (DEMO) only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

### Advanced settings

[Save](#) [Discard](#)

**Allow public client flows = NO**  
Only set to YES if Username and Password will be supported (not recommended, less secure).

### Advanced settings

**Allow public client flows** ⓘ

Enable the following mobile and desktop flows:

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

**App instance property lock** ⓘ

Configure the application instance modification lock. [Learn more](#) [Configure](#)

**Yes No**

**NOTE:** To allow/support for 'Username and Password' authentication, **Allow public client flows** must be set to **Yes**.

'Username and password' is the least secure authentication method. Web browser

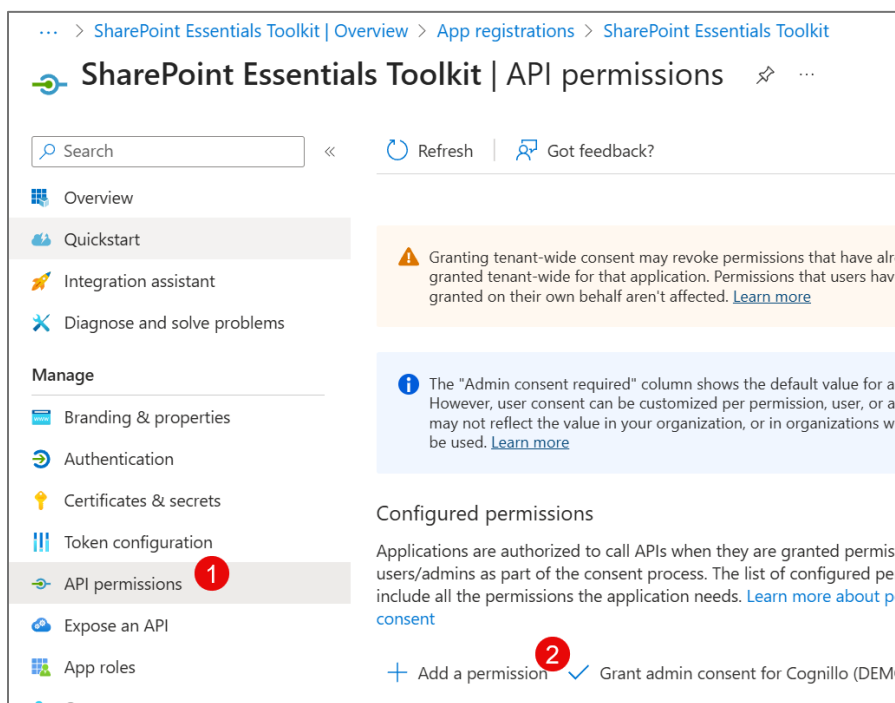
authentication or Certificate based authentication is recommended.

**NOTE:** It is important to use http and **not https** for this path as it can cause certificate binding issues when https is used, as the SharePoint Essentials Toolkit is a locally installed application and not a web application. See this [article](#) **‘Redirect URIs’** for more information.

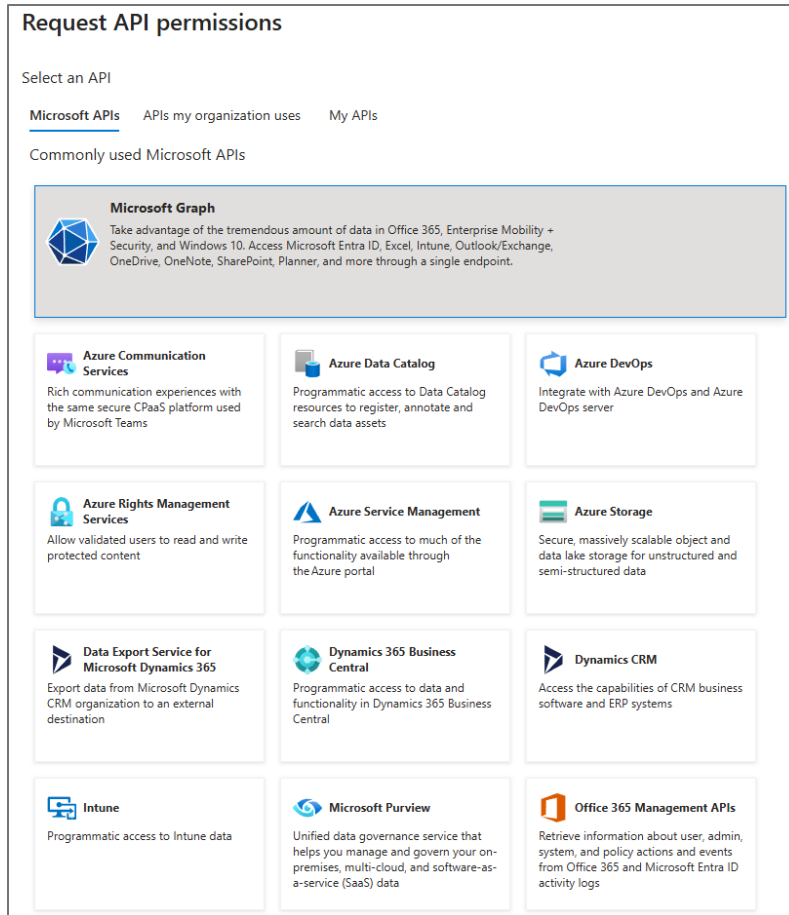
4. Click **‘Save’** if changes are made to this section.

### API Permissions Setup

1. In the Azure Portal, navigate to the App Registration created above.
2. Click **‘API permissions’** in the left navigation.



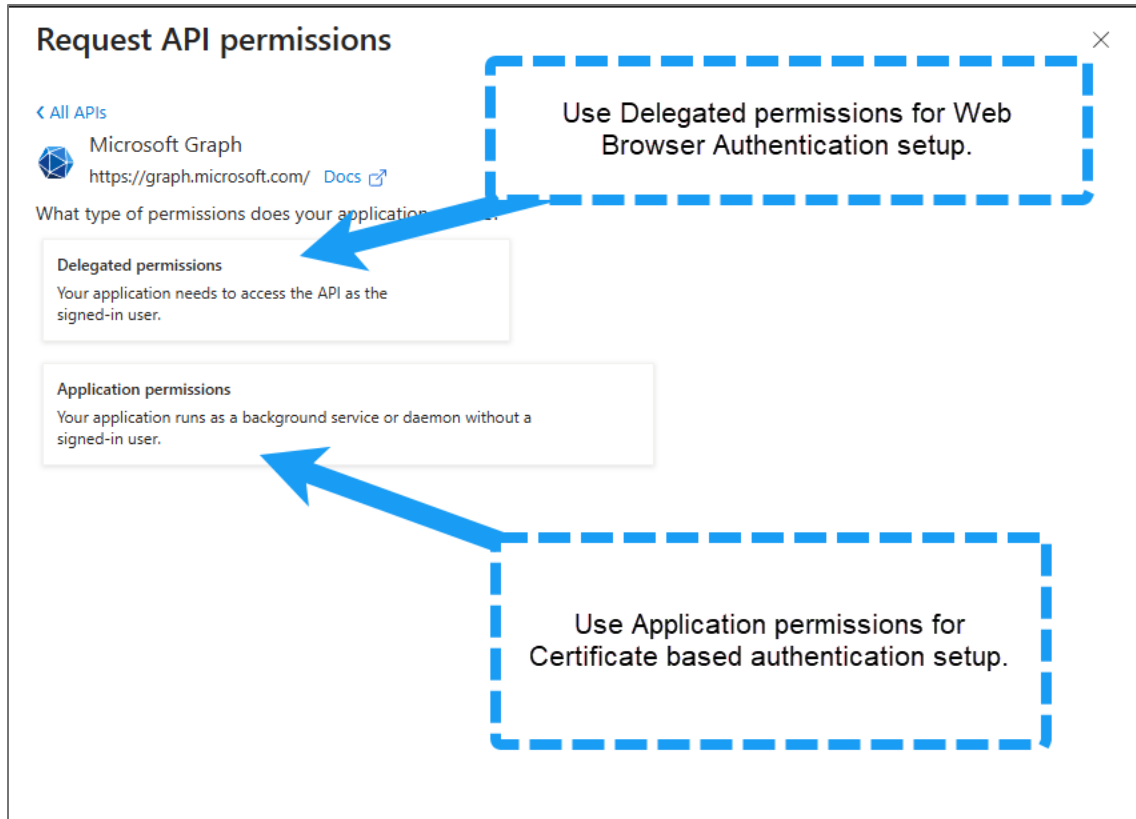
3. Click **‘Add a permission’**
4. See the **API Permissions table** below, click **Microsoft Graph** or appropriate tile



- Click **'Delegated permissions'** or **'Application permissions'**.

Web Browser Authentication – Use **Delegated Permissions**

Certificate-based authentication – Use **Application Permissions**



5. For each permission in the API Permissions Table below, paste the permission level into the search box and add it:

## Request API permissions

< All APIs


**Microsoft Graph**  
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

**Delegated permissions**  
Your application needs to access the API as the signed-in user.

**Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

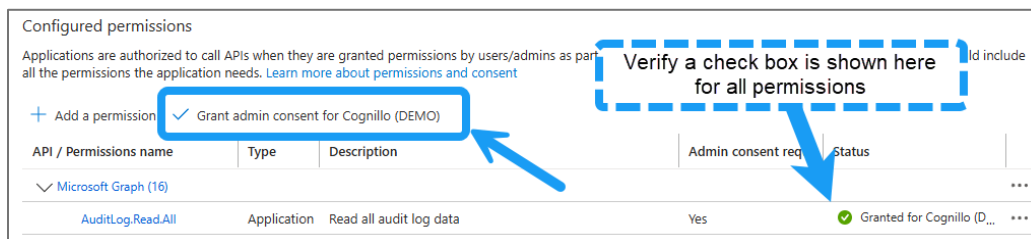
Select permissions expand all

Start typing a permission to filter these results

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

| Permission                                                                                                                                                                         | Admin consent required |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <input type="checkbox"/> openid <br>Sign users in                                               | No                     |
| <input type="checkbox"/> email <br>View users' email address                                    | No                     |
| <input type="checkbox"/> profile <br>View users' basic profile                                  | No                     |
| <input type="checkbox"/> offline_access <br>Maintain access to data you have given it access to | No                     |

6. After the API permissions have been added, click **'Grant admin consent for [tenant]'**.
  - a. This action requires elevated privileges.
  - b. For more information [Grant tenant-wide admin consent to an application - Microsoft Entra ID | Microsoft Learn](#)



7. The **'Status'** column should now show **"Granted for[tenant]"**.

### API Permissions Table

To access all SharePoint Essentials Toolkit features, see below required API permissions.

**NOTE:** If you configure the application to use delegated permissions, then the application will only delegate the permissions that the user has, with a 'maximum' permission level of 'Full Control' (using AllSites.FullControl). Users will only have access to what they already have in SharePoint when configured with delegated permissions.

**Delegated** (column) – For use when Delegated Permissions is used, such as with Web Browser Authentication.

**Application** (column) – For use when not using Delegated Permissions and user will authenticate to SharePoint using a certificate. This can be the same certificate or a different one than the one used for User Activity & Governance services (below).

**User Activity Certificate** (column) – For use when user will use User Activity & Governance Features. This is in addition to one or both Delegated & Application (Certificate-based) authentication.

| API Category Tile      | Delegated                           | Application                         | User Activity Certificate           | API Permission Level | Details                                                             |
|------------------------|-------------------------------------|-------------------------------------|-------------------------------------|----------------------|---------------------------------------------------------------------|
| <b>Microsoft Graph</b> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     | Directory.Read.All   | Permission Reports (Required to look up users and groups)           |
|                        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     | Files.ReadWrite.All  | Site & Content Analytics Reports                                    |
|                        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     | Group.Read.All       | Permission Reports (Required to view Entra ID domain group members) |
|                        |                                     |                                     | <input checked="" type="checkbox"/> | AuditLog.Read.All    | Sign in Activity Reports (coming soon)                              |
|                        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     | Sites.Read.All       | Required for Site & Content Analytics features                      |
|                        | <input checked="" type="checkbox"/> |                                     |                                     | User.Read            | Core functionality                                                  |
|                        |                                     | <input checked="" type="checkbox"/> |                                     | User.Read.All        | Core functionality                                                  |

|                                           |                                     |                                     |                                     |                                      |                                                                                                                                                   |
|-------------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | <input checked="" type="checkbox"/> |                                     |                                     | Mail.Send                            | Job alert email – send as the signed-in user                                                                                                      |
|                                           | <input checked="" type="checkbox"/> |                                     |                                     | Mail.Send.Shared                     | Job alert email – send from a shared mailbox                                                                                                      |
|                                           | <input checked="" type="checkbox"/> |                                     |                                     | Files.ReadWrite.All                  | Apply or remove sensitivity labels on selected files; send selected files to Microsoft 365 Archive (Sites.ReadWrite.All is accepted in its place) |
|                                           | <input checked="" type="checkbox"/> |                                     |                                     | InformationProtectionPolicy.Read     | List the sensitivity labels available to the signed-in user                                                                                       |
|                                           |                                     | <input checked="" type="checkbox"/> |                                     | Sites.ReadWrite.All                  | Application equivalent of Files.ReadWrite.All – sensitivity label actions and Send to Microsoft 365 Archive                                       |
|                                           |                                     | <input checked="" type="checkbox"/> |                                     | InformationProtectionPolicy.Read.All | Application equivalent of InformationProtectionPolicy.Read – list available sensitivity labels                                                    |
| <b>SharePoint</b>                         | <input checked="" type="checkbox"/> |                                     |                                     | AllSites.FullControl                 | Core functionality                                                                                                                                |
|                                           |                                     | <input checked="" type="checkbox"/> |                                     | Sites.FullControl.All                | Core functionality                                                                                                                                |
|                                           | <input checked="" type="checkbox"/> |                                     |                                     | Sites.Search.All                     | Core functionality                                                                                                                                |
|                                           | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     | TermStore.Read.All                   | Core functionality                                                                                                                                |
|                                           | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     | User.Read.All                        | Core functionality                                                                                                                                |
| <b>Office 365 Management Activity API</b> |                                     |                                     | <input checked="" type="checkbox"/> | ActivityFeed.Read                    | Required for Governance and User Activity features                                                                                                |

### Setup API Permissions for Governance & User Activity Features

To allow users to use the SharePoint Essentials Toolkit Governance & User Activity features, the following setup is required.

There are different features within Governance & User Activity, such as below:

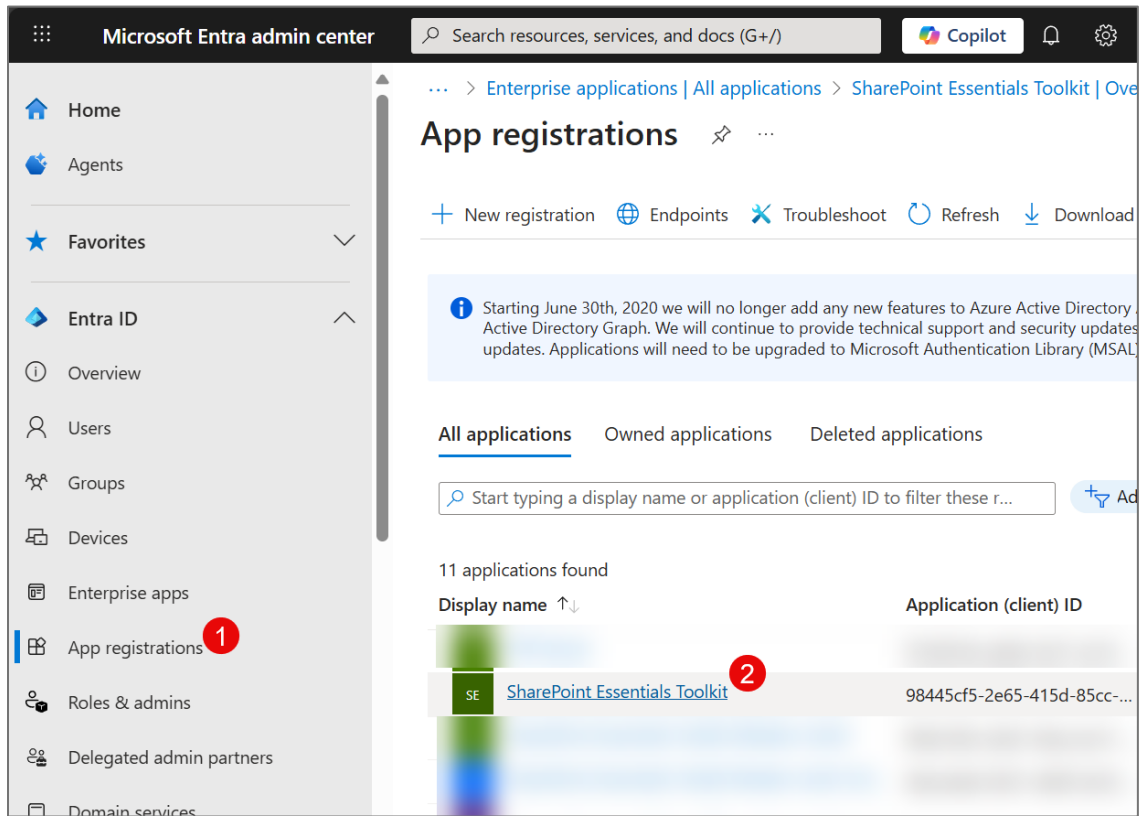
- User Activity – allows users to view events in content (content changes and permission or sharing changes).  
**For example:** Site, list and file, item, page changes. Such as deletions, edits, downloads, views, adding users, removing users, changes to permission levels, sharing of files or sharing links created.
- Sign In Activity – allows users to view user sign ins. This can be useful to determine the last activity or sign ins for certain users in order to determine if the user is inactive for a specified site.  
**For example:** The last time user ‘George Smith’ signed in.

### Enable the User Activity feature

Follow the steps below to enable use of the User Activity feature in the SharePoint Essentials Toolkit:

1. Navigate to the **Azure App Registration** section, select the SharePoint Essentials Toolkit app that was registered in previous steps.

You can also create a separate app registration for User Activity Services using steps above.



2. Click 'API Permissions', then 'Add a permission'

... > [SharePoint Essentials Toolkit | Overview](#) > [App registrations](#) > [SharePoint Essentials Toolkit](#)

## SharePoint Essentials Toolkit | API permissions

Search << Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems

### Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions** 1
- Expose an API
- App roles

**Grantee**

**Permissions**

**Admin consent required**

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have granted on their own behalf aren't affected. [Learn more](#)

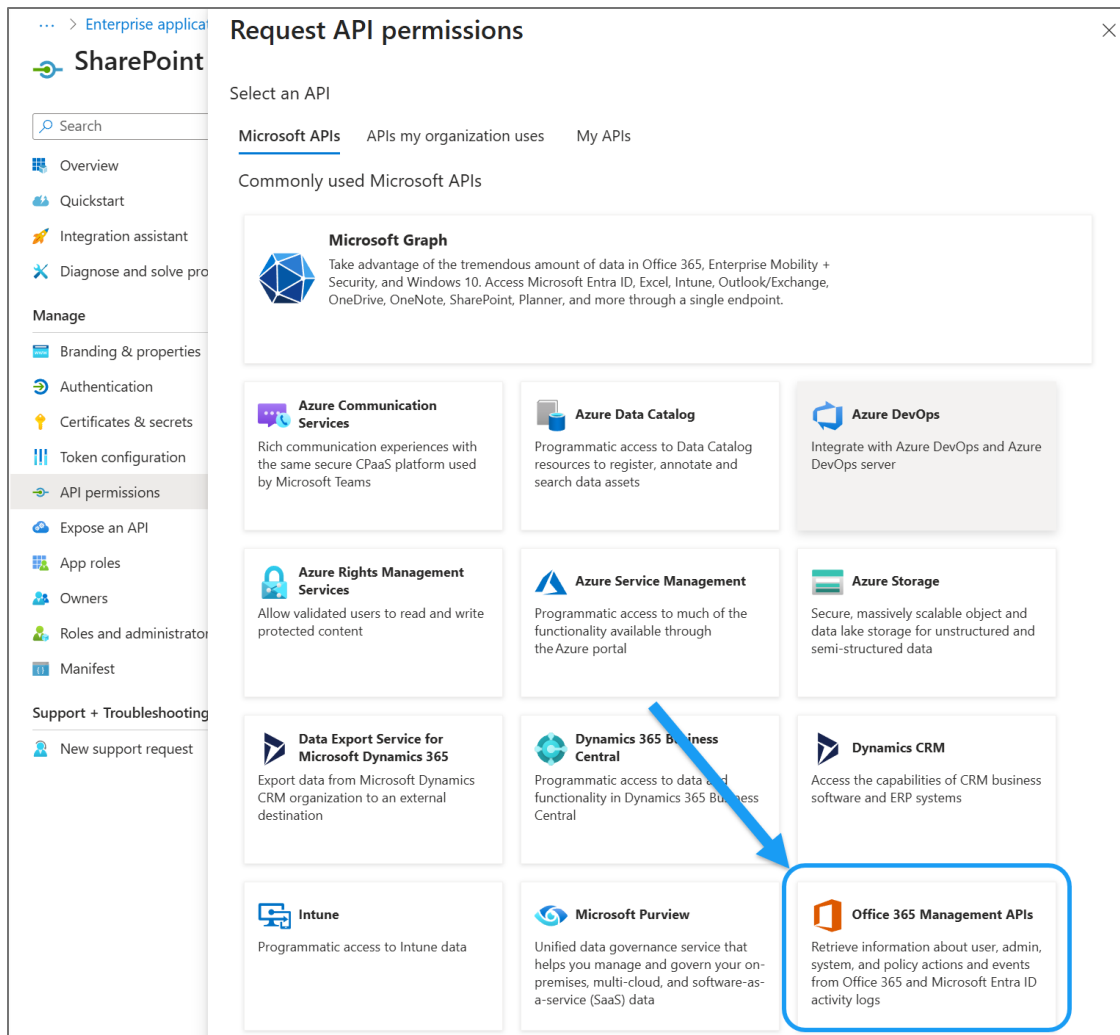
The "Admin consent required" column shows the default value for a permission. However, user consent can be customized per permission, user, or app. This may not reflect the value in your organization, or in organizations with which you are federated. [Learn more](#)

### Configured permissions

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 includes all the permissions the application needs. [Learn more about permissions](#)

**+** Add a permission 2 **✓** Grant admin consent for Cognillo (DEMO)

### 3. Select 'Office 365 Management APIs'



**Request API permissions**

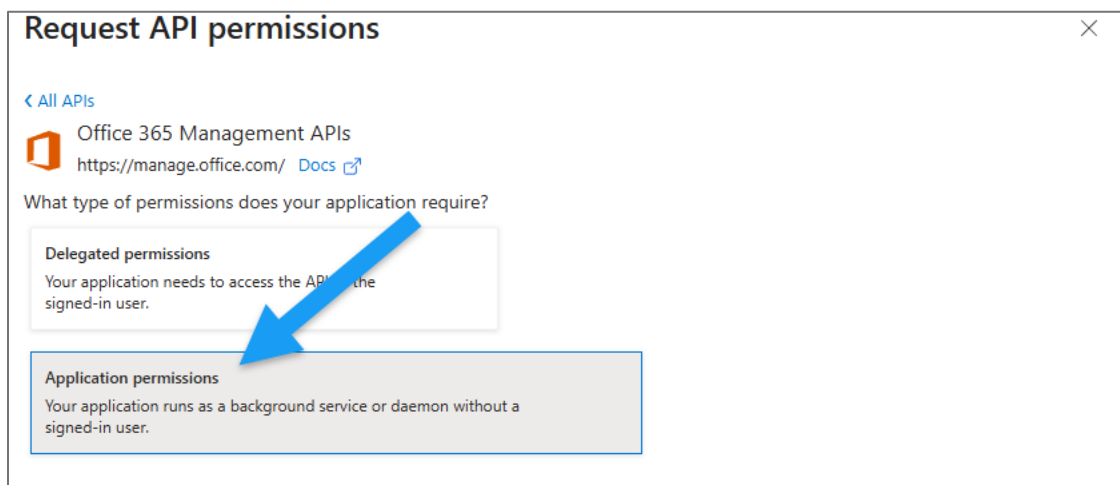
Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

- Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.
- Azure Communication Services**  
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams
- Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets
- Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server
- Azure Rights Management Services**  
Allow validated users to read and write protected content
- Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal
- Azure Storage**  
Secure, massively scalable object and data lake storage for unstructured and semi-structured data
- Data Export Service for Microsoft Dynamics 365**  
Export data from Microsoft Dynamics CRM organization to an external destination
- Dynamics 365 Business Central**  
Programmatic access to data and functionality in Dynamics 365 Business Central
- Dynamics CRM**  
Access the capabilities of CRM business software and ERP systems
- Intune**  
Programmatic access to Intune data
- Microsoft Purview**  
Unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data
- Office 365 Management APIs**  
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra ID activity logs

#### 4. Select 'Application permissions'



**Request API permissions**

< All APIs

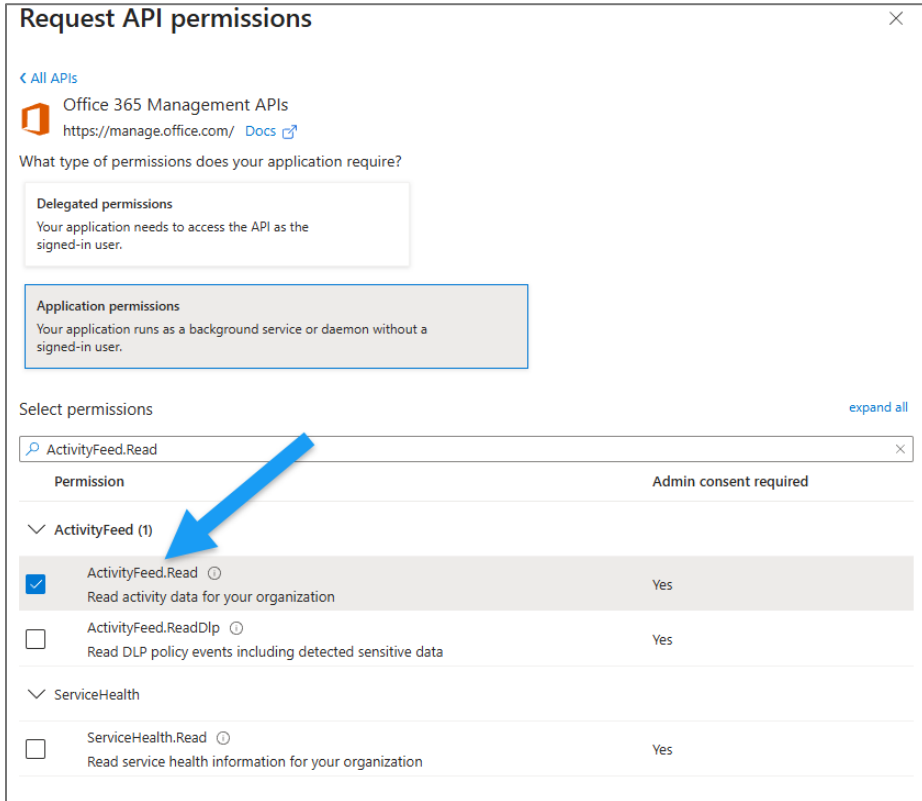
**Office 365 Management APIs**  
<https://manage.office.com/> Docs

What type of permissions does your application require?

- Delegated permissions**  
Your application needs to access the API as the signed-in user.
- Application permissions**  
Your application runs as a background service or daemon without a signed-in user.

5. Select '**ActivityFeed.Read**'. This will allow the application read activity data from Azure.

**IMPORTANT NOTE:** See [this information](#) about who can view user activity through the audit logs.



**Request API permissions**

< All APIs

Office 365 Management APIs  
<https://manage.office.com/> Docs

What type of permissions does your application require?

Delegated permissions  
Your application needs to access the API as the signed-in user.

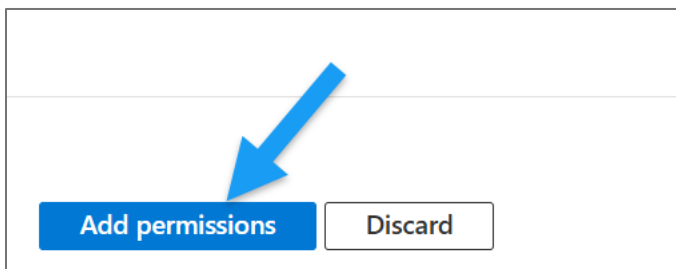
Application permissions  
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

ActivityFeed.Read

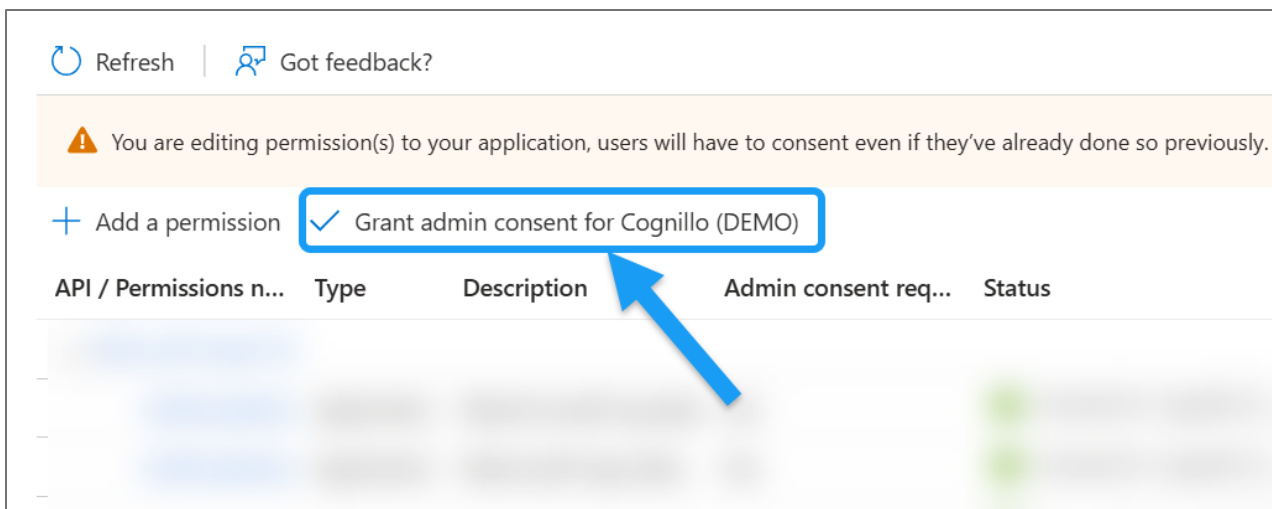
| Permission                                                                                                  | Admin consent required |
|-------------------------------------------------------------------------------------------------------------|------------------------|
| ActivityFeed (1)                                                                                            |                        |
| <input checked="" type="checkbox"/> ActivityFeed.Read ⓘ<br>Read activity data for your organization         | Yes                    |
| <input type="checkbox"/> ActivityFeed.ReadDlp ⓘ<br>Read DLP policy events including detected sensitive data | Yes                    |
| ServiceHealth                                                                                               |                        |
| <input type="checkbox"/> ServiceHealth.Read ⓘ<br>Read service health information for your organization      | Yes                    |

6. Click '**Add permissions**'

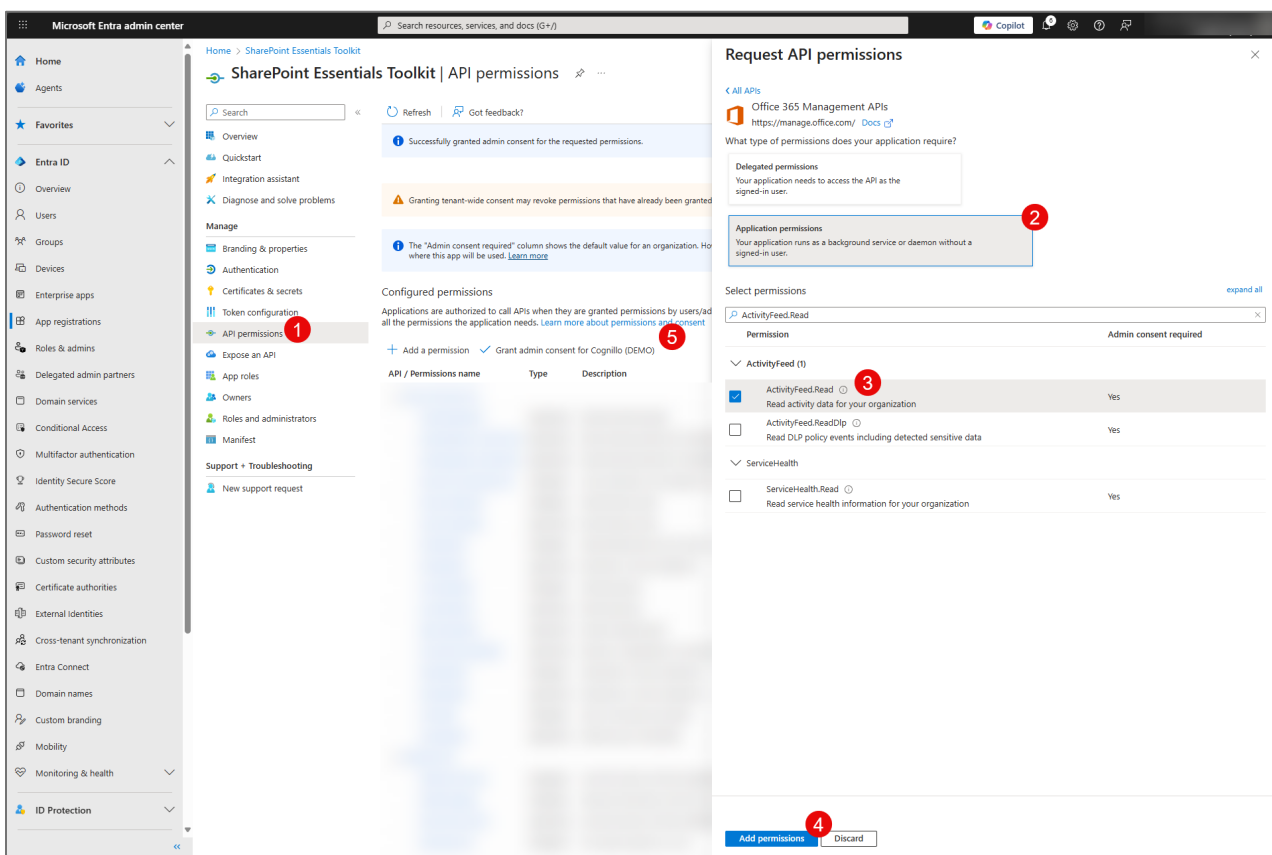


**Add permissions** Discard

7. Finally, click '**Grant admin consent for <tenant name>**'



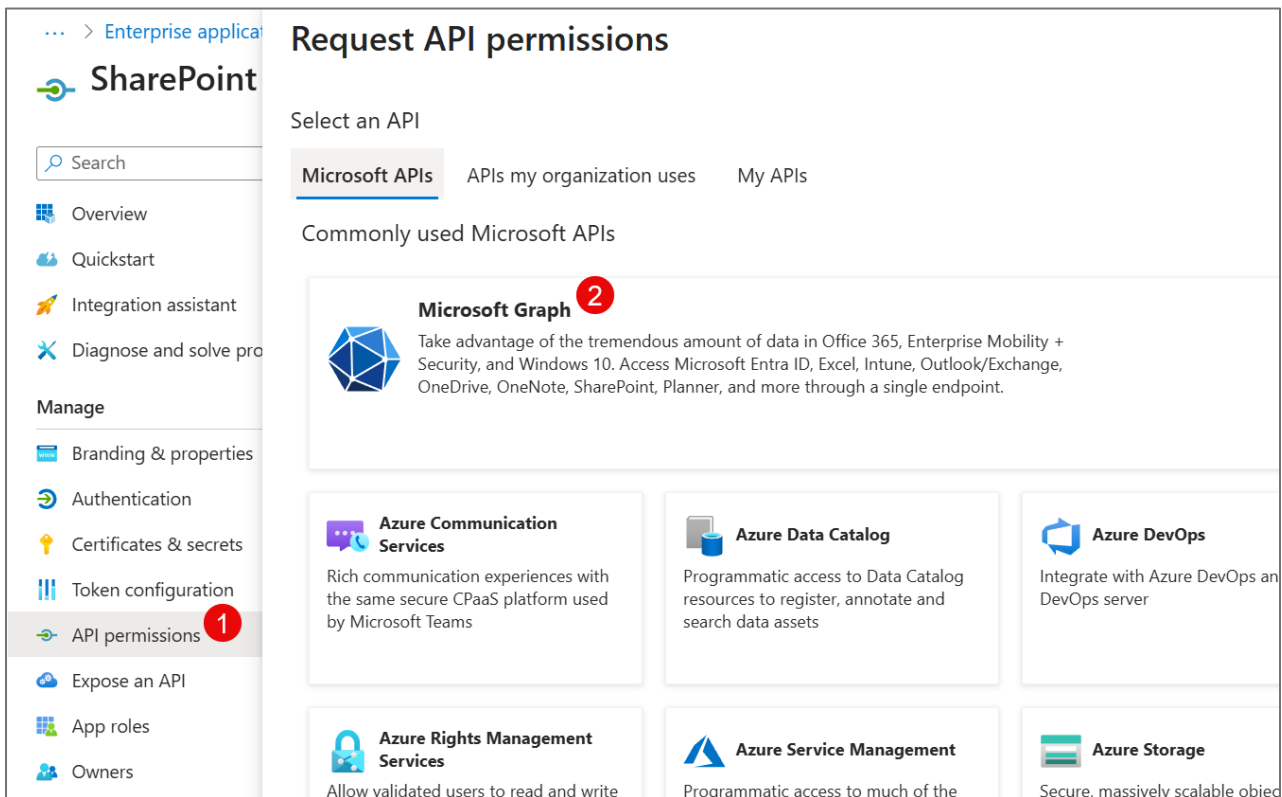
Summary of above steps below:



### Enable the Sign in Activity feature (future feature)

Add this API permission below to enable use of sign in reports in the SharePoint Essentials Toolkit. This report will provide users with details about the last sign in dates of users which can aid in finding orphaned accounts and identifying unused sites (with no sign ins within last N days).

1. Under the Azure App Registration section, click **'API permissions'**, then **'Microsoft Graph'**



The screenshot shows the 'Request API permissions' page in the Azure portal. The left sidebar contains the 'API permissions' link, which is highlighted with a red circle and the number 1. The main content area displays 'Microsoft Graph' as a commonly used API, also highlighted with a red circle and the number 2. Below this, several other APIs are listed in a grid, including Azure Communication Services, Azure Data Catalog, Azure DevOps, Azure Rights Management Services, Azure Service Management, and Azure Storage.

2. Click 'Application permissions'

## Request API permissions

< All APIs


 Microsoft Graph  
<https://graph.microsoft.com/>
[Docs](#)

What type of permissions does your application require?

**Delegated permissions**

Your application needs to access the API as the signed-in user.

**Application permissions**

Your application runs as a background service or daemon without a signed-in user.

- The following permissions must be added '**AuditLog.Read.All**'. '**Reports.Read.All**' is optional for a future update/release.

### Select permissions

[expand all](#)

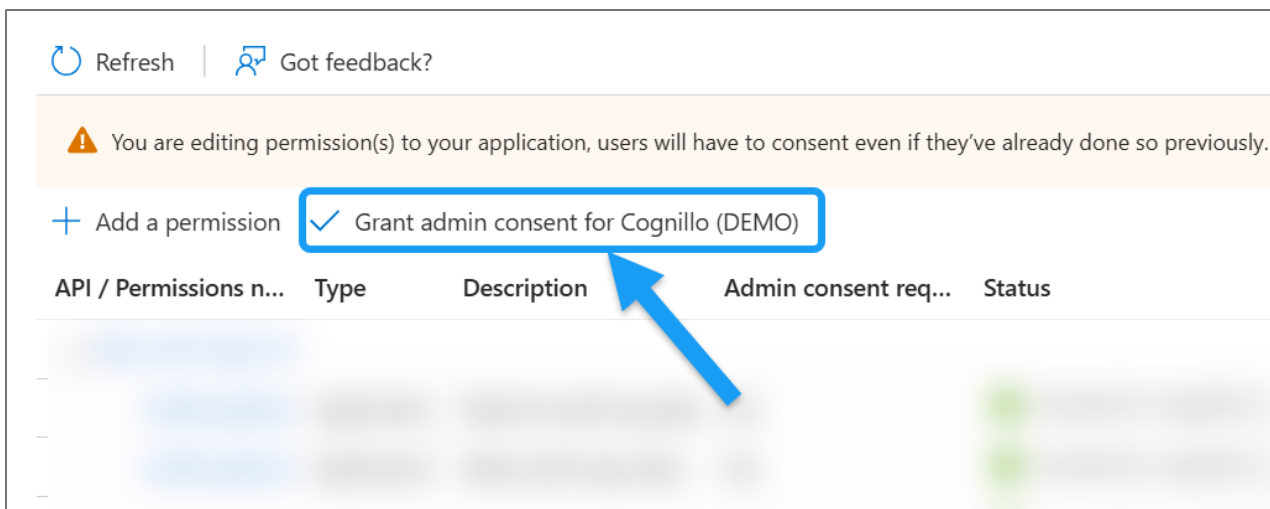
| Permission                                                                                                                                           | Admin consent required |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| AuditLog (1) <div> <input checked="" type="checkbox"/> <div> <b>AuditLog.Read.All</b> ⓘ<br/>           Read all audit log data         </div> </div> | Yes                    |

- Click '**Add permissions**'

Add permissions

Discard

- Finally, click '**Grant admin consent for <tenant name>**'



## (Medium Effort) Manual Registration using PowerShell

Two scripts in the toolkit download (folder Optional) do the Azure setup from the command line. They are the alternative to the in-app wizard for admins who prefer scripts, who need to run the setup from a machine without the toolkit installed, or whose tenant policy requires their own sign-in app.

| Script                       | Web Browser sign-in uses                                                                                                                 | Choose it when                                                                                   |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Setup-SPEAzure-SharedApp.ps1 | <b>Cognillo's shared app (multi-tenant).</b> One consent click; nothing is created in your tenant for sign-in except the consent record. | Most organizations. Same result as the in-app wizard.                                            |
| Setup-SPEAzure-OwnApp.ps1    | <b>Your own app registration (single tenant),</b> created by the script.                                                                 | Your organization requires its own registration, or wants to control the permission list itself. |

Both scripts also create the User Activity app registration (SharePoint Essentials Toolkit - User Activity) with a certificate and Office 365 Management APIs › ActivityFeed.Read, which the User Activity reports and Monitoring read from.

---

**NOTE: Prefer not to use PowerShell?** The in-app wizard (Home › Set up Azure app registration) does everything the SharedApp script does and also writes the connections for you. See "Fully Automated using app wizard" above.

---

### What You Need

- A **Global Administrator account** for the tenant.
- Windows 10/11 with PowerShell 5.1 or 7. No local admin rights. The script installs the Microsoft Graph PowerShell modules for the current user if they are missing.

- Internet access to PowerShell Gallery (for the modules) and to Microsoft Entra.
- SharePoint Online. The scripts do not apply to SharePoint on-premises.

**Time:** about ten minutes.

### *Step 1: Get the script*

The scripts are in the Optional folder of the toolkit download zip. Copy the one you chose to a local folder.

### *Step 2: Run it*

Open PowerShell (not as administrator; it is not needed), change to the folder and run:

Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy RemoteSigned # once, only if scripts are blocked

Unblock-File .\Setup-SPEAzure-SharedApp.ps1

.\Setup-SPEAzure-SharedApp.ps1

For your own sign-in app, use Setup-SPEAzure-OwnApp.ps1 in place of the SharedApp script in all three lines.

### *Step 3: Answer the prompts*

1. **Tenant.** Type your tenant domain (for example contoso.onmicrosoft.com) or tenant ID, or press Enter to pick the tenant at sign-in.
2. **Certificate password.** Choose a password for the .pfx file. You will type this same password into the toolkit later; keep it somewhere safe.
3. **Sign in.** A browser window opens. Sign in as the Global Administrator and accept the permissions the script asks for (they let it create app registrations and grant consent, and apply to your account only).

The script then:

- creates (or updates in place) the User Activity app registration,
- generates a self-signed certificate, uploads it, and saves the .pfx and .cer,
- adds ActivityFeed.Read and grants admin consent,
- **SharedApp:** opens the consent page for Cognillo's shared app in the browser. Sign in, tick **Consent on behalf of your organization** if shown, click Accept, then return to PowerShell and press Enter. The script verifies the consent was recorded.
- **OwnApp:** creates the SharePoint Essentials Toolkit sign-in app with the delegated permissions the toolkit uses and grants admin consent for it (if the automatic grant fails, it opens the consent page instead).

### *Step 4: Keep the summary file*

When it finishes, the script opens a text file named SharePoint Essentials Toolkit - Azure setup <date>.txt and saves it, together with the certificate files, in:

Documents\SharePoint Essentials Toolkit\Certificates

It contains your **Tenant ID**, the **App (client) ID** of each app the script created, the **.pfx path**, and the consent links. Everything you type into the toolkit in the next step is in this file.

#### *Step 5: Add the User Activity connection in the toolkit*

1. Open SharePoint Essentials Toolkit › Connections › New connection.
2. **Use it for:** Microsoft 365 user activity.
3. **Root site:** https://<tenant>.sharepoint.com (not the -admin address).
4. **Certificate:** browse to the .pfx from the summary file and enter its password.
5. **App (client) ID:** paste the ID of the User Activity app from the summary file. **Tenant ID:** paste from the summary file.
6. **Advanced › Cloud:** leave Azure Public Cloud unless your tenant is GCC High, DoD or 21Vianet.
7. Click **Test and save**.

The test signs in with the certificate. Admin consent can take a few minutes to apply; if the test reports no permissions yet, wait and test again.

#### *Step 6: Add the SharePoint connection (if you do not have one yet)*

**Connections › New connection › SharePoint sites & content › How to sign in: Web Browser › Advanced › Use an Azure app registration: On**, then:

- **SharedApp script: Register automatically with Cognillo's shared app = On.** The **Tenant ID** fills in automatically.
- **OwnApp script: Register automatically with Cognillo's shared app = Off.** Paste the **App (client) ID** of the SharePoint Essentials Toolkit sign-in app (not the User Activity one) and the **Tenant ID** from the summary file.

Click **Test and save**. Leave this connection as the **Default**; reports and fixes run through it.

#### *What was Created*

##### **In Microsoft Entra**

| Script    | App registrations                                                               | Enterprise applications                                                                                                                                                                        |
|-----------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SharedApp | SharePoint Essentials Toolkit - User Activity                                   | The same, plus SharePoint Essentials Toolkit (Cognillo's shared app; its consent record lives here. It does not appear under App registrations because it is registered in Cognillo's tenant.) |
| OwnApp    | SharePoint Essentials Toolkit and SharePoint Essentials Toolkit - User Activity | The same two                                                                                                                                                                                   |

The User Activity app has one certificate and one application permission, ActivityFeed.Read, admin-consented. The OwnApp sign-in app has delegated permissions only (SharePoint: AllSites.FullControl, Sites.Search.All, TermStore.Read.All, User.Read.All; Graph: User.Read, Directory.Read.All, Group.Read.All, Sites.Read.All, Files.ReadWrite.All, InformationProtectionPolicy.Read, Mail.Send, Mail.Send.Shared). Delegated means the toolkit can only ever do what the signed-in person can do.

### On the computer that ran the script

.pfx, .cer and the summary file in Documents\SharePoint Essentials Toolkit\Certificates. The certificate is valid for two years by default.

### Script Options

Both scripts accept the same options unless noted.

| Option                                           | Use when                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -TenantId, -CertificatePassword                  | Skip the prompts, for unattended runs.<br>Example: -CertificatePassword (Read-Host - AsSecureString)                                                                                                                                                                                                    |
| -UserActivityAppName and, OwnApp only, - AppName | Use different display names, or point at existing apps to update them in place.                                                                                                                                                                                                                         |
| -OutputFolder                                    | Write the certificate and summary somewhere other than Documents.                                                                                                                                                                                                                                       |
| -CertificateYearsValid                           | 1 to 10 years. Default 2.                                                                                                                                                                                                                                                                               |
| -IncludeCertificateSharePointAccess              | Also give the User Activity certificate app-only access to SharePoint (Sites.FullControl.All and related), for a certificate-based SharePoint sites & content connection or scheduled jobs that run without a signed-in user. Anyone holding the .pfx and password gets that access; keep them private. |
| -SkipAdminConsent                                | You are not a Global Administrator. The script configures everything it can; send the consent link(s) from the summary file to an admin.                                                                                                                                                                |

Re-running a script with the same app names updates the apps in place and adds a new certificate alongside the existing ones. Nothing is deleted.

### Troubleshooting

| Symptom                                    | What to do                                                                                                                                                                |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "Insufficient privileges" or consent fails | Sign in as a Global Administrator. Or run with - SkipAdminConsent and have an admin open the consent link(s) from the summary file.                                       |
| Module install fails                       | The machine cannot reach PowerShell Gallery. Install the modules on a connected machine with Install-Module Microsoft.Graph.Authentication, Microsoft.Graph.Applications, |

| <b>Symptom</b>                                       | <b>What to do</b>                                                                                                                                                                                                         |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                      | <i>Microsoft.Graph.Identity.SignIns -Scope CurrentUser, or run the in-app wizard instead.</i>                                                                                                                             |
| <i>"More than one app registration is named ..."</i> | <i>Rename or delete the duplicates in Microsoft Entra, or pass a different -UserActivityAppName / -AppName.</i>                                                                                                           |
| <i>Connection test fails with 401 or 403</i>         | <i>In Entra › App registrations › SharePoint Essentials Toolkit - User Activity › API permissions, confirm ActivityFeed.Read (Application) shows Granted for &lt;tenant&gt;. Consent can take a few minutes.</i>          |
| <i>Wrong App ID</i>                                  | <i>The User Activity connection needs the User Activity app's ID. The SharePoint connection uses the shared app (automatic) or, for OwnApp, the SharePoint Essentials Toolkit app's ID. Both are in the summary file.</i> |
| <i>No activity data</i>                              | <i>Audit logging must be on in Microsoft Purview, and events appear with a delay of up to 24 hours. Users only see activity for sites where they have at least Read access.</i>                                           |
| <i>Certificate expired</i>                           | <i>Re-run the same script. It adds a new certificate to the same app; update the .pfx and password on the connection.</i>                                                                                                 |

Prefer to click through the Azure portal by hand? See "Manual Registration using Azure Portal" above.

## Updating an Existing Azure App Registration for New Features

Customers using their own Azure App Registration must update any missing permissions and grant admin consent for new features to become available.

The Azure App Registration PowerShell script Setup-SPEAzure-OwnApp.ps1 (which replaces our old deprecated AzureAppRegistrationModernAuth.ps1) can be re-run against an existing app registration to update its permissions in place; it finds the app by name and does not create a duplicate. Use -AppName if your app registration is not named SharePoint Essentials Toolkit. It adds the following Microsoft Graph delegated permissions:

- **Mail.Send and Mail.Send.Shared** – send job alert email as the signed-in user or from a shared mailbox.
- **Files.ReadWrite.All** – apply or remove sensitivity labels on selected files and send selected files to Microsoft 365 Archive.
- **InformationProtectionPolicy.Read** – list the sensitivity labels available to the signed-in user.

Directory (people picker) search uses the Directory.Read.All and Group.Read.All Graph permissions the script has always granted; no change is needed for it. If you maintain the registration by hand, User.Read.All plus Group.Read.All also suffices.

The script grants admin consent when run as a Global Administrator, and opens the consent page if it cannot; if run with -SkipAdminConsent, grant consent afterwards. If consent is not granted, the affected actions report a permission error on the items they were run against and the remainder of the toolkit continues to work; directory search falls back to the SharePoint people picker.

### Notes for the new item actions:

- These actions run through Microsoft Graph and are only available on connections that have Azure App Registration enabled.
- Sensitivity label actions operate on the files you tick in a report (Content Search or Item Inventory). “Remove the label” strips the label from those selected files only; there is no tenant-wide label removal.
- Applying or removing a sensitivity label is a metered Graph API: the app registration must be linked to an Azure subscription with “Metered APIs and services in Microsoft Graph” enabled, otherwise the action fails with a payment-required error.
- Send to Microsoft 365 Archive requires Microsoft 365 Archive enabled in the SharePoint admin center and a pay-as-you-go billing policy connected in the Microsoft 365 admin center.
- Certificate (app-only) connections need the application-permission equivalents (Sites.ReadWrite.All and InformationProtectionPolicy.Read.All). Setup-SPEAzure-OwnApp.ps1 configures delegated permissions for sign-in; its -IncludeCertificateSharePointAccess switch adds app-only Sites.FullControl.All and Files.ReadWrite.All to the User Activity certificate app, but InformationProtectionPolicy.Read.All must be added manually.

## API Permissions for CERTIFICATE Based Authentication (without User Activity Services)

| API / Permissions name                               | Type        | Description                                            | Admin consent req... | Status                       |
|------------------------------------------------------|-------------|--------------------------------------------------------|----------------------|------------------------------|
| <a href="#">Microsoft Graph (6)</a>                  |             |                                                        |                      |                              |
| <a href="#">Directory.Read.All</a>                   | Application | Read directory data                                    | Yes                  | ✔ Granted for Cognillo (D... |
| <a href="#">Files.ReadWrite.All</a>                  | Application | Read and write files in all site collections           | Yes                  | ✔ Granted for Cognillo (D... |
| <a href="#">Group.Read.All</a>                       | Application | Read all groups                                        | Yes                  | ✔ Granted for Cognillo (D... |
| <a href="#">InformationProtectionPolicy.Read.All</a> | Application | Read all published labels and label policies for an... | Yes                  | ✔ Granted for Cognillo (D... |
| <a href="#">Sites.Read.All</a>                       | Application | Read items in all site collections                     | Yes                  | ✔ Granted for Cognillo (D... |
| <a href="#">User.Read.All</a>                        | Application | Read all users' full profiles                          | Yes                  | ✔ Granted for Cognillo (D... |
| <a href="#">SharePoint (3)</a>                       |             |                                                        |                      |                              |
| <a href="#">Sites.FullControl.All</a>                | Application | Have full control of all site collections              | Yes                  | ✔ Granted for Cognillo (D... |
| <a href="#">TermStore.Read.All</a>                   | Application | Read managed metadata                                  | Yes                  | ✔ Granted for Cognillo (D... |
| <a href="#">User.Read.All</a>                        | Application | Read user profiles                                     | Yes                  | ✔ Granted for Cognillo (D... |

## API Permissions for DELEGATED Authentication (without User Activity Services)

| API / Permissions name           | Type      | Description                                      | Admin consent req... | Status                       |
|----------------------------------|-----------|--------------------------------------------------|----------------------|------------------------------|
| ▼ Microsoft Graph (8)            |           |                                                  |                      |                              |
| Directory.Read.All               | Delegated | Read directory data                              | Yes                  | ✔ Granted for Cognillo (D... |
| Files.ReadWrite.All              | Delegated | Have full access to all files user can access    | No                   | ✔ Granted for Cognillo (D... |
| Group.Read.All                   | Delegated | Read all groups                                  | Yes                  | ✔ Granted for Cognillo (D... |
| InformationProtectionPolicy.Read | Delegated | Read user sensitivity labels and label policies. | No                   | ✔ Granted for Cognillo (D... |
| Mail.Send                        | Delegated | Send mail as a user                              | No                   | ✔ Granted for Cognillo (D... |
| Mail.Send.Shared                 | Delegated | Send mail on behalf of others                    | No                   | ✔ Granted for Cognillo (D... |
| Sites.Read.All                   | Delegated | Read items in all site collections               | No                   | ✔ Granted for Cognillo (D... |
| User.Read                        | Delegated | Sign in and read user profile                    | No                   | ✔ Granted for Cognillo (D... |
| ▼ SharePoint (3)                 |           |                                                  |                      |                              |
| AllSites.FullControl             | Delegated | Have full control of all site collections        | Yes                  | ✔ Granted for Cognillo (D... |
| TermStore.Read.All               | Delegated | Read managed metadata                            | Yes                  | ✔ Granted for Cognillo (D... |
| User.Read.All                    | Delegated | Read user profiles                               | Yes                  | ✔ Granted for Cognillo (D... |

## API Permissions for USER ACTIVITY App Registration (CERTIFICATE)

| <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 include all the permissions the application needs. <a href="#">Learn more about permissions and consent</a></p> <p>+ Add a permission    ✓ Grant admin consent for Cognillo (DEMO)</p> |             |                                          |                        |         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------------|------------------------|---------|
| API / Permissions name                                                                                                                                                                                                                                                                                                                                                                | Type        | Description                              | Admin consent required | Status  |
| <p>Office 365 Management APIs (1)</p>                                                                                                                                                                                                                                                                                                                                                 |             |                                          |                        |         |
| ActivityFeed.Read                                                                                                                                                                                                                                                                                                                                                                     | Application | Read activity data for your organization | Yes                    | ✓ Grant |

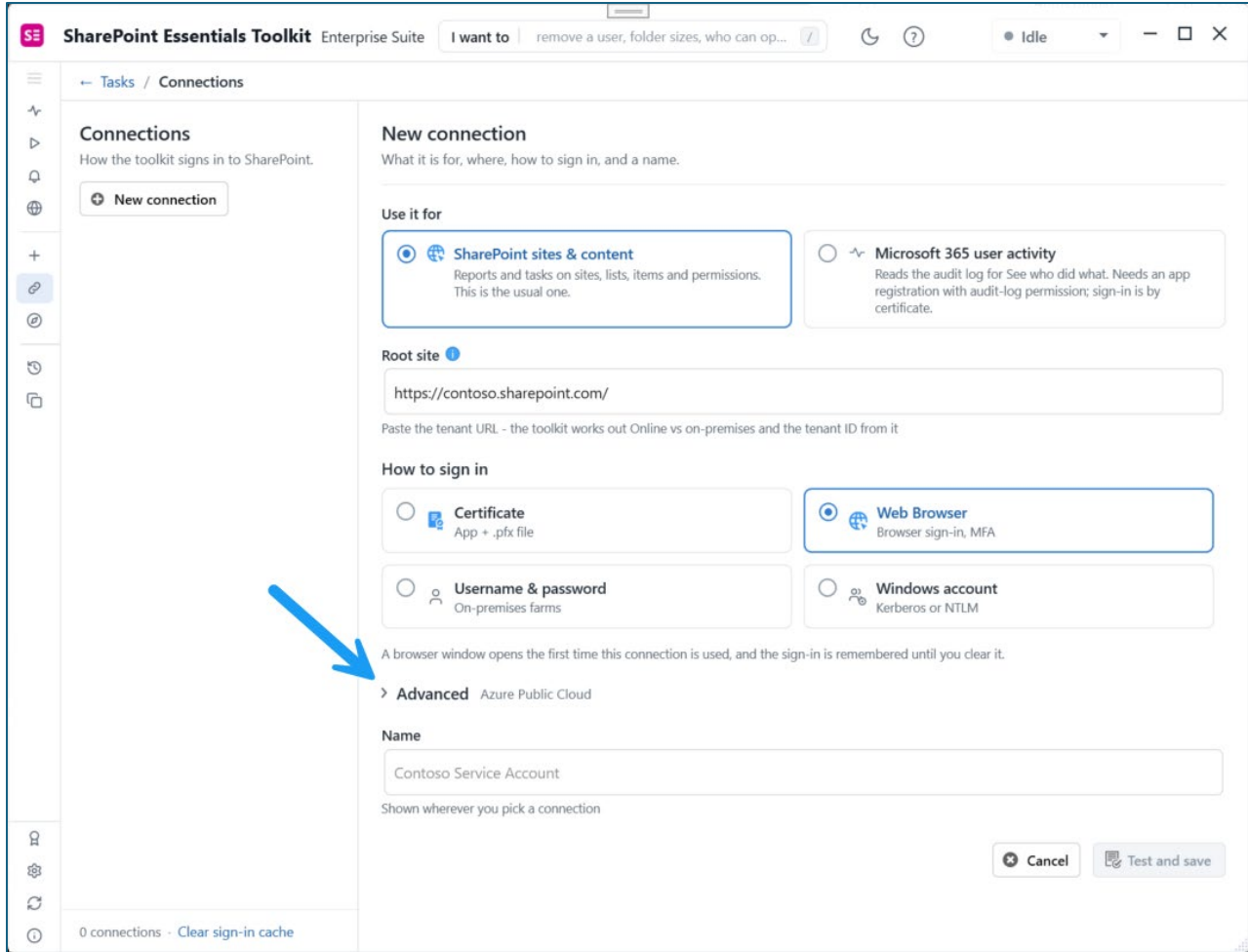
Optionally add AuditLog.Read.All, Reports.Read.All permissions for future release

| <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 include all the permissions the application needs. <a href="#">Learn more about permissions and consent</a></p> <p>+ Add a permission    ✓ Grant admin consent for Cognillo (DEMO)</p> |             |                                          |                        |         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------------|------------------------|---------|
| API / Permissions name                                                                                                                                                                                                                                                                                                                                                                | Type        | Description                              | Admin consent required | Status  |
| <p>Microsoft Graph (2)</p>                                                                                                                                                                                                                                                                                                                                                            |             |                                          |                        |         |
| AuditLog.Read.All                                                                                                                                                                                                                                                                                                                                                                     | Application | Read all audit log data                  | Yes                    | ✓ Grant |
| Reports.Read.All                                                                                                                                                                                                                                                                                                                                                                      | Application | Read all usage reports                   | Yes                    | ✓ Grant |
| <p>Office 365 Management APIs (1)</p>                                                                                                                                                                                                                                                                                                                                                 |             |                                          |                        |         |
| ActivityFeed.Read                                                                                                                                                                                                                                                                                                                                                                     | Application | Read activity data for your organization | Yes                    | ✓ Grant |

## Configure Web Browser Authentication (WBA) to use Azure App Registration in SharePoint Essentials Toolkit

Now that the API permissions are configured in Azure, we can now set up a connection in the SharePoint Essentials Toolkit that will use Azure App registration.

1. In SharePoint Essentials Toolkit, click Connections in the left navigation.



**SharePoint Essentials Toolkit** Enterprise Suite

I want to: remove a user, folder sizes, who can op...

Idle

Tasks / Connections

**Connections**  
How the toolkit signs in to SharePoint.

[New connection](#)

**New connection**  
What it is for, where, how to sign in, and a name.

**Use it for**

- ☒ **SharePoint sites & content**  
Reports and tasks on sites, lists, items and permissions. This is the usual one.
- ☐ **Microsoft 365 user activity**  
Reads the audit log for See who did what. Needs an app registration with audit-log permission; sign-in is by certificate.

**Root site**

Paste the tenant URL - the toolkit works out Online vs on-premises and the tenant ID from it

**How to sign in**

- ☐ **Certificate**  
App + .pfx file
- ☒ **Web Browser**  
Browser sign-in, MFA
- ☐ **Username & password**  
On-premises farms
- ☐ **Windows account**  
Kerberos or NTLM

A browser window opens the first time this connection is used, and the sign-in is remembered until you clear it.

**> Advanced** Azure Public Cloud

**Name**

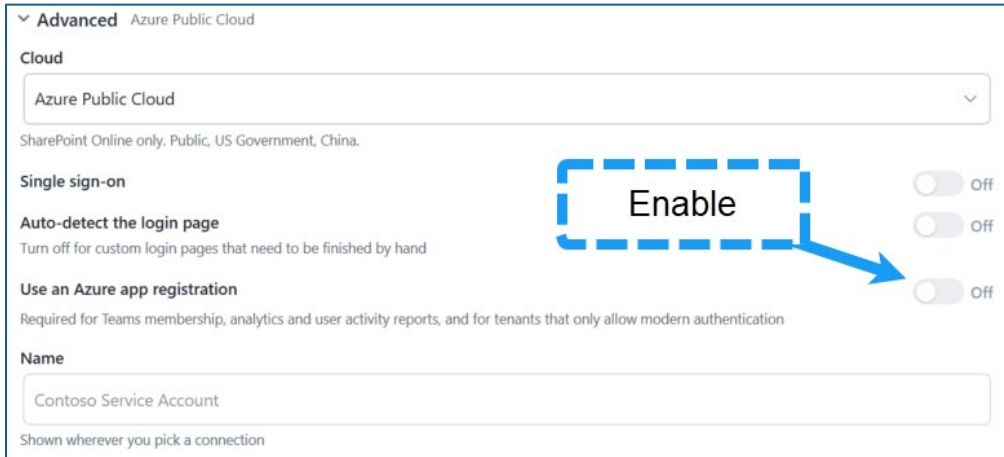
Shown wherever you pick a connection

[Cancel](#) [Test and save](#)

0 connections - [Clear sign-in cache](#)

- Set **"Use it for"** to **"SharePoint sites & content"**
- Enter the SharePoint **"Root Site"**.
  - For SharePoint Online, use the tenant url (ex. https://mycompany.sharepoint.com).
  - Do not use the admin site url (ex. https://mycompany-admin.sharepoint.com).
- For **"How to sign in"**, choose **"Web Browser"**, this is the default.
- Enter a **"Name"**. For example, 'Production Service Account'.
- Click **'Advanced'** to expand the App Registration options.
- For **"Cloud"** (Azure Authority Host), choose Azure Public Cloud or the appropriate cloud for your organization

8. Enable “Use Azure App Registration”.



Advanced Azure Public Cloud

Cloud

Azure Public Cloud

SharePoint Online only. Public, US Government, China.

Single sign-on

Auto-detect the login page

Turn off for custom login pages that need to be finished by hand

Use an Azure app registration

Required for Teams membership, analytics and user activity reports, and for tenants that only allow modern authentication

Name

Contoso Service Account

Shown wherever you pick a connection

Enable

## Fully Automated – using app Wizard

No steps needed.

## [Partially Automated](#) - Multitenant Setup – using URL

If using multitenant setup (you used the link to automatically configure app-registration), use the setting below:

▼ **Advanced** Azure Public Cloud

**Cloud**

Azure Public Cloud

SharePoint Online only

**Single sign-on**

**Auto-detect the login URL**

Turn off for custom login pages that need to be finished by hand

**Use an Azure app registration**

Required for Teams membership, analytics and user activity reports, and for tenants that only allow modern authentication

**Register automatically with Cognillo's shared app**

Turn off to use an app registered in your own tenant

**App (client) ID**

2c88dfed-4cde-4c8d-bb6f-5fc7b75f16f6

Cognillo's multi-tenant app. Consent is granted once per tenant.

**Tenant ID**

00000000-0000-0000-0000-000000000000

Filled in from the root site when possible

**Name**

Production Service Account

Shown wherever you pick a connection

Use this option when using the URL to perform App Registration

Copy consent URL / more info

Shared multitenant App Id

## Manual Setup - Single Tenant Setup

Once the app has been registered, we need to get the Azure App Id and Tenant Id from Azure.

## Get Tenant Id and Application Id from Azure Portal using a Web Browser

1. In the Azure Portal, navigate to the App Registration created above.
2. Copy the Application (client) ID and Directory (tenant) ID as shown below.

Home > App registrations > SharePoint Essentials Toolkit | API permissions > App registrations >

## SharePoint Essentials Toolkit

Search << Delete Endpoints Preview features

**Overview**

- Quickstart
- Integration assistant
- Diagnose and solve problems

**Manage**

- Branding & properties
- Authentication
- Certificates & secrets

**Essentials**

Display name  
[SharePoint Essentials Toolkit](#)

Application (client) ID  
[Redacted]

Object ID  
b3532696-e84a-47ab-aed1-08f2af5af1fb

Directory (tenant) ID  
[Redacted]

Supported account types  
[My organization only](#)

Client credentials  
[1 certificate, 0 secret](#)

Redirect URIs  
[0 web, 0 spa, 1 public client](#)

Application ID URI  
[Add an Application ID URI](#)

Managed application in local directory  
[SharePoint Essentials Toolkit](#)

Enter the Enterprise App Id and Tenant Id for your SharePoint Online App Registration

Advanced Azure Public Cloud

Cloud  
Azure Public Cloud

SharePoint Online only. Public, US Government, China.

Single sign-on

Auto-detect the login page  
Turn off for custom login pages that need to be finished by hand

Use an Azure app registration  
Required for Teams membership, analytics and user activity reports, and for tenants that only allow modern authentication

Register automatically with Cognillo's shared app  
Turn off to use an app registered in your own tenant

App (client) ID  
00000000-0000-0000-0000-000000000000

Tenant ID  
00000000-0000-0000-0000-000000000000

From the app registration in Entra

Filled in from the root site when possible

Name  
Production Service Account

Shown wherever you pick a connection

Set to off

## Test the Connection

Use the **“Test Login”** button to test the connection.

▼ Advanced Azure Public Cloud

Cloud

Azure Public Cloud

SharePoint Online only, Public, US Government, China.

Single sign-on

Off

Auto-detect the login page

Off

Turn off for custom login pages that need to be finished by hand

Use an Azure app registration

On

Required for Teams membership, analytics and user activity reports, and for tenants that only allow modern authentication

Register automatically with Cognillo's shared app

Off

Turn off to use an app registered in your own tenant

App (client) ID

Tenant ID

From the app registration in Entra

Filled in from the root site when possible

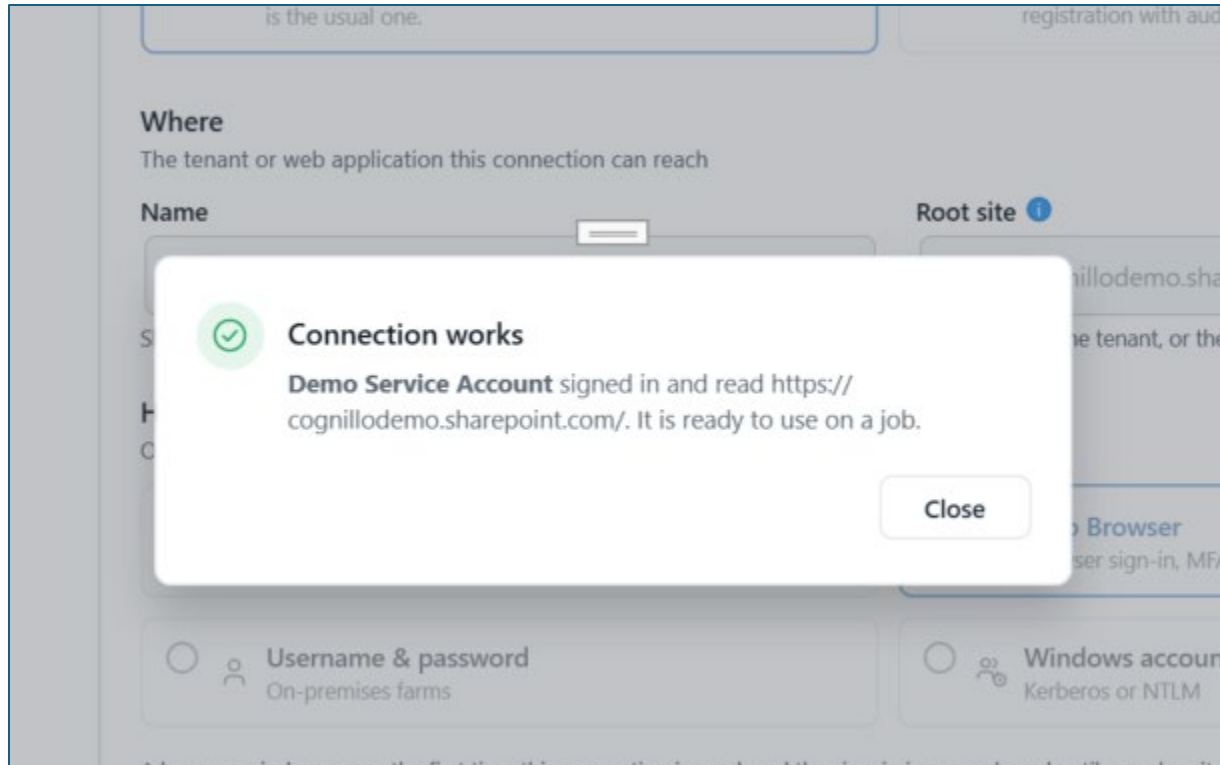
Name

Demo Service Account

Shown wherever you pick a connection

Cancel

Test and save



## Certificate based Authentication

### What is Azure App Registration Certificate-Based Authentication?

Certificate-based authentication with Azure App Registration allows applications to securely authenticate to Azure services—such as SharePoint Online and Azure audit logs—without needing user prompts for credentials. Instead of usernames and passwords, a digital certificate is used to verify the application's identity, streamlining automated access to Azure services that are need by the SharePoint Essentials Toolkit.

### Benefits of setting up Certificate based authentication

- Avoid issues with scheduled jobs.
  - Scheduled jobs may have issues where a security token for a user may expire due to Azure token policies.
- Allows the use of Governance & User Activity features.
  - The Governance and User Activity features in the SharePoint Essentials Toolkit require a certificate to be added to the registered application. This is needed to support connect to Azure services to retrieve audit log data.
- Avoid security prompts.
  - Using certificate-based authentication will cause the SharePoint Essentials Toolkit to authenticate through the certificate and avoid users from having to type credentials into the tool when they need to access SharePoint or Azure resources for reports.
- Change or deny access in one location
  - Denying access to SharePoint Essentials Toolkit can be done from a single location in the Azure App registration section by removing the certificate or changing the certificate password.

### Drawbacks of Certificate based authentication

- Additional configuration and management
  - Additional steps are required to configure Azure certificate authentication for the SharePoint Essentials Toolkit.
  - Certificates can be lost if they are shared with users. Cognillo is working on adding support for the Azure Key Vault to reduce this management overhead.
- Unintentionally giving too much access
  - Users who have the certificate configured for certificate-based authentication will have access to all resources that the application has access to. If the user does not have access to a certain SharePoint site, but the application has access to it, the user will be able to run reports and perform tasks that their user account may not have access to.
  - NOTE: Users will not be able to interactively log into SharePoint using the SharePoint Essentials Toolkit application certificate.

## Using the Azure Key Vault

Azure key vault support is coming soon. This will allow an Azure Key Vault to be used to store certificates.

## Configure Certificate based authentication

To enable application-level authentication, follow the steps below:

### Create the certificate

You can use a 3<sup>rd</sup> party certificate or create a self-signed certificate.

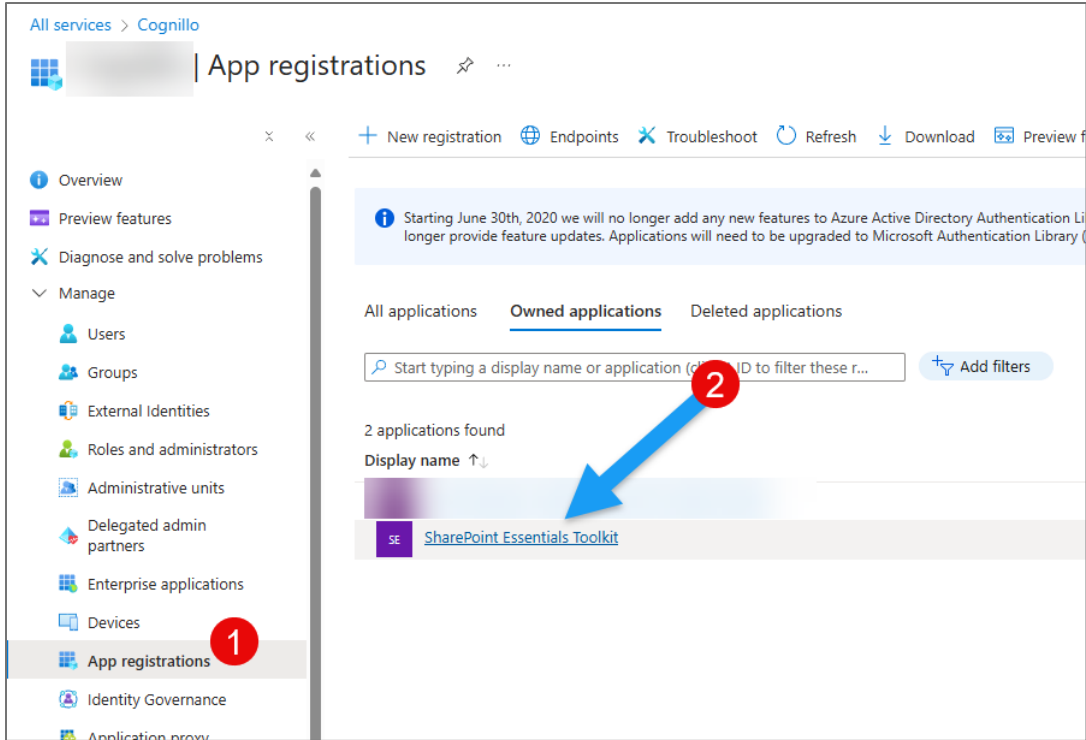
Cognillo has provided a script you may use to create a self-signed certificate; this is not recommended for production environments but is suitable for testing. You can download the script [here](#).

### *Using the self-signed certificate script*

1. Download the script using link above.
2. Open the file 'New-SelfSignedCertificate.txt' to get the commands to paste.
3. Modify the values as needed in the text file, such as the path to the downloaded ps1 script.
4. Run Windows PowerShell from your machine as an Administrator.
5. Use CD command to navigate to the correct directory of the script, such as:  
`cd "C:\SPE2025 script\"`
6. Paste the last command from the text file, example:  
`.\Create-SelfSignedCertificate.ps1 -CommonName "Cognillo" -StartDate 2024-01-01 -  
EndDate 2030-01-01`
7. This will generate a certificate file in the same folder as the script.

## Upload the certificate to Azure

1. Navigate to the Azure Entra ID portal
2. Click 'App Registrations' and select the application registered in [steps above](#).



All services > Cognillo

App registrations

Overview  
Preview features  
Diagnose and solve problems  
Manage  
Users  
Groups  
External Identities  
Roles and administrators  
Administrative units  
Delegated admin partners  
Enterprise applications  
Devices  
App registrations  
Identity Governance  
Application proxy

+ New registration | Endpoints | Troubleshoot | Refresh | Download | Preview

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL).

All applications | **Owned applications** | Deleted applications

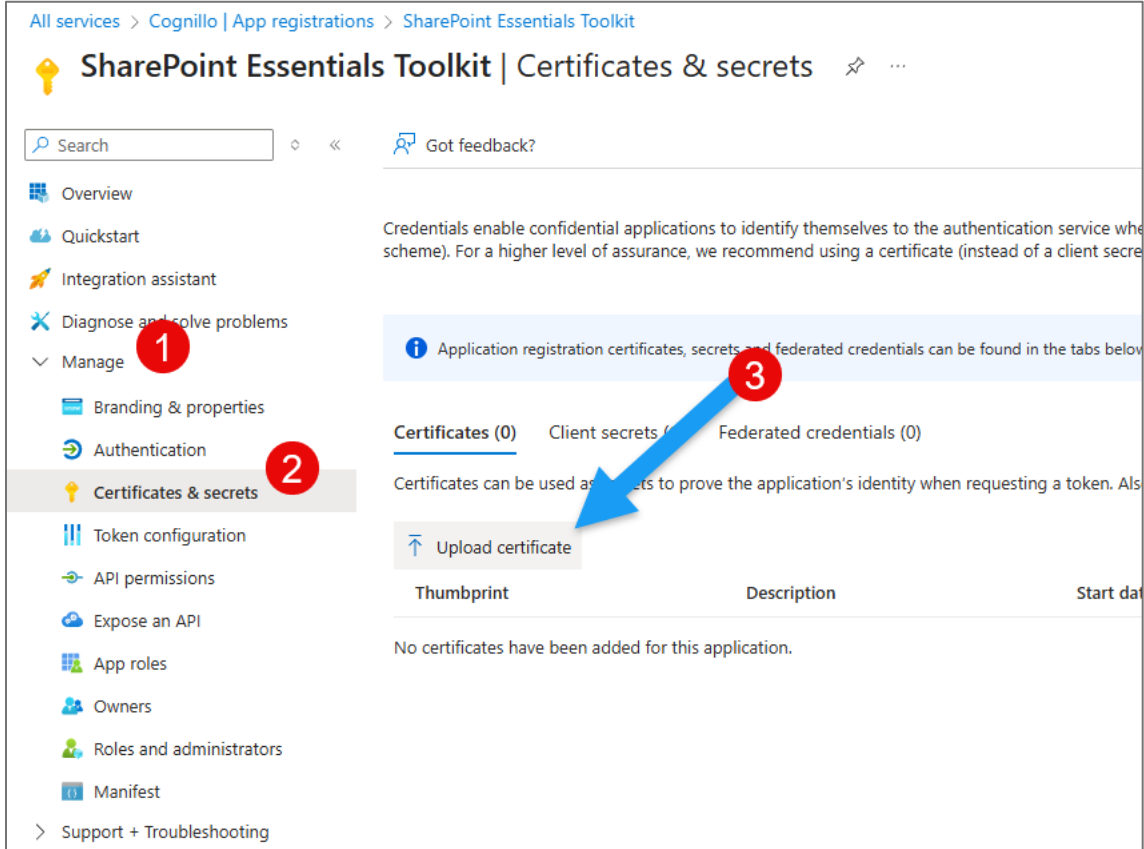
Start typing a display name or application (client ID) to filter these results

2 applications found

Display name ↑↓

SE SharePoint Essentials Toolkit

3. Expand the 'Manage' section and click upload certificate.



All services > Cognillo | App registrations > SharePoint Essentials Toolkit

SharePoint Essentials Toolkit | Certificates & secrets

Search

Got feedback?

Overview  
Quickstart  
Integration assistant  
Diagnose and solve problems  
Manage  
Branding & properties  
Authentication  
**Certificates & secrets**  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners  
Roles and administrators  
Manifest  
Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when using a confidential client (instead of a public client). For a higher level of assurance, we recommend using a certificate (instead of a client secret).

Application registration certificates, secrets and federated credentials can be found in the tabs below

**Certificates (0)** | Client secrets (0) | Federated credentials (0)

Certificates can be used as credentials to prove the application's identity when requesting a token. Also, they can be used to sign the application's manifest.

Upload certificate

| Thumbprint                                            | Description | Start date |
|-------------------------------------------------------|-------------|------------|
| No certificates have been added for this application. |             |            |

4. Upload the certificate and click 'Add'

### Upload certificate

Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt \*



Description

5. Verify the certificate is listed:

## SharePoint Essentials Toolkit | Certificates & secrets

[Got feedback?](#)

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets**
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

**Certificates (1)** Client secrets (0) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

[Upload certificate](#)

| Thumbprint               | Description | Start date | Expires    | Certificate ID                                                                                                                                                                                 |
|--------------------------|-------------|------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1B887A3D6447AB50C982C... | CN=Cognillo | 12/31/2023 | 12/31/2029 | 8827e56a-ec31-4...   |

6. Click 'API Permissions'
7. Add the API permissions needed for the SharePoint Essentials Toolkit as specified in this [section](#).

**IMPORTANT:** Ensure you use 'Application' and NOT 'Delegated' permissions when assigning API permissions.

# Setup Governance & User Activity Features

## Supported Environments

- SharePoint Online - National Public Cloud
- SharePoint Online - US Government L4
- SharePoint Online - US Government L5 (DOD)
- SharePoint Online - China operated by 21Vianet

## Unsupported Environments

- SharePoint On-premises

## Required Microsoft 365 licenses

The following Microsoft licenses are required

User Activity:

- Microsoft Purview Audit (Standard)
  - Microsoft 365 E3, A3, G3, and most Business plans (like Business Premium).
  - Allows up to 180 days of activity in reports.
- Microsoft Purview Audit (Premium)
  - Microsoft 365 E5, A5, G5, or a standalone compliance add-on for E3
  - Allows up to 1 year of activity in reports.

## Who can view User Activity?

The SharePoint Essentials Toolkit will not allow users to view activity data for SharePoint sites which they do not have at least READ permission level at the site level. The SharePoint Essentials Toolkit has built-in filtering (internally), to prevent users from viewing activity in sites which they do not have access to.

## Setup & Configuration

The Governance and User Activity feature requires Azure App Registration with certificate-based authentication.

### Pre-requisites

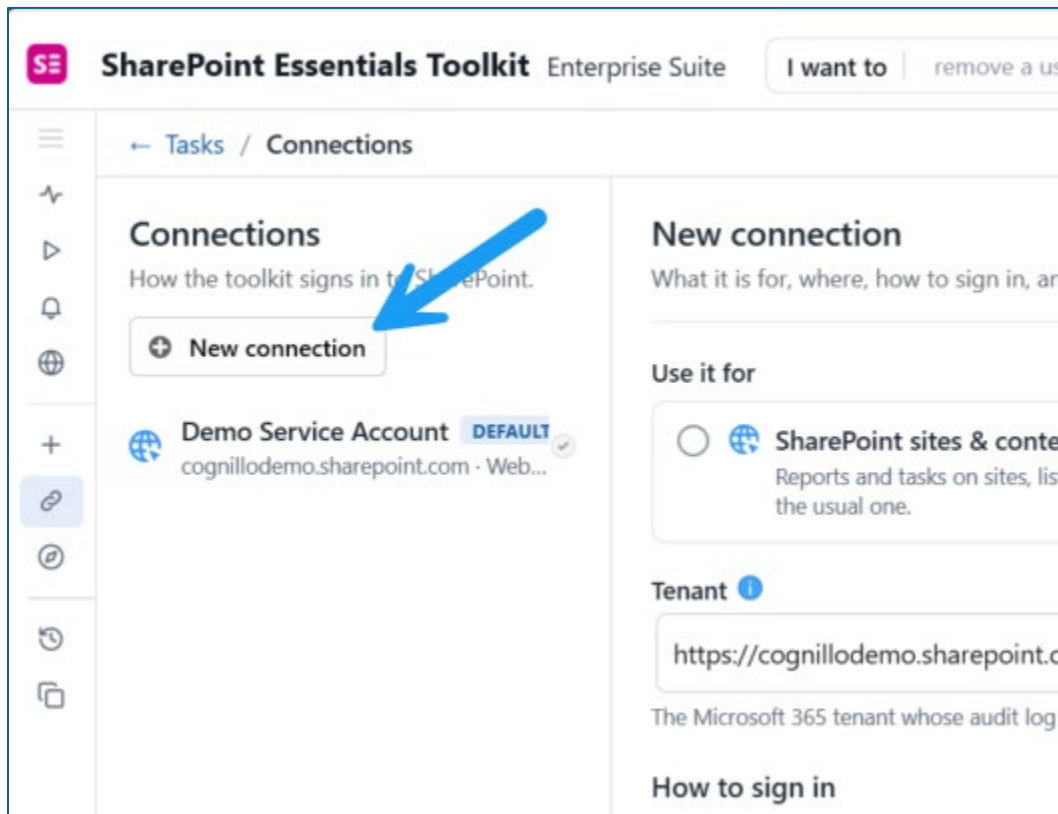
- A [certificate must be created](#) for the Azure Enterprise Application registered [above](#).
- API permissions must also be [configured](#) to use the Governance and User Activity features.

### Add the connection for the Governance and User Activity services:

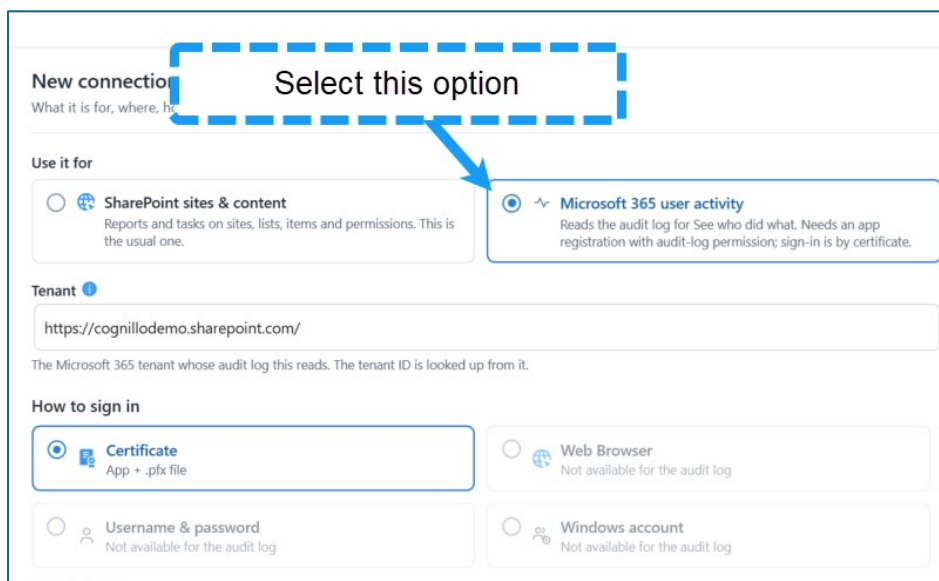
A Connection must be created in the tool (in My Connections), using the connection mode '**User Activity Services**'.

This connection will be in addition to any connection created for 'SharePoint Sites and Content'.

1. Open the SharePoint Essentials Toolkit
2. Click '**Connections**', then click '**New Connection**'



3. Enter a name for the profile, such as 'Governance and User Activity'
4. Select 'SharePoint User Activity Services'



5. Select the [certificate created](#) during Azure app registration.
6. Enter the Enterprise App Id and Tenant Id found from [this section](#)

**New connection**  
What it is for, where, how to sign in, and a name.

**Use it for**

☐  **SharePoint sites & content**  
Reports and tasks on sites, lists, items and permissions. This is the usual one.

☒  **Microsoft 365 user activity**  
Reads the audit log for See who did what. Needs an app registration with audit-log permission; sign-in is by certificate.

**Tenant** ⓘ

The Microsoft 365 tenant whose audit log this reads. The tenant ID is looked up from

**How to sign in**

☒  **Certificate**  
App + .pfx file

☐  **Username & password**  
Not available for the audit log

☐  **Not available for the audit log**

**Certificate file**

 **Browse...**

.pfx with private key

**Certificate password** Show

Encrypted and stored with this connection

**App (client) ID** **Tenant ID**

From the app registration in Entra Filled in from the root site when possible

> **Advanced** Azure Public Cloud

**Name**

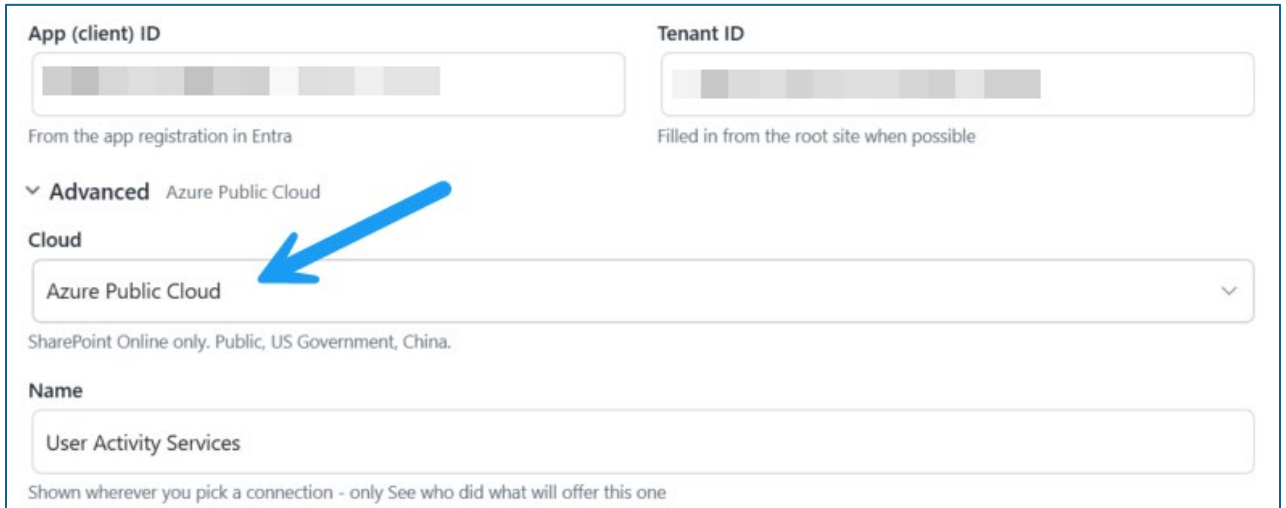
Shown wherever you pick a connection - only See who did what will offer this one

 **Cancel**  **Test and save**

7.

8. Advanced - Verify if you are using SharePoint Online public cloud (most common), or if your tenant is on a different provider such as US GCC High.

Click **'Save'**



The screenshot shows the 'Advanced' settings for 'User Activity Services'. The 'Cloud' dropdown is set to 'Azure Public Cloud', which is highlighted by a blue arrow. Below the dropdown, it says 'SharePoint Online only. Public, US Government, China.' The 'Name' field is set to 'User Activity Services'.

**App (client) ID**  
From the app registration in Entra

**Tenant ID**  
Filled in from the root site when possible

▼ **Advanced** Azure Public Cloud

**Cloud**  
Azure Public Cloud

SharePoint Online only. Public, US Government, China.

**Name**  
User Activity Services

Shown wherever you pick a connection - only See who did what will offer this one

Governance and User Activity services and features are now configured and ready to use.

## Scheduled Jobs

The SharePoint Essentials Toolkit schedules jobs through Microsoft Windows Task Scheduler.

To view details about using the Scheduler, see the [user guide](#).

## PowerShell Support

The SharePoint Essentials Toolkit supports PowerShell commands.

To view details about using the PowerShell commands with the SharePoint Essentials Toolkit, see the [user guide](#).

## Sensitivity Labels and Microsoft 365 Archive

This section covers what your tenant and the toolkit need for three features:

1. **Reading sensitivity labels in Item Inventory and Content Search reports** — no extra setup.
2. **Applying or removing sensitivity labels in bulk from a report** — needs your own app registration, a Certificate connection and a Microsoft Graph billing link.
3. **Sending files to Microsoft 365 Archive from a report** — needs Microsoft 365 Archive turned on in your tenant and your own app registration.

Each section lists requirements first, then the setup steps, then what to do when something goes wrong.

### Reading Sensitivity Labels in Reports

#### What it does

Item Inventory and Content Search reports show the sensitivity label on every file (**Sensitivity Label** and **Sensitivity Label Id** columns), the label on each site, and the default label on each library. Content filters can include or exclude items by label, so a report of "everything labelled Highly Confidential" is a filter, not a separate feature.

#### How it works

The toolkit reads the label from SharePoint itself through the standard SharePoint API, the same values the **Sensitivity** column shows in a library. Nothing is opened or decrypted, and Microsoft Graph is not involved.

#### Requirements

| Requirement      | Detail                                                     |
|------------------|------------------------------------------------------------|
| Connection type  | Any: Web Browser, Certificate, Username & password.        |
| Permissions      | Read access to the sites in the report. Nothing extra.     |
| App registration | Not required. Cognillo's shared app or your own both work. |
| Cost             | None.                                                      |

#### Good to know

- SharePoint fills the Sensitivity column a few seconds to a few minutes after a label is applied. A report run immediately after labelling may still show the old value; run it again.
- Files labelled on the desktop show their label once the file has synced back to SharePoint.
- Encrypted files report their label normally; the label is metadata, not content.

## Applying Sensitivity Labels in Bulk

### What it does

From an Item Inventory or Content Search report, tick files, open **Item Actions** (or **Search Result Actions**), choose **Add or change sensitivity label**, pick a label (or **Remove the label instead**), review, and apply. Each file is written individually and reported as succeeded or failed, with a change log in Job History and a **Retry failed** button.

### How it works

Each file is labelled through the Microsoft Graph `assignSensitivityLabel` API with the *privileged* assignment method (the equivalent of an administrator applying it) and a justification text for the audit log. Graph accepts the request immediately; SharePoint writes the label into the file in the background, normally within seconds. Audit events (`FileSensitivityLabelApplied`, `FileSensitivityLabelChanged`, `FileSensitivityLabelRemoved`) are logged by Microsoft Purview for every call.

**This API is metered by Microsoft.** Each call, successful or rejected, is billed to an Azure subscription you link to your app registration, currently **USD \$0.00185 per call** (10,000 files ≈ \$18.50). Current pricing: [Metered APIs and services in Microsoft Graph](#).

### Requirements

| Requirement                                                 | Detail                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Your own Azure app registration</b> in your tenant       | Cognillo's shared app cannot be used. Microsoft only lets an app be billed to a subscription in the tenant that owns the app.                                                                                                                                                                             |
| <b>Certificate sign-in</b> on the toolkit connection        | Microsoft only serves metered APIs to confidential clients. Web Browser and Username & password connections are public clients and are refused with <i>402 Payment Required</i> even when billing is linked.                                                                                              |
| <b>Application permissions</b> on the app (admin consented) | Microsoft Graph: <code>Files.ReadWrite.All</code> (or <code>Sites.ReadWrite.All</code> ) to label files; <code>InformationProtectionPolicy.Read.All</code> to list the tenant's labels. Plus whatever the connection already needs for reports, typically <code>SharePoint.Sites.FullControl.All</code> . |
| <b>Azure subscription</b> in the same tenant                | Any pay-as-you-go or EA subscription. It receives the metered charges.                                                                                                                                                                                                                                    |
| <b>Billing link</b> between app and subscription            | A <code>Microsoft.GraphServices/accounts</code> resource created with Azure CLI (steps below). One per app registration.                                                                                                                                                                                  |
| <b>Roles to do the setup</b>                                | Owner of the app registration, and Contributor on the subscription.                                                                                                                                                                                                                                       |
| <b>Supported files</b>                                      | .docx, .xlsx, .pptx and their macro/template variants. PDF after the tenant opts in (below). Not: SharePoint                                                                                                                                                                                              |

| Requirement             | Detail                                                                                        |
|-------------------------|-----------------------------------------------------------------------------------------------|
|                         | pages, 97-2003 Office formats (.doc, .xls, .ppt), images, text, OneNote, folders, list items. |
| <b>Supported clouds</b> | Microsoft global cloud only. Not GCC, GCC High, DoD or 21Vianet.                              |

## Step A — App registration

1. In the [Microsoft Entra admin center](#), **App registrations** → **New registration**. Name it e.g. SharePoint Essentials Toolkit (Certificate), single tenant, no redirect URL.
2. **Certificates & secrets** → **Certificates** → **Upload certificate**: upload the public .cer of the certificate whose .pfx the toolkit will use. (Create one with New-SelfSignedCertificate if you do not have one.)
3. **API permissions** → **Add a permission** → **Microsoft Graph** → **Application permissions**:
  - ☐ Files.ReadWrite.All (or Sites.ReadWrite.All)
  - ☐ InformationProtectionPolicy.Read.All
4. **Add a permission** → **SharePoint** → **Application permissions** → **Sites.FullControl.All** (so the same connection can run reports).
5. **Grant admin consent for <tenant>**. Every row must show a green tick.
6. From **Overview**, copy the **Application (client) ID** and **Directory (tenant) ID**.

## Step B — Link the app to an Azure subscription

Run in [Azure Cloud Shell](#) (PowerShell) or a local Azure CLI session, signed in to the same tenant. Replace the three placeholders.

```
$subscriptionId = "<Subscription ID>"
$appId          = "<Application (client) ID from Step A>"
$resourceGroup  = "rg-graph-metered-billing"          # any name

az account set --subscription $subscriptionId
az extension add --name graphservices --upgrade
az group create --name $resourceGroup --location eastus

az graph-services account create `
  --resource-group $resourceGroup `
  --resource-name "spe-toolkit-graph-billing" `
  --subscription $subscriptionId `
  --location global `
  --app-id $appId
```

A successful response includes "provisioningState": "Succeeded" and your app ID under properties.appId. Verify at any time with:

```
az graph-services account list --resource-group $resourceGroup `
```

```
--query "[].{name:name, appId:properties.appId, state:properties.provisioningState}"  
-o table
```

If the command answers *"The application was not found in this tenant"*, the subscription belongs to a different tenant than the app registration. Check with `az account show --query tenantId`.

## Step C — PDF support (optional)

PDF files are rejected until the tenant opts in. In SharePoint Online Management Shell, as SharePoint Administrator:

```
Connect-SPOService -Url https://<tenant>-admin.sharepoint.com  
Set-SPOTenant -EnableSensitivityLabelForPDF $true
```

Allow a few hours to take effect. Digitally signed PDFs are still rejected, because labelling would invalidate the signature.

## Step D — Toolkit connection

1. **Connections → New connection.** Root site: your tenant URL.
2. **How to sign in: Certificate.** Browse to the .pfx and enter its password.
3. Under **Advanced**, turn on **Use an Azure app registration**, turn **off** *Register automatically with Cognillo's shared app*, and enter the **App (client) ID** and **Tenant ID** from Step A.
4. **Test and save.**
5. Assign this connection to the sites you will label (Sites → edit → connection), or make it the default.

## Step E — Test with one file

1. Run an Item Inventory report on a library that holds a .docx.
2. Tick one file, choose **Add or change sensitivity label**, pick a label, **Review, Apply**.
3. The row shows *Labelled*. In SharePoint, the **Sensitivity** column updates within seconds to a couple of minutes; open the file's details pane ( ⓘ ) to see it sooner.

## Label requirements

- The label must be **published** in a Purview label policy and have the **Files** scope (Items → Files). Labels scoped only to Groups & sites or Meetings are accepted by Graph but never materialize on a file.
- If a label has sub-labels, pick the **sub-label**; a parent cannot be applied directly.
- Removing a label or applying a lower-priority one is a downgrade; the toolkit supplies the justification text Purview requires.
- Some labels that encrypt with user-defined permissions cannot be changed by an application and are reported as *not supported*.

## Troubleshooting

| Message                                                                           | Cause                                                                                                              | Fix                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Assigning a sensitivity label is a metered Microsoft Graph API... (402)</i>    | No billing link for the app ID the connection uses, <b>or</b> the connection is Web Browser / Username & password. | Check Step B with <code>az graph-services account list</code> ; confirm the app ID matches the connection; use a Certificate connection. After linking, restart the toolkit so a fresh token is issued. |
| <i>Microsoft Graph refused the request (403)</i>                                  | Missing or unconsented Application permission.                                                                     | Step A items 3–5; restart the toolkit (app tokens are cached for an hour).                                                                                                                              |
| <i>The tenant's labels could not be read: 403</i>                                 | InformationProtectionPolicy.Read.All missing, or token issued before consent.                                      | Add the permission, consent, restart. Labels already seen in the report can still be picked meanwhile.                                                                                                  |
| <i>Sensitivity label cannot be assigned since this file type is not supported</i> | Page, legacy Office format, image, or PDF without the tenant flag.                                                 | Only label supported files; run Step C for PDFs.                                                                                                                                                        |
| <i>The file is locked (423)</i>                                                   | Checked out, open in a co-authoring session, or being processed.                                                   | Check in / close and retry.                                                                                                                                                                             |
| Row says <i>Labelled</i> but SharePoint shows nothing                             | Background apply still running, or the label has no Files scope.                                                   | Wait a minute and refresh; check the label's scope in Purview; audit log activity<br><i>FileSensitivityLabelApplied</i> shows the outcome.                                                              |
| <i>The application was not found in this tenant (Azure CLI)</i>                   | Subscription is in a different tenant than the app.                                                                | Sign in to the app's tenant and use a subscription there.                                                                                                                                               |

## Cost control

Charges appear in **Azure Cost Management + Billing** on the linked subscription under the `Microsoft.GraphServices/accounts` resource. Create a monthly **Budget** with alerts on that subscription or resource group so volume is visible. Budgets alert but do not block; deleting the `Microsoft.GraphServices/accounts` resource is the hard stop (Graph returns 402 again immediately).

## Microsoft 365 Archive

### What it does

From an Item Inventory or Content Search report, tick files and choose **Send to Microsoft 365 Archive**. Archived files stay in place in the library, keep their metadata, permissions and search results, but their content is moved to cold storage: they cannot be opened, downloaded or edited until reactivated. This lowers your SharePoint storage consumption without deleting or moving anything.

## How it works

Each file is archived individually through the Microsoft Graph `driveItem/archive` action. The toolkit first checks the file's archive status so files that are already archived are reported as such rather than failing, then sends the archive request (synchronous) and reads the status back. Folders are not sent; archive the files inside them.

## Requirements

| Requirement                                              | Detail                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Microsoft 365 Archive turned on</b> in the tenant     | Microsoft 365 admin center → Settings → Org settings → <b>Pay-as-you-go services</b> → Settings → Storage services → <b>Archive</b> → turn on <i>SharePoint site archive</i> . Requires a pay-as-you-go billing policy (Azure subscription, resource group and region) connected under <b>Billing</b> first. SharePoint Administrator or Global Administrator role. See <a href="#">Set up Microsoft 365 Archive</a> . |
| <b>Your own Azure app registration</b> on the connection | <i>Use an Azure app registration on, Register automatically with Cognillo's shared app off.</i>                                                                                                                                                                                                                                                                                                                        |
| <b>Connection type</b>                                   | Web Browser <b>or</b> Certificate. This API is not metered, so public clients are fine.                                                                                                                                                                                                                                                                                                                                |
| <b>Permissions</b>                                       | Microsoft Graph <code>Files.ReadWrite.All</code> or <code>Sites.ReadWrite.All</code> — Delegated for Web Browser, Application for Certificate — admin consented. For Web Browser, the signed-in user also needs edit rights on the library.                                                                                                                                                                            |
| <b>Cost</b>                                              | Archived storage is billed per GB per month (currently <b>\$0.05/GB/month</b> ) <b>only</b> for the portion by which archived + active storage exceeds the tenant's licensed SharePoint quota. If you are under quota, archiving is free. Reactivation is free since 31 March 2025. See <a href="#">Pricing model for Microsoft 365 Archive</a> .                                                                      |

## Setup

1. **Billing policy.** Microsoft 365 admin center → **Billing** → **Pay-as-you-go services** (or *Setup* → *Pay-as-you-go*): connect an Azure subscription, resource group and region. This is the same policy Microsoft Syntex / SharePoint Premium uses; if one exists, reuse it.
2. **Enable Archive.** Settings → Org settings → Pay-as-you-go services → Settings → Archive → toggle **SharePoint site archive** on → **Confirm**. File-level archive is enabled for users by default when site archive is on.
3. **App registration.** Add `Files.ReadWrite.All` (Delegated for Web Browser connections, Application for Certificate connections) under Microsoft Graph, grant admin consent. If you completed the previous section, the Certificate app already has it.
4. **Connection.** Any connection with that app registration selected; Test and save.

5. **Test.** Tick one file in a report, **Send to Microsoft 365 Archive**, confirm, review, apply. The row shows *Archived*. In SharePoint the file shows an archive icon and opening it is blocked with a reactivation prompt.

## What users should expect

- Archived files cannot be opened, downloaded, edited or co-authored. Office for the web, mobile apps and older sync clients show errors for them.
- Reactivation is done in SharePoint (file → **Reactivate**) or by a SharePoint admin for whole sites. It is free, and takes from seconds up to 24 hours.
- A reactivated file **cannot be archived again for four months**.
- Cannot be archived: OneNote notebooks, SharePoint pages, files in Site Assets, folders.
- If Archive is later turned off or the billing policy becomes unhealthy, archived files stay archived and can still be reactivated, but new archive actions fail and archived storage counts as active again.

## Troubleshooting

| Message                                                          | Cause                                                                                           | Fix                                                                   |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <i>Microsoft 365 Archive is a pay-as-you-go service... (402)</i> | No billing policy, or Archive not enabled.                                                      | Setup steps 1–2. Allow a few minutes after enabling.                  |
| <i>Microsoft Graph refused the request (403)</i>                 | Permission missing / not consented, or (Web Browser) the user lacks edit rights on the library. | Setup step 3; check library permissions.                              |
| <i>...not enabled / not supported</i>                            | Archive not turned on, or the file is a page, OneNote notebook or Site Assets file.             | Enable Archive; skip unsupported files.                               |
| <i>The file is locked (423)</i>                                  | Already archived, or reactivation in progress.                                                  | Nothing to do; the toolkit reports already-archived files separately. |
| <i>...cannot be archived again for 120 days</i>                  | Recently reactivated.                                                                           | Wait out the four-month window.                                       |
| <i>Microsoft Graph could not find the file (404)</i>             | Moved or deleted since the report ran.                                                          | Refresh the report.                                                   |

## Quick Reference

|                      | Read labels in reports | Apply / remove labels                                                  | Microsoft 365 Archive                          |
|----------------------|------------------------|------------------------------------------------------------------------|------------------------------------------------|
| Own app registration | No                     | <b>Yes</b>                                                             | <b>Yes</b>                                     |
| Connection type      | Any                    | <b>Certificate only</b>                                                | Web Browser or Certificate                     |
| Graph permissions    | None                   | Application Files.ReadWrite.All + InformationProtectionPolicy.Read.All | Files.ReadWrite.All (Delegated or Application) |
| Tenant setup         | None                   | Azure CLI billing link per app                                         | Pay-as-you-go billing policy + Archive enabled |

|      | Read labels in reports | Apply / remove labels   | Microsoft 365 Archive            |
|------|------------------------|-------------------------|----------------------------------|
| Cost | None                   | \$0.00185 per file call | \$0.05/GB/month above quota only |

## Reference

- [Enable metered APIs and services in Microsoft Graph](#)
- [Metered APIs and services in Microsoft Graph \(pricing\)](#)
- [driveltm: assignSensitivityLabel](#)
- [Enable sensitivity labels for Office files in SharePoint and OneDrive](#)
- [Set up Microsoft 365 Archive](#)
- [Pricing model for Microsoft 365 Archive](#)