365 Indexer Enterprise

IT Administrator Guide

DRAFT

For use with dtSearch Desktop or dtSearch Network 2024.01 or later

Contents

What's New 5

Beta Software Notice 5

Introduction 6

Key differences from 365 Indexer 2.x 6

Multi-tenant deployments 6

Microsoft 365 clouds 6

Before you begin 7

Quick Reference 8

Registry Keys 8

PowerShell Commands 8

App Registration Client IDs 9

Config Site List Columns 9

Deployment Checklist 9

Prerequisites 11

Software 11

Azure/Entra roles required 11

Install PnP PowerShell 11

Azure App Registrations 12

Registration 1: 365 Indexer Enterprise 12

Registration 2: 365 Indexer PnP Admin Tool 13

Create the Config Site List 14

Create the SharePoint list 14

Add the required columns 14

Add approved sites 14

Windows Registry 15

Set EnterpriseClientId, Config Site URL & Config Site List Name 15

Set Site Serial Number 15

Disable OneNote Indexing 15

Set optional registry entries 15

DRAFT

Granting SharePoint Site Access 16
Connect to SharePoint 16
Grant access to a site 16
Verify the grant 16
Adding a new site later 16
Important notes 17
Certificate Registration 18
Certificate management 19
Naming certificates 19
Revoking a certificate 19
Certificate expiry 19
Machine migration 20
Ongoing Operation 21
What needs backing up 21
Roaming profiles and folder redirection 22
Moving or migrating indexes 23
Scheduled indexing requirements 24
Disabling OneNote Indexing 24
Event Viewer Logging 25
Where to find log entries 25
How to export logs for support 25
Event reference 25
Enabling diagnostic logging 28
Fallback Log File 28
Troubleshooting 29
“Need admin approval” when a user adds their account 29
The certificate dialog did not appear 29
Users see an empty site list in Create Index 30
SharePoint indexing fails with authentication errors 30
OneNote indexing stops working on schedule 30

DRAFT

Index appears empty after a scheduled run 30
Certificate expiry 31
Can't Reconnect the existing 2.4 version index. 31
Installation 32
Upgrading from 365 Indexer 2.x versions 32
Upgrading from 365 Indexer Enterprise up to 3.4.9738 32
Evaluation mode limits 33
Silent/unattended installation 33
Translation 34
Get Help 36
Feedback 36
Appendix 36
Changes since 3 Oct 2026 Issue 36
Changes since 25 Sep 2026 Issue: 37
Changes since 17 Aug 2026 Issue: 37
Changes since 5 Aug 2026 Issue: 37

DRAFT

What's New

365 Indexer Enterprise is a new product based on the earlier 365 Indexer 2.4 version.

See Release Notes for changes in each release.

See Appendix for any significant changes in this document since last issue.

Beta Software Notice

This software is a pre-release version provided for evaluation and testing. It may contain errors, defects, security vulnerabilities, or incomplete features, and its functionality, performance, and reliability are not guaranteed.

Please use the software at your own risk. Do not use it with critical, confidential, or irreplaceable data without suitable backups, and do not rely on it for essential business operations. Report any problems or feedback to support@electronart.co.uk or support@dtsearch.co.uk.. The software may be changed, suspended, or withdrawn at any time

DRAFT

Introduction

365 Indexer Enterprise enables organizations to make Microsoft 365 SharePoint and OneNote content searchable via dtSearch, while operating within enterprise security standards. Unlike the standard 2.x edition, 365 Indexer Enterprise uses Microsoft's Sites.Selected permission model, meaning the application can only access the specific SharePoint sites that you explicitly approve, not the entire tenant. This guide covers everything an IT Administrator needs to know to deploy, configure, and maintain 365 Indexer Enterprise. End users follow a separate User Guide.

Key differences from 365 Indexer 2.x

Feature	Standard 2.x	Enterprise 3.x
App identity	dtSearch UK's shared app registration	Your organization's own app registration.
SharePoint access	Tenant-wide (Sites.Read.All). Multi-tenant	Site-by-site (Sites.Selected) Single tenant. (See section below)
Who sets up accounts	User must be tenant admin	Any user with normal credentials
Site visibility	All sites in tenant	Only IT-approved sites. Optionally add Index all = all sites approved for that user
Certificate	Shared, embedded in app	Per-installation, in Certificate Store
IT Admin setup required	No	Yes - one-time, before first user and per-user certificate registration
OneNote access	App-only 2.3 Delegated (user signs in) 2.4	Delegated (user signs in)

Multi-tenant deployments

365 Indexer Enterprise is designed for deployment within a single Microsoft 365 tenant. Each installation supports one organization's Config Site and site approvals; accounts must belong to the tenant configured on that machine. Adding accounts from a different Microsoft 365 tenant on the same machine is not supported and will result in an empty or inaccessible site list for any account outside the configured tenant.

Microsoft 365 clouds

Commercial Microsoft 365 and US Government GCC (which uses the same Microsoft endpoints).

Contact dtSearch UK if GCC High or DoD (separate .us endpoints) is required, or if your organization requires support for multiple tenants on a single installation to discuss availability as part of a future release.

DRAFT

Before you begin

IMPORTANT
IT Admin setup (phase 1) should be completed BEFORE any user installs or tries to connect an account. If users install it first, they will see an empty site list with no explanation.

The recommended sequence is:

1. IT Admin completes all the one-time setup steps in phase 1 in the deployment checklist.
2. Users install 365 Indexer Enterprise
3. Each user clicks Add 365 account and signs in, this generates their certificate.
4. Users send the .cer file to IT Admin
5. IT Admin registers each user's certificate in the Entra portal (takes 2 minutes per user)
6. Users can now create indexes and see their approved sites

DRAFT

Quick Reference

This page summarizes the key information needed for day-to-day administration. Keep it to hand during deployment.

Registry Keys

Registry Value	Type	Purpose	Required?
EnterpriseTenantID	REG_SZ	Tenant ID (GUID) or domain, e.g. contoso.onmicrosoft.com	Optional. Only needed if your SharePoint name differs from your onmicrosoft.com name (e.g. after a SharePoint domain rename.) Normally worked out from ConfigSiteUrl.
EnterpriseClientId	REG_SZ	Application (client) ID)	Yes
ConfigSiteUrl	REG_SZ	URL of your SharePoint Config Site	Yes
ConfigSiteListName	REG_SZ	List name (default: 365IndexerApprovedSites)	Only if renamed
SerialNumber	REG_SZ	Enterprise serial (365110-XXXXXX-XXXX)	Recommended — alternative to per-user entry
OneNoteEnabled	DWORD	0 = disable OneNote, 1 = enable (default)	Optional
DiagnosticLogging	DWORD	0 = disable (default), 1 = enable.	Optional – See Troubleshooting
PersonalSitesMode	REG_SZ	Own (default) = Only rows for the signed-in user's own OneDrive. Group = Every OneDrive row the user's group is allowed, for managers, compliance staff, etc.	Optional
Language	REG_SZ	Sets the UI language. Value can be: • Language code such as fr-BE or de-DE • en for English • auto to follow the Windows language • Full path to a custom .lang file	Optional. Overrides user settings.

All keys under: HKEY_LOCAL_MACHINE\SOFTWARE\DTSUK\365 Indexer

PowerShell Commands

Run in PowerShell 7 (pwsh) as Administrator. Replace placeholders with your values.

Connect (using PnP Admin Tool Client ID):

```
Connect-PnPOnline -Url "https://[tenant].sharepoint.com" -Interactive -ClientId "[PnP Admin Tool Client ID]"
```

Grant site access:

```
Grant-PnPEntraIDAppSitePermission -AppId "[365 Indexer Enterprise Client ID]" -DisplayName "365 Indexer Enterprise" -Site "https://[tenant].sharepoint.com/sites/[SiteName]" -Permissions Read
```

Verify access:

```
Get-PnPEntraIDAppSitePermission -Site https://[tenant].sharepoint.com/sites/[SiteName]
```

DRAFT

App Registration Client IDs

Registration	Client ID	Purpose
365 Indexer Enterprise	[fill in after creating]	Used by the app itself
365 Indexer PnP Admin Tool	[fill in after creating]	Used for PowerShell grant ommands only — keep internal

NOTE *Fill in these Client IDs after completing the Azure App Registrations section. Keep the PnP Admin Tool Client ID internal - it has broad SharePoint permissions and should not be shared with users.*

Config Site List Columns

Column name	Type	Purpose
SiteUrl	Single line of text	Full URL of the approved SharePoint site
SiteDisplayName	Single line of text	Name shown to users in the site picker
AllowedGroup	Single line of text	Azure AD group display name. Leave blank for all users.

Deployment Checklist

Use this checklist when deploying 365 Indexer Enterprise. Complete items in order - steps marked IT Admin must be done before users install.

Phase 1 — IT Administrator setup (before any user installs)

Certificate registration is a manual, one-time step per user (See Certificate Registration section) Organizations with many users may wish to build their own automation for this, using Microsoft Graph or PowerShell against their own app registration – contact dtSearch UK support for guidance if needed.

☐ Created '365 Indexer Enterprise' app registration in Entra portal

☐ Noted Application (client) ID for Enterprise registration

☐ Added API permissions (see Registration 1): Microsoft Graph Sites.Selected (Application); User.Read, Sites.Read.All, Notes.Read.All, Group.Read.All, openid, profile, offline_access (Delegated); SharePoint Sites.Selected (Application); SharePoint AllSites.Read (Delegated)

☐ Granted admin consent for all permissions

☐ Added redirect URIs and enabled public client flows under Authentication

☐ Created '365 Indexer PnP Admin Tool' app registration

☐ Noted Application (client) ID for PnP Admin Tool registration

☐ Added AllSites.FullControl (Delegated) permission to PnP Admin Tool, granted admin consent

☐ Installed PowerShell 7 (pwsh) and PnP.PowerShell 3.x module

☐ Created 365IndexerApprovedSites list in SharePoint with required columns

☐ Added approved sites and group assignments to Config Site list

☐ Ran Grant-PnPEntraIDAppSitePermission for each approved site

☐ Verified grants with Get-PnPEntraIDAppSitePermission

DRAFT

☐ Set ConfigSiteUrl registry key on all target machines
☐ Set EnterpriseClientID registry key on all target machines
☐ Set ConfigSiteListName registry key (if list was renamed)
☐ Set SerialNumber registry key (if using organisation-wide serial)
☐ Set OneNoteEnabled = 0 registry key (if disabling OneNote)

Phase 2 — User installation

☐ User installs 365 Indexer Enterprise
☐ User launches app - confirms 'Version 3.4.x Enterprise' in status bar
☐ If serial not pre-deployed: user clicks Register and enters Enterprise serial (365110-XXXXXX-XXXX)
☐ User clicks Add 365 Account and signs in with corporate credentials
☐ Administrator approves the "Need admin approval" window on the user's PC (current release – see Troubleshooting)
☐ User emails .cer certificate file to IT Administrator

Phase 3 — IT Administrator certificate registration

☐ Received .cer file from user
☐ Uploaded .cer to 365 Indexer Enterprise app registration → Certificates & secrets → Upload certificate
☐ Added description identifying user and machine (e.g. 'J.Smith - Laptop - Jul 2026')
☐ Notified users that certificate is registered and they can proceed

Phase 4 — User: create and run index

☐ User clicks Create Index → Create a new index
☐ Approved sites appear in site picker (confirms Config Site list and certificate are working)
☐ User selects sites and completes index setup
☐ User clicks Run Indexer — index builds successfully
☐ User opens index in dtSearch Desktop and confirms content is searchable
☐ Optional: user sets up scheduled indexing

DRAFT

Prerequisites

You will need the following before starting setup:

Software

- PowerShell 7 (pwsh). Download from https://aka.ms/powershell
  Note: Windows PowerShell 5.1 (the built-in version) is NOT sufficient, it uses a different executable name (powershell vs pwsh) and a different module path.
- PnP.PowerShell 3.x module (requires PowerShell 7.4 or later)

Azure/Entra roles required

- SharePoint Administrator - for running the site-grant PowerShell commands
- Global Administrator, Cloud Application Administrator or Application Administrator - for granting admin consent on app registrations, and (in the current release) for approving the "Need admin approval" window when each user adds their account – see Troubleshooting

Install PnP PowerShell

Open PowerShell 7 as Administrator (search for pwsh, right-click, Run as Administrator):

```
Install-Module PnP.PowerShell -Scope CurrentUser -Force
```

DRAFT

Azure App Registrations

You need to create two separate app registrations on the Azure portal (portal.azure.com). These serve different purposes and must be kept separate, attempting to use one registration for both will fail.

Azure Active Directory is now **Microsoft Entra ID.**

Registration 1: 365 Indexer Enterprise

This is the application that 365 Indexer itself uses to access SharePoint on behalf of users.

1) In portal.azure.com, go to Azure Active Directory → App registrations → New registration.
2) Name it '**365 Indexer Enterprise**'. Under Supported account types choose **Accounts in this organizational directory only** and click Register.
3) Note the **Application (client) ID**, you will set this as the **EnterpriseClientID** Registry value later.
4) Go to API Permissions → Add a permission:
   a) Microsoft Graph → Application → Sites.Selected
   b) Microsoft Graph → Delegated → User.Read, Sites.Read.All, Notes.Read.All, Group.Read.All, and under OpenId permissions: openid, profile, offline_access (these sign-in permissions need admin consent when users are not allowed to consent to apps themselves)
   c) SharePoint → Application → Sites.Selected (needed in addition to the Microsoft Graph one; indexing reads SharePoint directly using the installation's certificate)
   d) SharePoint → Delegated → AllSites.Read
5) Click 'Grant admin consent for [your organisation]' to approve all permissions
   The only **Application** permissions are the two Sites.Selected entries. Do not add tenant-wide Application permissions such as Sites.Read.All or Sites.FullControl.All. Delegated permissions act as the signed-in user and can only reach what that user can already see. Removing a permission from the list does not withdraw consent already given; to withdraw it, use Revoke admin consent under **Other permissions granted for [organisation]**.
6) Go to Authentication → Add a platform → Mobile and desktop applications
   a) Add: http://localhost
   b) Add: https://login.microsoftonline.com/common/oauth2/nativeclient
   c) Set '**Allow public client flows**' to Yes
7) Click **Save**

NOTE
Do not add a certificate yet. Users generate their own certificates when they first add their account. See the Certificate Registration section.

DRAFT

Registration 2: 365 Indexer PnP Admin Tool

This registration is used only for running the PowerShell site-grant commands. It is not shipped with the software and is never seen by end users.

1) In portal.azure.com, create a new app registration named **'365 Indexer PnP Admin Tool'**
2) Note the Application (client) ID, you will need this later to enter in Windows Registry
3) Go to API Permissions → Add a permission → SharePoint → Delegated → AllSites.FullControl
4) Grant admin consent for this permission
5) Go to Authentication → Add a platform → Mobile and desktop applications
   a) Add: http://localhost
   b) Add: https://login.microsoftonline.com/common/oauth2/nativeclient
   c) Set 'Allow public client flows' to Yes
6) Click Save
7) No certificate is needed for this registration

DRAFT

Create the Config Site List

The Config Site list tells 365 Indexer which SharePoint sites each Azure AD group is allowed to index. Users see only the sites their group is approved for, they cannot see or access any other sites, even if those sites exist in the tenant. Users read the list as themselves, so every user needs at least Read access to it (for example as a Visitor of the Config Site). Sites added to the list later are picked up automatically by indexes set to Index all, the next time they run (after the site has been granted, see Granting SharePoint Site Access).

Create the SharePoint list

1. Go to your organization's SharePoint tenant (https://[yourtenant].sharepoint.com)
2. Navigate to the site where you want to host the config list
   (a dedicated IT admin site is recommended)
3. Click New → List → Blank list.
4. Name it exactly: **365IndexerApprovedSites** (no spaces)
5. Click **Create**

Add the required columns

Add the following columns to the list (click Add column for each):

Column name	Type	Purpose
SiteUrl	Single line of text	Full URL of the approved SharePoint site
SiteDisplayName	Single line of text	Friendly name shown to users in the site picker
AllowedGroup	Single line of text	Azure AD group display name. Leave blank to allow all users.

Add approved sites

For each SharePoint site you want to make available, add a row:

Column	Example value	Notes
Title	Finance Team Site	Any label, not displayed to users
SiteUrl	https://contoso.sharepoint.com/sites/Finance	Must match the site URL exactly
SiteDisplayName	Finance Team Site	This is what users see in the picker
AllowedGroup	Finance-Users	Azure AD group display name, or leave blank for all users
NOTE *You can have multiple rows pointing at the same site with different AllowedGroup values, to give access to multiple groups independently*		

DRAFT

Windows Registry

These can be deployed via Group Policy Preferences, a logon script, or as part of your software deployment package. The change takes effect the next time 365 Indexer is started.

Set EnterpriseClientId, Config Site URL & Config Site List Name

These are read from the Windows registry at startup. If these are not set, the site picker will show an empty list. Set the following values on each machine where 365 Indexer Enterprise is installed:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\DTSUK\365 Indexer
Value: EnterpriseClientId **Type**: REG_SZ

Data: [Application (Client) ID noted in Registration 1]

Value: ConfigSiteUrl **Type**: REG_SZ
Data: https://[yourtenant].sharepoint.com/sites/[your-admin-site]

Value: ConfigSiteListName **Type**: REG_SZ
Data: 365IndexerApprovedSites

Set Site Serial Number

If a serial number is not entered into the About box on 365 Indexer it will run in evaluation mode with limited features for 30-days. End users can enter a serial themselves, or to automatically register each copy of 365 Indexer as it is installed you can set the following values:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\DTSUK\365 Indexer
Value: SerialNumber **Type**: REG_SZ
Data: [your enterprise serial number]

Disable OneNote Indexing

If your organization does not want users to index OneNote notebooks, for example due to data governance requirements, you can disable the OneNote feature without reinstalling the software. Set the following registry value on each machine where 365 Indexer is installed:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\DTSUK\365 Indexer
Value: OneNoteEnabled **Type**: DWORD

Data: 0 (to disable) / 1 (to enable, default)

Set optional registry entries

Refer to the table here: Windows Registry

DRAFT

Granting SharePoint Site Access

For each SharePoint site in your Config Site list, you must run a PowerShell command to grant the 365 Indexer Enterprise app permission to access it. This uses the Sites.Selected permission model, the app can only access sites you explicitly grant.

Connect to SharePoint

Open PowerShell 7 as Administrator and connect using the PnP Admin Tool registration:

```
Connect-PnPOnline -Url "https://[yourtenant].sharepoint.com" -Interactive -ClientId "[PnP Admin Tool Client ID]"
```

A browser sign-in window will appear. Sign in with your Global Administrator account.

Grant access to a site

```
Grant-PnPEntraIDAppSitePermission `  -AppId "[365 Indexer Enterprise Client ID]" `  -DisplayName "365 Indexer Enterprise" `  -Site "https://[yourtenant].sharepoint.com/sites/[SiteName]" `  -Permissions Read
```

Repeat this command for each site in your approved list. One command per site, the same connection can be reused for multiple grants in the same session.

Verify the grant

```
Get-PnPEntraIDAppSitePermission -Site "https://[yourtenant].sharepoint.com/sites/[SiteName]"
```

This should return a row showing the 365 Indexer Enterprise app with Read permissions. A grant covers both the Microsoft Graph and SharePoint APIs, so one command per site is enough.

Adding a new site later

When you want to make a new site available to users:

- Add a row to the 365IndexerApprovedSites list in SharePoint
- Run the Grant-PnPEntraIDAppSitePermission command for the new site

No reinstallation or other changes are needed. The new site will appear in users' site pickers the next time they open the **Create Index** dialog. Users' **Index all** indexes include the new site from their next run.

DRAFT

Important notes

- Two separate app registrations are essential. Using the 365 Indexer Enterprise registration itself for the PnP connection will fail with Access Denied.
- PowerShell 7 must be launched as pwsh, not powershell. They are entirely different applications despite similar names.
- The SharePoint Administrator role must be assigned and given time to propagate Allow up to 15 minutes before running the grant command.
- The grant command must be repeated for every site individually. There is no 'grant all sites at once' option, this is by design.

DRAFT

Certificate Registration

365 Indexer Enterprise generates a unique security certificate for each installation. This certificate is used to authenticate the application to your Azure app registration. The private key is stored securely in the Windows Certificate Store and cannot be exported.

IMPORTANT

Certificate registration is a manual step performed by your IT Administration. We recommend testing on one machine first before rolling out to other users.

The process for each user installation:

1) User installs 365 Indexer Enterprise
2) User clicks Add 365 Account and signs in with their normal corporate credentials
3) The application generates a unique certificate and displays a dialog showing the path to a .cer file (saved in the user's %TEMP% folder, named 365Indexer_ followed by their sign-in name, e.g. 365Indexer_jane_smith_example_org.cer). In the current release, unless the user is an administrator, a "Need admin approval" window appears first, and an administrator must approve it on the user's PC before the certificate dialog is shown – see Troubleshooting
4) User clicks Open Folder, locates the .cer file, and emails it to the IT Administrator
5) IT Administrator uploads the .cer file to the 365 Indexer Enterprise app registration in the Entra portal:
   a) Go to portal.azure.com → Azure Active Directory → App registrations → 365 Indexer Enterprise
   b) Click Certificates & secrets → Upload certificate
   c) Browse to the .cer file and upload it
   d) Add a description to identify which user/machine this certificate belongs to.
6) IT Administrator notifies the user that the certificate has been registered
7) User can now create indexes and run the indexer

NOTE

Users can create an index and configure it before the certificate is registered, but expanding a site to choose individual lists, and running the indexer, need the certificate to be registered. If any indexes exist from earlier 2.3 versions, or 2.4 betas, do not try to Reconnect them, make fresh indexes.

DRAFT

Certificate management

Naming certificates

When uploading a certificate, add a description that identifies the user and machine (for example: 'Tom Brown - Laptop - July 2026'). This makes it easy to identify and revoke individual certificates if a device is lost or a user leaves.

Revoking a certificate

If a device is lost, stolen, or a user leaves the organization:

1) Go to portal.azure.com → App registrations → 365 Indexer Enterprise → Certificates & secrets
2) Find the certificate for that user/device (identified by the description you added)
3) Click the delete icon to revoke it

The revoked installation can no longer authenticate. Other users and installations are unaffected.

Certificate expiry

Certificates are valid for 2 years from the date of generation. When a certificate approaches expiry, the user will need to remove and re-add their account (which generates a new certificate) and the IT Admin will need to upload the new .cer file. We recommend tracking certificate expiry dates when you add the description.

DRAFT

Machine migration

If a user moves to a new machine, they will need to re-add their account on the new machine (generating a new certificate) and the IT Admin will need to register the new certificate. The old certificate should then be revoked.

Existing indexes can be reconnected on the new machine using the **Reconnect existing index** option in the **Create Index** dialog. (**DO NOT** reconnect indexes from earlier version 2.3, or 2.4 betas.)

If moving indexes, ensure they are not placed in locations in OneDrive or similar synched folders, also avoid folders that are scanned by Microsoft search or other similar programs..

DRAFT

Ongoing Operation

What needs backing up

Item	Location	Importance	Notes
Index folders	Configured by user (default: My Documents\365 Indexer\Indexes)	Critical	Contains indexed content. Loss requires re-indexing.
365indexer_ config.json	Inside each index folder	High	Self-describing config. Allows indexes to be moved and reconnected without reconfiguration.
Account config (.oAccount)	My Documents\365 Indexer\Config\Accounts	High	Contains index registrations and schedules. A backup copy is also kept in %LOCALAPPDATA%\365 Indexer\Backups\Accounts
MSAL token cache	%LOCALAPPDATA%\365 Indexer\Cache\UserTokens	Low	Cached sign-in. Used to read the Config Site list, for OneNote, and for SharePoint indexes set to Index all. If lost, the user signs in again on next use.
Certificate (private key)	Windows Certificate Store, Current User → Personal (not a file, cannot be copied or backed up conventionally)	Critical	One certificate per tenant, subject `CN=365 Indexer - {tenantId}`. Does not roam and is not included in any file -based backup. If lost (e.g. new machine, profile reset), the user must re-add their account, generating a new certificate that IT Administration must register.
Config Site list	SharePoint (your admin site)	Medium	Managed in SharePoint - backed up as part of normal SharePoint backup.

DRAFT

Roaming profiles and folder redirection

Some organizations use roaming user profiles or Folder Redirection / OneDrive Known Folder Move (KFM) to make a user's files available across machines. 365 Indexer Enterprise's files are affected differently depending on where they live, and this can cause confusing behaviour if not accounted for

Certificates and cached tokens never roam.
%LOCALAPPDATA% is always machine-specific by design, regardless of roaming profile or folder redirection policy. This means:

- A user's certificate (stored in the Windows Certificate Store) and cached sign-in token exist **only on the machine where the account was added**.
- If a user's profile roams to a new machine, their index configuration and index content may appear to follow them (see below) but they will still be prompted to sign in again, and a **new certificate will be generated that IT Administration must register**, exactly as described in Machine migration.

IMPORTANT
If **Documents** is redirected via Known Folder Move (including OneDrive's automatic Known Folder Move), index folders will be redirected too.
By default, 365 Indexer stores indexes under Documents\365 Indexer\Indexes. If your organization has enabled Known Folder Move for Documents - a common OneDrive deployment setting - this location is silently relocated into OneDrive's sync scope, **without the user or IT Administrator explicitly choosing an index location there.**

Storing an actively updated index inside a folder that a cloud sync client (OneDrive, or similar) is simultaneously monitoring can cause file lock contention during indexing, leading to failed or incomplete index updates. See Troubleshooting: *Index appears empty after a scheduled run*.

Recommendation: if your organization uses Known Folder Move or OneDrive sync, either:

- Exclude the 365 Indexer\Indexes subfolder from OneDrive sync (via OneDrive's folder-level sync exclusion settings), or
- Direct users to choose a non-redirected location (e.g. a local path outside Documents) when creating an index

DRAFT

Moving or migrating indexes

Because each index folder contains a self-describing 365indexer_config.json file, indexes can be moved to a different location, server, or machine without losing their configuration.

To move an index folder:

1) Copy the index folder (including the 365indexer_config.json file) to the new location
2) In 365 Indexer on the destination machine, click **Create Index** on the appropriate account node
3) Select **Reconnect an existing index**
4) Click **Next**, then **Browse** to the index folder at the new location
5) 365 Indexer will read the configuration file and restore the index registration automatically
6) Click **Save**

NOTES

Scheduled tasks are not migrated automatically, the user will need to re-set the schedule after reconnecting

DO NOT locate indexes in folders on OneDrive or similar synched folders.

DRAFT

Scheduled indexing requirements

Scheduled indexing runs as a Windows Task Scheduler task under the user's own account. The following conditions must be met for scheduled indexing to work:

- The user must be logged in to Windows (tasks are configured to 'Run only when user is logged on')
- The machine must be powered on and not in sleep mode at the scheduled time
- Network access to SharePoint/Microsoft 365 must be available
- For OneNote indexes and SharePoint indexes set to Index all, the user must have signed in to 365 Indexer, and the sign-in must not have expired (typically 90 days of inactivity).
- SharePoint indexes with selected sites use the installation's certificate and need no sign-in.

NOTE
OneNote indexing requires an interactive sign-in on first use to establish a cached token. Subsequent scheduled runs use the cached token silently. If the token expires (typically after 90 days of inactivity), the user must open 365 Indexer and run a manual OneNote index once to re-establish the cache before scheduled indexing will resume.

OneNote indexing is user-scoped, the app accesses notebooks that the signed-in user personally has access to in Microsoft 365. Unlike SharePoint, IT Administrators cannot restrict which individual notebooks a user can index. If fine-grained control over notebook access is required, disable OneNote indexing entirely.

If a scheduled **Index all** cannot read the approved sites list, it logs a warning and leaves the existing index unchanged.

Disabling OneNote Indexing

If your organization does not want users to index OneNote notebooks, for example due to data governance requirements, you can disable the OneNote feature without reinstalling the software. See the Windows Registry section.

DRAFT

Event Viewer Logging

365 Indexer Enterprise writes events to Windows Event Viewer so that IT administrators can monitor indexing activity without the application being open, and so that events can be picked up by existing log-monitoring or SIEM tooling.

Where to find log entries

Log entries appear in Event Viewer under: Windows Logs → Application

Filter on the Source column value **365 Indexer** to isolate 365 Indexer entries from other application events.

How to export logs for support

1) Open Event Viewer (Windows key + R, type eventvwr.msc, press OK)
2) In the left-hand panel select Windows Logs → Application
3) In the right-hand panel select Filter Current Log
4) In Event sources select 365 Indexer, press OK
5) In the right-hand panel select Save All Events As and Save as type: CSV, click Save

Small CSV files can be emailed to support@dtsearch.co.uk

Event reference

Level	Message	Meaning	Action needed
Information	Index task started	A scheduled or manually triggered index run has begun.	None.
Information	Index task finished	The run was completed normally.	None.
Information	Task cancelled	The run was stopped before completion.	Confirm this was expected. If unexpected, check for machine sleep, network loss, or task interruption.
Information	Found self-describing config	365 Indexer automatically reconnected an index that had been moved	Usually none. Worth noting if unexpected —

DRAFT

		or whose registration was missing.	may indicate index folder was moved.
Information	No sites configured in task options	Run Indexer was clicked on a reconnected index that has no sites configured yet. The existing index content is preserved.	Users should click Edit on the index to configure which sites to include, then run again.
Information	"Existing certificate reused... " (User has clicked "Add 365 Account" and signed into same account again and their corticate has not expired)	Existing certificate reused for tenant [GUID] (expires 2028-07-10). No new certificate registration is required.	None
Information	"A NEW certificate was generated..." (User has clicked "Add 365 Account" and signed into their account. Their certificate has expired, or within 30 days of expiry	A NEW certificate was generated for tenant [id]... This certificate must be sent to and registered by IT Administration before authentication will succeed.	This new certificate must be sent to and registered by IT Administration
Warning	Skipping permanently inaccessible site/group	A SharePoint site or Microsoft 365 group that no longer exists was encountered and skipped.	None - these are cleaned up automatically. If the site should exist, check it in SharePoint Admin.
Warning	OneNote scheduled indexing failed: requires interactive login	The OneNote authentication token has expired. Scheduled indexing cannot continue without a user signing in.	User must open 365 Indexer and run a manual OneNote index once to re-cache the token.
Warning	SharePoint/OneNote index swap skipped: new index appears empty	The indexer ran but produced no content. The existing index has been preserved.	Check Event Viewer for preceding errors. May indicate throttling,

DRAFT

			network issues, or no sites configured.
Warning	Enterprise build: ConfigSiteUrl registry value is not set. Set HKLM\\SOFTWARE\\DTSUK\\365 Indexer\\ConfigSiteUrl to the URL of your Config Site. Users will see an empty site list.	The ConfigSiteUrl registry value is not set.	Set the ConfigSuteURL
Warning	Account added, but this installation's certificate could not authenticate yet (expected until IT Administration registers it)	Normal for a new certificate	Register the user's .cer file.
Warning	Index '...' was not updated: could not read the approved sites list	Index all run could not read the Config Site list, usually an expired sign-in on a scheduled run	Open 365 Indexer and run the index once manually.
Warning	Index '...' was not updated: no approved sites were found for this account	Index all run, but the Config Site list has no rows for this user	Check the user's AllowedGroup rows.
Severe	OneNote token cache persistence FAILED	The application cannot save the authentication token to disk. OneNote scheduled indexing will not work.	Check that %LOCALAPPDATA%\365 Indexer\Cache\UserTokens is accessible and not blocked by security software.
Error	Could not sign in to Microsoft Graph with this installation's certificate...	Certificate not registered, or revoked	Upload the user's current .cer.
Error	Containing AADSTS700027	The certificate used is not registered on the app	Upload the user's .cer. The thumbprint in the message identifies it.

Known harmless entries

The following entries may appear and can be safely ignored:

- Viva Engage system group error (Code 20160) a Microsoft system group that cannot be indexed. This is expected and permanent.

DRAFT

- Access denied for deleted SharePoint sites. Sites that have been deleted from SharePoint, but whose IDs still appear temporarily in search results. These are skipped automatically.
- .NET Runtime profiling messages, unrelated Windows system events that appear in the Application log alongside 365 Indexer entries.

Enabling diagnostic logging

If you are experiencing configuration issues that are not explained by the standard Event Viewer entries, set DiagnosticLogging = 1 in the registry to enable additional diagnostic output. Diagnostic entries are prefixed with [DIAG] in Event Viewer for easy identification.

Disable diagnostic logging again once the issue is resolved, leave it enabled permanently only if specifically requested by dtSearch UK support.

Fallback Log File

Location: %LOCALAPPDATA%\365 Indexer\Logs\365Indexer_fallback.log
(typically C:\Users\<username>\AppData\Local\365 Indexer\Logs\365Indexer_fallback.log)

365 Indexer normally writes its log entries to the Windows Event Log. If an event log entry cannot be written, for example, because the current user account does not have permission to verify or create the event source, 365 Indexer automatically falls back to writing the same entry to this text file instead, so no diagnostic information is lost.

DRAFT

Troubleshooting

"Need admin approval" when a user adds their account

After the user signs in with **Add 365 Account**, a window titled "Consent Required" shows "Need admin approval – 365 Indexer Enterprise needs permission to access resources in your organisation that only an admin can grant".

In the current release this appears even when every permission in Registration 1 shows "Granted for [your organisation]". After the user signs in, 365 Indexer opens Microsoft's admin consent page for your app registration, and only an administrator can complete that page. The user's sign-in itself succeeds (Entra sign-in logs show it as successful). This step will be removed in a future update. Until then, for each user:

1. If an earlier attempt did not finish, have the user delete the leftover certificate first (see The certificate dialog did not appear below).
2. The user clicks **Add 365 Account** and signs in with their own account.
3. When "Need admin approval" appears, an administrator (Global Administrator, Cloud Application Administrator or Application Administrator) clicks **Have an admin account? Sign in with that account** in that same window on the user's PC, signs in and approves. This re-confirms the permissions already granted; it does not add any new ones.
4. Account setup continues under the user's own account and the certificate dialog appears. Register the .cer file as described in Certificate Registration.

If the user clicks **Return to the application without granting consent**, account setup stops and the account is not added; they can try again.

If Entra sign-in logs show "Admin consent is required for the permissions requested by this application" (AADSTS65001 or AADSTS90094), a permission has not had admin consent. Check every item in Registration 1 step 4, including openid, profile and offline_access, and click **Grant admin consent for [your organisation]**. The Enterprise application's Permissions page (Enterprise applications → 365 Indexer Enterprise → Permissions) shows what has actually been granted. Users do not need to be assigned to the application.

The certificate dialog did not appear

365 Indexer creates the installation's certificate during **Add 365 Account** and shows the certificate dialog only when it creates a new one. If an earlier attempt did not finish (for example at the "Need admin approval" window), the certificate was created but never shown, and later attempts reuse it without the dialog.

If you have **not** registered a certificate for this user yet:

1. The user closes 365 Indexer.
2. The user runs **certmgr.msc**, opens **Personal** → **Certificates** and deletes any certificate whose name begins "365 Indexer - ".

DRAFT

3. The user opens 365 Indexer, removes the account if it is in the tree view, and clicks **Add 365 Account** again. A new certificate is created and the dialog shows the .cer file's location in their %TEMP% folder.

Do not have the user delete a certificate you have already registered – their indexing would stop until you register the new one. A registered certificate does not need to be sent again, which is why the dialog does not appear when a user removes and re-adds an account.

Users see an empty site list in Create Index

This means either:

- The IT Admin has not yet completed the Azure app registration and site grant steps : complete these first
- The Config Site list does not contain any rows for the user's Azure AD group: add the appropriate rows
- The user's Azure AD group membership has not propagated: allow up to 1 hour for group membership changes to take effect

SharePoint indexing fails with authentication errors

Check the following:

1. Confirm the user's certificate has been uploaded to the 365 Indexer Enterprise app registration in Entra portal
2. Confirm the Sites.Selected permission has been granted for the relevant site using the PowerShell grant command
3. Check that admin consent has been granted for all required permissions in the app registration
4. Confirm both Application permissions are present and granted: Microsoft Graph Sites.Selected and SharePoint Sites.Selected (shown as Office 365 SharePoint Online on the Enterprise application's Permissions page)

OneNote indexing stops working on schedule

The MSAL authentication token has likely expired. The user must:

1. Open 365 Indexer
2. Click on their OneNote index
3. Click **Run Indexer** to trigger a manual run, this will prompt for sign-in if the token has expired
4. Sign in when prompted
5. Scheduled indexing will then resume silently

Index appears empty after a scheduled run

If a scheduled index run completes, but the index is empty or unchanged, check Event Viewer for:

DRAFT

- 'No sites configured in task options' the index was reconnected but not yet configured. Users need to click Edit and configure sites.
- 'SharePoint index swap skipped: new index appears empty', the crawl produced no content. Usually caused by throttling (too many API requests) or network connectivity during the scheduled window.
- 'OneNote scheduled indexing failed: requires interactive login'. See OneNote troubleshooting above.

Certificate expiry

If a user reports that indexing stopped working and their certificate is approaching or past its 2-year expiry date:

1) Ask the user to remove their account in 365 Indexer (right-click account → Remove account)
2) User re-adds their account - a new certificate is generated
3) User emails the new .cer file to IT Admin
4) IT Admin uploads the new .cer to the app registration and deletes the old one

Can't Reconnect the existing 2.4 version index.

When trying to Reconnect an existing 2.4 version index, it might display warnings:

- "Site Not Approved" "This index is configured to **index all** SharePoint sites, which is not supported by this edition's site-by-site permission model."
- "Site Not Approved" "This index references one or more SharePoint sites, that are not currently approved for this installation."

Reconnect is blocked for any index containing any site not currently approved or is configured as "Index all sites" with a clear message naming the specific unapproved site(s) and logged to Event Viewer for an audit trail (From build 3.4.9723).

It might be possible to click the Edit button to change from 'Index All' to 'Index selected' and choose the sites the user requires if they are currently listed. Consider if the index should be deleted or if the current approved site list needs updating.

DO NOT try to Reconnect old 2.3 version indexes to 365 Indexer Enterprise, it will not work, they are not self-describing.

From build 3.4.9764 an **Index all** index reconnects and indexes all sites approved for the user. Indexes with individually selected sites are still checked against the approved list.

DRAFT

Installation

365 Indexer Enterprise is an add-on product for use with dtSearch Desktop or dtSearch Network 2024.01 or later.

IMPORTANT
Before installing 365 Indexer you must install a copy of dtSearch Desktop or dtSearch Network on the machine where indexes will be created and maintained.

Install 365 Indexer on the same machine where dtSearch Network is installed. The application will automatically detect where dtSearch is installed and will warn if it cannot be found.

Default install folder: ...\Program Files (x86)\DTSUK\365 Indexer\

Upgrading from 365 Indexer 2.x versions

After you uninstall using Windows Add or remove programs feature the serial number, configuration and indexes remain so that you can continue to search the indexes using dtSearch Desktop., Furthermore, you can install updated 2.x versions without having to login again and can continue to add or update existing indexes.

However, when you subsequently install 365 Indexer Enterprise it will not display those existing accounts or use the existing serial number, this is by design. 365 Indexer Enterprise edition requires IT Administrators to register the product with the site license serial number and connect with appropriate SharePoint sites.

If your organization no longer needs to search existing 2.x indexes you can use the Index Manager in dtSearch Desktop to delete individual indexes or Library Manager to remove all of them. This does not remove the index folders from the filesystem; to prevent someone using dtSearch Desktop to Recognize them, you should manually delete the index folders from the filesystem. You should also use Task Manager to remove any scheduled indexing tasks associated with version 2.x.

You can safely Reconnect 2.4 version indexes to 3.4 Enterprise after build 3.4.9723 (15 Aug 2026). See Troubleshooting “Can’t reconnect an existing 2.4 version index”

Upgrading from 365 Indexer Enterprise up to 3.4.9738

Before upgrading:

1. Add the new API permissions in Registration 1 and grant admin consent.
2. Make sure each user's certificate is registered.
3. After upgrading, each user is asked to sign in once more.
   Scheduled OneNote and **Index all** runs resume after that sign-in.
4. If your tenant previously consented to the 'DtSearch UK - 365 Indexer' app, you could remove it under Enterprise applications once no 2.x installations need it.

DRAFT

Evaluation mode limits

Without a serial number, the application runs in evaluation mode with the following limits:

- Scheduled indexing is not functional
- SharePoint: only 6 items per list are indexed
- OneNote: maximum 3 pages per notebook section are indexed

To remove the limits, click Register in the application and enter your serial number.

Silent/unattended installation

365 Indexer Enterprise uses a standard MSI installer and supports the following command-line switches for deployment via SCCM, Intune, or similar tools:

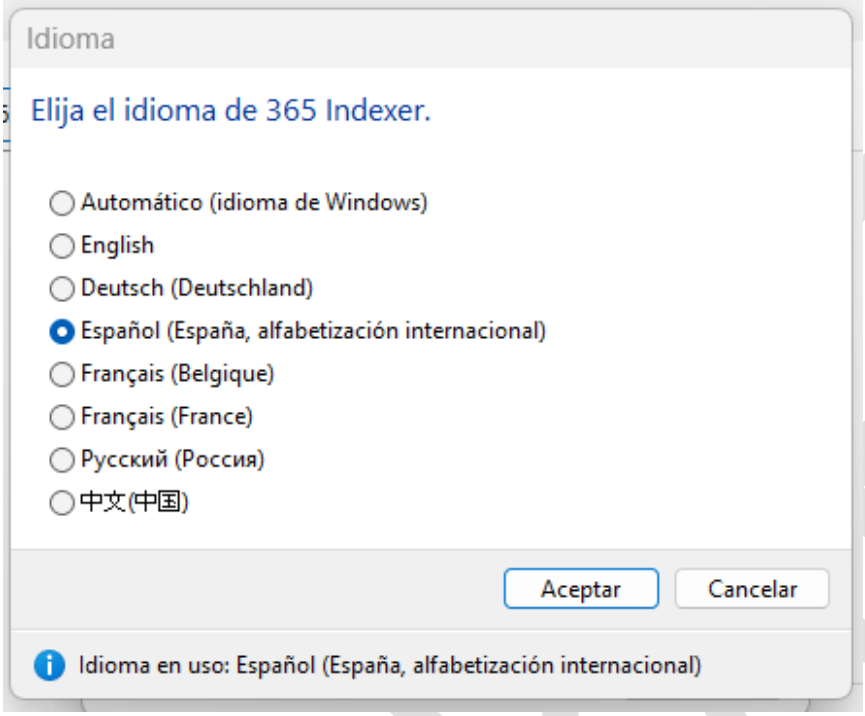
```
setup.exe /quiet /norestart
```

NOTE
The application must still be configured interactively by each user after installation, silent install deploys the binary but does not configure account connections or indexes.

DRAFT

Translation

The default language of the user interface is English. Several .lang files are supplied in the I18n folder which users can choose from using a Language selector in the About box, or they can choose Auto to automatically select a .lang file to match the Windows language. Optionally a language Registry key can be used to override the user settings.

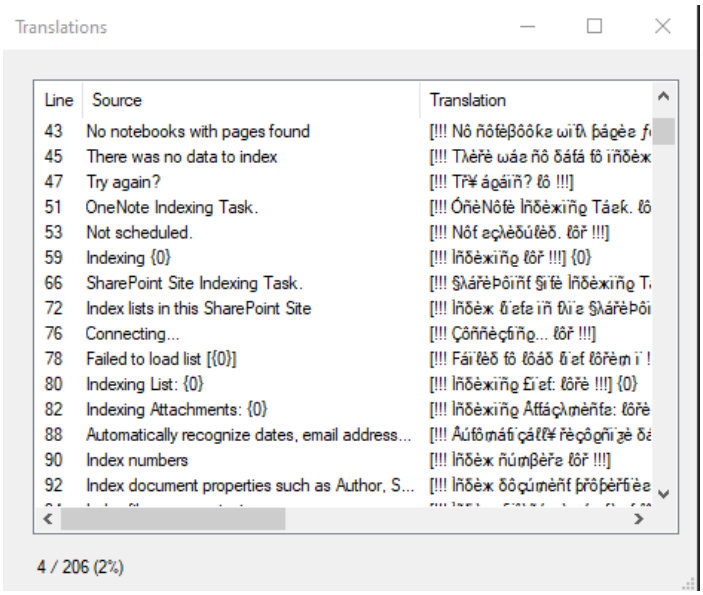


To add other languages, make a copy of the **qps-ploc_365_Indexer.lang** file in the **\I18N** subfolder. Place the untranslated copy of the template file in the same folder as the **365 Indexer.exe** file and run 365 Indexer, you will see all the English text is replaced by pseudo-language with a width 30% wider than English to take into account the typical expansion that occurs in translating from English to many other languages. Text Labels in 365 Indexer will automatically expand to accommodate the length of the text.

To assist translators, 365 Indexer can be run with a command line:
cd "C:\Program Files (x86)\DTSUK\365 Indexer\365 Indexer.exe" -t

This will display the list of phrases to translate, as each line is translated and the surrounding [[ ]] are removed, it will indicate what number and percentage of lines are translated.

DRAFT



Translate the appropriate text using a text editor*

Save it in utf-8 format (we suggest you rename it using IETF language tags (e.g. **fr-CA.lang** for Canadian French) and place the file in the I18n folder (or the same folder as 365 Indexer.exe.)

*Our free **Language File Editor** Is suitable.

DRAFT

Get Help

Need assistance with evaluating or setting up 365 Indexer Enterprise? Contact support@dtsearch.co.uk. Always quote your product version and serial number when contacting support.

Training articles for dtSearch Desktop/Network and add-on products are available at:
https://www.dtsearch.co.uk/dtsupport/training

Feedback

Please send feedback on this guide to support@dtsearch.co.uk we want it to be genuinely useful for IT administrators evaluating and deploying 365 Indexer Enterprise.

Appendix

NOTE (References to certain builds do NOT mean they have been publicly released, they may be builds for internal or limited release. Ensure that any builds you obtain are from signed setup.exe or signed .msi files).

Changes since 3 Oct 2026 Issue

- Registration 1: added SharePoint → Application → Sites.Selected (previously missing from the list) and the openid, profile and offline_access sign-in permissions; deployment checklist updated to match.
- Azure/Entra roles: Cloud Application Administrator added.
- Certificate Registration: where the .cer file is saved, and the "Need admin approval" window.
- Troubleshooting: new sections "Need admin approval" when a user adds their account and The certificate dialog did not appear; SharePoint authentication errors now checks both Sites.Selected permissions.

DRAFT

Changes since 25 Sep 2026 Issue:

- Added new heading: Set optional registry entries
- New optional registry value **Language**
- Translation page shows user options

Changes since 17 Aug 2026 Issue:

- Registration 1: new required API permissions and single-tenant setting (from build 3.4.9764).
- Deployment Checklist updated to match.
- New optional registry values **EnterpriseTenantId** and **PersonalSitesMode**
- New section: Supported Microsoft 365 clouds.
- Key differences new App identity row.
- Certificate Registration: certificate is now used for all background access.
- Config Site list: users need Read access; **Index all** picks up newly approved sites.
- Scheduled indexing requirements: **Index all** needs a current sign-in.
- Event reference and Troubleshooting: new certificate, sign-in and approved-sites entries.
- Reconnect: **Index all** indexes can be reconnected again.
- New section: Upgrading from 365 Indexer Enterprise 3.4 beta builds.

Changes since 5 Aug 2026 Issue:

- Correction to 'Key differences from 365 Indexer 2.x' table OneNote connection 2.3 v 2.4
- Added new section Roaming profiles and folder redirection
- Upgrading from earlier 2.x versions – Reconnecting 2.4 indexes (From build 3.4.9723)
- Updated "What needs backing up" table, new row 'Certificate (private key)'
- Added new section Multi-tenant deployments and notes in the table in previous section.
- Added to Event Viewer Logging > Event Reference two extra Information level events about user clicking **Add 365 Account** and certificate generation. (From build 3.4.9719)
- Correction: Data for EnterpriseClientId Registry entry was a URL instead of Application (Client ID).

DRAFT