



Integrate. Collaborate. Migrate.

# Configuration Guide

PowerSyncPro Migration Agent

Last updated: 26 March 2025



## Contents

---

PowerSyncPro Overview .....	5
Release Notes .....	6
Introduction .....	6
Prerequisites .....	6
Installation Guide.....	6
Key Concepts .....	7
Global Settings .....	8
Users .....	8
User Roles .....	9
Agent Viewer .....	10
Licences .....	11
Expired Licenses .....	13
Dashboard .....	14
Download Agent .....	15
msi .....	15
msi with .Net .....	16
Agent Installation .....	16
Settings.....	16
Directories.....	16
Schedule.....	16
Sync Profile .....	17
Creating a Bulk Enrollment Token.....	18
Bulk Enrollment Token Expiring .....	20
Pre Shared Keys “PSK” .....	21
Certificates.....	22
Runbooks.....	24
Default Processing.....	25

Creating a Runbook .....	26
Startup .....	27
User Experience .....	29
Device State .....	41
Permission Updates .....	51
App Reconfiguration .....	54
Completion .....	64
Batches .....	67
Assign Runbook .....	68
Runbook .....	68
Available From Time .....	69
Enforced After Time .....	69
Time zone .....	70
Computers .....	72
Drop down picklist .....	73
Import from CSV .....	73
Self Service Migrations .....	76
Options .....	77
Register Migration Agent .....	77
Check Runbooks .....	78
Migrate Now .....	78
About .....	80
Exit .....	80
Reports .....	82
Single Object Report .....	82
Runbook Status Report .....	85
User Profile Report .....	85
Agents .....	85
Agent Progress .....	86
Agent Details .....	88
Agent Logs .....	89



Failed Communications .....	90
Translation Table .....	91
Event Logs.....	92
Windows Hello for Business .....	94
Autopilot .....	94
Troubleshooting.....	95
Appendix - Entra Join settings for Microsoft 365.....	97
Entra ID .....	97
Entra Device settings.....	97
Intune .....	98
Mobility (MDM and WIP).....	98
Conditional Access .....	100
Licencing.....	101
Device platform restrictions.....	102
Device limit restrictions .....	102
DNS Records .....	102
Event Logs .....	104
Users .....	105
Per User MFA.....	105





## PowerSyncPro Overview

---

### Windows Workstation Migration Agent

The PowerSyncPro Migration Agent facilitates a quick 'return to operation' for your end-users following a migration event by reconfiguring the device join state, Windows user profiles and Microsoft core applications.

PowerSyncPro Migration Agent can migrate tens of thousands of machines in parallel. Typically, workstations migrate in less than 30 minutes.

Using the PowerSyncPro Migration Agent eliminates the need to perform bulk workstation replace/swap outs, reimaging workstations or attempting to manually reconfigure workstations with a complex set of documented end-user or administrator steps that are prone to error.

### Use cases

PowerSyncPro can take a Windows workstations from a device join state of

- Active Directory Joined
- Hybrid Entra Joined
- Entra Joined

And migrate to any of the same device join states in the same or different endpoint

- Active Directory Joined
- Hybrid Entra Joined
- Entra Joined

Depending on your chosen configurations, the workstation Migration Agent will reconfigure the workstation join status, repermission Windows user profiles, reset Microsoft core Office Applications, reset the workstations Intune enrollments, Azure Information Protection, Windows Hello for Business, and Autopilot settings. Additional custom commands can be executed pre and post migration. PowerSyncPro provides comprehensive logging and dashboards.

### Active Directory Migrations

PowerSyncPro facilitates Active Directory migrations by making objects such as Users, Groups and Contacts in a target Active Directory ready for migration or cutover via Directory Synchronisation. It synchronizes all or a subset of attributes and can synchronize SID to SIDHistory and passwords, enabling a seamless transition.

### Microsoft 365

Designed with Microsoft 365 and Entra ID in mind, PowerSyncPro supports Microsoft 365 tenant-to-tenant migrations acquisitions and divestitures. PowerSyncPro Migration Agent can take workstations from Hybrid Entra joined to Entra joined either in the same tenant or cross tenant.

## Release Notes

Current GA versions release notes are available here:

<https://downloads.powersyncpro.com/current/PSPMA-ReleaseNotes.pdf>

## Introduction

---

This configuration guide assumes that you have successfully completed the PowerSyncPro Server installation and prerequisites including any required firewall changes and DNS changes to support network requirements and that you have created the appropriately permissioned source and target Service Accounts, Entra App registrations, SSL Certificates and any other Active Directory, Entra and Intune requirements to support your migration scenario.

This document does not seek to be a design document or provide advice on project delivery.

Before configuration and deployment into a production environment you should complete your requirements gathering and design phase. A good understanding of Active Directory Domain join, Entra join and Intune enrollment is required to ensure you maximise the best possible result.

We would strongly recommend ensuring that you are able to meet your future device join state requirements manually first on pilot/test workstations in advance of using PowerSyncPro. Confirm that you have the correct configuration in place for your end-state and that your users are able to log in successfully and consume services in the target

## Prerequisites

<https://downloads.powersyncpro.com/current/PSPMA-Prerequisites.pdf>

## Installation Guide

<https://downloads.powersyncpro.com/current/PSPMA-InstallationGuide.pdf>



## Key Concepts

---

The PowerSyncPro Workstation Migration Agent is installed as a small agent on Windows workstations running as System and installed as a Windows Service. The Agent is an MSI installer and can be installed via any normal software deployment mechanism.

The migration agent periodically communicates with the backend PowerSyncPro server to receive instructions in the form of **Batches** and **Runbooks**. The workstation needs reliable connectivity to the PowerSyncPro server to retrieve and execute its migration instructions and return logging information. The PowerSyncPro server also provides the user translation mapping file required for repermissioning.

- **Runbooks** contain the core execution steps and phases of your workstation Migration that include Startup, Device State, Permission Updates, Application Reconfiguration and Completion as well as the ability to configure the User Experience to support multilingual capabilities.
- **Batches** include the Runbooks and the scheduled date and time to execute those runbooks, and the set of computers that this runbook applies to.

When the runbooks execute, end-users, if they are logged in, will see notifications when the migration is due to start or is available and about the current progress. A Lock Screen image can be presented during the migration event if configured (recommended).

All steps that are run on the devices are recorded to the Windows Application Event Log and rolled up to the PowerSyncPro Server.

At the end of the migration phases the Windows workstation will have left its source environment and be joined to a different target environment with the core Microsoft Applications reconfigured in fresh start mode. Device join state and application reconfiguration may vary depending on your specific use case.



## Global Settings

### Users

**Default User:** We strongly recommend changing the default Admin password at first logon, and then create dedicated logons for operators.

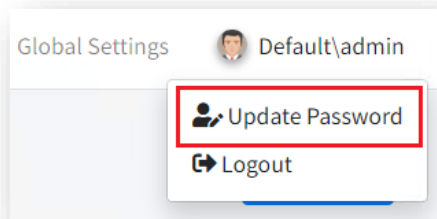


Figure 1 update Password and Logout

### Adding a User

From Global Settings, choose Users

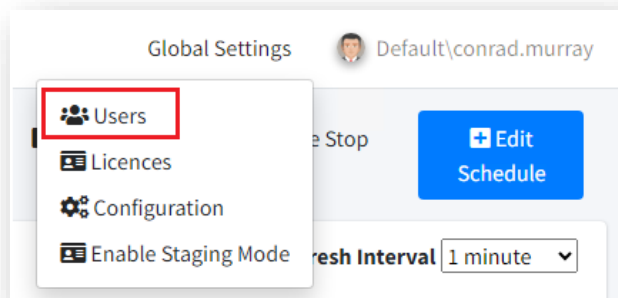
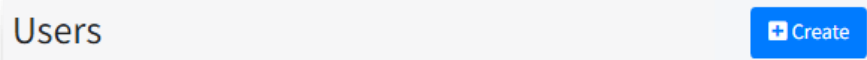
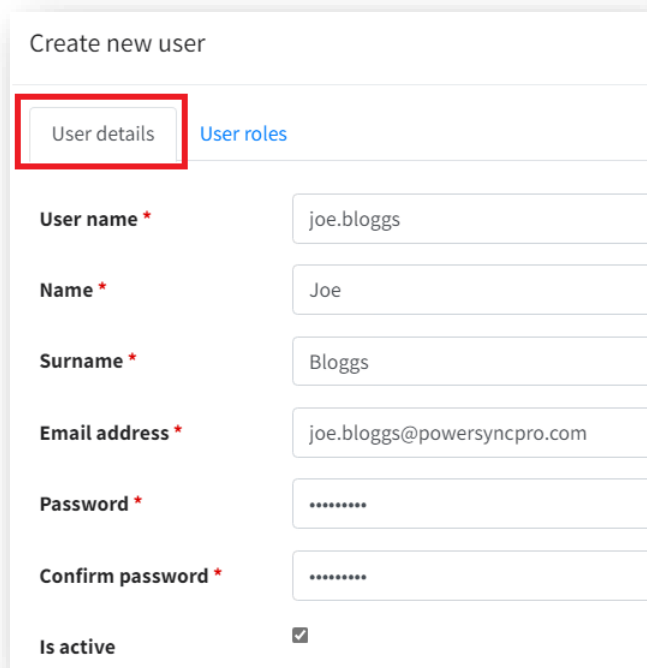


Figure 2 Add a User

And then Create







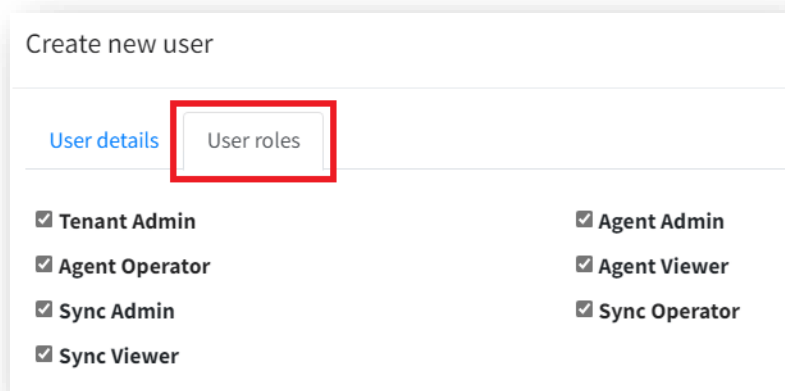
The screenshot shows the 'Create new user' form with the 'User details' tab selected. The form contains the following fields and values:

Field	Value
User name *	joe.bloggs
Name *	Joe
Surname *	Bloggs
Email address *	joe.bloggs@powersyncpro.com
Password *	.....
Confirm password *	.....
Is active	<input checked="" type="checkbox"/>

Figure 3 Create new user.

## User Roles

There are seven defined User roles available to choose from.



The screenshot shows the 'Create new user' form with the 'User roles' tab selected. The form displays seven roles, all of which are checked:

Role	Selected
Tenant Admin	<input checked="" type="checkbox"/>
Agent Operator	<input checked="" type="checkbox"/>
Sync Admin	<input checked="" type="checkbox"/>
Sync Viewer	<input checked="" type="checkbox"/>
Agent Admin	<input checked="" type="checkbox"/>
Agent Viewer	<input checked="" type="checkbox"/>
Sync Operator	<input checked="" type="checkbox"/>

Figure 4 PSP Users Roles

Role	Description
<b>Tenant Admin</b>	Overall admin within PowerSyncPro, including Tenant Settings, and adding and removing tenants. PowerSyncPro was designed to be multi-tenant but has never been tested that way and should not be configured in a multi-tenant configuration.
<b>Sync Admin</b>	Able to fully administer all screens in the Sync Service area of PowerSyncPro.
<b>Sync Operator</b>	Able to run the schedule but not update the configuration, able to view all screens in the Sync Service area of PowerSyncPro.
<b>Sync Viewer</b>	Able to view all screens in the Sync Service area of PowerSyncPro.
<b>Agent Admin</b>	Able to fully administer all screens in the Migration Agent area of PowerSyncPro.
<b>Agent Operator</b>	Able to schedule migrations but not update the configuration, able to view all screens in the Migration Agent area of PowerSyncPro.
<b>Agent Viewer</b>	Able to view all screens in the Migration Agent area of PowerSyncPro.

Figure 5 PowerSyncPro RBAC Roles

You may wish to consider **Agent Viewer** for some of your stakeholders that will not be migration operators.

### Agent Viewer

If you create a User with the Viewer Roles, this will change what options are available to the logged in user.

Create new user

User details

User roles

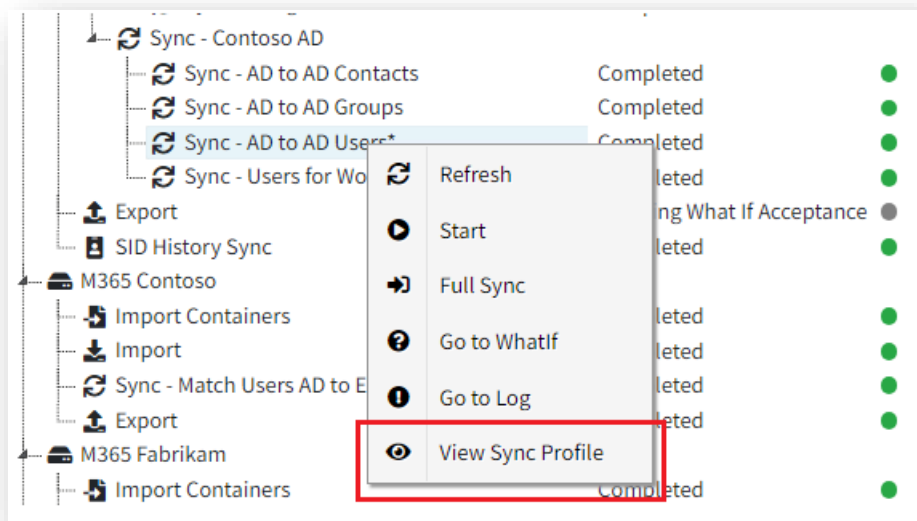
☐ Tenant Admin
 ☐ Agent Admin

☐ Agent Operator
 ☒ Agent Viewer

☐ Sync Admin
 ☐ Sync Operator

☒ Sync Viewer

e.g. Edit options will be hidden and 'Right click' options will change from Edit Sync profile to View Sync Profile



View only, Edit not available.

AD to AD Contacts	Contoso AD	Fabrikam AD	Contact	✕	Create Or Update	<a href="#">View</a>
AD to AD Groups	Contoso AD	Fabrikam AD	Group	✕	Create Or Update	<a href="#">View</a>
AD to AD Users	Contoso AD	Fabrikam AD	User	✕	Create Or Update	<a href="#">View</a>

## Licences

Your partner or PowerSyncPro directly will supply you with a valid licence key to support your deployment. Either Directory Sync only, workstation migration only, or both.

When requesting a licence you will need to provide the FQDN fully qualified domain name(s) of the Domain(s) in scope, and the Azure tenant name(s) (\*.onmicrosoft ) for Entra ID if being used - for all directories. e.g.

- contoso.local
- fabrikam.local
- consto.onmicrosoft.com

- [fabrikam.onmicrosoft.com](http://fabrikam.onmicrosoft.com)

Select “Tenant Settings” on top right of webpage and select “Licences”

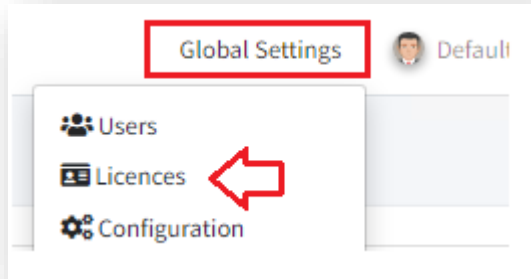


Figure 6 Tenant Settings, Licences

Click “Add” and paste in the licence key provided.

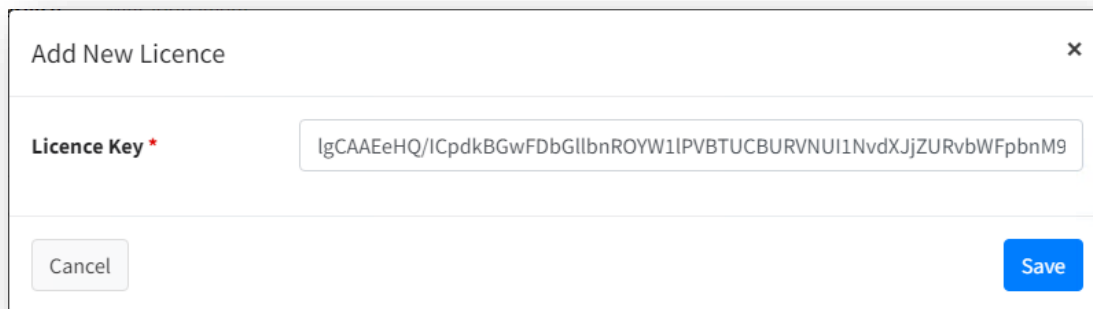
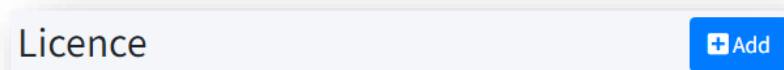


Figure 7 Add new licence.

One applied successfully your licenses will appear like this:



Name	Type	Source Domains	Target Domains	Device Count	Migration Expiry
PSP TEST	Sync, Migration	psptestsrc.local, psptestsrc.onmicrosoft.com, psptesttrg.local, psptesttrg.onmicrosoft.com	psptesttrg.local, psptesttrg.onmicrosoft.com, psptestsrc.local, psptestsrc.onmicrosoft.com	10000	01/01/2030

Figure 8 Successful Licence applied.

## Expired Licenses

The licence must be applied within 30 days otherwise it will expire, and you will see an error like below.

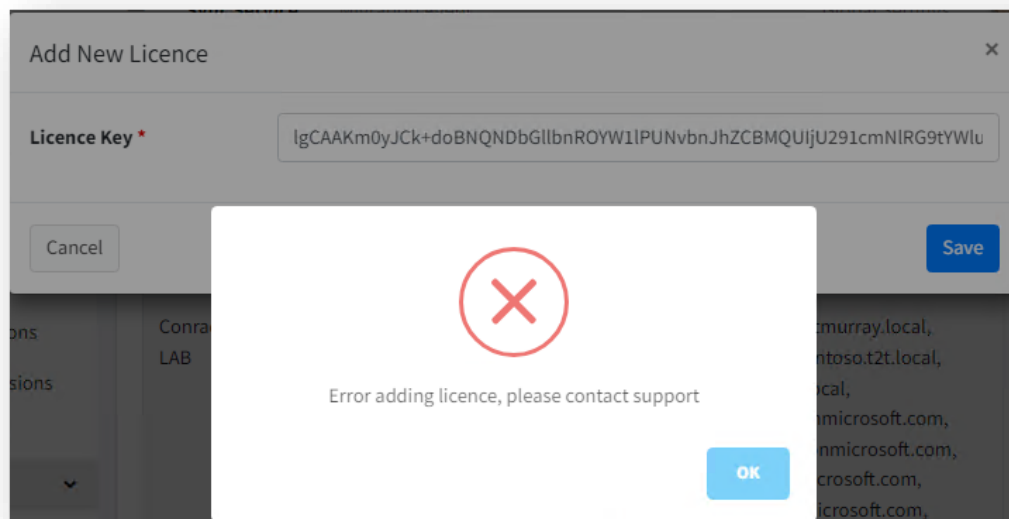


Figure 9 Expired Licenses



## Dashboard

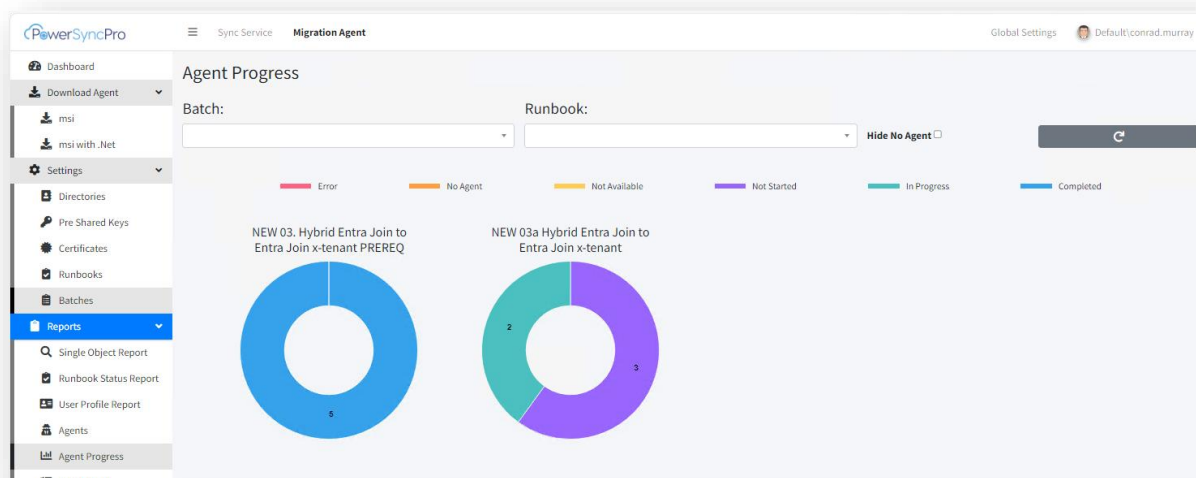


Figure 10 Dashboard.

The Dashboard gives a graphical representation of your overall batch progress. You can filter by Batch or Runbook. You can right click on the donuts to go directly to further detail or log information.

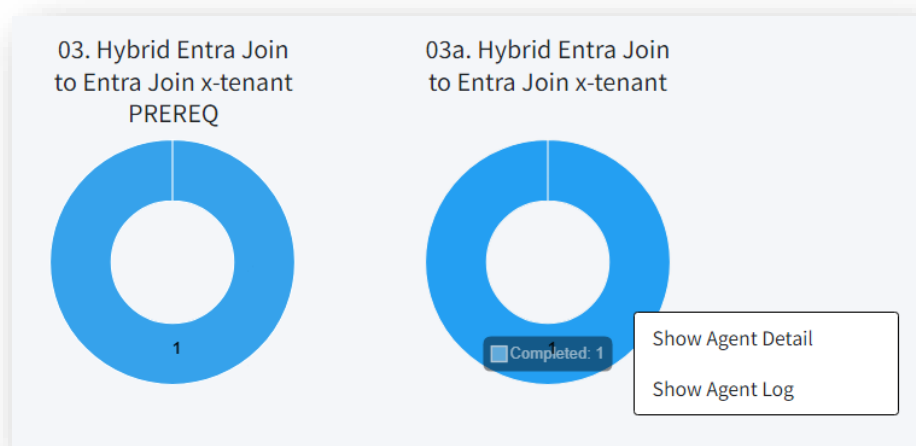


Figure 11 Progress donuts.

The lower sections of the dashboard will give you runtime statistics of devices in progress and which phase they are currently at.

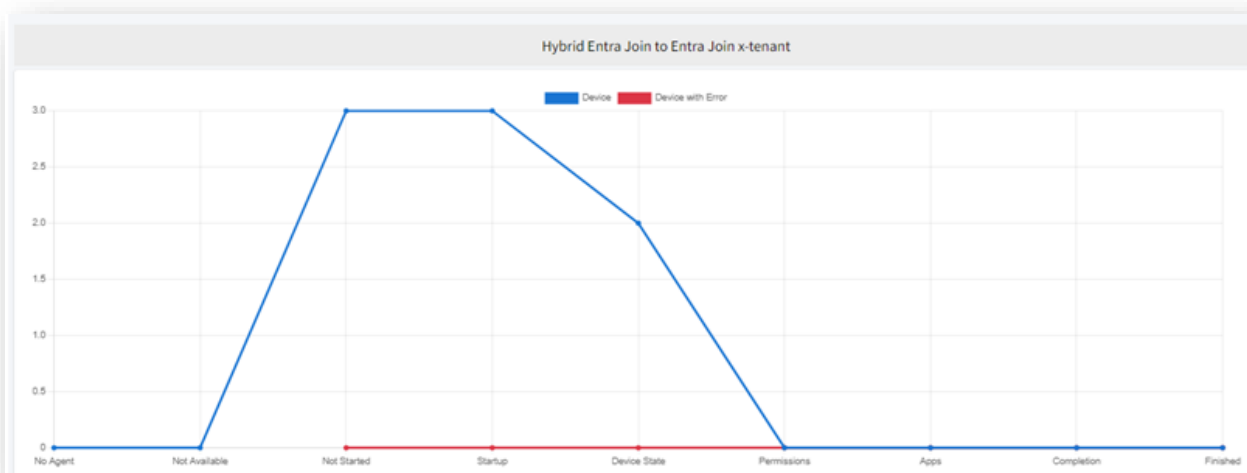
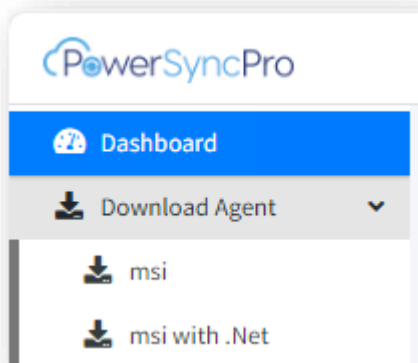


Figure 12 Progress graphs

## Download Agent



### msi

This MSI does **NOT** install the .NET 8.x Desktop Runtime prerequisites. You can use this if you already have the pre-requisites installed on the Windows workstations, or if you want to be able to patch .Net separately to the migration agent.

<http://localhost:5000/downloads/PSPMigrationAgentInstaller.msi>

## msi with .Net

This MSI contains the files it needs from the .NET 8.x Desktop Runtime. Due to this, the MSI is much larger. The installation will deploy the .NET Desktop Runtime files that are required in the **PowerSyncPro install directory only**, meaning .Net 8 Desktop Runtime will not show up in add/remove programs and can't be patched separately to the migration agent. This also means that if the Agent is uninstalled, it will remove these .Net files as well.

<http://localhost:5000/downloads/self-contained/PSPMigrationAgentInstaller.msi>

## Agent Installation

The installation of PowerSyncPro migration agent can be deployed via your preferred software deployment methods e.g. SCCM, Altiris, Intune, GPO etc.

Installation instructions for the agent are available here:

<https://downloads.powersyncpro.com/current/PSPMA-InstallationGuide.pdf>

## Settings

---

### Directories

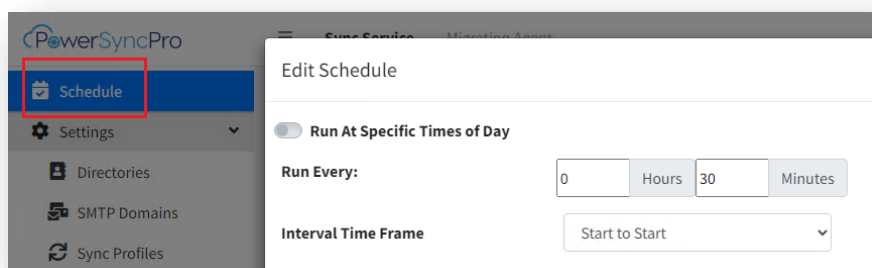
Please see the document PowerSyncPro Configuration Guide.pdf and review the Directories section there. <https://downloads.powersyncpro.com/current/PSPSync-ConfigurationGuide.pdf>

You must have configured your SOURCE directory at a minimum so that PowerSyncPro can import the devices you wish to work with. It is the Importing of devices that allows them to be selected as in scope for migration in batches.

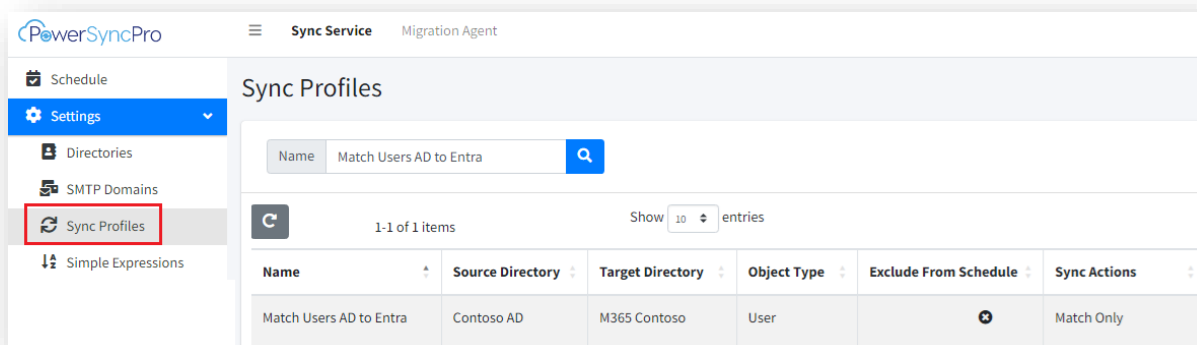
### Schedule

Be sure to enable the Schedule to suit your needs so that Users and Devices are imported to the PowerSyncPro Database regularly. The Schedule is not enabled by default.





## Sync Profile



If re-permissioning of profiles etc on workstations will be required i.e. you are migrating between different device join states, then you **must** have configured your SOURCE and TARGET directories so that PowerSyncPro can import the users you need to work with. Once your Directories have run an import, and you have correctly *scoped* users then they can become matched.

Therefore, you **MUST** have at least a Match only sync profile, (or a Create/Update Sync profile) for all the users that are in scope for your migration project.

It is the correct matching of users between Source and Target that builds a permissions mapping file, this is known as the User Translation Table.

The process of Matching users populates the [User Translation Table](#). The User Translation Table contains a record of the SIDs for each user. It is the SID that is used for looking up permissions on the Windows Profiles, registry keys, files, folders, shares, Windows Services, IIS and Scheduled Tasks that will be re-permissioned during the conversion of Windows user profiles on a device.

## Creating a Bulk Enrollment Token

The one additional step required in Directory Configuration to support migrating devices to Entra is configuration of a Bulk Enrollment Token. Go to your Entra ID Directory configuration profile and put it into Edit Mode. Click the “Generate Bulk Enrollment Token” option.

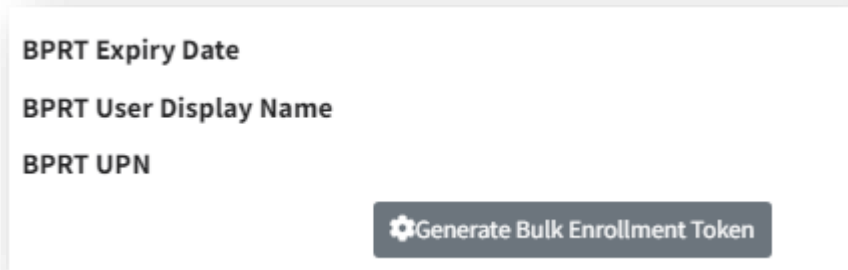


Figure 13 Generate Bulk Enrollment Token

- **Days Valid For:** The maximum Days Valid for is **180** – **do not exceed 180 days** as it will have no affect.
- **BPRT User Display Name:** Give it a meaningful name that so that is can be easily identified in your Entra ID

Click Generate

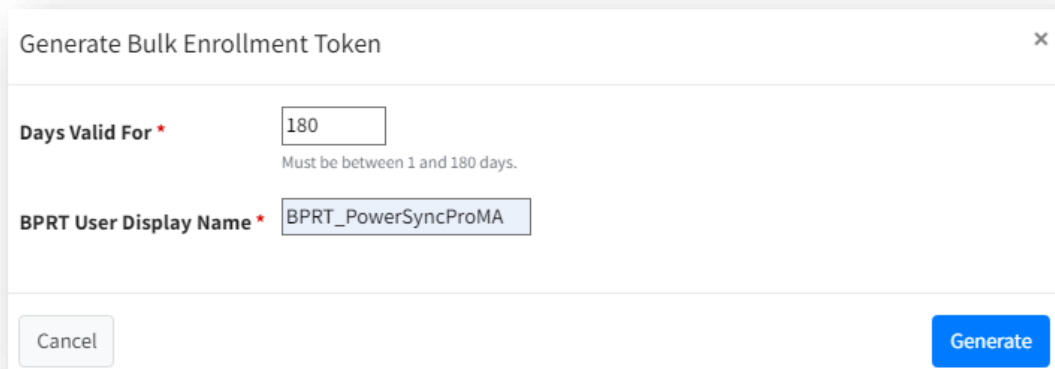


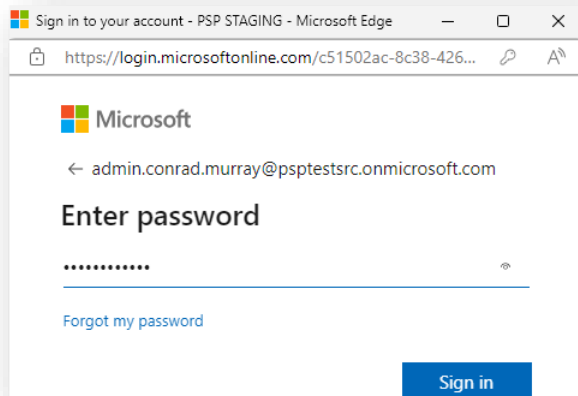
Figure 14 Generate Bulk Enrollment Token



You will be directed to a Microsoft Authentication browser pop up where you should sign in with an account that has sufficient rights to complete this task e.g. Global Admin.

**This account should not be from a federated domain.**

See <https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-bulk-enroll> for more details)



If your login is successful, you will be returned to the Directory Profile with the BPRT section populated. **Now click SAVE.**

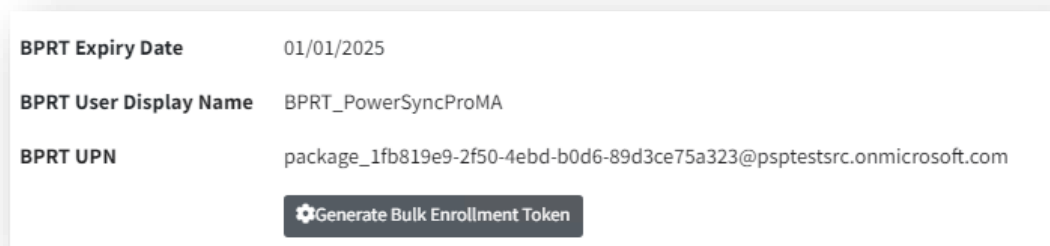


Figure 15 Bulk Enrollment Token created.

**Note:** You may on a rare occasion see this error when trying to create the Bulk Enrollment token: **"AADSTS90092: Non-retryable error has occurred"**



To fix this, you may need to create a Service Principal called Microsoft.Azure.SyncFabric.

Check to see if it exists:-

```
Get-AzureADServicePrincipal | Where-Object {$_.AppId -eq "00000014-0000-0000-c000-000000000000"}
```

Use this cmdlet to create it:

```
New-AzureADServicePrincipal -AccountEnabled $true -AppId 00000014-0000-0000-c000-000000000000 -AppRoleAssignmentRequired $False -DisplayName Microsoft.Azure.SyncFabric -Tags {WindowsAzureActiveDirectoryIntegratedApp}
```

## Bulk Enrollment Token Expiring

A Warning will be displayed when your bulk enrolment token is close to expiring.

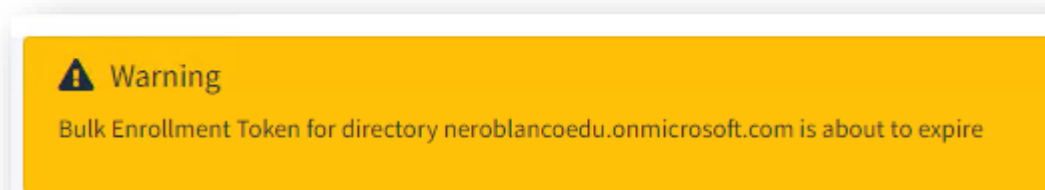
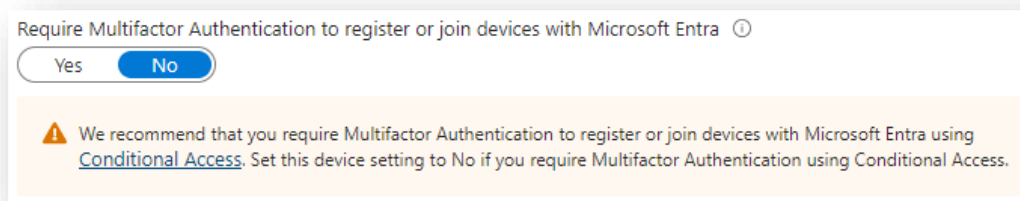


Figure 16 Bulk Enrollment Token close to expiring.

If you see this screen, you can simply generate a new Bulk Enrollment token. The previous one will remain. Runbooks will automatically be updated with the latest one.

**Note:** The setting in Entra: **Require Multifactor Authentication to register or join devices with Microsoft Entra** must be set to No for automated Entra join with PowerSyncPro to correctly execute.



## Pre Shared Keys “PSK”

During the installation of the workstation Migration Agent on devices you will be required to provide a pre shared key (PSK) to initially encrypt the communication between the agent and the PowerSyncPro server. After this initial communication, the Agent will download the certificate from PowerSyncPro and then create its own local Certificate.

### Create a PSK

Click Create from the Pre Shared Keys screen and then generate.

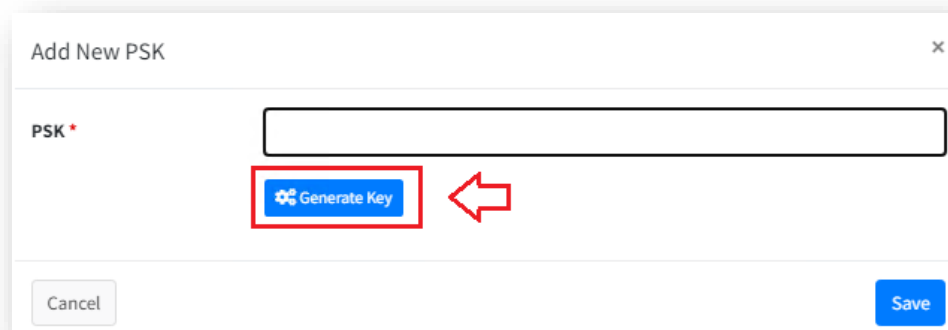
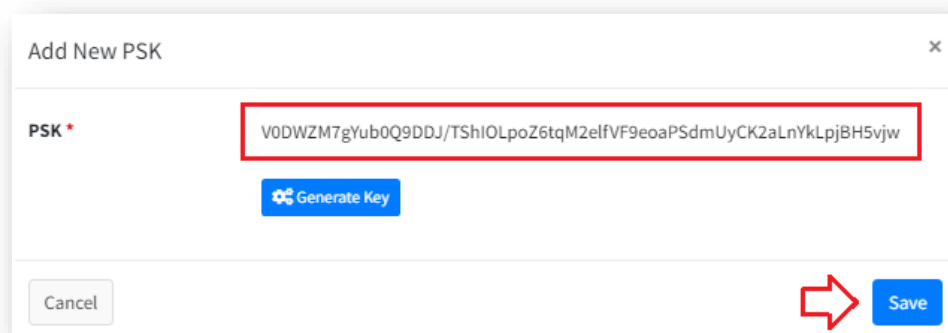
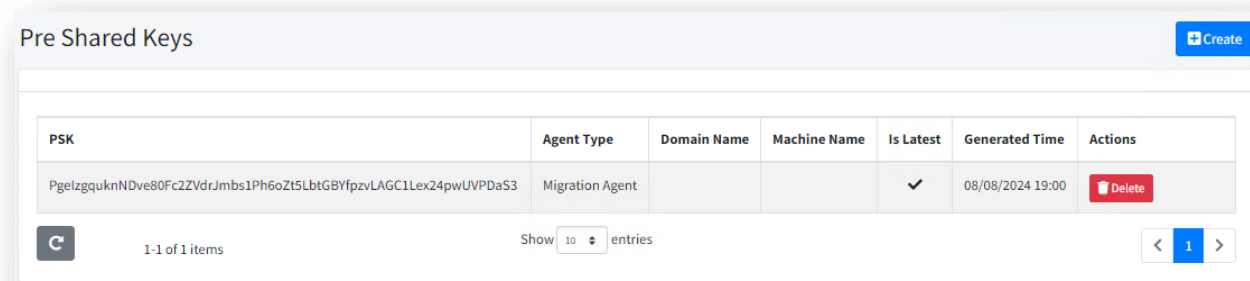


Figure 17 Generate a PSK



A dialog box titled "Add New PSK" with a close button (X) in the top right corner. It contains a text input field labeled "PSK \*" with a red asterisk. The input field contains the text "V0DWZM7gYub0Q9DDJ/TShiOLpoZ6tqM2elfVF9eoaPSdmUyCK2aLnYkLpjBH5vjw", which is highlighted by a red rectangular box. Below the input field is a blue button labeled "Generate Key" with a key icon. At the bottom left is a "Cancel" button, and at the bottom right is a "Save" button. A red arrow points from the "Save" button towards the bottom right of the dialog.

Figure 18 PSK generated.



A screenshot of the "Pre Shared Keys" interface. At the top right is a blue "Create" button. Below the title is a table with the following columns: PSK, Agent Type, Domain Name, Machine Name, Is Latest, Generated Time, and Actions. The table contains one row with the following data: PSK: PgelzguqnNDve80Fc2ZVdrJmbs1Ph6oZt5LbtGBYfpzvLAGC1Lex24pwUVPDaS3, Agent Type: Migration Agent, Domain Name: (empty), Machine Name: (empty), Is Latest: (checkmark), Generated Time: 08/08/2024 19:00, and Actions: Delete (red button). Below the table, there is a "Show 10 entries" dropdown and a pagination control showing "1" of 1 items.

PSK	Agent Type	Domain Name	Machine Name	Is Latest	Generated Time	Actions
PgelzguqnNDve80Fc2ZVdrJmbs1Ph6oZt5LbtGBYfpzvLAGC1Lex24pwUVPDaS3	Migration Agent			✓	08/08/2024 19:00	Delete

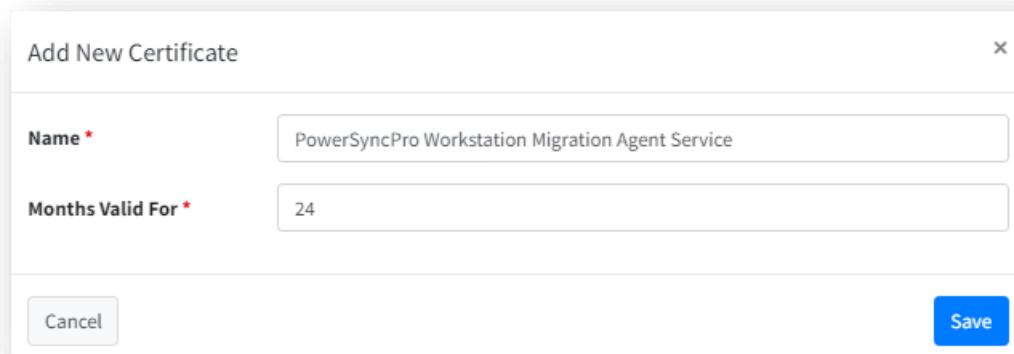
Figure 19 Successful PSK creation.

## Certificates

This Certificate is different to the SSL Certificate that is bound to the endpoint. The PowerSyncPro certificate is used after registration to sign and encrypt communication between the PowerSyncPro Service and the Remote Agent.

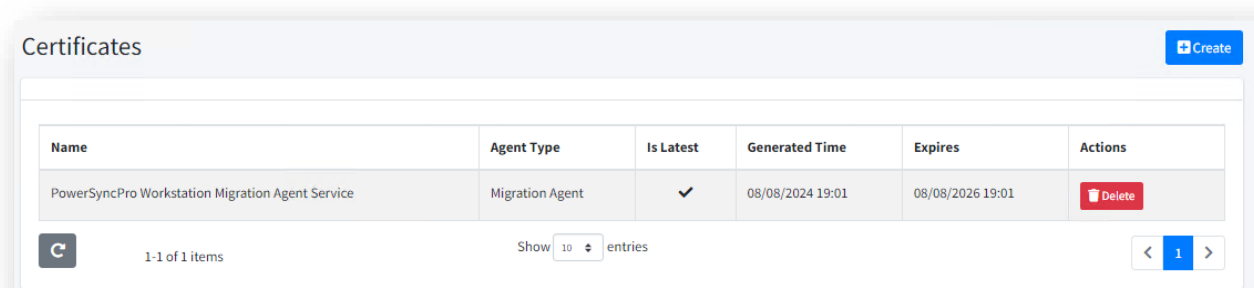
Click Create Certificate.

- **Name:** Defaults to **PowerSyncPro Workstation Migration Agent Service**. You can accept the default or choose your own.
- **Months Valid for:** Defaults to 12. You can choose a value that meets your business needs.



A dialog box titled "Add New Certificate" with a close button (X) in the top right corner. It contains two input fields: "Name \*" with the value "PowerSyncPro Workstation Migration Agent Service" and "Months Valid For \*" with the value "24". At the bottom, there are "Cancel" and "Save" buttons.

Figure 20 Add new Certificate.



A table titled "Certificates" with a "Create" button in the top right corner. The table has six columns: Name, Agent Type, Is Latest, Generated Time, Expires, and Actions. It contains one row for the "PowerSyncPro Workstation Migration Agent Service" certificate. Below the table, there is a pagination bar showing "1-1 of 1 items", a "Show 10 entries" dropdown, and navigation arrows.

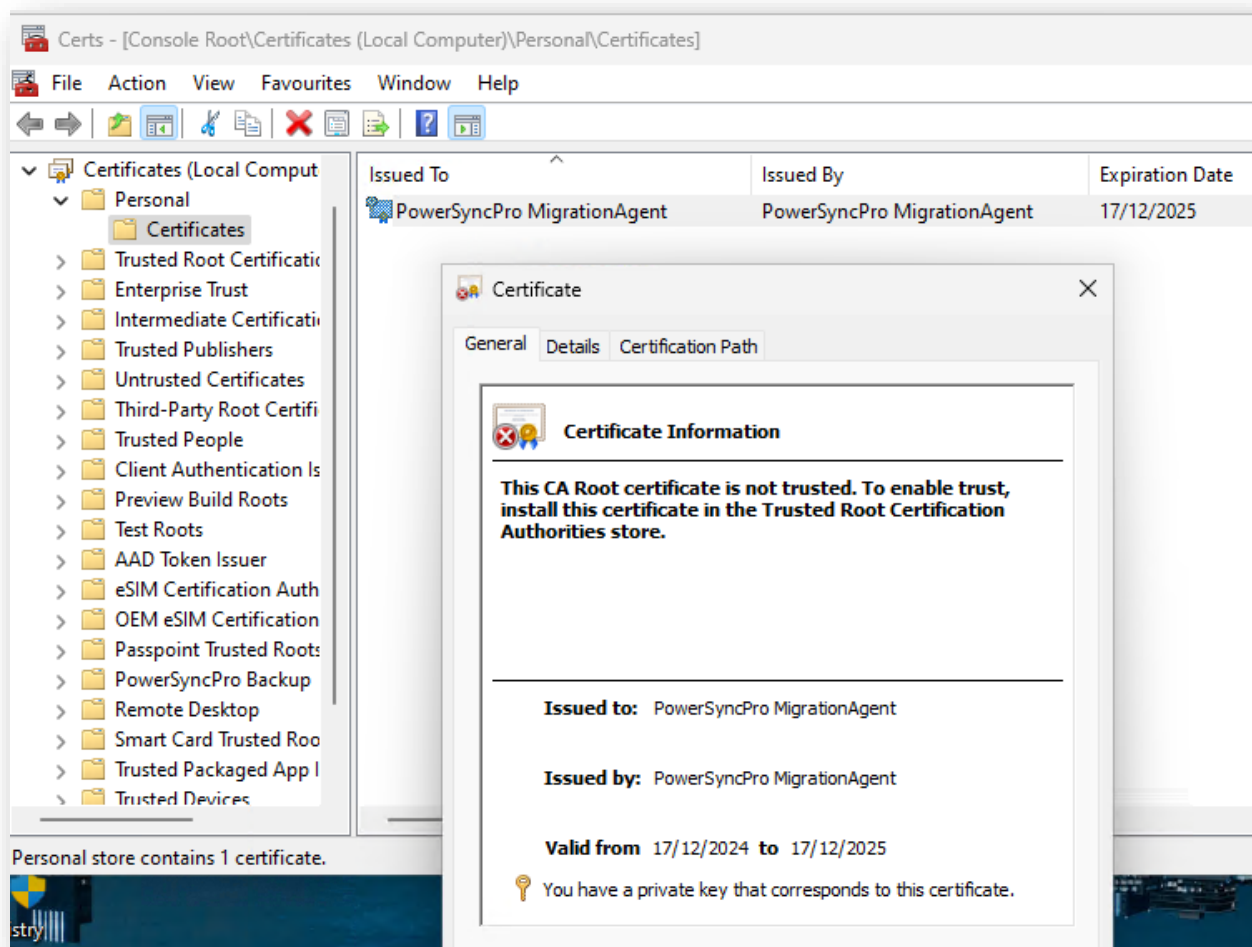
Name	Agent Type	Is Latest	Generated Time	Expires	Actions
PowerSyncPro Workstation Migration Agent Service	Migration Agent	✓	08/08/2024 19:01	08/08/2026 19:01	Delete

Figure 21 Successful PSP certificate creation.

## Local Certificate

After the Migration Agent is installed, you will see a new Certificate on the device like this:





## Runbooks

Runbooks contain the core execution steps of your workstation Migration. The choices you make here are the instructions sent to the device. Runbooks are added to Batches.

The Agent installed on your workstation will pull down its assigned runbooks per the Batch the workstation is assigned to immediately after it has registered. Initially it checks back with the PowerSyncPro server every 1, 2, 4, 8, 16, 32 minutes until it gets a batch assignment and then hourly after that.

If the workstation is not yet assigned to a Batch and therefore no Runbooks, it will contact the PowerSyncPro Server every hour to request updated configurations. Once the workstation had

been added to a Batch it will continue to contact the PowerSyncPro Server every hour to request updated Batch and Runbook information until its scheduled start time.

If the workstation is restarted, or the PSPMA Service is restarted, it will contact the PowerSyncPro Server to requested updated configurations.

Prior to a migration executing, the Agent will make one final call to the PowerSyncPro Server to check for any updated information, e.g. if it has been moved to a different Batch with a different start time, or that batch has been updated with a new Runbook. In this case it will execute on the latest information.

## Default Processing

While the runbook configuration screens contain choices of what to execute, some steps are automatically executed depending on the options chosen on the Device State tab. If the option to Remove from is set to “All Directories, Active Directory or Entra ID” then the following will be run.

Those are:

- Startup - Disabling the BitLocker protectors. If a device is BitLocker protected PowerSyncPro can still migrate this device by suspending the BitLocker protectors during the migration event.
  - Runs if a directory join option is selected (Unless **do not run start-up** is ticked)
- Startup - Backup Legal Notice
  - Always. (Unless **Do not run start-up** is ticked)
- Device State - Backing up All Local Group Members
  - Only if a leave directory option and a directory join option are selected
- Device State - Backing up AppX application
  - Only if a directory join option is selected
- Device State - Reset Windows Hello for Business
  - Only if a directory join option is selected

## Harvesting user Profiles

While the agent is on the device, it will audit the workstation for User Profiles and report these to the PSP Server. This information is available on the **User Profile Report** and can be used to assist with targeting Devices and Users together.

Machine Name	Directory Name	User Directory	User name	Profile Path	Last Local Logon Time	Object Sid
OMEGA1.contoso.t2t.local	CONTOSO	OMEGA1.contoso.t2t.local	conradmurray	C:\Users\conradmurray	03/09/2024 22:20:12	S-1-5-21-2475149661-411046844-1846898376-1001
OMEGA1.contoso.t2t.local	CONTOSO	contoso.t2t.local	admin.conrad.murray@contoso.t2t.dev	C:\Users\admin.conrad.murray	03/09/2024 22:28:10	S-1-5-21-986870641-247417481-986676165-1104
OMEGA1.contoso.t2t.local	CONTOSO	contoso.t2t.local	mickey.mouse@contoso.t2t.dev	C:\Users\mickey.mouse	03/09/2024 23:17:15	S-1-5-21-986870641-247417481-986676165-1154
OMEGA1.contoso.t2t.local	CONTOSO	contoso.t2t.local	andy.murray@contoso.t2t.dev	C:\Users\andy.murray	03/09/2024 23:16:44	S-1-5-21-986870641-247417481-986676165-1165
OMEGA1.contoso.t2t.local	CONTOSO	contoso.t2t.local	sarah.cooper@contoso.t2t.dev	C:\Users\sarah.cooper	03/09/2024 23:18:19	S-1-5-21-986870641-247417481-986676165-1168
OMEGA1.contoso.t2t.local	CONTOSO	contoso.t2t.local	John.Jones@contoso.t2t.dev	C:\Users\john.jones	03/09/2024 23:17:35	S-1-5-21-986870641-247417481-986676165-1169
OMEGA1.contoso.t2t.local	CONTOSO	contoso.t2t.local	jim.hopper@contoso.t2t.dev	C:\Users\jim.hopper	03/09/2024 22:43:36	S-1-5-21-986870641-247417481-986676165-4132

Figure 22 User Profile Report

## Creating a Runbook

### Name

Give your Runbook a meaningful name that can be seen in reports and when choosing in Batches.

### Source Directories

Source directories will default to listing all directories that you have configured. This is used in Batches to know which runbooks are available for selection in your Batch configuration, and also controls which domains it is going to check for the SIDs in that have been found on the machine to try to find a translation (e.g. in a multi-domain forest a machine may have SIDs from a different domain that the one that the machine is joined to). Generally you can just accept the default.

### Target Directory

This is the directory to which your workstation should be joined to. This also controls which BPRT token is presented in the Device State option. This is used in Batches to know which runbooks are available for selection in your Batch configuration

**Note:** If you are migrating to a different Microsoft 365 tenant, but your workstation is to become Entra Hybrid Joined, then your target Directory should be the target Active Directory for this selection, not the target Entra.

### Allow on Server OS

This is defaulted to **OFF** so that if an Agent is pushed accidentally to a Server, and that Server came into scope per a Batch, it still would not be executed.

### Prerequisite Runbooks

If you have defined a Runbook that should be run in advance of the main migration here is where it is listed. This runbook you are working with will not be executed unless the prerequisite runbook

has completed first. A Prerequisite runbook may contain steps like “Cache User Credentials” in advance of an AD to AD migration, or “Make OneDrive Files Cloud Only” a week in advance. (More on this later)

## Startup

### User Interaction

The choices are Silent Mode and Show Progress

- **Silent Mode:** The user will be unaware of any runbook execution. These will run silently in the background. This is typically used for prerequisite runbooks.
- **Show Progress:** User will see dialog screens such as Your migration is available, Your migration is about to start, Migration in Progress, Migration completed.

### Do Not Run Startup

This will not execute any of steps listed on the Startup tab – even if they are populated.

### Migration in Progress Image

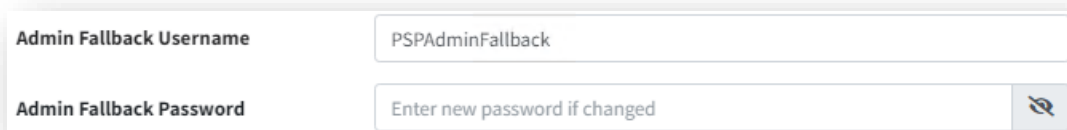
Optional **but Recommended:** This is a customization available that the user will see at the Lock Screen after the first reboot so that users are aware that a Migration is in progress.

**Users should NOT log in to their workstation whilst this screen is present. This can cause the repermission of the registry to fail.**

The Lock Screen image setting is cleared down when the migration completes. The users previous Lock Screen image will be restored and the user is able to log in at this point.

### Admin Fallback Account

Optional. If you include an account here, it will be created as a local workstation Account and added to the Local Administrators group on the workstation. It will persist during the migration event and will be deleted at the end of the migration event, unless you configure **Delay deletion of fallback account**



Admin Fallback Username	PSPAdminFallback
Admin Fallback Password	Enter new password if changed

Figure 23 Local Admin fallback account

### Admin Fallback Username

We recommend using this feature so that in the event of a migration failure you can login to the device to check the event logs and take any remediation actions. This can be especially vital when migrating workstations to Entra Joined because once a workstation is disjoined from its source AD or Entra, you may lose the ability to get back on to the device if it does not successfully join its target and you do not know the current local administrator password.

### Admin Fallback Password

This is the password assigned to the above Local Administrator account.

**NOTE:** The password complexity that you use here must match any policy requirements on the device, otherwise you will see an event log error like: *The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements* and will not be created.

### Delay deletion of fallback account by

Delay deletion of fallback account by  days

Optional: If you opt to create an admin fallback account from above, and leave this option as 0, the fallback account will be deleted at the migration completion phase. It may be preferable for your business and use-case to persist the fallback admin account during your post-migration support window e.g. 7 days allowing you a way to login to the device for troubleshooting. Valid values are whole numbers from 0 to 365.

### Command Package to Run

Here you can include a file to execute any valid commands on the device that will run as System. The file used here should be a compressed .zip file.

It must contain at least a file called **cmdline.cmd** plus any other associated files needed. Inside the cmdline.cmd file, you can list all the commands you wish to execute.

### Example 1

Here we are copying a PDF file that the user can refer to that will be in the C:\Migration folder and executing a PowerShell script called PreMigrationCleanUpScript.ps1

```
IF NOT EXIST C:\Migration (  
    MKDIR C:\Migration
```



```
)  
  
copy .\PreMigrationInstructions.pdf c:\Migration\PreMigrationInstructions.pdf  
/Y  
copy .\PreMigrationCleanUpScript.ps1  
c:\Windows\Temp\PreMigrationCleanUpScript.ps1 /Y  
  
start /WAIT PowerShell.exe -ExecutionPolicy Unrestricted -File  
c:\Windows\Temp\PreMigrationCleanUpScript.ps1
```

In this example, your ZIP file should contain all three files:

- cmdline.cmd
- PreMigrationInstructions.pdf
- PreMigrationCleanUpScript.ps1

## Example 2

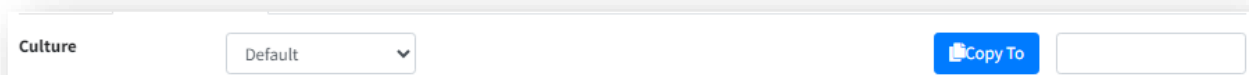
Here we are setting a legal notice banner during the migration in addition to the lock screen image you may have configured earlier to create another gate for users to discourage them from logging in before the migration has completed.

This would just be two lines in a cmdline.cmd file

```
reg add  
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"  
/v legalnoticecaption /t REG_SZ /d "MIGRATION IN PROGRESS" /f /reg:64  
  
reg add  
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"  
/v legalnoticetext /t REG_SZ /d "Your migration has not completed yet. Are  
you sure you still wish to sign in? Continuing beyond this point could cause  
your migration to fatally fail" /f /reg:64
```

## User Experience

### Culture



This setting allows PowerSyncPro Migration Agent to present notifications to your end users based on their local language. To use this feature you need to populate the language culture code in ISO

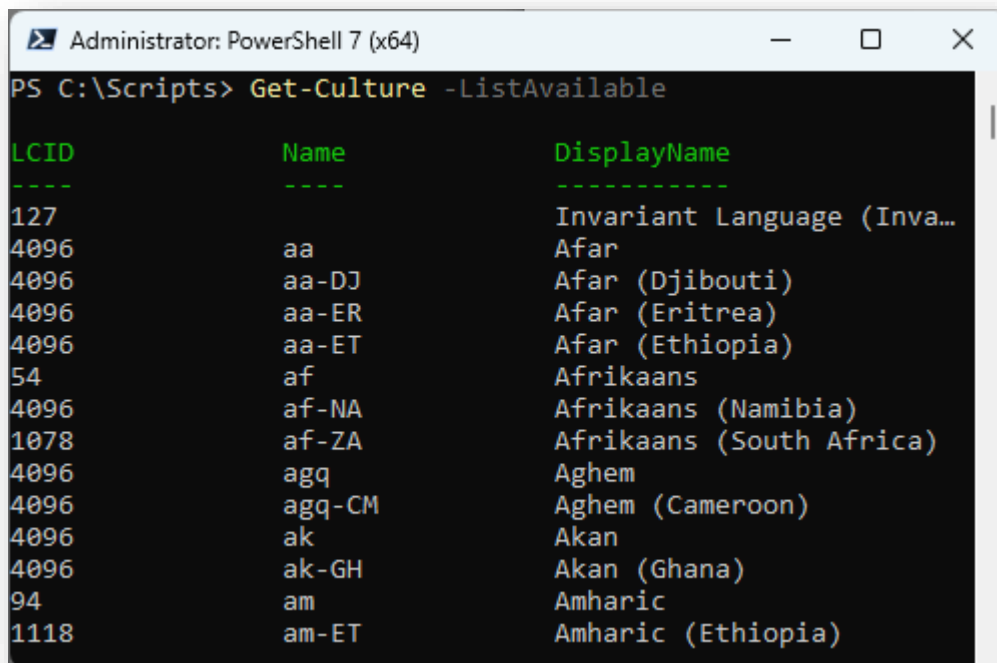
format to the “Copy To” box. This will create a duplicate of the current PSP User Experience culture to which you can then make language specific changes so that your end users will see the messages and notifications in their own language. What the end user will see will be determined by the settings on their own workstation.

To find the correct culture code to use, you can run this at Windows PowerShell. It is the “Name” value that you will need.

```
[System.Globalization.CultureInfo]::GetCultures([System.Globalization.CultureTypes]::AllCultures) | Sort-Object DisplayName | Select-Object Name, DisplayName, IetfLanguageTag | Format-Table -AutoSize
```

In PowerShell 7

```
Get-Culture -ListAvailable | Sort-Object DisplayName | Format-Table -AutoSize
```



```
Administrator: PowerShell 7 (x64)
PS C:\Scripts> Get-Culture -ListAvailable

LCID      Name      DisplayName
----      -
127       Invariant Language (Inva...
4096      aa        Afar
4096      aa-DJ     Afar (Djibouti)
4096      aa-ER     Afar (Eritrea)
4096      aa-ET     Afar (Ethiopia)
54        af        Afrikaans
4096      af-NA     Afrikaans (Namibia)
1078      af-ZA     Afrikaans (South Africa)
4096      agq       Aghem
4096      agq-CM    Aghem (Cameroon)
4096      ak        Akan
4096      ak-GH     Akan (Ghana)
94        am        Amharic
1118      am-ET     Amharic (Ethiopia)
```

For each Culture that you use “Copy To”, the Culture drop-down list will increase



Startup | User Experience | Device State | Permission Updates | App Reconfiguration | Completion

**Culture** fr-FR Delete Culture Copy To

**QR Code Url** am.com/information

☒ Cache Credentials ☐ Migration Available ☐ Migration Starting ☐ Migration In Progress ☐ Migration Complete

Item	Value
Window Title	Informations d'identification du cache
Main Message	Nous migrons vers le domaine <b>**{TargetDomain}**</b> . Veuillez contacter ((IT Service Desk) (mailto:emailaddress@contoso.com)) pour obtenir de l'aide.

## QR Code URL

Here you can optionally configure a URL that will be presented to users as a QR code that they can scan from a mobile device. This can be useful if you need to provide additional information about the migration. E.g. Next Steps, Support information, how to configure a mobile device etc.

Each user experience section is appended with a # anchor, so if you use anchors in your landing page that match the user experience headings then users will be taken directly to it via each QR code they see

e.g. <https://migration.fabrikam.com/information>

**QR Code Url** https://migration.fabrikam.com/information

will become like this in the QR code.

<https://migration.fabrikam.com/information#CacheCredentials>  
<https://migration.fabrikam.com/information#MigrationAvailable>  
<https://migration.fabrikam.com/information#MigrationStarting>  
<https://migration.fabrikam.com/information#MigrationInProgress>  
<https://migration.fabrikam.com/information#MigrationComplete>  
<https://migration.fabrikam.com/information#ServiceUnavailable>

## No QR Code Required

If you NOT want any QR code to be shown at all, then you should simply clear the default value and have it equal to NULL i.e. blank

QR Code Url

## Cache Credentials

Cache Credentials	Item	Value
<input type="checkbox"/> Migration Available	Window Title	Cache Credentials
<input type="checkbox"/> Migration Starting	Main Message	We are migrating to the **{TargetDomain}** domain. Please contact ((IT Service Desk) (mailto:emailaddress@contoso.com)) for support.
<input type="checkbox"/> Migration In Progress		
<input type="checkbox"/> Migration Complete		

Cache credentials are used when performing an AD-to-AD migration and where the Offline Domain Join “ODJ” option is chosen. You should not choose this option when migrating to Entra.

Cache Credentials





Please provide your login details for the charlie.local domain, this will ensure you will be able to log on after the migration. If you are not the primary user on this machine, then please press cancel and ask the primary user to complete this step by logging on and waiting for this prompt.

Username

Password

We are migrating to the **charlie.local** domain. Please contact [IT Service Desk](#) for support.

If a user enters the wrong target credentials or the target Domain controller cannot be reached you will see an error like this:

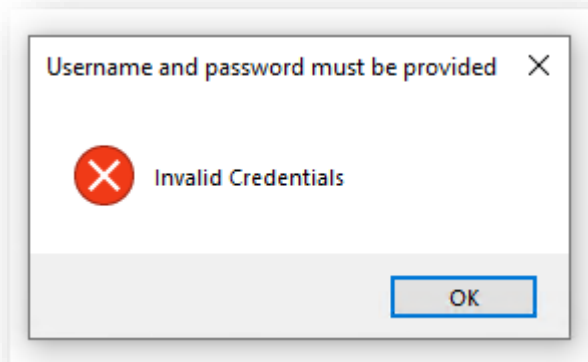


Figure 24 Invalid Cache Credentials entered



## Migration Available

QR Code Url

https://powersyncpro.com/powersyncpro-migration-agent/

Cache Credentials

**Migration Available**

Migration Starting

Migration In Progress

Migration Complete

Service Unavailable

Item	Value
Window Title	Migration Available
Main Message	<div> A migration is available to be run.  Please save your work and start the migration now, or wait until a better time.   The migration will be forced to occur at: {StartDate}. </div>
Snooze Label	or, snooze until
Snooze Button	Snooze
Snooze 5 Minutes	<div>5</div> <div>Minutes</div>
Snooze 15 Minutes	<div>15</div> <div>Minutes</div>
Snooze 30 Minutes	<div>30</div> <div>Minutes</div>
Snooze 1 Hour	<div>1</div> <div>Hour</div>
Snooze 4 Hours	<div>4</div> <div>Hours</div>
Snooze 1 Day	<div>1</div> <div>Day</div>
Snooze 1 Week	<div>1</div> <div>Week</div>
Start Button	Start

Figure 25 Migration Available user experience.

If you have opted to allow users to opt in to a migration by taking advantage of the “Available From” in a batch, then when that date and time have passed users will be notified that their migration is available to run.

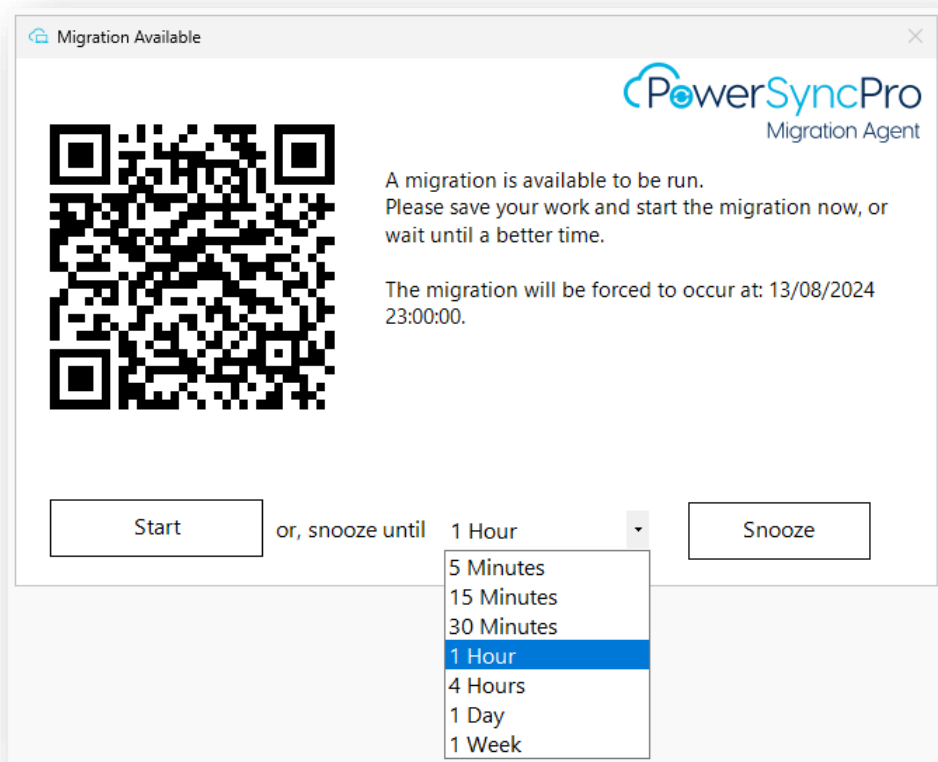


Figure 26 Migration Available example.



## Migration Starting

QR Code Url											
<a href="https://powersyncpro.com/powersyncpro-migration-agent/">https://powersyncpro.com/powersyncpro-migration-agent/</a>											
<div>Cache Credentials</div> <div>Migration Available</div> <div><b>Migration Starting</b></div> <div>Migration In Progress</div> <div>Migration Complete</div> <div>Service Unavailable</div>	<table border="1"> <thead> <tr> <th>Item</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Window Title</td> <td>Start Device Migration</td> </tr> <tr> <td>Main Message</td> <td> <p>Your device migration will start in {0} minutes. Please save your work.</p> <p>Do you want to start your device migration now? If so click Yes, otherwise click No</p> </td> </tr> <tr> <td>Yes Button</td> <td>Yes</td> </tr> <tr> <td>No Button</td> <td>No</td> </tr> </tbody> </table>	Item	Value	Window Title	Start Device Migration	Main Message	<p>Your device migration will start in {0} minutes. Please save your work.</p> <p>Do you want to start your device migration now? If so click Yes, otherwise click No</p>	Yes Button	Yes	No Button	No
Item	Value										
Window Title	Start Device Migration										
Main Message	<p>Your device migration will start in {0} minutes. Please save your work.</p> <p>Do you want to start your device migration now? If so click Yes, otherwise click No</p>										
Yes Button	Yes										
No Button	No										

Figure 27 Migration Starting user experience.

If a user is logged in when their migration event is due to start, they will receive this notification. If this is the mandated migration event, they will be able to defer the migration for up to 60 minutes. After the 60 minutes the migration will run automatically. If the user clicks “No” here, they will get reminders at 45 minutes, 30 minutes, 15 minute, 10 minutes, 5 minutes, 2 minutes and 1 minute. This notification sits on top of all windows and cannot be closed by the user.



Figure 28 Migration starting example.

If no user is logged in when the migration is due to start, no countdown will occur and the migration will begin at its scheduled time.

## Migration In Progress

**QR Code Url**

☐ Cache Credentials  
☐ Migration Available  
☐ Migration Starting  
☒ **Migration In Progress**  
☐ Migration Complete  
☐ Service Unavailable

Item	Value
Window Title	Migration in progress
Main Message	Migration in progress, please wait..

Figure 29 Migration in Progress user experience.

When a migration commences, and a user is logged in they will see a notification that the migration is in progress. They should not attempt to interact with their device when this message is seen. This notification sits on top of all windows and cannot be closed by the user.

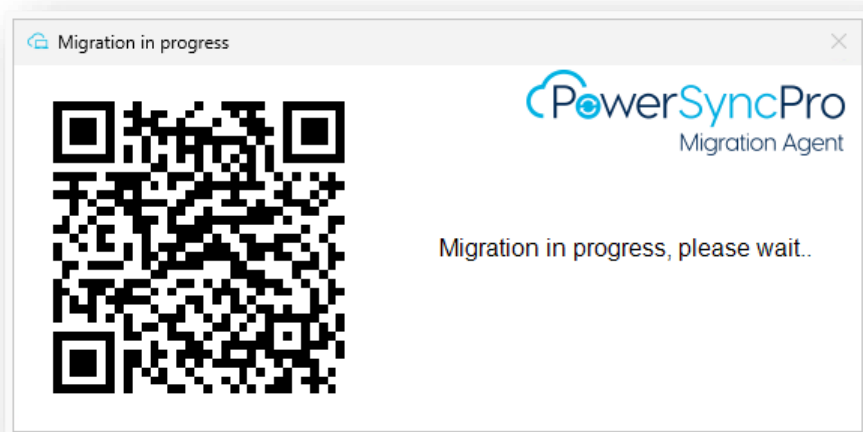


Figure 30 Migration in progress example.

Migration Complete

QR Code Url

https://powersyncpro.com/powersyncpro-migration-agent/

Cache Credentials

Migration Available

Migration Starting

Migration In Progress

**Migration Complete**

Service Unavailable

Item	Value
Window Title	Migration Complete
Main Message	The migration agent has now completed.
Ok Button	OK

Figure 31 Migration Complete user experience.

For every user profile found on the device that was migrated, each time they log in for the first time they will receive a confirmation notification that their migration successfully completed.

**Note:** If the Migration Agent is uninstalled in between a user logging in, this message will not be seen.



Figure 32 Migration Complete

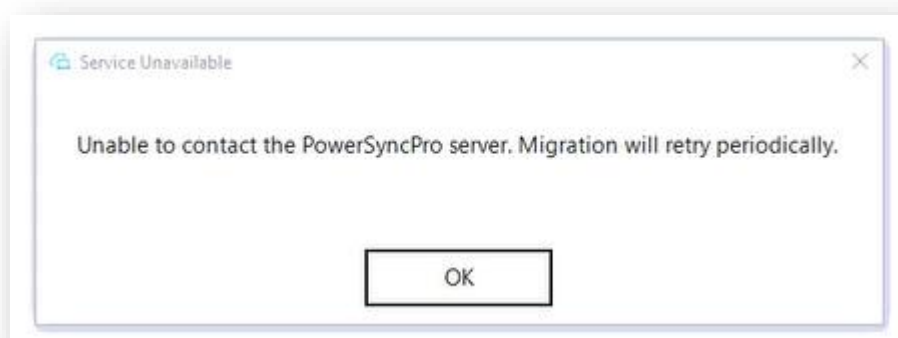
## Service Unavailable

QR Code Url	<input type="text" value="https://powersyncpro.com/powersyncpro-migration-agent/"/>	
<input type="checkbox"/> Cache Credentials <input type="checkbox"/> Migration Available <input type="checkbox"/> Migration Starting <input type="checkbox"/> Migration In Progress <input type="checkbox"/> Migration Complete <input checked="" type="checkbox"/> Service Unavailable	Item	Value
	Window Title	<input type="text" value="Service Unavailable"/>
	Main Message	<input type="text" value="Unable to contact the PowerSyncPro server. Migration will retry periodically."/>
	Ok Button	<input type="text" value="OK"/>

Figure 33 Service unavailable user experience.

When a migration attempts to start and execute, it will first check that it has a connection to the PowerSyncPro Server to get the latest Batch and Runbook information and be able to send up its logs during the migration event.

If the PowerSyncPro Server is unreachable, a notification will be displayed to the user if they are logged in.



The workstation Agent will continue to try to reach the PowerSyncPro. Those attempts will incrementally increase doubling the interval each time up to 64 minutes. i.e. 1, 2, 4, 8, 16, 32 and 64 minutes. The agent will continue to re-try every 64 minutes until either the service or workstation is restarted.



## Device State

The Device state tab controls how devices will be disjoined or joined to source and target. Not all options are displayed by default. Additional settings and configurations are presented depending on the type of migration you are performing.

We would strongly recommend ensuring that you are able to meet your future device join state requirements manually first on pilot/test workstations in advance of using PowerSyncPro to confirm that you have the:

- Correct configuration in place for your desired end-state
- Your users are able to log in successfully and consume services in the target
- That they are not blocked / restricted by unexpected policies, compliance requirements or other things such as VPN or mandatory software or minimum versions.

## Cache User Credentials

Tick this when you are performing AD to AD Offline Domain Join migrations. For a user to be able to successfully log in to their device after an Offline Domain Join migration, their credentials must be stored on the device at least once so that they are able to login without direct line of sight to their new target Domain Controller. i.e. they are a remote user. When running Cache Credentials the device must have ability to reach the target Domain Controller to validate those credentials.

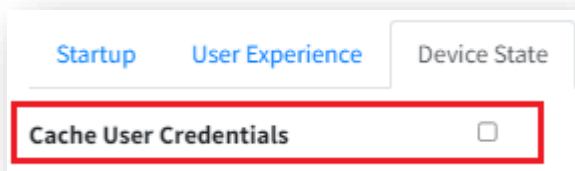


Figure 34 Cache credentials.

**NOTE:** Active Directory Trusts. If you are undertaking an Offline Domain Join migration you will need to have Active Directory Trusts in place for users to be able to Cache Credentials.

## Remove From

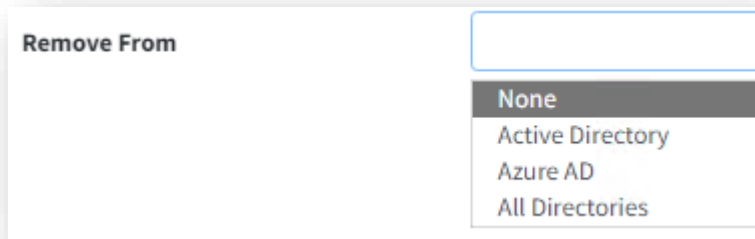


Figure 35 Remove device from options.

This is where you define how your workstation will be processed from its current join state.

### None

Do nothing with its current domain joined state. This will typically be your choice for prerequisite runbooks.

### Active Directory

This will update the device state to make it a WORKGROUP Device. This is like a domain disjoin. If you have machines in Hybrid state and you are migrating to another Active Directory where the device will become Entra Hybrid Joined then use the Remove From All Directories option instead of just Active Directory.

**NOTE:** This phase will not delete the device from the on-premises Active Directory nor mark the Computer account as disabled.

If there is a subsequent **Domain Join** step, it will perform that after it has processed the **Remove From** step. A reboot will be executed at this phase.

### Azure AD

This will update the device to no longer be joined to Entra and will also clear any Microsoft Intune Enrollments. This step is the same as running `dsregcmd /leave`. If there is a subsequent **Domain Join** step, it will perform that after it has processed the **Remove From** step. A reboot will be executed at this phase.

### Entra Join to Entra Join or CDJ

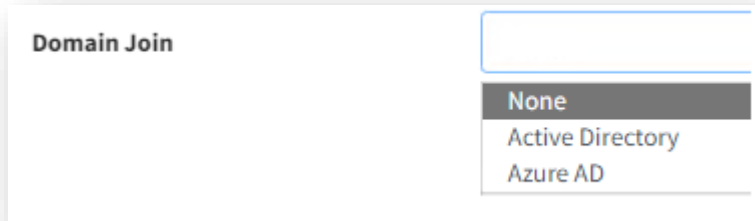
A use case for this option maybe be Entra Join to Entra Join device migrations, or where you are migrating the user and workloads to a different Microsoft 365 tenant, **but the**

workstation will continue to reside in its current Active Directory for the time being. See notes on CDJ later.

## All Directories

This is the combination of **Remove From** Active Directory and Azure AD from above.

## Domain Join



The screenshot shows a 'Domain Join' label next to a dropdown menu. The menu is open, displaying three options: 'None' (highlighted in dark grey), 'Active Directory', and 'Azure AD'.

Figure 36 Domain Join options.

## None

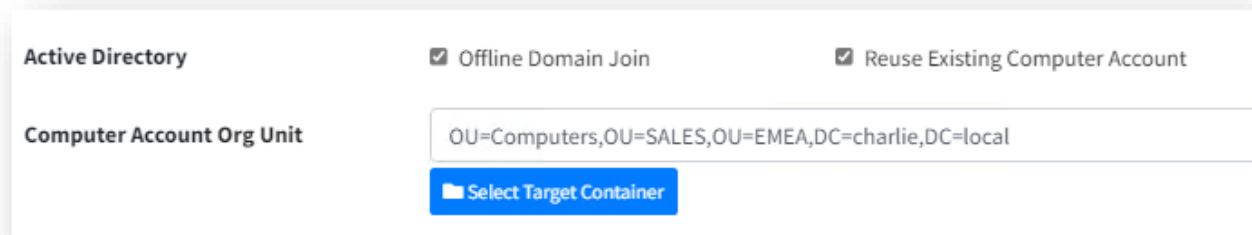
Do nothing with its current domain joined state. If you set **Remove From** to None because this workstation will continue to reside in its current Active Directory join state, then you would leave this set to none.

This will also typically be your choice for prerequisite runbooks.

## Active Directory

Chose this option if you are migrating to a different Active Directory. If you choose this option, then the following additional settings are required:

## Active Directory



The screenshot shows a configuration form for 'Active Directory'. It includes two checked checkboxes: 'Offline Domain Join' and 'Reuse Existing Computer Account'. Below these is a text field labeled 'Computer Account Org Unit' containing the value 'OU=Computers,OU=SALES,OU=EMEA,DC=charlie,DC=local'. A blue button labeled 'Select Target Container' is positioned below the text field.

Figure 37 Select target OU for AD Domain join.

## Offline Domain Join

If you choose Offline Domain Join “ODJ” you will need to have selected Cache User Credentials in a prerequisite runbook or ensure that you also select it in this same Runbook. The migration will not move forward if selected in the main runbook until the user has completed this step so this migration cannot be run unattended if they have not cached their credentials.

When you use ODJ as an option, the account listed on your target Directory configuration is responsible for contacting target domain controller and preparing the ODJ information. -The ODJ information is prepared at the time the migration is executed so the PowerSyncPro server must have a persistent connection to the target Active Directory.

### Offline Domain Join and Remote Sync Agents

Currently Offline Domain Join does not work when you have your Directory configured to use a Remote Sync Agent. To work around this, you should configure your Directory to classic mode.

## Reuse Existing Computer Account

If the computer account already exists in the target Active Directory, then you will need to tick this box.

Microsoft introduced security updates in October 2022 (KB5020276) to prevent unauthorized re-use of existing computer accounts during the domain join process. These updates are designed to mitigate vulnerabilities that could lead to a domain takeover.

If you do not select this option, and an identically named Computer account is found in the target, then the migration will stop at this phase and write an error to the Event Logs and PSP Server. The device state will be in WORKGROUP at this point.

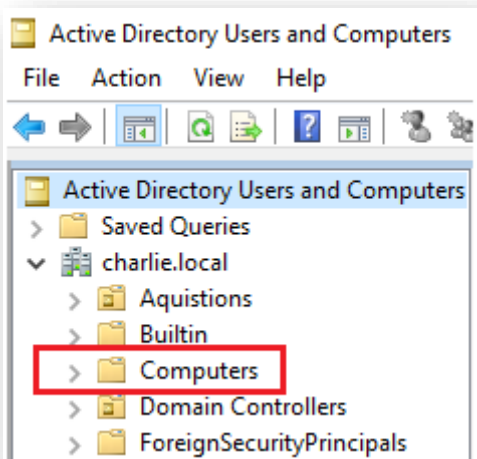
If you are migrating AD to AD, we would recommend performing an audit and discovery in advance to check for Computer name clashes.

## Computer Account Org Unit

This is the Organizational Unit (OU) in the target Active Directory where the computer account will be created.

**NOTE:** The Default root Computers object in Active Directory is not an OU. It is a Container. E.g. **CN=Computers,DC=fabrikam,DC=local**





Therefore you cannot list this as a target OU. If you need to use the Computers Container, then you should leave this value blank.

A form titled 'Computer Account Org Unit'. It features a single-line text input field that is currently empty. Below the input field is a blue button with a folder icon and the text 'Select Target Container'.

Figure 38 Leave blank for default computers container

When this value is blank, the Domain default for Computer account creation will be used. Typically this is the Computers container. If you have used the **redircmp.exe** tool then the default Computers container will be at another location.

## Domain Join Username

If you do not use Offline Domain Join, but instead will do the AD to AD migration in real time “online” then you must provide credentials for an account that has permissions to AD Join computers. The "Create Computer objects" permission.

- The minimum Active Directory privilege required to add a computer account into Active Directory is the "Create Computer objects" permission. This permission can be granted to a standard user or a group at the specific Organizational Unit (OU) level where the computer accounts are created.

- Delegated Permissions: If a user or a group needs to join more than 10 computers or if they need to join computers in a specific OU, they must be explicitly granted the "Create Computer objects" permission in that OU.
- Domain Admins: Members of the Domain Admins group have the necessary permissions by default to add computer accounts anywhere in the domain. We do not advocate using a Domain Admin account for this purpose.

## Domain Join Password

This is the password of the service account used above. You should take care to ensure this password does not expire, and if/when it is rotated that you remember to update it here.

## Rename Computers

Rename Computers

## Computer Name

If your use case is that you want or need to rename computers in the target, then you can use this option.

*Options: %SERIAL% for the device serial number or %RAND:X% to generate X number of random digits.*

**NOTE:** If you rename a computer using this method, it is the old computer name that will be seen in all PSP Server logs and other places.

## Set Hybrid Join Controlled Validation

This setting is used when you are migrating users and workloads between tenants, but NOT between Active Directories.

## Use Case

End state users will be connecting to a different tenant from what their source Active Directory hosting their computer is Entra Hybrid with.

Meaning that the source Active Directory has Entra Connect configured to synchronise Computers to Entra ID and is configured for Entra Hybrid Join. Workstations require Entra Hybrid Join in conditional access policies.

The target tenant you are migrating to, also requires workstations to become Entra Hybrid Joined and require Entra Hybrid Join in conditional access policies. However the workstation is still in the source Active Directory and has SCP information for the source tenant.

PowerSyncPro Migration Agent will, if configured, set the correct registry keys on the device so that it will skip SCP from the source AD and use local CDJ. Those registry keys are:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD.
  - Value name: TenantId
- HKEY\_LOCAL\_MACHINE\Key Path: SOFTWARE\Microsoft\Windows\CurrentVersion\CDJ\AAD.
  - Value name: TenantName

There is some extra work required for the target Entra Connect to sync in the source Active Directory computers, and you may need to make additional SCP configurations. This is a task for the project team. You can read more information here: [Targeted deployments of Microsoft Entra hybrid join - Microsoft Entra ID | Microsoft Learn](#)

## Hybrid Tenant Name

This is the \*.onmicrosoft.com name assigned to your tenant. You can get this information at the Microsoft 365 Admin Portal. Settings\Domains.

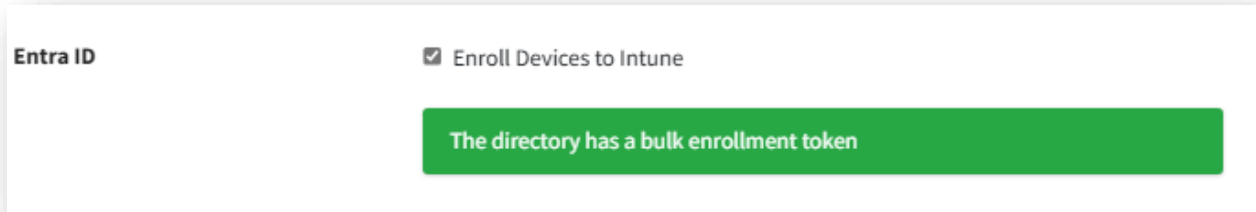
## Hybrid Tenant ID

This is the tenant Id. You can get this from Azure at [https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/ActiveDirectoryMenuBlade/~/\\_/Overview](https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/_/Overview) or Azure AD PowerShell using: (Get-AzureADTenantDetail).ObjectId or with Microsoft Graph PowerShell: (Get-MgOrganization).Id

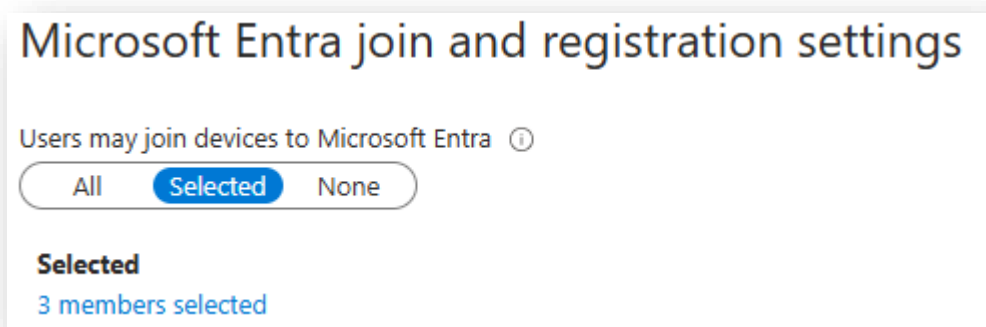
In your configuration, you would configure the device to leave Azure AD (Entra ID) but **NOT** Active Directory or All directories. You would set the target Domain Join to none.

Remove From	Azure AD
Domain Join	None
Set Hybrid Join Controlled Validation	<input checked="" type="checkbox"/>
Hybrid Tenant Name	pspfabrikam.onmicrosoft.com
Hybrid Tenant ID	d404cf81-40be-4c2b-af2a-0353ecf58683

## Entra ID



NOTE: When joining devices to Entra, the Bulk Enrolment Token MUST be able to join devices to Microsoft Entra.



If the above setting is not set to “All” then the Bulk Enrolment Account must be at least added to the selected members.

## Members allowed to join devices

PSP Contoso - Microsoft Entra ID

+ Add × Remove

Search

Type : 2 selected

Display name



User name



Type



BPRT\_20240217

package\_e7d0cce3-77da-45c9-80c1-439f5c0a6be4@t2t.dev

User

Devices that are joined to Entra ID will list the BPRT as the Owner. This is by design. You can update it afterwards following these instructions if you desire:

[https://powersyncpro.helpjuice.com/en\\_US/bprt-is-the-owner-workstation-in-entra](https://powersyncpro.helpjuice.com/en_US/bprt-is-the-owner-workstation-in-entra)

**NOTE:** Require Multifactor Authentication to register or join devices with Microsoft Entra must be set to No.

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

Yes

No

### The directory does not have a bulk enrollment token

The bulk enrolment token check is done against your directory configuration. You cannot proceed to complete a migration to Entra ID if no bulk enrolment token has been created. [See creating a Bulk Enrollment Token](#)

Azure Active Directory

☐ Enroll Devices to Intune

The directory does not have a bulk enrollment token

## Enroll Devices to Intune

PowerSyncPro Migration Agent cannot forcibly enroll a device, it is not possible to inject a device into Intune. Under normal operating conditions it is the scheduled task: "Schedule created by enrollment client for automatically enrolling in MDM from AAD" that is run once at user logon that attempts to enroll the device.

The option **"Enroll Devices to Intune"**, when selected, will check if the device is enrolled to Intune and report to the event log and PSP Server. If the agent sees that the device is not enrolled, it will call the DeviceEnroller.exe every hour until it sees that it has successfully enrolled and will update the event logs.

Enrolling a device to Intune requires your tenant to be correctly configure for Intune Enrollment and users to be correctly licensed (EMS) to be allowed to enroll devices into Intune. Enrollment will occur when the first valid user logs in and is repeated hourly until successful.

See here for Intune [Tenant Configuration](#) assistance and troubleshooting,

## Local Administrators Group

When a workstation is Entra joined it will add the GUID of the Global Administrator Role and the GUID of the Cloud Device Administrator Role to the Local Administrators Group.

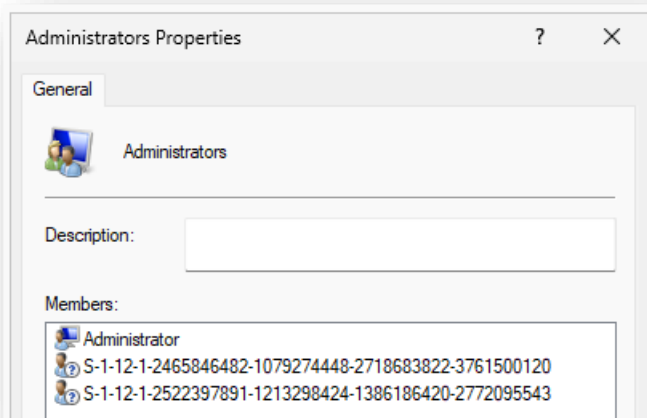


Figure 39 Local Administrators Group

If the user or group was explicitly previously a member of the Local Administrators Group then they will be translated to their target user account/group and retain Local Administrative privileges.

## Permission Updates

Startup User Experience Device State **Permission Updates** App Reconfiguration Completion

**Update Permissions**

☐ Don't update permissions  
☐ Only add permissions  
☒ Add and remove permissions

**Areas**

<input checked="" type="checkbox"/> Windows Profiles	<input checked="" type="checkbox"/> File Shares	<input checked="" type="checkbox"/> SQL
<input checked="" type="checkbox"/> File System	<input checked="" type="checkbox"/> Printers	<input checked="" type="checkbox"/> IIS
<input checked="" type="checkbox"/> Registry	<input checked="" type="checkbox"/> Services	<input checked="" type="checkbox"/> DCOM
<input checked="" type="checkbox"/> Local Groups	<input checked="" type="checkbox"/> User Rights	<input checked="" type="checkbox"/> Scheduled Tasks

**Areas to Ignore**

%SystemRoot%\\*  
%ProgramFiles%\\*  
%ProgramFiles(x86)%\\*  
\*:\System Volume Information\\*

### Update Permissions

- **Don't update permissions**

Use this when you are **NOT** moving a device between Active Directories or Entra Id. This is the default.

- **Only add permissions**

Use this when you only want to add the translated users/groups to the likes of File and Registry permissions. It is often used for file server migrations ahead of the domain being changed on the server.

- **Add and remove permissions**

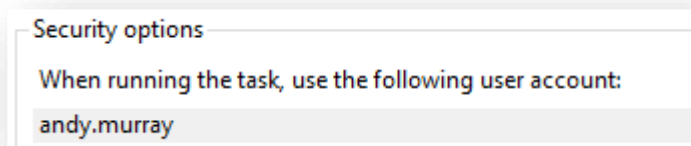
Use this when you are migrating devices between Active Directories or Entra Id.

### Areas

All the areas selected here will be re-permissioned based on the Update Permissions selected from above.

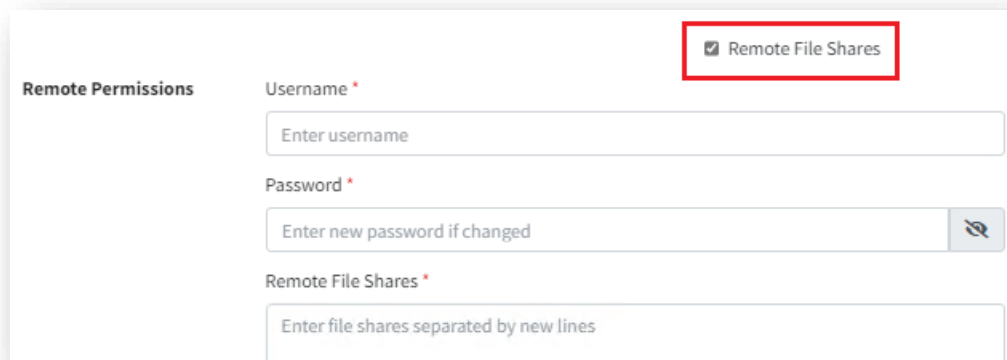
- Windows Profiles
- File System
- Registry
- Local Groups

- File Shares
- Local Printer Shares
- Services
- User Rights Assignment
- SQL Server Logons
- IIS
- DCOM
- Scheduled Tasks
  - As of version 3.1.24255.5 there is a known limitation migrating schedule tasks where the Security options have been configured to use a dedicated username with password.



- Remote File Shares

## Remote File Shares



**Remote Permissions**

☒ Remote File Shares

Username \*

Enter username

Password \*

Enter new password if changed

Remote File Shares \*

Enter file shares separated by new lines

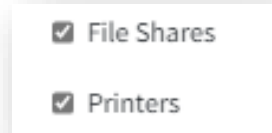
Figure 40 Configure Remote File Shares

PowerSyncPro can modify NTFS permissions based on the User translation Table for any remote file shares listed here, assuming that the master account defined has the appropriate rights to do so, and that the share is reachable for the duration of the migration event. PowerSyncPro can



repermission NTFS File Shares and NAS Devices. Windows Server can of course run the agent locally, but other OS flavours currently cannot and need a remote agent to do this work for them.

You do not need to use this option if you are repermissioning **LOCAL** printer or folder shares. You should use the File Shares and Printers option for this capability.



## Username

This should be the username of an account that has the appropriate rights to modify the share permissions of any remote file shares listed below.

## Password

This is the password of the account from above.

## Remote File Shares

This should be the explicit published full path of the shares you want to modify. You should take care to ensure that you use case sensitivity when appropriate if you are working with non-Windows devices like a NAS on UNIX share etc.

E.g.

[\\server\sales](#)

[\\server\marketing](#)

[\\server\hr\\$](#)

[\\server\d\\$\it\source](#)

[\\FRODONIX\LOTR\Gandalf](#)

You should not use drive letters here. e.g. S:\SoftwareLibrary\Office

## Areas to Ignore

Any areas listed here will not be processed by the Agent. The default areas are not required to be processed for repermissioning but you can also add others to meet your own use case and business needs.



## App Reconfiguration

App reconfiguration is limited to the Microsoft Application Suite: Office, Microsoft Teams, OneDrive for Business, OneNote and Edge browser. This section also allows to you reset a machines AIP current state.

### App Reconfiguration

#### App Reconfiguration

- ☐ Don't reconfigure applications  
☒ Reconfigure applications

- **Don't reconfigure applications**

Use this option when you are **not** moving a workstation between Microsoft 365 tenants or on-premises cross forest Exchange migrations. Typically, this might be when you are converting a device from on-premises AD joined and Hybrid Entra Joined to become only Entra Joined, or when you are moving a device between Active Directories but not changing the tenant the applications are connecting to.

- **Reconfigure applications**

Use this option when you are moving a workstation between Microsoft 365 tenants or between Active Directories where user would be connecting to a new on-premises Exchange.

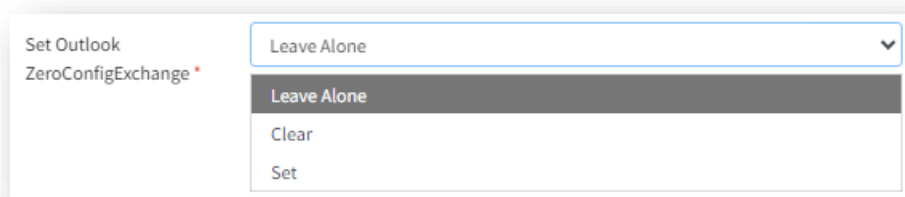
## Applications

### Outlook

This setting will reconfigure the Outlook application post-migration to be in the fresh start experience. For Outlook classic, the legacy profile data will be preserved but hidden. Outlook will start and prompt the user for their configuration details to create a new profile unless the organisation has opted to use Zero Configuration for Exchange.

### Set Outlook ZeroConfigExchange

This is an additional Outlook Configuration setting.



ZeroConfigExchange (ZCE) can be used to create new profiles for users with minimal user interaction. That is, the user does not have to enter any configuration data... only data that every user should already know (account name and/or password).

- Leave Alone
- Clear
- Set

Generally unless you know you have a specific need or configuration you can accept the default of “Leave Alone”

The source legacy Outlook profile will be hidden, but not deleted. When a user starts Outlook for the first time post-migration, they will be presented with the Outlook first start experience.

## Other M365 Apps

Other M365 Apps refers to the signed in Office Applications and resets the Office licensing/activation. It will also reset Microsoft Teams and OneNote to the fresh start experience.

## Edge Browser

The default work profile will be configured so that post migration the user is able to sign out and sign back in. The reason for doing this is that during that process the user can choose to merge the passwords, favourites, etc from the old account into the new account. This is a requirement if they wish to use a signed in Edge profile in the target tenant.

Users will need to sign out once and sign back in again to reactivate a signed in and synchronised browser profile.

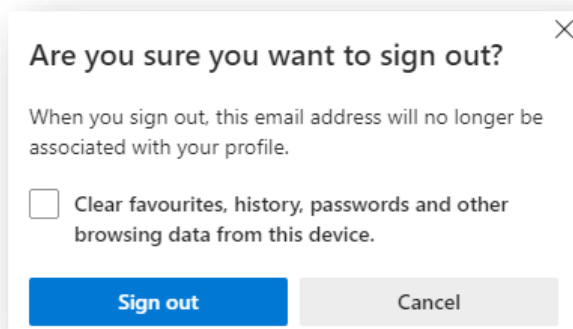


Figure 41 Sign out of Edge.

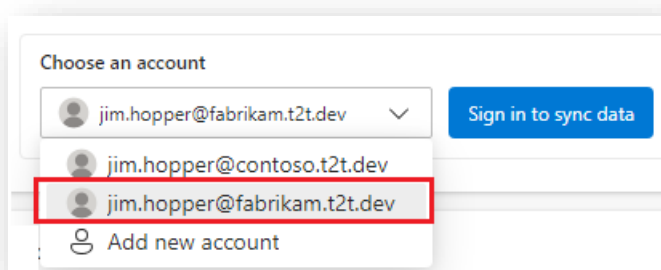


Figure 42 Sign in to Edge.

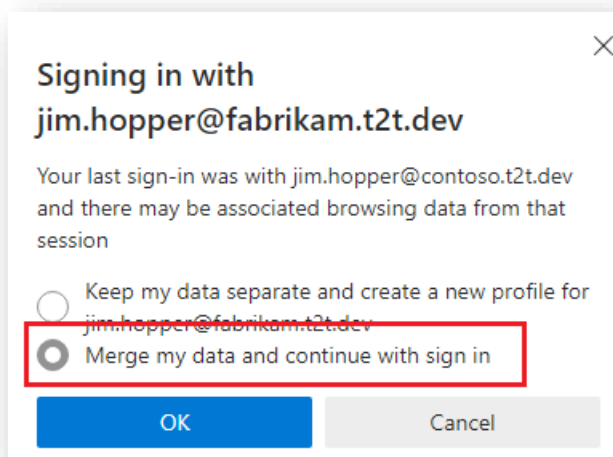


Figure 43 Merge Edge data.

## Make OneDrive Files Cloud Only

Typically, this option is used in prerequisite runbooks, to ensure that files are dehydrated before the account is unlinked.

We recommend running this prerequisite around a week before your migration event to ensure the maximum number of files are marked as files on demand.

### When this configuration is required:

If you are migrating a user between two Microsoft 365 tenants and you need to reset the Microsoft Applications on the device.

### Why this setting required:

If you do NOT configure this setting, then post-migration the user will have two instances of their OneDrive data. One instance will be their target OneDrive that will be their “Blue” folder – their real day-to-day OneDrive for Business working area. The legacy OneDrive folder will still be present with all the users legacy stale data.

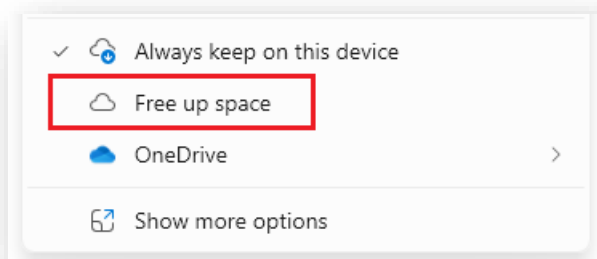


Users can be confused and may inadvertently start using data from the legacy OneDrive or save new data to the legacy OneDrive location. They may also be tempted to move all the legacy data to their target OneDrive overwriting later versioned data, or duplicating data if they nest it inside their target OneDrive.

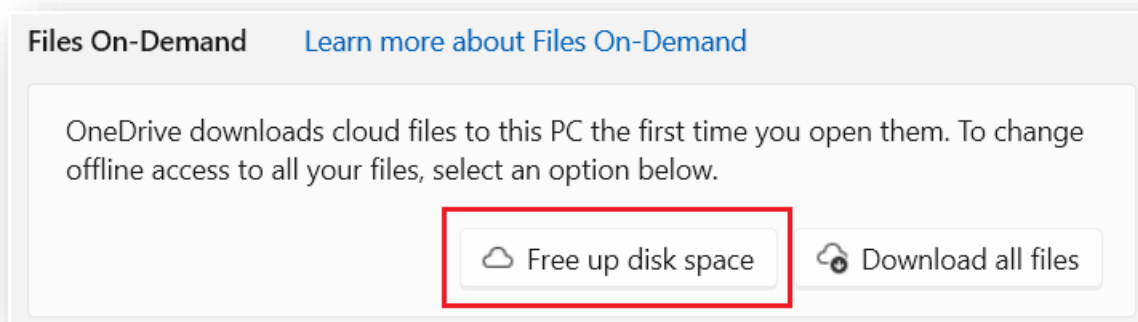
When you use this configuration pre-migration, the files and folders have their attribute marked as a stubbed “on-demand” item. When the migration runs, the OneDrive for Business accounts for the source tenant(s) listed in your configuration are disconnected and all stubbed items are removed.

## Files On-Demand

When this setting is used, all OneDrive synced items will be marked as “Files On-Demand” / Cloud Only”. This is the equivalent of setting “Free up space” in Windows Explorer.



Or



When this setting is enabled, ALL connected OneDrive syncs will be marked Cloud Only – including any SharePoint / Teams document libraries.

If consumer Personal OneDrive has been configured on the device, this will not be reconfigured.

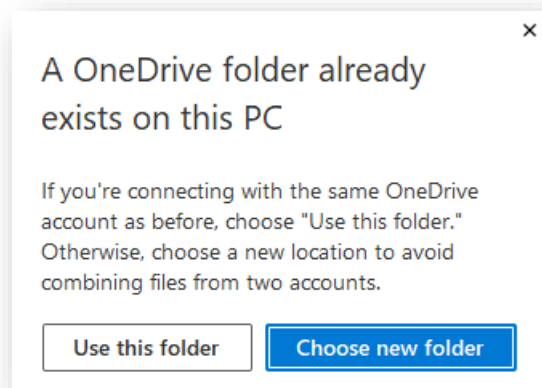
If another organisation OneDrive for business has been configured, and is not listed in your tenants, it will not be reconfigured.

If the user has been synchronising Teams or SharePoint document libraries for the tenants(s) listed these will be disconnected and will need to be reconfigured post migration. Any files that were not marked cloud only, will remain on the device in the original folder.



Any items that were not marked as Cloud Only are moved to the target OneDrive folder to ensure no data loss.

If any files are moved to the target OneDrive folder, users will see a message to use the exiting folder location. They should select **Use this folder** here.



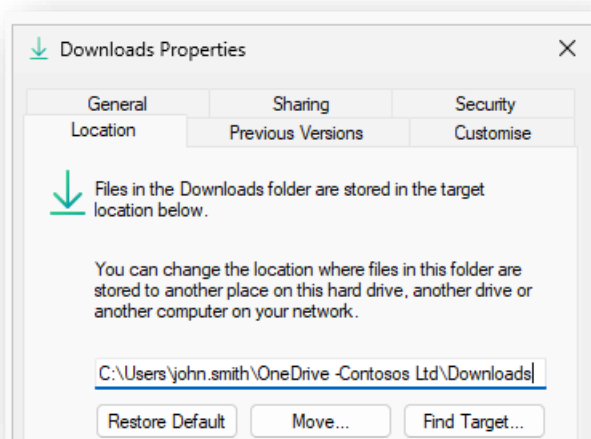
It is important to run this step since any files that are not marked as Files On-Demand will be copied to the target folder on the device. This could lead to duplicate files when sync occurs for the first time to the target OneDrive.

### Known Folder Move – KFM

If KFM has been configured in the source environment, this setting will be cleared. If it is configured in the target as a policy, then it will be re-applied as part of that policy post-migration when the user reconnects OneDrive for Business.

### User configured Folder Redirections

If the user has made additional folder redirections to OneDrive such as Downloads, Music or Videos, then the user will need to reapply those manual re-directions.



## OneDrive for Business

### Set OneDrive SilentAccountConfig

If you enable this feature, OneDrive.exe attempts to silently (without user interaction) sign-in to the work or school user account that was used to sign into Windows (known as the Windows Primary Account). That Windows account must be a Microsoft Entra account or be linked to a Microsoft Entra account through a hybrid authentication configuration.

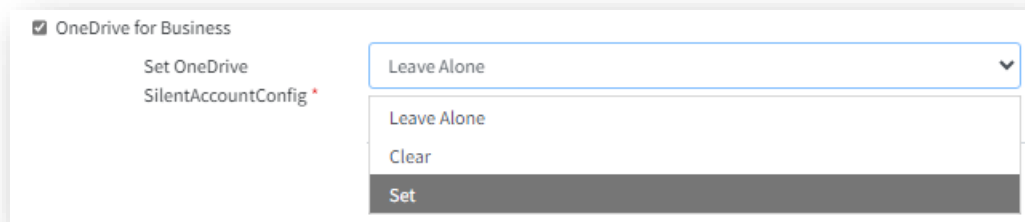


Figure 44 Set OneDrive SilentAccountConfig

### Options:

- Leave Alone
- Clear
- Set

Generally unless you know you have a specific need or configuration you can accept the default of “Leave Alone”




## Source Tenant(s)

Source Tenant(s) *	9bc4a702-2977-4d17-8f19-64d596b61cbe
--------------------	--------------------------------------

This setting refers to the clearing down of any connected OneDrive's on the device i.e. marking the files for on-demand and disconnecting the account. If you are listing multiple tenants here, each guid must be on a separate line.

This your Azure tenant ID value. This can be found at:

[https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/ActiveDirectoryMenuBlade/~/Overview](https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/Overview)

Basic information	
Name	PSP Contoso
Tenant ID	9bc4a702-2977-4d17-8f19-64d596b61cbe 

## Target Folder Name

Target Folder Name *	OneDrive - PSP Contoso
	'OneDrive - Company Name'

This value is critical to your OneDrive migration configuration. This value will be used to create the target OneDrive for Business folder name on the users workstation where non-stubbed items will be moved to.

This value configured as: 'OneDrive - [+ Organization information]'

Be careful to ensure that there are no leading or trailing spaces, and that you have “*space hyphen space*” after the OneDrive prefix and that it is a single hyphen/dash, not a MS Word autocorrected double dash

The Organization information is available at:

<https://admin.microsoft.com/Adminportal/Home#/Settings/OrganizationProfile/./Settings/L1/OrganizationInformation>

## Organization information

This info will be displayed in places like sign-in pages and bills to your organization.

[Learn more about editing your organization's info](#)

Name \*

PSP Contoso

## Azure Information Protection

Configuring this setting resets the user settings for the Azure Rights Management service. Use this option if you are migrating AIP keys between tenants as part of your project.

- The Windows workstation will be bootstrapped by PowerSyncPro to get the new keys/policies from the new tenant.
- AIP encrypted files will only open again from the target tenant providing they have been migrated correctly and that the AIP keys from the Source tenant have been added to the target tenant.
- When users connect to a rights protected document the first time in the target post-migration, they will see a screen like this.

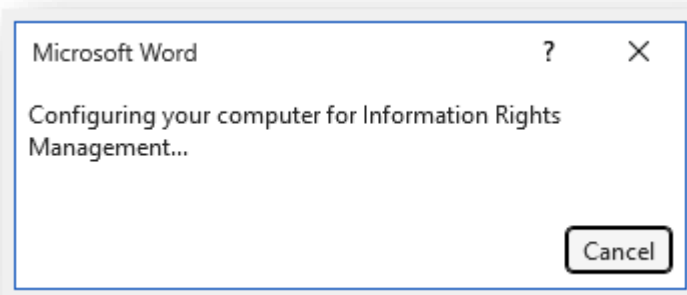


Figure 45 Configuring your Computer for Information Rights Management

## Configuration

☒ Azure Information Protection

Source Host(s) \*

Target Host \*

Figure 46 Reset user settings for Azure Rights Management

This value is your DistributionPointURL. This can be retrieved using PowerShell with:

```
Connect-AipService
Get-AipServiceConfiguration | FL *DistributionPointUrl
```

e.g.

```
PS C:\Scripts> Get-AipServiceConfiguration | FL *pointurl

LicensingIntranetDistributionPointUrl : https://93d0ccaa-e416-4c74-a673-9f0df129847a.rms.eu.aadrm.com_wmcs/licensing
LicensingExtranetDistributionPointUrl : https://93d0ccaa-e416-4c74-a673-9f0df129847a.rms.eu.aadrm.com_wmcs/licensing
CertificationIntranetDistributionPointUrl : https://93d0ccaa-e416-4c74-a673-9f0df129847a.rms.eu.aadrm.com_wmcs/certification
CertificationExtranetDistributionPointUrl : https://93d0ccaa-e416-4c74-a673-9f0df129847a.rms.eu.aadrm.com_wmcs/certification
```

Figure 47 DistributionPointURLs.

**Source Host(s)**

93d0ccaa-e416-4c74-a673-9f0df129847a.rms.eu.aadrm.com

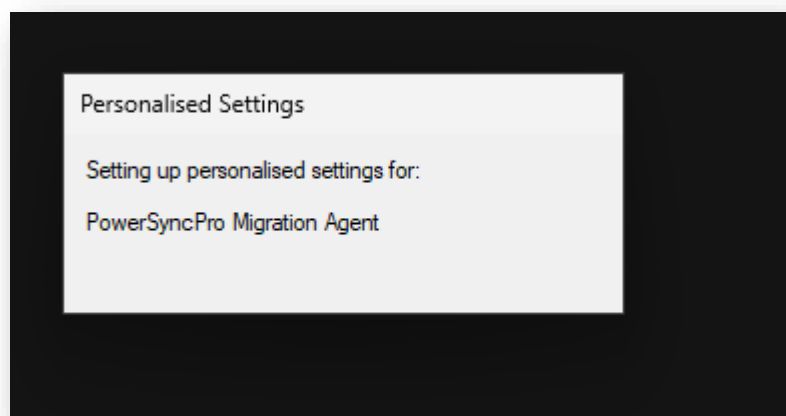
**Target Host**

94d2fbe9-764a-4753-99a0-8fd78eba436f.rms.eu.aadrm.com

**AppX Packages**

At the completion of the migration and the final reboot, users will be able to log back in. There is one final step that will occur that must run under the user context. This is the re-permissioning of AppX packages. AppX packages are things like the Microsoft Store, Company Portal, Quick Assist, Sticky Notes, Calculator, Weather and many others, in fact could be ~100.

Users will see this screen:



It is very important that this process is left to complete as it is still an integral part of the migration and stated earlier this governs the behaviour of things like the Microsoft Store, Company Portal and many other Apps.

## Completion

**Default Processing**

If any startup default processing was configured, they will be reverted during completion. This is, deleting the Admin Fallback account, re-enabling BitLocker protectors, restoring Local Groups memberships, restoring the legal notice, cleaning up the Lock Screen settings.

## Do Not Run Completion

This will not execute any of steps listed on the Completion tab – even if they are populated.

## Set Proxy AutoDetect

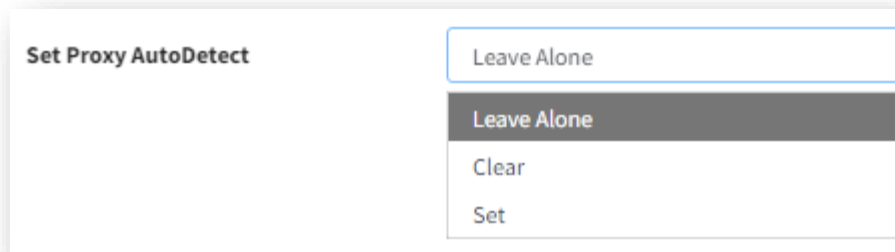
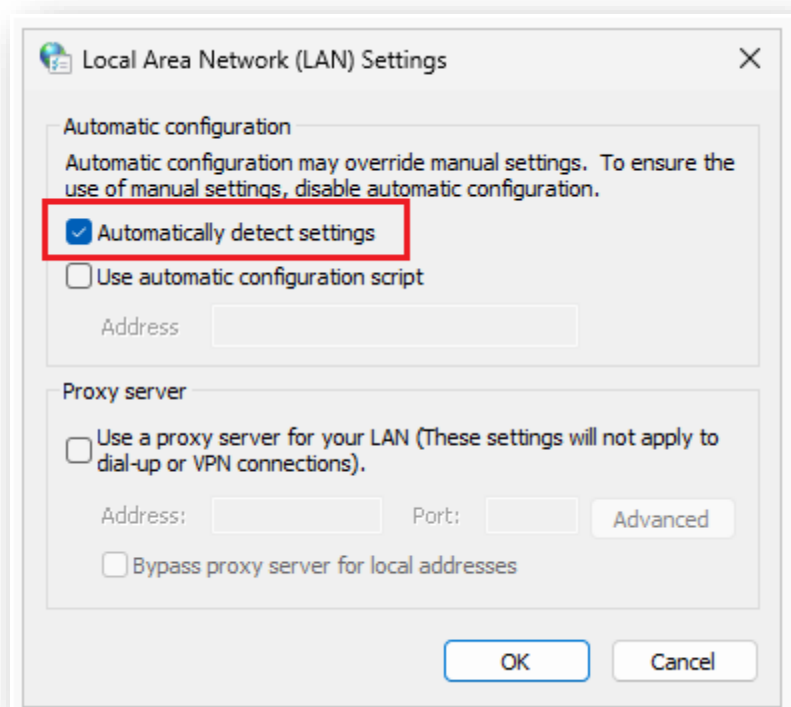


Figure 48 Set Proxy AutoDetect

Use this option if you need to directly configure the Local Area Network Settings used on the Internet Options Connections tab\LAN Settings.



Generally unless you know you have a specific need or configuration you can accept the default of “Leave Alone”

## Command Package to Run

Here you can include a file to execute any valid commands on the device that will run as system. The file used here should be a compressed .zip file.

It must contain file called **cmdline.cmd** at any other files you need. Inside the cmdline.cmd file you can list all the commands you wish to execute.

## Uninstall Agent

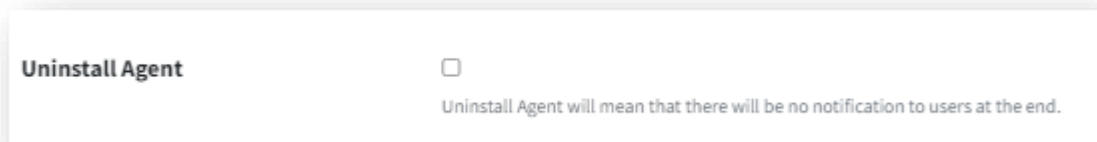


Figure 49 Uninstall Agent

You can use the PowerSyncPro Runbooks to self uninstall the Agent. If you elect this option, then note users will NOT see the Migration Completed notification.

Typically we would expect the same software deployment mechanism that installed the Agent would also be used to uninstall the agent. If you choose to use PowerSyncPro to perform the uninstallation, we recommend having this run at a later date, e.g. 14 days later, as a dedicated one off stand-alone Runbook in dedicated batches. You should ensure that your primary runbook was listed as a prerequisite so that you do not inadvertently uninstall the agent before your migrations have executed.

## Batches

**Name**
Wave 1 - Hybrid Entra Join to Entra Join cross-tenant

**Source Directory**
CONTOSO

**Target Directory**
Tenant Fabrikam

**Runbooks**

Name	Available Time	Start Time	Timezone
Hybrid Entra Join to Entra Join cross-tenant (Prerequisites)		16/09/2024 12:00 pm	Local
Hybrid Entra Join to Entra Join cross-tenant	17/09/2024 12:00 pm	18/09/2024 12:00 pm	Local

Show 10 entries

Computers

**All Computers**
☐

**No Computer**
☒

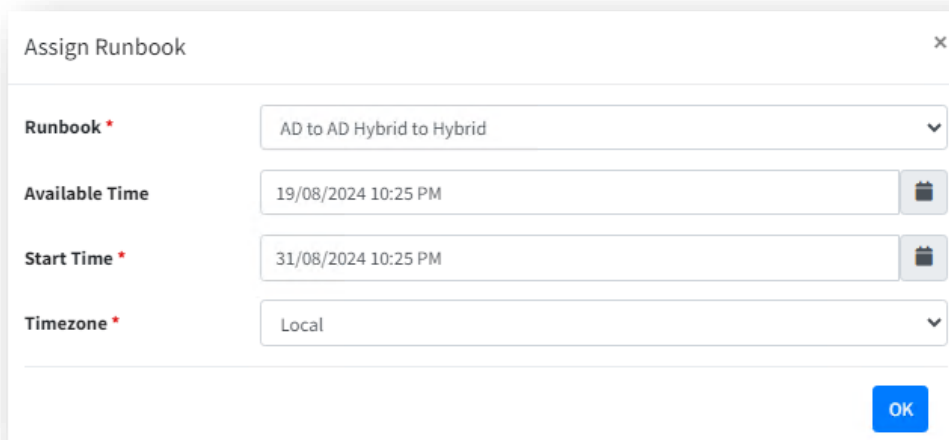
Except the following computers

Name	Object Guid	Object Sid
OMEGA1	A57A570F-AB35-4B94-A36A-C016B9FB7010	S-1-5-21-986870641-247417481-986676165-4138

Figure 50 Batches.

Batches contain the runbooks to execute along with the start time and date to run a migration, and if a migration will be available to run earlier than the mandated time.

## Assign Runbook

A screenshot of the 'Assign Runbook' dialog box. It has a title bar with a close button. The dialog contains four fields: 'Runbook \*' with a dropdown menu showing 'AD to AD Hybrid to Hybrid'; 'Available Time' with a text input '19/08/2024 10:25 PM' and a calendar icon; 'Start Time \*' with a text input '31/08/2024 10:25 PM' and a calendar icon; and 'Timezone \*' with a dropdown menu showing 'Local'. An 'OK' button is at the bottom right.

Assign Runbook

Runbook \* AD to AD Hybrid to Hybrid

Available Time 19/08/2024 10:25 PM

Start Time \* 31/08/2024 10:25 PM

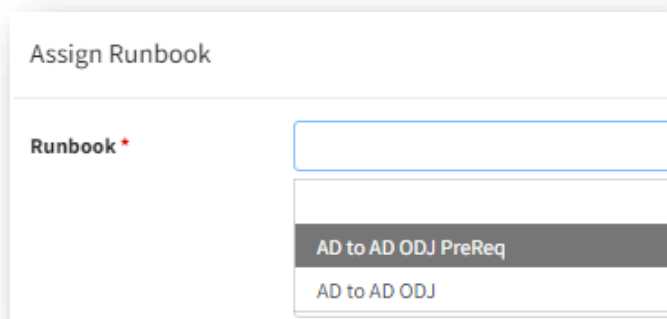
Timezone \* Local

OK

Figure 51 Creating a batch with runbooks.

## Runbook

Here you can choose the Runbooks defined earlier. Only runbooks that are configured for the same Source directory that match the Batch source directory will be shown here.

A screenshot of the 'Assign Runbook' dialog box. The 'Runbook \*' field is a list box showing two options: 'AD to AD ODJ PreReq' (highlighted) and 'AD to AD ODJ'.

Assign Runbook

Runbook \*

- AD to AD ODJ PreReq
- AD to AD ODJ

Figure 52 Assign Runbook

If you are using prerequisite runbooks, you should ensure that there Start Time is **BEFORE** your main device execution Runbook.



## Available From Time

If you select this option, then the agent on the workstation will present a dialog advising the user that their migration is available to be run from that date and time onwards. If the user is ready and available to migrate, then they can initiate the migration. The user can also defer or “Snooze” the migration. Only clicking Snooze will make this dialog box go away.

This is not required for Runbooks that run silently – usually prerequisite runbooks.

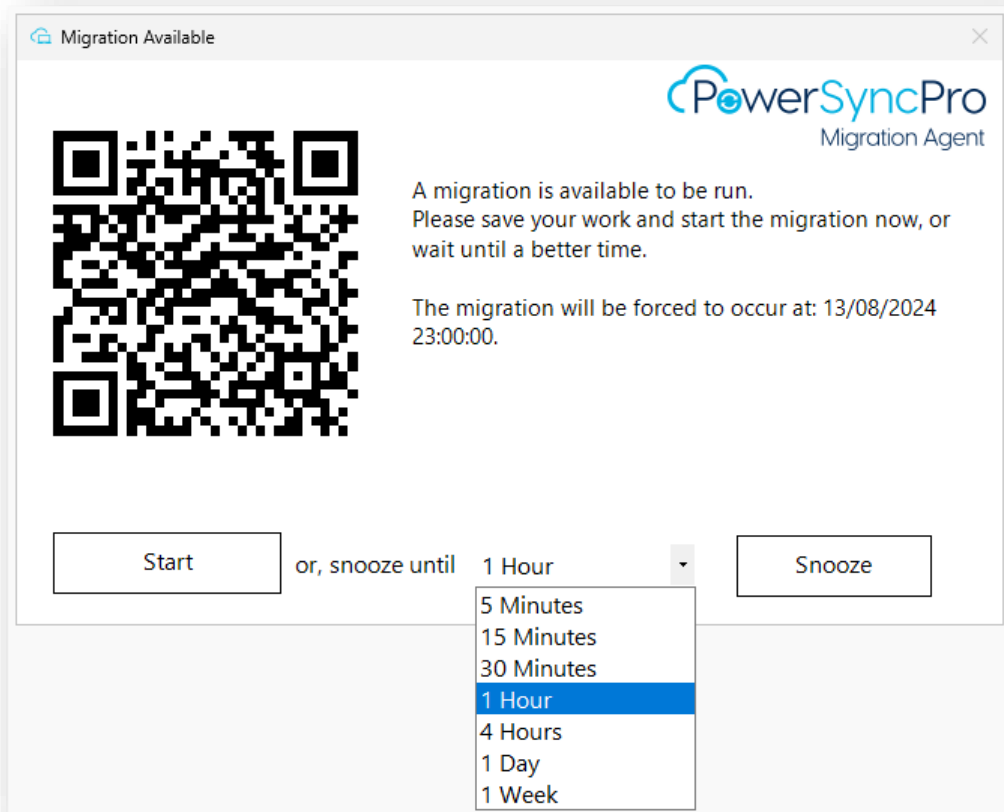


Figure 53 migration Available.

## Enforced After Time

This is the mandated run time. If no user is not logged in, but the machine is turned on, and the PowerSyncPro server is reachable, then the migration will start and execute within 15 minutes of the listed date and time.

If a user is logged in, then they will receive a notification that the migration will run within the next 60 minutes. If they do not respond to this message, then the migration execution will countdown giving a new warning at 45, 30, 15, 10, 5, 2 and 1 minute(s). At the end of the countdown the migration will begin executing.

The logged in user, if they are ready, can initiate the migration at any time within that countdown by clicking Yes to start the migration.

The user cannot cancel the migration at this point. An Administrator would be able to cancel the migration by stopping the PowerSyncPro service and using task manager to kill this task.

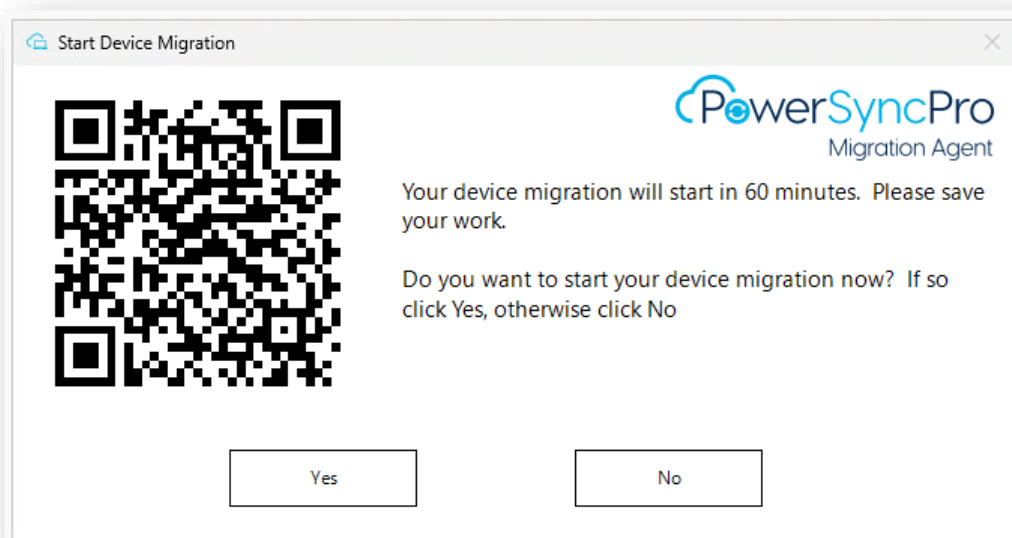


Figure 54 Start Device Migration

## Time zone

### Local

This configures the migration to run on the workstations time. i.e. **Local to that device.**

### UTC

You can use UTC if you prefer to centralise and orchestrate all your migrations to run at a specific time. e.g. 7am UTC would be:

UTC	Paris	EDT/EST	Hong Kong	Dubai	Sydney
7am	9am	3am	3pm	11am	5pm

Assign Runbook
×

Runbook \*

AD to AD (Pre-Reqs)

Available From

11/12/2023 02:45 PM

Enforced After \*

11/12/2023 02:50 PM

Timezone \*

Local

OK

Figure 55 Choose time and date to run batch.

Runbooks
Add

Name	Available From	Enforced After	Timezone	Actions
AD to AD (Pre-Reqs)	11/12/2023 02:45 pm	11/12/2023 02:50 pm	Local	Edit Delete
AD2ADPwD	29/02/2024 03:35 pm	29/02/2024 03:35 pm	UTC	Edit Delete

Show 10 entries

1

Figure 56 Successful batch created.

## Computers

Figure 57 Add computers to batch.

Batches are where you list your computers that should execute the assigned runbooks. Workstations can be added one at a time from the drop down pick list or imported in bulk from a CSV. For a workstation to be available to be added to a Batch, the Directory associated with the source migration must have Computers selected as an Import option and have been run.

### All Computers – except the following computers

If you select All Computers this means any computer, unless they are explicitly listed, that have been imported to PSP and have the Migration Agent installed will be in scope to execute the migration.

### No Computer – except the following computers

If you select No Computers this means that only Computers that are explicitly listed, that have been imported to PSP and have the Migration Agent installed will be in scope to execute the migration.

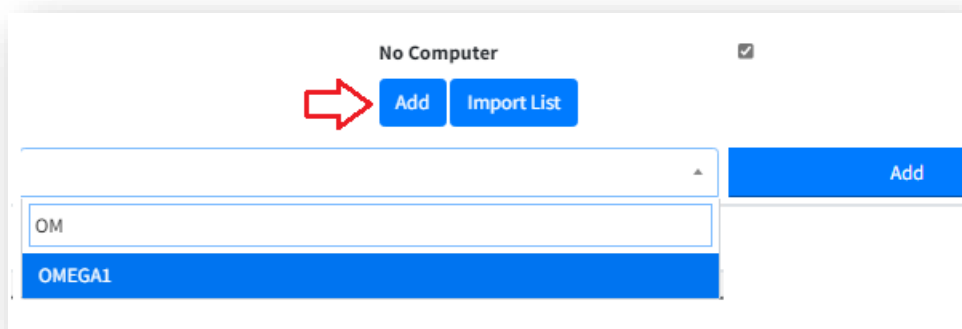
You must choose one of the options:

## All Computers ☐

Please choose to include either all or no computer.

### Drop down picklist

Use the **Add** option to choose individual computers. You can scroll to find your computer or use type-ahead to search for it. This dropdown list will only show 100 Computers, so if you cannot find your device by scrolling, then you need to use the type-ahead search capability. Be sure to click the other Add button to add to your collection.



The screenshot shows a form titled "No Computer" with a checked checkbox. Below the title are two buttons: "Add" and "Import List". A red arrow points to the "Add" button. Below these buttons is a dropdown menu. The dropdown menu is open, showing a search input field with "OM" entered. Below the search field, the option "OMEGA1" is highlighted. To the right of the dropdown menu is another "Add" button.

Figure 58 Add computer manually.

### Import from CSV

If you prefer to import from CSV, you need a two column CSV. Column headings should be: "name", "objectGuid"

Click the **Import List** button

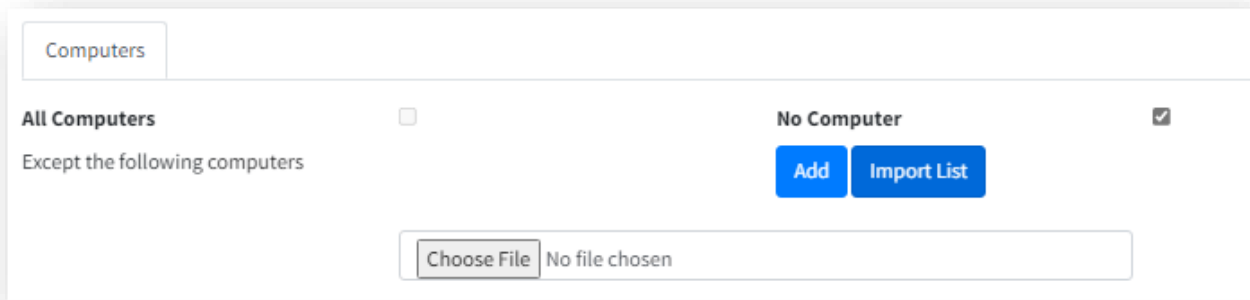


Figure 59 Import computers from csv.

To generate a list you can use Get-ADComputer from PowerShell in Active Directory to assist.

e.g.

```
Get-ADComputer -Filter * -SearchBase "[your OU]" | Select-Object Name, ObjectGUID |
Export-Csv -Path ~\downloads\computers.csv -NoTypeInformation -Encoding UTF8
```

```
PS C:\Scripts> Get-ADComputer -SearchBase "OU=Computers,OU
Name       : ALPHA1
ObjectGUID : 382b9c38-55d3-4996-9318-58529cd1f2f3
```

Figure 60 Get-ADComputer

Example CSV

NOTE: The column headings are case sensitive.

**"Name", "ObjectGUID"** and **"name","objectGuid"** are not the same.

So be sure open and edit your CSV before importing it

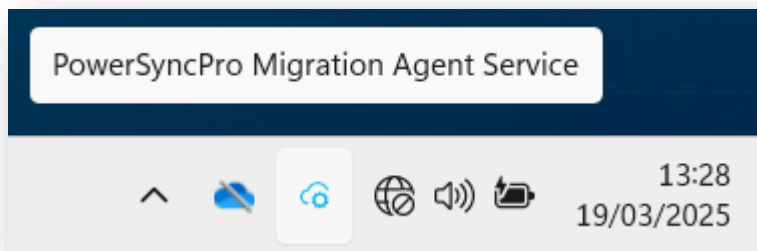
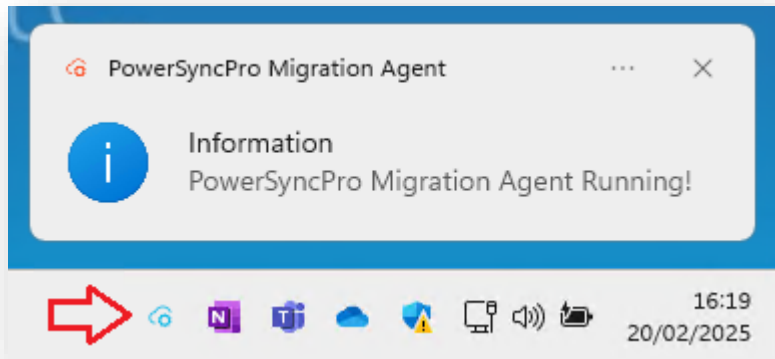
**"name", "objectGuid"**

```
"ALPHA1", "382b9c38-55d3-4996-9318-58529cd1f2f3"
"BETA1", "a4b4bc53-d734-48e0-be27-589342c91c3e"
"GAMMA1", "5af7d51c-eb45-43fd-b0ce-37db64dfad61"
"DELTA1", "1e3a01d5-1296-42bf-b4f2-123af970083d"
"EPSILON", "e29e8e50-13ea-41d9-b109-62db6eba5bdb"
```



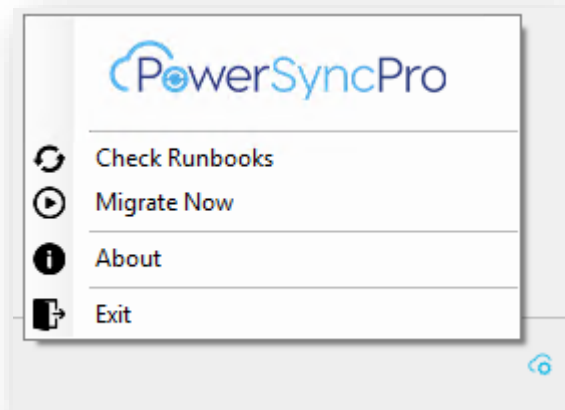
## Self Service Migrations

The PowerSyncPro service will be available in the System Tray and users can right click to perform certain actions:

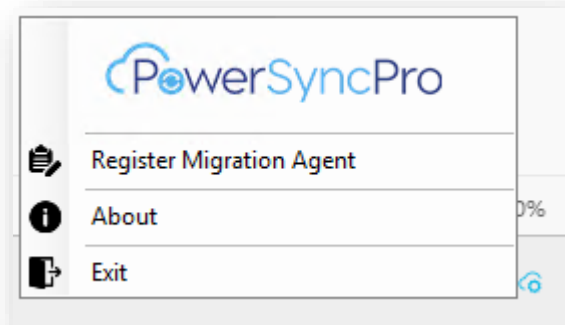




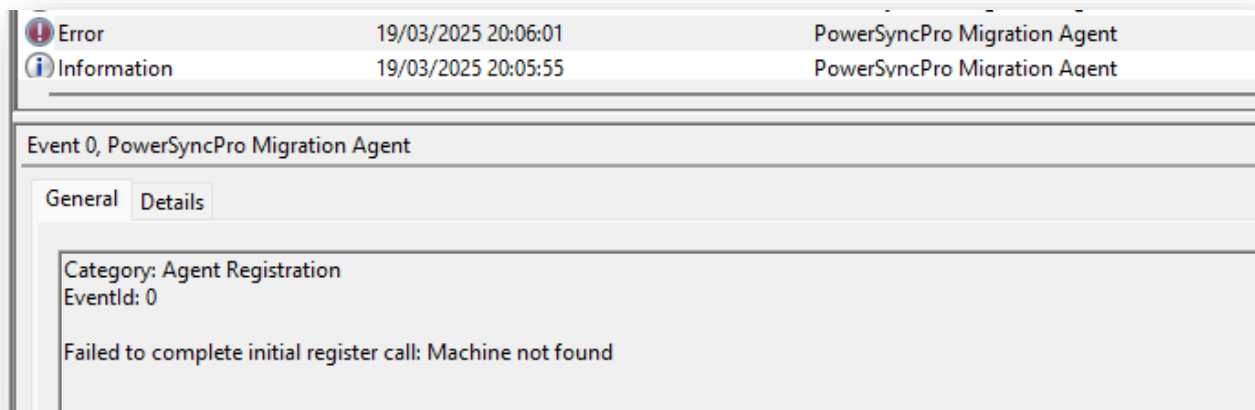
## Options



## Register Migration Agent



This option may be present if there has been a problem during the installation of the Migration Agent and it has failed to register in the PowerSyncPro back-end database. You may see an event log error like this:



Once this is resolved you will be able to return to the device and force it to register.

## Check Runbooks

Agents will check every hour since it last checked, or when the Windows Service is restarted (or if the machine is rebooted)

If a Workstation was added to a Batch (at short notice) containing a Runbook since the Agent last checked in to the PowerSyncPro Server, then checking for a Runbook will pull down the latest Runbook.

If that new information is for the machine to migrate now or in the past, then the migration will start, otherwise the latest Runbooks will be downloaded.

## Migrate Now

### Self Service Migrations

If the option in a Batch is set to “*Available From*” - **and that date has passed**,

<b>Runbook *</b>	00 Hybrid Entra Joined to Cloud Native (Contoso)	▼
<b>Available From</b>	01/03/2025 07:00 AM	📅
<b>Enforced After *</b>	31/03/2025 07:00 AM	📅
<b>Timezone *</b>	Local	▼

then users have the option to initiate the migration themselves by right clicking the system tray icon and clicking **Migrate Now**

If the user has “Snoozed” a Migration Available prompt,

Migration Available

PowerSyncPro  
Migration Agent

A migration is available to be run.  
Please save your work and start the migration now, or wait until a better time.

The migration will be enforced to run at: 30/06/2025 11:00:00.

Start

or, snooze until

1 Hour ▼

Snooze

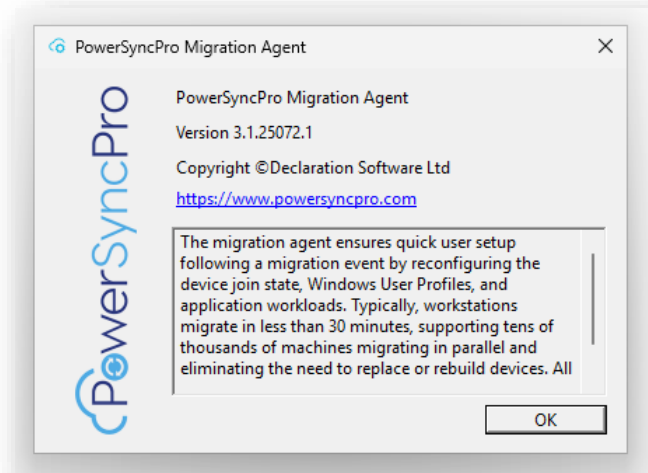
but now has the availability to perform the migration, then they can initiate the migration without waiting for the snoozed time to pass:

**NOTE:** The Migrate now option will not execute unless the “Available From” or “Enforced From” date and time has passed on the Batch information.

If Batch and Runbook information has been silently pushed to the device, then users may not have seen the “Available From” dialog box. This may be a project implementation decision to allow users to control their own convenient migration window without disturbing them with a dialog box.

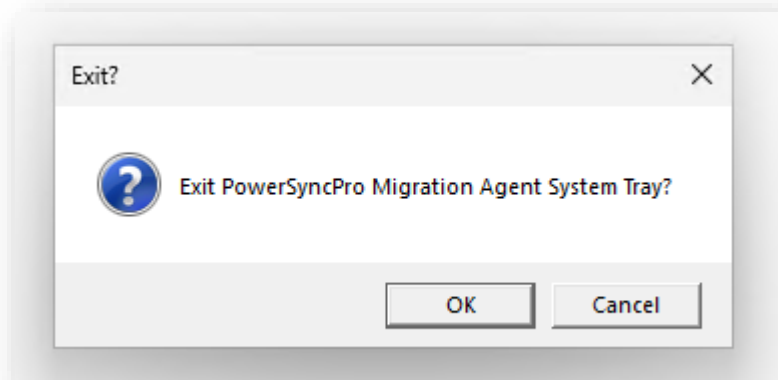
## About

This will give the current installed agent version on the device that could be useful for support engineers.



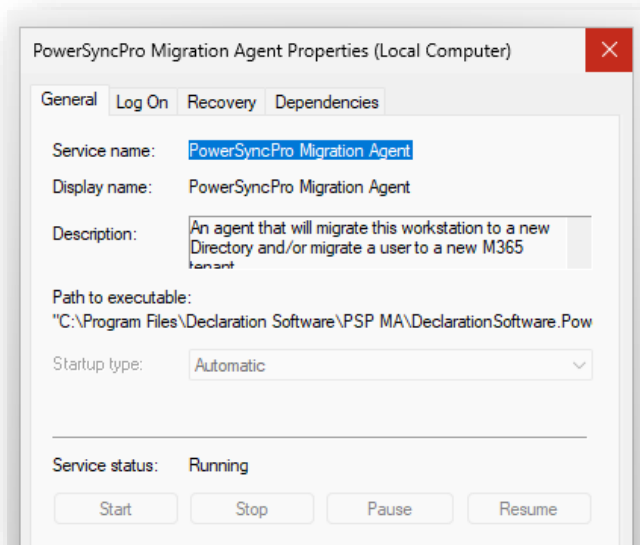
## Exit

Exit will only close the System Tray icon. It **does not stop** the service or stop a migration in progress.



- It **will not cancel** an in-progress migration

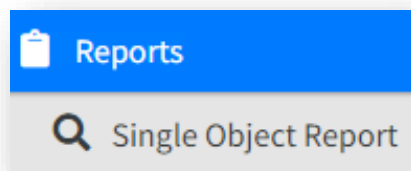
- It will not Stop the PowerSyncPro Migration Agent Service



## Reports

---

### Single Object Report



As the title suggests, this allows you to look up any object in the PSP Database and see what information it holds for it. You can look up Users, Groups or Devices.

This report is particularly useful to check if Computers are in your database and what Batches they are in.

Click on “Reports” in the navigator  
Select “Single Object Report”

**Directory:** Choose Directory for where your object is. This will be the Source directory for Computers.

**Search For:** You can use exact name. This is typically the common name of the object you are searching for, or you can use a wildcard, this is represented by the \* symbol.

## Single Object Report

Directory \*

psptestsrc.local

Search For

win\*

This will search the object name and user principal name. Use \* as wildcard.

Search

☐ View as Target Object

Tick to show the object syncing to the found object.

Object Name	Object Container
Win11Join	psptestsrc.local/DSL PSP/Twan



1-1 of 1 items

Show 10 entries

You can use multiple “\*” in your search to make your searches more granular, e.g. **omega\*** or **\*mega\***

## Single Object Report

Directory \*

psptestsrc.local

Search For

\*in1\*

This will search the object name and user principal name. Use \* as wildcard.

Search

☐ View as Target Object

Tick to show the object syncing to the found object.

Object Name

Object Container

Win11Join

psptestsrc.local/DSL PSP/Twan



1-1 of 1 items

Show 10 entries

From the Results, you can click on the object name in blue text.

Object Name

Object Container

OMEGA1

contoso.t2t.local/PSP/PSPMA/03. Hybrid Entra Join to Entra Join x-tenant/Computers

The resulting output provide detail about the Attributes, Migration Batches, User Profiles and Errors.

Overview

Attributes

Migration Batches

User Profiles

Errors

Batch Name

Source Directory

Target Directory

All Computers

Wave 1 - Hybrid Entra Join to Entra Join cross-tenant

CONTOSO

Tenant Fabrikam

False



## Runbook Status Report

This is the abridged migration status report of any runbook that is deployed to a device and its current status.

## User Profile Report

The migration Agent on a workstation will harvest any user profiles present on the device. This report can be especially useful if you are unsure which devices are tied to which users. By Exporting this report you can work with the data in Excel or other data manipulation tool to calculate device and user pairing that than can then be fed into Batches and scheduling.

User Profile Report

Machine Directory:  Machine Name:  User Directory:  User:

Use % as wildcard.

Search Reset Filters

Download CSV

Machine Name	Directory Name	User Directory	User name	Profile Path	Last Local Logon Time	Object Sid
DELTA1.itmurray.local	itmurray.local	DELTA1.itmurray.local	conradmurray	C:\Users\conradmurray	03/05/2024 17:57:06	S-1-5-21-330167997-4161477486-3793173472-1001
DELTA1.itmurray.local	itmurray.local	itmurray.local	jason.bourne@t2t.dev	C:\Users\jason.bourne	22/08/2024 23:38:13	S-1-5-21-3771727941-671935673-1569594425-10171
DELTA1.itmurray.local	itmurray.local	itmurray.local	admin.conrad.murray@itmurray.com	C:\Users\admin.conrad.murray	03/05/2024 17:59:56	S-1-5-21-3771727941-671935673-1569594425-1104

Figure 61 User Profile Report

## Agents

This will show you any successful Agent registrations from workstations and last contact. If you do not see your workstation listed here, it will not run the migration.

Here you can filter or search by: Directory Version, Machine Name.

Agents

Directory:  Version:  Machine Name:

Machine Name	Directory Name	Agent Type	Version	OS Version	Registration Complete	Last Contact	Actions
BETA1.itmurray.local	itmurray.local	Migration Agent	3.1.24239.2	Microsoft Windows 10 Enterprise (10.0.19045) - 64-bit	✓	27/08/2024 23:42	<input type="button" value="Delete"/>
CLIENT1.itmurray.local	itmurray.local	Migration Agent	3.1.24239.2	Microsoft Windows 10 Enterprise (10.0.19045) - 64-bit	✓	28/08/2024 10:52	<input type="button" value="Delete"/>
DELTA1.itmurray.local	itmurray.local	Migration Agent	3.1.24239.2	Microsoft Windows 10 Enterprise (10.0.19045) - 64-bit	✓	27/08/2024 23:51	<input type="button" value="Delete"/>
EPSILON1.itmurray.local	itmurray.local	Migration Agent	3.1.24239.2	Microsoft Windows 11 Enterprise (10.0.22631) - 64-bit	✓	28/08/2024 12:23	<input type="button" value="Delete"/>

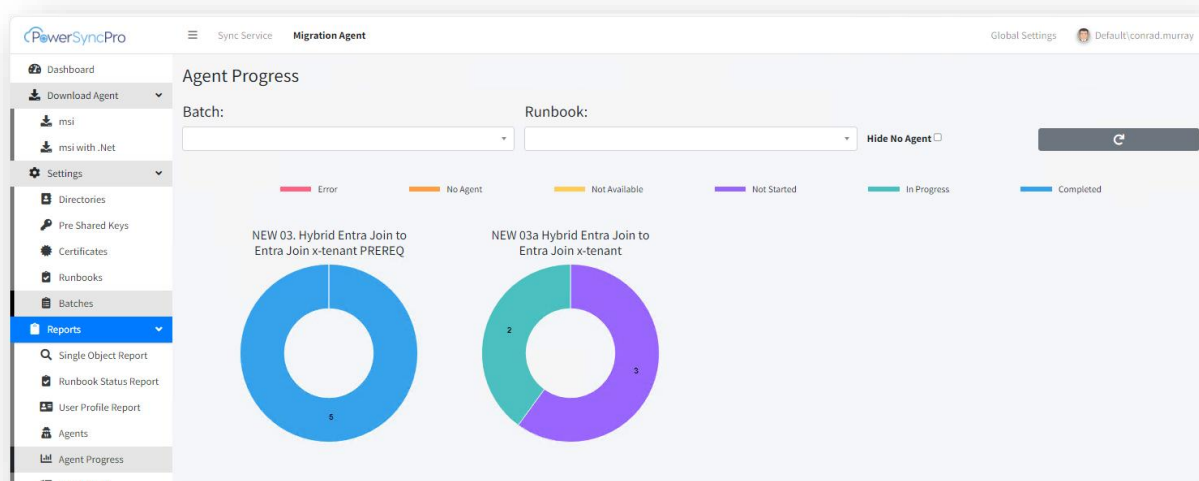
Figure 62 Agents.

Agent Progress

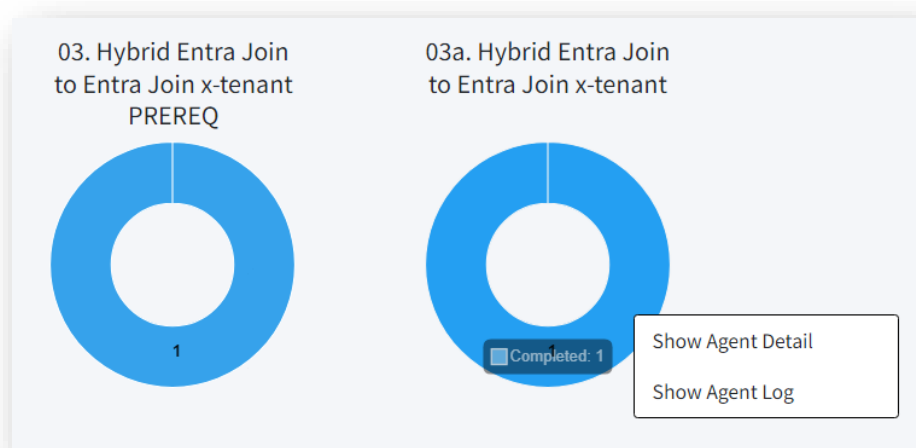
Agent Progress is the graphical summary of your migration events by Batch and Runbook. This is the same view as the Dashboard.

The legend is:

- Error
- No Agent
- Not Available
- Not Started
- In Progress
- Completed



The Dashboard gives a graphical representation of your overall batch progress. You can filter by Batch or Runbook. You can right click on the donuts to go directly to further detail or log information.



The lower sections of the dashboard will give you runtime statistics of devices in progress and which phase they are currently at.

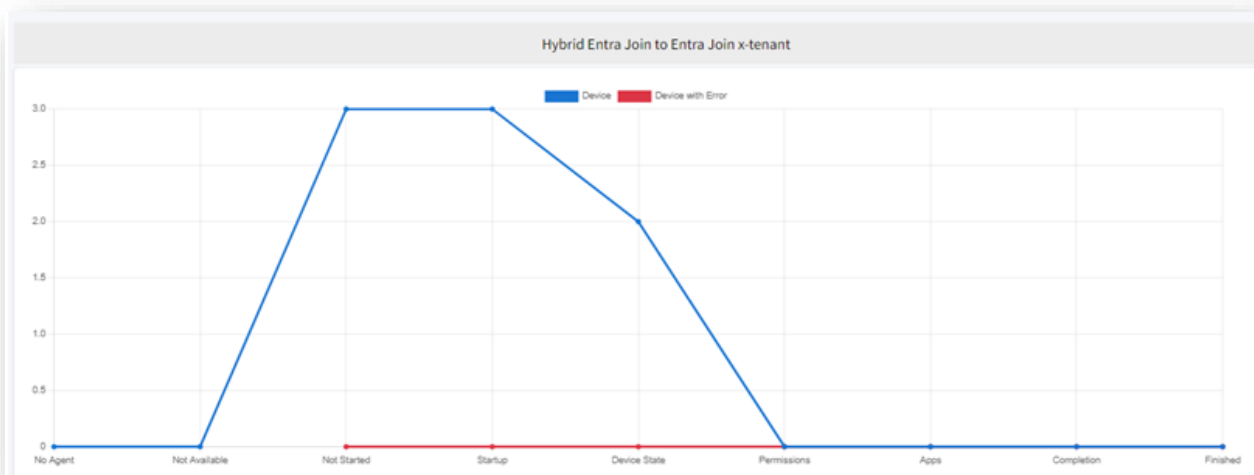


Figure 63 Progress graphs

Agent Details

Agent Detail is the **SUMMARY** of Runbook and Phase, without listing the extended actions performed (see Agent Logs). This section is intended for high level device summary progress reporting:

Here you can filter by: Batch, Runbook, Phase and Status.

Agent Detail

Batch: Runbook: Phase: Status:

Reset Filters

Download CSV

Computer Name	Runbook	Phase	Status	Last Update	Last Error
contoso.i2t.local\THETA4.contoso.i2t.local	Hybrid Joined to Entra Joined Cross Tenant Prerequisites		Completed	03/10/2024 14:24:42	
contoso.i2t.local\THETA4.contoso.i2t.local	Hybrid Joined to Entra Joined Cross Tenant Prerequisites	Completion	Completed	03/10/2024 14:24:42	
contoso.i2t.local\THETA4.contoso.i2t.local	Hybrid Joined to Entra Joined Cross Tenant Prerequisites	Apps	Completed	03/10/2024 14:24:40	
contoso.i2t.local\THETA4.contoso.i2t.local	Hybrid Joined to Entra Joined Cross Tenant Prerequisites	Permissions	Completed	03/10/2024 14:24:26	
contoso.i2t.local\THETA4.contoso.i2t.local	Hybrid Joined to Entra Joined Cross Tenant Prerequisites	Device State	Completed	03/10/2024 14:24:26	
contoso.i2t.local\THETA4.contoso.i2t.local	Hybrid Joined to Entra Joined Cross Tenant Prerequisites	Startup	Completed	03/10/2024 14:24:26	
contoso.i2t.local\THETA4.contoso.i2t.local	Hybrid Joined to Entra Joined Cross Tenant		NotStarted		

Figure 64 Agent Details

During the migration event, five phases are executed: Startup, Device State, Permissions, Applications, Completion. These align to the Runbook phases.

Agent Details can be downloaded to a CSV for ease

## Agent Logs

This is the full log of every action taken on a device. The information here is what is sent back from the device to the PSP Server. If the workstation loses communication with the PSP Server there may be more information still in the Windows Event log on the device that has not yet been sent back to the PSP Server.

You can search, filter and download as CSV.

### Agent Logs

Runbook:	Phase:	Severity:
<input type="text"/>	<input type="text"/>	Warning
Computer:	User:	
<input type="text"/>	<input type="text"/>	<button>Apply</button> <button>Reset Filters</button>
<small>Use * as wildcard.</small>	<small>Use * as wildcard.</small>	

Download CSV

NOTE: If you use a search filter, then Download CSV will only download the returned results.

Computer Name	Login Name	Runbook	Phase	Action	Severity	Message	Message Date
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Clearing Enrollment	22/08/2024 23:55:18
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Clear out Cloud Domain Join Info	22/08/2024 23:55:18
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Clear out Domain info.	22/08/2024 23:55:18
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Removing last logged in user information	22/08/2024 23:55:18
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Leaving MDM.	22/08/2024 23:55:18
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Completed Workgroup Join 0x0	22/08/2024 23:55:18
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Joining WorkGroup.	22/08/2024 23:55:12
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Completed Leaving Active Directory 0x0	22/08/2024 23:55:12
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Leaving Local AD	22/08/2024 23:55:11
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Left Azure AD	22/08/2024 23:55:11
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Leave Directory	Info	Leaving Azure AD	22/08/2024 23:55:09
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Backup Local Group Members	Info	Backup All Local Group Members has completed	22/08/2024 23:55:07
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Backup Local Group Members	Info	Backing up All Local Group Members to file	22/08/2024 23:55:07
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Backup Local Group Members	Info	Get All Local Group Members has completed	22/08/2024 23:55:07
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Backup Local Group Members	Info	Getting all local group members	22/08/2024 23:55:03
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Backup Local Group Members	Info	Start backing up local group members.	22/08/2024 23:55:03
itmurray.local\DELTA1.itmurray.local	ITMURRAY\jason.bourne	AD to AD ODJ	Device State		Info	Backed up 108 AppX applications for user S-1-5-21-3771727941-671935673-1569594425-10171	22/08/2024 23:55:03
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State		Info	Backing up AppX application information	22/08/2024 23:55:02
itmurray.local\DELTA1.itmurray.local	ITMURRAY\jason.bourne	AD to AD ODJ	Device State	Reset Windows Hello for Business	Info	Removed DefaultAccount for S-1-5-21-3771727941-671935673-1569594425-10171	22/08/2024 23:55:01
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Reset Windows Hello for Business	Info	Removing WindowsHello files under C:\Windows\ServiceProfiles\LocalService\AppData\Local\Microsoft\Ngc\	22/08/2024 23:55:01
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Cache User Credentials	Info	User ITMURRAY\jason.bourne entered in new credentials - logged in as jason.bourne@charlie.k2t.dev	22/08/2024 23:55:01
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Cache User Credentials	Info	Asking user ITMURRAY\jason.bourne to supply new credentials	22/08/2024 23:53:06
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State	Cache User Credentials	Info	Translating the user profiles	22/08/2024 23:53:06
itmurray.local\DELTA1.itmurray.local		AD to AD ODJ	Device State		Info	Running phase Device State	22/08/2024 23:53:06

## Failed Communications

The Failed Communication report shows any agents that have managed to contact the PSP server but there is some reason why they cannot register, e.g. machine is not found (i.e. PSP has not yet imported this machine) or machine already registered (i.e. PSP already has an agent for this domain/machine name).

## Failed Communications

Domain Name:
Machine Name:

Use \* as wildcard.

Machine Name	Domain Name	Message Date	Message
CONWIN11A.itmurray.local	itmurray.local	09/08/2024 19:35:01	Agent not registered
CONWIN11A.itmurray.local	itmurray.local	09/08/2024 19:35:00	Agent not registered
CONWIN11A.itmurray.local	itmurray.local	09/08/2024 19:35:00	Agent not registered

## Translation Table

The User Translation Table contains a record of the SIDs for each user. It is the SID that is used for looking up permissions on the registry, files, folders, shares, Windows Services, IIS and Scheduled Tasks that will be re-permissioned during the conversion of Windows user Profiles on a device.

You must have configured your SOURCE and TARGET directories so that PowerSyncPro can import the users you need to work with, if re-permissioning workstations will be required. Once your Directories have run an import, and you have correctly scoped users then they can become matched.

It is the correct matching of users from Source and Target that builds a permissions mapping file. Therefore you **MUST** have at least a Match only sync profile, or a Create/Update Sync profile for all of the users that are in scope for your migration project if your use case includes re-permission of Windows Profiles. i.e. you are migrating between different device join states.

The process of Matching users populates the User Translation Table.

**IMPORTANT:** If you are re-permissioning Windows User Profiles and your users do not appear in the User Translation Table then DO NOT progress to migrations until you resolve this issue.

The User Translation Table entries are downloaded to the workstation during the actual migration. Only the users that have a profile on the device are downloaded and for any other users that are listed on File/Registry permissions (but do not have a Windows User Profile on the device) to keep the end to end process as efficient as possible.

PowerSyncPro Sync Service Migration Agent Global Settings Default (conrad.murray)

Dashboard Download Agent msi msi with .Net Settings Directories Pre Shared Keys Certificates Runbooks Batches Reports Single Object Report Runbook Status Report User Profile Report Agents Agent Progress Agent Detail Agent Logs Failed Communications Translation Table

## Translation Table

Directory \* charlie.local Search

Download CSV

Source Security Id	Source User Principal Name	Source Object Name	Source Directory	Target Security Id	Target User Principal Name	Target Object Name
S-1-5-21-3771727941-671935673-1569594425-1237	Aaron.Hall@itmurray.com	Aaron Hall	itmurray.local	S-1-5-21-4232039141-3017970785-3733165135-2606	Aaron.Hall@charlie.t2t.dev	Aaron Hall
S-1-5-21-3771727941-671935673-1569594425-1386	Abi.Jones@itmurray.com	Abi Jones	itmurray.local	S-1-5-21-4232039141-3017970785-3733165135-3772	Abi.Jones@charlie.t2t.dev	Abi Jones
S-1-5-21-3771727941-671935673-1569594425-1388	Abigail.Watson@itmurray.com	Abigail Watson	itmurray.local	S-1-5-21-4232039141-3017970785-3733165135-3758	Abigail.Watson@charlie.t2t.dev	Abigail Watson
S-1-5-21-3771727941-671935673-1569594425-1406	Adam.Pearson@itmurray.com	Adam Pearson	itmurray.local	S-1-5-21-4232039141-3017970785-3733165135-3779	Adam.Pearson@charlie.t2t.dev	Adam Pearson
S-1-5-21-3771727941-671935673-1569594425-1417	Adrian.Hewitt@itmurray.com	Adrian Hewitt	itmurray.local	S-1-5-21-4232039141-3017970785-3733165135-3764	Adrian.Hewitt@charlie.t2t.dev	Adrian Hewitt
S-1-5-21-3771727941-671935673-1569594425-10195	al.pacino@t2t.dev	Al Pacino	itmurray.local	S-1-5-21-4232039141-3017970785-3733165135-3855	al.pacino@charlie.t2t.dev	Al Pacino
S-1-5-21-3771727941-671935673-1569594425-10160	Alan.Brown@itmurray.com	Alan Brown	itmurray.local	S-1-5-21-4232039141-3017970785-3733165135-3795	Alan.Brown@charlie.t2t.dev	Alan Brown

## Event Logs

Every action taken by the workstation Agent is written to the event logs. All these activities are also sent up to the PSP Server and will be seen in the Agent Logs section.

In the event of an issue with your migration, the local Application Event logs are the first place to go and check what happened. Support may ask you to export these for troubleshooting purposes.



PowerSyncPro Migration Agent    Number of events: 11

Number of events: 11

Level	Date and Time	Source	Event ID	Task Category
Information	08/08/2024 19:23:27	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:27	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:26	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:26	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:26	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:21	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:21	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:21	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:20	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:19	PowerSyncPro Migration Agent	0	None
Information	08/08/2024 19:23:19	PowerSyncPro Migration Agent	0	None

Event 0, PowerSyncPro Migration Agent

General    Details

Category: Agent Registration  
EventId: 0

Registration successful

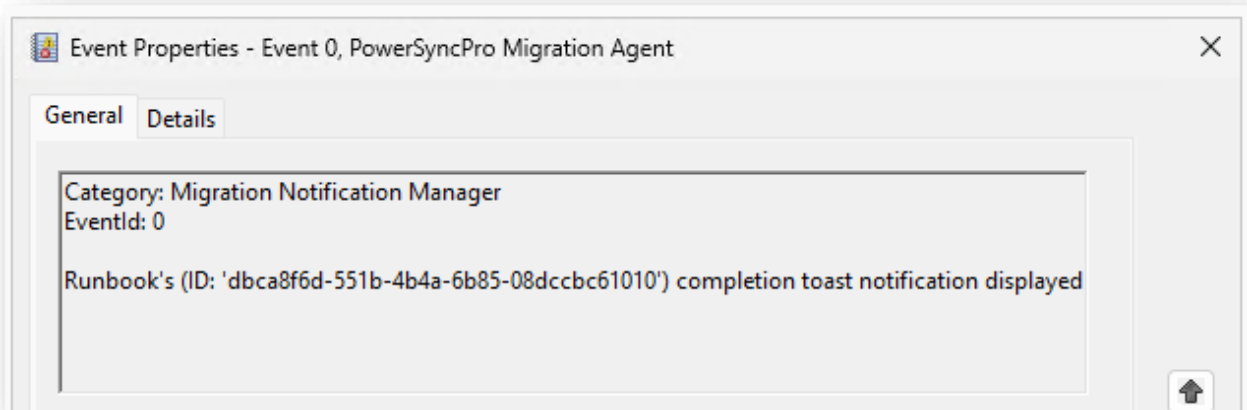
Log Name:    Application  
Source:    PowerSyncPro Migration Ag    Logged:    08/08/2024 19:23:21  
Event ID:    0    Task Category:    None

Event Properties - Event 0, PowerSyncPro Migration Agent

General    Details

Category: Runbook Completed  
EventId: 0

Runbook 'Hybrid Entra Join to Entra Join cross-tenant' (ID: 'dbca8f6d-551b-4b4a-6b85-08dccbc61010') completed



## Windows Hello for Business

If a workstation migrates between device join state and is connected in the source to a tenant that has been enabled for Windows Hello for Business (WHfB), PowerSyncPro will reset the WHfB device configuration so that it can receive the target tenant WHfB configuration. This will require the user to go through the WHfB wizard again and create a new PIN for example if this is a requirement.

Note that if you do not want to have the end user prompted to register for WHfB then you will need to use a completion script to disable the registry keys.

```
if(!(Test-Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork')) {  
    New-Item -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork' -Type  
    Container  
}  
New-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork' -Name  
'Enabled' -Value "0" -PropertyType DWORD -Force  
New-ItemProperty -Path 'HKLM:\SOFTWARE\Policies\Microsoft\PassportForWork' -Name  
'DisablePostLogonProvisioning' -Value "0" -PropertyType DWORD -Force
```

## Autopilot

If a workstation migrates between device join state and is connected in the source to a tenant that has been enabled for Autopilot, and that device was in scope for Autopilot then PowerSyncPro will reset the Autopilot configuration on the device itself.

**Note:** PowerSyncPro does not orchestrate the clean-up of Autopilot in the source tenant so you should plan accordingly to ensure your workstations can “Fresh Start” from the target tenant if that is a requirement.

You can delete the Autopilot record from the source tenant **after** the machine has migrated off that tenant, and then an Autopilot Policy assigned to a group that contains the devices can be used to harvest the hashes and bring the devices into Autopilot in the target tenant.

If you are migrating Intra-tenant, i.e. taking a device from Entra Hybrid Joined to Entra Joined, then the device will still be eligible for Autopilot depending on your Autopilot configuration in the tenant and how devices are onboarded into Autopilot.

## Troubleshooting

The Windows Application Event Logs should be the first place you check for any migration issues on the device. The PSP Server Agent Logs and Failed Communications may have information as well, but the event logs will have the primary reasons.

### Connectivity

The workstation that is migrating **must** always have connectivity to the PowerSyncPro server during the migration. If the migration fails to start, check this first. Is the PSP Server online, service running and responding on the endpoint? Does the workstation have a network connection? Is the end-point name resolvable? Did it start on a wired LAN connection and then get moved to Wi-Fi that has not connected? Is a VPN required? Is there a proxy in the middle that is preventing access?

### Check the endpoint

The best way to check is open a browser and connect directly to the PSP Server endpoint. If the page loads below with no errors you have successfully connected.

e.g.

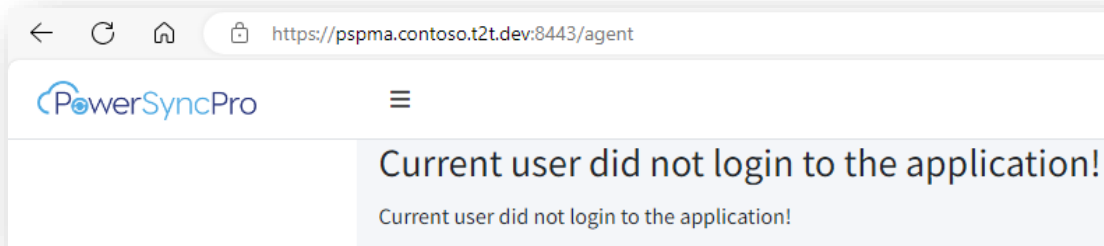


Figure 65 Connected to endpoint

For Entra Join migrations, the workstation will need internet connectivity to Azure and the associated Azure and Entra Id endpoints.



## Appendix - Entra Join settings for Microsoft 365

---

PowerSyncPro Migration Agent can only work within the limitations of the target tenant configuration. If you are seeing Entra Join or Intune Enrollment failures, then review the following.

If you are working towards Microsoft Entra joined devices then here below are some example settings that you should consider and review for your own environment and ensure that they are set appropriately for your business needs and project aspirations.

This section is **not included as a definitive design guide** for your Entra Devices, merely as a helpful list of places to check if you are troubleshooting Entra Join and Intune Enrolment.

We strongly advice that you configure Azure, Entra and Intune to your own organisation's requirements and regularly check the Microsoft documentation as it is updated regularly and subject to change.

## Entra ID

---

### Entra Device settings

#### Microsoft Entra join and registration settings

This setting must be configured appropriately for your users to be able to join a device to Entra. This does not have to be **All**, you can also use **Selected** users via Entra ID Security Groups.

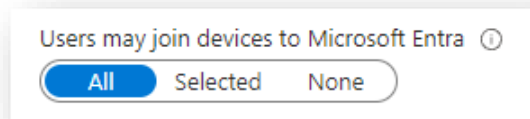


Figure 66 Users may join devices to Microsoft Entra

#### Require Multifactor Authentication to register or join devices with Microsoft Entra

Carefully consider your configuration here, it is recommended to control this via Conditional Access and have this setting set to **No**.

Require Multifactor Authentication to register or join devices with Microsoft Entra ⓘ

☐ Yes ☒ No


 We recommend that you require Multifactor Authentication to register or join devices with Microsoft Entra using [Conditional Access](#). Set this device setting to No if you require Multifactor Authentication using Conditional Access.

Figure 67 Require Multifactor Authentication to register or join devices with Microsoft Entra

### Maximum number of devices per user

Maximum number of devices per user ⓘ

20 (Recommended) ▼

### Local administrator settings

- Global administrator role is added as local administrator on the device during Microsoft Entra join.

Local administrator settings

Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview) ⓘ

☒ Yes ☐ No

## Intune

### Mobility (MDM and WIP)

Choose MDM user scope. If your users are not in scope via All, or via a Group, then they will not be able to MDM Enroll a device.



MDM user scope	Windows Information Protection (WIP) user scope
<div> MDM user scope ⓘ  <input type="radio"/> None <input type="radio"/> Some <input checked="" type="radio"/> All  MDM terms of use URL ⓘ  <input type="text" value="https://portal.manage.microsoft.co..."/>  MDM discovery URL ⓘ  <input type="text" value="https://enrollment.manage.microso..."/>  MDM compliance URL ⓘ  <input type="text" value="https://portal.manage.microsoft.co..."/>  <a href="#">Restore default MDM URLs</a> </div>	<div> Windows Information Protection (WIP) user scope ⓘ  <input checked="" type="radio"/> None <input type="radio"/> Some <input type="radio"/> All  WIP terms of use URL ⓘ  <input type="text"/>  WIP discovery URL ⓘ  <input type="text" value="https://wip.mam.manage.microsoft..."/>  WIP compliance URL ⓘ  <input type="text"/>  <a href="#">Restore default WIP URLs</a> </div>

### Important

When a user is in both the MDM user scope and WIP user scope:

- The MDM user scope takes precedence if they are on a corporate-owned device.
  - The device automatically enrolls in Microsoft Intune when they set it up for work.
- The WIP user scope takes precedence if they bring their own device “BYOD” Personal Device.
  - The device does not enroll in Microsoft Intune for device management.
  - Microsoft Purview Information Protection policies are applied if you configured them.

In **Entra ID** under **Mobility (MDM and WIP)**, you typically see two entries:

1. **Microsoft Intune**
2. **Microsoft Intune Enrollment**

### Do You Need to Configure Both?

Yes, **both entries are required** for a full **Intune MDM deployment**:

- **Microsoft Intune Enrollment** must be configured to allow users to enroll devices.
- **Microsoft Intune** must be configured to apply policies and manage the devices post-enrollment.

If you don't configure **Microsoft Intune Enrollment**, users may face issues enrolling their devices into Intune, especially with **BYOD (Bring Your Own Device)** scenarios.

### Differences Between the Two

Feature	Microsoft Intune Enrollment	Microsoft Intune
Purpose	Handles the initial device enrollment process.	Manages devices after they are enrolled.
Configuration	Required to allow users to enroll their devices into Intune.	Required for device management policies, compliance policies, and app deployment.
Assignment	Assigned to users who need to enroll devices.	Assigned to users or groups who need device management.
MDM Scope	Should include users who need to self-enroll devices.	Must be configured for managing devices via Intune.
Default Presence	Required for device enrollment and usually pre-configured.	Always present when Intune is enabled.

## Conditional Access

You need to Exclude the **Microsoft Intune Enrollment** App from MFA in the Target resources section on a CA policy.





Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*

Assignments

Users ⓘ

[All users included and specific users excluded](#)

Target resources ⓘ

[All cloud apps included and 1 app excluded](#)

Network NEW ⓘ

[Any network or location and 2 excluded](#)

Conditions ⓘ

[3 conditions selected](#)

Control access based on all or specific network access traffic, cloud apps or actions.  
[Learn more](#)

Select what this policy applies to

Cloud apps

Include **Exclude**


Select the cloud apps to exempt from the policy

Edit filter

[None](#)

Select excluded cloud apps

[Microsoft Intune Enrollment](#)


Microsoft Intune Enrollment  
d4ebce55-015a-49b5-a083-c84d1797ae...

If **Microsoft Intune Enrollment** is not present, you may need to run the following to add it.  
From an AzureAD PowerShell

```
New-AzureADServicePrincipal -AppId d4ebce55-015a-49b5-a083-c84d1797ae8c
```

## Licencing

### Users

Users need to be appropriately licensed to be able to Enroll a device. This is usually with the EMS (Enterprise Mobility + Security) Add-On (E3 or E5) or any higher SKU that contains that option such as Microsoft 365 E3/E5 or Microsoft 365 Business Premium.

<https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses>

### Workstations

Windows 10 and 11 devices need to be at the Pro or Enterprise edition, Windows 10/11 Education and Windows 10/11 IoT Enterprise.

## Device platform restrictions

Personally owned needs to be set to allowed for Intune Enrollment.

Type	Platform	versions	Personally owned
Android Enterprise (work profile)	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>
Android device administrator	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>
iOS/iPadOS	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>
macOS	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Restriction not supported	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>
Windows (MDM) ⓘ	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>	Allow min/max range: <input type="text" value="Min"/> <input type="text" value="Max"/>	<input checked="" type="button" value="Allow"/> <input type="button" value="Block"/>

## Device limit restrictions

Device limit restrictions			
Define how many devices each user can enroll.			
Priority	Name	Device limit	Assigned
Default	All users and all devices	5	Yes

## DNS Records

Your DNS Records should be in place for auto enrollment. The required DNS records and verification can be seen in your Microsoft 365 Admin Portal.




Basic Mobility & Security					
	Type	Status	Name	Value	TTL
<input type="checkbox"/>	CNAME	✓ OK	enterpriseregistration.contoso	enterpriseregistration.windows.net	1 Hour
<input type="checkbox"/>	CNAME	✓ OK	enterpriseenrollment.contoso	enterpriseenrollment-s.manage.microsoft.com	1 Hour

Figure 68 Intune enrollment DNS entries.

## CNAME validation

CNAME validation can be done at the Intune Admin Portal.

### Enrollment options

	Automatic Enrollment	Configure Windows devices to enroll when they join or register with Azure Active
	CNAME Validation	Test company domain CNAME registration for Windows enrollment.
	Co-management Settings	Configure co-management settings for Configuration Manager integration.
	Device platform restriction	Configure which platform versions can enroll

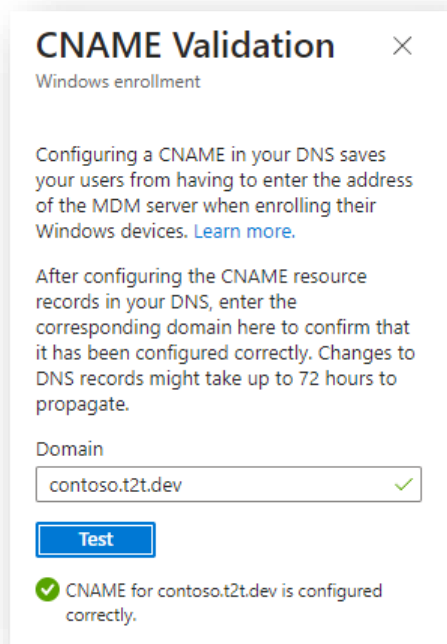
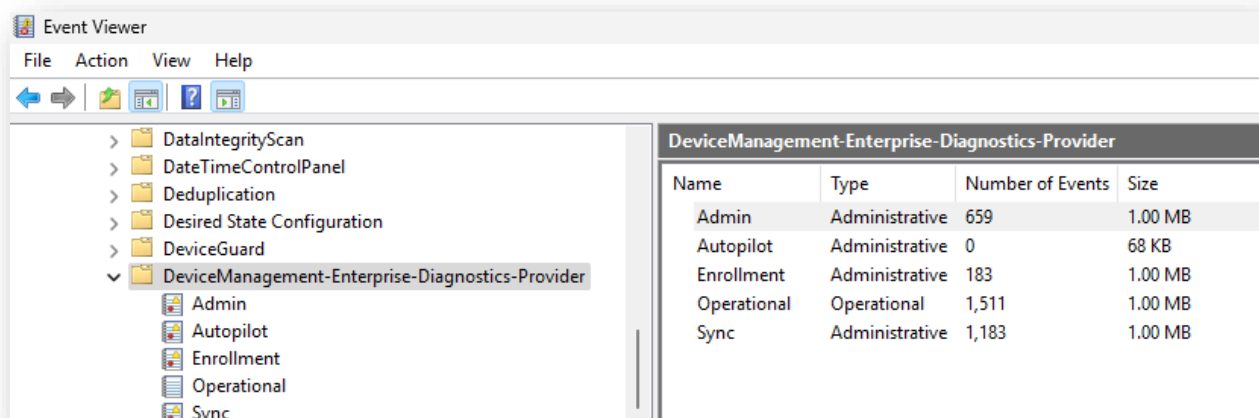


Figure 69 Intune CNAME validation.

## Event Logs

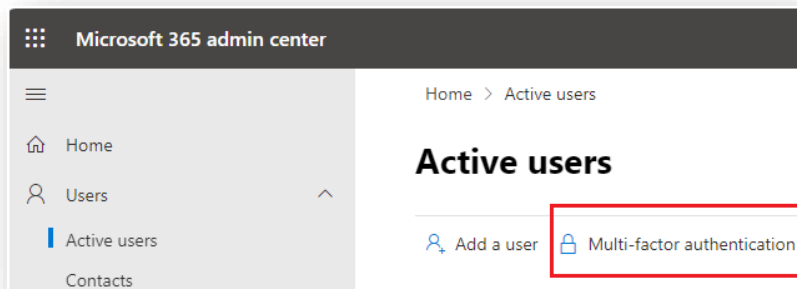
Enrolment issues are seen in these event logs: Applications and Services Logs > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider



## Users

### Per User MFA

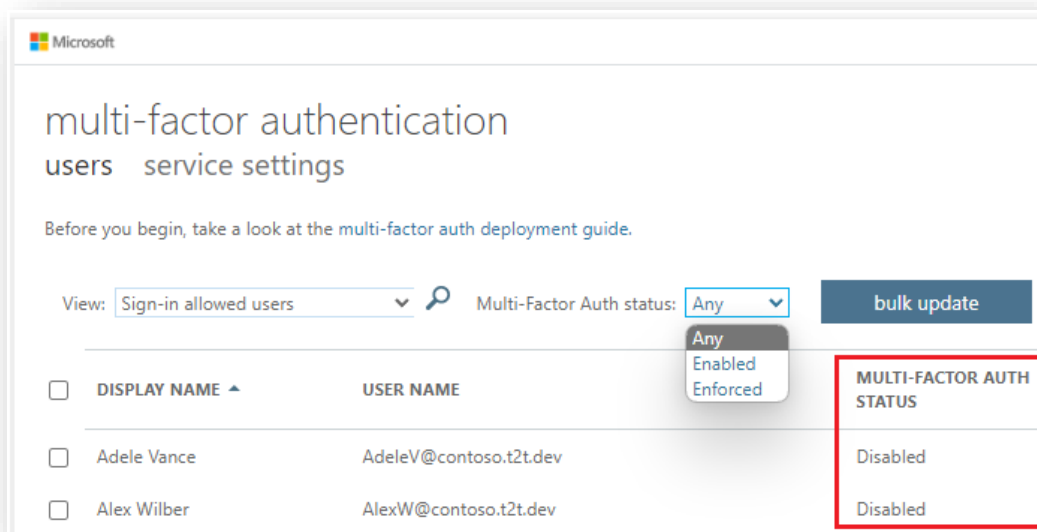
Per User MFA should not be enabled. From the Microsoft 365 Admin portal, go to the Users section and open multi-factor authentication.



Or go direct from here:

<https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx>

Check MFA Auth Status



If it is not disabled here, then users will still be MFA challenged on their devices.