

PowerSyncPro

Integrate. Collaborate. Migrate.

Configuration Guide

PowerSyncPro Sync Service

Last updated: 26 March 2025



Contents

Contents	2
PowerSyncPro Overview	7
Release Notes	7
Introduction	7
Prerequisites	8
Installation Guide.....	8
End-User License Agreement.....	8
Global Settings	8
Users	9
User Roles	10
Licences.....	12
Staging Mode.....	13
SQL Database Backup / Restore.....	14
PowerSyncPro Migration Agent Migration History.....	15
Schedule.....	15
Schedule Right Click Options	17
Job Status Icons.....	19
Refresh Interval.....	20
Next Run	20
Run Now	20
Pause Schedule.....	21
Resume Schedule.....	21
Force Stop.....	21
Directories	21
Create a Directory Profile.....	22
Active Directory	22
Entra ID	26
Link Entra ID Exchange	28
Google Workspace Directory Setup	29



- Refresh Schema..... 31
- Import Containers 31
- Import Objects..... 31
- SMTP Domains 31
 - Considerations 32
 - Allow Sync Addition 33
 - Allow Sync Removal 34
 - Create new SMTP Domain Configuration..... 34
 - Configure smtp / x500 / sip entries to flow to proxyAddresses 34
 - Configuring SMTP Domain Values to flow..... 36
 - Download CSV..... 37
 - Import bulk domains 38
 - Example of SMTP Domains Configuration 40
- Sync Profiles 40
 - Key Concepts 41
 - Schema Attributes 41
 - One-way sync 41
 - What If 41
 - Directory Sync Flow 42
 - Deletion Threshold..... 43
 - Active Directory Recycle Bin 44
- Creating a Sync Profile 44
 - Exclude From Schedule: 46
 - Name 46
 - Source Directory 46
 - Target Directory 46
 - Template 46
 - Copy Existing Profile 47
 - Object Type 47
 - Sync Action 48
 - Create Object Type:..... 49



- Match Object Type 49
 - Create or Update Behaviour..... 50
- Convert Contact 50
 - Create or Update Behaviour for Convert Contact..... 51
- Scope..... 51
 - Descoped Objects 52
 - Scope by Source Containers 52
 - Target Container 53
 - Create Target Container 55
 - Scope by 57
- Match..... 59
- Map 60
 - Download CSV..... 60
 - Import..... 60
 - Create..... 61
 - Different Directory Schema Types 61
 - Attribute Manipulation..... 62
 - Microsoft Exchange Attributes 65
- Sync Options 65
 - Delete Target Objects..... 65
 - Sync SID History 66
 - Legacy Password Sync 69
 - Modern Password Sync 70
 - Sync Group Members..... 70
 - Retain Target Group Members..... 71
 - Convert Contact 71
 - Invite Redirect URL..... 71
 - User Account..... 72
- Mail Enable..... 73
 - Default processing..... 73
 - Mail Enable Options 74



Simple Expressions	76
Regular Expressions	82
Complex Expressions	83
C# objects and methods.....	86
Examples	87
Ignored Objects	103
Jobs	104
Refresh Schema.....	105
Import Containers	105
Import Objects.....	106
Sync Objects	107
Export Objects	107
Sync SID History	108
Sync Passwords.....	108
Job Queue	109
Remote Agents	110
SSL and Ports	110
Pre Shared Keys “PSK”	111
Certificates.....	113
Approve Remote Agent	116
Service	117
Failed Communications	117
Remote Sync Agent	117
Sync Agent Configuration	117
Directories Configuration	120
Remote Password Agent.....	122
Sync Profile Configuration	122
Schedule.....	123
Remote Agent Proxy	123
Service Connection Points.....	124
Using SCPs with Remote Sync and Remote Password Agents.....	124



Reports	126
Single Object Report.....	126
Overview	129
Break Relationship	129
Attributes	130
Migration Batches	130
User Profiles	131
Errors	131
What If Report.....	131
What If from the Schedule Screen	132
Running a What If from Reports	133
Results.....	133
Accepting a What If Report	135
Message Logs	137
Filter	138
Log Info Messages.....	139
Results.....	139
Password Sync Logs.....	141
Windows Application Event Log	141
Support.....	143



PowerSyncPro Overview

Directory Synchronization

PowerSyncPro addresses identity management in coexistence, modernization, or migration scenarios by synchronising users, groups, and members. It ensures these elements stay current, like how Entra Connect Sync synchronises from Active Directory to Entra ID. Full imports and syncs for hundreds of thousands of objects are completed in minutes, while delta runs finish in seconds or minutes.

Designed with Microsoft 365 and Entra ID in mind, PowerSyncPro supports Microsoft 365 tenant-to-tenant migrations and divestitures. It also synchronizes objects from Google Workspace to Entra ID or Active Directory. PowerSyncPro can be hosted in a DMZ or Azure with lightweight Sync Agents in the client infrastructure.

Active Directory Migrations

PowerSyncPro also facilitates Active Directory migrations by making objects in a target Active Directory ready for migration or cutover. It synchronizes all or a subset of attributes and can synchronize SID to SIDHistory and passwords, enabling a seamless transition. PowerSyncPro can synchronise modern passwords where RC4 has been disabled.

Windows Workstation Migration Agent

The migration agent ensures quick user setup following a migration event by reconfiguring the device join state, Windows User Profiles, and application workloads. Typically, workstations migrate in less than 30 minutes, supporting tens of thousands of machines migrating in parallel and eliminating the need to replace or rebuild devices. All managed from a central dashboard with monitoring and reporting.

Release Notes

Current GA versions release notes are available here:

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

Introduction

Before configuration and deployment into a production environment you should complete your requirements gathering and design phase. A good understanding of attributes is required to ensure you maximise the best possible result.

You should consider in particular; attribute mappings and attribute manipulation to rewrite attributes as needed to your target directory, especially mail, userPrincipalName, proxyAddresses, targetAddress and how theses should be handled pre and post migration if that is your project type.



This configuration guide assumes that you have successfully completed the PowerSyncPro Server installation and prerequisites including any required firewall changes to support network requirements and that you have created the appropriately permissioned source and target Service Accounts, Group Managed Service Accounts, Entra App registrations, Google Service Account, SSL Certificates and any other Active Directory requirements to support password sync and SID History sync.

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

All screenshots contained in this document are representative examples taken from test and demo lab environments.

Prerequisites

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

Installation Guide

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

End-User License Agreement

<https://downloads.powersyncpro.com/current/Declaration-Software-End-User-License-Agreement.pdf>

Global Settings

First login.

First time login credentials will be provided by support. Navigate to <http://localhost:5000> and you will be presented with a log in dialog box.





Figure 1 PowerSyncPro Login Screen

Users

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

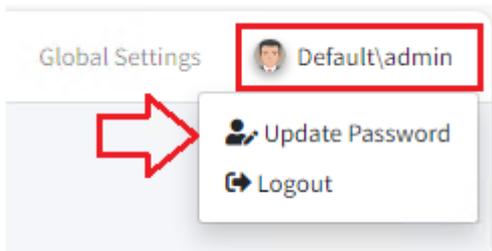


Figure 2 update Password and Logout

Adding a User

From tenant settings, choose Users



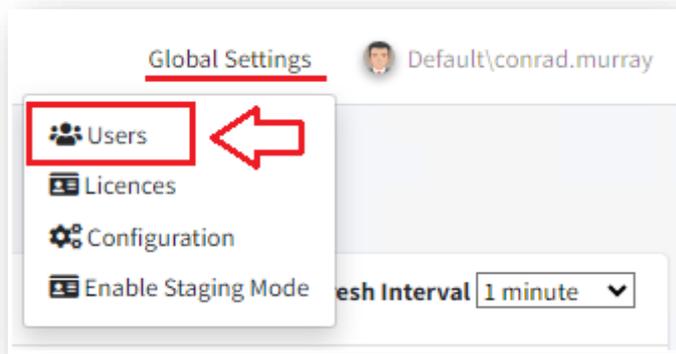


Figure 3 Configure Users

And then Create

A screenshot of the 'Create new user' form. The 'User details' tab is selected and highlighted with a red box. The form contains the following fields:

- User name *: joe.bloggs
- Name *: Joe
- Surname *: Bloggs
- Email address *: joe.bloggs@powersyncpro.com
- Password *: [masked]
- Confirm password *: [masked]
- Is active:

Figure 4 Create new user

User Roles

There are seven defined User roles available to choose from.



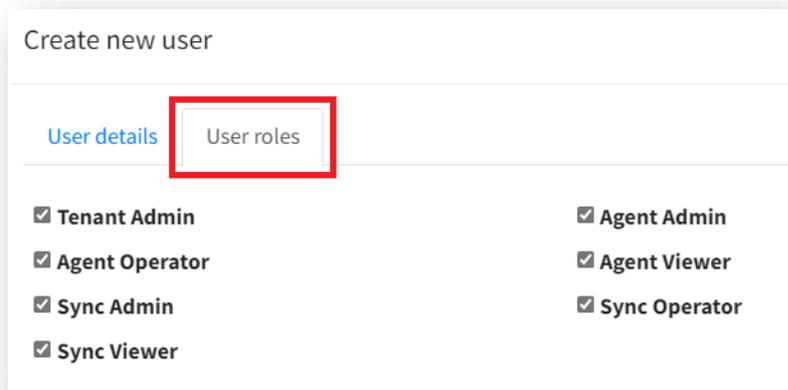


Figure 5 PSP Users Roles

Role	Description
Tenant Admin	Overall admin within PowerSyncPro, including Tenant Settings, and adding and removing tenants. Multi-tenant feature is reserved for future use and should not be configured
Sync Admin	Able to fully administer all screens in the Sync Service area of PowerSyncPro
Sync Operator	Able to run the schedule but not update the configuration, able to view all screens in the Sync Service area of PowerSyncPro
Sync Viewer	Able to view all screens in the Sync Service area of PowerSyncPro
Agent Admin	Able to fully administer all screens in the Migration Agent area of PowerSyncPro
Agent Operator	Able to schedule migrations but not update the configuration, able to view all screens in the Migration Agent area of PowerSyncPro
Agent Viewer	Able to view all screens in the Migration Agent area of PowerSyncPro

Figure 6 PowerSyncPro User Roles



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. PowerSyncPro DirSync is fully functional without a licence key - with the exception of export objects.

When requesting a licence you will need to provide the FQDN fully qualified domain name(s) of the Domain(s) in scope, and the Microsoft 365 / Azure tenant name(s) (*.onmicrosoft.com) for Entra ID if being used - for all directories. e.g.

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

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

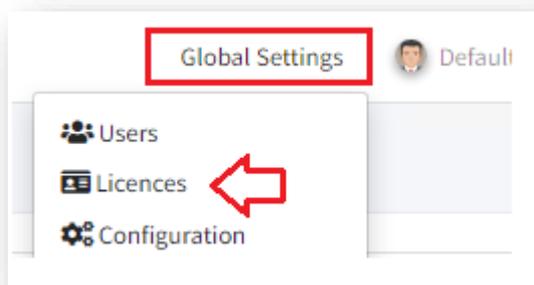
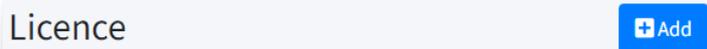
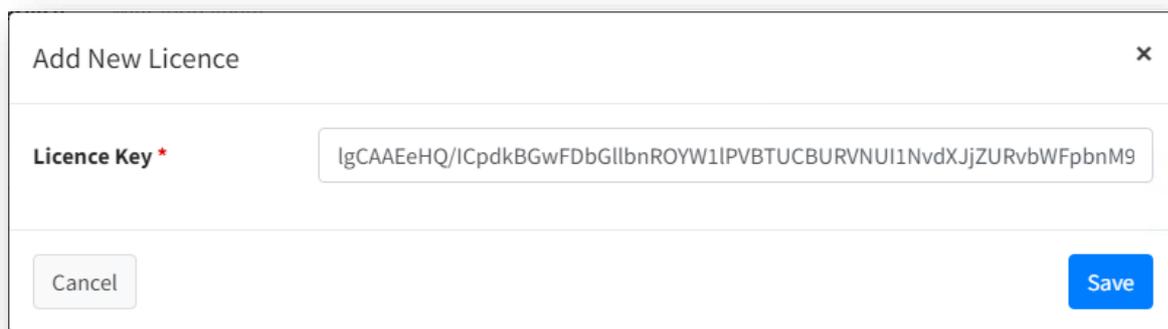


Figure 7 Tenant Settings, Licences



Click “Add” and paste in the licence key provided



A dialog box titled "Add New Licence" with a close button (X) in the top right corner. It contains a "Licence Key" field with a red asterisk, containing the alphanumeric string "lgCAAEEHQ/ICpdkBGwFDbgllbnROYW1IPVBTUCBURVNUI1NvdXJjZURvbWFpbnM9". At the bottom, there are "Cancel" and "Save" buttons.

Figure 8 Add new licence

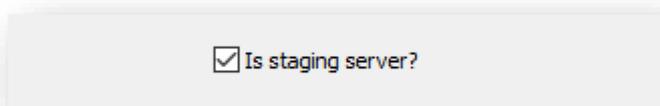
One applied successfully your licenses will appear like this:

Name	Type	Source Domains	Target Domains	Device Count	Migration Expiry	Actions
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	Delete

Figure 9 Successful Licence applied

Staging Mode

PowerSyncPro can be configured with a warm standby to support upgrades or DR. This option can be chosen during the installation screens,



A checkbox labeled "Is staging server?" which is checked.

Figure 10 Enable Staging Mode

or afterwards in the UI



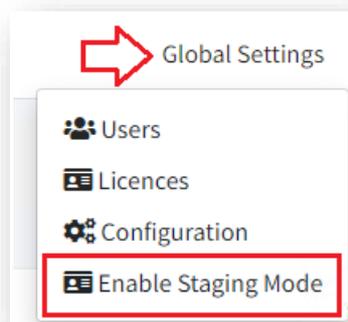


Figure 11 Enable Staging Mode

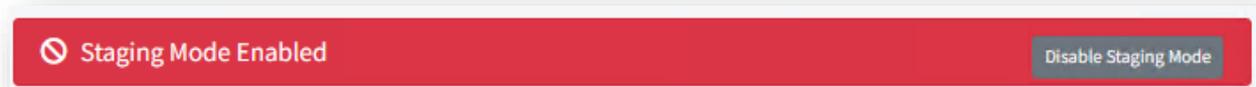


Figure 12 Staging Mode Enabled

Staging mode will run IMPORT & SYNC but not **EXPORT**.

NOTE: Configurations changes made on your primary server are not automatically replicated to the Staging Server unless you are considering SQL always on, or SQL clustering, mirroring or log shipping.

SQL Database Backup / Restore

You can create a backup of the production PSP Server SQL database and restore that SQL database to your staging environment. However, you need to be aware that there are encrypted tables in SQL that are tied to the service account that created them.

When installing and configuring the staging server and you have elected to restore the production server SQL database, then you must also copy the .dat files found in C:\ProgramData\Declaration Software\PowerSyncPro to the same location on the staging server

- PowerSyncProData.dat
- PowerSyncProData.Local.dat

If you have elected to restore the production server SQL database, then you must also use the same service account on both servers that run the PowerSyncPro service itself. Our recommendation is using a single Group Managed Service Account across the two servers.

Finally copy over any certificates used by the SSL endpoint.

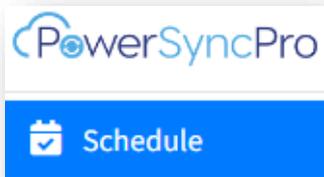
PowerSyncPro Migration Agent Migration History

NOTE: When PowerSyncPro Migration Agent is being used, only the Primary Server will host information about the migration history of Windows Devices that have reported in. So, if you are likely to need to operate from the staging server for an extended duration, then you should consider a periodic SQL backup/restore. We do support any form of SQL Clustering or HA, but only one PowerSyncPro service should be running against a single database.

Endpoints

Finally, it is worth noting that your Remote Agents and Migrations Agents will be configured with a single URL that is pointing at the primary server. These will all need to be updated in the event of an extended failover to staging.

Schedule



The schedule controls how often you want the automated Directory Syncs to run. You should set this schedule to meet your business requirements. The default is 30 minutes but is not enabled by default when you first install PowerSyncPro.

Options Include:

- Run At Specific Times of The Day
- Run Every x Hours x Minutes
 - Interval Time Frame
 - Finish To Start (schedule the start of the next run based on the finish time of the last schedule run)

- Start to Start (schedule the start of the next run based on the start time of the previous schedule run)

Click on “Schedule” on left side pane to open submenu.
Click on “Edit Schedule” and choose your preferred option.

Run At Specific Times of Day

Run Every: 0 Hours 30 Minutes

Interval Time Frame: Finish to Start

Start to Start

Finish to Start

Cancel

Figure 13 Run on a scheduled interval

or

Edit Schedule

Run At Specific Times of Day

+Add Time of Day

06:00

12:00

18:00

00:00

Figure 14 Edit Schedule

Example view of job schedule



The job schedule is built for you when you create sync profiles and mark them as being part of or excluded from the schedule. PowerSyncPro will run as many jobs in parallel as it can to shorten the duration for a single full schedule run.

Job	Status	Last Started	Processed	Skipped	Errors	Warnings
psptestsrc.local	Not Run					
Import Containers	Completed	18 October 23 - 02:34 pm	27	0	0	0
Import	Completed	18 October 23 - 02:59 pm	1461	0	0	0
psptesttrg.local	Not Run					
Import Containers	Completed	18 October 23 - 02:34 pm	27	0	0	0
Import	Completed	18 October 23 - 02:59 pm	1463	0	0	0
Sync	Not Run					
Sync - psptestsrc.local	Not Run					
Sync - Source to Target Contacts*	Completed	16 October 23 - 10:26 am	0	0	0	0
Sync - Source to Target Groups*	Completed	16 October 23 - 10:26 am	635	635	0	0
Sync - Source to Target Users*	Completed	16 October 23 - 10:50 am	800	0	0	0
Export	Awaiting What If Acceptance	Not Run	0	0	0	0
SID History Sync	Idle	Not Run	0	0	0	0
Password Sync	Idle	Not Run	0	0	0	0

Figure 15 Example view of job schedule

Schedule Right Click Options

Within the schedule, for ease, you can Right Click the title to initiate jobs.

Job	Status	Last Started	Processed	Skipped	Errors	Warnings
psptestsrc.local	Not Run					
Import Containers	Completed	18 October 23 - 03:04 pm	27	0	0	0
Import	Completed	18 October 23 - 03:04 pm	0	0	0	0
psptesttrg.local	Not Run					
Import Containers	Completed	18 October 23 - 03:04 pm	27	0	0	0
Import	Completed	18 October 23 - 03:04 pm	0	0	0	0
Sync	Not Run					
Sync - Source to Target Contacts*	Completed	18 October 23 - 03:04 pm	0	0	0	0
Sync - Source to Target Groups*	Completed	18 October 23 - 03:04 pm	635	635	0	0
Sync - Source to Target Users*	Completed	18 October 23 - 03:04 pm	800	0	0	0
Export	Awaiting What If Acceptance	Not Run	0	0	0	0
SID History Sync	Idle	Not Run	0	0	0	0
Password Sync	Idle	Not Run	0	0	0	0

Figure 16 Right Click Import

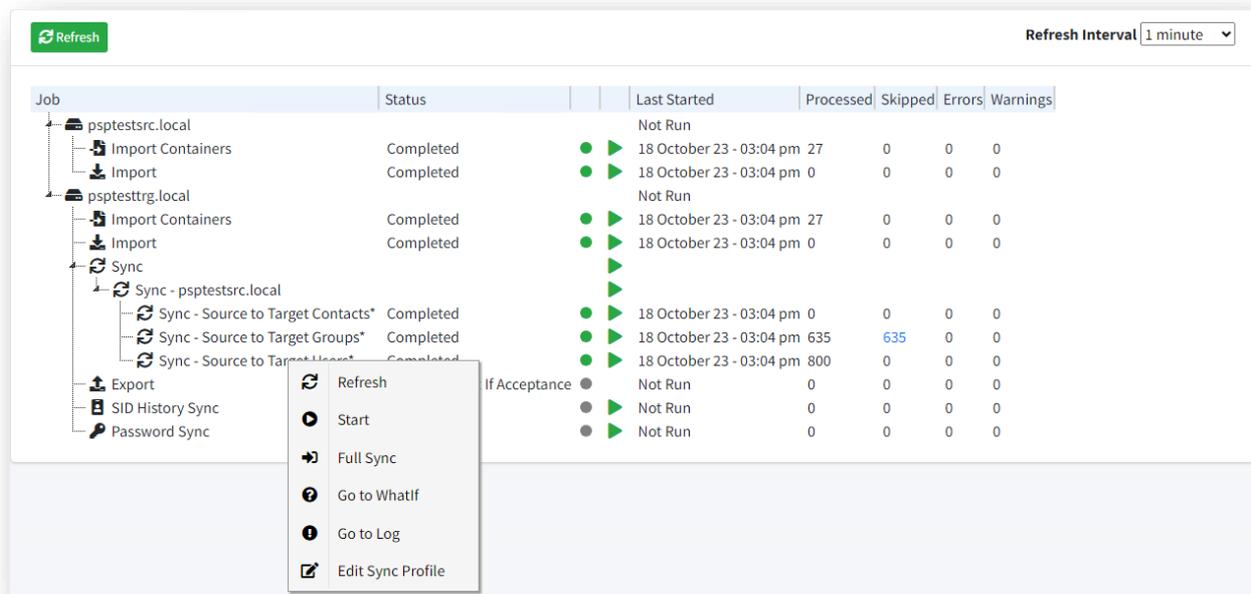


Figure 17 Right click a Sync Profile

Right click Options

Note: "Refresh" refreshes the Schedule screen immediately

Job	Right Click Option
Directory	Edit Directory Refresh Schema
Import Containers	Start or Stop Go to Log
Import	Start or Stop Full Import Go to Log
Sync	Start or Stop Full Sync Go to What If Go to Log
Sync Profiles	Start or Stop Full Sync Go to What If Go to Log Edit Sync Profile
Export	Start or Stop Go to What If Go to Log
SID History Sync	Start or Stop



	Go to Log
Password Sync	Start or Stop Go to Log

Start from Icon

Jobs can also be started and stopped via the green triangle and red square in the Job Action column (next to Job Status).

Status		Last Started
Failed	● ▶	Not Run 2 July 24 - 07:19 pm
Queued	● ■	2 July 24 - 07:19 pm
Idle	● ▶	Not Run

Figure 18 Start from icon

Job Status Icons

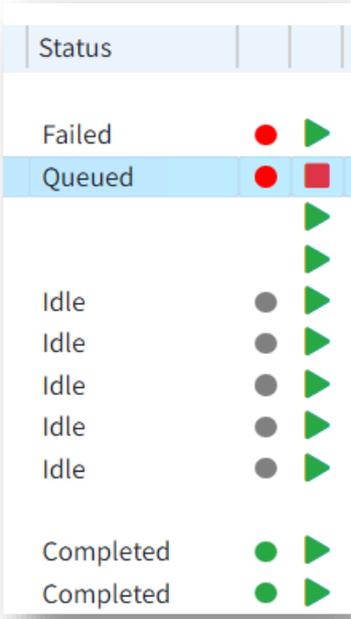
	●	Green Dot	Last job run - successful
	●	Orange Dot	Last Job run – completed with warnings, but no errors
	●	Red Dot	Last Job run – failed or completed with errors/warnings
	●	Gray Dot	Job never ran
	● ▶		

Figure 19 Job status icons

Refresh Interval

This refers to the Schedule screen that you are viewing in the console only.

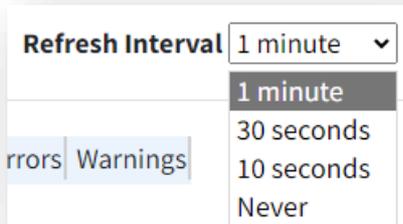
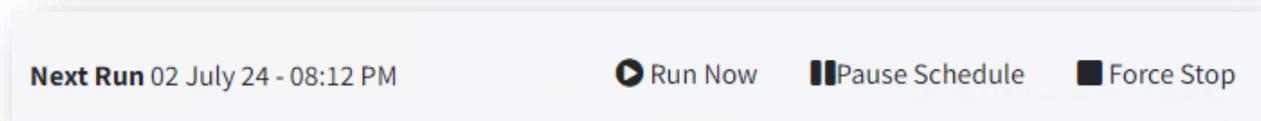


Figure 20 Refresh Interval

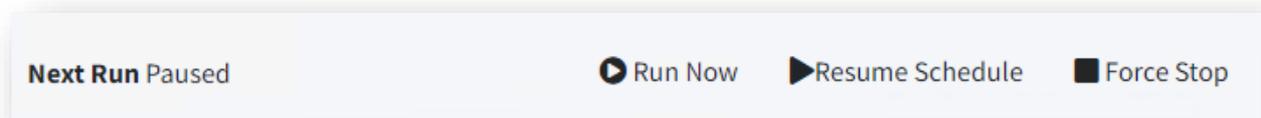
Next Run

Based on your schedule settings, e.g. start Finish to Start, or run at specific times, this tells you when the next synchronisation for all profiles will run.

Next Run - date and time



Next Run - Paused



Run Now

Disregarding when the next run is, this will immediately run all sync profiles that are enabled. This will run Import, Sync, Export.



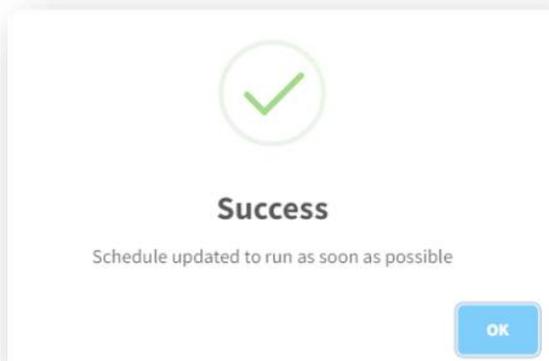


Figure 21 Run sync now success

Pause Schedule

Pause the schedule. This will pause it indefinitely until Resume Schedule is clicked.

Resume Schedule

Resume the schedule. Note, this will not immediately start a synchronisation.

Force Stop

If any part of the synchronisation is running this will hard stop anything in progress. This will not stop future runs. Synchronisation will run again at the next scheduled run time.

Directories

You must create Directory profiles before you can create Sync Profiles or PowerSyncPro Migration Agent Batches.

A directory is a store of information that you want to import from, and potentially export to. Examples are an Entra ID tenant and an Active Directory Domain.

Note that multi-domain forests are handled one domain at a time.

You do not need to specify SOURCE or TARGET Directories. A Directory profile can be both. The use of Source and Target is determined in your Sync Profiles.

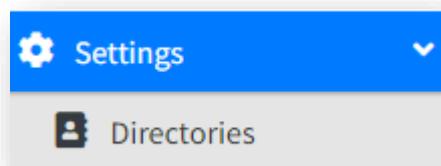


DisplayName	Directory Type	Server Name	Credential Name	Recycle Bin Enabled	Exchange Schema Version	BPRT Expiry Date
CONTOSO	Active Directory	DC01.contoso.t2t.local	psp@contoso.t2t.local	✓	17003	
FABRIKAM	Active Directory	DC01FAB.fabrikam.t2t.local	psp@fabrikam.t2t.local	✓	17003	
PSPGoogleDevSRC	Google Workspace	C0230lops		✓		
Tenant Contoso	Entra ID	9bc4a702-2977-4d17-8f19-64d596b61cbe	2376ad95-f8d2-4491-ac8a-ca261f870fba	✓		01/03/2025
Tenant Fabrikam	Entra ID	d404cf81-40be-4c2b-af2a-0353ecf58683	bec4542a-1d4e-4666-9d3e-c6de32dbf5a1	✓		01/03/2025

Figure 22 Example of configured directories

Create a Directory Profile

Click on “Settings” arrow on left side pane to open submenu. Select “Directories”.



Active Directory

STEPS

- Click “Create”
- **Directory Type:** Choose “Active Directory” from the dropdown menu
- **Server Name:** This is the FQDN of your preferred domain controller
- **Credential Type:** Choose “User Account”
- **Username** Specify your service account.
- **Credential:** Add your service account password to the “Credential” field.
- **Port:** The default port is the LDAP Port is TCP 389 and does not need to be populated unless you have configured your environment away from the defaults



- If you have configured your environment for secure LDAP, you should check SSL and list your port number, the default for SSL is TCP 636 if it is left blank.
- **Export Deletion Threshold:** The number of pending export deletions that should trigger a hold on exporting. Set to your business needs. E.g. Entra Connect is 500 by default, but 100 is typically acceptable.
- **Import Object Types:** In most scenarios you would select only the object types that you want or need to synchronise from and to. The ability to limit here is for performance reasons. Devices only needs to be selected if you are intending to also use the PowerSyncPro Migration Agent for Windows 10/11 migrations
- **Linking Attribute:** Internally, PowerSyncPro uses the ObjectGUID of objects as the glue to bind them. Populating this setting will write the ObjectGUID to your chosen attribute so that you are able see via auditing and reporting or in AD Users and Computers if PowerSyncPro is working with this object. It also allows PowerSyncPro to use this linking attribute to match objects following a SQL restore if the matching attributes might have changed and were not mapped.
- **Allow Import System SIDs:** By default, PowerSyncPro will not import objects who's RID is before 1000, which includes all the standard administrative users and groups. You can enable this option to import these system objects. If you have a specific business need to synchronise these system objects, or membership of the system groups then you can enable this, but we would recommend leaving this setting as unchecked.
- **Allow Import Exchange System Objects:** By default, PowerSyncPro will not import objects that are Exchange System Objects. You can enable this option to import these system objects. If you have a specific business need to synchronise these Exchange system objects, or membership of the Exchange system groups then you can enable this, but we would recommend leaving this setting as unchecked.

Label	Description
Legacy Exchange DN Root	This is read from Active Directory when Exchange is deployed, and is used as the prefix for any newly generated LegacyExchangeDN value
Exchange Schema Version	This is read from Active Directory when the Exchange Schema has been applied
Recycle Bin Enabled	This is read from Active Director

- Click "Save"



After you click save, the Directory configuration will be validated and immediately import the Directory schema.

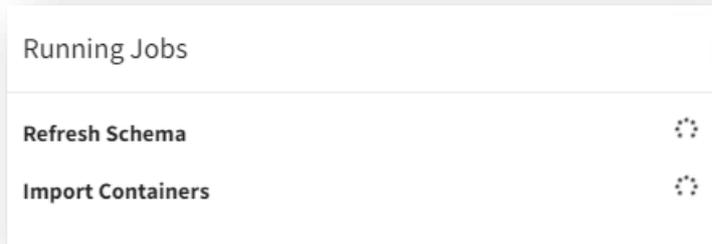


Figure 23 Refresh schema runs after adding a directory



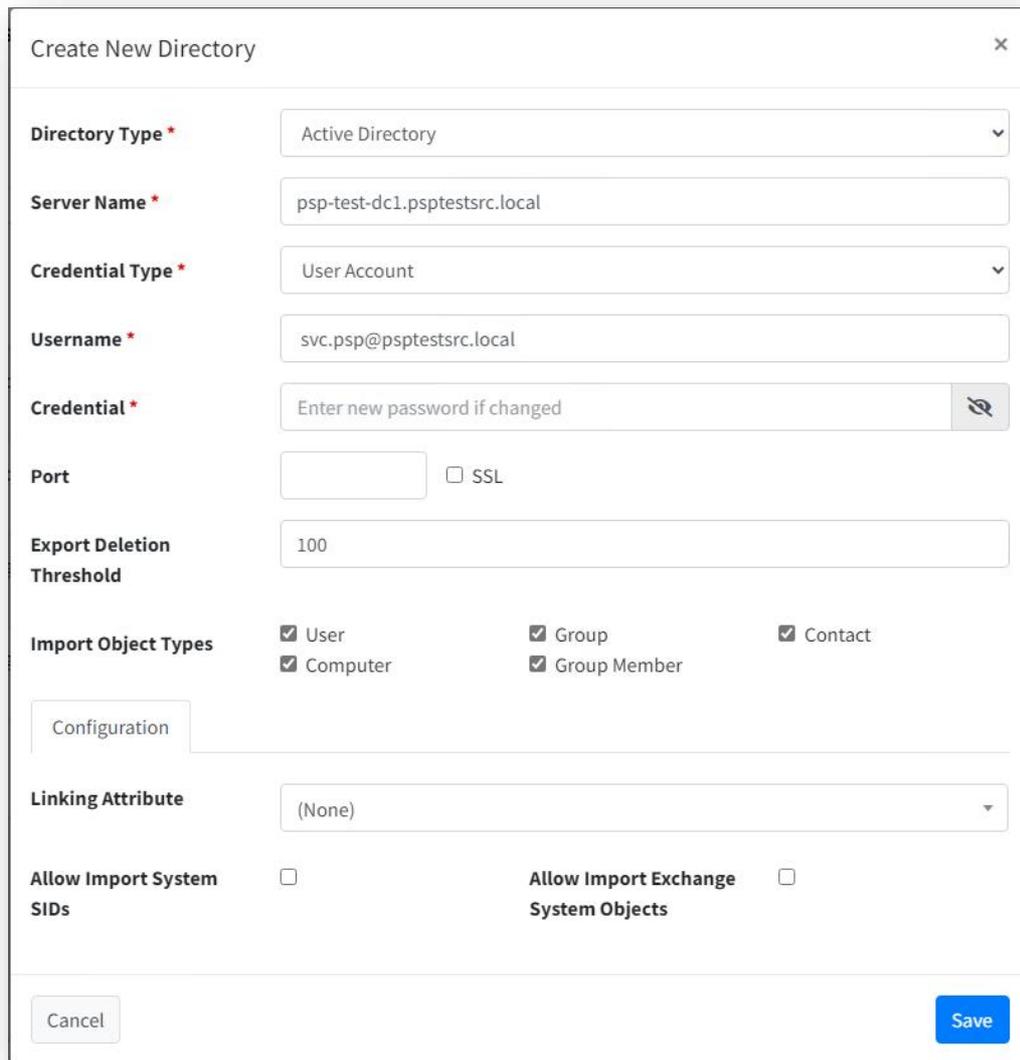


Figure 24 Create New Directory

Microsoft Exchange Schema Information

If the Active Directory has been extended for Microsoft Exchange, then the Information tab will be populated with the Microsoft Exchange Schema Information the next time you view the profile configuration

e.g.



Configuration	Information
Legacy Exchange DNRoot	/o=PSPTTESTSRC/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)
Exchange Schema Version	17003
Recycle Bin Enabled	<input checked="" type="checkbox"/>

Figure 25 Microsoft Exchange Schema Information

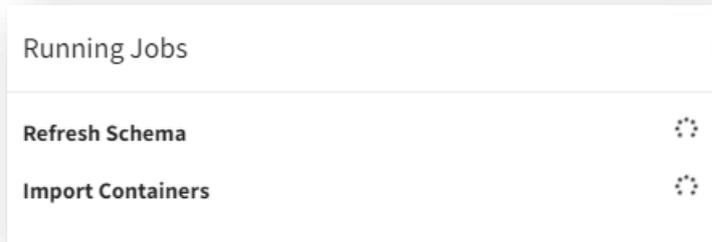
Entra ID

STEPS

- Click “Create”.
- **Directory Type:** Choose “Entra ID” from the dropdown menu
- **Display Name:** This is the *.onmicrosoft.com value from your tenant e.g. contoso.onmicrosoft.com
- **Tenant ID** This is your Entra ID’s Tenant ID (also called directory ID)
- **Application ID:** This is the App Registration Application Id from your prerequisites.
- **Client Secret:** This is the App Registration Client Secret Value from your prerequisites.
- **Export Deletion Threshold:** The number of pending export deletions that should trigger a hold on exporting. Set to your business needs. E.g. Entra Connect is 500 by default, but 100 is typically acceptable.
- **Import Object Types:** In most scenarios you would select only the object types that you want or need to synchronise from and to. The ability to limit here is for performance reasons. Devices only needs to be selected if you are intending to also use the PowerSyncPro Migration Agent for Windows 10/11 migrations
- **Entra ID Exchange:** If you will be synchronising Exchange Online Distribution Groups then you need to select this option. See the prerequisites document for additional configuration information.
- **Certificate Thumbprint:** Only required if you have selected Entra ID Exchange from above. This is the Certificate Thumbprint Registration Client Secret Value from your prerequisites.
- **Bulk Enrolment Token:** This can only be created after you have saved your Entra ID Directory configuration once.

- **Authority URL:** This is used if you will be creating Guest accounts. This is the URL Guest recipients will receive
- Click “Save”

After you click save, the Directory configuration will be validated and immediately import the Directory schema.



Create New Directory ✕

Directory Type *

Display Name *

Tenant ID *

Application ID *

Client Secret *

Export Deletion Threshold

Import Object Types
 User Group
 Device Group Member

Entra ID Exchange Link Entra ID Exchange

Certificate Thumbprint

Bulk Enrollment Token

Authority URL

i Can only generate a bulk token once the directory is saved.

Figure 26 New Entra ID Directory created

Link Entra ID Exchange

Entra ID Exchange: If you will be synchronising Exchange Online Distribution Groups then you need to select this option. See the prerequisites document for additional configuration information.

Entra ID Exchange	<input checked="" type="checkbox"/> Link Entra ID Exchange
Certificate Thumbprint	16791F7EB0988C02443E9631149B6795B37438EE

Figure 27 Link Entra ID Exchange

NOTE: If you configure this after you have created your Entra Directory, then you **MUST** also run **Refresh Schema** to bring in the Exchange Online attributes to use in any future Sync Profiles

Running Jobs
Refresh Schema 

Google Workspace Directory Setup

STEPS

- Click "Create"
- **Directory Type:** Choose "Google Workspace" from the dropdown menu
- **Display Name:** This is just a label, so use something descriptive here. E.g. your Primary SMTP Domain for Google Workspace
- **Customer Id:** You can obtain the Customer Id from the Account Settings page:
<https://admin.google.com/u/1/ac/accountsettings>

 Account settings	Profile
	Name PSPGoogleDevSRC
	Customer ID C0230lops
	Profile information Profile settings

Figure 28 Google Customer ID

- **Service Account Token:** This is the file created from step 4 in the Prerequisites guide

- **Export Deletion Threshold:** Set to your business needs. E.g. Entra Connect is 500 by default, but 100 is typically acceptable.
- **Import Object Types:** In most scenarios you would select only the object types that you want or need to synchronise from and to.
- **Click Save**

After you click save, the Directory configuration will be validated and immediately import the Directory schema.

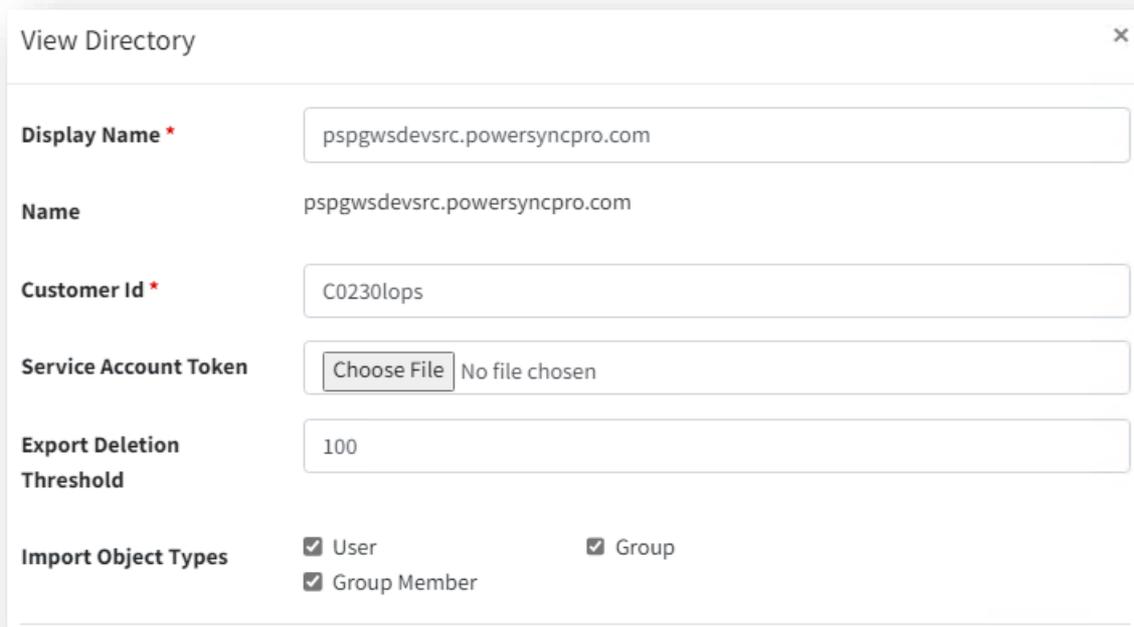
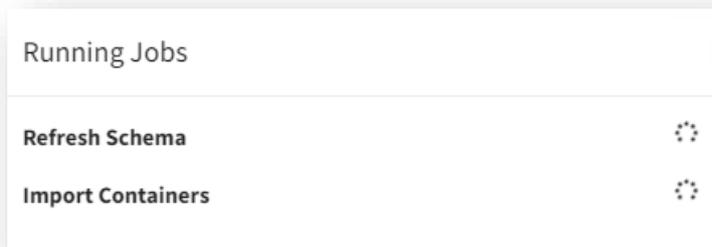


Figure 29 Google Directory successfully created

Refresh Schema

When you create a directory the first time this automatically runs. You must run this again if you know that the schema has changed. e.g. If you were to extend your Active Directory to support Microsoft Exchange, or if you patch Microsoft Exchange as this often makes changes to the schema.

The Schema is critical to PowerSyncPro directory as it brings in all available attributes that are then shown within the rest of the configuration.

Import Containers

You should run this before creating any Sync profiles. This will import for Active Directory, all OUs, that you will need on sync profiles for scoping and writing to target OUs, and from Google all containers.

Import Objects

The very first time you import objects a Full Import is run. This will bring in every object type selected on the directory configuration, and for each object type it will import the attributes that PSP needs given the sync profiles and features that have been configured.

On scheduled execution, delta imports are run. This will only import changed attributes for objects.

If you make a configuration change to a sync profile that requires a different attribute to be imported, then a full import is run the next time import runs.

SMTP Domains

The SMTP Domains feature allows you to control the flow of proxyAddresses from Source to Target, or if you specifically want to remove a proxyAddresses entry from a target object.

By default, if this setting is NOT configured then no proxyAddresses will be synchronised, even if proxyAddresses is mapped in a sync profile.

The exception to this configuration is for Primary Mail Address. If the source mail attribute is populated then the mail attribute from an object will be written to the target proxyAddresses entry as the Primary SMTP Address value.



You may only need to synchronise certain protocols in proxyAddresses, like x500, sip, smtp but not x400. Each protocol can be added with Allow Sync Addition/Allow Sync Removal set to control the addition and removal of this protocol's entries from the target object.

You may only need to synchronise a subset of smtp/sip domains. e.g. the project could be a divestiture and only a subset of domains are being moved over, or some domains are being decommissioned and are not required, or some domains are local only.

Considerations

Primary SMTP Address

If you are setting different Primary SMTP Address values then you will need a complex expression for the mail attribute, and this will automatically flow to proxyAddresses as the Primary SMTP Address once you have the allow sync addition domain added.

proxyAddresses entries

You will need to use a complex expression for proxyAddresses to re-write the domain portion on entries if you are also wanting to add other email addresses like previous name changes or genuine alternate email address variations.

targetAddress

You may also need to have a mapping rule for targetAddress if you are in a pre-cutover stage.

If you are in long term coexistence with another organisation and are intending to only create Mail-Enabled Users (or Mail Contacts) then you will need to have a mapping for targetAddress and give consideration as to what you want the UPN and Primary SMPT Address to be in the target.

Moving Domains

If you are migrating the Domain as part of a migration effort, you should consider not flowing the migrating Domain until you have verified the Domain in the target and it is ready for use.

Entra Connect has a known issue/feature/by design where if a proxyAddresses entry was added to an on-premises object, *before the domain was validated in Entra*, then any subsequent Entra Connect sync runs will not pick up those entries as they are not seen as a "change".

It is therefore prudent to NOT add additional proxyAddresses entries before the domain has been validated in a target tenant.

Sometimes, the domain is going to be migrated to the target tenant but remains in the source tenant to start with.



By deferring the addition of the domain to proxyAddresses until that domain has been added and verified to the target tenant, you have an easy way to cutover the domain from one side to the other (assuming it is not going to be deleted from the source Active Directory / Entra Id too).

If you are deleting the domain in the source then care must be taken to not import the deletion of those proxyAddress entries until they have been synchronised to the other side, and then the SMTP Domain must be removed from the PSP configuration or set to **Allow Sync Removal = False** before any importing of objects that contain the proxyAddress removals that took place in the source domain)

NOTE: We strongly advise checking your What If report when executing this phase.

What If Report

Be sure to run a What If report to confirm that your proxyAddresses changes are working as expected.

Allow Sync Addition

- For any additional smtp domain value to synchronised and added to the target you MUST first have the sole value **smtp** listed as a domain. This tells PowerSyncPro that any proxyAddresses that begins with smtp are in scope, followed by any other domain values listed here that are then evaluated
- For x500 addresses, you only need to list x500 as the domain name. All x500 addresses will be processed

The colon is NOT required at any time in these setting screens. i.e. smtp and x500 are correct, **smtp:** or **x500:** are incorrect

proxyAddresses attribute mapping

NOTE: In addition to setting these options, you must also map the proxyAddresses attribute in your sync profile for these to flow.

Source Attribute	Target Attribute	Simple Expression Name	Complex Expression Name
proxyAddresses	proxyAddresses		rewrite proxyAddress entries

Figure 30 mapping proxyAddresses



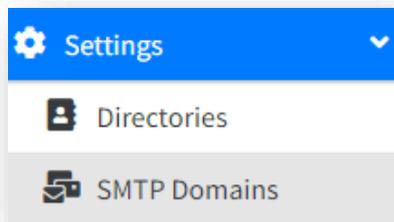
Allow Sync Removal

If you need to *remove* a proxyAddresses entry from a target object then you can use this option. If an object comes into scope, and is matched, and the profile is configured for update only, or create and update it will remove any domain configured for removal.

When you add or remove any smtp domains, PowerSyncPro sees this as a configuration change and the sync profile will change to Awaiting What If acceptance and will need to be accepted.

Create new SMTP Domain Configuration

Click on “Settings” arrow on left side pane to open submenu
Select “SMTP Domains” from the left-hand navigator



Configure smtp / x500 / sip entries to flow to proxyAddresses

Requirement: As previously outlined, for any additional smtp domain value to be synchronised and added to the target you MUST first have the sole value smtp listed as a domain. This tells PowerSyncPro that any proxyAddresses that begins with smtp are in scope, followed by any other domain values listed here that are then evaluated.

Steps

- Click “Create”
- Choose your target Directory from the “Directory” dropdown menu. This is the directory for the objects of which you want to add or remove proxyAddresses entries
- Specify **smtp** in the “**SMTP Domain Name**” field. This is not case sensitive. SMTP and smtp have the same effect. SMTP will not preclude other non-primary proxyAddresses entries from flowing
- Click on “Allow Sync Addition” checkbox
- Click “Allow Sync Removal” checkbox
- Click “Save”

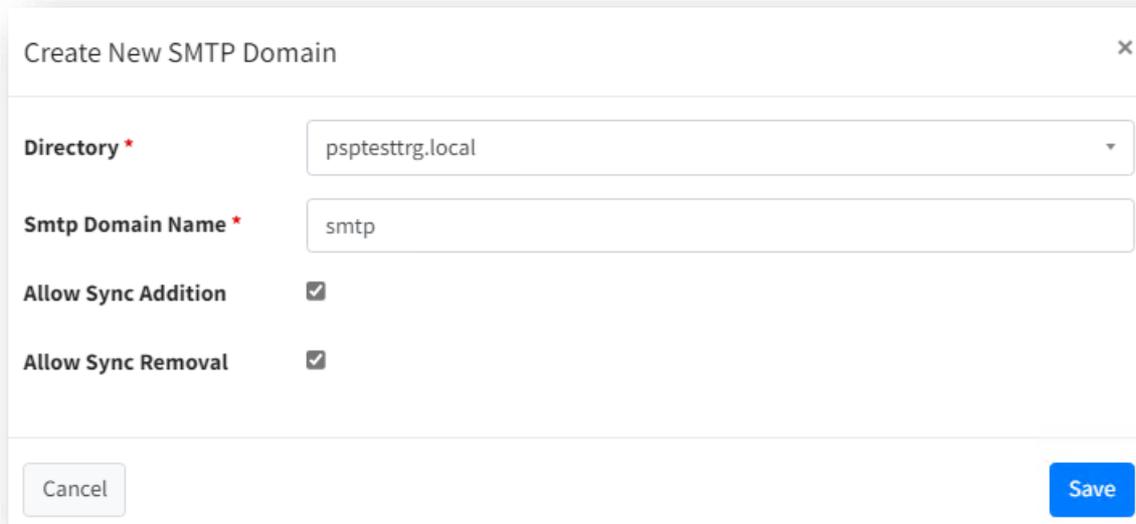


Figure 31 shows a dialog box titled "Create New SMTP Domain" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Directory ***: A dropdown menu showing "psptesttrg.local".
- Smt Domain Name ***: A text input field containing "smtp".
- Allow Sync Addition**: A checked checkbox.
- Allow Sync Removal**: A checked checkbox.

At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Save" on the right.

Figure 31 add smtp addresses

Repeat the same process to allow x500 address flow

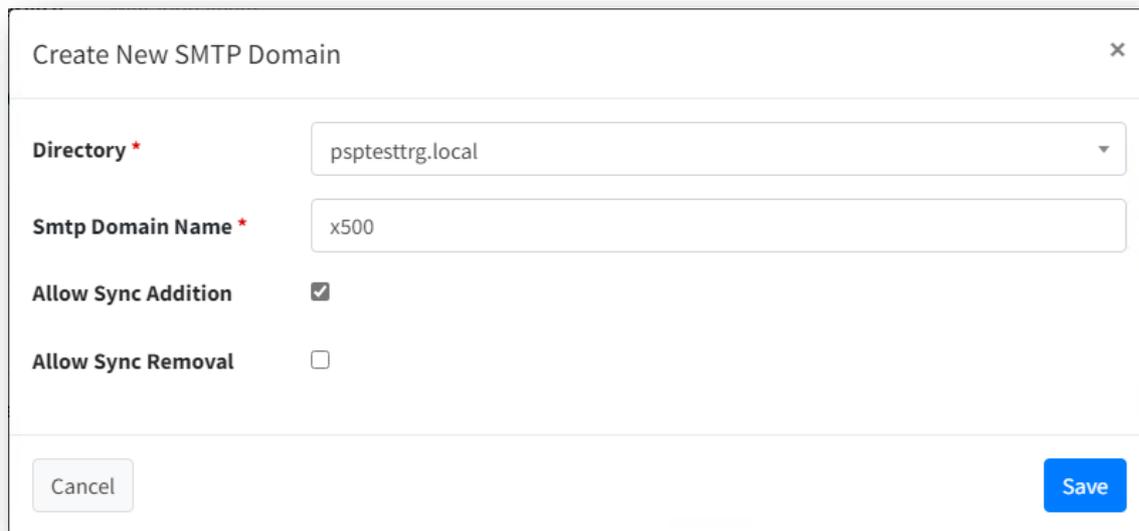


Figure 32 shows a dialog box titled "Create New SMTP Domain" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Directory ***: A dropdown menu showing "psptesttrg.local".
- Smt Domain Name ***: A text input field containing "x500".
- Allow Sync Addition**: A checked checkbox.
- Allow Sync Removal**: An unchecked checkbox.

At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Save" on the right.

Figure 32 add x500 addresses

Repeat the same process to allow sip address flow



Create New SMTP Domain ✕

Directory *

Smtp Domain Name *

Allow Sync Addition

Allow Sync Removal

Configuring SMTP Domain Values to flow

- Click “Create”
- Choose your target Directory from the “Directory” dropdown menu
- Specify the **domain value address** in the “Smtp Domain Name” field this is the right part of @.
 - The @ symbol is not required
- Click on “Allow Sync Addition” checkbox
- Leave “Allow Sync Removal” checkbox unchecked
- Click “Save”

Create New SMTP Domain

Directory * psptesttrg.local

Smtp Domain Name * psptestsource.powersyncpro.com

Allow Sync Addition

Allow Sync Removal

Cancel Save

Figure 33 Adding an SMTP Domain value to flow

Download CSV

You can make a backup of your current SMTP Configurations if needed.

SMTP Domains

Create Import Download Template

Directory (All) Domain Name

Download CSV

Figure 34 Download SMTP Domains configurations



Import bulk domains

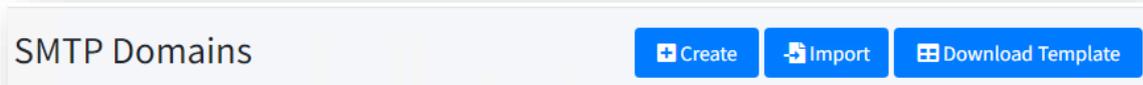


Figure 35 Import Domains from CSV

If you have a large amount of SMTP Domains to work with, then importing from CSV may be more efficient.

NOTE: This will REPLACE any previous configurations you may have already created. If you have made a backup via Download CSV you can simply manipulate this file and add entries.

Steps

First either download the Template, or build your own three column CSV with:

- smtpDomainName
- allowSyncAddition
- allowSyncRemoval

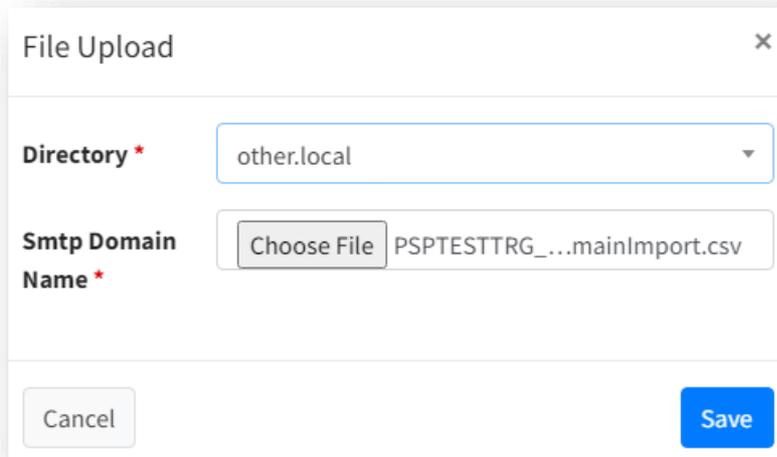
Populate the rows as necessary e.g.

smtpDomainName	allowSyncAddition	allowSyncRemoval
smtp	TRUE	TRUE
x500	TRUE	FALSE
sip	TRUE	FALSE
removethis.local	FALSE	TRUE
fabrikam.local	TRUE	FALSE
fabrikam.com	TRUE	FALSE
fabrikam.mail.onmicrosoft.com	TRUE	FALSE

Now choose Import

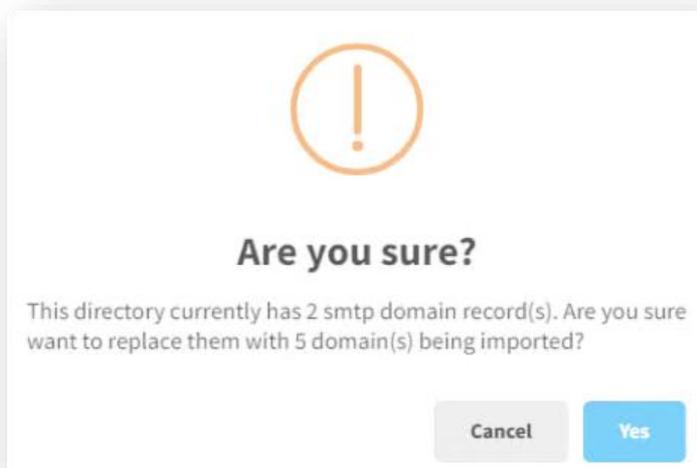
Select your target Directory from the drop down and chose your CSV created from earlier.





A dialog box titled "File Upload" with a close button (X) in the top right corner. It contains two main sections: "Directory *" with a dropdown menu showing "other.local", and "Smtp Domain Name *" with a "Choose File" button and a text field containing "PSPTESTTRG_...mainImport.csv". At the bottom, there are "Cancel" and "Save" buttons.

Figure 36 Upload CSV file for Domains



A confirmation dialog box with a large orange warning icon at the top. The text reads: "Are you sure? This directory currently has 2 smtp domain record(s). Are you sure want to replace them with 5 domain(s) being imported?". At the bottom, there are "Cancel" and "Yes" buttons.



Example of SMTP Domains Configuration

Domain Name	Allow Sync Addition	Allow Sync Removal
powersyncpro.com	true	false
pspgwsdevsrc.powersyncpro.com	true	true
psptesttarget.powersyncpro.com	true	false
psptesttrg.mail.onmicrosoft.com	true	false
sip	true	false
smtp	true	true
x500	true	false

Figure 37 Example Domains configuration

Sync Profiles

NOTE: You will need to have created **Directories** before you configure **Sync Profiles**.

Supported Sync Scenarios:

- Active Directory to Active Directory with passwords and SIDHistory
- Active Directory to Entra ID (without passwords)
- Entra ID to Active Directory (without passwords)
- Entra ID to Entra ID (without passwords)
- Google to Active Directory (without passwords)
- Google to Entra ID (without passwords)

Supported Sync Object Types:

- Users
- Contacts
- Entra ID Guests
- Active Directory Groups (all)
- Entra ID Groups

- Exchange Online Distribution Groups
- Google Groups

Directory Sync is not limited to the same source and target object type. e.g.

- Source Users or Groups can be created as a target Mail Contacts
- Target Contacts can be converted to a User or Group
- On-premises Active Directory Users can be created as an Entra ID Guest

Key Concepts

Schema Attributes

You need to have a good understanding of schema attributes for the respective directories you are working with. This will be important when you are mapping attribute values, particularly across different directory types or you need to perform attribute manipulation.

One-way sync

The source objects are ALWAYS authoritative for attributes, meaning that if you update an object in the target, and that object and those attributes are in scope for a sync profile, **then they will be overwritten by the source object on next sync.**

It is possible that you have **two one-way syncs** for a subset of attributes and passwords, but every sync is a one-way sync. If you have two one-way syncs, then the last change seen by PowerSyncPro will win.

Group Membership. It is an available configuration to retain target group memberships and not synchronise any source members

Scope/Match/Map

Directory Sync profiles mainly consist of the following: **scoping, matching, and attribute mappings.** These key components ensure your target objects are created and/or updated in the correct state for your business needs.

The Directory Sync Profile does much more than this through the other Sync Options as will be seen in later sections.

What If

PowerSyncPro DirSync is configured to not execute a new profile until the operator has approved the What If report. This will be seen at the schedule screen.

This is to ensure there is a “*belt & braces*” approach to DirSync so that unintentional changes are not applied to the target environment due to misconfiguration.

What If is **always applied** to new profiles and also on subsequent DirSync Profile edits, or other configurations like Complex Expressions and SMTP Domains changes.

The What If report or Single Object Report will allow you to spot check that your DirSync design and aspirational changes are in fact going to be applied correctly. What If reports are covered in more detail later.

Directory Sync Flow

PowerSyncPro will perform its end to end synchronisation as follows: Import/Sync/Export

Import

An Import will bring every object in scope from the directory. This is an important feature to note as this allows us to have the complete view of all directory objects to ensure we can work with conflicts even if they are not currently scoped on a sync profile. Imports that run on a schedule are Delta unless a configuration change such as changes to the attribute mapping tables requires a Full Import.

Full import v delta import

You should not need to choose between full or delta import as the schedule will elevate to full import or full sync when it needs to.

- Full import will re-read all of the objects from the directory and reconcile with what PowerSyncPro has stored
- Delta Import only imports the changes since the last import
 - All scheduled runs are delta
- The scheduled runs will elevate to full import when it needs to
- A full sync will always follow after full import

Sync

This is the process of evaluating the configuration profile by scope and matching, object type, target type, sync action, and evaluating any transformations such as attribute mapping, attribute rewriting via simple and complex expressions, mail options and account enable options.

Full sync v delta sync

You should not need to choose between full or delta sync as the schedule will elevate to full sync when it needs to.

- Full Sync will re-sync all of the in scope objects
- Delta Sync will only synchronise those objects marked as having been updated/requiring a sync
 - All scheduled runs are delta
- The scheduled runs will elevate to full sync when it needs to
- A full sync will always follow after a full import

Export

This is the final writing of objects and their attributes to the target directory based on your sync profile configurations. Export is suspended if a What If report is pending.

Export is not available if there is no valid licence key.

Deletion Threshold

Power Sync Pro Directory configuration allows to set a deleted objects limit so that a configuration error can limit that amount of potential damage done unintendedly.

Export Deletion Threshold	<input type="text" value="100"/>
----------------------------------	----------------------------------

Figure 38 Export Deletion Threshold

Import	Completed	● ▶
Sync		▶
Sync - itmurray.local		▶
Sync - Contoso to Fabrikam Match and Convert to MEU	Completed	● ▶
Sync - Contoso to Fabrikam Groups	Completed	● ▶
Sync - Contoso to Fabrikam Users	Completed	● ▶
Sync - Divest Widgets	Completed	● ▶
Export	<u>Awaiting Deletion Threshold Confirmation</u>	● ▶
SID History Sync	Completed	● ▶
Password Sync	Completed	● ▶

Figure 39 Awaiting Deletion Threshold Confirmation

Active Directory Recycle Bin

We highly recommend enabling the Active Directory Recycle Bin in all your Active Directory Environments. PowerSyncPro can search and restore objects that were deleted or fell out of scope in the source and were deleted in the target.

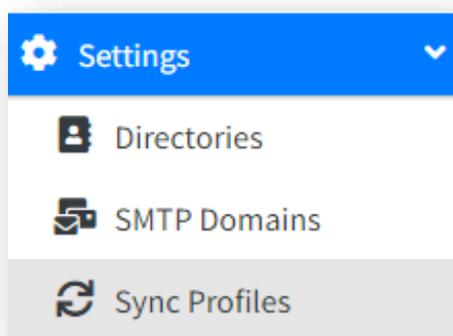
- `Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target contoso.com`
- `Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -Target fabrikam.com`

You may additionally need to grant the PowerSyncPro service account rights over the Recycle Bin.

Action	Object Name	Object Container
Update (Restore from Recycle Bin)	Wynter Elliott	charlie.local/Aquistions/Contoso
Update (Restore from Recycle Bin)	Zoe Courtney	charlie.local/Aquistions/Contoso
Update (Restore from Recycle Bin)	Wendy Webb	charlie.local/Aquistions/Contoso
Update (Restore from Recycle Bin)	Will Gaudoin	charlie.local/Aquistions/Contoso

Figure 40 Restore from Recycle Bin

Creating a Sync Profile



The Sync Profile is the fundamental configuration item that controls what synchronises between the directories. You can have multiple Sync Profiles for a directory, and multiple Sync Profiles for an object type, although care must be taken with overlapping Sync Profiles since you cannot synchronise two source objects to the same target object.

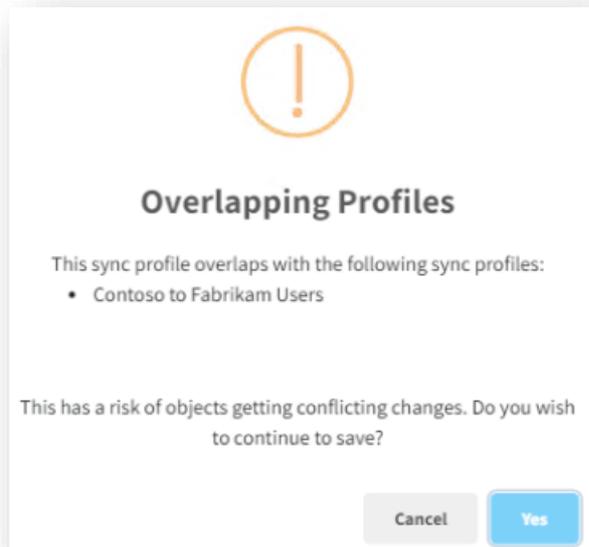


Figure 41 Overlapping Profiles

Click on “Create” to create new sync profile.



Figure 42 Create Sync Profile



Exclude From Schedule:

Exclude From Schedule

Figure 43 Exclude from Schedule

Use this if you do not want this profile to run at all. No scheduled Imports/Sync/Exports will be executed against Sync Profiles that are excluded from the schedule.

NOTE: A sync profile that is excluded from schedule **can still be run manually** from the Jobs option. Additionally, if you run a What If for “All” sync profiles on a directory, it will run Import and Sync for an excluded profile.

Leaving it unselected **does not mean it will run immediately after you save the profile**. All new and edited sync profiles must pass through the What If acceptance gate first.

Name

Choose a meaning descriptive name in your profile. This will appear on your schedule and other reports.

Source Directory

Choose the correct source Directory for your use case that you configured earlier.

Target Directory

Choose the correct Directory for your use case that you configured earlier.

Template

A set of pre-canned starter Templates are provided with a starter set of Object Types and Sync Action plus suggested set of mapping attributes.

It is NOT an exact solution for your own business or project needs and will almost certainly need additional customisation.

Template are presented based your Source and Target Directory types. E.g. AD to AD, Entra ID to Entra ID or Entra ID to AD

You can choose one of the following templates.

Active Directory to Active Directory

- Contacts
- Groups
- Users

Entra ID to Entra ID

- Groups
- Users

Google Workspace to Active Directory

- Groups
- Users

Copy Existing Profile

If you have previously created a Sync Profile and it *mainly* matches your requirements for an additional profile, then you can build a new sync profile baseline from that profile and then customise it as needed.

An existing profile option will only be presented where your Source and Target Directory type are the same e.g. AD to AD, AD to Entra ID, Entra ID to Entra ID.

Copy Existing Profile is especially useful where you have a completely different requirement for scoping and mappings, but there is enough commonality to give you a head start baseline. An example might be copying a user's type profile to use for Shared Mailboxes.

Object Type

This is your Source Object Types that you are working with. The options will vary depending on your Source Directory selected:

- Active Directory will present: Contact, Group, User
- Entra ID will present Group and User
- Google Workspace will present: Group, User



Sync Action

The action that this profile will take:

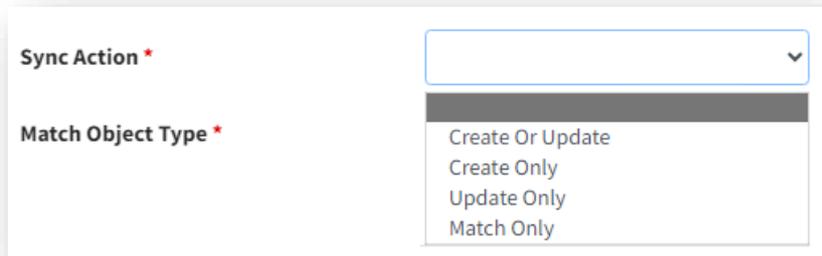


Figure 44 Sync Action

- **Create or Update**

Use when you are absolutely sure of your scoping and matching for users, you can use this option.

Create will occur where there is no Match found based on your Match rules and where PPSync has the appropriate rights to Create an object in the target and where there would not be a hard conflict / AD violation that would cause it to fail. i.e. sAMAccountName already in use.

Update will occur when your object is Matched based on your Match rules. If an object is matched, then all attributes will flow from the Source to the Target. Update is often useful when there may have been a manual or other process to create objects in the target but they are not quite as you want them or are out of date.

NOTE: Beware of using this for first time syncs. An unexpected or unwanted update to a target object could overwrite the UPN, mail and sAMAccountName as well as the password if that option is selected.

- **Create Only:** Recommended for first time User Syncs so that you do not inadvertently update a mismatched / conflicted / clashed User.
 - Once PowerSyncPro has created a user, it will implicitly also update that user in subsequent syncs due to having created it.
- **Update Only:** If you do not need to create any new objects, but only update existing objects. This is used for reverse standalone password syncs. See Password Sync later



- **Match Only:** This is used for PowerSyncPro Migration Agent to build a User Translation Table used for repermissioning Windows Profiles when using PowerSyncPro Migration Agent.
 - **NOTE:** objects that already matched by any of the three above options will automatically be added to the User Translation Table. A dedicated Match Only profile is not required for Workstation Migrations if the above is already satisfied.

NOTE on implicit matching

If PowerSyncPro *creates* an object it will automatically become **matched** for future syncs via its own internal matching tables. PowerSyncPro uses the ObjectGUID of objects as the glue to bind them. Therefore, if your Sync profile is configured as Create Only, or Create or Update, you should take care to note that objects **created by PSP will also be updated on subsequent syncs**.

This is by design.

Create Object Type:

Your choices are dependent on your target Directory type:

- For Active Directory your options are Contact, Group or User.
- For Entra ID your choices are Group, Internal Member, Internal Guest, External Member and External Guest.
- Source Users and Groups can also be created as Contacts in the target.

Match Object Type

Match Object Type is used to limit the target objects it tries to match to. This is used in combination with your Match Rules that you will configure.

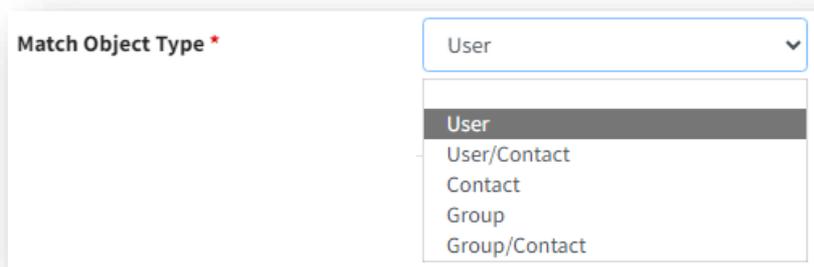


Figure 45 Match object type

User/Contact

Use match by User/Contact if you need to convert target contacts to users.

Group/Contact

Use match by Group/Contact if you need to convert target contacts to groups.

Create or Update Behaviour

The following behaviour will be seen when the defined attribute used in your **match rules** is a match (or unmatched). This behaviour will apply when **Convert Contact** option **not** selected,

	Match Found	Match Not Found
Create Only	Do nothing	Create object
Create or Update	Update target	Create object
Update Only	Update target	Do nothing

A warning will be written to the Message Logs where a conflict is detected.

Convert Contact

Convert Contact is a special Sync Action that is available on Sync Options and is discussed in a later section.

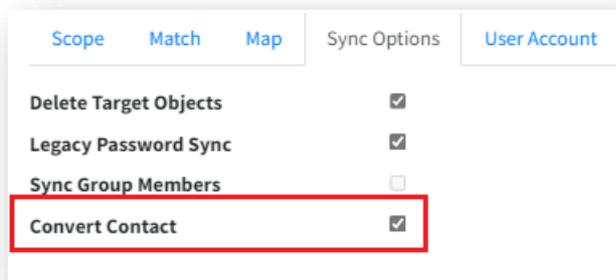


Figure 46 Convert Contact

This requires your Match Object Type to be User/Contact or Group/Contact.

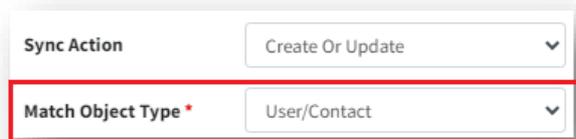


Figure 47 Match by User/Contact

Create or Update Behaviour for Convert Contact

The following behaviour will be seen when the defined attribute used in your **match rules** is a match (or unmatched).

	Matched Contact Found	Matched Object Type Found	Matched object AND Contact found	Match not Found
Create Only	Matched Contact converted	Do nothing – log entry written	Do nothing – log entry written	Create new object
Create or Update	Matched Contact converted	Attributes updated	Merge	Create new object
Update Only	Do nothing – log entry written	Attributes updated	Merge	Do nothing

Scope

Scoping can be very simple from “All” through to fine level granular scoping by OUs, inclusion attribute(s), exclusion attribute(s), or by using complex expressions.

All scoping options set on this screen are evaluated e.g.

If you choose to scope on:

- Source Container: pspdevsrc.local/Contoso/users (And Children)
- Inclusion Attribute: extensionAttribute10 = SYNC
- Exclusion Attribute: department = Engineering

Then an Object located in this OU, **AND** has both extensionAttribute10 = SYNC **AND** department = Engineering will **NOT** be synchronised.

Any exclusion will supersede all inclusions.



Descoped Objects

NOTE: If an object should fall out of scope in a sync profile, and you have enabled Delete Target Objects, then those objects will be DELETED in the Target.

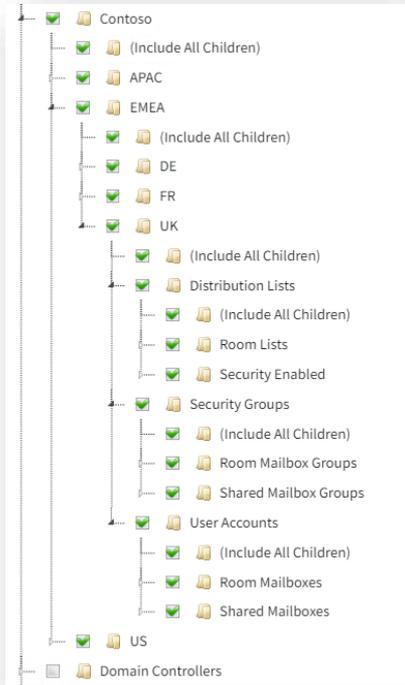
Scope by Source Containers

Containers and Organizational Units are used interchangeably in PowerSyncPro. You should have run Import containers before making your selections, or they may not all appear. Selecting (include All Children) will toggle the child OUs on and off for ease.

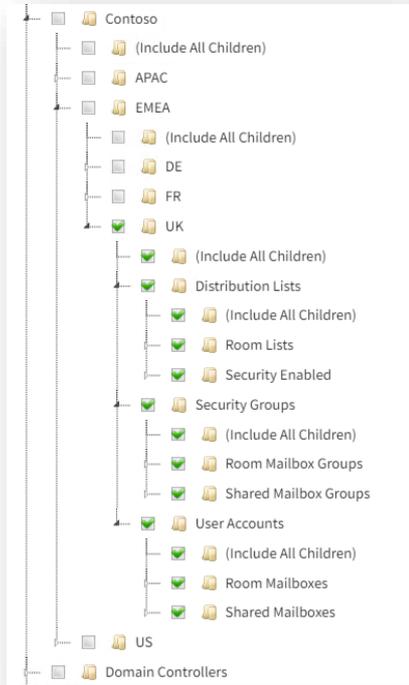
You can choose

- All objects and child OUs in an OU
- A single OU, or multiple OUs and all child OUs
- A single OU, or multiple OUs within an OU structure

All objects in a root OU and all objects in child OUs



All objects in a single OU and all objects in a child OUs



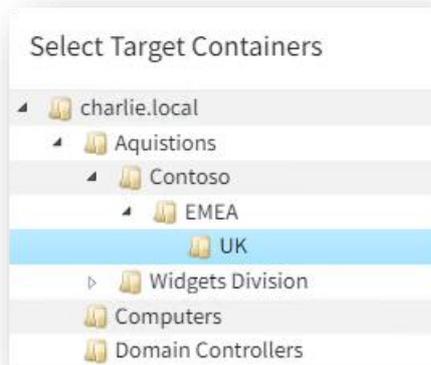
Objects in a single OU within an OU structure



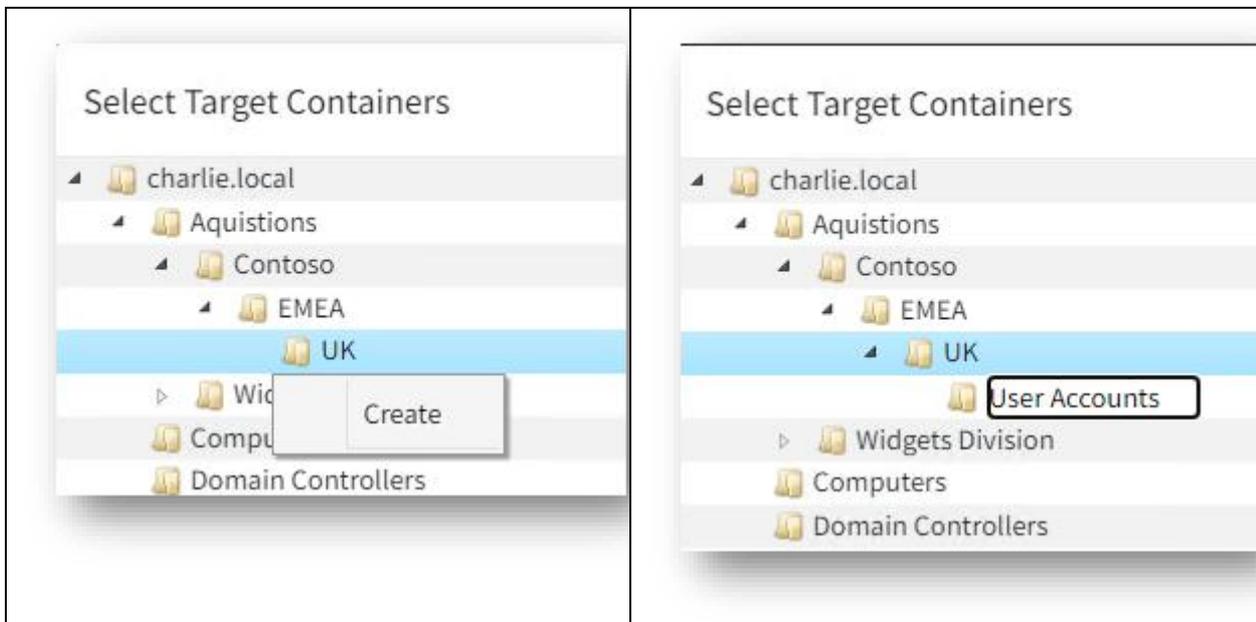
Target Container

You can choose an existing container.





or elect to create a single new OU directly via the sync. This creation will happen on the export phase of PSP.



NOTE: Creating an OU / Container here is not dependent on using the Create options below.



Create Target Container

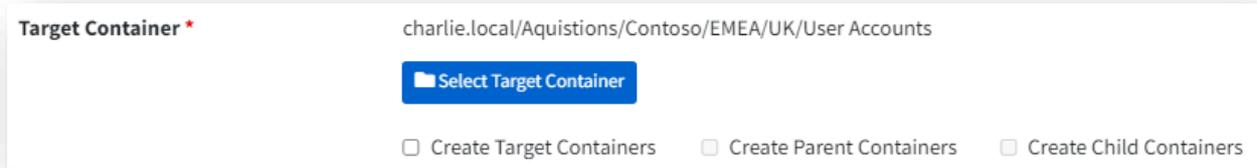


Figure 48 Create target containers

Create Target Container

If you do not select **Create Target Containers** then the Target Container you specified will get all the newly created objects placed directly within it. i.e. a flat structure.

If you do select **Create Target Containers**, then the Target Container you specified will get the name of the Container selected from the *Source Containers* created as a child of the Target Container you selected from above. Then the objects are placed within their respective child container(s).

So, if you selected Widgets Division/UK and Widgets Division/US as source containers, and **Acquisitions** as your Target Container, then you will end up with Widgets Division as an OU under **Acquisitions** with UK and US as children and the objects in the respective container depending on where they came from.

Create Parent Containers

If you select Create Parent Containers then as well as creating the Container selected in the Source Containers, it will also create all parent containers of that selected Container.

So if you selected your source as: Widgets Division/UK and Widgets Division/US then your Target Container “**Acquisitions**” will contain Widgets Division and beneath that will be UK, US

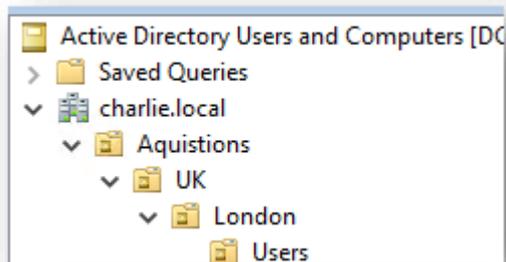
e.g.

SOURCE	TARGET
<ul style="list-style-type: none"> ▼ Widgets Division <ul style="list-style-type: none"> > US UK 	<ul style="list-style-type: none"> ▼ charlie.local <ul style="list-style-type: none"> ▼ Aquisitions <ul style="list-style-type: none"> > UK > US

Create Child Containers

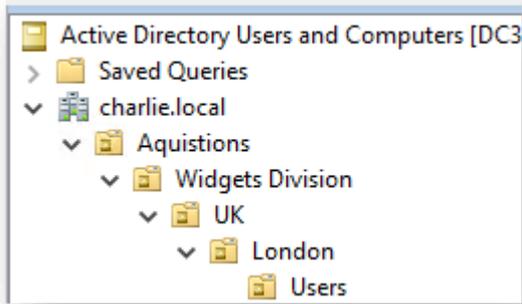
If you select Create Child Containers, then as well as creating the Container selected in the Source Containers, it will also create any child Containers of that Source Container depending on where the source object is located.

So if you selected your source as Widgets Division/UK (and ticked all sub containers) and your objects are located in London/Users underneath that, and target as **Acquisitions** then you would end up with: Acquisitions/UK/London/Users



If Create Parent Containers is also selected then you will have: Acquisitions/Widgets Division/UK/London/Users





For all three of these Create Container options, if the object in the source is moved then it will be moved in the target too, however empty Containers in the target won't be deleted when the last object is deleted from that Container

A container will only be created in the target if there is a valid in scope object synchronising from the source to the target. i.e. empty containers will not be created unless they are part of the tree to the lowest OU containing an object.

If you leave these options enabled, they will continue to create OUs per the above on each sync.

Scope by

Inclusion Attribute

Using scope by Inclusion Attribute is a finer level of scoping allowing you to only include objects that meet your attribute criteria regardless of your OU scoping.

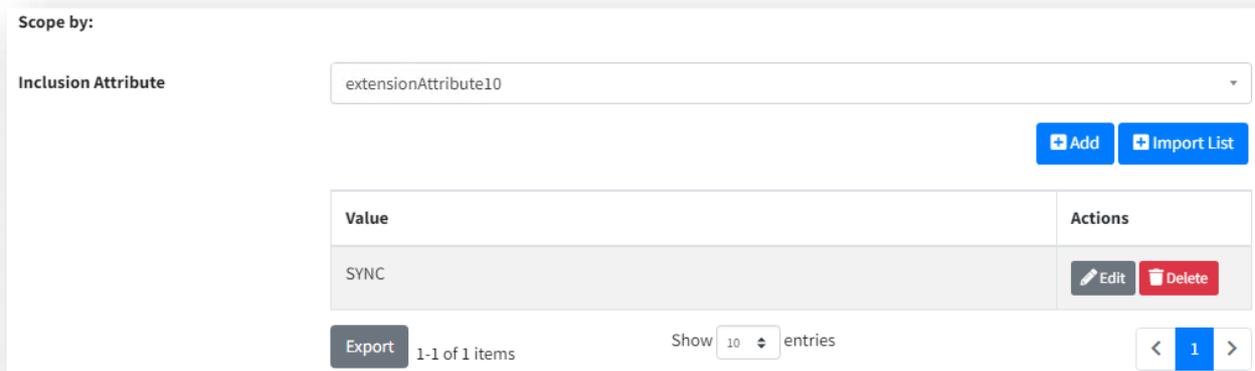


Figure 49 Inclusion attribute

Choose from the available attributes for your directory selected. Attributes will only be available for your particular schema. i.e. Active Directory, Entra ID or Google.

Attribute values are not case sensitive.

Multiple values

You can use multiple values here by using the Import List option.

Exclusion Attribute

Value	Actions
Engineering	Edit Delete

Figure 50 Exclusion attribute

Multiple values

You can use multiple values here by using the Import List option.

Scope by Complex Expression

The expression to evaluate on any in scope objects (after checking the inclusion/exclusion values above), which may cause the object to be marked out of scope.

Complex expressions are detailed later, but you can use C# to build a complex scenario to meet your scoping needs.

e.g. I want to only scope the following:

- Active Directory Enabled accounts and
- with an email address that ends with @widgets.com and
- the Department contains Research and
- the Country is UK and
- State or City is London and

- The Job title contains Developer and
- msExchRecipientTypeDetails = 1

Then you can use a complex expression to achieve this level of granularity.

Note on include/exclude and complex expressions.

These are all evaluated. If you scope by OU, inclusion attribute, exclusion attribute and complex expressions they are all calculated. If at any point an object achieves **not scoped status**, then no further evaluation occurs.

Match

Use when you need to match objects for the purpose of updating them. Use when you are creating objects, to ensure that you don't create a duplicate object when there is already an existing object that is in conflict.

User Translation Table

Matching is also used for the purpose of creating a user translation table that is required when performing Windows Workstation Migrations. The user translation table is a list of source and target SIDs that is used when repermissioning Windows User Profiles.

Match is evaluated on an **“OR”** basis, so ANY match on any of the attributes you list here is considered a Match. They are evaluated in the order you list them here and will work through the list checking for any protentional match.

“AND” matching is not supported.



Source Attribute	Target Attribute	Complex Expression Name
employeeID	employeeID	
sAMAccountName	sAMAccountName	
displayName	displayName	
userPrincipalName	userPrincipalName	Match Users by UPN

Figure 51 Matching objects by attribute

Map

The mapping section is where you can choose the subset of attributes you would like written to the target objects.

If you used “Create Sync Profile from Template”, then some of these will be populated for you, but please note that a template is only a **base set of attributes** and is unlikely to be fully fit for use for your own use cases. It does not include any Exchange Schema Attributes.

Download CSV

Here you can download your current mappings via the Download CSV option for purposes of re-use or documentation.

Import

If you want to bulk Import a set of mappings you can first use **Download Template** that will give you the headings to use:

- SourceAttributeName
- TargetAttributeName
- SimpleExpressionName
- ComplexFunctionName

Only Source and Target headings are required. You can use the Simple expression and Complex Function if you have created these in advance. If you make a mistake in your attributes, or you choose attributes in your source or target that are not available in your schema, then these lines will simply be ignored.

Create

For all other individual mappings or customised mappings use Create. You can map like for like e.g.

- DisplayName to DisplayName
- givenName to givenName
- sn to sn
- department to department

or you can map to a different attribute e.g.

- employeeID to SAMAccountName
- company to extensionAttribute1

You can map the same Source to multiple target attributes e.g.

- employeeID to employeeID
- employeeID to SAMAccountName
- employeeID to mailNickname

NOTE on special attribute processing

- **legacyExchangeDN**

Does not need to be explicitly mapped. If the Mail Enable option is set, then this attribute will be written to the target proxyAddresses attribute as an x500 address. x500 must be listed in SMTP domains.

- **showInAddressBook**

Does not need to be explicitly mapped. If Mail Enable option is set, then this attribute will be populated in the target if the Exchange Schema extensions exist.

Different Directory Schema Types

If you are synchronising from Active Directory to Entra ID or Google to Active Directory then you will need to know the corresponding attribute name for a correct mapping. e.g.

Active Directory to Entra ID



AD Source Attribute	Entra ID Target Attribute
displayName	DisplayName
givenName	GivenName
sn	Surname
mail	Mail
userPrincipalName	UserPrincipalName
sAMAccountName	MailNickname
c	Country
telephoneNumber	BusinessPhones
mobile	MobilePhone

Google Users to Active Directory

Google Source Attribute	AD Target Attribute
FullName	displayName
Aliases	proxyAddresses
PrimaryEmail	mail
GivenName	givenName
PrimaryEmail	userPrincipalName
FamilyName	sn

Attribute Manipulation

In your target environment you may have a need to create objects with attributes presented in a different way. This is where you can rewrite attributes with either a Simple Expression or a Complex Expression (see later for more information). An example may be that a global organisation has a requirement for all users last name to be upper case, and that all mail addresses be lowercase. You may want to append Company Name or Department to the DisplayName for clarity in the Global Address List.

Mapping without a Source Pairing

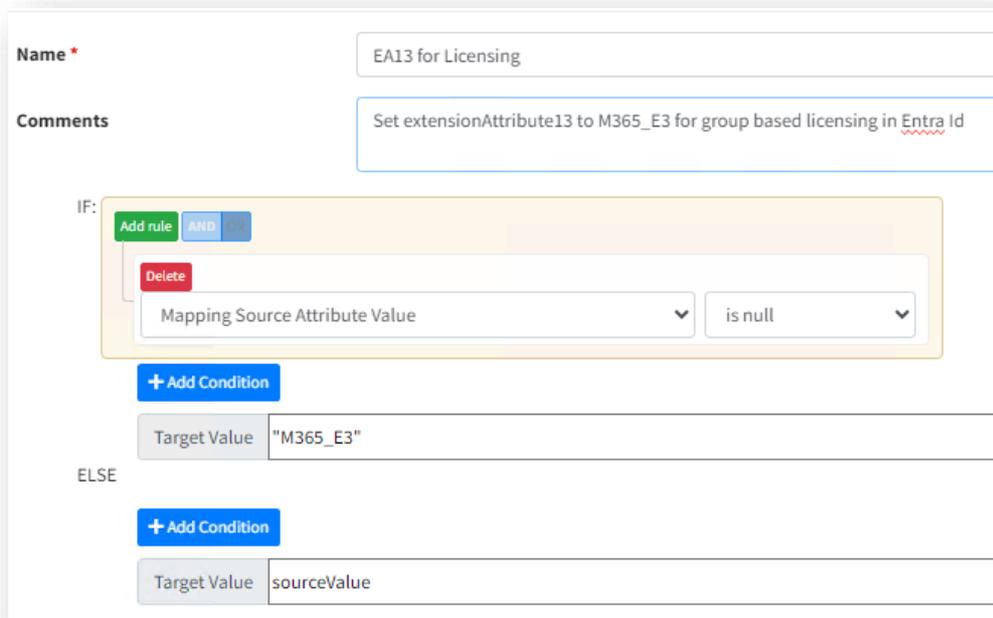
Additionally you may have a scenario where the source Active Directory is not extended for Microsoft Exchange but you have a requirement to map a target Attribute such as msExchRecipientTypeDetails or targetAddress etc



Another scenario could be that you need to populate an attribute such as an extensionAttribute that is used in Entra ID to build a Dynamic Group that is used for Group based licensing and that particular attribute is reserved solely for that purpose in the target.

Source Attribute	Target Attribute	Simple Expression Name	Complex Expression Name
	extensionAttribute13		EA13 for Licensing

Figure 52 Mapping without a source attribute



The screenshot shows a configuration window for a mapping rule. The 'Name' field is 'EA13 for Licensing' and the 'Comments' field contains 'Set extensionAttribute13 to M365_E3 for group based licensing in Entra Id'. Under the 'IF:' section, there is a condition: 'Mapping Source Attribute Value' is null. Below this, there are two 'Add Condition' buttons. The 'ELSE' section has a 'Target Value' of 'sourceValue'. The 'IF' section also has a 'Target Value' of '"M365_E3"'. There are also 'Add rule' and 'AND' buttons in the 'IF' section, and a 'Delete' button for the condition.

Figure 53 Complex Expression to set a string value



Simple Expression

Source Attribute	Target Attribute	Simple Expression Name
displayName	displayName	Suffix Company to DisplayName
givenName	givenName	
initials	initials	
sn	sn	uppercase

Figure 54 Example Simple Expression in a mapping

Complex Expression

It may be a requirement in your organization to have email address and UPN formatted as firstname.lastname + target organization domain name. e.g.

JSmith@contoso.com should be created as john.smith@fabrikam.com

Source Attribute	Target Attribute	Simple Expression Name	Complex Expression Name
userPrincipalName	userPrincipalName		Set UPN to fabrikam.com
mail	mail		Set Mail to fabrikam.com
proxyAddresses	proxyAddresses		rewrite proxyAddresses

Figure 55 Example complex expression in a mapping

See Complex Expressions later.

Microsoft Exchange Attributes

As stated earlier, shipped templates do not include any Microsoft Exchange Schema extension attributes. You should carefully plan for the msExch* attributes that you need to flow and the impact they will have in the target.

If you populate certain msExch* attributes that are defined for Shared Mailboxes / Rooms, e.g.

- msExchRecipientDisplayType
- msExchRecipientTypeDetails
- msExchRemoteRecipientType

and if Entra Connect is being used in your target, then this will have the effect of telling Exchange Online to provision a Shared Mailbox / Room.

Quite often this will be part of your design and can be incredibly useful.

Sync Options

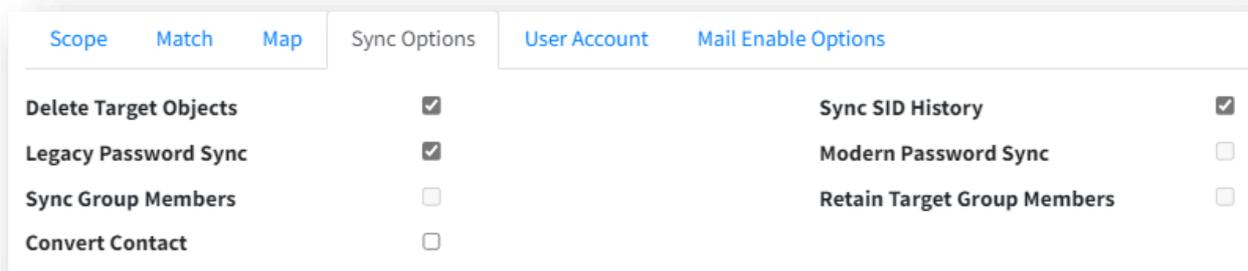


Figure 56 Sync Options

Delete Target Objects



Once PowerSyncPro becomes authoritative for an object in its scope, it will also be able to delete objects in the target if they are deleted in the source or fall out of scope. If this is not a feature you require then you should deselect it here.

Delete Target Objects



Active Directory Recycle Bin

We highly recommend that you enable the Active Directory Recycle bin in your environments. PowerSyncPro will search the Recycle Bin when a sync runs and will restore an object if it has a match for it.

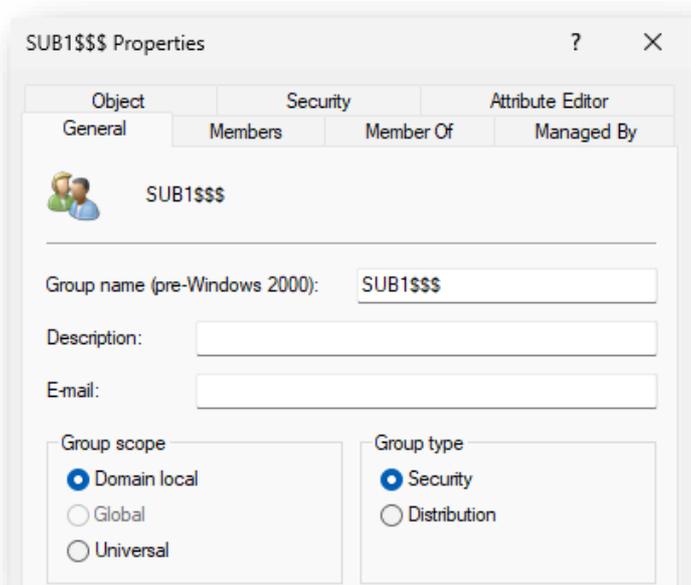
Sync SID History

If you are performing an Active Directory migration, you will almost certainly need to migrate the SID information to the SIDHistory on the target. Use this option to achieve this. Previous SIDHistory is also synchronised.

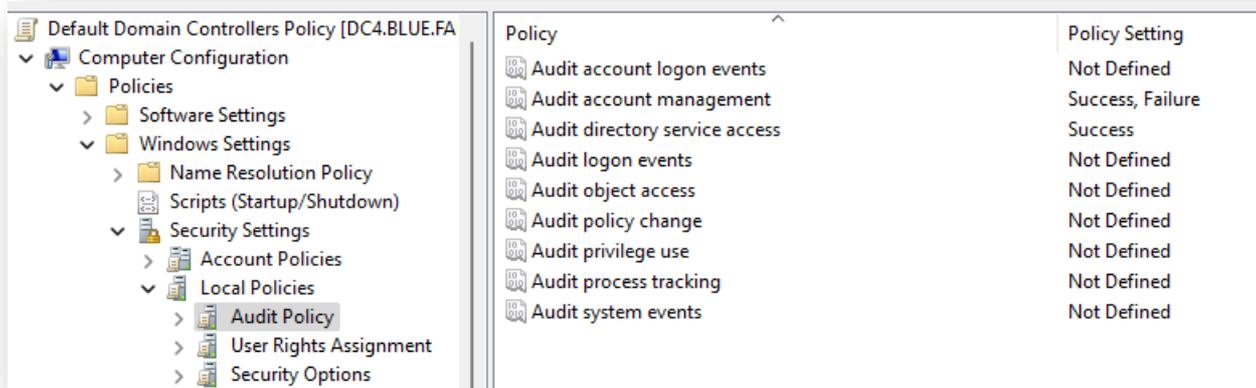
Synchronising SID to SIDHistory requires additional Active Directory configuration in your environments such as:

In the source domain:

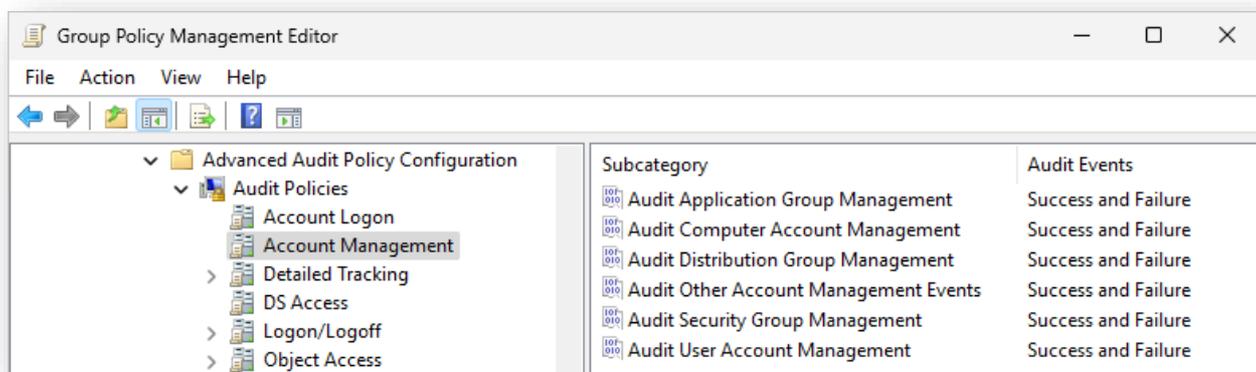
- A local group called SourceDomain\$\$\$ - where SourceDomain is *your* actual Active Directory Domain

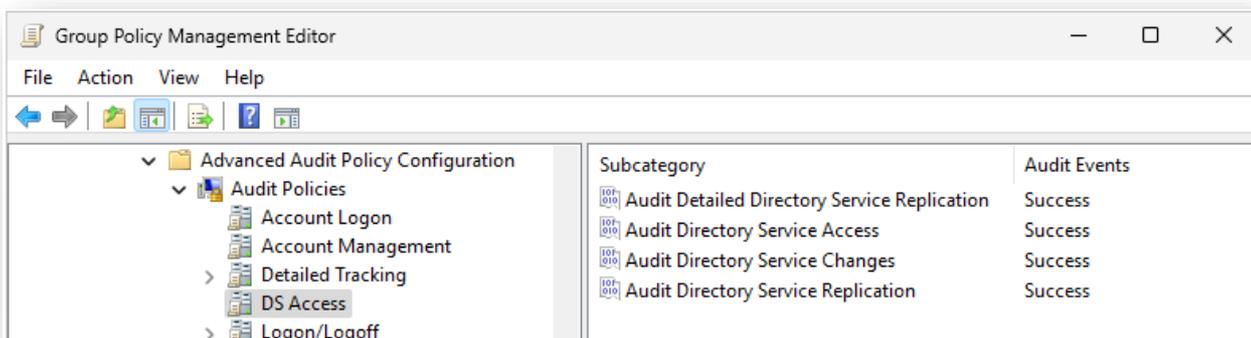


- Enable TCP/IP client support on the source domain PDC emulator
 - Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
 - REG_DWORD TcpipClientSupport = 1
- Enable auditing in the target domain on the Default Domain controllers Policy



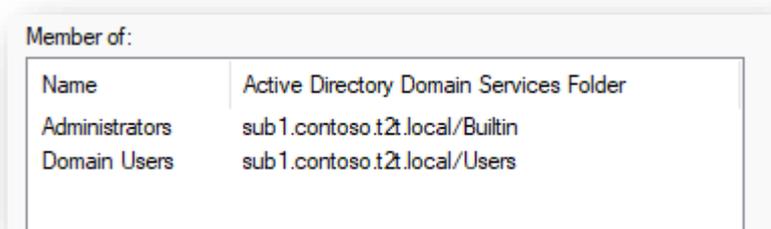
- Enable Advanced Auditing in the target domain Default Domain controllers Policy (when you have advanced audit policy enabled)



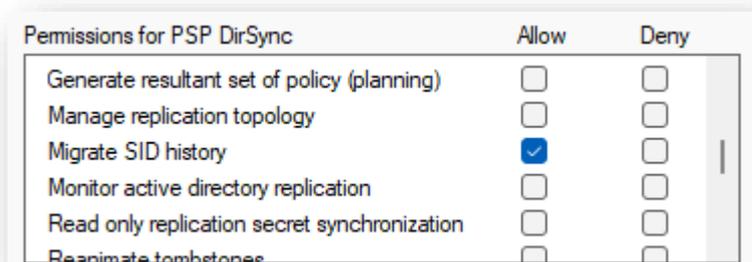


Account Permissions

- Source credentials must have administrator access to the source PDC emulator

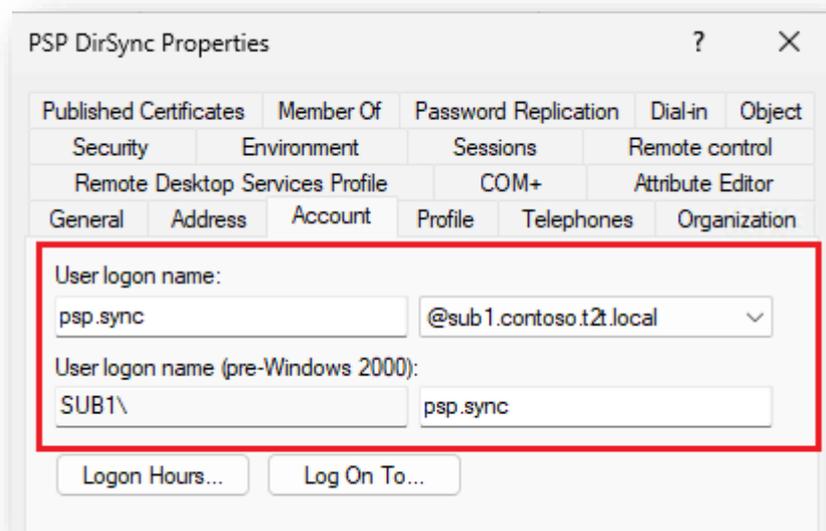


- Migrate SIDHistory permissions are required on the target domain

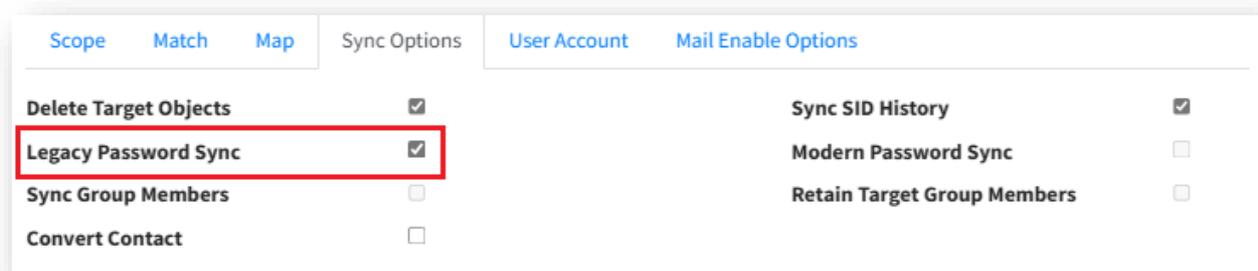


Note: The sAMAccountName of Service account that is executing the SID to SIDHistory sync must match the UPN left part if you have used userPrincipalName in your Directory configuration.





Legacy Password Sync



Tick this option if you need to synchronise passwords between Active Directory Domains. Note, it is only the hash that is copied, not the actual password. Regardless of your target Active Directory password requirements this value will be written. i.e. if your source password is 8 characters and simple, but your target requires a complex password of at least 12 characters, **the source password will still be written.**

Active Directory user Account option “User must change password at next logon” will also flow as part of the password sync. userAccountControl can be mapped to achieve other account related options.

Synchronising passwords requires additional configuration in your environments.



Permissions for PSP DirSync	Allow	Deny
Reanimate tombstones	<input type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes All	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes In Filtered Set	<input type="checkbox"/>	<input type="checkbox"/>
Replication synchronization	<input type="checkbox"/>	<input type="checkbox"/>
Run Protect Admin Groups Task	<input type="checkbox"/>	<input type="checkbox"/>

Modern Password Sync

Scope	Match	Map	Sync Options	User Account	Mail Enable Options
Delete Target Objects			<input checked="" type="checkbox"/>		
Legacy Password Sync			<input type="checkbox"/>		
Sync Group Members			<input type="checkbox"/>		
Convert Contact			<input type="checkbox"/>		
				Sync SID History	<input checked="" type="checkbox"/>
				Modern Password Sync	<input checked="" type="checkbox"/>
				Retain Target Group Members	<input type="checkbox"/>

This option requires the Remote Password Sync Agent installed on every Domain Controller.

This option will facilitate syncing passwords where the environment has been configured to no longer use RC4 and only use AES/SHA for password hashes. It intercepts the password and uses that to set the password on the target directory in near real time.

NOTE: With this method it is important that the target’s password complexity requirements are the same or less restrictive than the source.

You can only either use Legacy or Modern Password Sync – not both.

Sync Group Members

If you are performing synchronisation of Groups, you may have a requirement to create empty groups and not bring over group membership from the source, or if there are existing groups in the target with the same name and function and you do not want to alter the group memberships of. In this case you should de-select Sync Group Members.

Retain Target Group Members

If this option is not selected, then the complete list of source group memberships will replace any target group memberships.

If this option is selected then existing group members who are not migrated will remain, even if the target group is updated after a synchronisation. Target Group memberships are not updated to the source (unless there is a corresponding sync profile for the reverse sync)

Convert Contact

Use this option if you have known contacts in the target that represent users or groups from the source. It may be that another tool or manual process had created contacts to support a consolidate Global Address List but you now need to convert them to actual User or Group object types.

Invite Redirect URL

The redirect URL to use within the welcome message sent to Guests that are created. The default is set to: `https://myapps.microsoft.com/?tenantid=<the target directory tenant id>`

The screenshot shows a configuration window with several sections:

- Object Type ***: User (dropdown)
- Sync Action ***: Create Or Update (dropdown)
- Create Object Type ***: External Guest (dropdown)
- Match Object Type ***: User (dropdown)
- Sync Options**: A tabbed interface with 'User Account' selected.
- Delete Target Objects**:
- Retain Target Group Members**:
- Sync Group Members**:
- Send Invite Message For External Users**:
- Invite Redirect URL ***: `https://myapps.microsoft.com/?tenantid=a888482e-470b-4069-a64e-46f22bc75a61`

Figure 57 Invite Redirect URL

User Account

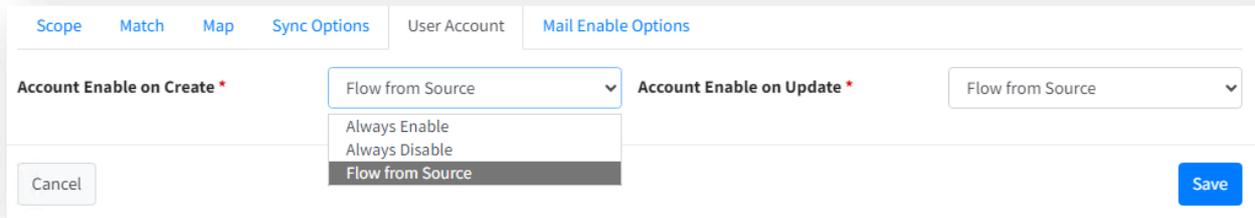


Figure 58 User Account Sync Option on Create

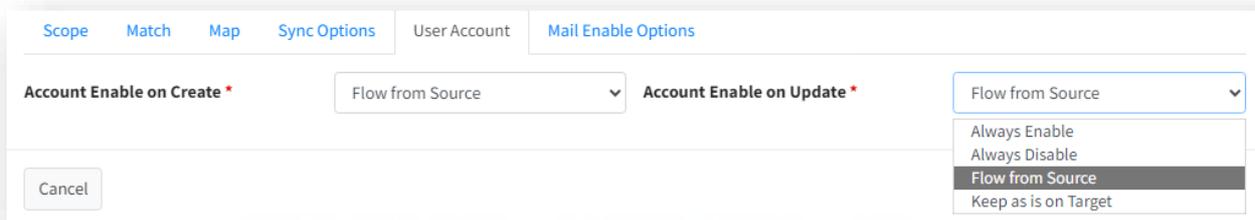


Figure 59 User Account Sync Option on Update

Account Enable

This feature allows you to define how Active Directory User Accounts should be configured in your target during the create process, or subsequent updates that are processed.

You have the options of:

Flow from Source

This has the effect of replicating the source status of a user account. i.e. the status quo.

Always Disable

Irrespective of the source account status, this will make the account AD Disabled in the target. This may be useful for pre-staging to ensure end-users cannot log in too early if they become aware of the account. It is also often useful for creating Shared Mailboxes or Room Mailboxes that are typically AD Disabled Accounts.

Always Enable

Irrespective of the source account status, this will make the account AD Enabled in the target. This may be required during or after a migration event in which you wish to go live in the target for end-users.

Keep as is on Target

This ensures that if the account status has been edited / updated on the target, then PSP will leave it alone “as is” and do nothing.

Mail Enable

Default processing

PSP will always process the following attributes

- mail
- mailNickname
- proxyAddresses
- groupType
- reportToOriginator

If those attributes are present on the source object, they will be written to target. The legacyExchangeDN is written to the proxyAddresses attribute as an x500 address.

If they are not present, PowerSyncPro will build them. and set the appropriate target attributes. i.e. sAMAccountName to mailNickname

NOTE: If the mail attribute is not present on the source object, then no mail attribute will be written to the target. This is by design.

Plus the following attributes are written for mail-enabled users *if* the target schema is extended for Microsoft Exchange

- legacyExchangeDN This is created as a GUID +mailNickname or sAMAccountName if mailNickname is not present
- msExchRecipientDisplayType set as required for User/Group/Contact
- msExchRecipientTypeDetails set as required for User/Group/Contact
- showInAddressBook set per target if present in the Address Lists Container in the Configuration\Services\Microsoft Exchange\[org]

NOTES:

msExchVersion is NOT set by default. If you have a reason to set this then please create a mapping and if necessary, use a Simple Expression to hard code a value.

msExchRemoteRecipientType is also not set by default. If you have a need to set this to control the mailbox in Microsoft 365/EXO, then use Complex Expressions to get / set msExchRecipientDisplayType, msExchRecipientTypeDetails and msRemoteRecipientType as desired

Attribute Mappings Precedence

If there are attribute mappings present in the mapping configuration, they will always be processed.

Mappings supersede Default processing. e.g. there is a mapping such as sAMAccountName to mailNickname or a complex expression to set mail, proxyAddresses or msExch* attributes - then those mappings will take precedence.

Mail Enable Options

The screenshot shows the 'Mail Enable Options' configuration panel. It has tabs for 'Scope', 'Match', 'Map', 'Sync Options', 'User Account', and 'Mail Enable Options'. The 'Mail Enable Options' tab is active. There are six dropdown menus arranged in two columns. The left column contains: 'Mail Enable on Create *' (Flow from Source), 'EAP Enable on Create *' (Always Disable), and 'Hide From GAL on Create *' (Flow from Source). The right column contains: 'Mail Enable on Update *' (Flow from Source), 'EAP Enable on Update *' (Always Disable), and 'Hide From GAL on Update *' (Flow from Source). The 'Hide From GAL on Create *' dropdown menu is open, showing three options: 'Always Enable' (highlighted), 'Always Disable', and 'Flow from Source'. There is a 'Cancel' button on the left and a 'Save' button on the right.

The screenshot shows the 'Mail Enable Options' configuration panel, similar to the one above. The 'Hide From GAL on Update *' dropdown menu is open, showing four options: 'Flow from Source' (highlighted), 'Always Enable', 'Always Disable', and 'Keep as is on Target'. There is a 'Cancel' button on the left and a 'Save' button on the right.

Options available for configuration are:

- Mail Enable



- EAP Enable- (Exchange Address Policy)
- Hide from GAL – (Global Address List)
- Keep as is on Target

These can be set for new Object creation and Update object.

Mail Enable

Flow from Source

This has the effect of replicating the source mail-enable status of a user account. i.e. the status quo. This should be used with a combination of attribute mappings with Always Enable.

Always Enable

If this option is set to Always Enable, or Flow from Source (where the source object is mail-enabled) then PSP will set the appropriate attributes on a target object so that it will appear to be a Mail-Enabled object in the target.

Always Disable

If the Mail Enable feature is set to Always Disable then Default processing does not occur for new objects and only attribute mappings are applied.

If Always Disable is selected on Update or a target is matched and updated, then the legacyExchangeDN and showInAddressBook will be cleared (but not for mailboxes)

Note: Always Disable will never be executed against a target Mailbox

This option cannot *Mailbox* enable users in on-premises, but the flow of attributes can be used to have an Entra Connect enabled environment in the target have Exchange Online trigger a mailbox creation. Useful for Shared Mailboxes, Rooms and Equipment.

Keep as is on Target

This ensures that if the account status has been edited / updated on the target, then PSP will leave it alone “as is” and do nothing.

Conclusion

If your objective is to have mail-enabled users in the target, then use a combination of attribute mappings with Always Enable

Enable EAP (Exchange Address Policy)

For EAP – Exchange Address Policy you may want this to always be disabled so that you can control the exact email address that is configured for objects. You do not need to map these attributes.

```
msExchPoliciesExcluded = {26491cfc-9e50-4857-861b-0cb8df22b5d7}  
msExchPoliciesIncluded = {26491cfc-9e50-4857-861b-0cb8df22b5d7}
```

The target may have a different policy, and it is likely that you will want the source object values to define the email address or set them explicitly with the use of a complex expression.

Enable Hide from GAL (Global Address List)

It may be that initially you want all objects hidden from the Global Address List while you are in pre-migration design phase and do not want target users to see them in the Global Address List just yet. At the cutover date you might switch this to Disabled or Flow from Source.

msExchHideFromAddressLists attribute is set as follows:
True/False/Not set

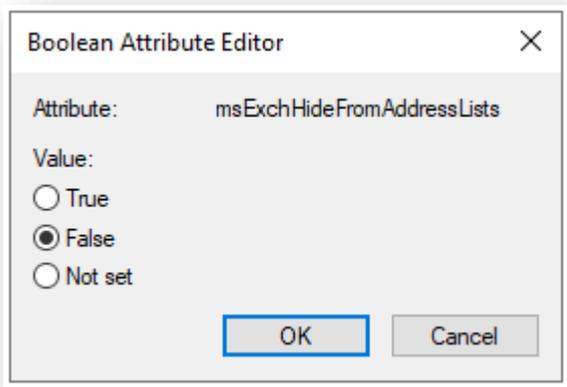


Figure 60 msExchHideFromAddressLists

Simple Expressions

A simple expression is a set of rules that are applied in sequence to manipulate each source attribute value until the end of the list of rules, or until Stop Processing = 1 on any of the rules. These perform faster than complex expressions but are limited in their scenarios.

NOTE: Simple (and Complex) Expressions need to be created in advance before they can be used on a Sync Profile.

Simple Expressions are primarily used for the more basic of use cases for attribute rewriting in your mapping table, such as: add/remove/replace strings, prefix/suffix and upper / lower case. Complex

Expressions are much more feature rich and flexible and more likely to be able to achieve your desired goal. There is a marginal performance difference using Simple Expressions versus Complex Expressions, but in our testing that has been barely noticeable even with hundreds of thousands of objects synchronising.

What If

After you have worked with your rewrite expressions be sure to check the What If or Single Object report before running an export to ensure you achieve your desired results.

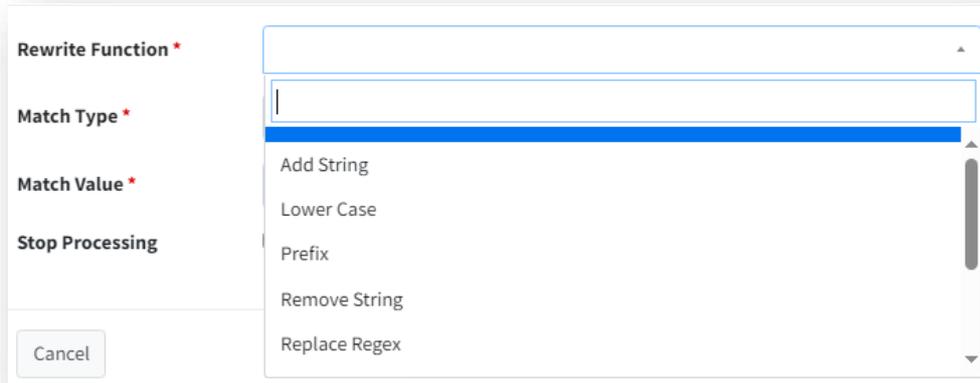


Figure 61 Simple Expressions

Options

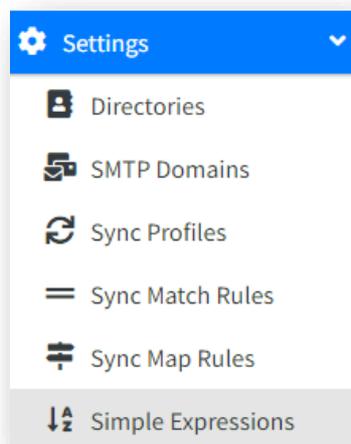
Depending on the rewrite function there may be additional fields

Function	Description
Add String	Adds New Value to the list of values for the target object
Lower Case	Forces the source value to be lower case
Prefix	Adds the specified Prefix to the start of the source value
Remove String	Removes the source value altogether
Replace RegEx	Replaces the Pattern in the source value with Replacement
Replace String	Replaces the Find Value in the source value with Replace value
Suffix	Adds the specified Suffix to the end of the source value
Truncate	Truncates the source value at the specified Length
Upper Case	Forces the source value to be upper case

Create Simple Expressions



Go to Settings and choose Simple Expressions



The following examples will show you how to create some simple expressions, in this case, lowercase and uppercase.

Click “Create”

- Name: Give your Simple Expression a meaningful name e.g. “**prefix lowercase and truncate**” in the “Name” field
- Comments: Add any comments that might help with further explanation of this expression

Add Only Matches

Enabling **Add Only Matches** will only add values that matched one or more of the simple expressions. Disabling **Add Only Matches** will always add the source values themselves PLUS values that matched one or more of the simple expressions

Add Only First Match

Enabling **Add Only First Match** will only add the value that first matched the simple expression and doesn't then process other source values. Disabling **Add Only First Match** will always process all source values. If you need to update all values for a multi-valued attribute, then you should not enable this.

Create New Simple Expression

Name * mailNickName Migrate to Fabrikam

Comments Prefixed with contoso_, Convert to Lowercase, Truncate to 64 characters

Add Only Matches

Add Only First Match

Figure 62 Create simple expression

Click “Create” to create new rule.

Rewrite Function

Choose your Rewrite Function

Match Type

This defines how you want to narrow down the source attribute value to apply the rewrite function to:

- Like: a simple wild card expression
- RegEx: a full regular expression

Choose Like or Match. Generally you would use “Like” here unless you are working with specific string values.

Match Value

The value to use for checking if the source attribute value should be rewritten. You can use asterisk * here, or a value if you are only wanting to work with specific string values.

Stop Processing

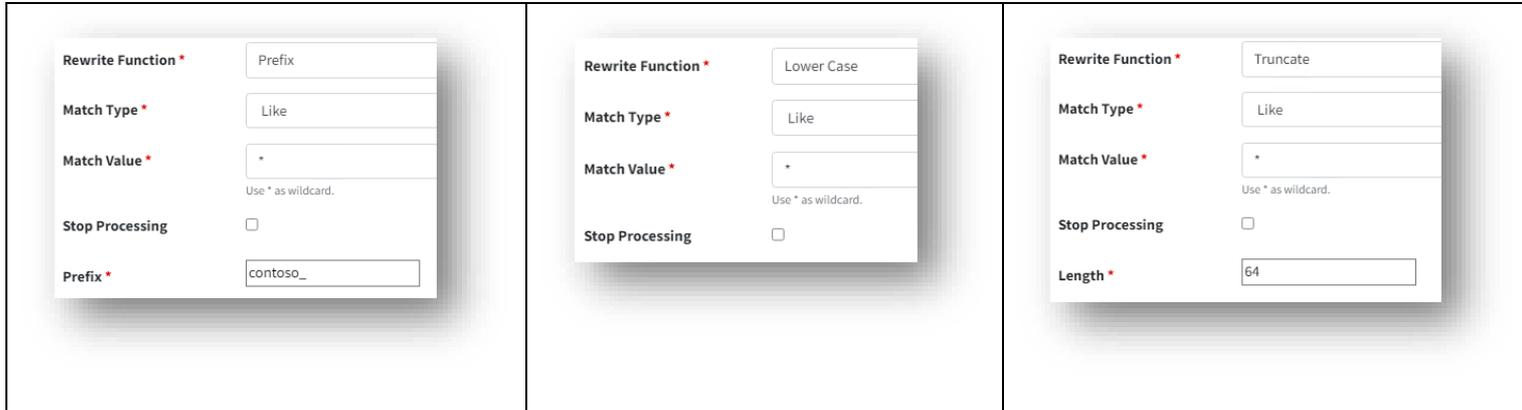
If this is unchecked then the expression will continue to any process other Rewrite functions you have in this expression. If you use **Stop Processing** then you may want to consider the ordering.

Click “Save”

EXAMPLE

- Prefix with contoso_

- Converted to Lowercase
- Truncated to 63 characters



Create New Simple Expression

Name * mailNickName Migrate to Fabrikam

Comments Prefixed with contoso_ Convert to Lowercase Truncate to 64 characters

Add Only Matches

Add Only First Match

Rules + Create

	Rewrite Function	Match Type	Match Value	Parameter1	Parameter2	Parameter3	Parameter4	Stop Processing	Actions	Order
+	Prefix	Like	*	contoso_				✖	Edit Delete	↑ ↓
+	Lower Case	Like	*					✖	Edit Delete	↑ ↓
+	Truncate	Like	*	64				✖	Edit Delete	↑ ↓

1-3 of 3 items Show 10 entries < 1 >

Figure 63 Configure simple expression

Working example
Source mailNickname



Widgets.Engineering.Operations.Weekend.Support.Notifications
(60 Characters)

Becomes:

contoso_widgets.engineering.operations.weekend.support.notifica
(prefixed and truncated to 63 Characters)

Suffix

In this example we can use a Simple Expression to add the migrating Source Company Name to Display Name or Department:

Rewrite Function *	Suffix
Match Type *	Like
Match Value *	*
	Use * as wildcard.
Stop Processing	<input type="checkbox"/>
Suffix *	(Contoso Ltd)

Figure 64 Simple Expression for Suffix

Upper Case

In this example we could use upper case to set all syncing objects SN / Last Name to upper case

Rewrite Function *	Upper Case
Match Type *	Like
Match Value *	*
	Use * as wildcard.
Stop Processing	<input type="checkbox"/>

Figure 65 Simple Expression for upper case

In this example we could use this to replace any attribute that sees a value that needs to be replaced everywhere: e.g. Company Name

Rewrite Function *	Replace String
Match Type *	Like
Match Value *	*
	Use * as wildcard.
Stop Processing	<input type="checkbox"/>
FindValue *	Contoso
ReplaceValue	Fabrikam

Figure 66 Simple Expression for Replace String

Regular Expressions

Regular expressions can be used both as the match type and as the find/replace.

So you can say match `^(\d{3})-Contoso$` to mean any 3 digits followed by -Contoso. For the Find and Replace you can use complex regular expressions to pick out parts of the source value, e.g.



Find `[a-zA-z0-9](.*)"(.*)@(.*)` Replace `$3$1@$4` to change [firstname.lastname@domain.com](#) to [firstinitiallastname@domain.com](#) or other weird and wonderful things you can do with regex replacements.

The screenshot shows a configuration window for a Rewrite Function. It contains the following fields and options:

- Rewrite Function ***: A dropdown menu with "Replace Regex" selected.
- Match Type ***: A dropdown menu with "Like" selected.
- Match Value ***: A text input field containing an asterisk (*). Below it is the text "Use * as wildcard."
- Stop Processing**: An unchecked checkbox.
- Pattern ***: An empty text input field.
- Replacement**: An empty text input field.

Complex Expressions

Complex Expressions are used for both scoping (to narrow down which objects are in scope for a sync profile) as well as mapping (to make decisions based on multiple source attributes, or to complete complicated transformations (rewrites) on the source attribute value.

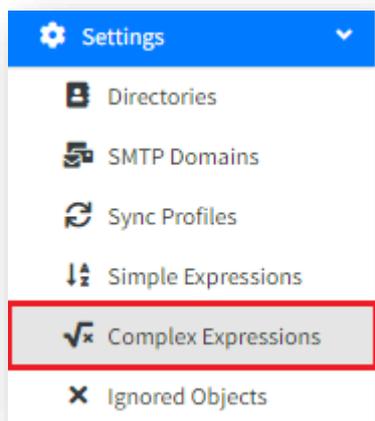


Figure 67 Complex Expressions

Complex Expressions are extremely flexible and powerful and allow you to get very specific and very granular in your syncing needs.

| Complex Expressions have largely superseded Simple Expressions.

A Complex Expression is a nested IF/Then/Else statement with each IF able to contain multiple rules combined with either an AND or an OR. Within each rule you can put attribute name, function and value.

Each Complex Expression you create is specifically tied to a directory pair and can therefore only be used on a sync profile that matches your directory pairing.

Complex Expressions can be used on:

- Scoping
- Matching
- Mapping

Unless otherwise stipulated, you should assume that everywhere in Complex Expressions you should be working with case sensitive syntax except for the attribute values themselves. When using attributes here, you must use the LDAP case of attributes, hyphens need to be removed. For Active Directory these can be found at: <https://learn.microsoft.com/en-us/windows/win32/adschema/attributes-all>

All attributes can be referenced by name, for attributes with hyphens you must remove the hyphens to refer to that attribute, or you can use the GetValue helper function

e.g. SAM-Account-Name should be reference as sAMAccountName (the Ldap-Display-Name)

Source Value

This is always in the IF section. You can use AND/OR and conditions. You can use C# methods (with some exceptions) as needed.

You can also just use “**Mapping Source Attribute Value**” if you intend to use the same complex expression on multiple attributes. E.g. mail and UPN

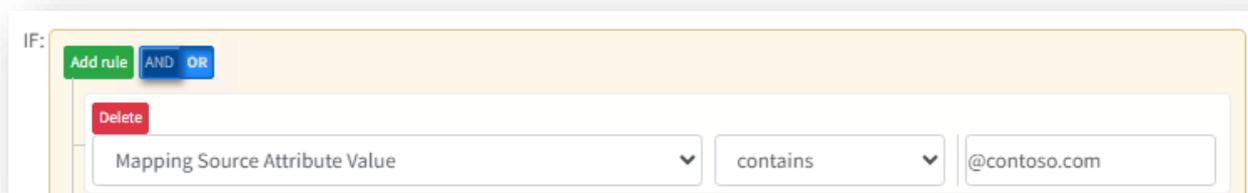
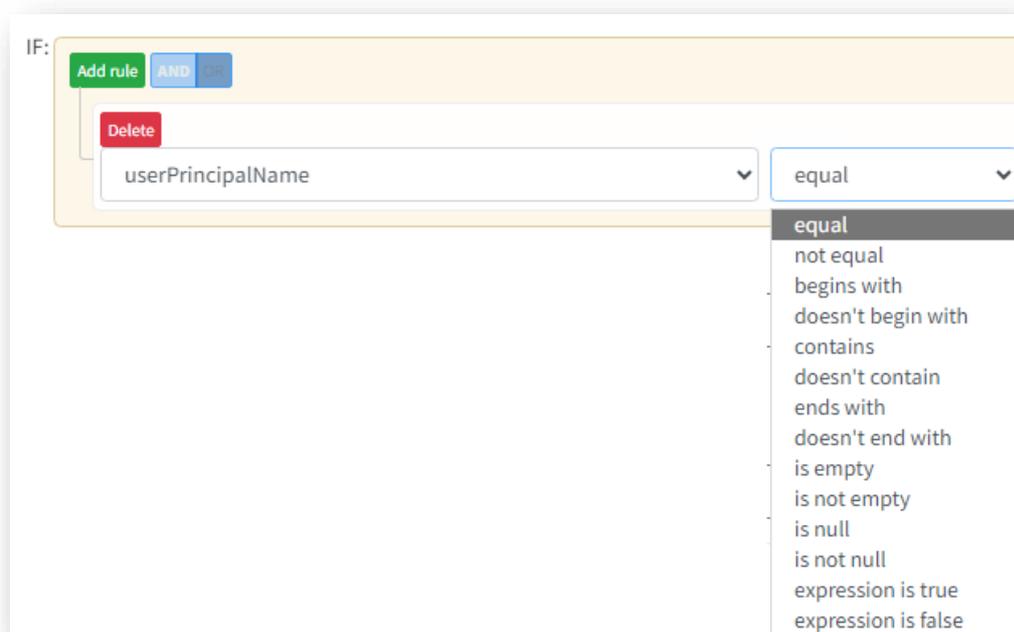


Figure 68 Mapping Source Attribute Value



IF attribute:

The list of functions are as follows

Function	Comment
Equal	Attribute value equals a specific value
Not equal	Attribute value not equal to a specific value
Begins with	Attribute value begins with the specified string
Doesn't begin with	Attribute value doesn't begin with the specified string
Contains	Attribute value contains the specified string
Doesn't contain	Attribute value doesn't contain the specified string
Ends with	Attribute value ends with the specified string
Doesn't end with	Attribute value doesn't end with the specified string



Is Empty	Attribute value is empty (note that NULL <> empty)
Is not empty	Attribute value is not empty
Is null	Attribute value is null
Is not null	Attribute value is not null
Expression is true	
Expression is false	
Any	Multi value attribute has at least value
Any_Containing	Multi value attribute has at least value containing the specified string
Any_not_Containing	Multi value attribute has at least value not containing the specified string
Any_Equal	Multi value attribute has at least one value equal to the specified string
Any_not_Equal	Multi value attribute has at least value not equal to the specified string

You should note that empty (not empty) and null (not null) can be different. A good understanding of attributes is required here.

Target Value

This is used in the THEN/ELSE. You can use C# methods (with some exceptions) as needed.

C# objects and methods

You can use C# like code to set an attribute value.

Note that the code syntax is case sensitive. i.e.

- `sourcevalue.replace` is not the same as `sourceValue.Replace`
- `.split` is not the same as `.Split`

Example Code Snippets

Purpose	Snippet
Convert to ImmutableId	<code>Convert.ToBase64String(ObjectGUID.ToByteArray())</code>
Concatenation	<code>sAMAccountName + "@contoso.com"</code>
Left part plus domain	<code>userPrincipalName.Split('@')[0] + "@contoso.com"</code>
Replacement	<code>sourceValue.Replace("@", "__at__") + "@contoso.com"</code>

Validation

When creating Complex Expressions the wizard will validate your Syntax:

Success:





Fail:



Examples

MAPPING

UPN and Mail

Here, I want to set the migrating users UPN to `fabrikam.com` unless they are in the engineering department in which case then I want to set the UPN to `engineering.fabrikam.com` otherwise write the source UPN.

If UPN contains *contoso* or *widgets*, then set UPN as **leftpart of source + @fabrikam.com**

If UPN contains *contoso* or *widgets* AND IF department begins with *engineering*, then set UPN as **leftpart of source + @engineering.fabrikam.com**

As stated earlier, Complex Expressions for mapping and matching are tied to directory pairings. For Scoping only one Directory is required.

CREATE



Create Complex Expression

Name *

Type *

Source Directory *

Target Directory *

After creating the complex expression, you'll be able to go to edit it to set the logic. The type and directories cannot be changed.

Edit Complex Expression

NOTE: be careful with the **AND/OR** as they are both blue and it is easily forgotten to toggle and not always obvious when the **AND/OR** is depressed.

- Light blue and focused is selected
- Dark blue and shadow is **NOT** selected

OR state

IF:

Figure 69 OR state enabled

AND state

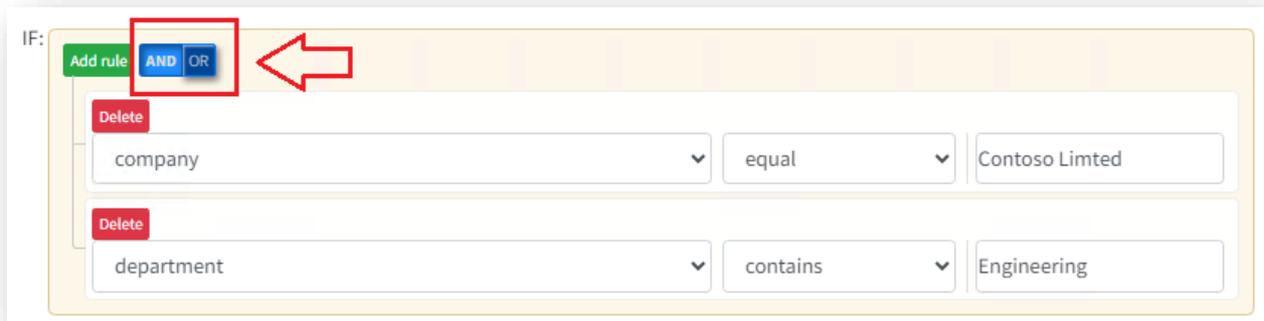


Figure 70 **AND** state enabled

Edit Complex Expression
✕

Name *

Comments

IF: Add rule AND OR

Delete

▼

▼

Delete

▼

▼

IF: Remove Condition

Add rule AND OR

Delete

▼

▼

+ Add Condition

Target Value ✔

ELSE

+ Add Condition

Target Value ✔

ELSE

+ Add Condition

Target Value ✔

Cancel
Save

Figure 71 Set target UPN

Target Value examples

userPrincipalName.Split('@')[0] + "@engineering.fabrikam.com"
 userPrincipalName.Split('@')[0] + "@fabrikam.com"

And for mail I would have:



Name * Set Mail to fabrikam.com

Comments set the migrating users mail to fabrikam.com

IF:

- Add rule** **AND** **OR**
- Delete** mail contains contoso
- Delete** mail contains widget
- + Add Condition**
- Target Value mail.Split('@')[0] + "@fabrikam.com" ✓

ELSE

- + Add Condition**
- Target Value mail ✓

Figure 72 Set target mail attribute

Here I am not treating engineering users differently for mail.

proxyAddresses

If you are migrating domains as part of your project, then most likely you will simply want to flow proxy addresses “as is”. However, if you are *not flowing domains* because this is a divestiture and the domains need to remain in the source then you would most likely need to rewrite the proxy address entries to maintain a degree of replyability, especially if you are rewriting the From, To, Cc and Bcc in your migration tools.

The Complex Expression for proxyAddresses uses a different pattern because it is a multi-valued attribute and you need to process all entries on that attribute. Here we can use: “Mapping Source Attribute Value”

So in this example I am writing:

IF

any entry in the proxyAddresses attribute contains @contoso.com or @widgets.com then re-write that entry as fabrikam.com

AND IF

Any entry in the proxyAddresses attribute contains @contoso.local then re-write that entry as fabrikam.local

AND IF

Any entry in the proxyAddresses attribute contains @contoso.mail.onmicrosoft.com then re-write that entry as @fabrikam.mail.onmicrosoft.com



Name *

Comments

IF:

Add rule **AND** **OR**

Delete Mapping Source Attribute Value contains @contoso.com

Delete Mapping Source Attribute Value contains @widgets.com

+ Add Condition

Target Value: ✓

ELSE

IF: **Remove Condition**

Add rule **AND** **OR**

Delete Mapping Source Attribute Value contains @contoso.local

+ Add Condition

Target Value: ✓

ELSE

IF: **Remove Condition**

Add rule **AND** **OR**

Delete Mapping Source Attribute Value contains @contoso.mail.onmicrosoft

+ Add Condition

Target Value: ✓

ELSE

+ Add Condition

Target Value: ✓

In my Mappings on my Sync Profile I would now have:



Source Attribute	Target Attribute	Simple Expression Name	Complex Expression Name
userPrincipalName	userPrincipalName		Set UPN to fabrikam.com
mail	mail		Set Mail to fabrikam.com
proxyAddresses	proxyAddresses		rewrite proxyAddress entries
displayName	displayName	Suffix Company to DisplayName	
givenName	givenName		
initials	initials		
sn	sn	uppercase	
company	company	Rewrite Company Name	

Figure 73 Mappings with Complex Expressions

If we look in the Single Object Report for one of my users Report, this is what we see:

Attribute	Source Value	Future Target Value
company	Contoso	Fabrikam
displayName	Chris Carter	Chris Carter (Contoso Ltd)
mail	chris.carter@contosos.com	chris.carter@fabrikam.com
proxyAddresses	SMTP:chris.carter@contoso.com smtp:chris.c.carter@widgets.com smtp:chris.carter@contoso.mail.onmicrosoft.com smtp:chris.carter@contoso.local smtp:CCarter@widgets.com	SMTP:chris.carter@fabrikam.com smtp:chris.c.carter@fabrikam.com smtp:chris.carter@fabrikam.mail.onmicrosoft.com smtp:chris.carter@fabrikam.local smtp:CCarter@fabrikam.com
sn	Carter	CARTER
userPrincipalName	chris.carter@contosos.com	chris.carter@engineering.fabrikam.com



ConsistencyGuid

There may be an occasion where you need to capture the existing mS-DS-ConsistencyGuid in its ImmutableId format for later use. The ImmutableId is used by Entra ID to link on-premises and Cloud objects.

Here we can say that if the mS-DS-ConsistencyGuid is NULL then convert the ObjectGuid to the ImmutableId format

We can use:

```
Convert.ToBase64String(ObjectGuid.ToByteArray())
```

```
Convert.ToBase64String(msdsConsistencyGuid.ToByteArray())”
```

e.g.

Name * ConsistencyGuid

Comments Convert ConsistencyGuid to ImmutableId for later use.

IF:

- Add rule** **AND** **OR**
- Delete**
- mS-DS-ConsistencyGuid is null
- + Add Condition**

ELSE

- + Add Condition**
- Target Value** Convert.ToBase64String(ObjectGuid.ToByteArray()) ✓
- Target Value** Convert.ToBase64String(msdsConsistencyGuid.ToByteArray()) ✓

From my What If report



Attribute	Source Value	Future Target Value
extensionAttribute7		01AxjNcb5k6ij/L/AqORig==

SCOPING

An example of Scoping for Entra ID where you need Sync profiles to work with Guests, Members and Groups

With Entra ID there are no Containers to work, so we need to work with attribute if you only want a subset.

Here is an example for Entra ID Security Groups.

I do not want to synchronise Groups that are Dynamic or Unified or on-premises synchronised or Mail Enabled – therefore leaving me only Entra ID Cloud native Security Groups.

Name * Entra ID Groups Eligible

Comments

IF:

Add rule **AND** **OR**

Delete GroupTypes any equal Unified

Delete GroupTypes any equal DynamicMembership

Delete OnPremisesSyncEnabled equal false true

Delete MailEnabled equal false true

+ Add Condition

In Scope:

ELSE

+ Add Condition

In Scope:

Figure 74 Scope for Entra ID Security Groups

Here I am scoping only for Entra ID Guest Accounts



Name *

Comments

IF:

Add rule AND OR

Delete

+ Add Condition

In Scope:

ELSE

+ Add Condition

In Scope:

Figure 75 Scope for Entra ID Guests

Here I am scoping only for Entra ID Members



Name *

Comments

IF:

Add rule AND OR

Delete

+ Add Condition

In Scope:

ELSE

+ Add Condition

In Scope:

Figure 76 Scope for Entra ID Members

Here I want to scope for a subset of divesting users in Active Directory. I only want users from the Engineering Department AND where the account is enabled AND they are based in the United Kingdom AND have an email address with widgets.



Name *

Comments

IF:

IF:

IF:

IF:

In
Scope:

ELSE

In
Scope:

ELSE

In
Scope:

ELSE

In
Scope:

ELSE

In
Scope:



Figure 77 Scope by multiple attributes

MATCHING

Complex Expressions for matching allow you to build an attribute from the source, that would match at object in the target.

e.g. If the source userPrincipalName and mail are first letter of first name + surname @ domain name, but in the target, they are [firstname.lastname@domain.com](#)

e.g.

	Contoso	Fabrikam
givenName	Conrad	Conrad
SN	Murray	Murray
userPrincipalName	cmurray@contoso.com	conrad.murray@fabrikam.com

So, you could have a complex expression like:

givenName+"."+SN + "@fabrikam"

The screenshot shows the configuration interface for a matching rule. The rule is named "Match Contoso to Fabrikam". The comments section contains the text: "Convert source UPN values to firstname.lastname@fabrikam.com and check for a match." The rule is configured with an "IF" condition: "userPrincipalName is not null". Below the condition, there are two "Target Value" fields. The first field contains the expression "givenName+'.'+SN + '@fabrikam'" and has a green checkmark. The second field is empty and has a green checkmark, with a note below it stating "No value specified so the source value will be used".

So, [CMurray@contoso.com](#) matches [conrad.murray@fabrikam.com](#)

Or, if it was an exact a left part match but different right part in on-premises AD

The screenshot shows the configuration interface for a rule in PowerSyncPro. At the top, the 'Name' field is set to 'Match Contoso to Fabrikam'. Below it is a 'Comments' field. The main configuration area is divided into 'IF' and 'ELSE' sections. The 'IF' section contains a condition where 'userPrincipalName' is 'is not null'. Below this is a 'Target Value' field with the expression 'UserPrincipalName.Split('@')[0] + "@fabrikam.com" and a green checkmark. The 'ELSE' section has a 'Target Value' field that is empty, with a green checkmark and a note below it: 'No value specified so the source value will be used'. There are buttons for 'Add rule', 'AND', 'Delete', and '+ Add Condition' throughout the interface.

Or, if it was an exact a left part match in a pre-migration (domain not yet cutover) to Entra you might have something like:



Name * Match Contoso to Fabrikam

Comments

IF:

Add rule **AND** **OR**

Delete

userPrincipalName **▼** is not null **▼**

+ Add Condition

Target Value UserPrincipalName.Split('@')[0] + "@fabrikam.onmicrosoft.com" **✓**

ELSE

+ Add Condition

Target Value **✓**

i No value specified so the source value will be used

Ignored Objects

- Settings** **▼**
- Directories
- SMTP Domains
- Sync Profiles
- Sync Match Rules
- Sync Map Rules
- Simple Expressions
- Complex Expressions
- Ignored Objects**

Ignored Objects is used to remove the matched objects from import and from export, regardless of directory settings for system objects.



Entries in this list are ALWAYS explicitly excluded from sync - even if they are in scope and matched.

There is a baseline list of objects that is automatically pre-populated for each directory that is added.

Label	Description
Ignored Object Name	The pattern to match to the cn attribute value of the object
Directory	The directory that this Ignored Object should be checked for

This is the current list of 21 Active Directory ignored objects that are pre-populated.

Ignored Object Name Actions

- ADSyncAdmins
- ADSyncBrowse
- ADSyncOperators
- ADSyncPasswordSet
- DHCP Administrators
- DHCP Users
- DiscoverySearchMailbox {*-*-*-*-*}
- DnsAdmins
- DnsUpdateProxy
- Exchange Install Domain Servers

You can add more to match your environment. E.g. you may have some other “Super Admin” groups, or restricted groups for special projects or VIPs.

Jobs

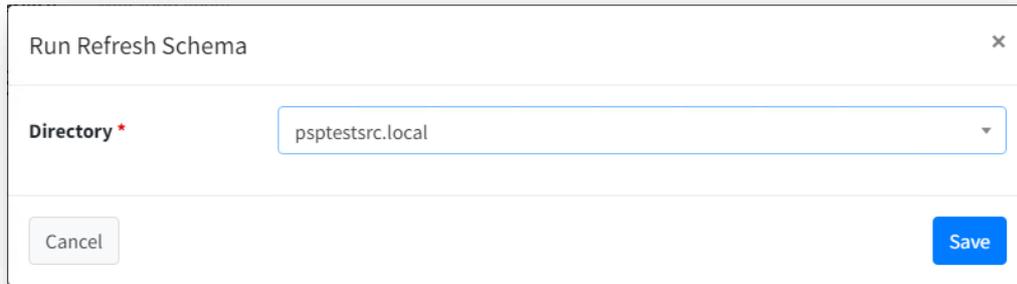
All jobs for Sync Profiles that are not excluded from schedule will run per the configured schedule.

If you need to run a specific job manually, you can right click from the schedule screen or come to the Jobs section and run a job manually. Previous run jobs are listed here with their Status, Start Time, Finish Time and statistics. Inserts, Updates, Deletes, No Changes, Errors and Warnings.

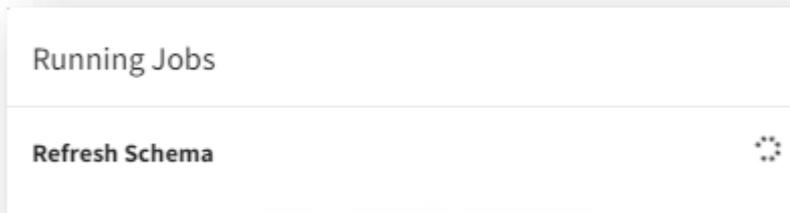
In normal operation you should not need to run these manually except for Refresh Schema that should be run if you know any updates have occurred to your directory schema. E.g. a Microsoft Exchange CU has been applied that made schema changes.

There is no issue to run jobs manually outside of the schedule.

Refresh Schema

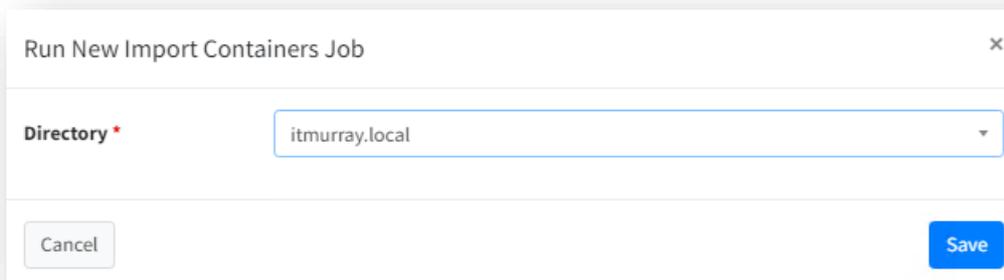


A dialog box titled "Run Refresh Schema" with a close button (X) in the top right corner. It features a "Directory *" dropdown menu with "psptestsrc.local" selected. At the bottom, there are "Cancel" and "Save" buttons.



A panel titled "Running Jobs" showing a single job entry: "Refresh Schema" with a circular refresh icon to its right.

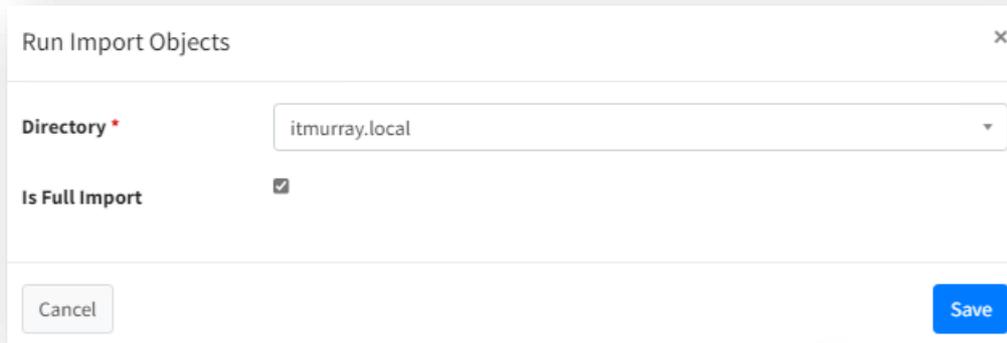
Import Containers



A dialog box titled "Run New Import Containers Job" with a close button (X) in the top right corner. It features a "Directory *" dropdown menu with "itmurray.local" selected. At the bottom, there are "Cancel" and "Save" buttons.



Import Objects



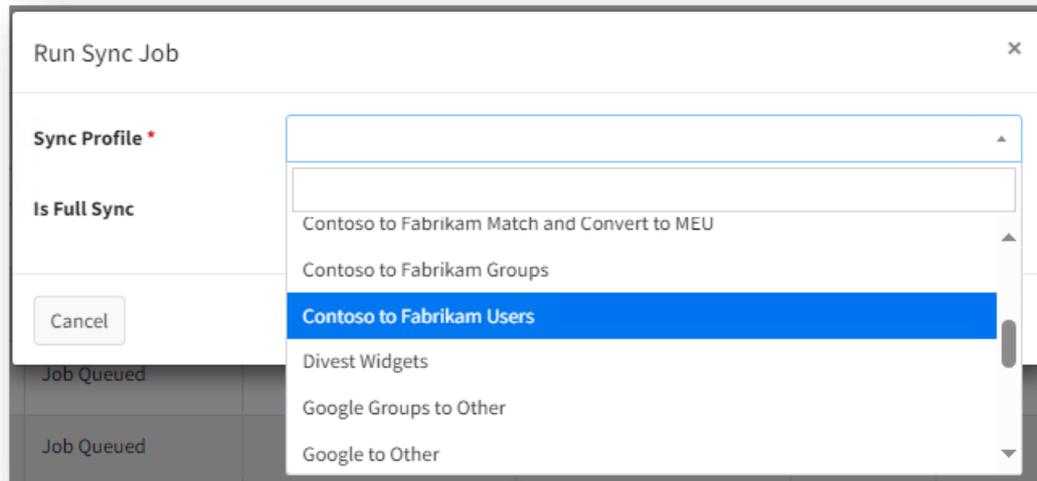
Is Full Import

You should not need to choose between full or delta import as the schedule will elevate to full import or full sync when it needs to.

A full import can take significantly more time to run than just scheduled delta imports and it may also overrun and then impact scheduled delta runs. You should only run this when needed. PowerSyncPro manages the *when and if* needs to run a Full Import.

- Full import will re-read all the objects from the directory and reconcile with what PowerSyncPro has stored
- Delta Import only imports the changes since the last import. For AD this is the USN, for Entra ID this is the graph delta query
- All scheduled runs are delta but will elevate to full import when it needs to
- A full sync will always follow after a full import.

Sync Objects



You should not need to choose between full or delta sync as the schedule will elevate to full sync when it needs to.

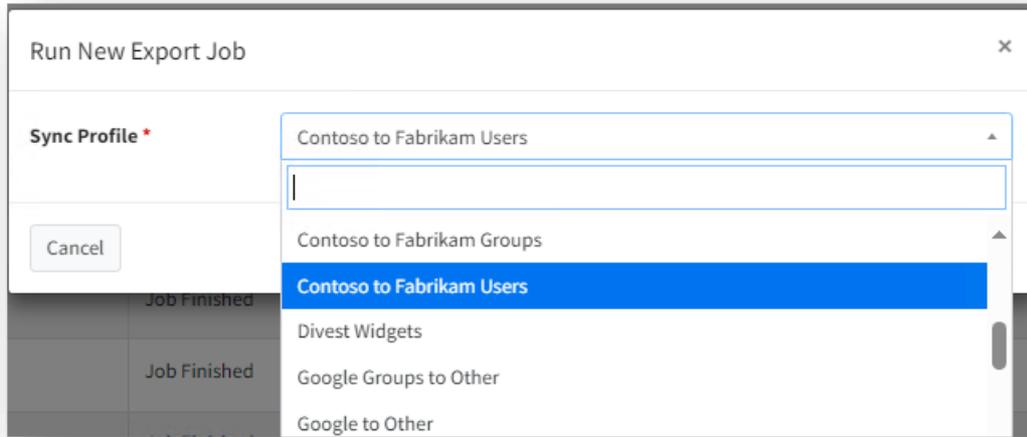
A full sync can take significantly more time to run than just scheduled delta syncs. You should only run this when needed. PowerSyncPro manages *when and if* it needs to run a Full Sync.

- Full Sync will re-sync all of the in scope objects
- Delta Sync will only synchronise those objects marked as having been updated/requiring a sync
- All scheduled runs are delta. The scheduled runs will elevate to full sync when it needs to
- A full sync will always follow after a full import.

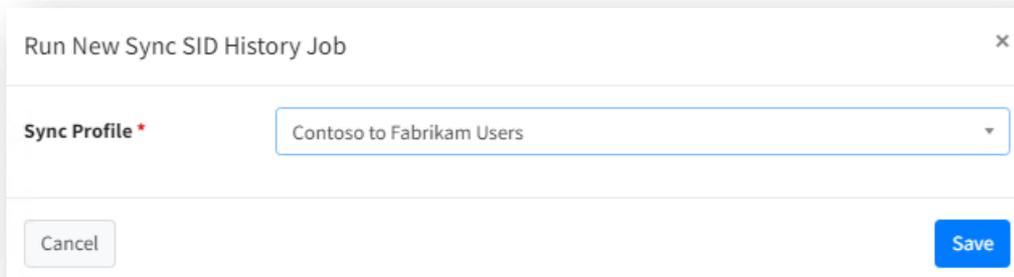
Export Objects

Here you can run an Export for one specific profile, rather than all profiles per the scheduler.

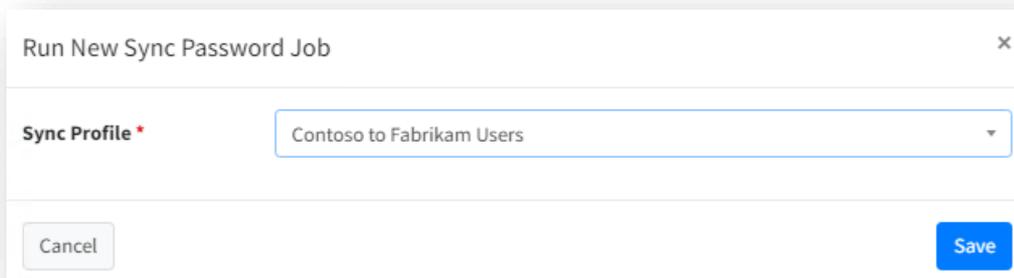




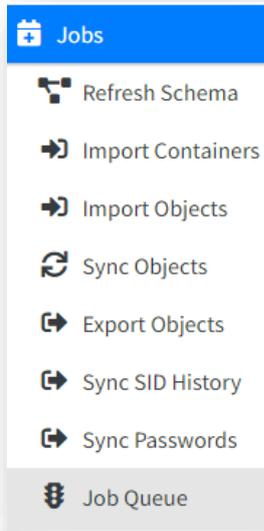
Sync SID History



Sync Passwords



Job Queue

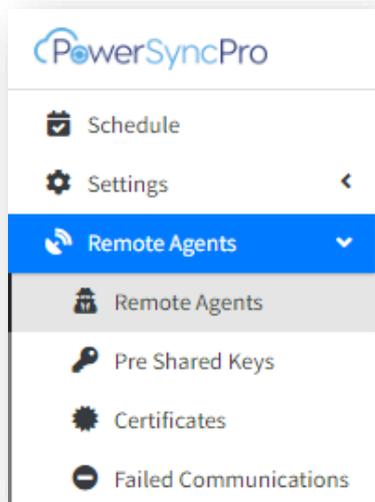


The Job Queue will show, as it says, any jobs waiting to run. In normal operation this view should be mainly empty.

If you see an uncleared job here, this could indicate a problem. You may be advised by support to delete a stuck job, restart the service and see if normal operations resume.

If you still have stuck jobs here, this indicates a wider problem that needs further investigation.

Remote Agents



If you chose Remote Agents as part of your installation, then an additional set of configurations will appear on the navigator that require additional configuration.

Remote Agents allow you to have a lightweight agent installed in your environment but have the PowerSyncPro server hosted in a different network. This is especially useful where you have disconnected networks that cannot easily be connected. The Remote Agents allow you to host the PowerSyncPro server in a DMZ or Azure without the need to open all required ports for Active Directory.

You must configure the Pre Shared Key and Certificate before moving to an Agent installation.

Installation

The Remote Sync Agent can be installed on any Active Directory Member Server, whereas the Remote Password Agent **must** be installed on each Domain Controller.

SSL and Ports

The Remote Agents communicate over SSL (HTTP/2) and only requires a single TCP port to be opened. The PowerSyncPro server must have a valid certificate available to and trusted by the Remote Sync Server. This can be a self-signed certificate although a 3rd party certificate is recommended.

The TCP Port can be defined per your own environment. TCP Port 5001 is the default Remote Agents port chosen by the PowerSyncPro Server.

NOTE: The Subject or Subject Alternate Name must be an exact match of your SSL Certificate Subject. Your endpoint, however, can be any of the other Subject Alternative Names on your certificate including wildcards. e.g. <https://psp.contoso.com:5001/Agent>. If you browse to that URL using a Web Browser then there should be no security warnings

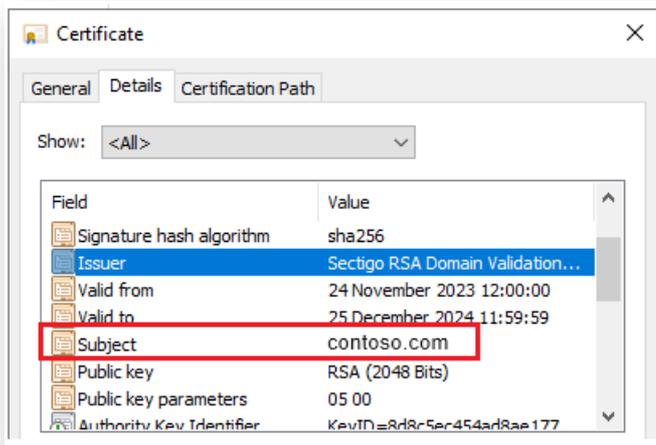


Figure 78 Certificate Subject Name

Pre Shared Keys “PSK”

During the installation of the Remote Agent you will be required to provide a pre shared key 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. (See certificates later)

Create

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

- **Agent Type:** This is Password Agent or Sync Agent depending on the type of Remote Agent you are installing.
- **Domain Name:** This is the FQDN of the domain the server hosting the sync agent is installed on.
- **Machine Name:** This is the NetBIOS *hostname only* of the server hosting your Remote Sync Agent. Do not use the host FQDN here.

Add New PSK ✕

Agent Type * Sync Agent ▼

PSK * 8GwOFStWoAzc5qUjYaUY+RgbT5Ia14s9hDszBvKBP7wng+CczJxpD9Tks+REWTO1

⚙️ Generate Key

Domain Name * contoso.t2t.local

Machine Name * PSPRemoteAgent

Cancel Save

Figure 79 Pre Shared Key configuration for Remote Sync Agent

Pre Shared Keys

1-1 of 1 items Show 10 entries

PSK	Agent Type	Domain Name	Machine Name	Is Latest	Generated Time
8GwOFStWoAzc5qUjYaUY+RgbT5Ia14s9hDszBvKBP7wng+CczJxpD9Tks+REWTO1	Sync Agent	contoso.t2t.local	PSPRemoteAgent	✓	05/03/2025 12:07

You will use the Pre Shared Key during your installation of the Remote Agent.

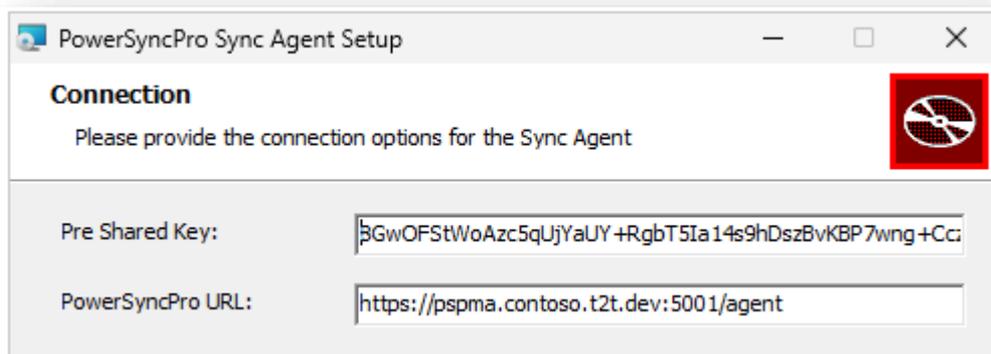


Figure 80 Pre Shared Key used during installation

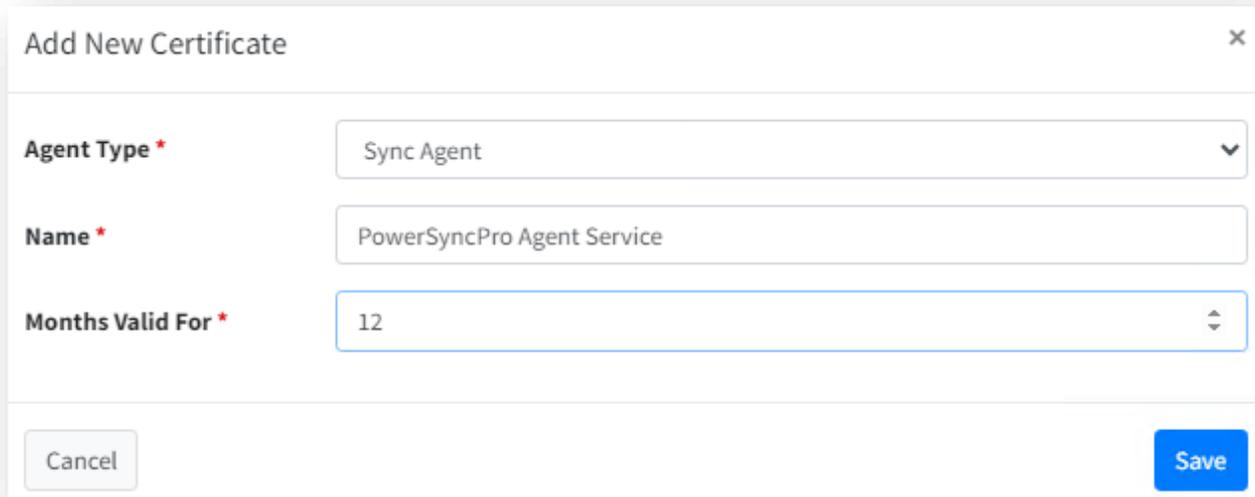
Note: The Pre Shared Key is used once per Remote Agent and will be removed once the Remote Agent is accepted into the console.

Certificates

This Certificate is different to your SSL Certificate and is used after registration to sign and encrypt communication between the PowerSyncPro Service and the Remote Agent.

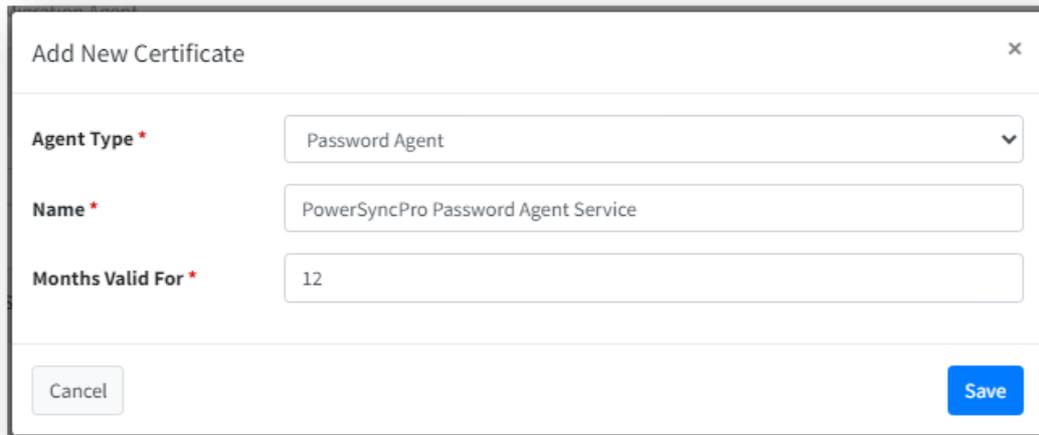
Click Create Certificate.

- **Agent type:** This is Password Agent or Sync Agent depending on the type of Remote Agent you are installing
- **Name:** Defaults to **PowerSyncPro Agent Service**. You can accept this or choose your own.
- **Months Valid for:** Defaults to 12. You can choose a value that meets your business needs.



The screenshot shows a dialog box titled "Add New Certificate" with a close button (X) in the top right corner. It contains three input fields: "Agent Type" with a dropdown menu set to "Sync Agent", "Name" with the text "PowerSyncPro Agent Service", and "Months Valid For" with the value "12". At the bottom, there are "Cancel" and "Save" buttons.

Figure 81 PSP Remote Sync Agent certificate creation



The screenshot shows a dialog box titled "Add New Certificate" with a close button (X) in the top right corner. It contains three input fields: "Agent Type" with a dropdown menu set to "Password Agent", "Name" with the text "PowerSyncPro Password Agent Service", and "Months Valid For" with the value "12". At the bottom, there are "Cancel" and "Save" buttons.

Figure 82 Add new certificate



Certificates

Name	Agent Type	Is Latest	Generated Time	Expires
PowerSyncPro Agent Service	Sync Agent	✓	30/05/2024 15:13	30/05/2026 15:13

Figure 83 Certificate created

After installing a Remote Agent two additional certificates will be present on your Member Server and/or Domain Controller in the Computer Personal Store.

Certificates on Remote Sync Agent Server

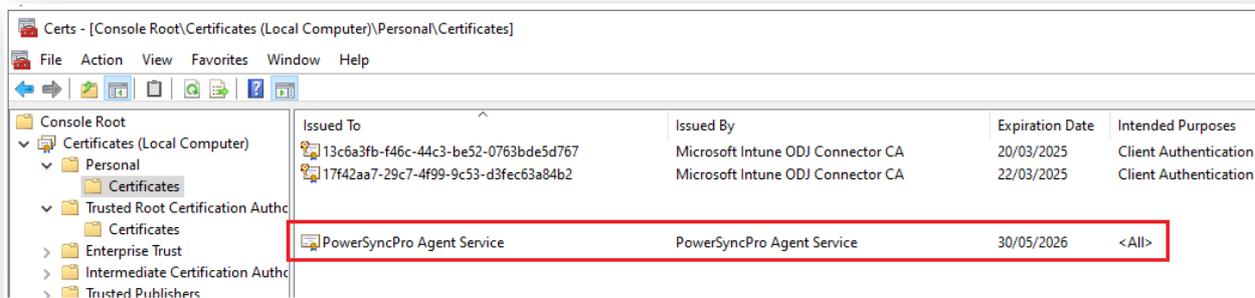


Figure 84 Local certificates on a Remote Sync Server

Certificates on a Password Sync server

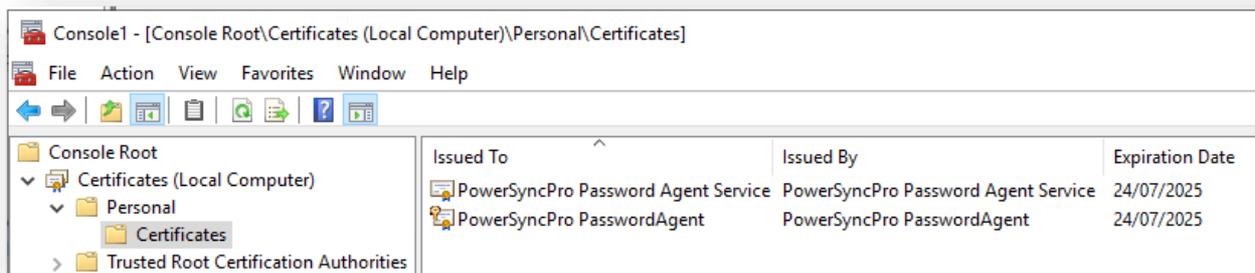


Figure 85 Local certificates on a Password Sync Server

Approve Remote Agent

After you have successfully run the installer on your Remote Agent server, you will need to return to the Remote Agents section in PowerSyncPro and approve the agent. The reason for this is that the Remote Agents have privileged capabilities and therefore a double opt in is deemed necessary.

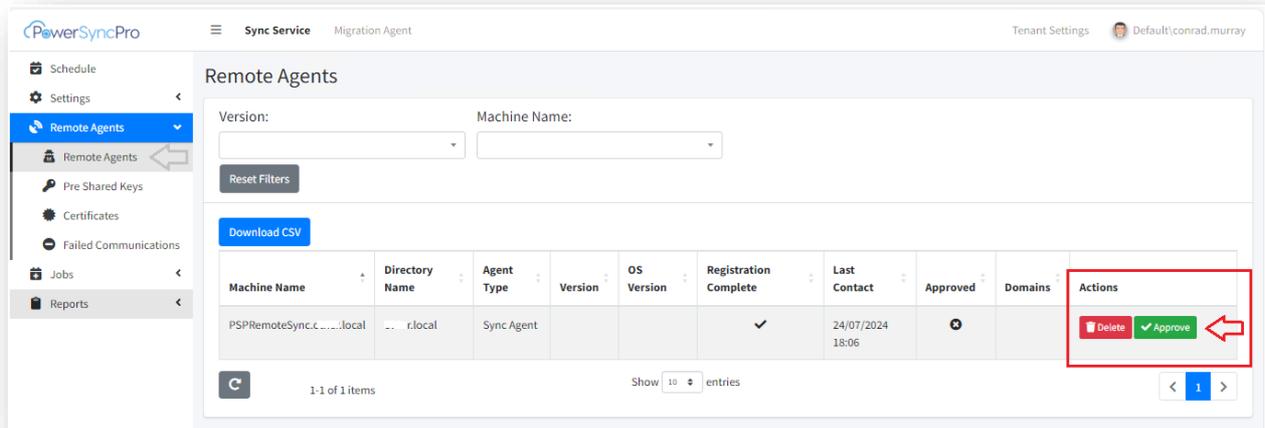
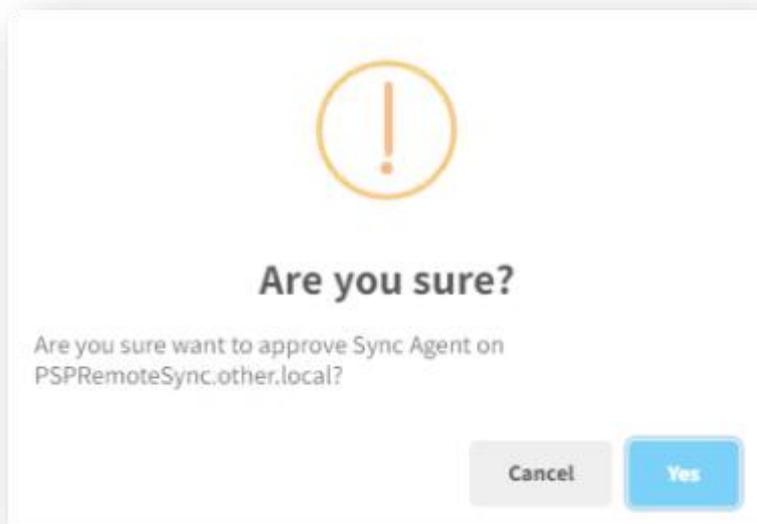


Figure 86 Approve Remote Agent



Service

After a successful installation and configuration you will see the PowerSyncPro Sync Agent or PowerSyncPro Password Agent service listed and running.

Power	Manages power policy and power policy ...	Running	Automatic
PowerSyncPro Sync Agent	PowerSyncPro Sync Agent Service	Running	Automatic (Delayed Start)
Print Spooler	This service spools print jobs and handles	Running	Automatic

Failed Communications

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

Remote Sync Agent

Aside from allowing sync across disconnected networks, another key benefit of the Remote Sync Agent is that the configuration and credentials to access the various domains lives purely on the Remote Sync Agent server. The PowerSyncPro Service has no knowledge other than which Remote Sync Agent services which Directory.

NOTE: At the moment it is important that if you have multiple Remote Sync Agents for the same Directory, then they should all use the same Domain Controller/Server. This is due to how PowerSyncPro checks for changes. In a later version we will resolve this by allowing a Domain Controller/Server to be switched by triggering a full import/sync

Sync Agent Configuration

After you have run the installer, you will need to run the configuration tool.

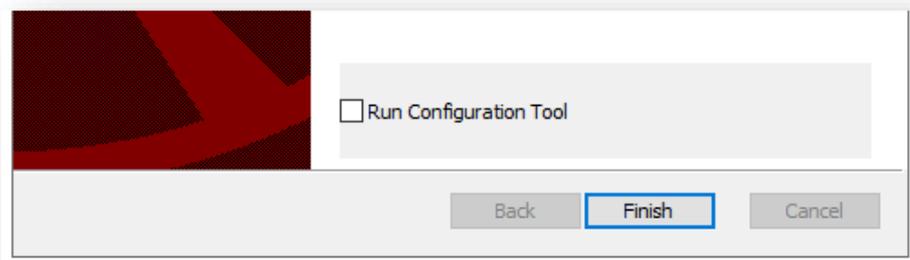


Figure 87 Run Configuration Tool - Remote Sync Agent

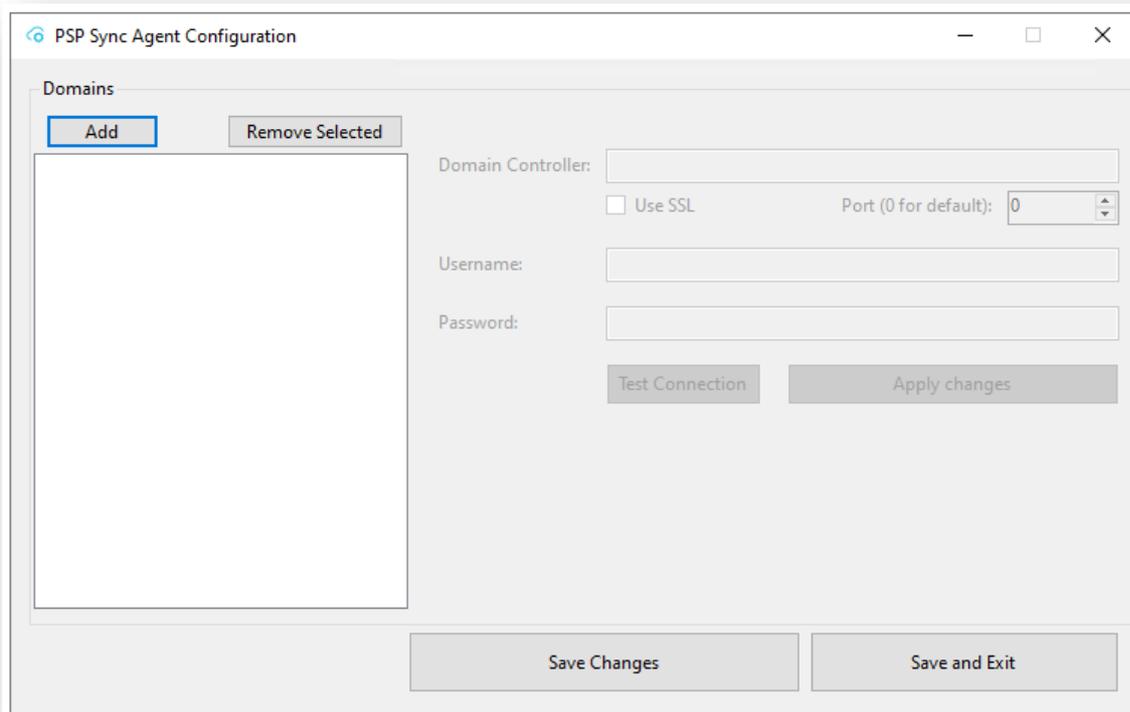


Figure 88 PSP Sync Agent Configuration

Click Add

This section is much like your Directories configuration in the PowerSyncPro Console.

Domain controller:	This is the Domain Controller that this Remote Sync Agent talks to.
Use SSL:	Tick this if your Domain Controllers are configured for secure LDAP
Port	There is no need to change this for SSL or non SSL unless you have configured custom ports to communicate with your Domain Controller
Username:	this is the Service Account with the privileges to read or write in your Active Directory
Password	Password of the Service Account



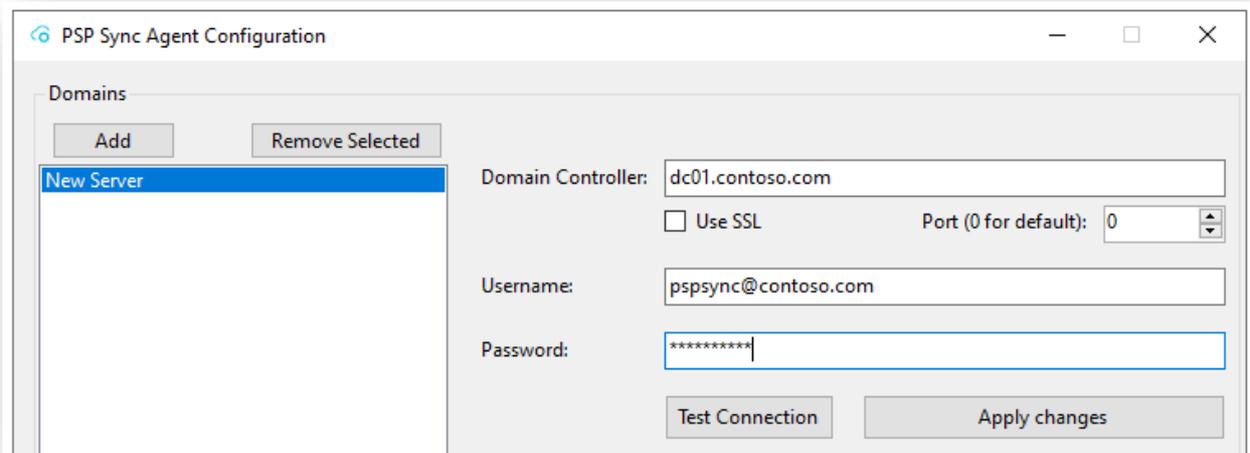
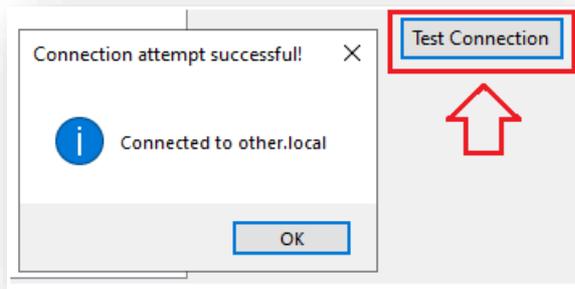
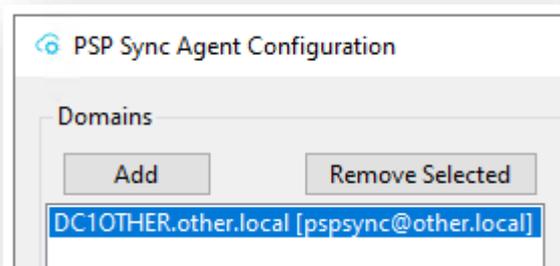


Figure 89 PSP Sync Agent Configuration new server

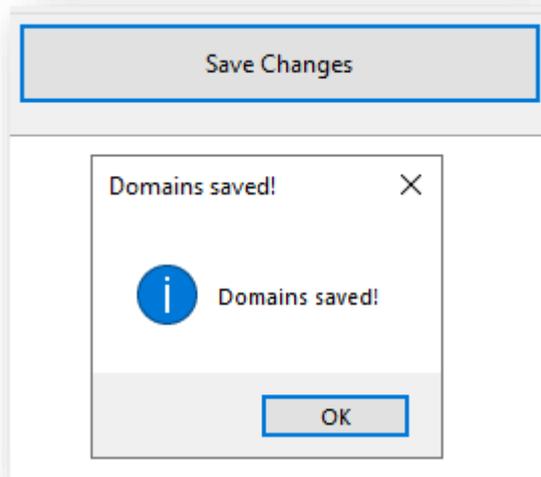
Test Connection



Apply Changes



Save Changes / Save and Exit



NOTE: If you are synchronising SIDHistory, the Remote Sync Agent configuration requires both Source and Target credentials listed on the configuration.

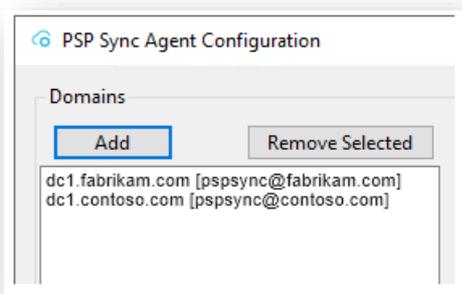


Figure 90 Successful Sync Agent Configuration

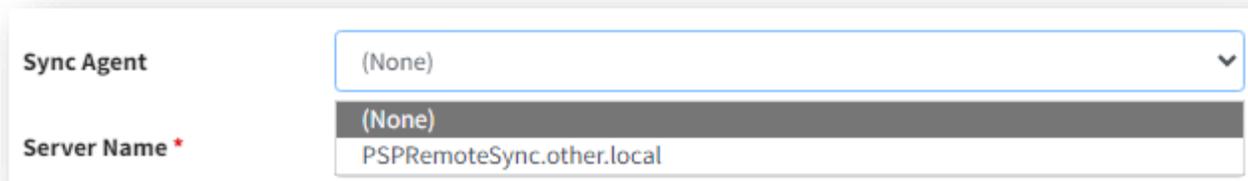
Directories Configuration

After you have completed your work for installation and configuration on the member server running the sync agent, you now need to return to the PSP console to complete the directories configuration.

Select your Directory and click Edit.

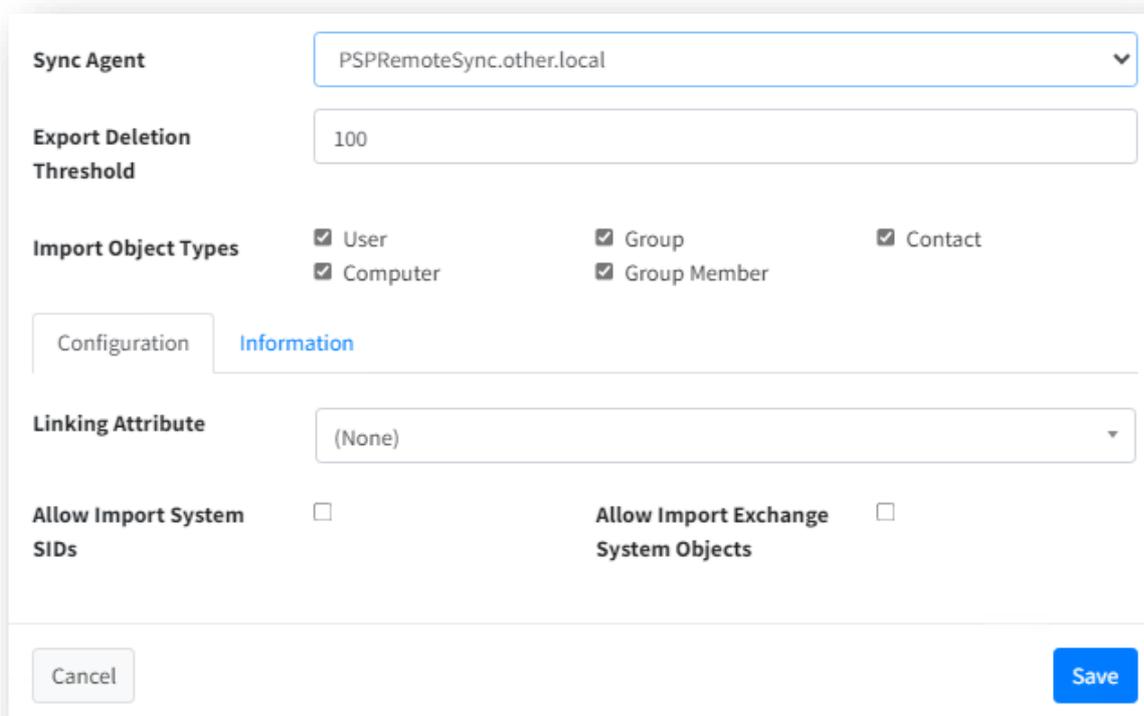
You should now see the Sync Agent drop down populated with your newly deployed Remote Sync Agent





A screenshot of a web interface showing a dropdown menu for 'Sync Agent'. The dropdown is open, displaying '(None)' as the selected option. Below it, another '(None)' option is visible, and at the bottom, 'PSPRemoteSync.other.local' is listed as an available option.

Choose your agent from the dropdown. You will see Server name, Credential Type, Username, Credential and Port disappear. This is by design.



A screenshot of the 'Remote Sync Agent' configuration dialog. The 'Sync Agent' dropdown is set to 'PSPRemoteSync.other.local'. The 'Export Deletion Threshold' is set to '100'. Under 'Import Object Types', the following options are checked: User, Computer, Group, Group Member, and Contact. There are two tabs: 'Configuration' and 'Information', with 'Information' being the active tab. The 'Linking Attribute' dropdown is set to '(None)'. There are two checkboxes: 'Allow Import System SIDs' and 'Allow Import Exchange System Objects', both of which are currently unchecked. At the bottom, there are 'Cancel' and 'Save' buttons.

Figure 91 Use remote agents in directory configuration

Click Save to complete the configuration of Remote Sync Agent. You may wish to run jobs: Refresh Schema, Import Containers and Import Objects once from the Jobs option to confirm successful operation of the sync agent.



Remote Password Agent

The primary purpose of the password agent is to support modern passwords where the environment has been configured to no longer use RC4 and only use AES/SHA for password hashes. It intercepts the password and uses that to set the password on the target directory in near real time. With this method it is important that the target's password complexity requirements are the same or less restrictive than the source.

NOTE: Due to the password filter being used, the Password Agent must be installed on all Domain Controllers in your environment, specifically any Domain Controller where a user is likely to change their password.

Sync Profile Configuration

To use Modern Password Sync you need to enable this on your Sync Profiles. This is configured on the Sync Options tab. The default is Legacy Password Sync. You cannot use both, so you need to deselect Legacy Password Sync and select Modern Password Sync.

Before

Scope	Match	Map	Sync Options	User Account	Mail Enable Options
Delete Target Objects			<input checked="" type="checkbox"/>		Sync SID History <input checked="" type="checkbox"/>
Legacy Password Sync			<input checked="" type="checkbox"/>		Modern Password Sync <input type="checkbox"/>
Sync Group Members			<input type="checkbox"/>		Retain Target Group Members <input type="checkbox"/>
Convert Contact			<input type="checkbox"/>		

After

Scope	Match	Map	Sync Options	User Account	Mail Enable Options
Delete Target Objects			<input checked="" type="checkbox"/>		Sync SID History <input checked="" type="checkbox"/>
Legacy Password Sync			<input type="checkbox"/>		Modern Password Sync <input checked="" type="checkbox"/>
Sync Group Members			<input type="checkbox"/>		Retain Target Group Members <input type="checkbox"/>
Convert Contact			<input type="checkbox"/>		

Schedule

Password Sync will no longer appear on the schedule as it is real time with Modern Password Sync and Password Sync Agent.

Before

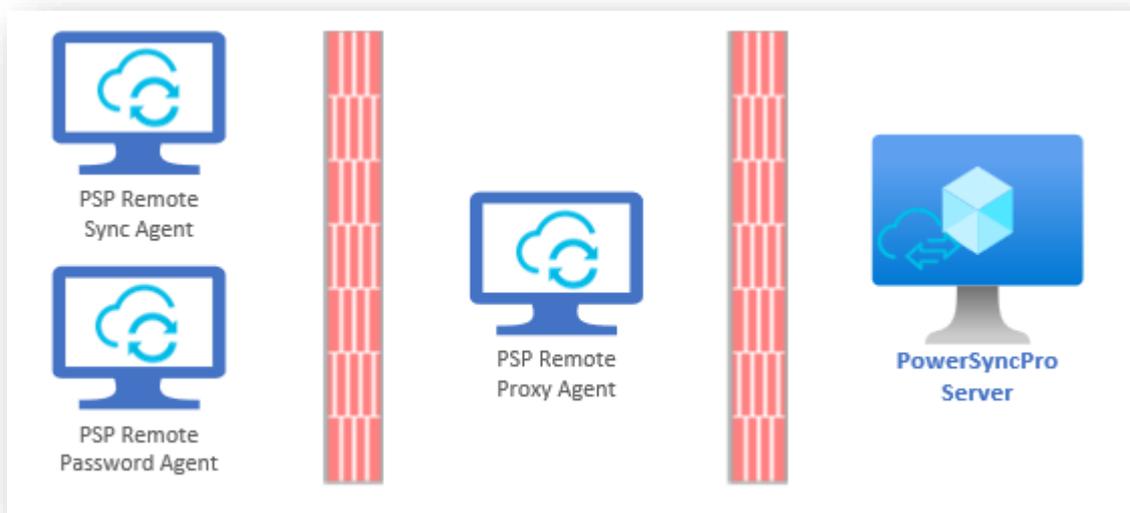
Export	Awaiting What If Acceptance	●	23 July 24 - 10:51 am	2	0	2	0
SID History Sync	Completed	● ▶	23 July 24 - 10:51 am	0	0	0	0
Password Sync	Completed	● ▶	23 July 24 - 10:51 am	0	0	0	0

After

Export	Awaiting What If Acceptance	●	25 July 24 - 12:53 am	0	0	0	0
SID History Sync	Completed	● ▶	24 July 24 - 06:12 pm	0	0	0	0

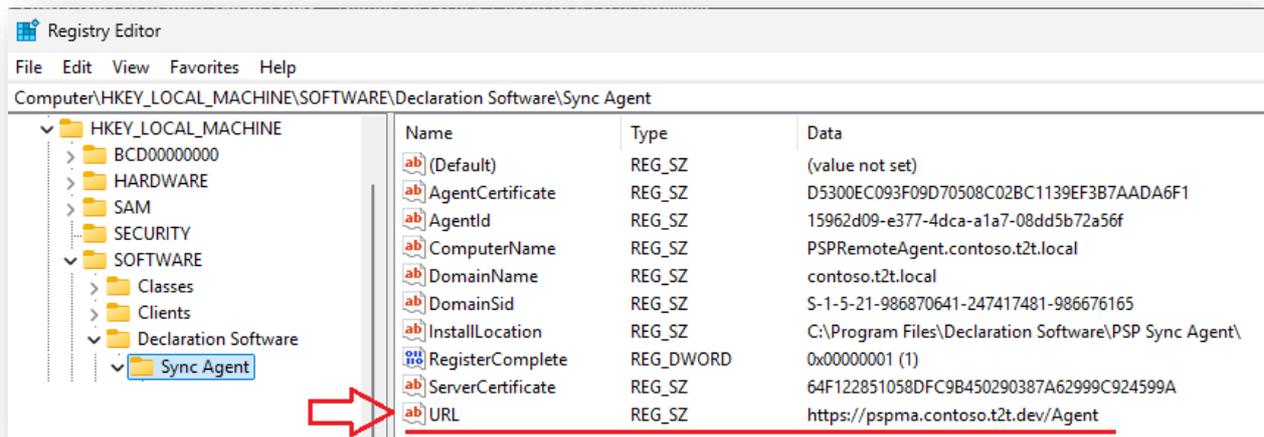
Remote Agent Proxy

The PowerSyncPro Remote Agent Proxy is a HTTP/2 REST and Streaming HTTPS Proxy that sits between the Remote Sync and Remote Password Agents and the PowerSyncPro Server.



If the agent finds one or more URLs in the SCP, it will try each one in turn until it finds one that is working.

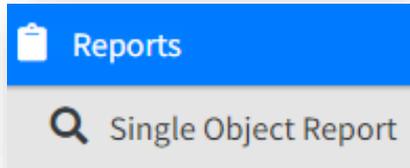
If no working SCP proxy URLs are found, then the Remote Agent's local registry configuration URL will be attempted as a fallback.



Periodically, a worker process in Sync and PW Agents looks for new SCPs and sets a flag. If the flag is set and the agent becomes idle, it reloads the SCP URLs so that the next request uses the next set of URLs.

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 for a granular check of “What If” changes to a Sync Profile and what will happen to your object if you approve the What If report.

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

Directory: Choose Directory for where your object is. This can be Source or Target, but the resulting output will show you values for both.

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 joh*

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.

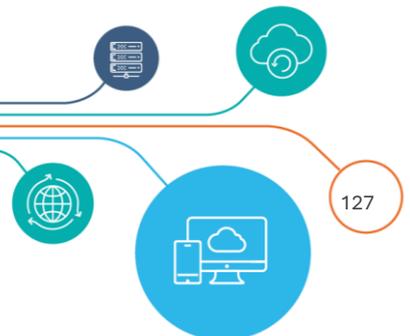
Object Name	Object Container
Johann Berg	psptestsrc.local/DSL PSP/Mike/Users
John Ruddy	psptestsrc.local/DSL PSP/Mike/Users
Johanna Rytting	psptestsrc.local/DSL PSP/Mike/Users
John Stones	psptestsrc.local/DSL PSP/Mike/Users

1-4 of 4 items

Show 10 entries

Figure 92 Single Object Report

You can use multiple "*" in your search to make your searches more granular, e.g. ***oh*ryt***



Single Object Report

Directory * psptestsrc.local

Search For *oh*ryt*

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
Johanna Rytting	psptestsrc.local/DSL PSP/Mike/Users

C 1-1 of 1 items Show 10 entries

Figure 93 Single Object Report search

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

Object Name	Object Container
Andy Murray	itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ

The resulting output provide a lot of detail. The top half is the Basics section and any awaiting Password or SIDHistory sync details.

Single Object Report

View Target Object From:

	Source Object	Target Object
Object Name	Andy Murray	Andy Murray
Object Container	itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ	charlie.local/From itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ
User Principal Name	andy.murray@t2t.dev	andy.murray@charlie.t2t.dev
Password Sync		Waiting
SID History Sync		Waiting

The bottom half gives you tabbed information about your object, and additional Basic information.

Overview

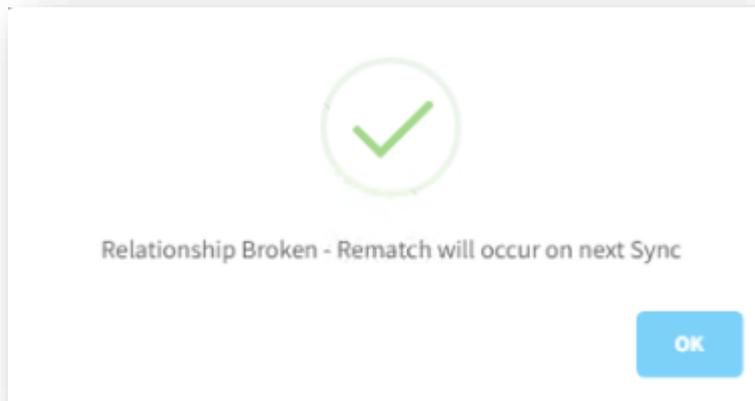
This includes the Match rule used for this object and if there are any pending actions. This report can show Active Directory and Entra ID deleted objects too, so that you can break the relationship to a deleted object if needed. When a deleted object is shown then the Object Name and the Object Container will both be in bold and have a prepended value to make it clear that this is a deleted object. Of course the attributes shown for a deleted object are limited.

Overview			
Attributes Migration Batches User Profiles Errors			
	Source Object	Target Object	Future Target Object
Name	Andy Murray	Andy Murray	Andy Murray
Directory	itmurray.local	charlie.local	charlie.local
Container	itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ	charlie.local/From itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ	charlie.local/From itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ
Type	User	User	User
Match Rule	(employeeID) andy.murray	(employeeID) andy.murray	
Pending Action			Update

Break Relationship

The Single Object report can be used to break the relationship between synced objects which will force a full rematch of that object. This can be useful if a mistake was made, e.g. a source object matched with a user's admin account instead of their regular account. You can fix the underlying issue in the directory to ensure a future match will link to the correct target user, then run the Single Object Report for that user, click Break Relationship and run the schedule as normal.

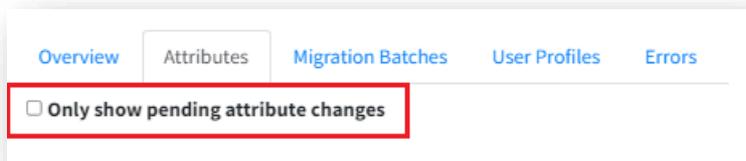




Attributes

Only attributes from your attribute mapping table are shown here. In this screen you can see side by side the current Source and Target attributes PLUS future target values that are awaiting export following an Import and Sync. Changes are shown in bold.

You can scope by Only attributes pending change



Attribute	Source Value	Existing Target Value	Future Target Value
description	Former Wimbledon Champion		Former Wimbledon Champion
homePhone	+1 555 TENIS		+1 555 TENIS
streetAddress	Wimbledon Tennis Centre		Wimbledon Tennis Centre

Migration Batches

This tab will show what PowerSyncPro Migration Agent batches an object is part of. This is especially useful for Devices.

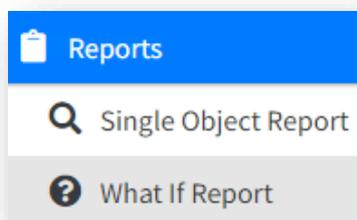
User Profiles

The User Profiles Report is populated with all the Windows Profiles on each machine that has successfully registered their agent. It is periodically updated so that changes in Windows Profiles are picked up. The idea here is to give insight into which users are logging on to which machines, in case you know who you want to migrate, but not which devices they are using.

Errors

Any errors will be seen here.

What If Report



The What If Report is a fail-safe mechanism to ensure that you are completely informed about the changes you might potentially be implementing, much like the well-known PowerShell switch. You will be able to view at an object level all proposed changes in a report like Single Object Report:

NOTE: You must accept the What If report before an Export will run.

The object will have

- Source Object
- Target Object – Current attributes
- Future Target Object – Changes that will be made on export

Whenever you create a brand new sync profile, it always goes to **What If** acceptance before exporting.

If you make an Edit to a Sync profile, or edit a Complex Expression or Simple Expression or SMTP Domain that is configured on a directory they are used on in a Sync Profile – then you will be required to accept the **What If** Report

What If from the Schedule Screen

You can see when a What If report acceptance is required by looking at the schedule. Each Sync Profile awaiting What If acceptance will have an asterisk next to it, and the Export will be suspended

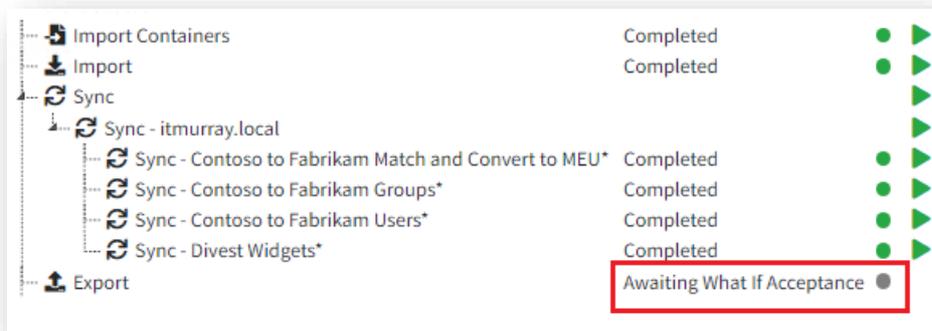


Figure 94 Awaiting What If Acceptance

You can right click any Sync Profile and go directly to that What If report.

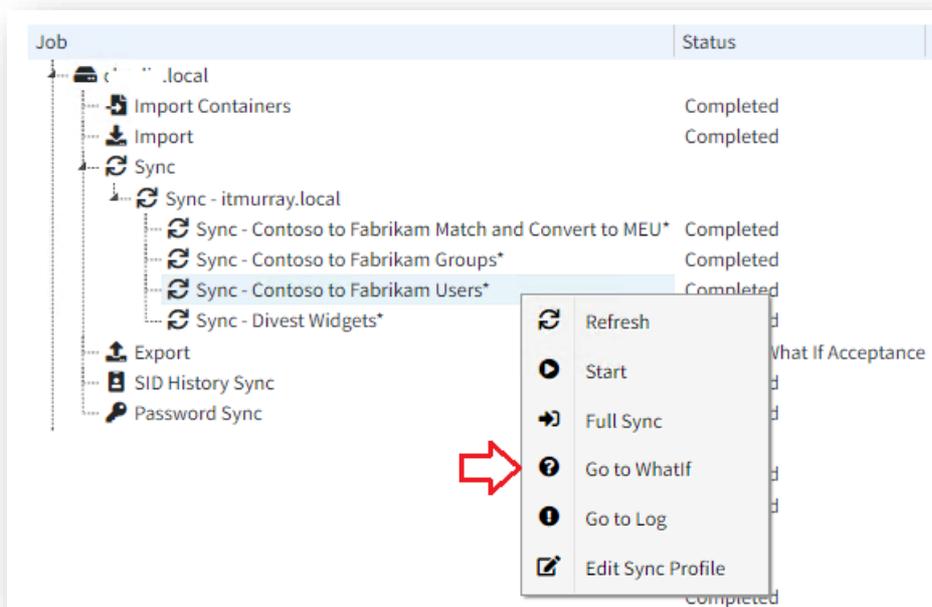


Figure 95 Go to What If

Running a What If from Reports

From the What If Reports, you can run a What If report for all sync profiles attached to a directory, or just one sync profile

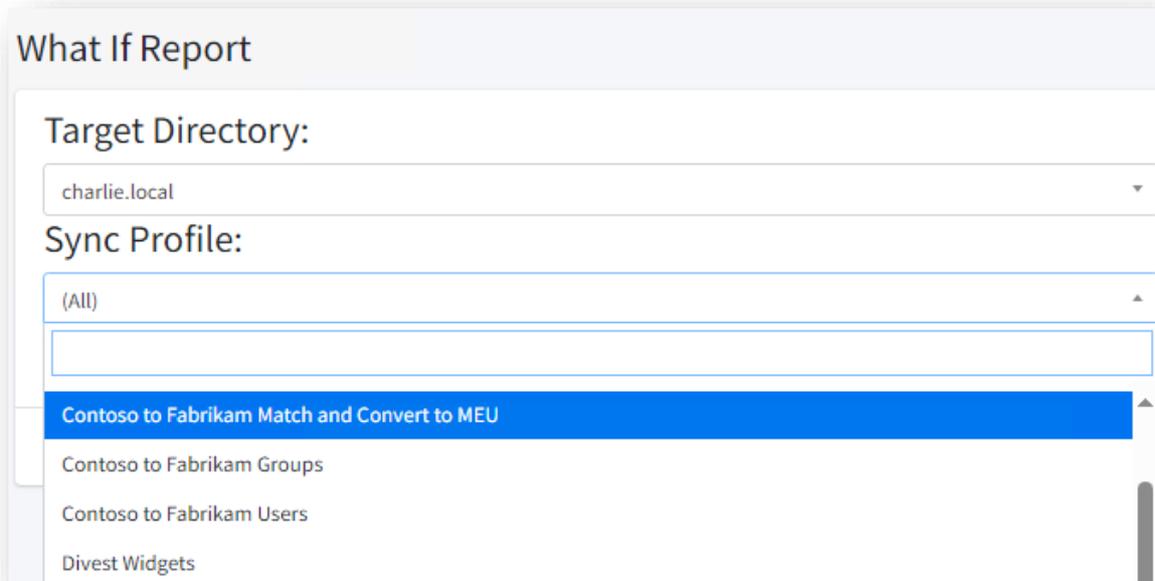


Figure 96 Run a What If

When you click search, if an up to date Sync is required, it will automatically be run. This will happen if you have made changes to your Sync Profile, but not yet executed Import/ & Sync

Results

You can export to CSV if preferred, or view directly in the UI, you can also search the UI if there is a specific reference object you want to check.



What If Report

Target Directory:

Sync Profile:

Action	Object Name	Object Container	Source Object Name	Source Object Container	Sync Profile
Create	Chris French	charlie.local/Aquisitions/Contoso/EMEA/UK/User Accounts/Engineering	Chris French	itmurray.local/Contoso/EMEA/UK/User Accounts/Marketing	Contoso to Fabrikam Users
Create	Chris Carter	charlie.local/Aquisitions/Contoso/EMEA/UK/User Accounts/Engineering	Chris Carter	itmurray.local/Contoso/EMEA/UK/User Accounts/Engineering	Contoso to Fabrikam Users
Delete	Margaret Jackson		Margaret Jackson	itmurray.local/Contoso/EMEA/UK/User Accounts	Contoso to Fabrikam Users
Delete	Mark Edmonds		Mark Edmonds	itmurray.local/Contoso/EMEA/UK/User Accounts	Contoso to Fabrikam Users
Delete	Matt Striner		Matt Striner	itmurray.local/Contoso/EMEA/UK/User Accounts	Contoso to Fabrikam Users

Figure 97 What If Report

You can click directly on an object to see the changes that will be made.

What If Object

Overview

	Source Object	Target Object	Future Target Object
Name	Andy Murray	Andy Murray	Andy Murray
Container	itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ	charlie.local/From itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ	charlie.local/From itmurray.local/10. Hybrid Entra Join to Hybrid Entra Join x-tenant via CDJ
Type	User	User	User
Match Rule	(employeeID) andy.murray	(employeeID) andy.murray	

Attributes

Attribute	Source Value	Existing Target Value	Future Target Value
accountExpires	9223372036854775807	9223372036854775807	9223372036854775807
c	GB	GB	GB
cn	Andy Murray	Andy Murray	Andy Murray
co	United Kingdom	United Kingdom	United Kingdom
company	All England Lawn Tennis & Croquet Club	All England Lawn Tennis & Croquet Club	All England Lawn Tennis & Croquet Club
countryCode	826	826	826
department	PSPMA Matching	PSPMA Matching	PSPMA Matching
description	Former Wimbledon Champion		Former Wimbledon Champion

Figure 98 What If Report Single Object Result



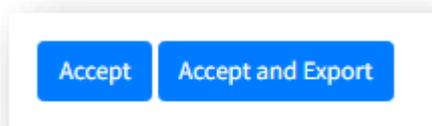
This can be especially important for checking critical attributes like mail, UPN if you are re-writing those attributes:

Accepting a What If Report

Once you are satisfied all looks good and as you are expecting then you can click accept the reports.

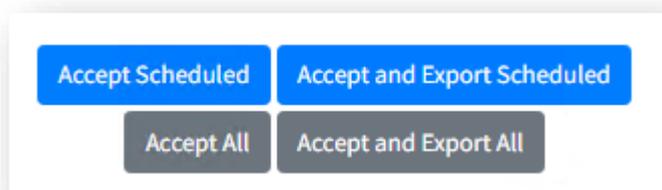
When a single sync profile is selected:

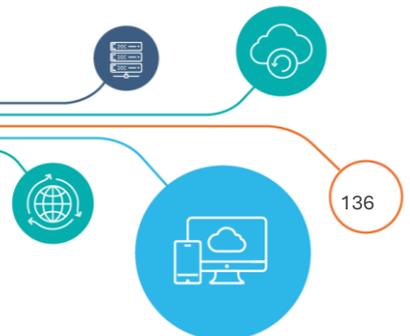
- Accept will just accept the profile and allow it to be exported (manually or via schedule)
- Accept and Export will accept the profile and trigger the export job, just for the selected profile



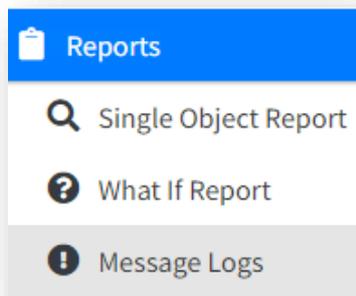
If all profiles of the target directory are selected:

- Accept Scheduled will just accept sync profiles for the target directory, that are part of the schedule
- Accept and Export Scheduled will accept and trigger export jobs for sync profiles for the target directory that are part of the schedule
- Accept All will accept all sync profiles for the target directly - **regardless of if they are included in the schedule i.e. excluded from schedule.**
- Accept and Export All will accept and trigger an export for all sync profiles for the target directly - **regardless of if they are included in the schedule i.e. excluded from schedule.**





Message Logs



Message logs allow you to see all activity for a job. i.e.

- Refresh Schema
- Import Containers
- Import Objects
- Sync Objects
- Export Objects
- Sync SID History
- Sync Passwords

You can access Message Logs from the left-hand navigator, or from the Schedule by clicking any number in the results, errors or warnings columns.

Import Containers	Completed	● ▶	26 July 24 - 03:53 pm	73	0	0	0
Import	Completed	● ▶	26 July 24 - 03:53 pm	971	0	0	0
Sync		▶					
Sync - itmurray.local		▶					
Sync - Contoso to Fabrikam Match and Convert to MEU	Completed	● ▶	26 July 24 - 03:53 pm	1	0	0	0
Sync - Contoso to Fabrikam Groups	Completed	● ▶	26 July 24 - 03:53 pm	0	0	0	0
Sync - Contoso to Fabrikam Users	Completed	● ▶	26 July 24 - 03:53 pm	2	0	0	0
Sync - Divest Widgets	Completed	● ▶	26 July 24 - 03:53 pm	15	0	0	0
Export	Completed	● ▶	26 July 24 - 03:53 pm	0	0	0	0
SID History Sync	Completed	● ▶	26 July 24 - 03:54 pm	18	0	0	0
Password Sync	Completed	● ▶	26 July 24 - 03:23 pm	2	0	0	0

Filter

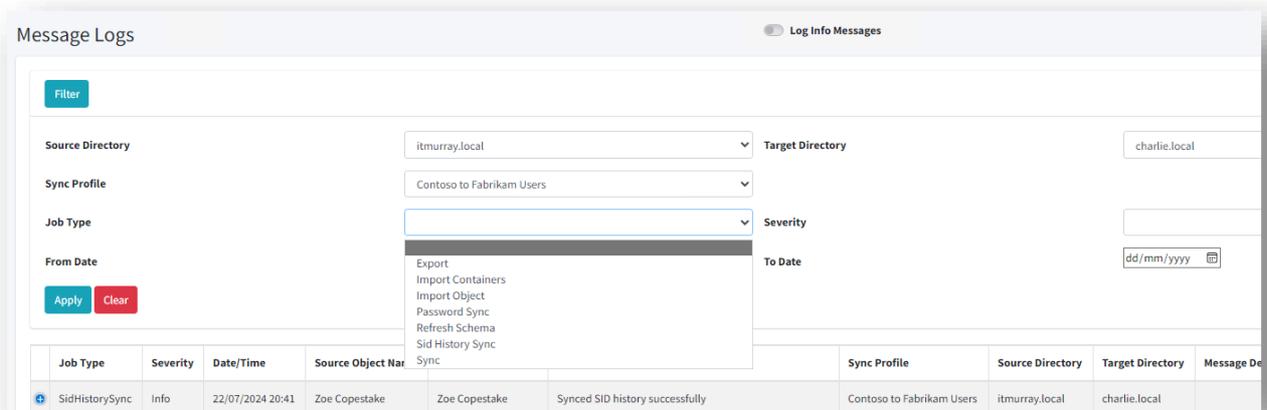


Figure 99 Filter Message Logs

Filter allows you to scope your report per Directory, Sync Profile, Job Type, Severity and date range.

Job Type

- Export
- Import Containers
- Import Object
- Password Sync
- Refresh Schema
- Sid History Sync
- Sync

Severity

- Information
- Warning
- Error
- Skip

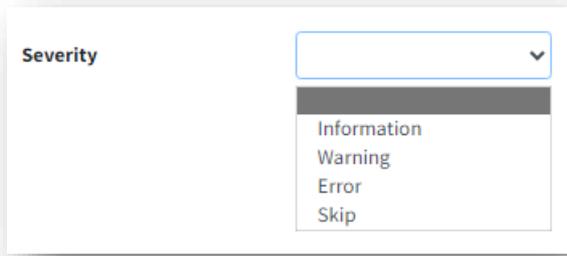


Figure 100 Message Logs - Filter by Severity

Log Info Messages

You can enable “Log Info Messages” to see more detail per object. Note that this does have an impact on performance, and more importantly on the database size (especially for those using SQL Express)

Results

Click a whole row, will open the Single Object Report for that Source object.

Job Type		From Date		To Date		Severity
Password Sync		26/07/2024				
Apply Clear						
	Job Type	Severity	Date/Time	Source Object Name	Target Object Name	Message
+	PasswordSync	Info	26/07/2024 15:23	Chris French	Chris French	Synced password
+	PasswordSync	Info	26/07/2024 15:23	Chris French	Chris French	Passwords last set is non-zero so not setting
+	PasswordSync	Info	26/07/2024 15:23	Chris Carter	Chris Carter	Synced password
+	PasswordSync	Info	26/07/2024 15:23	Chris Carter	Chris Carter	Reset PwdLastSet
C 1-4 of 4 items		Show 100 entries				
Download CSV						

Figure 101 Message Log results



Sync	Info	26/07/2024 15:23	Chris French		Ran complex expression Set UPN to fabrikam.com userPrincipalName	Contoso to Fabrikam Users	itmurray.local	charlie.local	'chris.french@widgets.com' to 'chris.french@fabrikam.com'
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Exporting value for: sAMAccountName	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Exporting value for: displayName	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Suffix Company to DisplayName: Rewrite rule matched attribute	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Suffix Company to DisplayName: Rewrite rule matched attribute	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Exporting value for: sn	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	uppercase: Rewrite rule matched attribute	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Exporting value for: streetAddress	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Exporting value for: company	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Rewrite Company Name: Rewrite rule matched attribute	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Exporting value for: countryCode	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Exporting value for: department	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French	Chris French	Exporting value for: mail	Contoso to Fabrikam Users	itmurray.local	charlie.local	
Sync	Info	26/07/2024 15:23	Chris French		Ran complex expression Set Mail to fabrikam.com mail	Contoso to Fabrikam Users	itmurray.local	charlie.local	'chris.french@widgets.com' to 'chris.french@fabrikam.com'

Job Type	Severity	Date/Time	Source Object Name	Target Object Name	Message	Sync Profile	Source Directory	Target Directory
PasswordSync	Info	26/07/2024 15:23	Chris French	Chris French	Synced password	Contoso to Fabrikam Users	itmurray.local	charlie.local
PasswordSync	Info	26/07/2024 15:23	Chris French	Chris French	Passwords last set is non-zero so not setting	Contoso to Fabrikam Users	itmurray.local	charlie.local
PasswordSync	Info	26/07/2024 15:23	Chris Carter	Chris Carter	Synced password	Contoso to Fabrikam Users	itmurray.local	charlie.local
PasswordSync	Info	26/07/2024 15:23	Chris Carter	Chris Carter	Reset PwdLastSet	Contoso to Fabrikam Users	itmurray.local	charlie.local
SidHistorySync	Info	26/07/2024 15:23	Chris French	Chris French	Synced SID history successfully	Contoso to Fabrikam Users	itmurray.local	charlie.local
SidHistorySync	Info	26/07/2024 15:23	Chris Carter	Chris Carter	Synced SID history successfully	Contoso to Fabrikam Users	itmurray.local	charlie.local
Export	Info	26/07/2024 15:23		Tara Wheatley	Deleted object	Contoso to Fabrikam Users	itmurray.local	charlie.local

Source Object Guid 3EFAB6D2-B293-462F-989B-9FEDEF618B9D

Target Object Guid 939D0158-12F4-4B4A-8209-346E26A60E0A

Source User Principal Name Tara.Wheatley@itmurray.local

Target User Principal Name Tara.Wheatley@charlie.t2t.dev

Source sAMAccountName TWheatley

Target sAMAccountName TWheatley

Source Mail Tara.Wheatley@itmurray.com

Target Mail Tara.Wheatley@charlie.t2t.dev

Source Distinguished Name CN=Tara Wheatley,OU=User Accounts,OU=UK,OU=EMEA,OU=Contoso,DC=itmurray,DC=local

Target Distinguished Name CN=Tara Wheatley,OU=User Accounts,OU=UK,OU=EMEA,OU=Contoso,OU=Aquisitions,DC=charlie,DC=local



Password Sync Logs

Password Sync Logs

Filter

Source Agent	Target Agent	Username	Correlation Id	Severity	Date/Time	Message
DC2.itmurray.local				Warning	30/07/2024 16:35	Agent has not been seen in 1 hours
DC1OTHER.other.local				Warning	30/07/2024 16:35	Agent has not been seen in 1 hours
DC2.itmurray.local		caitlin.gonzales	f9612907-5704-4a45-8ea9-f959fb1fca8	Information	29/07/2024 16:03	User password was changed at 29/07/2024 16:02:39 +12:00. Sending 0 translated headers.
DC2.itmurray.local		caitlin.gonzales	6d4af426-f6d1-48c7-9b44-77f5bfedcbad	Information	26/07/2024 16:38	User password was changed at 26/07/2024 16:38:42 +12:00. Sending 0 translated headers.

1-4 of 4 items Show 10 entries < 1 >

Download CSV

Figure 102 Password Sync Logs

This will show you information about user password changes and failed Agent connectivity.

Windows Application Event Log

Several PSP Server activities are written to the Windows Event Log in Application Event Log.



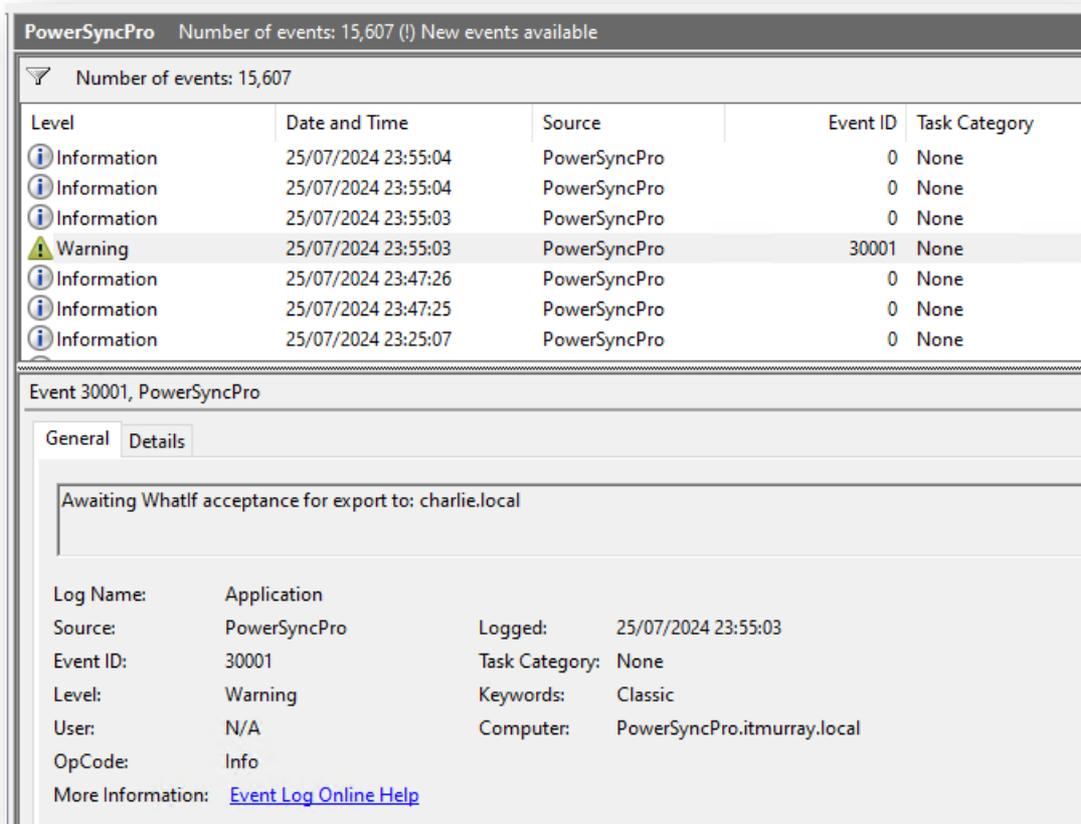


Figure 103 Windows Application Event Logs

Start	End	Name
1	5000	System Reserved
5001	10000	Operational messages
10001	15000	Refresh Schema
15001	20000	Import Containers
20001	25000	Import Objects
25001	30000	Sync Objects
30001	35000	Export Objects
35001	60000	Reserved for future use



60001	65536	Migration Agent
20000	Warning	The HTTPs certificate does not have a private key. Please check that manage private key rights are assigned
30001	Warning	What if report has not been approved
30002	Warning	Awaiting deletion threshold confirmation
30003	Warning	Source Directory Licence Missing
30004	Warning	Target Directory Licence Missing
30005	Warning	Skipped For Staging Mode
60001	Information	Runbook Completed <i>PSP Service detects where Runbook completes and logs some additional information (Runbook Name, Runbook ID, Directory and Machine Name)</i>

Support

You can raise Support tickets at: <https://tickets.powersyncpro.com/>

