PowerSyncPro

Integrate. Collaborate. Migrate.

# Prerequisites

## PowerSyncPro Service

Last updated: 26 March 2025

PowerSyncPro

# Contents

# Purpose of this Document

This document describes the prerequisites needed for PowerSyncPro Service. Note that a Proof of Concept "POC" is explicitly in a **non-production** environment. We cannot issue a licence for a POC in a production environment.

# Server Sizing

The recommended size for the PowerSyncPro Server depends on the number of Migration Agents reporting to it, as well as the number of objects being synchronised.

Up to 1,000 Agents and 100,000 Objects

- 2 vCPU
- 16 GB RAM
- Additional 100 GB data drive
- SQL Express can be used

Up to 10,000 Agents and 1,000,000 objects

- 4 vCPU
- 32 GB RAM
- Additional 250 GB data drive
- Full SQL version is needed

Servers that are running the Remote Sync Agent, or Remote Proxy Agent should have at least 2 vCPU, 4GB RAM. Domain Controllers running the Remote Password Agent don't need any additional hardware over and above what a standard Domain Controller needs.

The servers can be physical or virtual and can be in private or public cloud. Using remote agents, the PSP Server itself can be in a DMZ or largely isolated network without needing access to the on-premises domains. The main requirement is network connectivity as discussed in the sections below.

# Supported Scenarios

The PowerSyncPro Server can be installed in a Workgroup, in a source or target Active Directory. It can be a physical or virtual server and can be in private or public cloud.

We recommend that you install PowerSyncPro into an Active Directory domain, hosting its own SQL Server instance, and with low latency access to all the directories it needs to access. PowerSyncPro is more latency sensitive on writes, so if a choice is needed then place it closer to the target directories.

To provide DR we recommend using two PowerSyncPro servers, both hosted within an Active Directory domain and using the same Group Managed Service Account. Both PowerSyncPro servers each have their own SQL Server instance, and a database backup can be restored from one to the other after configuration changes have been made. That way the configuration will be identical on both servers. One server must be placed into staging mode.

NOTE that this basic level of DR is only for the Synchronisation side. The Migration Agent requires clustering for DR with SQL High Availability.

# Prerequisite Software

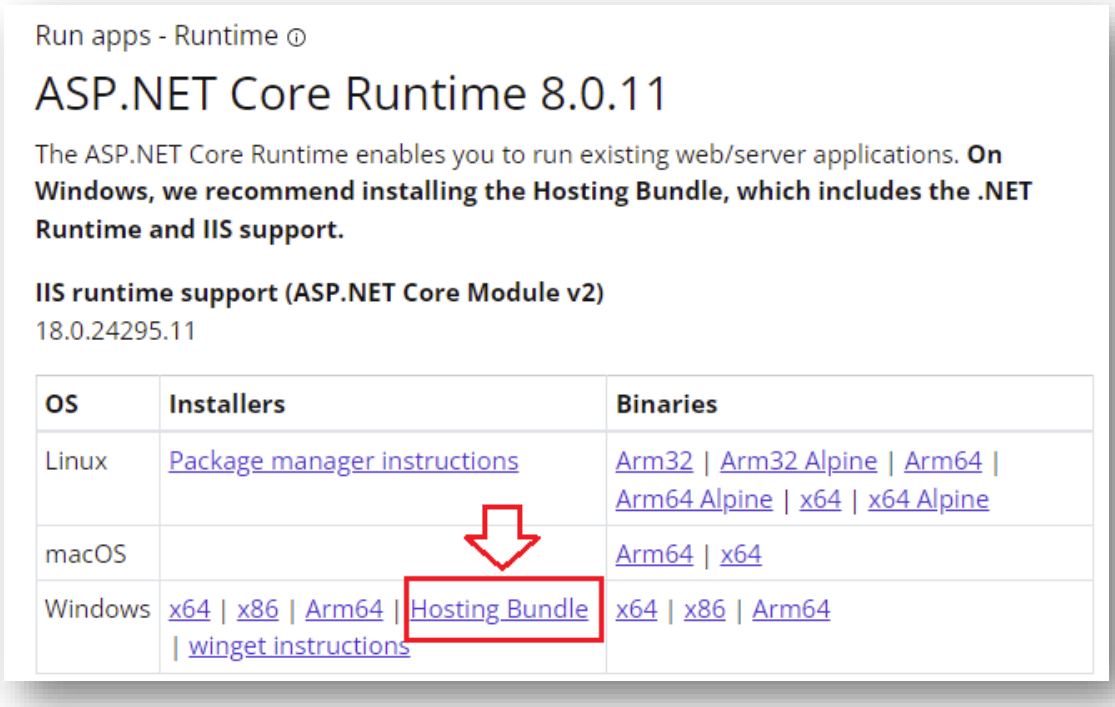
## PowerSyncPro Service

The following software dependencies exist

- Windows Server 2016 or later
- SQL Server 2019 or later
    - SQL Express 2019 or later is also a valid option
- SQL Server Management Studio
    - https://learn.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver16
- For Active Directory syncs, Domain Controllers running Windows Server 2003 or later are needed

The following software must be installed prior to installing PowerSyncPro. Note that the below generally require a reboot after the installation

- .Net ASP.NET Core Runtime 8.x (hosting bundle) (https://dotnet.microsoft.com/en-us/download/dotnet/8.0)




- Microsoft Visual C++ Redistributable (https://aka.ms/vs/17/release/vc_redist.x64.exe)

> **NOTE:** if you are upgrading from the .NET 6 version of PSP then before you run the PSP Service installer, please update appsettings.json to add TrustServerCertificate=true; to the SQL Connection string. Failure to do so will result in a failed upgrade, and will then require a reinstall of PSP (with the existing database).

## PowerSyncPro Remote Agents

The Remote Password Agent requires Microsoft Visual C++ Redistributable (https://aka.ms/vs/17/release/vc_redist.x64.exe)

The Remote Sync Agent requires .Net 8.x Desktop Runtime) (https://dotnet.microsoft.com/en-us/download/dotnet/8.0)

Aside from that the software can run on any supported Microsoft Server Operating System and can run on 2vCPU with 4GB RAM.

## Internet Information Services – IIS

If you want to use IIS as a reverse proxy, then before running the PowerSyncPro installer, IIS has to be installed, and URL Rewrite/MS Application Request Routing needs to have been installed and enabled.

### Base IIS

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

### URL Rewrite

URL Rewrite: The Official Microsoft IIS Site
https://www.iis.net/downloads/microsoft/url-rewrite

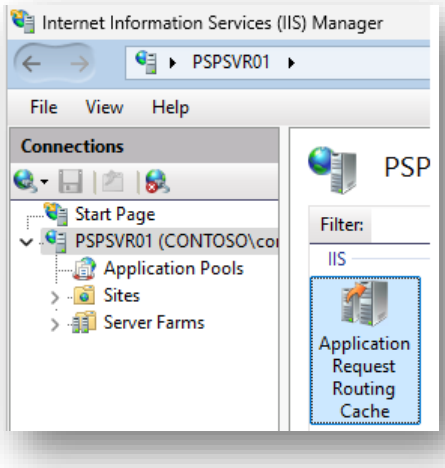
### Application Request Routing

Download Microsoft Application Request Routing 3.0 (x64) from Official Microsoft Download Center
https://www.microsoft.com/en-us/download/details.aspx?id=47333

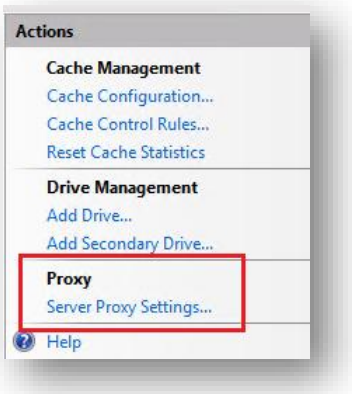
### Enable Application Request Routing on IIS

To enable ARR on IIS:

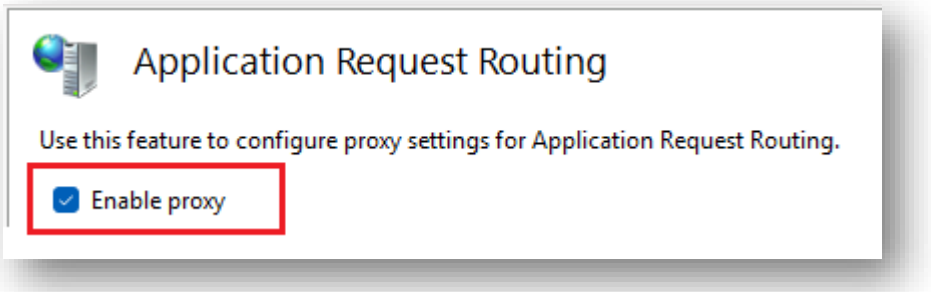
1. Open Internet Information Services (IIS) Manager
2. In the **Connections** pane, select the server
3. In the server pane, double-click **Application Request Routing Cache**



4. In the Actions pane, click **Server Proxy Settings**




5. On the Application Request Routing page, select **Enable proxy**




6. In the Actions pane, click Apply

# PSP Service and PSP Agent

## Endpoint

The communication between your remote agents and the PowerSyncPro server needs to be configured end-to-end for the endpoint name you choose. You will almost certainly need to open firewall ports and add a DNS record internally and externally. The endpoint will be referenced as an http(s) name e.g. http://psp.contoso.com:5000/Agent or https://psp.contoso.com/Agent

By default with no additional configuration, Windows workstation migration agents can connect to the PowerSyncPro server Kestrel endpoint on the FQDN of the server e.g. http://pspservero1.contoso.local:5000/Agent (providing TCP Port 5000 is allowed inbound on the server).

Network traffic between the workstation and the server for migration agent activity is always encrypted using the PowerSyncPro Certificate configuration in the Migration console, albeit that the whole session is not encapsulated in SSL. To achieve this, you should configure an appliance in front of the PSP Server or us an IIS Reverse Proxy on the server with a URL rewrite configured.

**Workstation Migration Agent**

Every PSP Workstation Migration Agent must be able to get to "/agent" for the PSP Service. This is both for registration and runbook retrieval/execution. In most cases this will mean publishing the PSP Service to the Internet, and then control that to only allowing "/agent" to be accessed.

**Remote Agents**

Every Remote Sync/Password or proxy agent must be able to get to the port specified during install for the Kestrel endpoint (default 5001). e.g. https://psp.contoso.com:5001/Agent

This can either be direct from those agents or via proxy agents that are discovered using an Active Directory stored Service Connection Point (see the configuration guide for more information).

## Network Ports

If you use IIS/Application Gateway/Load Balancer as a reverse proxy then communication can be simplified. Note that the Remote Agents (Proxy, Sync and Password) must not go via an appliance that can't communicate via HTTP/2 to the backend service. HTTP/2 is required for the gRPC part of the agents.

| From | To | Protocol | Port | Comments |
|---|---|---|---|---|
| **PSP Service** | AD Domain Controller | TCP | 389 | |
| **PSP Service** | AD Domain Controller | TCP | 636 | Optional. Requires additional configuration |
| **PSP Migration Agent** | PSP Service | TCP | 443 | Using the reverse proxy |
| **PSP Proxy Agent** | PSP Service | TCP | 5001 | Port can be changed at installation time |

| | | | | |
|---|---|---|---|---|
| **PSP Sync Agent** | PSP Proxy Agent | TCP | 5001 | Port can be changed at installation time. Not needed if a Proxy Agent has been deployed |
| **PSP Password Agent** | PSP Proxy Agent | TCP | 5001 | Port can be changed at installation time. Not needed if a Proxy Agent has been deployed |

If you DO NOT use IIS/Application Gateway/Load Balancer as a reverse proxy then communication is directly to the ports configured during the install (5000 and 5001 by default).

| From | To | Protocol | Port | Comments |
|---|---|---|---|---|
| **PSP Service** | AD Domain Controller | TCP | 389 | |
| **PSP Service** | AD Domain Controller | TCP | 636 | Optional. Requires additional configuration |
| **PSP Migration Agent** | PSP Service | TCP | 5000 | Port can be changed at installation time |
| **PSP Sync Agent** | PSP Service | TCP | 5001 | Port can be changed at installation time. If a proxy agent is available then that is chosen route |
| **PSP Password Agent** | PSP Service | TCP | 5001 | Port can be changed at installation time . If a proxy agent is available then that is chosen route |
| **PSP Proxy Agent** | PSP Service | TCP | 5001 | Port can be changed at installation time |
| **PSP Sync Agent** | PSP Proxy Agent | TCP | 5001 | Port can be changed at installation time |
| **PSP Password Agent** | PSP Proxy Agent | TCP | 5001 | Port can be changed at installation time |

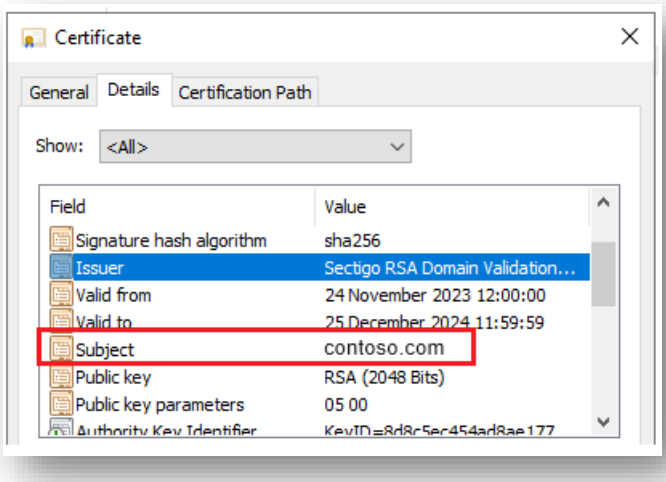
## SSL

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



# PSP Service and Active Directory

## General Sync

### Network Ports

The following ports are needed to do an Object Sync or Match, note that if remote sync agents are used then the PSP Service does not need any communication with those domains directly.

| From | To | Protocol | Port | Comments |
|---|---|---|---|---|
| **PSP Service** | Source Domain Controller | TCP | 389 | |
| **PSP Service** | Source Domain Controller | TCP | 636 | If LDAP over SSL is configured |
| **PSP Service** | Target Domain Controller | TCP | 389 | |
| **PSP Service** | Target Domain Controller | TCP | 636 | If LDAP over SSL is configured |
| **PSP Sync Agent** | Source Domain Controller | TCP | 389 | |
| **PSP Sync Agent** | Source Domain Controller | TCP | 636 | If LDAP over SSL is configured |
| **PSP Sync Agent** | Target Domain Controller | TCP | 389 | |
| **PSP Sync Agent** | Target Domain Controller | TCP | 636 | If LDAP over SSL is configured |

### Permissions

The following permissions are needed for an Object Sync

#### Source Active Directory

- Read Access to all Objects
- Read Access to the Recycle Bin (see enable rights to AD Recycle Bin)

#### Target Active Directory

- Read/Write Access to all Objects in scope (Typically by delegating access to target OUs)
- Read/Write Access to the Recycle Bin
- Delegated access to re-animate objects from the Recycle Bin

Note that Password Sync and SID History Sync have additional requirements, listed below.

## Password Sync

Passwords can be synced between Active Directory domains only, and there are two methods for syncing passwords. The Legacy Password Sync way is using the NTHash based sync which relies on RC4 being left enabled in Active Directory. The Modern Password Sync way is using the remote password agent installed on every DC where a user may change their password

### Network Ports

The following additional ports are needed to do Legacy Password Sync

| From | To | Protocol | Port | Comments |
|---|---|---|---|---|
| **PSP Server** | Target PDC FSMO Holder | TCP | 135 | RPC Endpoint Mapper |
| **PSP Server** | Target PDC FSMO Holder | TCP | RPC Ports | |

The Modern Password Sync way does not need any additional ports

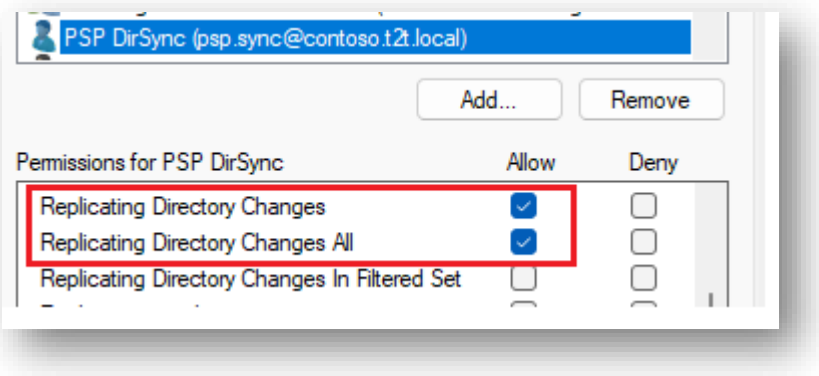
### Permissions

The permissions required are the same for both the Legacy and Modern Password Sync methods

#### Source Active Directory

Grant the PowerSyncPro Service Account the following rights at the Domain level.

- Replicating Directory Changes
- Replicating Directory Changes All



Target Active Directory

- Full Control over the User Accounts

## SIDHistory Sync

SIDHistory can be synced between Active Directory domains only. Directory Sync supports SID History migration for environments that have an Active Directory trust configured as well as environments without a trust configured. To facilitate the SID History migration, the following is a list of minimum requirements to configure to facilitate using Directory Sync with your On-Premises Active Directory.

If using a remote sync agent, then for SID History to sync each remote sync agent must be configured with credentials for both the source and target domains.

### Network Ports

The following additional ports are needed to do SID History Sync without remote sync agents

| From | To | Protocol | Port | Comments |
|---|---|---|---|---|
| **PSP Server** | Target PDC FSMO Holder | TCP | 135 | RPC Endpoint Mapper |
| **PSP Server** | Target PDC FSMO Holder | TCP | RPC Ports | |
| **Target PDC FSMO Holder** | Source PDC FSMO Holder | TCP | 135 | RPC Endpoint Mapper |
| **Target PDC FSMO Holder** | Source PDC FSMO Holder | TCP | RPC Ports | |

The following additional ports are needed to do SID History Sync WITH remote sync agents

| From | To | Protocol | Port | Comments |
|---|---|---|---|---|
| **PSP Sync Agent** | Target PDC FSMO Holder | TCP | 135 | RPC Endpoint Mapper |
| **PSP Sync Agent** | Target PDC FSMO Holder | TCP | RPC Ports | |
| **Target PDC FSMO Holder** | Source PDC FSMO Holder | TCP | 135 | RPC Endpoint Mapper |
| **Target PDC FSMO Holder** | Source PDC FSMO Holder | TCP | RPC Ports | |

## Permissions

### Source Active Directory

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

This is typically enabled for Domain Admins and Enterprise Admins, but can be enabled for a specific group or user by following the below steps:

a) Navigator to Built-in organization unit in Active Directory Users and Computers.
b) Locate the Administrators group and ensure the source service account is a member of the group. (direct or nested)

## Target Active Directory

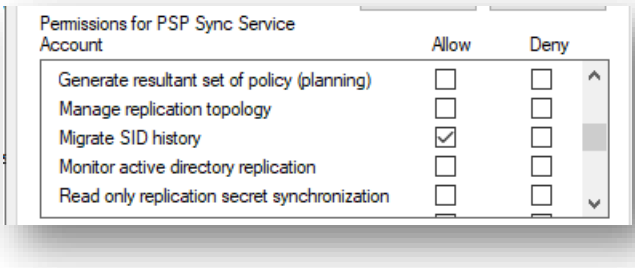
### SID History

If you are intending on synchronising SIDHistory, then you will need to make additional configurations.

Migrate SID History permissions are required on the target domain. This is typically enabled for Domain Admins and Enterprise Admins, but can be enabled for a specific group or user by following the below steps:

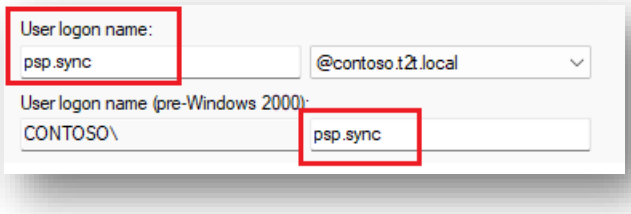
a) Right-click on your target domain in Active Directory Users and Computers.
b) Select the Security tab and add or update the desired group or user and enable the **"Migrate SID History"** permission.

***Delegated Rights on the Domain: Migrate SID History***




Your Service account will also need to be a member of the Administrators Group.

> **NOTE:** The sAMAccountName must match the left part of the userPrincipalName of your PowerSyncPro Service Account




## Active Directory Configuration

### Source Active Directory

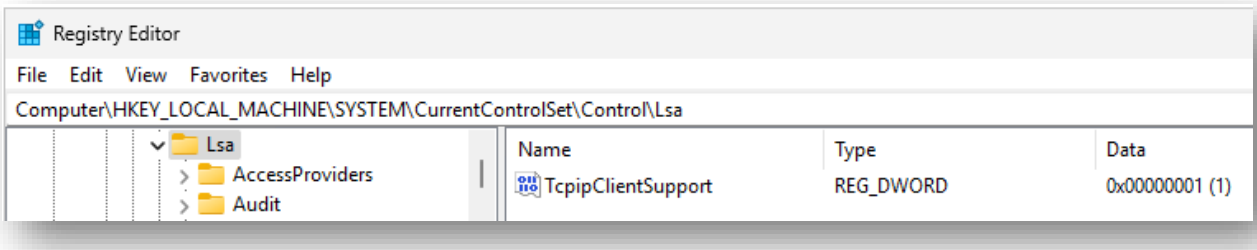
**Domain Local Group**

- In the source AD Domain, create a local group called SourceDomain$$$, where SourceDomain is the NetBIOS name of your source AD Domain.
    - For example, if your domain's NetBIOS name is CONTOSO, you must create a domain local group named CONTOSO$$$.

**Enable TCP/IP client support**

Enable TCP/IP client support on the source domain PDC emulator:

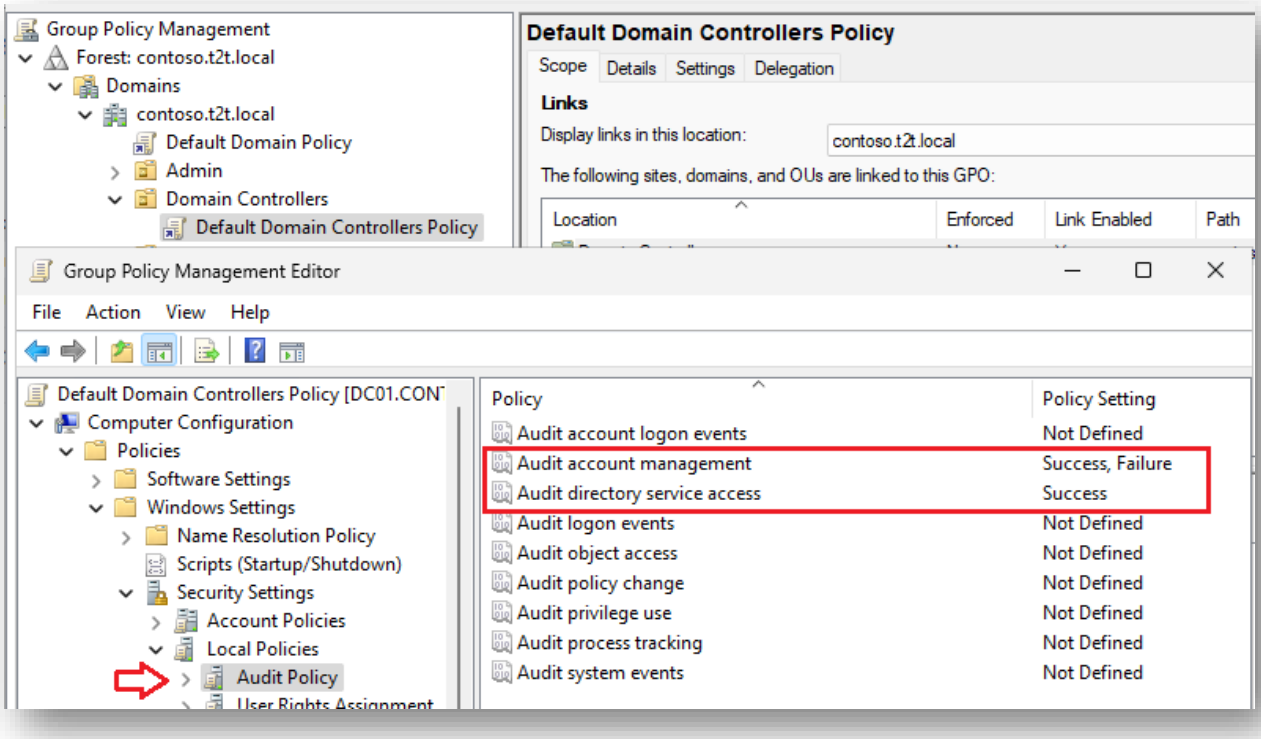
a) On the domain controller in the source domain that holds the PDC emulator operations master (also known as flexible single master operations or FSMO) role
b) Open regedit
c) In Registry Editor, navigate to the following registry subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
d) Create or modify the registry entry TcpipClientSupport, of data type REG_DWORD
    a. Sett the value to 1.



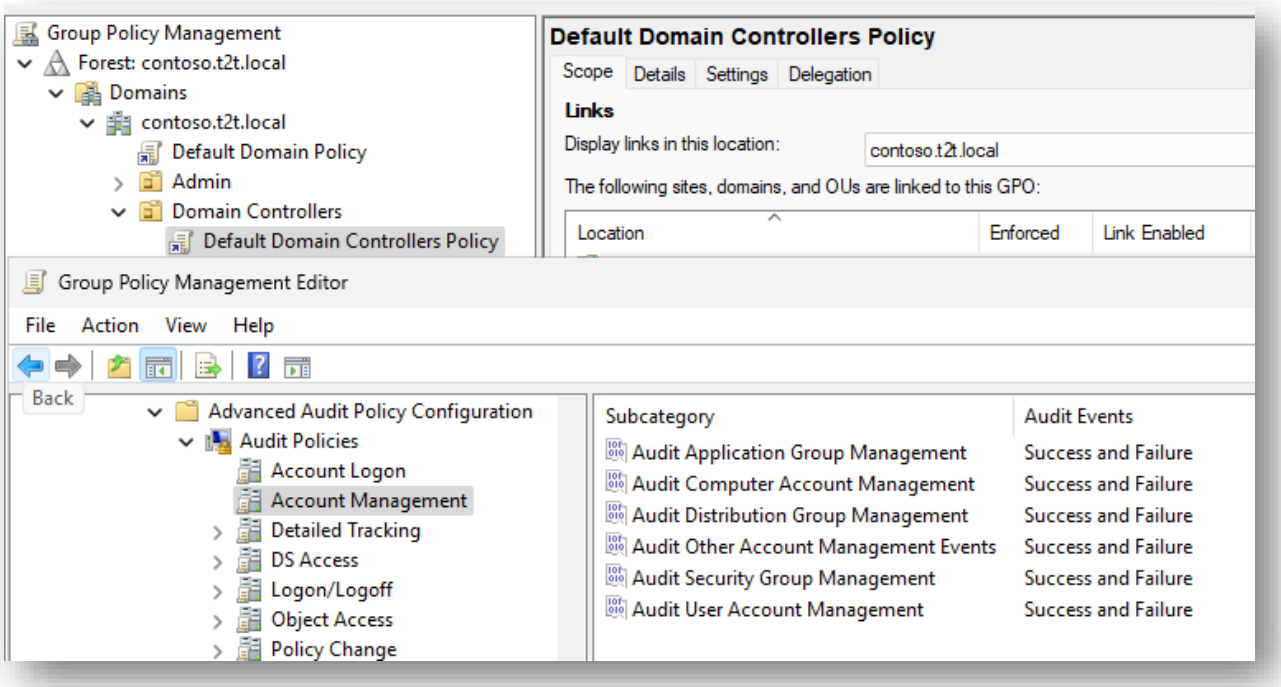

e) Close Registry Editor and then restart the computer.

**Auditing**

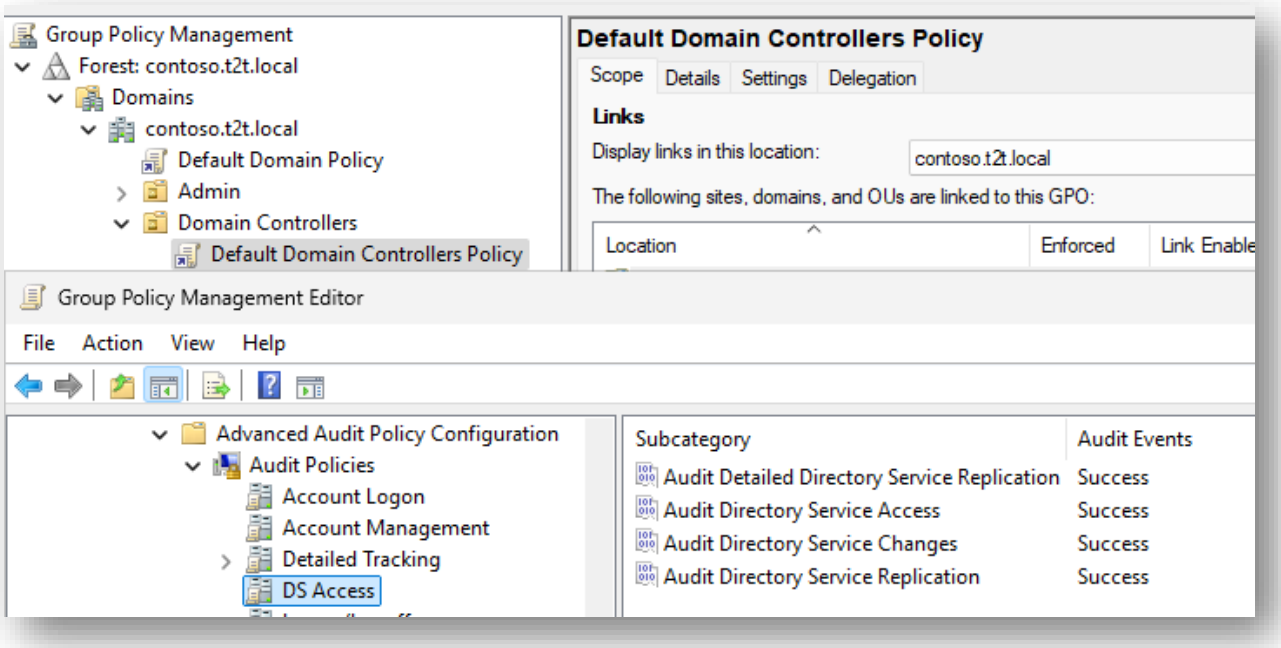
- Enable Auditing (if classic auditing is used); within group policy **Default Domain Controllers Policy** go to Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, Audit Policy and enable **Success and Failure** for
    - Audit Account Management
    - Audit Directory Service Access




- Enable Auditing (if advanced auditing is used); within group policy **Default Domain Controllers Policy** go to Computer Configuration, Policies, Windows Settings, Security Settings, *Advanced Audit Policy Configuration*, Audit Policies and enable **Success and Failure** for
    - Account Management; Audit Application Group Management
    - Account Management; Audit Computer Account Management
    - Account Management; Audit Distribution Group Management
    - Account Management; Audit Other Account Management Events
    - Account Management; Audit Security Group Management
    - Account Management; Audit User Account Management




- DS Access; Audit Detailed Directory Service Replication
- DS Access; Audit Directory Service Access
- DS Access; Audit Directory Service Changes
- DS Access; Audit Directory Service Replication

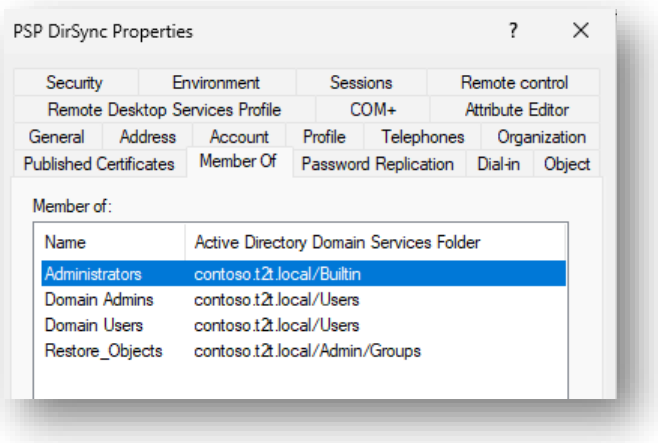



**Administrator access to the source PDC emulator**

The source credentials must have administrator access to the source PDC emulator. This is typically enabled for Domain Admins and Enterprise Admins, but can be enabled for a specific group or user by following the below steps:

Navigator to Built-in organization unit in Active Directory Users and Computers.

Locate the “Administrators” group and ensure the source service account is a member of the group.



Target Active Directory
**Auditing**

- Enable Auditing (if classic auditing is used); within group policy **Default Domain Controllers Policy** go to Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, Audit Policy and enable **Success and Failure** for
    - Audit Account Management
    - Audit Directory Service Access
- Enable Auditing (if advanced auditing is used); within group policy **Default Domain Controllers Policy** go to Computer Configuration, Policies, Windows Settings, Security Settings, *Advanced Audit Policy Configuration,* Audit Policies and enable **Success and Failure** for
    - Account Management; Audit Application Group Management
    - Account Management; Audit Computer Account Management
    - Account Management; Audit Distribution Group Management
    - Account Management; Audit Other Account Management Events
    - Account Management; Audit Security Group Management
    - Account Management; Audit User Account Management
    - DS Access; Audit Detailed Directory Service Replication
    - DS Access; Audit Directory Service Access
    - DS Access; Audit Directory Service Changes
    - DS Access; Audit Directory Service Replication

**Note:**
It may also be necessary to reboot the domain controller to have auditing take effect.

Even with group policy applied on the default domain controller for the domain audit, the server audit setting on the primary domain controller (PDC) may not be enabled. Please confirm this setting is enabled for the local security policy on the PDC server. If not enabled, use the local security policy to enable this setting.

## AD Recycle Bin

### Enable rights over the AD Recycle Bin

Enable the AD Recycle Bin if it is not already enabled:
Run the following command and an elevated PowerShell prompt:

```
Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet -
Target [your AD Forest]
```

Create a Global Security Group called **"Restore_Objects"** and add the PSP Service Account to this Group

Run the following commands and an elevated command prompt:

```
dsacls "dc=yourdomain,dc=local" /g "Restore_Objects:ca;Reanimate Tombstones"
dsacls "CN=Deleted Objects,dc=yourdomain,dc=local" /takeownership
dsacls "CN=Deleted Objects,dc= yourdomain,dc=local" /g "Restore_Objects:LCRP"
dsacls "dc=yourdomain,dc=local" /I:T /g "Restore_Objects:WPCC"
```

# PSP Service and Entra ID

## Network Ports

| From | To | Protocol | End-point |
|---|---|---|---|
| **PSP Server** | Azure AD | TCP Port 443 | *.auth.microsoft.com, *.msftidentity.com, *.msidentity.com, account.activedirectory.windowsazure.com, accounts.accesscontrol.windows.net, adminwebservice.microsoftonline.com, api.passwordreset.microsoftonline.com, autologon.microsoftazuread-sso.com, becws.microsoftonline.com, ccs.login.microsoftonline.com, clientconfig.microsoftonline-p.net, companymanager.microsoftonline.com, device.login.microsoftonline.com, graph.microsoft.com, graph.windows.net, login.microsoft.com, login.microsoftonline.com, login.microsoftonline-p.com, login.windows.net, logincert.microsoftonline.com, loginex.microsoftonline.com, login-us.microsoftonline.com, nexus.microsoftonline-p.com, passwordreset.microsoftonline.com, provisioningapi.microsoftonline.com 20.20.32.0/19, 20.190.128.0/18, 20.231.128.0/19, 40.126.0.0/18, 2603:1006:2000::/48, 2603:1007:200::/48, 2603:1016:1400::/48, 2603:1017::/48, 2603:1026:3000::/48, 2603:1027:1::/48, 2603:1036:3000::/48, 2603:1037:1::/48, 2603:1046:2000::/48, 2603:1047:1::/48, 2603:1056:2000::/48, 2603:1057:2::/48 |

Office 365 URLs and IP address ranges
[Office 365 URLs and IP address ranges - Microsoft 365 Enterprise | Microsoft Learn]

## Entra App Registration

For PowerSyncPro to communicate with your tenant, you will need to create an App registration.

## Automated script to create Entra App registration

You can automate the creation of the application using the script from our knowledge base. You will need to have global admin rights, the Tenant ID and Microsoft Graph PowerShell.

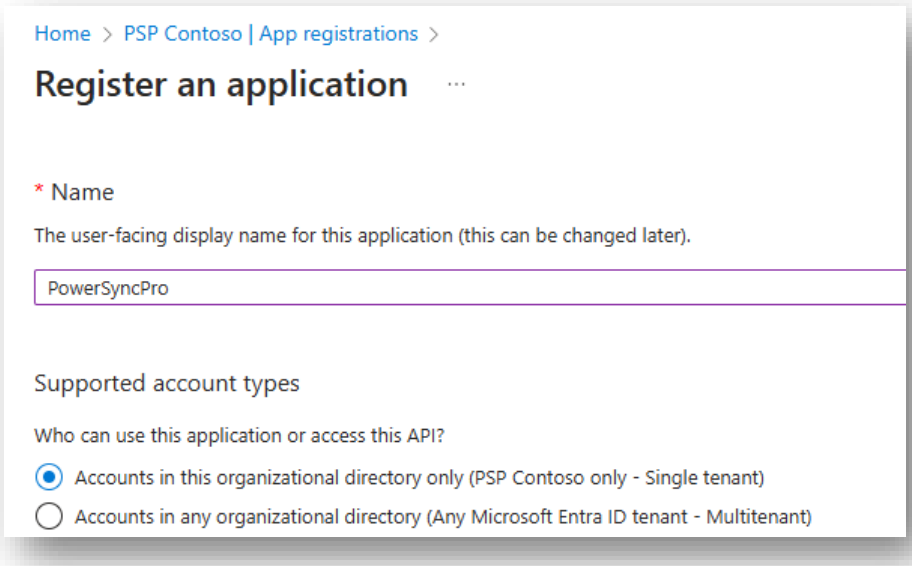
For full requirements review this KB article.

https://kb.powersyncpro.com/en_US/create-powersyncpro-entraid-application

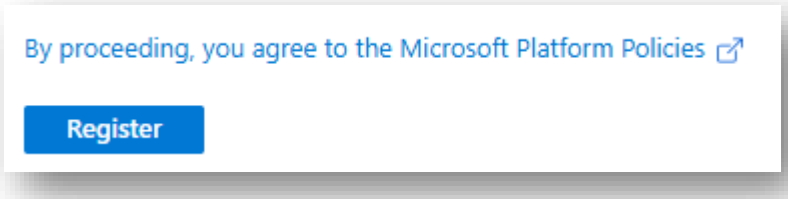
## Manual creation of Entra App registration

### Source Entra ID

Create an Azure AD App Registration.  Give it a meaningful name and choose “Accounts in this organizational directory only (PSP Contoso only - Single tenant)” for Supported account types.

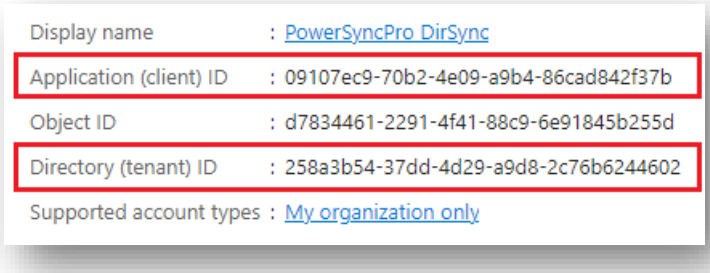


Click Register




Be sure to make a note of the **Application (client) ID**, the **Directory (tenant) ID** and the **Client Secret Value** that is generated (later in the process). You will need these in your PowerSyncPro Directory Configuration.

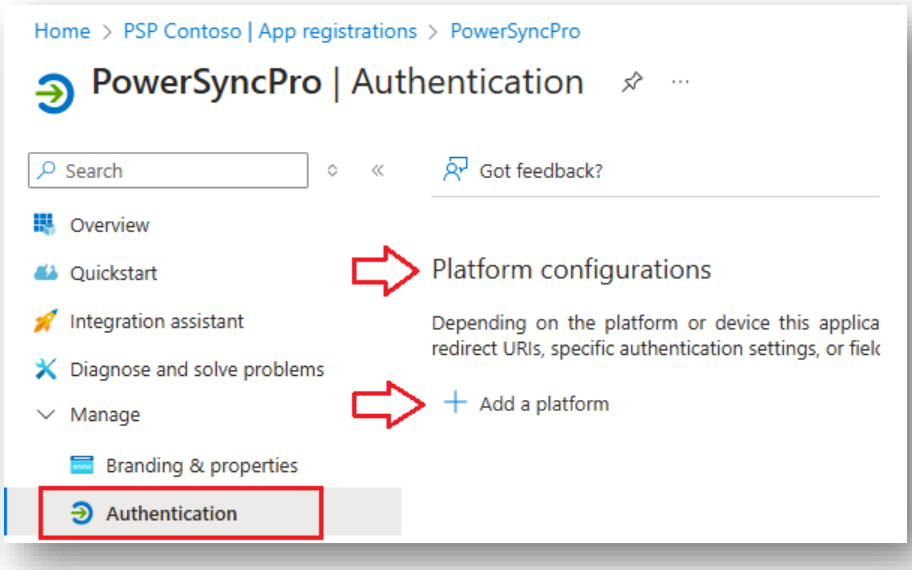
**Application (client) ID and Directory (tenant) ID**



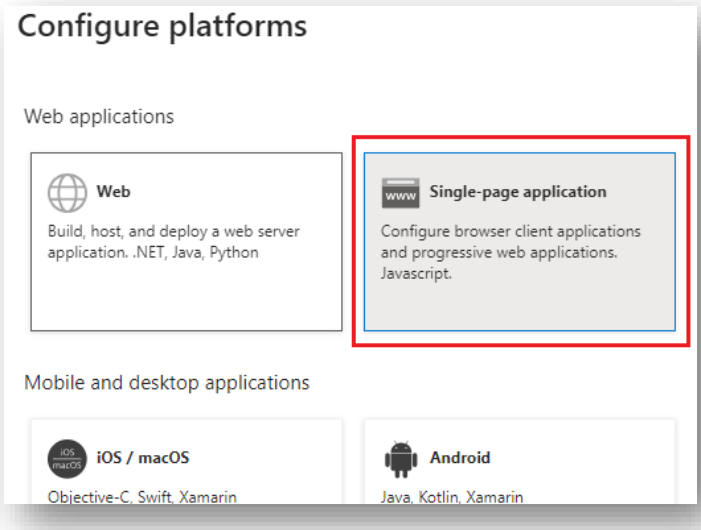

## Redirect URI

In the app registration for the Target Entra ID, to generate Bulk Enrollment Tokens (BPRT), to support Entra Join device migrations, the app registration needs to have a Single Page Application redirect URI. The URI should match the URI that you use to administer the PowerSyncPro administration service followed by /redirect

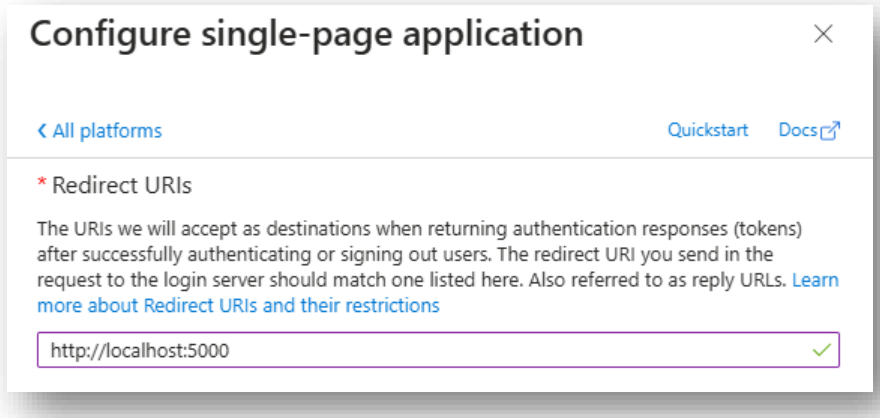
Go to:
Authentication\Platform configurations\Add a platform



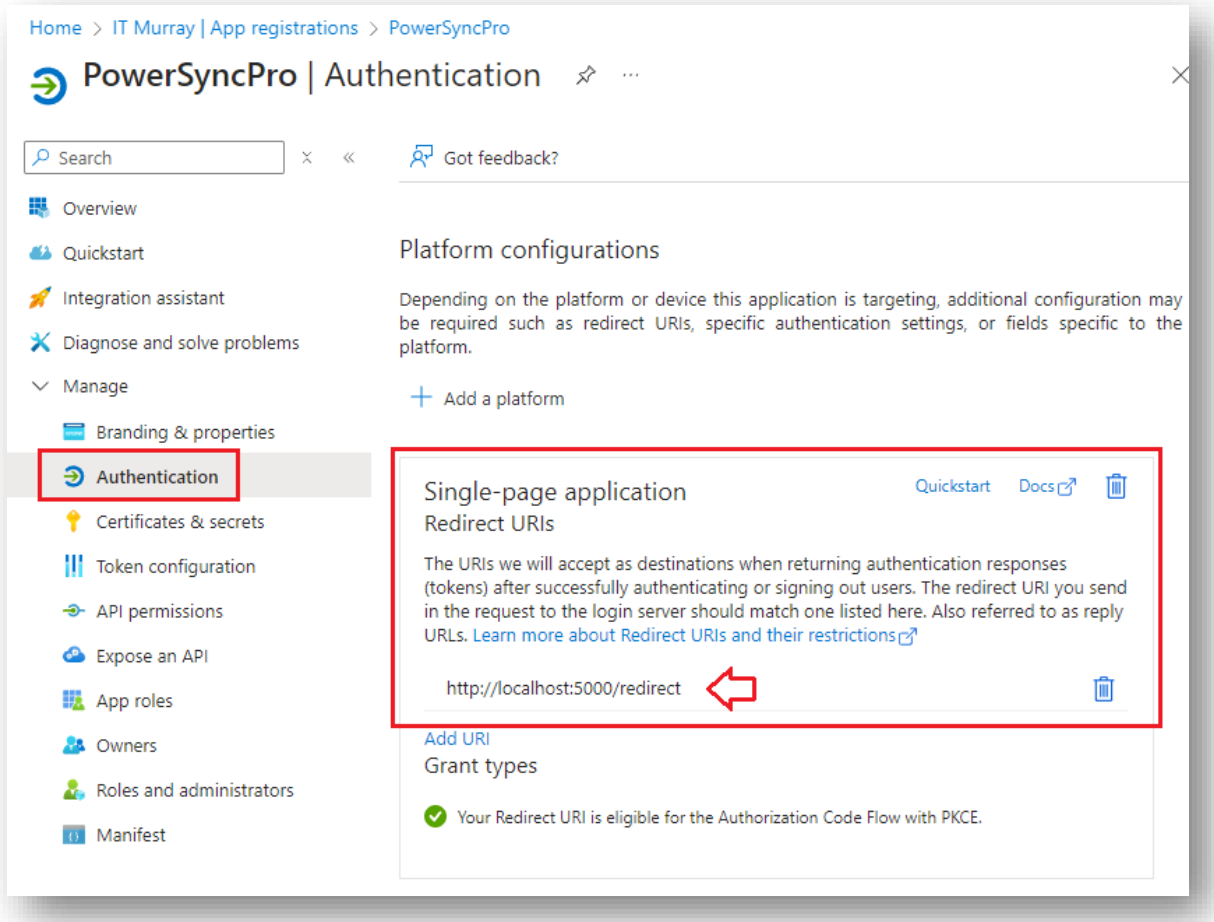

and choose **Single-page application**




add http://localhost:5000/redirect and click Configure


Configure single-page application
All platforms
Quickstart
Docs
* Redirect URIs
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions
http://localhost:5000


Configure
Cancel

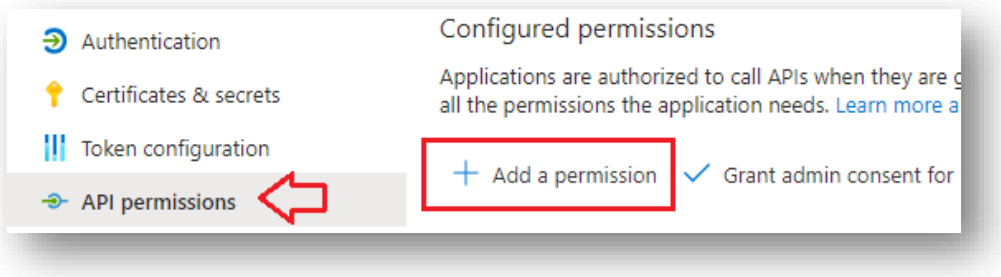

Home > IT Murray | App registrations > PowerSyncPro
PowerSyncPro | Authentication
Search
Got feedback?
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Platform configurations
Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.
Add a platform
Single-page application
Quickstart
Docs
Redirect URIs
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions
http://localhost:5000/redirect
Add URI
Grant types
Your Redirect URI is eligible for the Authorization Code Flow with PKCE.

## API permissions

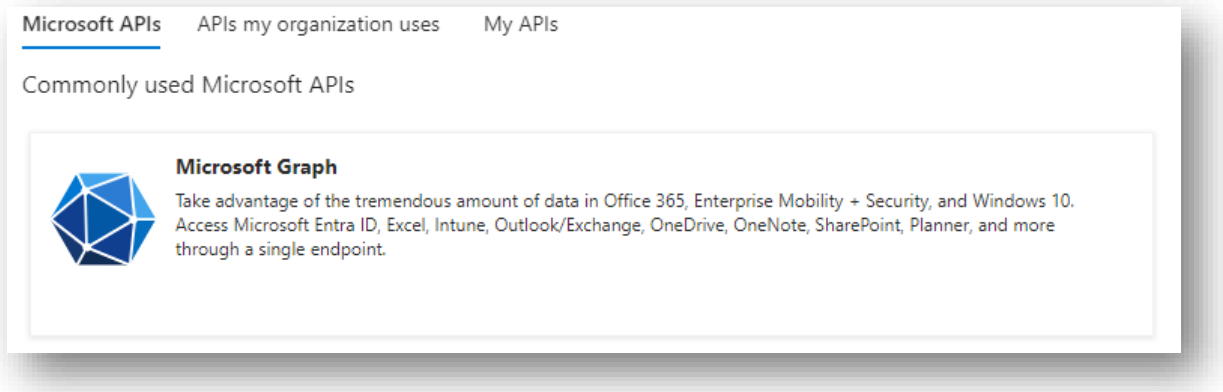
**Use Case**

For Directory Synchronisation and Workstation Migrations you will need the following permissions. Add the following API permissions.

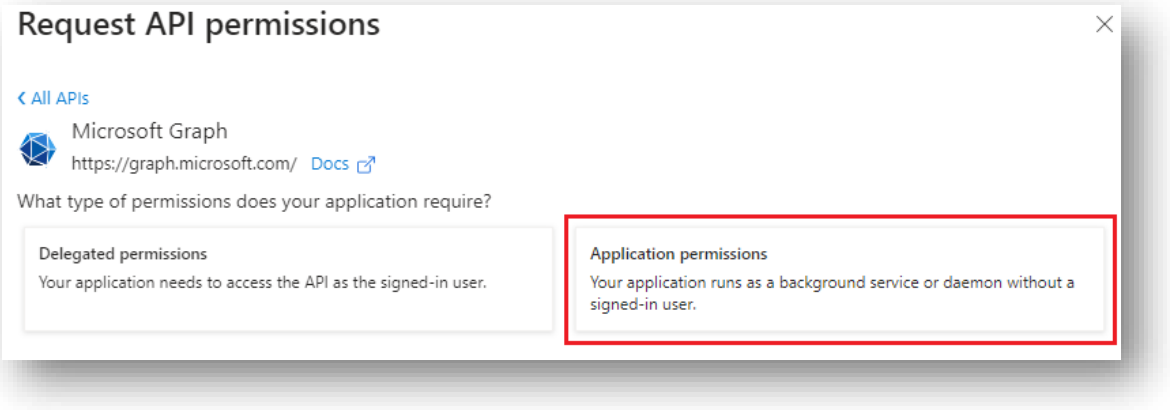
Go to Add a permission,




select Microsoft APIs**Microsoft Graph**




Choose **Application permissions**



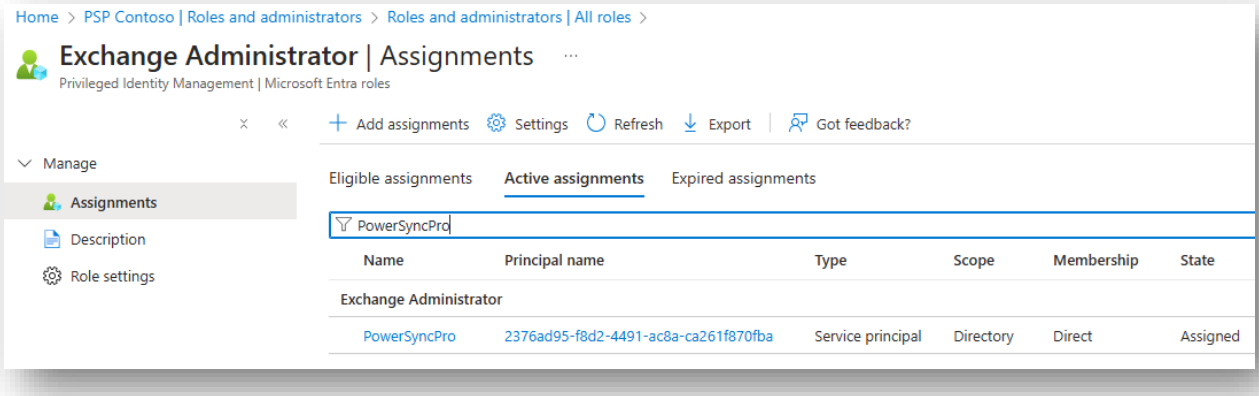

Note for the Source Directory these are all Read Permissions. If you are anticipating on doing a two-way sync, then these will need to be read and write.

| API / Permissions name | Type | Description |
|---|---|---|
| **Microsoft Graph** | | |
| Device.Read.All | Application | Read all devices (if importing devices) |
| Directory.Read.All | Application | Read directory data (if using any directory extensions) |
| Domain.Read.All | Application | Read domain data (to get the onmicrosoft.com name) |
| Group.Read.All | Application | Read all groups (if importing groups) |
| GroupMember.Read.All | Application | Read all group memberships (if importing group members) |
| User.Read.All | Application | Read all users' full profiles (if importing users) |

If you will be synchronising Exchange Online to Exchange Online objects, you will also need:

| API / Permissions name | Type | Description |
|---|---|---|
| **Office 365 Exchange Online** | | |
| Exchange.ManageAsApp | Application | Manage Exchange As Application (if importing from Exchange Online is required) |

If you are planning to synchronise Exchange Online Distribution Groups that are not security enabled, then you additionally need to add the App Registration into the appropriate Entra Role Group.

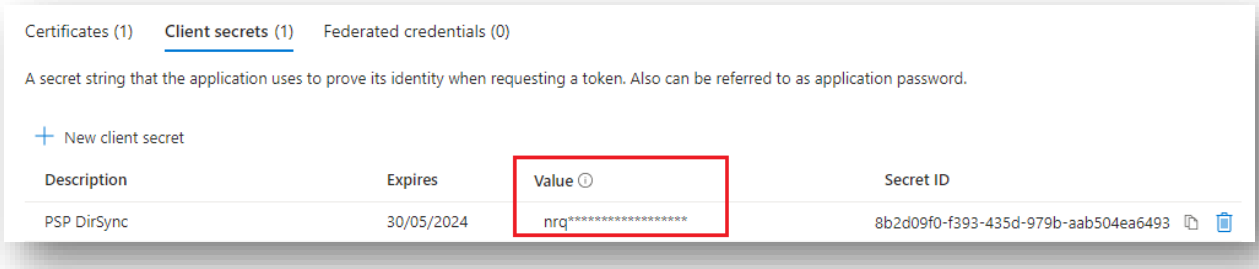



## Client Secret

Generate a Client Secret

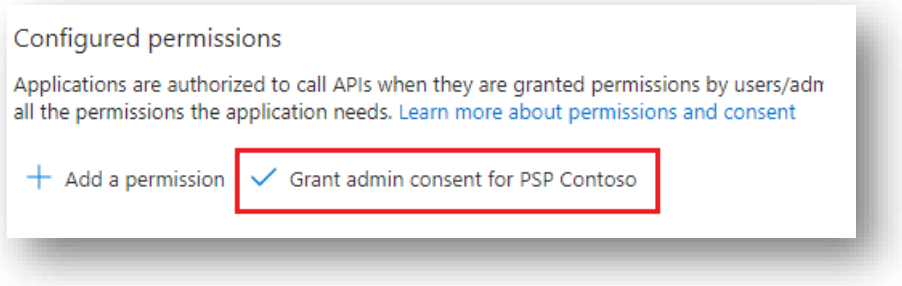
App Secret Value

> Be sure to copy this before you leave this screen as it is **only shown once.**




**Admin Consent**

Remember to Grant admin consent for your tenant.




### Example App Registration Manifest

For ease here is part of a manifest file that can be pasted into the App Registration **"requiredResourceAccess"** section.

```
"requiredResourceAccess": [
   {
      "resourceAppId": "00000003-0000-0000-c000-000000000000",
      "resourceAccess": [
         {
            "id": "7438b122-aefc-4978-80ed-43db9fcc7715",
            "type": "Role"
         },
         {
            "id": "7ab1d382-f21e-4acd-a863-ba3e13f7da61",
            "type": "Role"
         },
         {
            "id": "dbb9058a-0e50-45d7-ae91-66909b5d4664",
            "type": "Role"
         },
         {
            "id": "5b567255-7703-4780-807c-7be8301ae99b",
            "type": "Role"
         },
         {
            "id": "98830695-27a2-44f7-8c18-0c3ebc9698f6",
            "type": "Role"
         },
         {
            "id": "df021288-bdef-4463-88db-98f22de89214",
            "type": "Role"
         }
      ]
   },
   {
      "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
      "resourceAccess": [
         {
            "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
            "type": "Role"
```

```
            }
        ]
    }
],
```


## Target Entra ID

Create an Azure AD App Registration. If you are doing Directory Synchronization AND Workstation Migrations that will become Entra Joined, then you will need all of these API permissions.

### Redirect URI

In the app registration for the Target Entra ID, to generate Bulk Enrollment Tokens (BPRT), to support Entra Join device migrations, the app registration needs to have a Single Page Application redirect URI. The URI should match the URI that you use to administer the PowerSyncPro administration service followed by /redirect

Go to:
Authentication\Platform configurations\Add a platform and choose Single-page application. Add http://localhost:5000/redirect and click configure.

### API permissions

Add the following API permissions.

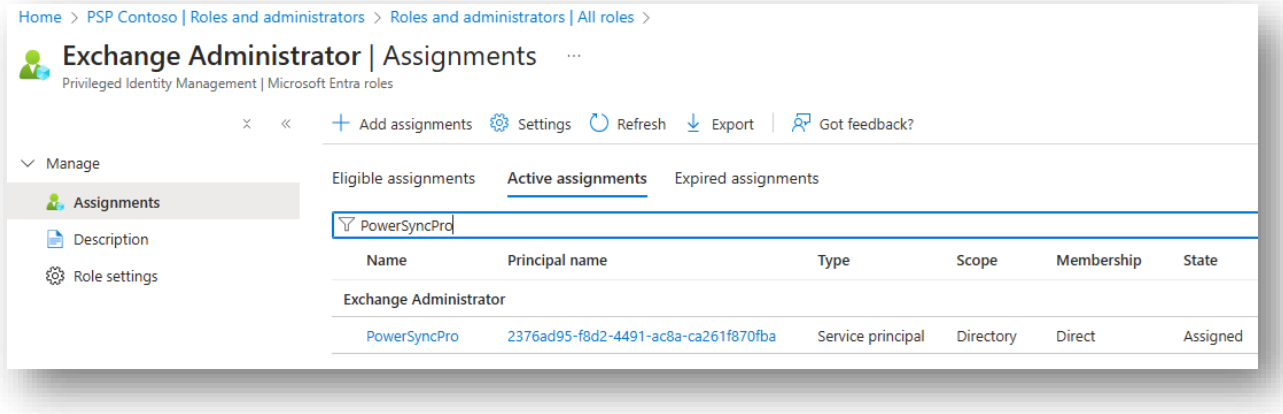
Go to Add a permission, select Microsoft APIs**Microsoft Graph.** Choose **Application permissions (except for Device Registration Service)**

| API / Permissions name | Type | Description |
|---|---|---|
| **Microsoft Graph** | | |
| Directory.Read.All | Application | Read directory data (to get any directory extensions) |
| Domain.Read.All | Application | Read domain data (to get the onmicrosoft.com name) |
| Group.Create | Application | Create groups (to create groups) |
| Group.ReadWrite.All | Application | Read and write all groups (to update/delete groups) |
| GroupMember.ReadWrite.All | Application | Read and write all group memberships (to update group membership) |
| User.Invite.All | Application | Invite guest users to the organization (to create external guests) |
| User.ReadWrite.All | Application | Read and write all users' full profiles (to create/update/delete users) |

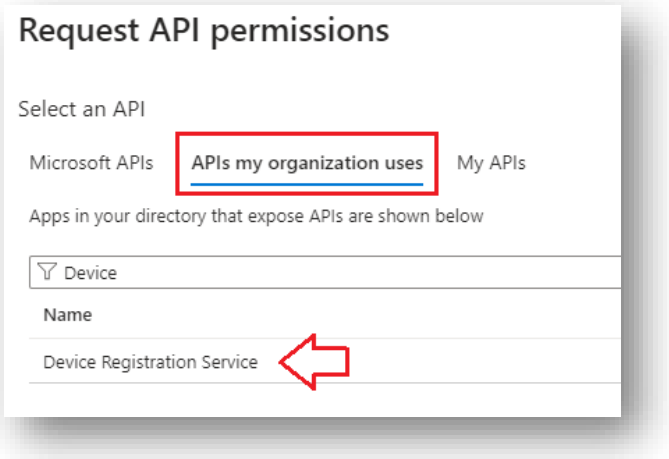
If you will be synchronising Exchange Online to Exchange Online objects, you will also need:

| API / Permissions name | Type | Description |
|---|---|---|
| **Office 365 Exchange Online** | | |
| Exchange.ManageAsApp | Application | Manage Exchange As Application (if importing from Exchange Online is required) |

If you are planning to synchronise Exchange Online Distribution Groups that are not security enabled, then you additionally need to add the App Registration into the appropriate Entra Role Group.




For **Device Registration Service,** this is in APIs my organization uses and is a Delegated permission.



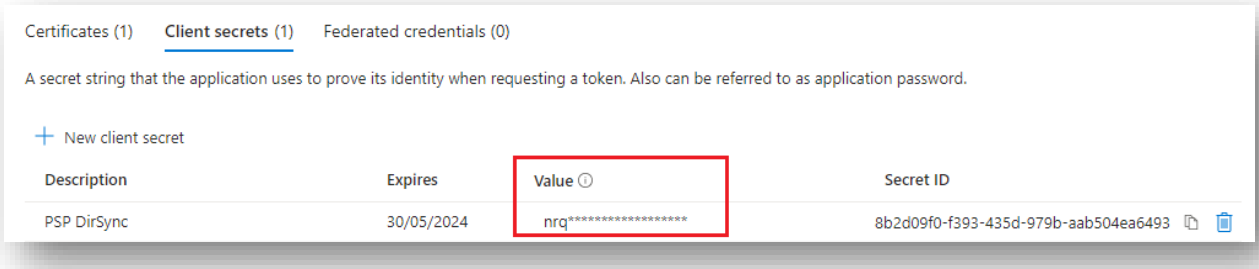

| API / Permissions name | Type | Description |
|---|---|---|
| **Device Registration Service** | | |
| Self_service_device_delete | Delegated | User can delete devices that belong to them |

Client Secret

Generate a Client Secret

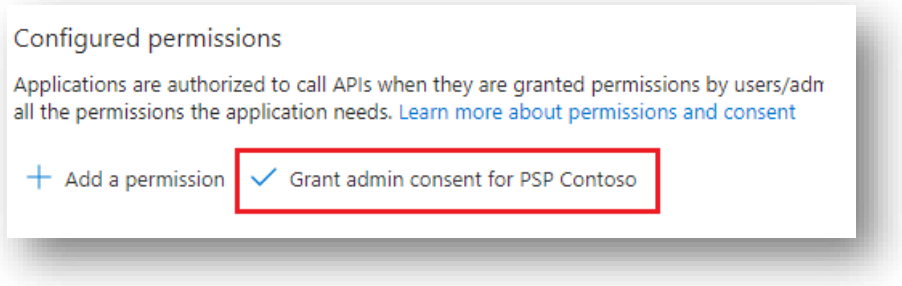
App Secret Value

> Be sure to copy this before you leave this screen as it is **only shown once.**




**Admin Consent**

Remember to Grant admin consent for your tenant.




### Example App Registration Manifest

For ease here is part of a manifest file that can be pasted into the App Registration **"requiredResourceAccess"** section.

```
"requiredResourceAccess": [
    {
        "resourceAppId": "00000003-0000-0000-c000-000000000000",
        "resourceAccess": [
            {
                "id": "7438b122-aefc-4978-80ed-43db9fcc7715",
                "type": "Role"
            },
            {
                "id": "7ab1d382-f21e-4acd-a863-ba3e13f7da61",
                "type": "Role"
            },
            {
                "id": "dbb9058a-0e50-45d7-ae91-66909b5d4664",
                "type": "Role"
            },
            {
                "id": "bf7b1a76-6e77-406b-b258-bf5c7720e98f",
                "type": "Role"
            },
            {
                "id": "62a82d76-70ea-41e2-9197-370581804d09",
                "type": "Role"
            },
            {
                "id": "dbaae8cf-10b5-4b86-a4a1-f871c94c6695",
                "type": "Role"
            },
            {
                "id": "09850681-111b-4a89-9bed-3f2cae46d706",
                "type": "Role"
            },
            {
                "id": "741f803b-c850-494e-b5df-cde7c675a1ca",
                "type": "Role"
            }
        ]
    },
```

```
    {
        "resourceAppId": "01cb2876-7ebd-4aa4-9cc9-d28bd4d359a9",
        "resourceAccess": [
            {
                "id": "086327cd-9afe-4777-8341-b136a1866bb3",
                "type": "Scope"
            }
        ]
    },
    {
        "resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
        "resourceAccess": [
            {
                "id": "dc50a0fb-09a3-484d-be87-e023b12c6440",
                "type": "Role"
            }
        ]
    }
],
```

e.g.

| API / Permissions name | Type | Description | Admin consent required | Status |
|---|---|---|---|---|
| Device Registration Service (1) | | | | |
| self_service_device_delete | Delegated | User can delete devices that belong to them | No | Granted for PSP Contoso |
| Microsoft Graph (7) | | | | |
| Device.Read.All | Application | Read all devices | Yes | Granted for PSP Contoso |
| Domain.Read.All | Application | Read domains | Yes | Granted for PSP Contoso |
| Group.Create | Application | Create groups | Yes | Granted for PSP Contoso |
| Group.ReadWrite.All | Application | Read and write all groups | Yes | Granted for PSP Contoso |
| GroupMember.ReadWrite.All | Application | Read and write all group memberships | Yes | Granted for PSP Contoso |
| User.Invite.All | Application | Invite guest users to the organization | Yes | Granted for PSP Contoso |
| User.ReadWrite.All | Application | Read and write all users' full profiles | Yes | Granted for PSP Contoso |
| Office 365 Exchange Online (1) | | | | |
| Exchange.ManageAsApp | Application | Manage Exchange As Application | Yes | Granted for PSP Contoso |

## Device Migrations ONLY

### SOURCE

If you are not doing Directory Synchronisation and only Device migrations, then you only need the following API Permissions in the source.

| API / Permissions name | Type | Description |
|---|---|---|
| **Microsoft Graph** | | |
| Device.Read.All | Application | Read all devices (if importing devices) |
| Directory.Read.All | Application | Read directory data (if using any directory extensions) |
| Domain.Read.All | Application | Read domain data (to get the onmicrosoft.com name) |
| User.Read.All | Application | Read all users' full profiles (if importing users) |

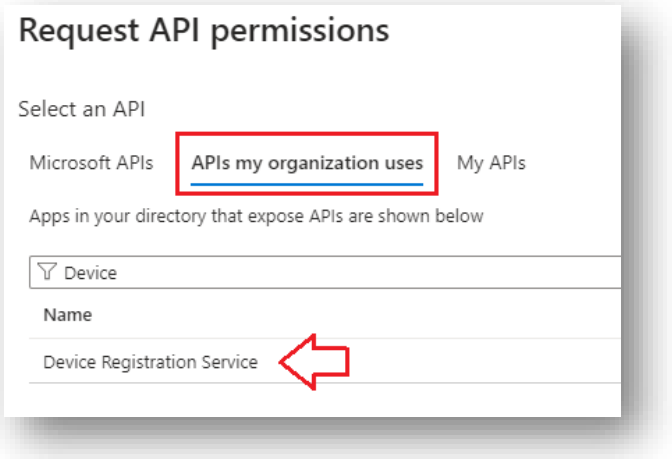
### TARGET

If you are not doing Directory Synchronisation and only Device migrations, then you only need the following API Permissions in the target.

You will still need User.Read.All for your user matching sync profile to create an address translation table.

| API / Permissions name | Type | Description |
|---|---|---|
| **Device Registration Service** | | |
| self_service_device_delete | Delegated | User can delete devices that belong to them |
| **Microsoft Graph** | | |
| User.Read.All | Application | Read all users' full profiles |
| Device.Read.All | Application | Read all devices (if importing devices) |

For **Device Registration Service,** this is in APIs my organization uses and is a Delegated permission.




## Exchange Online Directory Sync

If you are planning to synchronise Exchange Online Distribution Groups that are not security enabled, then you to perform the following steps:

**Exchange Online PowerShell module**

Install the Exchange Online PowerShell module on the PowerSyncPro Server. This cannot be *scoped*.

```
Install-PackageProvider -Name NuGet -Force
Install-Module -Name PowerShellGet -Force
Install-Module -Name "ExchangeOnlineManagement" -Force -AllowClobber
```

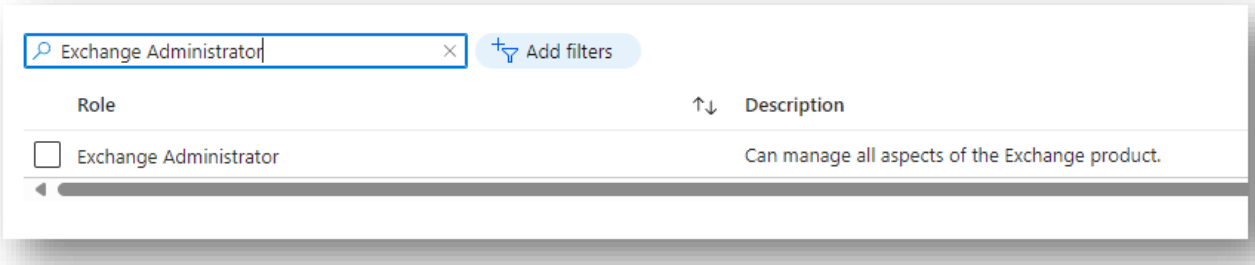
**API Permissions**

Add **Exchange.ManageAsApp** to the API Permissions

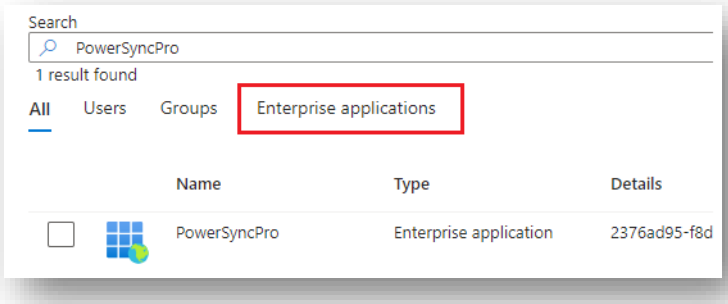
| API / Permissions name | Type | Description |
|---|---|---|
| **Office 365 Exchange Online** | | |
| Exchange.ManageAsApp | Application | Manage Exchange As Application (if importing from Exchange Online is required) |

**Exchange Administrator Role**

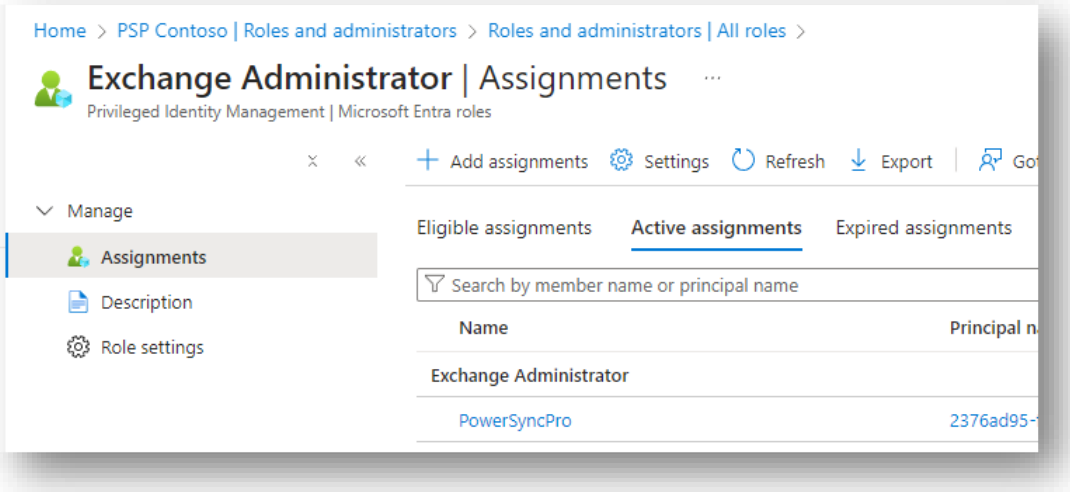
And add the App Registration into the appropriate Entra Role Group. Go to Entra Roles and administrators and click on the **Exchange Administrator** Role




- Click Add assignment
- Select Member
- In Users start typing the name of your App Registration, this will light up the hidden choice of “Enterprise Applications”

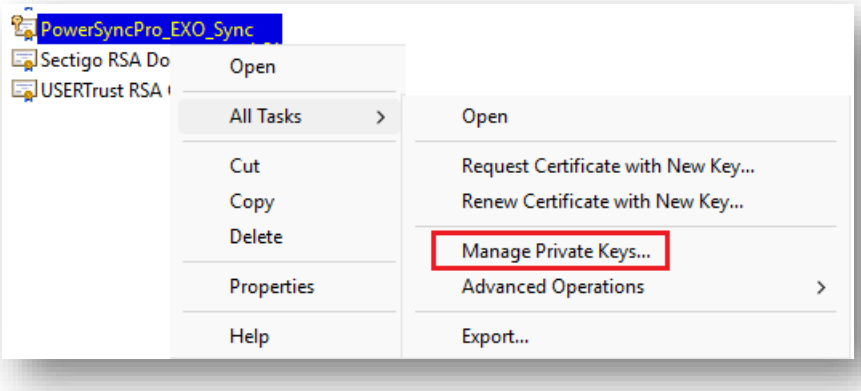


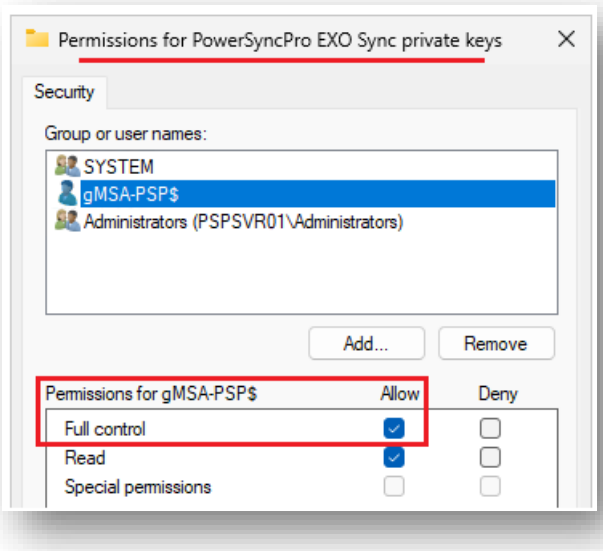

Select the name of your App Registration, Enter a justification and finish.




**Certificate**

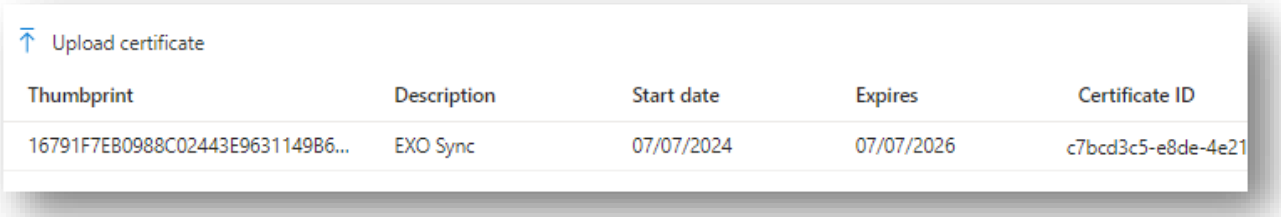
You will also need to create a certificate on the PSP Server and grant the PSP Service account full control to the private keys.





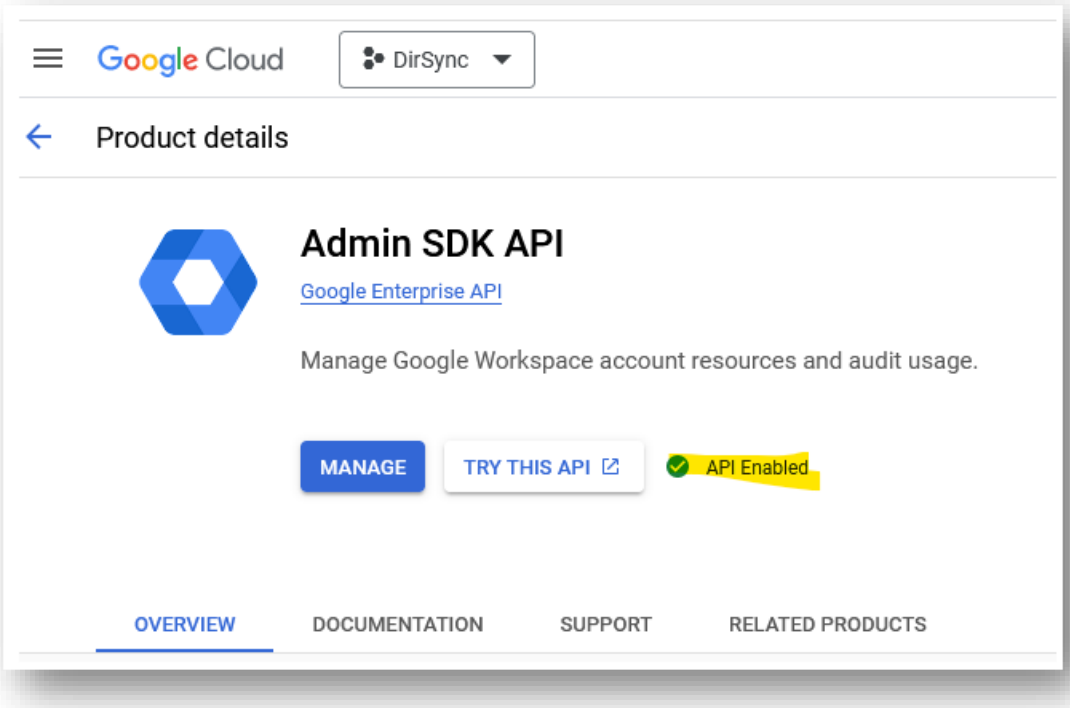

Then export the certificate and upload that *.cer file to your Entra App registration:

- Go to your App Registration, Certificates & secrets
- Upload a Certificate




## Google Workspace

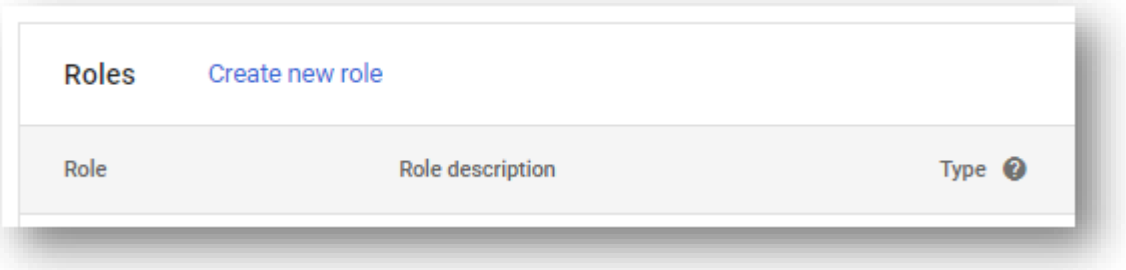
1. Create new project for the organisation in Google Cloud – this requires Organization Admin Role https://developers.google.com/workspace/guides/create-project
2. Enable the Admin SDK Library for the project https://developers.google.com/workspace/guides/enable-apis



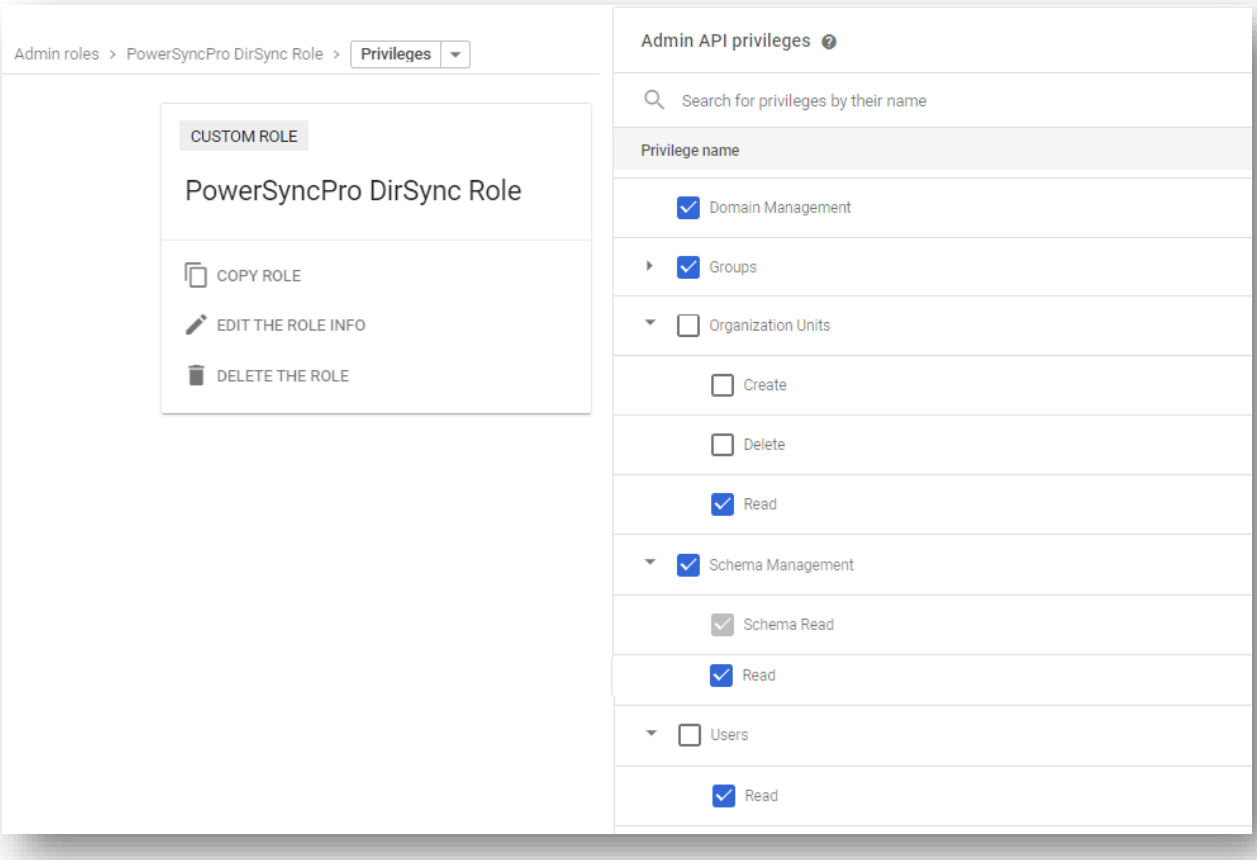

3. Create a service account. Follow: https://developers.google.com/workspace/guides/create-credentials#service-account
4. Create JSON credentials file for the service account - https://developers.google.com/workspace/guides/create-credentials#create_credentials_for_a_service_account

   **NOTE:** When the json file is created it is a one-time creation so you must keep a copy of it safe
5. For assigning permissions, you can use some of the system made ones like "Groups Admin" and "User Management" a role will have to be made in Google Workspace: https://admin.google.com/u/1/ac/roles

## Admin Roles




If you want more granular control, you can create a custom one. If you wish to use custom schemas you will need to add the permission to read it with a new role by **configuring Schema Management**. **Domain settings** may be required so PSP can read the domain name.




Permissions required for import:

- Organisational units > Read
- Groups (if importing groups)
- Schema Management -> Schema Read (if wanting to import custom schema attributes for users)
- Users > Read (if importing users)

# Appendix 1

## Group Managed Service Account

### Configuring a Group Managed Service Account gMSA

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/service-accounts-group-managed

If you have not used a gMSA before, then you may need to run these commands in advance.

```
Install-WindowsFeature RSAT-AD-PowerShell
Import-Module ActiveDirectory
Add-KDSRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

```
New-ADServiceAccount -Name gMSA-PSP -DNSHostname 'gMSA-PSP.yourdomain.local' -
ManagedPasswordIntervalInDays 30 -PrincipalsAllowedToRetrieveManagedPassword
"CN=PSPServer,CN=Computers,DC=yourdomain,DC=local" -Enabled $True -PassThru
```

**Confirm Creation with:**

```
Get-ADServiceAccount -Filter * | where-object {$_.ObjectClass -eq "msDS-
GroupManagedServiceAccount"}
```

or

```
Get-ADServiceAccount gMSA-PSP -Properties * | FL Name, DNSHostName, SamAccountName,
PrincipalsAllowedToRetrieveManagedPassword, ObjectCategory
```

If you are intending to use gMSA in DR mode then you should create an AD Security Group, e.g. “PowerSyncProFarm” add your two servers as members and then run:

```
Set-ADServiceAccount gMSA-PSP -PrincipalsAllowedToRetrieveManagedPassword
"CN=PowerSyncProFarm,OU=Servers,DC=contoso,DC=local"
```

### Test that the PSP Server(s) will operate with a gMSA

**On the PSP Server(s)**

```
Test-ADServiceAccount gMSA-PSP
```