integriti
INTEGRATED SOLUTIONS

INTEGRITI ENTRA ID (AZURE ACTIVE DIRECTORY) PLUGIN

INNER RANGE recommends that all Inner Range systems be installed & maintained by FACTORY CERTIFIED TECHNICIANS.

For a list of Accredited Dealers in your area refer to the Inner Range Website.
http://www.innerrange.com

ASIAL MEMBER
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED
GOLD MEMBER

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

Certified System
Quality
ISO 9001

Table of Contents

Description

Note: This Integration was previously the "Azure AD Integration", but was updated to "Entra ID" after Microsoft renamed that feature. The cloud service containing Entra ID is still referred to as "Azure", so that name has been kept in the documentation where appropriate.

The Entra ID Active Directory Integration synchronises Users and user changes from Entra ID into Integriti. Users that are added to or changed in Entra ID will be imported to Integriti on a schedule configured in the Integrated Device, including Full and Partial Imports.

Full Imports will update all Users/Properties, add new Users and, if configured, will also remove deleted Users from Integriti that were not included in the Full Import. The Full Import updates can be limited by selecting Groups from the Entra ID Organisation that Users must be a member of to be imported and updates.

Partial Imports pick up changes to Users that were imported by the last Full Import.

Capabilities	Ver	Y/N	New
Can Import Users from Entra ID	23	✓	
Can Export Users to Entra ID		×	
Filter User Imports on Groups in Entra ID	23	✓	
Full/Partial Import configuration	23	✓	
Advanced Capabilities			
Can target specific sites/partitions in Integriti	23	✓	

Integriti Entra ID Plugin

Required Integriti Version License

The Integriti Entra ID Integration requires an Integriti Business or Corporate/Infiniti v24 license or higher to be present on the product key running the integration.

Minimum Installed Integriti Version

The Integriti Entra ID Integration is only compatible with an installation of Integriti Business/Corporate or Infiniti that is v24.0 or higher.

Licensing Requirements

The Integriti Entra ID integration requires no additional licenses, it is included with Business or Corporate versions of Integriti.

Tested Against

The Integriti Entra ID Integration v1.2 was built and tested against Azure Core v1.2500.22.33004 connecting to Entra ID Active Directory as of May 2024.

Configuration

Installation

Close all instances of the Integriti software suite on the PC to install the integration on, including stopping all running Integriti services (if installing on the Integriti server).

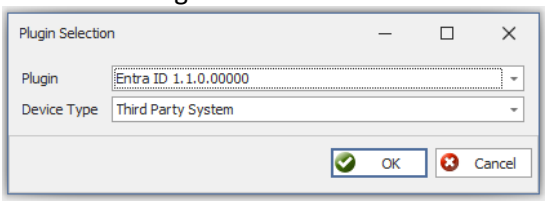
Download and run the Entra ID Integration installer on all Integriti servers first, before running on all client workstations that will be interacting with the integration; including updating the integration's configuration and invoking commands.

After the installation has completed, remember to start all of the services that were stopped prior to running the installation.

If reverting to an earlier version of an Integriti Integration, ensure that the currently installed version of the integration is uninstalled prior to installing the earlier version.

Enrolment

1. In Integriti System Designer, select 'New Integrated Device' from the System tab.
2. Select the integration to enrol from the list that appears and press Ok.



NOTE: The same version of each integration must be installed on both the Integriti Integration Server and on the Integriti Client Workstation that is enrolling the integration for it to be enrolled.

If the desired integration does not appear in the drop-down list, ensure that both the 32-bit and 64-bit (for supported OS's) Integriti Integration Servers are running.

3. In the editor window that appears, give the newly created device a Name and optionally enter some Notes describing the device.

4. **Persisted Connection Run Mode** - Select the preferred Persisted Connection Run Mode. This is necessary for features such as event and camera state monitoring. This typically does not affect the ability to view video or invoke commands on this device and its child devices.

   The following options are available for the Persisted Connection Run Mode:
   Automatically Maintain Connection on Any Single Server – This is the recommended option if a persisted connection is to be enabled and will ensure that there is always one Integriti Integration Server connected to the 3rd party system, provided at least one Integriti Integration Server is available.
   In high availability systems, if the Integriti Integration Server that this device's persisted connection is running on goes offline, the persisted connection will automatically start up again on another running server.
   Maintain Connection on the Specified Server – This option will run the persisted connection to the 3rd party system only on the specified server and no others. This is the best option to use if only one of the available Integration Servers is able to connect to the 3rd party system. If the specified server goes offline, the integration will lose its connection to the 3rd party system until the specified integration server comes back online.
   Simultaneously Maintain Connection on All Servers – This option will establish a persisted connection to the 3rd party system on every Integriti Integration Server at the same time. This can result in the most simultaneous connections to the 3rd party system, and can result in duplicate Review Records being logged for events received from the 3rd party system.
   Disabled – Disables the persisted connection to the 3rd party system for this device. This option should only be used if event and state monitoring are not required from this device and will result in one fewer connections being made to the 3rd party system at all times This may be useful if only a limited number of simultaneous connections are permitted by the 3rd party system.
5. **Connection Configuration -** On the 'Device Properties' tab, under 'Connection Configuration', configure the integration specific properties, including details on connecting to the Entra ID system. For more details on how to configure integration specific properties, please refer to the "Device Attributes".
6. Select the Save button to save the newly created device.

Save and close the editor window for the new device and, if enabled, a persisted connection will automatically begin to the Entra ID system and start listening for incoming requests.

Entra ID Specific Setup

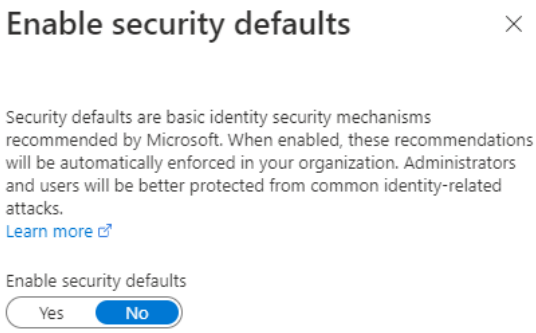
In terms of setting up Entra ID to be ready for the Integration to connect to, there are two things that need to be set up and configured before proceeding with setting up the Integration.

The first is disabling the Microsoft Security Defaults so that Username and Password logins for the Integration can be enabled without requiring Multi-factor Authentication. The second is setting up an App Registration to allow the Integration access to the Directory as well as defining the permissions it has for the Directory.

Security Defaults

When the Microsoft Security Defaults are active, logging into Entra ID using Username and Password is not possible, which is required for the Integration to be able to work without User input and synchronise User changes from the Directory on a schedule.

To disable these defaults, from the Home menu, click 'Microsoft Entra ID', then on the left under 'Manage', click 'Properties'. From there, scroll to the bottom of the page and click 'Manage Security Defaults' under 'Access management for Azure resources'. Then ensure 'Enable security defaults' is set to No.



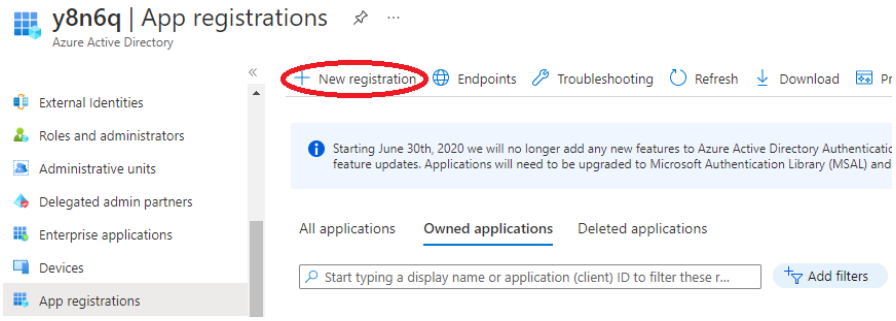
Note: This can remove some security mechanisms from the organisation (eg. Requirement for MFA on all Users), however these defaults are not recommended when the organisation is using Conditional Access rules, Azure's security configuration rules that are far more granular and powerful. If you are using Conditional Access, you may already have this disabled as the two cannot be active at the same time.

For more information regarding the Security Defaults, you can follow the 'Learn more' link in the above screenshot. It is highly recommended that you read this to understand the measures that will be removed by changing this setting.

App Registration

App Registrations in Entra ID are used to manage a third party's connection and access rights to the Entra ID's API and is required for the Integration to be able to connect to a specific organisation.

To create an App Registration for the Integration, from the Home page, click 'Microsoft Entra ID', then click 'App Registrations' on the left under the 'Manage' category. From here you can add a Registration as seen below.



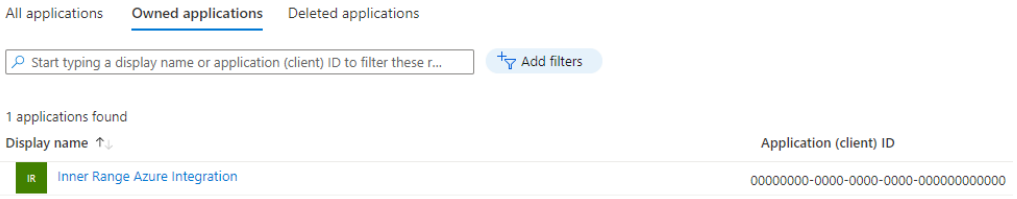
Both the name of the Registration and the 'Supported account types' will be configured to create the Registration. Take note of the 'Supported account types' selected, as this needs to be reflected in the Integration's 'Login Account Type' setting once set up:

- This organisation directory only → Users From Entra ID Tenant
- Any organisation directory → Work and School Microsoft Accounts
- Any organisation directory or personal account → Work, School and Personal Microsoft Accounts
- Personal Microsoft Accounts only → Personal Microsoft Account

For the simplest configuration, it is recommended to use 'This organisation directory only' and inviting external accounts into the organisation with access to this App Registration of using that account is required (logging in with external accounts using other settings can cause issues logging in due to their own log-in requirements like Multi-factor Authentication).

Note: Only 'Users From Entra ID Tenant' will allow for users in the Entra ID Tenancy to be used by the Integration to log in without being associated with an external Microsoft Account.

Once the Application is registered, it should appear in the 'Owned applications tab' in the screenshot below:



Once created you can define the API Permissions for Microsoft.Graph. To add these permissions, click 'Add a permission' then search for "Microsoft Graph" or the name of your App Registration, then 'Delegated permissions'. Select the desired permission in the list of permissions, then 'Add Permission'.

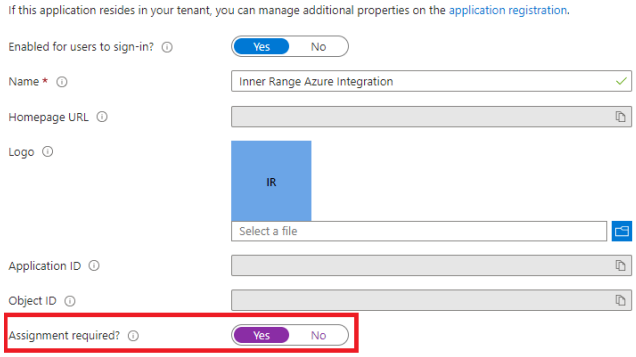
The following permissions are required for the Integration to utilise the App Registration:

- User.Read
- User.Read.All
- Group.Read
- Group.Read.All
- GroupMember.Read

Granting Permission to App/Enterprise Registration

By default, an App Registration allows any User to log in using it to use the functions it was permitted in the previous step. However, we can require permissions for access to the App Registration.

Access to this registration can be restricted by modifying the associated Enterprise Registration; from the Home page, click 'Microsoft Entra ID', then click on 'Enterprise Applications', then the associated Registration (shares the name and Application ID of the App Registration). From there, click on 'Properties', then turn on 'Assignment required?' as below:



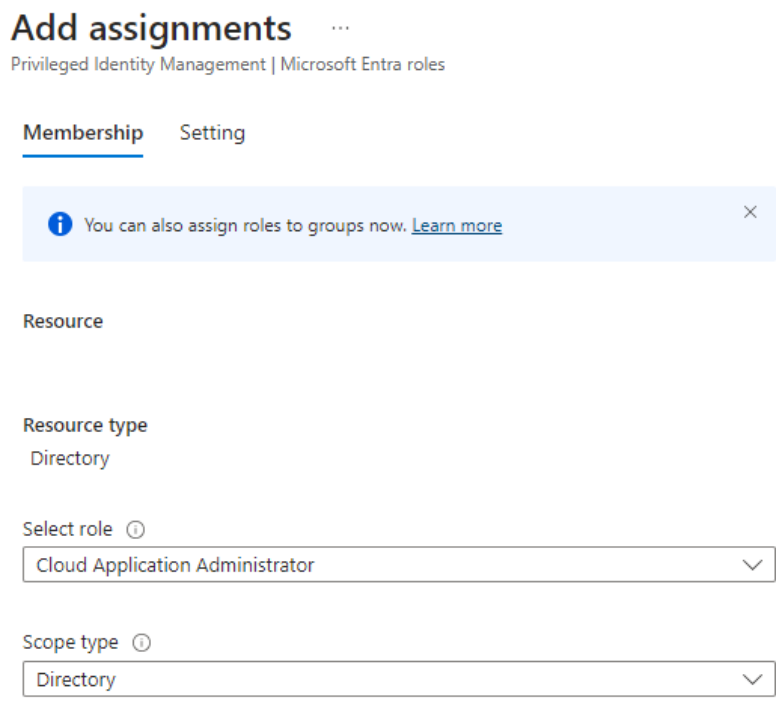
This will then require any User account attempting to use the Registration via the Integration to have the following:

- A Role from the list in 'Roles and Administrators'
- Added to the Users in 'Users and Groups'

Any User can be given this permission, including the Administrator account for the tenancy. A new account can also be created to be the only account having access to the Registration to avoid giving existing accounts for other purposes do not have access to it.

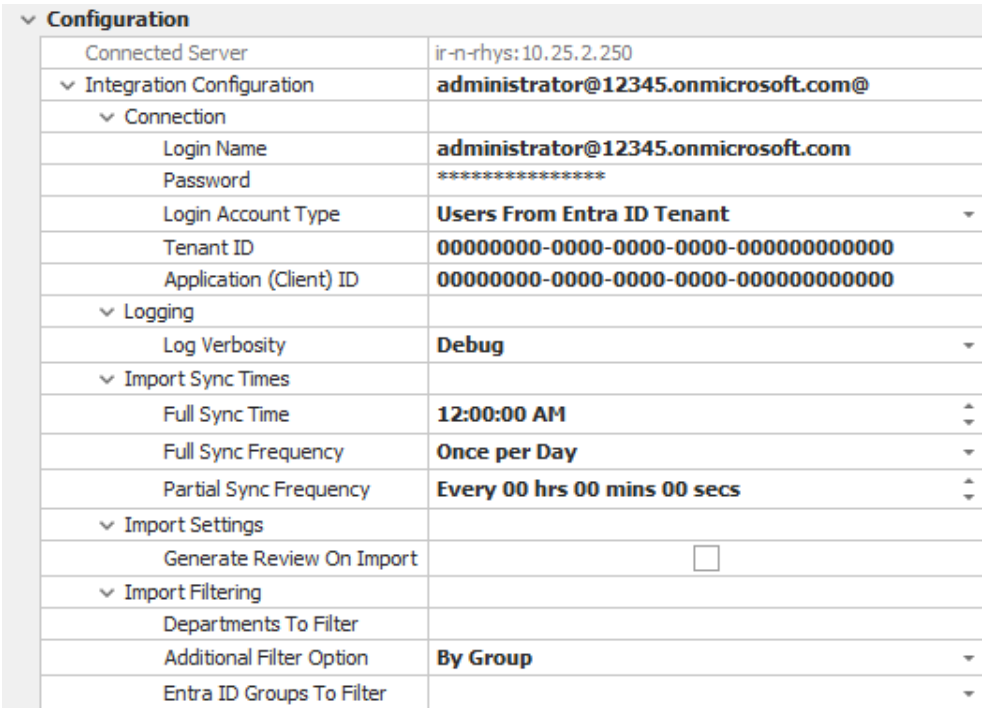
To give the desired User access to the App Registration, first add the User to the Enterprise Registration by clicking on ‘Users or Groups’ while still editing it, then clicking ‘Add user/group’, then selecting them.

This User will also need to be assigned a Role that appears in the Enterprise Registration. By default a Role called ‘Cloud Application Administrator’ should be in this list, which is perfectly suited for this User. To assign it to them, from the Home page, click ‘Microsoft Entra ID’, then click ‘Users’ and find the User in question. Then click ‘Assigned Roles’, then ‘Add assignments’, selecting the Role you would like to assign with the scope of ‘Directory’ as shown below:



Device Attributes

Note: To ensure configuring the Entity Import settings is as simple as possible, once the 'Connection' section has been configured, use 'Refresh Device' before configuring anything else.



Connection

- *Login Name* – The login Name or email address of the account logging in to the Entra ID Organisation.
- *Password* – The password used to log in with the account specified in Login Name to the Entra ID Organisation.
- *Login Account Type* – Select the type of Account used to give the Integration access to the Entra ID Organisation.
    - Work, School or Personal Microsoft accounts to log in.
    - Work and School Microsoft accounts to log in.
    - Personal Microsoft accounts to log in only.
    - Users from the specified Entra ID Organisation. Tenant ID must be configured as well.
- *Tenant ID* – The ID of the Tenant in which an account must exist to log in using the Integration
- *Application (Client) ID* **–** The ID of the App Registration in the Entra ID that will give the Integration access to read Users from Entra ID.

Import Sync Times

- *Full Sync Time* – Select the time of day for full synchronisations to occur. This will add and remove users as well as synchronising changes.
- *Full Sync Frequency* – Choose how often a full sync should happen.
- *Partial Sync Frequency* – Select a frequency for partial synchronisation to occur. This will only synchronise changes made to users in the Active Directory that will appear in the Entra ID's User Changes and will not re-synchronise the Navigation Group (if enabled).

Import Settings

- *Generate Review on Import* – If set, Review will be generated whenever an Import is performed.

Import Filtering

- *Departments To Filter* – Enter one or more possible 'Department' property values that an Entra User must have for the User to be imported.
  Each entry should be separated by a semi-colon. Eg: Retail;Management;Tech Support
  If left blank, 'Department' will not be applied as a filter.
- *Additional Filter Option* – Select an additional Filter applied to User Imports from Entra. Note that at least one filtering option (Department, Office Location or Groups) must contain a value/selection to Import Users.
- *Office Locations To Filter* – Enter one or more possible 'Office Location' property values that an Entra User must have for the User to be imported.
  Each entry should be separated by a semi-colon. Eg:
  Sydney;Melbourne,Victoria;Mount Waverly
  If left blank, 'Office Location' will not be applied as a filter.
- *Entra ID Groups To Filter* – Select the Groups to which Users must belong to be imported by the Integration. This list is populated by using 'Refresh Device'.
  If left blank, 'Groups' will not be applied as a filter.

Full Import Configuration

Full Imports from Entra ID can take some time to complete, especially for Organisations with a large number of Users. As such, it is recommended that Full Imports are scheduled for a time of day that they will not impact other day-to-day functions.

Note: Full Imports are also performed when the Integrated Device is reset, for example by saving changed settings.

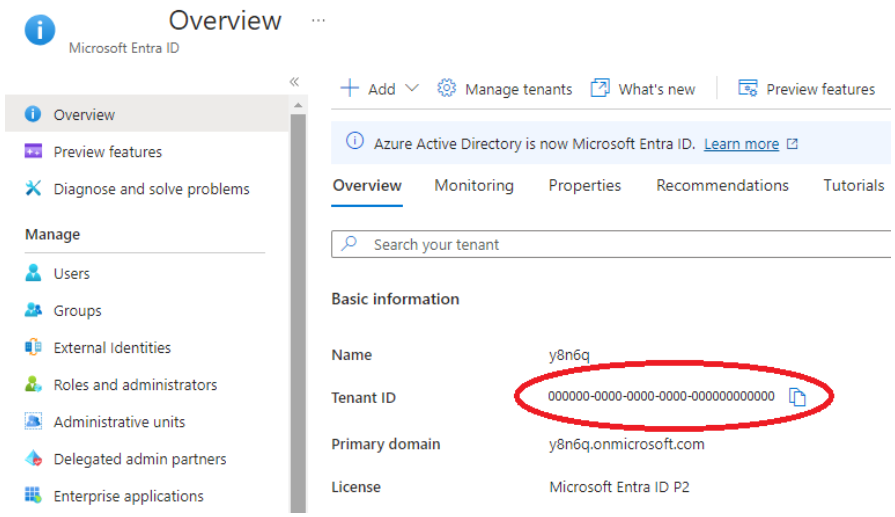
Where to find Entra ID specific Information

Several Device properties require collecting information from places in Entra ID. This section details where they can be found, as it can be confusing where some information is in Entra ID.

Tenant ID

The Tenant ID is essentially the ID for the Active Directory of the system and is required when restricting the accounts that are logging into Entra ID to the ones that are in the Tenancy in question.

This can be found in the 'Overview' of the Active Directory. From Azure's Home, click 'Microsoft Entra ID', it should then be visible in the 'Overview'. (If this does not appear, click 'Overview' on the left of the screen to view it)



The Tenant ID is a Guid as seen in the above screenshot, which can be copied using the button to the right of the value.

Login Name

The Login Name used in the Integration will be the login of a Microsoft account able to access the Entra ID organisation. When using the 'Specific Tenant' option, the Login Name will need to be sourced from the User in Entra ID.

The Login Name will be the 'User Principal Name' of the User that will be used, which is typically the full First Name of the User, the first letter of the Second Name, then '@{Primary Domain}, which can be seen in the previous screenshot.
Eg. 'JohnC@12345.onmicrosoft.com'

The administrator account is 'Administrator@12345.onmicrosoft.com' by default.

The User's Principal Name can be changed, however, so to confirm the Principal Name, click the 'User' button under 'Manage' on the left side of the screen when you have navigated to 'Overview' as described above. In the list of Users, the Principal Name will be visible.

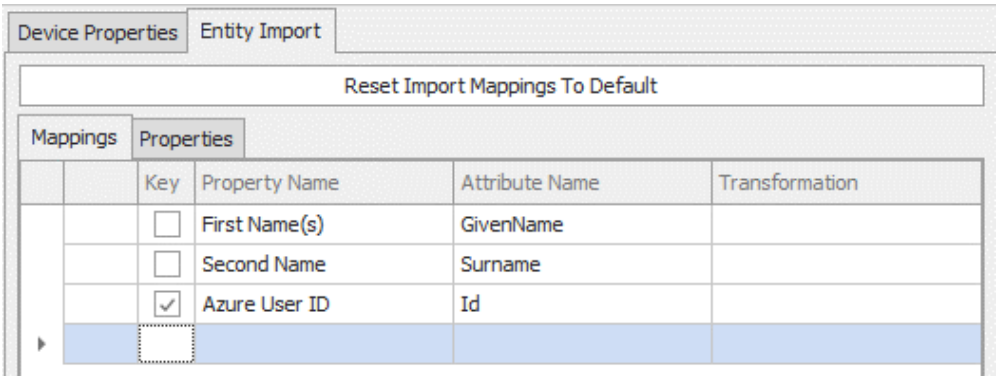
Application (Client) ID

This ID is used to specify the App Registration that is configured to allow the Integration to read Users from the AD. This is set up as part of the 'Entra ID Specific Setup' section of this document.

The ID of the App Registration can be found in the overview of the App Registration, as seen in the 'Entra ID Specific Setup'.

Import Settings

The settings for mapping the Properties of a User in Entra ID to Users in Integriti are found under the 'Entity Import' tab in the Integrated Device's Editor. Under this tab are two more tabs, 'Mappings' and 'Properties' as seen below.



The 'Mappings' editor is the same as those used to edit Import mappings for CSV and the Active Directory Communication Handler; 'Property Name' refers to the Integriti User property name and 'Attribute Name' refers to the Entra ID User property. A mapping can also be made a Key field, indicating it uniquely identifies a User, by checking the tickbox in the 'Key' column.

The 'Reset Import Mappings To Default' button can also be used to reset the Mappings in the 'Mappings' tab if needed, returning the Mappings to the Integration's default.

Note: The default mappings include a Mapping for the Entra ID User property 'Id' that maps to a Custom Field. If the Custom Field's Name as seen above does not appear in the 'Property Name' for that mapping, ensure 'Refresh Device' has been performed and search for the name in the 'Property Name' dropdown box or use the reset feature to return it to default.

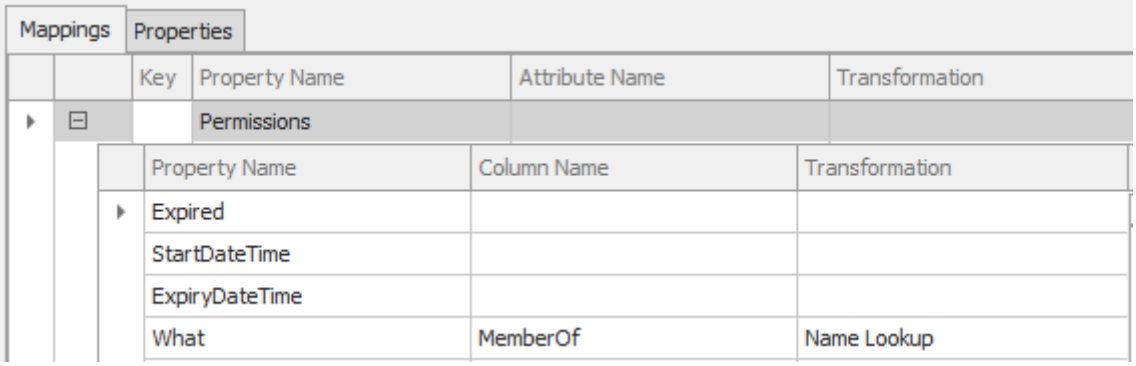
Note: The 'PhotoData' Attribute in Entra ID will only be synchronised during a Full sync.

Using the 'MemberOf' Property for Permissions

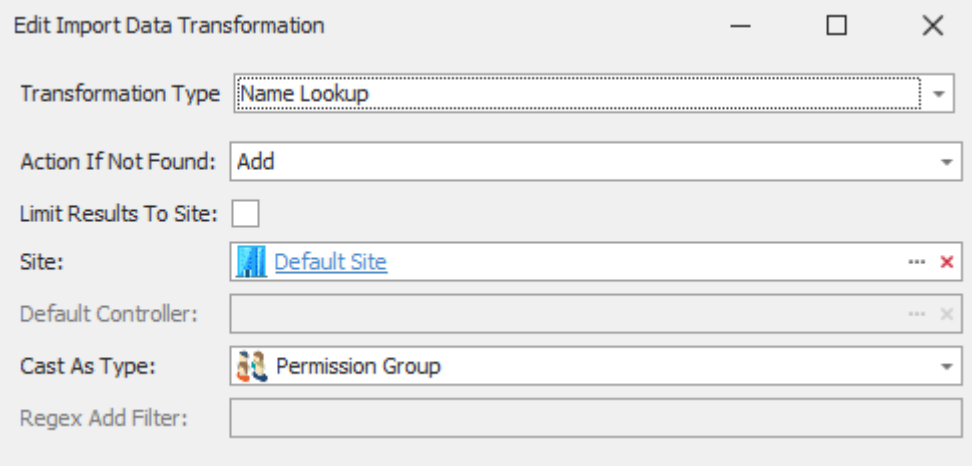
In addition to filtering User's by their Group membership in Entra, they can also be used to generate permissions for imported Users and Permission Groups for the Groups of which they are members.

This is achieved by mapping the 'MemberOf' property to a child property of the 'Permissions property, as well as applying a 'Name Lookup' transform to said mapping.

In the 'Entity Import' tab, under 'Mappings', configure a 'Permissions' mapping by mapping 'What' with 'MemberOf', as seen below:



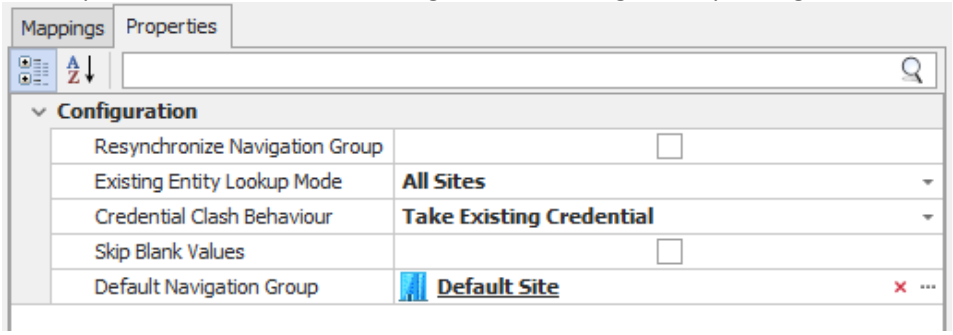
Once this is configured, click the 'Transformation' column for this mapping entry, and click the '…' button to open the Data Transform editor. In this, select the 'Name Lookup' Transformation Type, then configure the rest as seen below:



This will mean that for each incoming 'MemberOf' Group name, a User will be assigned a Permission for an existing Permission Group matched on name, or a new Permission Group if no matches are found, avoiding the need to manually add Permission Groups for each Group needed.

Note: It is recommended after initial configurations and synchronisation that the 'Action If Not Found' setting in the 'Name Lookup' transform be changed to 'Skip' to avoid adding any unwanted Permission Groups, resulting in many unused Permission Groups if allowed to add them over a long period of time.

In the 'Properties' tab, additional settings for controlling the Import logic can be found:



- *Resynchronize Navigation Group* – Select to delete all users in the selected navigation group that aren't in the Active Directory on each full synchronisation.
- *Existing Entity Lookup Mode* – Specify where to look for matching existing entities when importing an Entity. This determines whether the changes made by the import should be restricted to only a specified site or can effect entity in other sites in the system.
- *Credential Clash Behaviour* – Select the intended behaviour for when a Credential to be saved already exists and results in a Credential Clash.
- *Skip Blank Values* – Select to prevent changes being made to a property if it has been emptied. This prevents values being overwritten by blank values.
- *Default Navigation Group* – Select the site to synchronise Users to/from. Customise existing Entity lookup settings through 'Existing Entity Lookup Mode' to specify which Sites to lookup entities in. NOTE: Only newly created entities will be created into this site – When an existing entity is found in another Site, it will remain in that site unless an explicit mapping is added to the Import Mappings.

Troubleshooting

'Your app has been throttled' exceptions in log	This exception is caused by many consecutive attempts from the Integration to get an Authentication Token from Azure. It can be triggered because of a small Partial Sync Frequency and encountering an authentication issue. This can be resolved by disabling the Integration for 2 minutes and restarting the Integration. This issue can be avoided by setting a larger Partial Sync Frequency to not overload Azure when the Integration encounters an error.
'Invalid Authentication Token' exceptions in log	This exception is caused by incorrect authentication details. Generally, this is caused by incorrect username and/or password or inadequate permissions.
A User in a Group not selected in Import Settings was imported	It has been observed that Entra ID forcibly adds Users to the Organisation's default Group (usually named after the organisation) if a User is not in them. If you have included a Group like this in the Import Settings and do not wish to synchronise all Users, it is recommended to not use this group in 'Groups To Filter By'.
User Cards not being generated on Import using 'Take Existing' Credential Clash settings	When a User's Card from an Import matches another Card, 'Take Existing' will give the User that Card but only if that Card is active and not being used by another User. As a result, Users imported can be left with no Card if that Card exists and is used by another User (possibly in the same import) or if the Card is not Active.
The Integration is not starting and showing a message saying 'No Filter Options were selected'	At least one of the filter options in the Integrated Device must be configured for the Integration to start up and Import Users. Ensure that there is at least one entry or selection made in the Departments/Office Locations/Groups to Filter by properties in the Integrated Device, then save to restart the Integration.