aura

hello@weareaura.com

Aura Connect New Sync Guide & FAQ

Date: November 2024

Contents

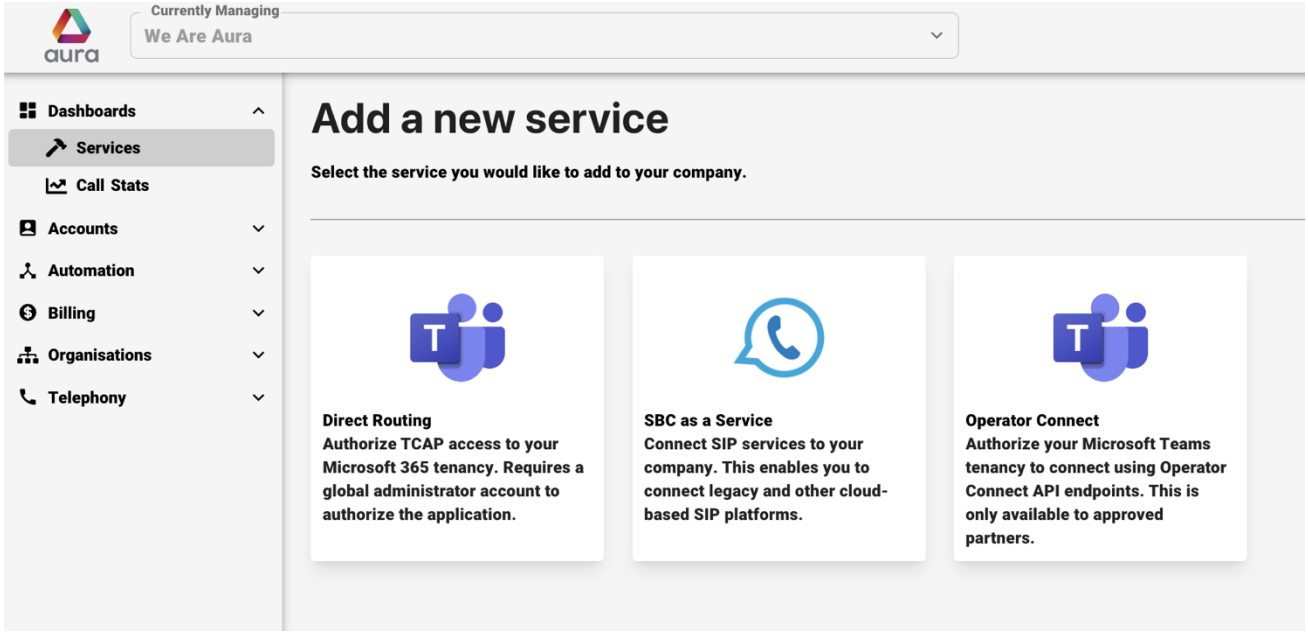
New Customer Aura Connect User Synchronisation

Aura Connect provides Customers and our Partners with the ability to manage both Telephone Number routing and assignment. This document details the options available and technical requirements to support these features.

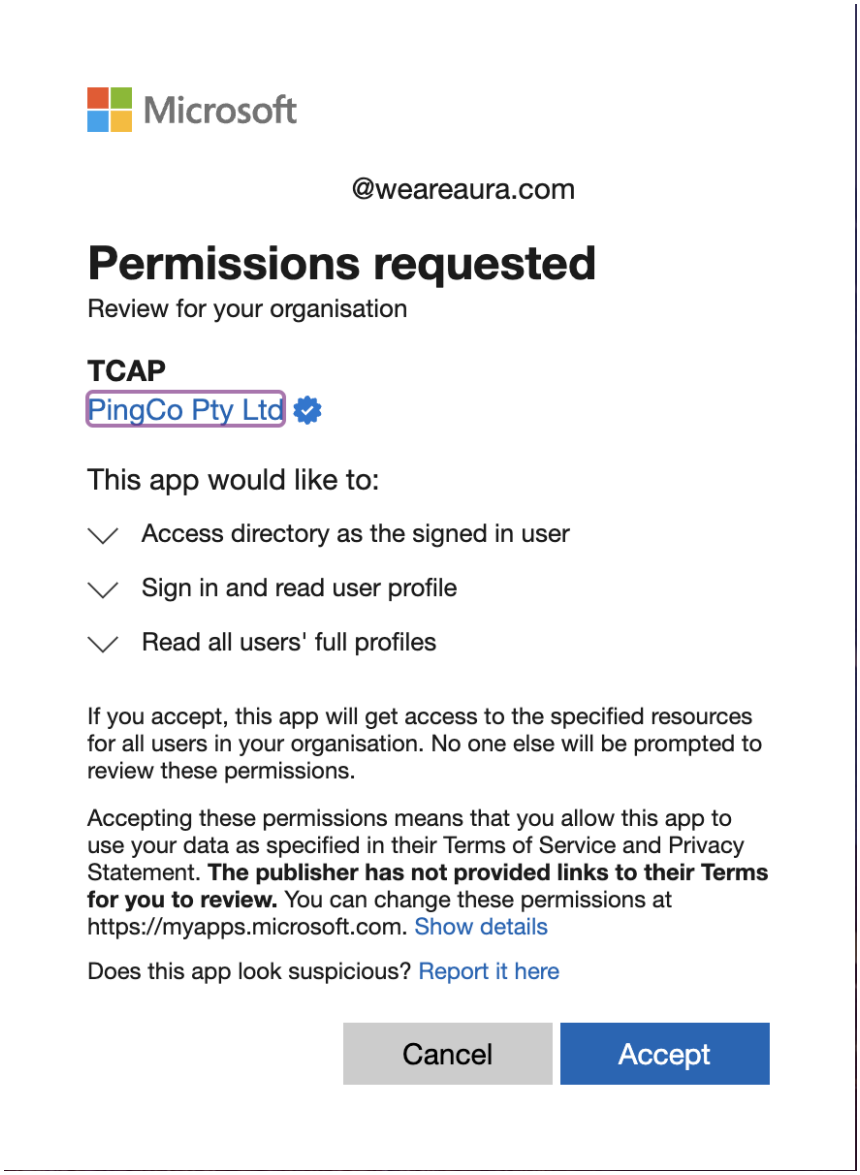
Requirements can, and do, differ between Teams Calling delivery options, Direct Routing and Operator Connect.

The Synchronization Service

When either Operator Connect or Direct Routing services are added within Aura Connect, the Synchronization Service (Sync) is enabled by default for most of our customers.



Enabling Sync requires a user with Global Administrator permissions within the Microsoft 365 tenant to grant permissions for Aura Connect to pair with the tenant. Upon doing so, the admin agrees to grant the Aura Connect TCAP application the necessary permissions as displayed.



The function of Sync varies between Direct Routing and Operator Connect. See Appendix A for further detail.

By default the Sync application requests the permissions shown in the table below. For ease of deployment, management and future feature enablement of Aura Connect it is recommended to utilize the TCAP hosted application and default permissions.

Mandatory Sync App Permissions

Permission	Claim Value
Access Directory as the signed in user	Directory.AccessAsUser.All
Sign in and read user profile	User.Read
Read all users' full profiles	User.Read.All

Custom Applications – Supporting GCC High

To meet the unique and evolving requirements of the United States Department of Defense, as well as contractors holding or processing DoD controlled unclassified information (CUI) or subject to International Traffic in Arms Regulations (ITAR), Microsoft offers GCC High and DoD environments.

This provides a segregated, compliant Microsoft 365 service. However, with this comes restrictions on what services can run within and connect to the Teams tenant.

As the standard Aura Connect Sync application cannot operate from within GCC High, customers wishing to utilize TCAP within a GCC High tenant must create the app directly and work with Aura to configure the service utilizing a customer specific application instance.

Following creation of a custom application, the Application ID and Client Secret must be shared with Aura for configuration of services. Upon expiry of a Client Secret, a new one must be generated and shared for update.

Please see Appendix B for further detail on creation and configuration of a custom application.

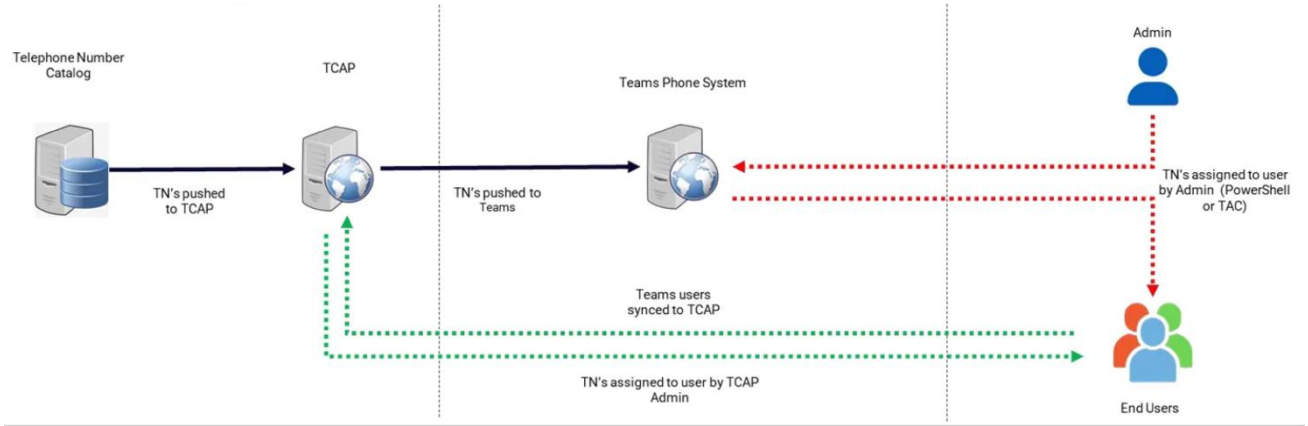
Operating Without Sync

In Appendix A, it can be observed that Direct Routing has a higher dependency on Sync to be enabled in order to configure the core Direct Routing services. In the event a customer has any objections to the permissions required for User Sync, it may be preferable to deploy Operator Connect as Sync is not required for Setup and Activation.

In this configuration, Sync would never be enabled for a customer and Aura Connect would be utilized solely for Number Management. Assignment of numbers would then be managed directly within Teams Admin Center or PowerShell, requiring a Teams Administrator to manually manage such tasks.

For ease of deployment, management and future feature enablement of Aura Connect it is recommended to utilize Sync for full Aura Connect TCAP functionality and service management. However, the service supports customers in their preferred service management configuration.

The following provides an overview of how services are managed with and without Sync.



Both can be delivered and managed by:

Number Management – No customer permissions required. Always accessed via TCAP

- *Note - Direct Routing requires Sync permissions for setup*

PLUS ONE OF THE FOLLOWING:

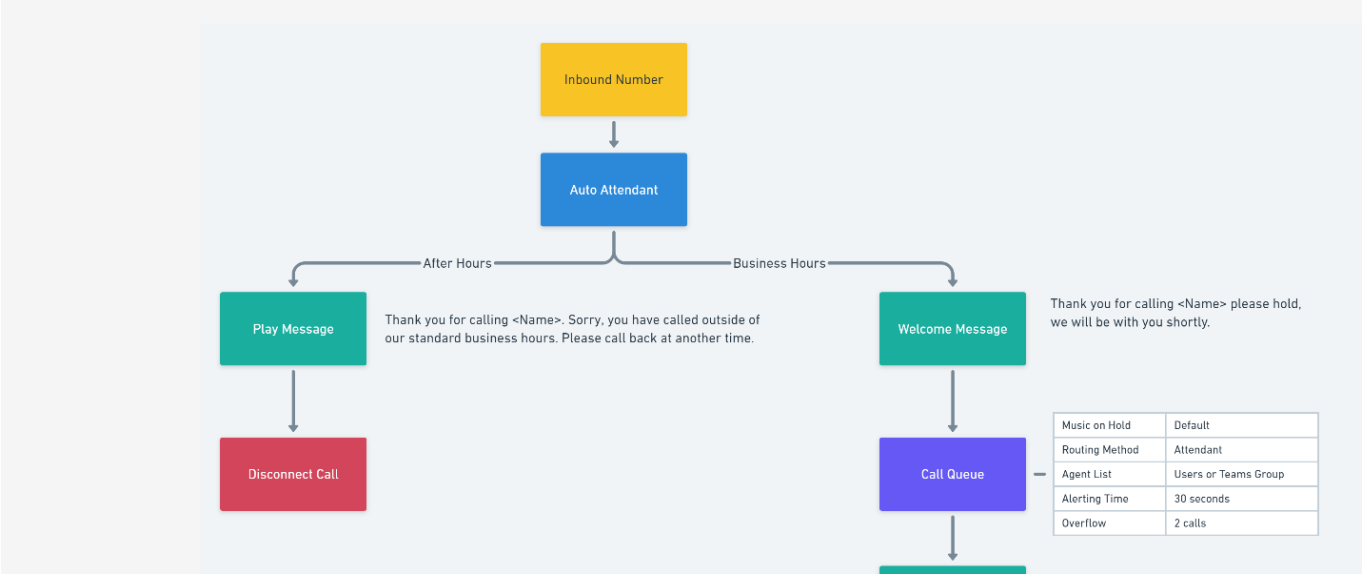
User Management WITH Sync – Requires Graph API permission and service account with MFA exclusions. TCAP can be used to manage users.

OR

User Management WITHOUT Sync - Customer owns all user management via PowerShell or Teams Admin Centre

Resource Group Creation

Aura Connect provides functionality to automatically create **Teams Call Queues** and **Auto Attendants** and all underlying configuration via the Resource Account Builder tool.



As of August 2024, Microsoft only support creation of Resource Accounts under the scope of Global or User Admins. Subsequently, to achieve this, TCAP creates a Service Account with User Admin permissions within the tenant. This is only utilized for the purpose of the Resource Account Builder and shall be retired immediately upon Microsoft making available the functionality to create resource accounts without said permissions.

When enabled, a secure service account with Teams Admin permissions is created within the Microsoft 365 Tenant, i.e. tcap.teams@tenant.onmicrosoft.com. This account is platform-accessible only, the password is hashed and not readable. The list of attributes that the account can read/write are listed in the Permissions Requested screen when a tenant is paired with TCAP.

Due to the manner in which the service account is utilized during its process, Multifactor Authentication and other Conditional Access Policies must be disabled on the account. The service cannot answer an MFA challenge when completing its automated tasks. If you need further assistance on disabling MFA there is a guide available or contact our customer success team.

The complex password for the user account is not accessible or readable to users. This is stored encrypted and hashed, with the hash key not within either the TCAP code base, or database. This is accessed only from specific server roles during the automation process and never accessed directly by any human interface.

Overview for Existing Customers

A New User Synchronisation methodology was implemented by Aura Connect on Sep 21st. The following provides answers to questions which may arise from the customer community as a result.

What is Sync used for in Teams?

Integration	With Sync	Without Sync
Service Configuration - Tenant Association - Domain Validation - Voice Policies - Dial Plans	✓	✓ OC Only
Number Management - Routing - Usage Types - Release	✓	✓ OC Only
User Management - Read User List from Teams - Assign/Unassign Numbers	✓	✗
Resource Account Management - Read List from Teams - Assign/Unassign Numbers	✓	✗
Resource Account Builder - Create Resource Accounts - Create CQ/AA logic	✓	✗
Billing - Read active Users/RSG - NOT applicable to active numbers	✓	✗

What has changed?

Aura implementing changes to our user sync services, including initiating the removal of the tcap.teams Service Account requirement, reducing permissions required for the app, and following Microsoft's best practices for authentication.

Why?

The changes focused on providing solutions for multiple elements:

1. To address customer security concerns
2. Simplify the setup and support process
3. **Prepare for mandatory MFA enforcement by Microsoft.**

Specifically with regards to MFA, had Aura not adapted to Microsoft new requirements, it would have rendered all sync processes unavailable. Please refer to Microsoft documentation pertaining to this announcement:

Mandatory Microsoft Entra multifactor authentication (MFA) - Microsoft Entra ID | Microsoft Learn

Is this more secure?

Yes. The new authentication method utilised by Aura Connect for Sync follows Microsoft best practices for automation of such processes.

In addition, this allows customers to

1. No longer require Conditional Access exemptions on the Service Account
2. No longer require MFA exemptions on the Service Account
3. No longer require Password Policy exemptions on the Service Account
4. Prepare for full removal of tcap.teams Service Account

When was this change communicated?

Aura issued Partner and Customer communications on September 11th 2024, advising of the pending update to the sync process.

Are Admin roles in my tenant still required

While the role of the tcap.teams Service account is now greatly reduced, and indeed not required at all for the majority of functionality, the automation processes still requires admin access to the tenant. As part of the New Sync deployment, these permissions were moved to the TCAP Enterprise Application

This is divided between

- Teams Admin

Teams Admin is required for all service management, including

- Direct Routing management and configuration
- User Management
- Resource Account Management

- User Admin

User Admin is required for future state Resource Account Management. Currently this may be possible via Teams Admin, however Microsoft themselves are changing this requirement. Please refer to Microsoft communications on this topic:

Upcoming changes for creating and managing Teams Phone resource accounts - Microsoft Community Hub

Why do we still see the TCAP.TEAMS Service Account?

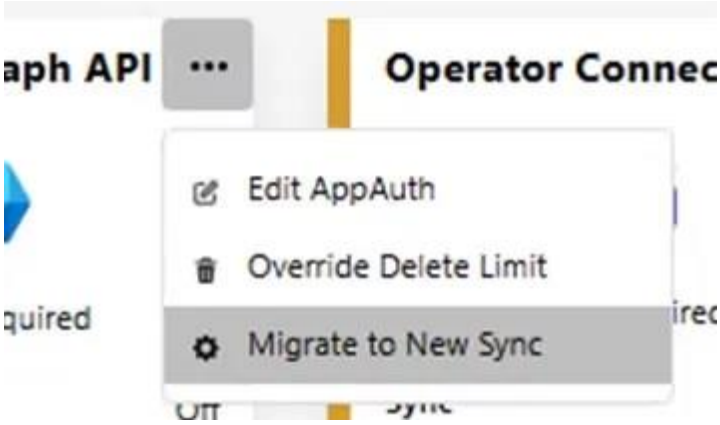
The tcap.teams Service Account is still required for creating resource accounts, but this dependency will be removed as soon as Microsoft supports the new model for this functionality. No other functionality utilises the service account.

If a customer removes/blocks Service account access, this shall only impact the ability to create new resource accounts via Aura Connect and report back an error specific to this. These errors do not contribute to App Auth Failure counts and will not impact calling based on error failure counts.

Do Partners/Customers need to do anything?

Customers have already been migrated to the new sync model automatically and will be synchronising under this model already. This has already yielded significantly positive results in that previous sync failures due to resource account failures also automatically resolved.

A customer can further choose to migrate to their own application for sync. This is via a simple one click process on their service card.



What happens if a customer deletes/blocks access to the app?

Deleting or blocking the app will degrade the sync service, potentially disabling calling features until access is granted again.

If a customer causes a service impacting change by blocking or deleting, then they must resync to resume calling services.

To restore functional access to a failed sync, a Global Admin on the customer side must Grant Access via the service card.

My app shows degraded

This status indicates a sync issue, which can often be resolved by Grant Access/Migrate via the Service card.

It is expected that following the deployment of New Sync, all services currently degraded due to Service Account failures should now be resolved. However in the event customers applied other manual intervention prior to deployment, such as:

- Deleting the TCAP Enterprise Application
- Removing Permissions on the Application

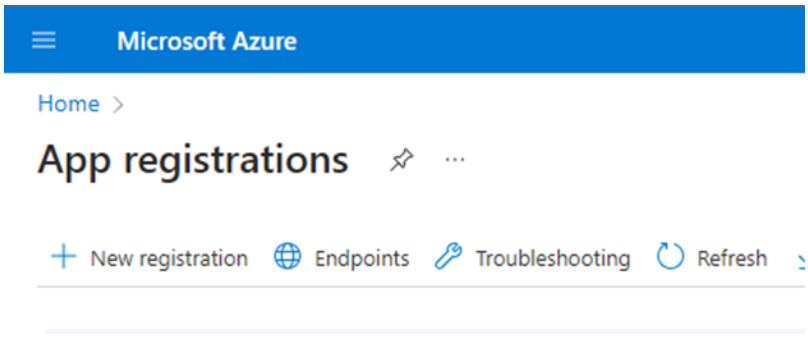
Then these will not auto recover and would still require a Global Admin on the tenant to provide access. During this time calling services will be disabled.

Appendix A – Supported Functionality With/Without Sync

Feature	With Sync	Without Sync
Service Configuration & Activation		
FQDN creation of SBCs within customers tenant	☑ Direct Routing Only	☒
TCAP DNS Update	☑ Direct Routing Only	☒
Validate Domains	☑ Direct Routing Only	☒
Activate Domains	☑ Direct Routing Only	☒
Creation of Dial Plans	☑ Direct Routing Only	☒
Creation of Voice Routes	☑ Direct Routing Only	☒
Number Management		
Assign trunk	☑	☑
Caller ID	☑	☑
Usage type	☑ Operator Connect Only	☑ Operator Connect Only
Upload numbers to Teams Admin Center	☑ Operator Connect Only	☑ Operator Connect Only
User Management		
Read Teams users	☑	☒
Assign numbers	☑	☒
Resource Account Management		
Create resource accounts	☑	☒
Assign templates	☑	☒
Assign numbers	☑	☒

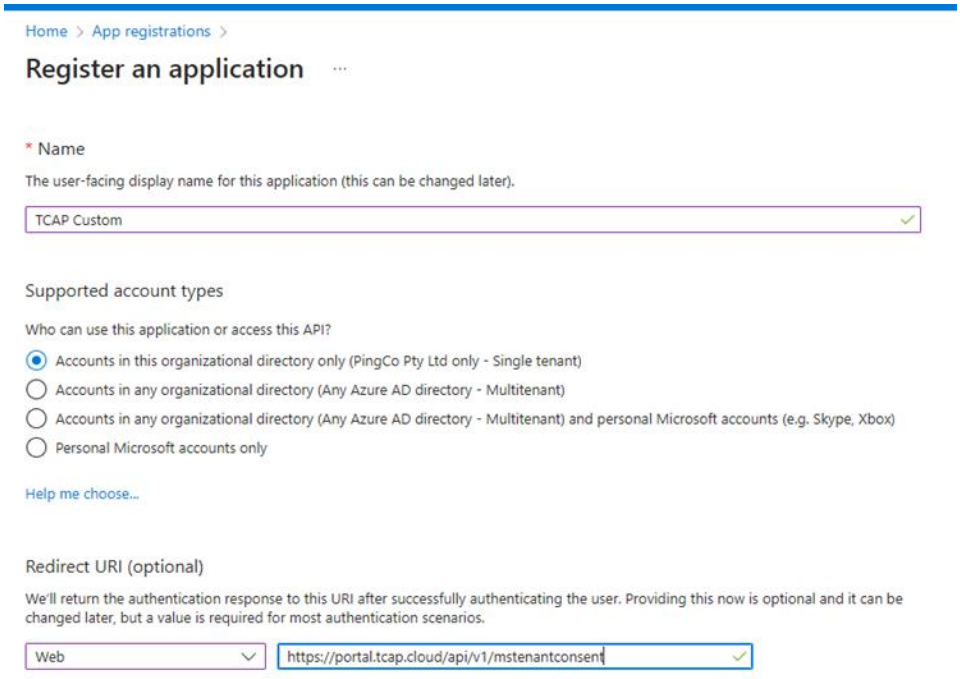
Appendix B – Creating a Custom Application (GCC High Only)

- Log into https://portal.azure.com as a Global Administrator
- Open App Registrations and select New Registration

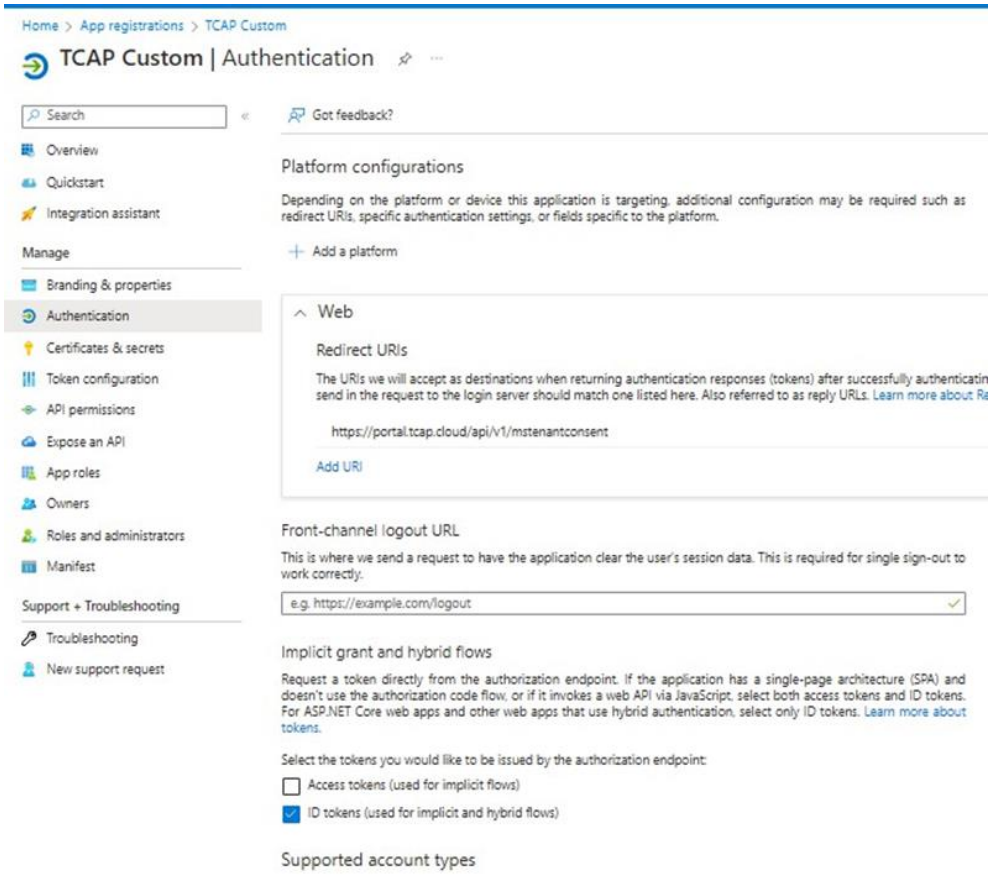


- Fill in the following values
    - Name – Aura Connect TCAP Custom
    - Redirect URL - [https://portal.tcap.cloud/api/v1/mstenantconsent.](https://portal.tcap.cloud/api/v1/mstenantconsent)[https://portal.tcap.cloud/api/v1/mstenantconsent)](https://portal.tcap.cloud/api/v1/mstenantconsent)

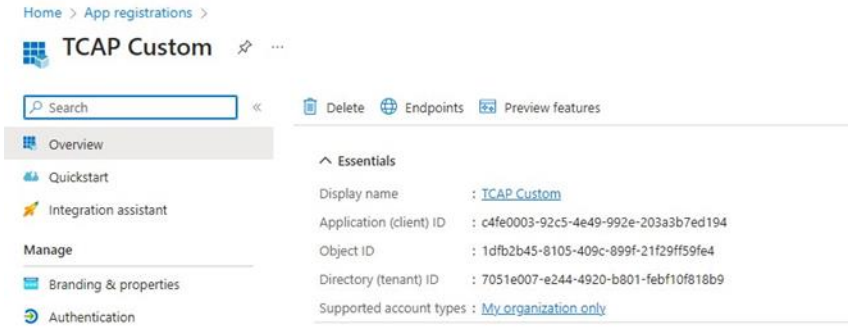
NOTE: Do not change/customize the domain for the URL. This should remain portal.tcap.cloud even on custom applications.



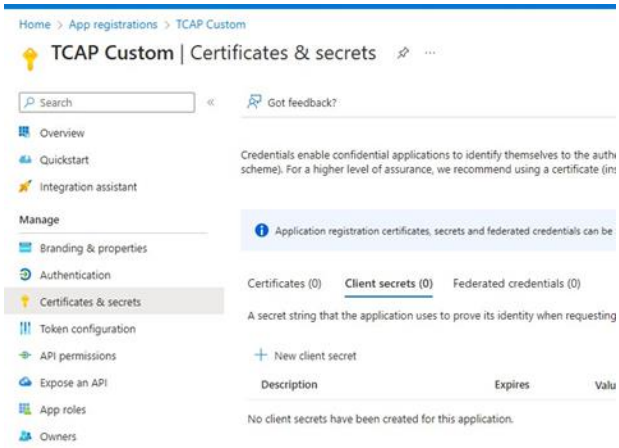
- Under Authentication, Check ID Tokens



- Copy the Application (client) ID value and store for future reference

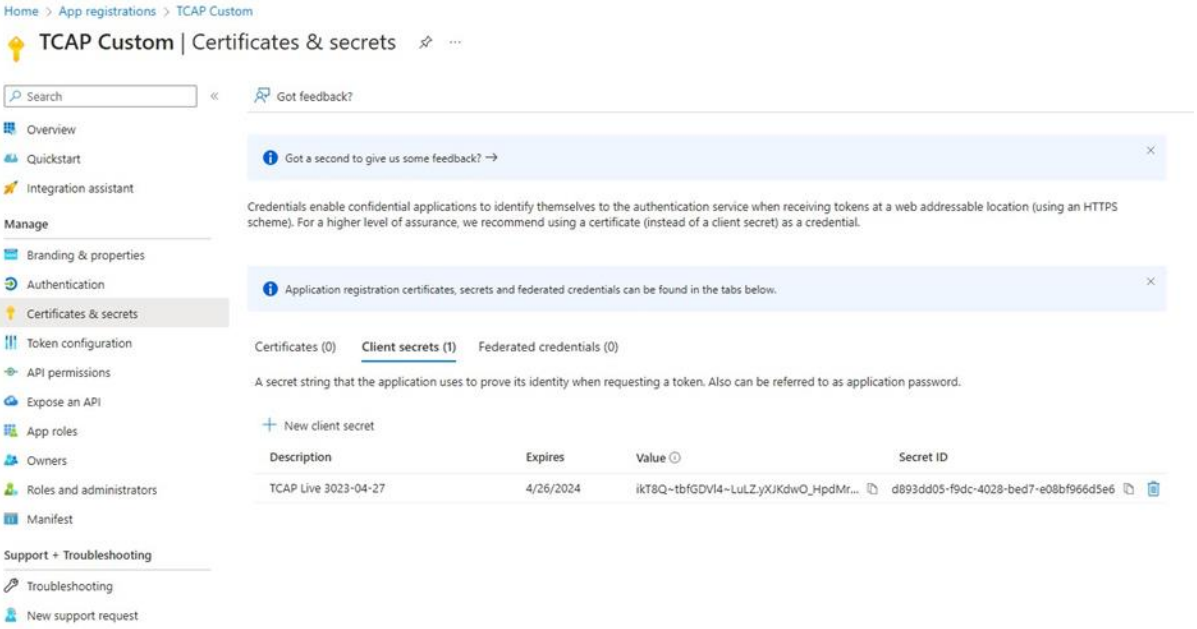


- Certificates & secrets, Create a new Client Secret (36 months preferred)

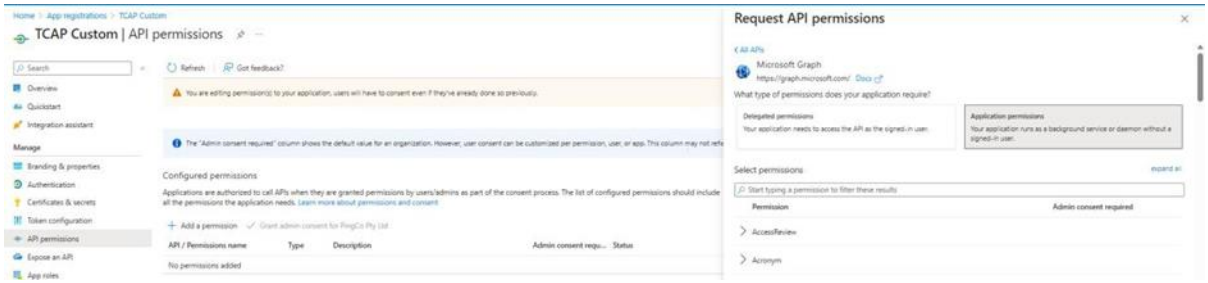


- Copy Secret ID value and store for future reference:

NOTE: If you do not copy this value here, there is no way to access it again later. You will need to delete the secret and generate a new one.



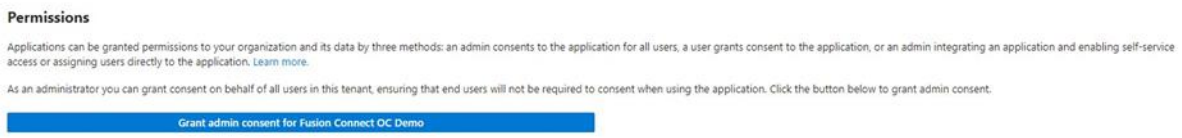
- Under API Permissions, select ‘Add a Permission’, Select ‘Microsoft Graph’ and select ‘Application Permissions’.



- Add the following permissions:

Permission	Claim Value
Read the members of all teams	TeamMember.Read.All
Read and write all users' full profiles	User.ReadWrite.All
Read and write domains	Domain.ReadWrite.All
Read all call records	CallRecords.Read.All
Read role management data for all RBAC providers	RoleManagement.Read.All
Read PSTN and direct routing call log data	CallRecord-PstnCalls.Read.All
Read and write all group memberships	GroupMember.ReadWrite.All
Read all usage reports	Reports.Read.All

- After adding permissions click on 'Grant admin consent for [Company Name]' and continue (requires a global admin login)



- Select Branding & Properties and add MPN ID and optional branding
- Securely provide the previously captured Application ID and Client Secret to Aura for service configuration.