LocoDELEGATIONS: Microsoft Entra ID Integration Guide

Group-based configuration for council IT administrators

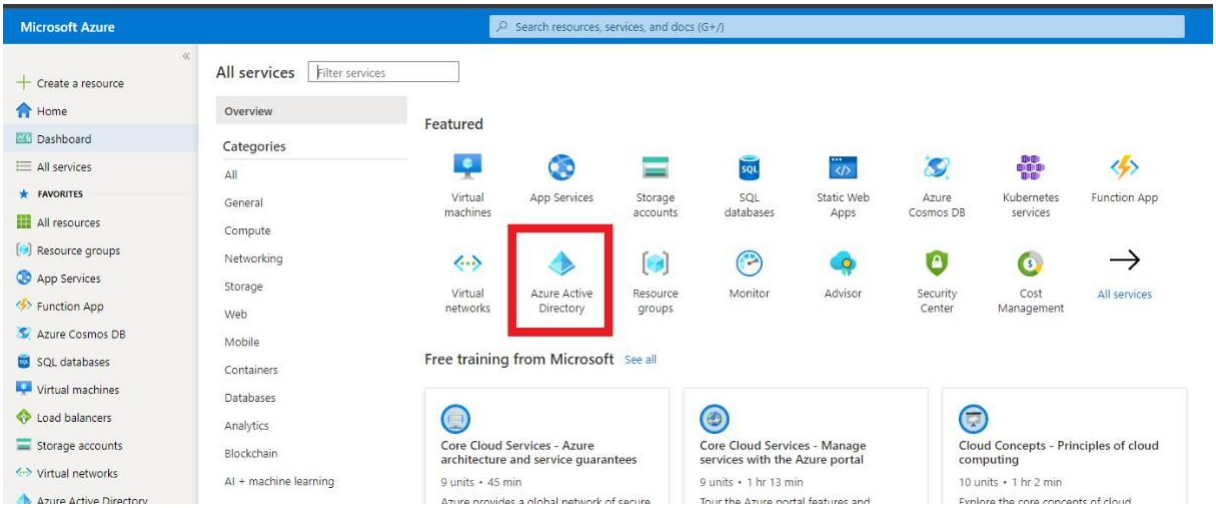
Updated August 2026

This guide explains how a council IT administrator can configure optional Microsoft Entra ID single sign-on for LocoDELEGATIONS. Record the identifiers requested throughout the process in a secure working document. Coordinate the final connection and secure transfer of the required values with LocoSOFT.

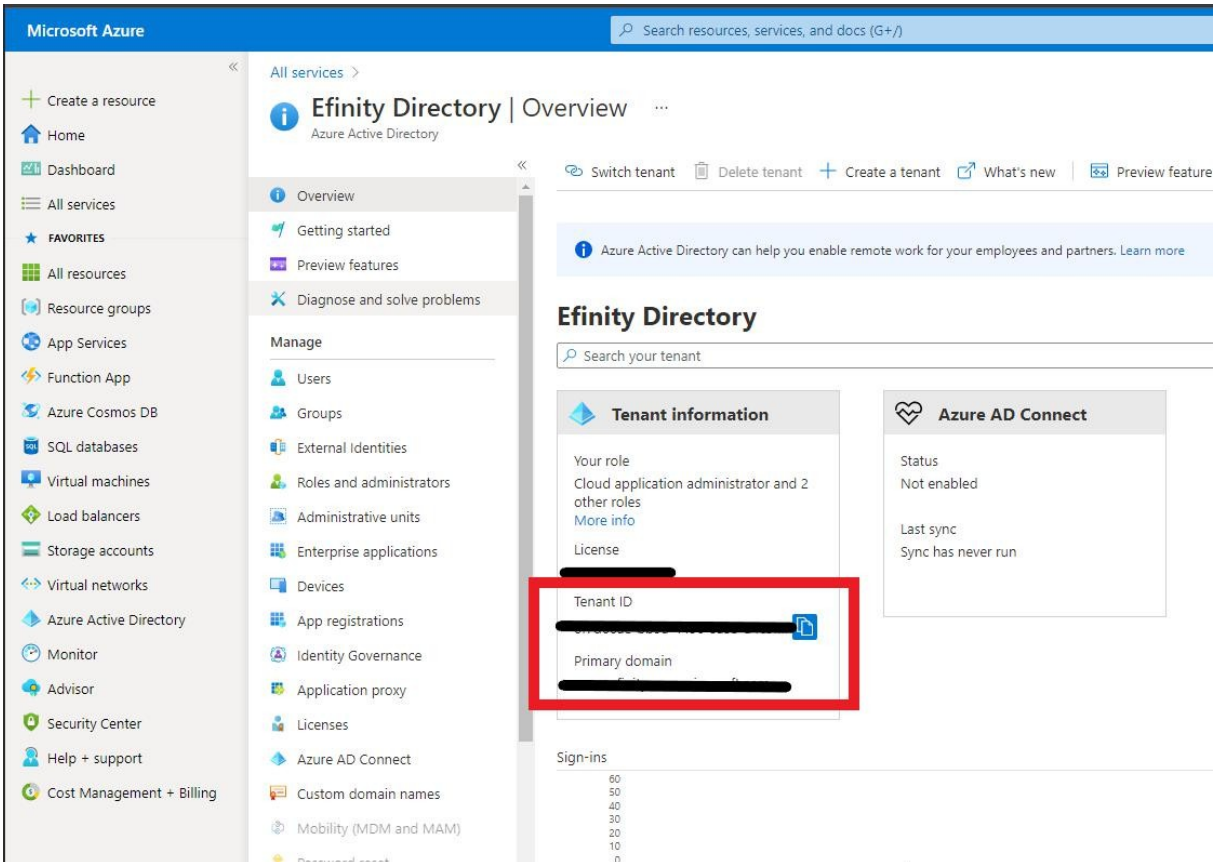
Important: the current configuration uses Microsoft Entra security groups. LocoDELEGATIONS references each group by its Object ID (GUID), not its display name.

Setup steps

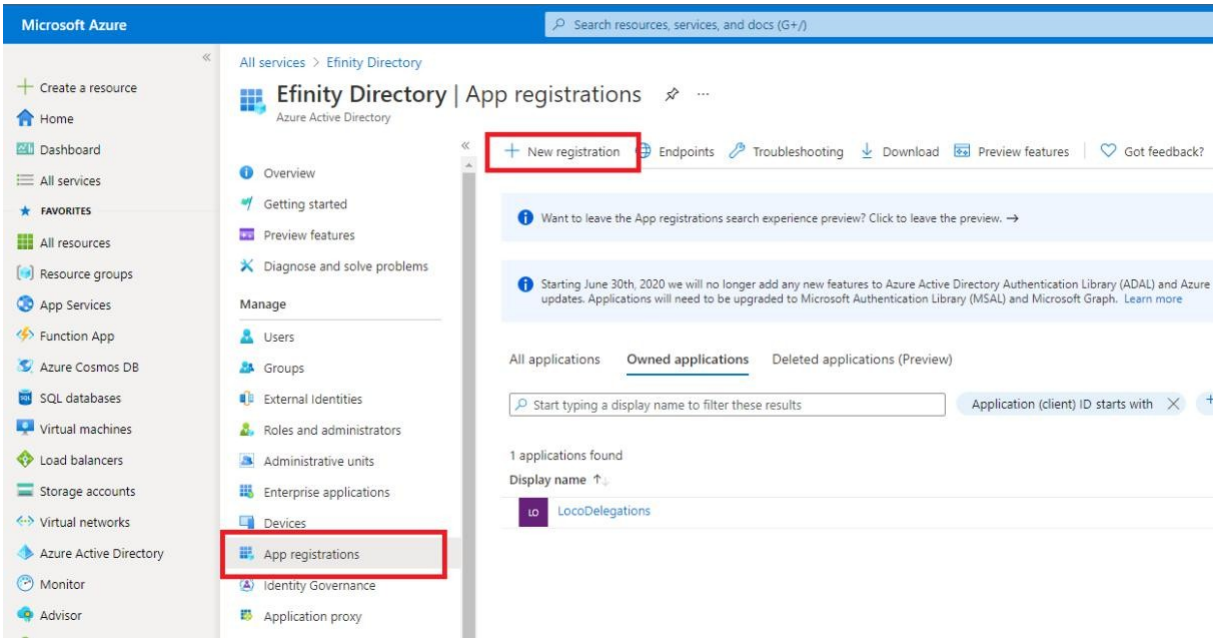
1) Open the Microsoft Entra admin centre (or Microsoft Azure portal) and navigate to Microsoft Entra ID.



2) On the Overview page, record the **Directory (tenant) ID**. Microsoft may display this within the tenant information or Essentials section.



3) Open **App registrations**, select **New registration** and create a new app registration.



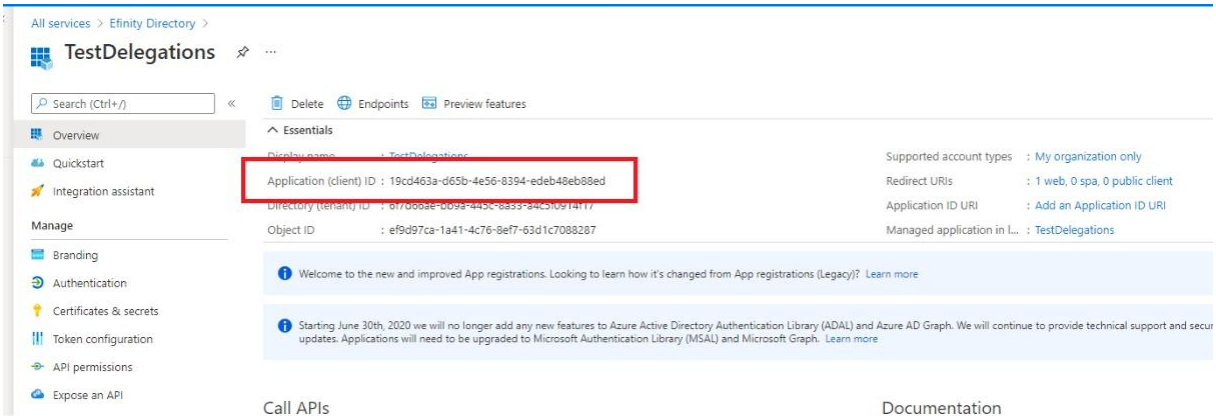
Enter the following registration details:

Name: Use a recognisable name such as LocoDELEGATIONS.

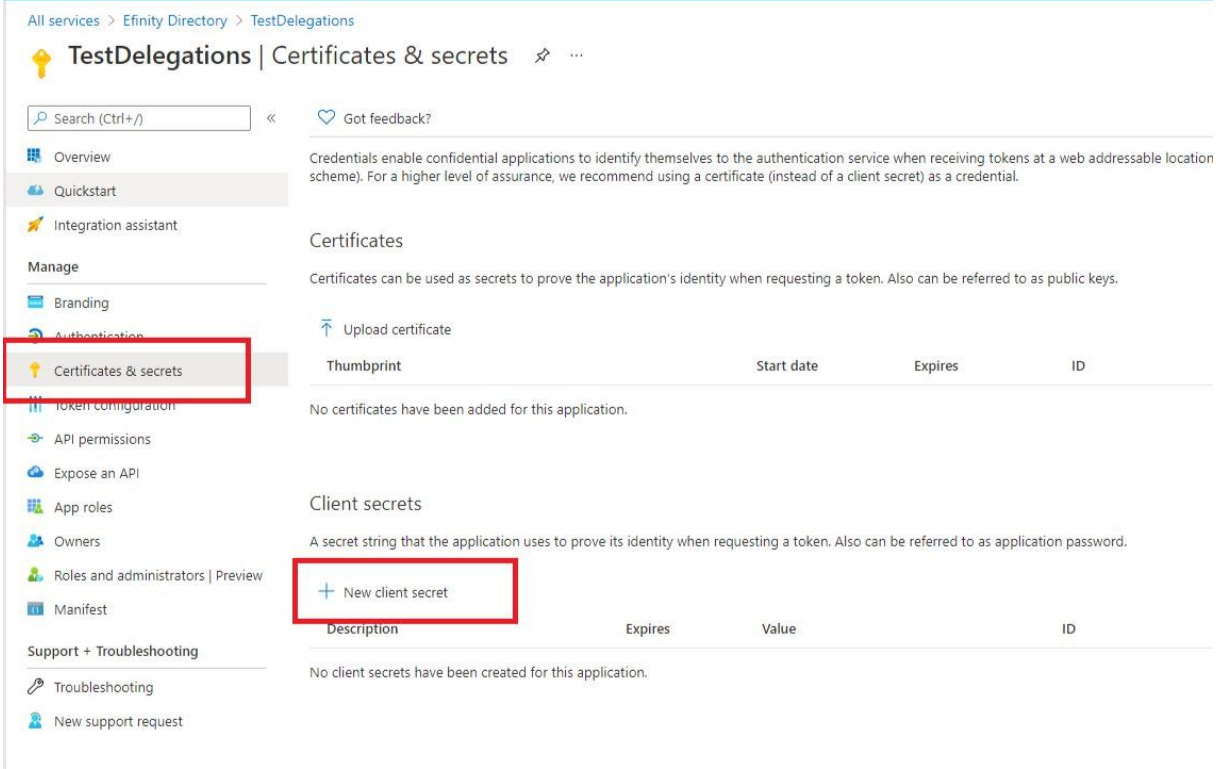
Supported account types: Select **Accounts in this organisational directory only**.

Redirect URI: Select **Web** and enter the council-specific LocoDELEGATIONS address supplied by LocoSOFT, followed by ***/signin-oidc***.

4) After the app registration is created, open its Overview page and record the **Application (client) ID**.



5) Open **Certificates & secrets** and select **New client secret**.



Create the client secret using the following guidance:
Description: Use a recognisable description such as LocoDELEGATIONS.

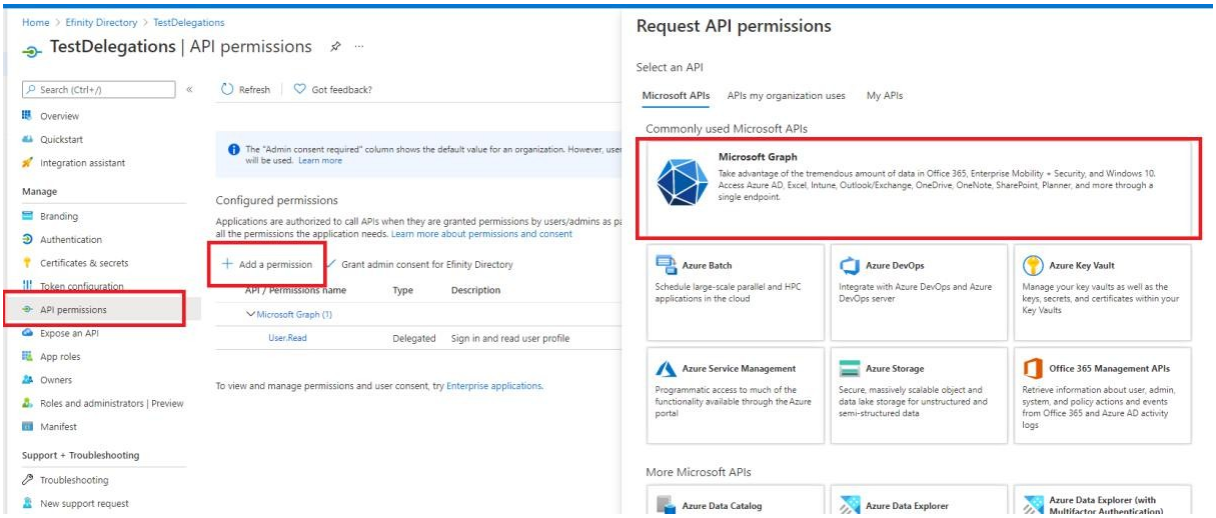
Expiry: Choose an expiry period that complies with the council's security policy. Track the expiry date and arrange renewal with LocoSOFT before the credential expires.

Record the secret value securely when it is created. Microsoft Entra will not display the complete value again. Do not send the client secret through ordinary email unless a secure method has been expressly agreed with LocoSOFT.

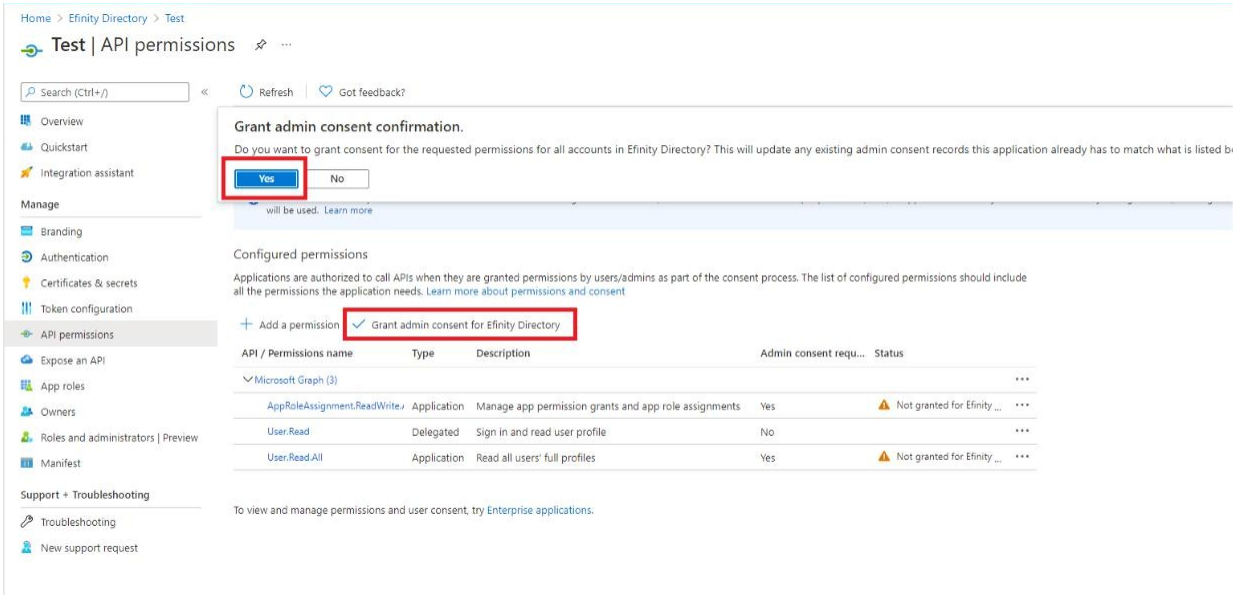
6) Open **API permissions**, select **Add a permission** and choose Microsoft Graph.

Choose **Application permissions** and add only the two permissions required for the current group-based configuration: **User.Read.All** and **GroupMember.Read.All**.

Group.Read.All and AppRoleAssignment.ReadWrite.All are not required for the current group-based setup. The screenshots are retained as navigational examples; use the permission names above as the authoritative requirements.

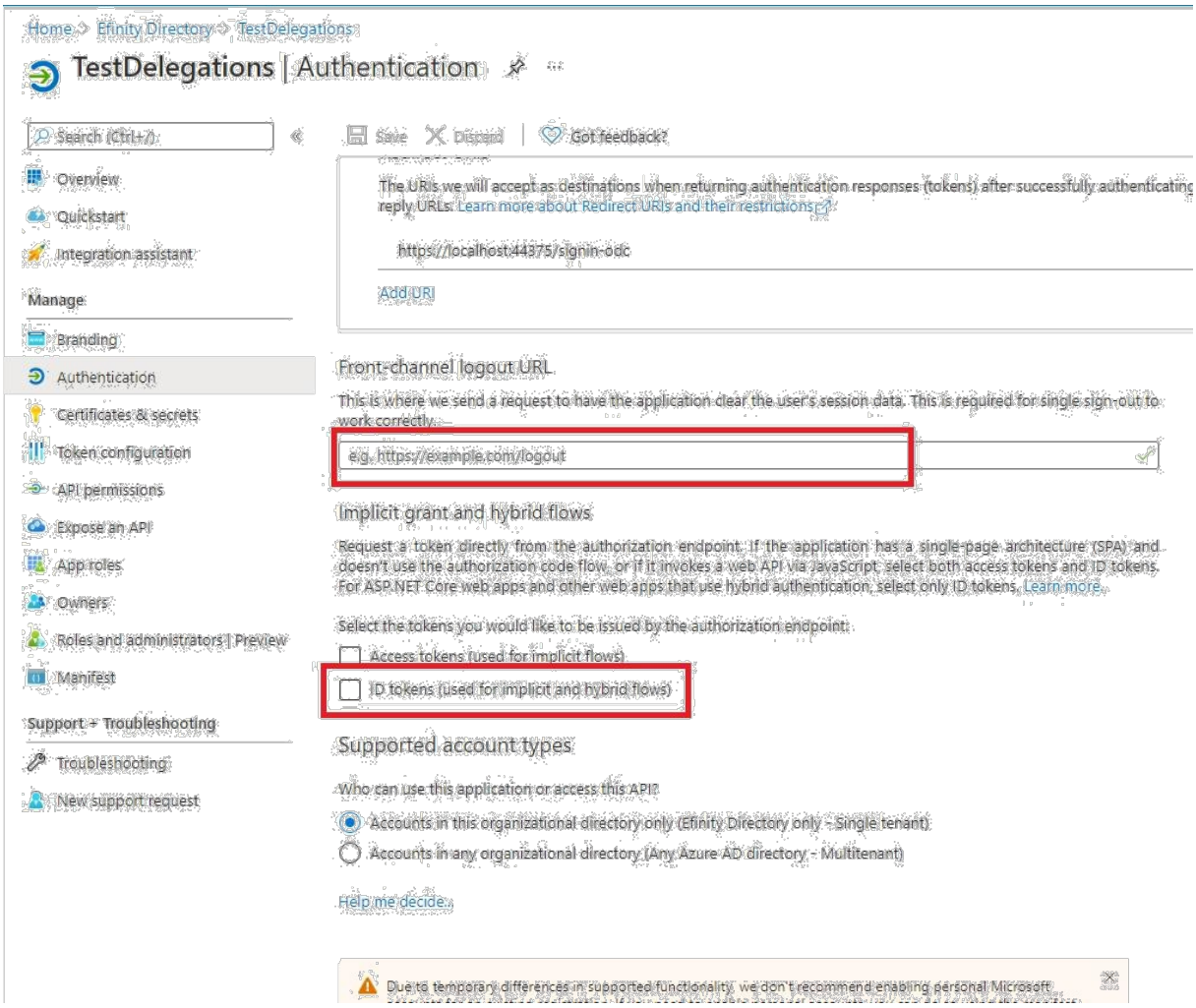


After adding both permissions, grant administrator consent for the council tenant.



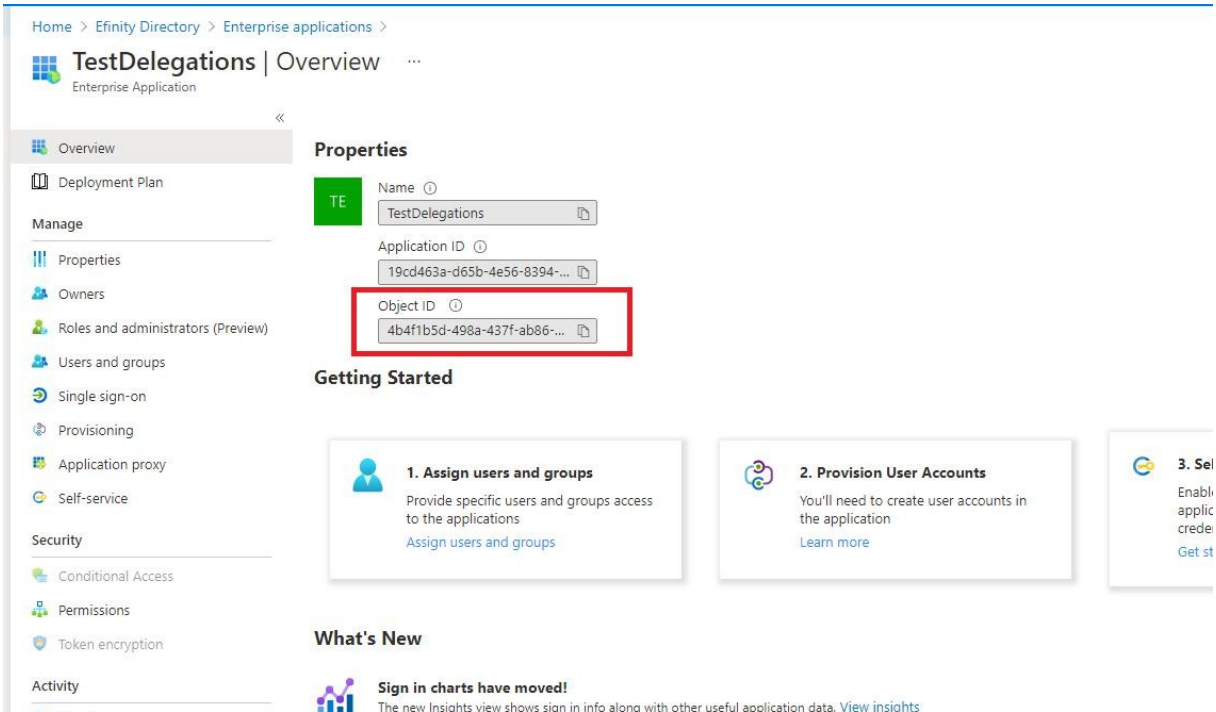
7) Open the app registration's **Authentication** settings.

   For the **Front-channel logout URL**, enter the council-specific LocoDELEGATIONS address supplied by LocoSOFT, followed by **/signout-oidc**. Under **Implicit grant and hybrid flows**, enable **ID tokens**. Save the authentication settings.



8) In the app registration manifest, set **"groupMembershipClaims": "SecurityGroup"**. This lets LocoDELEGATIONS read nominated Microsoft Entra security-group memberships at sign-in.

9) The next step is to record the enterprise application Object ID. From Microsoft Entra ID, open **Enterprise applications**, find the application created in the previous steps, open its Overview page and record its **Object ID**.



10) Open **Groups** and create or nominate the security groups agreed with LocoSOFT.
Record the Object ID (GUID) for each group. Display names may follow the council's naming conventions; the Object ID is the identifier used by LocoDELEGATIONS.

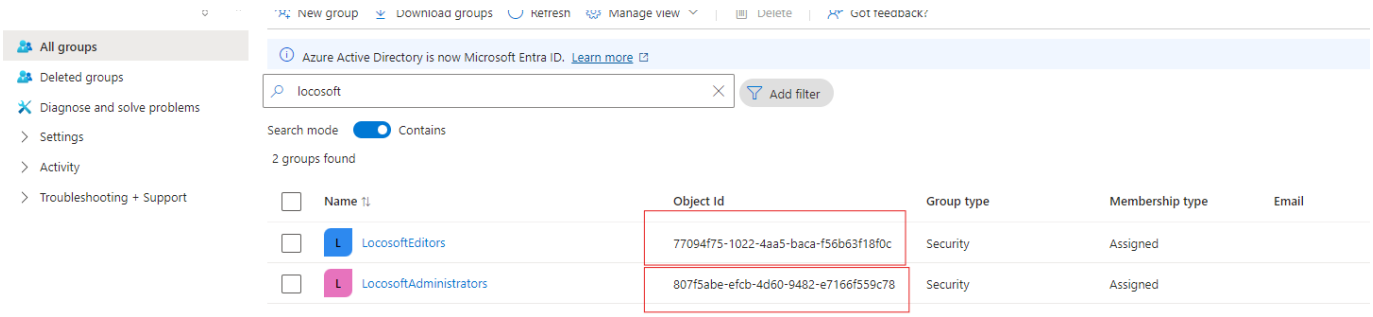
Create or nominate three security groups with these functions:

1) **Suggested name: LocoSOFT Administrators**

   Description: Administrators have full application access, including user-management functions.
2) **Suggested name: LocoSOFT Editors**

   Description: Editors can maintain application content, including legislation, bylaws and delegations, but do not have Administrator-level user management.
3) **Suggested name: Warrant Delegation Users**

   Description: Members can be assigned as delegates for warrants.



11) Assign appropriate users to the Administrator, Editor and Warrant Delegation Users security groups. Keep Administrator membership limited to users who genuinely require it, and review Administrator and Editor membership regularly.
The Warrant Delegation Users group remains required for users who can be assigned as delegates for warrants.

12) When the configuration is complete, coordinate secure transfer of the following values to LocoSOFT:
    - Application (client) ID
    - Client secret value
    - Directory (tenant) ID
    - Enterprise application Object ID
    - Administrator group Object ID
    - Editor group Object ID
    - Warrant Delegation Users group Object ID

LocoSOFT will complete the application-side configuration and coordinate testing. Transfer the client secret only through the agreed secure setup process. For assistance, contact support@locosoft.co.nz.