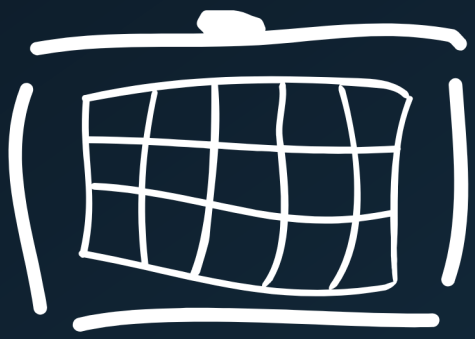


Radiator

CONFIGURATION GUIDE

Microsoft Entra ID multi-tenant App creation for Radiator Policy Server authentication

Date: 2026-11-16

Creating an application to the Microsoft Entra ID is essential for establishing a trust relationship between Radiator Policy Server and the Microsoft identity platform. With the application you enable identity and access management (IAM) for Radiator Policy Server, allowing it to securely interact with Microsoft services and APIs.

The created trust is unidirectional. Radiator Policy Server trusts the Microsoft identity platform, and not the other way around. Once created, the application object can't be moved between different tenants.

This guide covers the **multi-tenant** scenario, where the application lives in one tenant while the user accounts that authenticate through it live in a different tenant. If your application and your user accounts are in the same tenant, follow the single-tenant Microsoft Entra ID App creation for Radiator Policy Server authentication guide instead.

When to use a multi-tenant application

Use a multi-tenant application when the application and the user accounts are in separate Microsoft Entra tenants. Throughout this guide two tenants are referred to by name:

- **Application tenant**: The tenant where the Radiator application is registered and kept.
- **Identity tenant**: The tenant that owns the user accounts (for example a parent company tenant).

The important constraint comes from the Resource Owner Password Credentials (ROPC) flow that Radiator Policy Server uses to authenticate users. ROPC validates the password against the tenant ID used in the Radiator configuration, and only for the users who are members (native accounts) of that tenant. Microsoft's ROPC flow does not support guest (B2B) accounts, federated accounts, or accounts that require MFA.

A guest object in a tenant is only a reference, the actual credential lives in the user's home tenant. Because of this:

- Tenant ID on the Radiator configuration has to point to the tenant where the accounts are native members. This is the Identity tenant.
- Register the application as a multi-tenant application so its service principal can be provisioned in the Identity tenant.

In the scenario in this guide the application is registered in the **Application tenant** and the accounts are members of the **Identity tenant**, so the application is created as multi-tenant and consented in the Identity tenant, and Radiator's configuration points at the Identity tenant.

New application or existing application

You have two options for obtaining the multi-tenant application in the Application tenant:

- **Create a completely new multi-tenant application.** Follow "Create the application" below to register a new application and select the multi-tenant account type during registration. Use this when you do not yet have a Radiator application, or when you prefer to keep the cross-tenant setup separate from an existing single-tenant one.
- **Convert your existing single-tenant application to multi-tenant.** If you already have a working single-tenant Radiator application, you do not need to create a new one. Change its *Supported account types* to multi-tenant and reuse the same client ID, secret, and API permissions. Use this when you want to extend your current setup to the Identity tenant without re-registering.

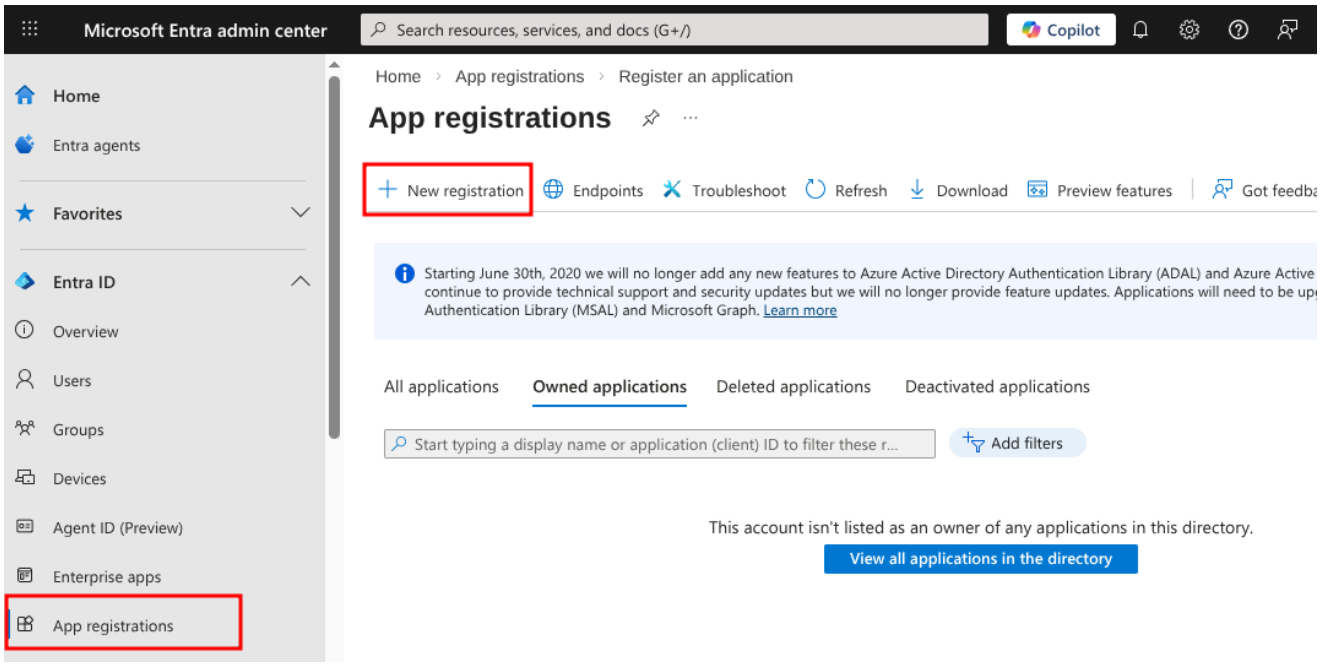
Both paths lead to the same result: a multi-tenant application in the Application tenant that the Identity tenant administrator then consents to (see "Grant admin consent in the Identity tenant"). If you are creating a new application, continue with "Create the application". If you are converting an existing application, skip to "Convert an existing single-tenant application".

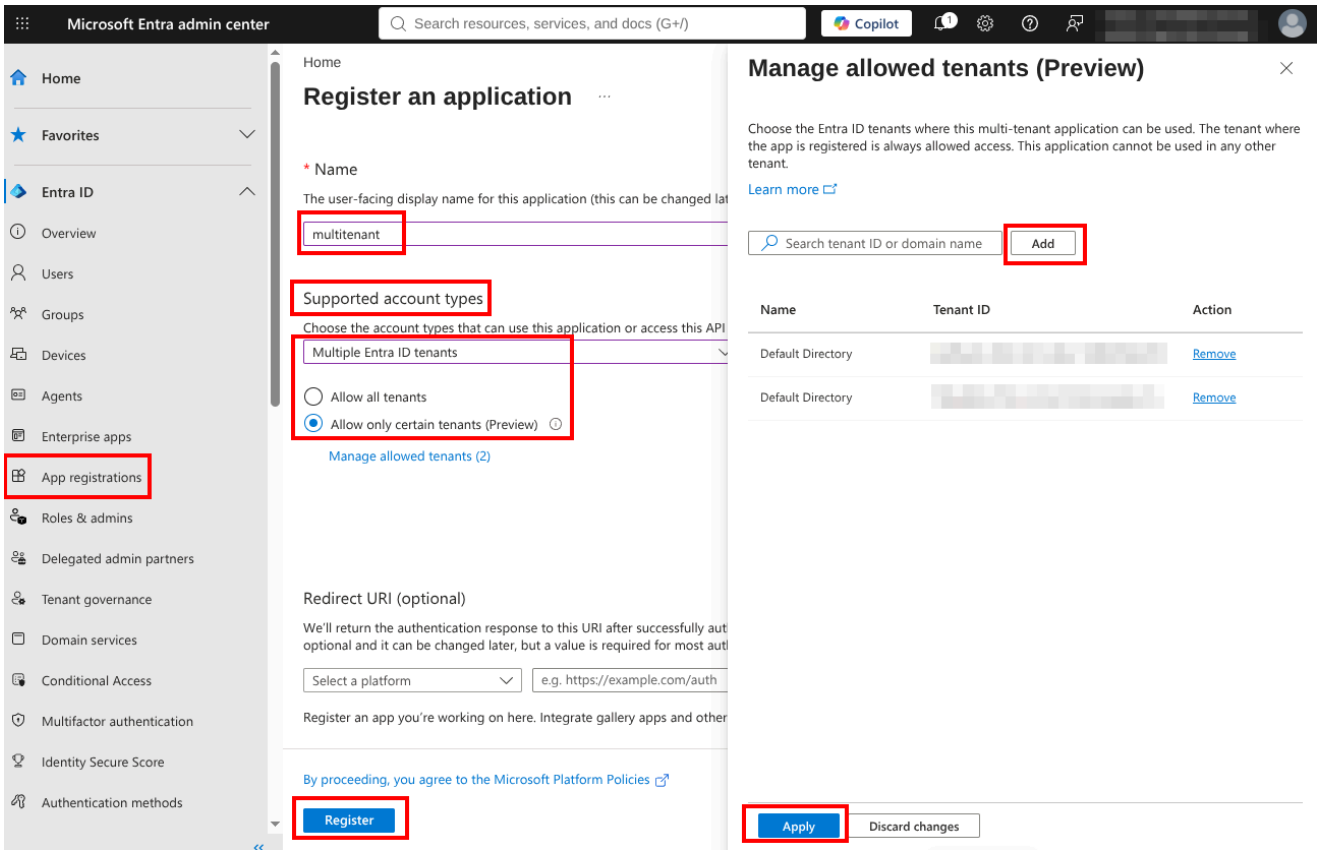
Create the application

Create the app registration in the **Application tenant** by following these steps:

1. Sign in to the Microsoft Entra admin center as a user with at least an *Application Developer* role
2. If you have access to multiple tenants, select the **Application tenant** (the tenant where the application is kept).
3. Browse to **App registrations** and select **New registration**.
4. Enter a meaningful **Name**. App users can see this name, and it can be changed at any time. You can have multiple app registrations with the same name.
5. Under **Supported account types**, select **Multiple Entra ID tenants** and select either **Allow all tenants** or limit access to specific tenants with **Allow only certain tenants**. If limiting the allowed tenants, add them in the **Manage allowed tenants** view. This is the setting that allows the application to be consented and used in the Identity tenant.

6. Select **Register** to complete the app registration.



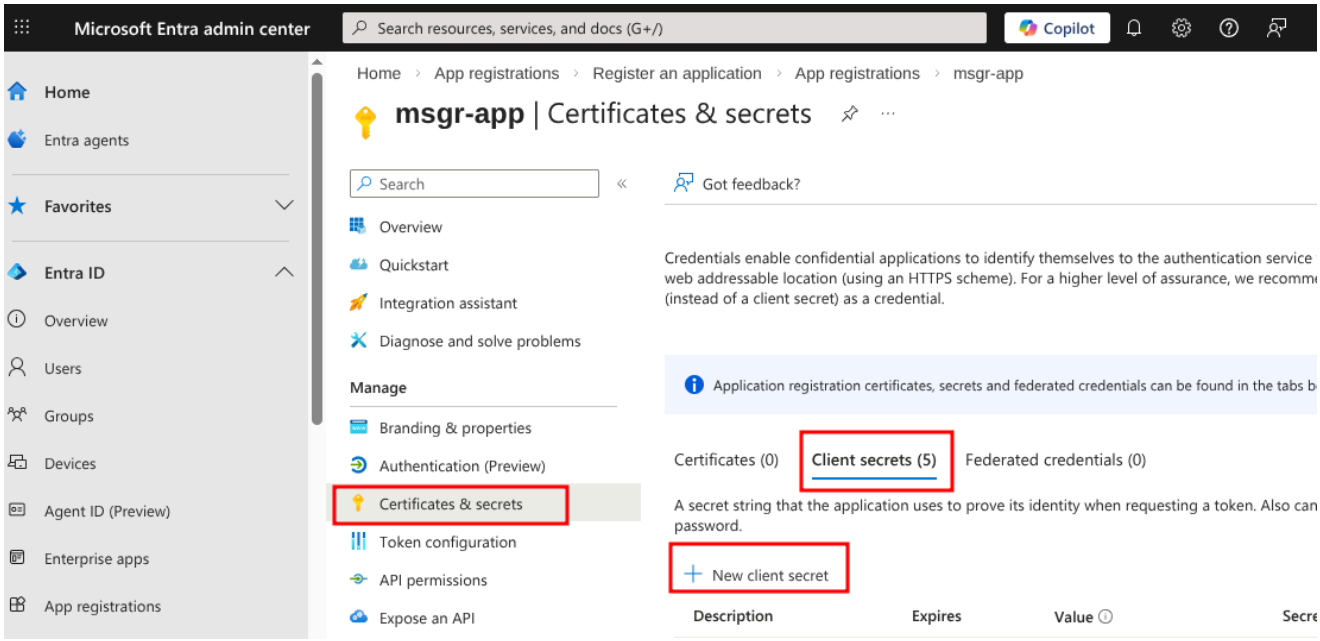


Add credentials

After registering an app you need to add client secrets (sometimes known as application password) as credentials. Credentials allow Radiator Policy Server to authenticate as itself, requiring no interaction from a user at runtime. The secret is created on the application in the **Application tenant**; the same client ID and secret are used regardless of which tenant validates the user.

1. In the Microsoft Entra admin center of the **Application tenant**, in **App registrations**, select your application.

2. Select **Certificates & secrets** > **Client secrets** > **New client secret**.



3. Add a description for your client secret.
4. Select an expiration for the secret or specify a custom lifetime.
5. Select **Add**.
6. *Record the secret's value* for use in Radiator Policy Server configuration (see Radiator Entra ID configuration guide). This secret value is *never displayed again* after you leave this page. If you lose the secret, you will have to create a new one.

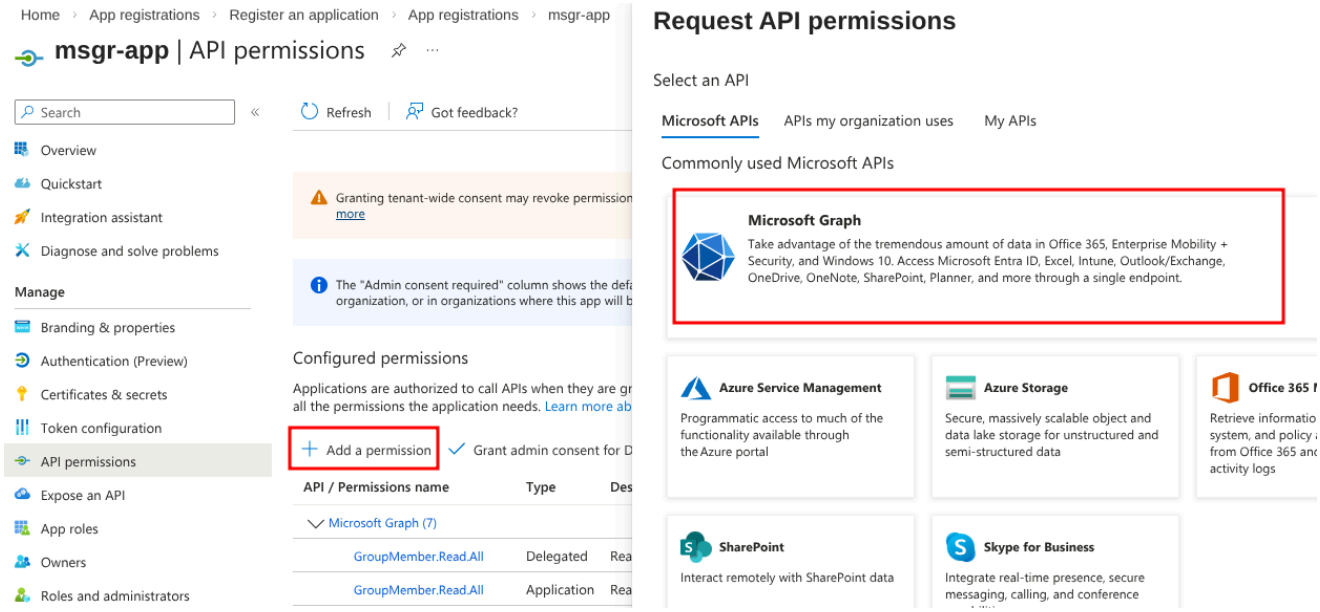
Set permissions

Permissions are configured on the application in the **Application tenant**. They travel with the multi-tenant application and are presented for approval when the Identity tenant administrator grants admin consent.

Resource Owner Password Credentials flow

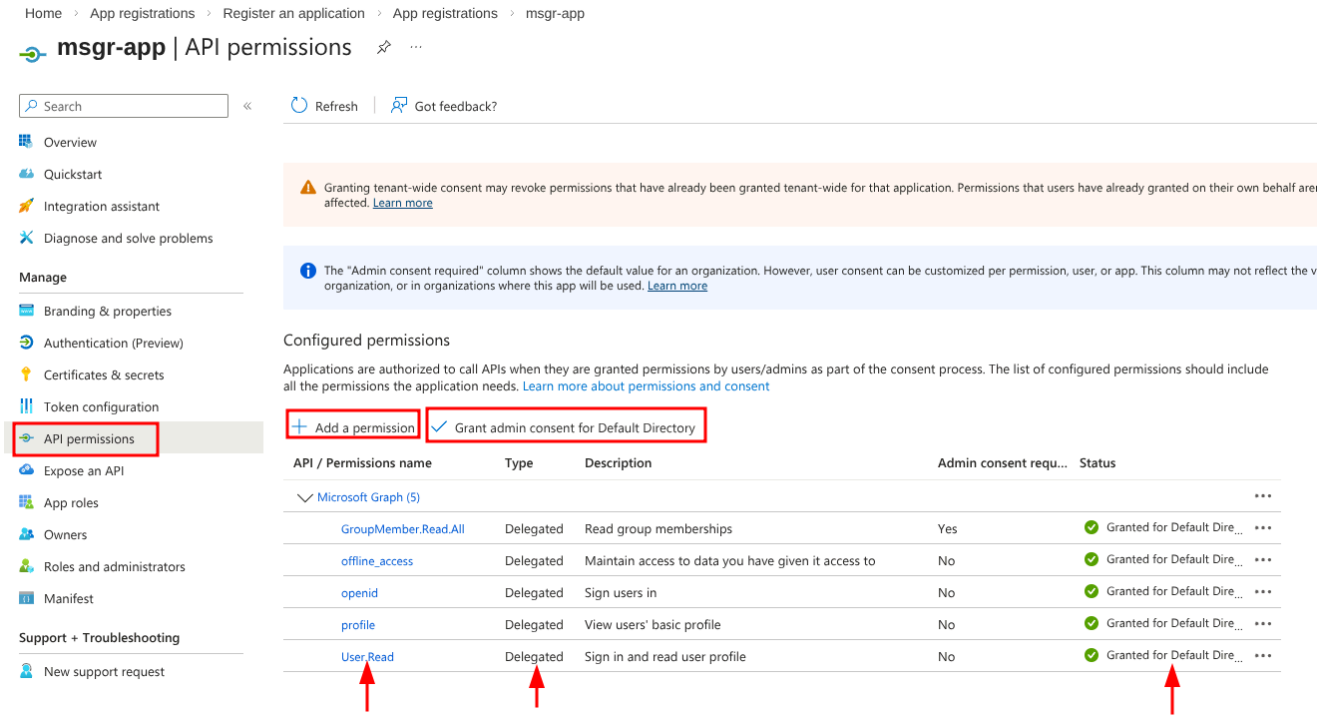
Radiator Policy Server also needs to access the data stored in Microsoft Graph. For Resource Owner Password Credentials (ROPC) flow configure delegated permission to Microsoft Graph to enable Radiator Policy Server to query the groups users belong to as well as authenticate the user based on Microsoft Entra.

1. From the **Overview** page of your client application, select **API permissions** > **Add a permission** > **Microsoft Graph**



2. Select **Delegated permissions**
3. Under **Select permissions**, select the following permissions:

- GroupMember.Read.All
- openid
- profile
- User.Read

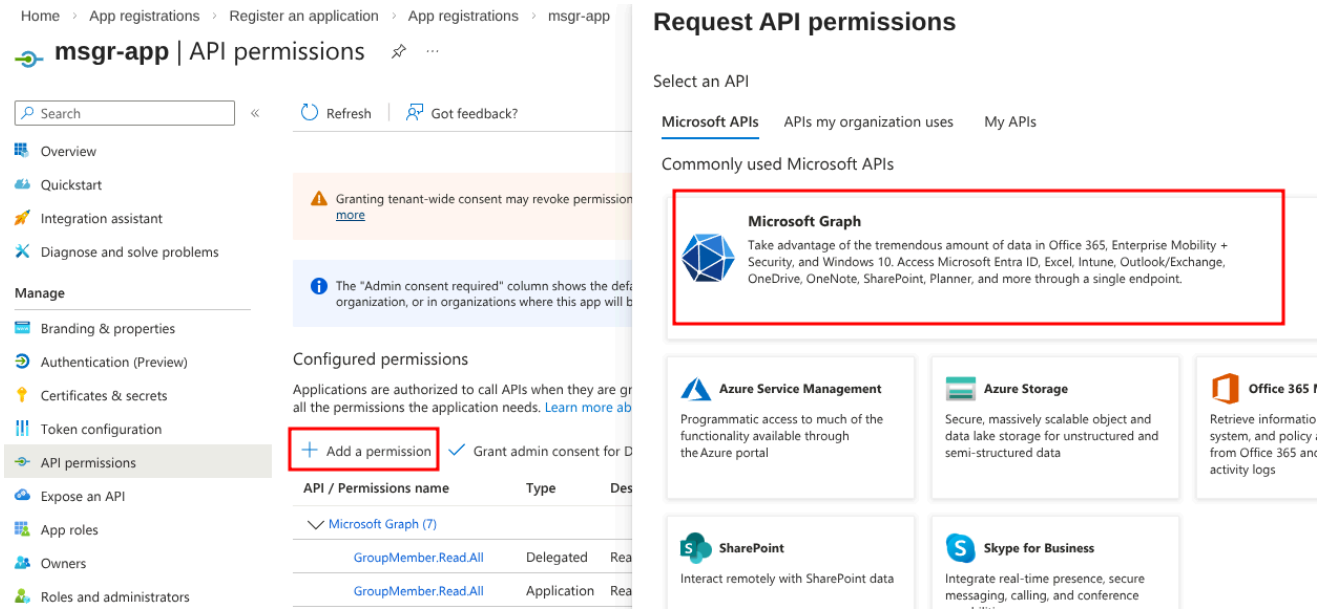


4. Some permissions require an Admin grant. In the multi-tenant scenario the required admin consent is granted by the **Identity tenant** administrator (see "Grant admin consent in the Identity tenant" below), not in the Application tenant. You do not need to grant admin consent in the Application tenant unless you also authenticate users from the Application tenant.

Client credentials flow

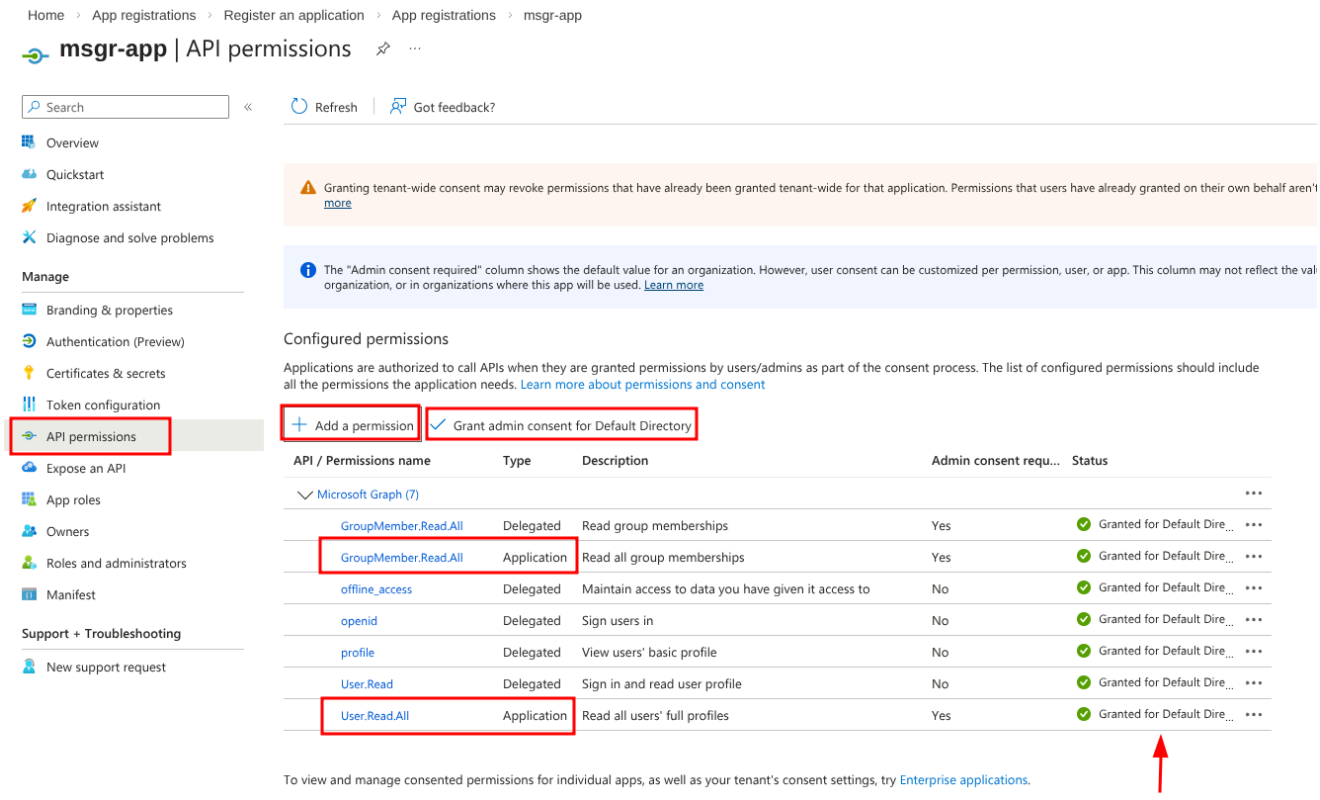
Permissions for Client credentials flow can be added to the same app used by the ROPC flow.

1. From the **Overview** page of your client application, select **API permissions** > **Add a permission** > **Microsoft Graph**



2. Select **Application permissions**
3. Under **Select permissions**, select the following permissions:

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



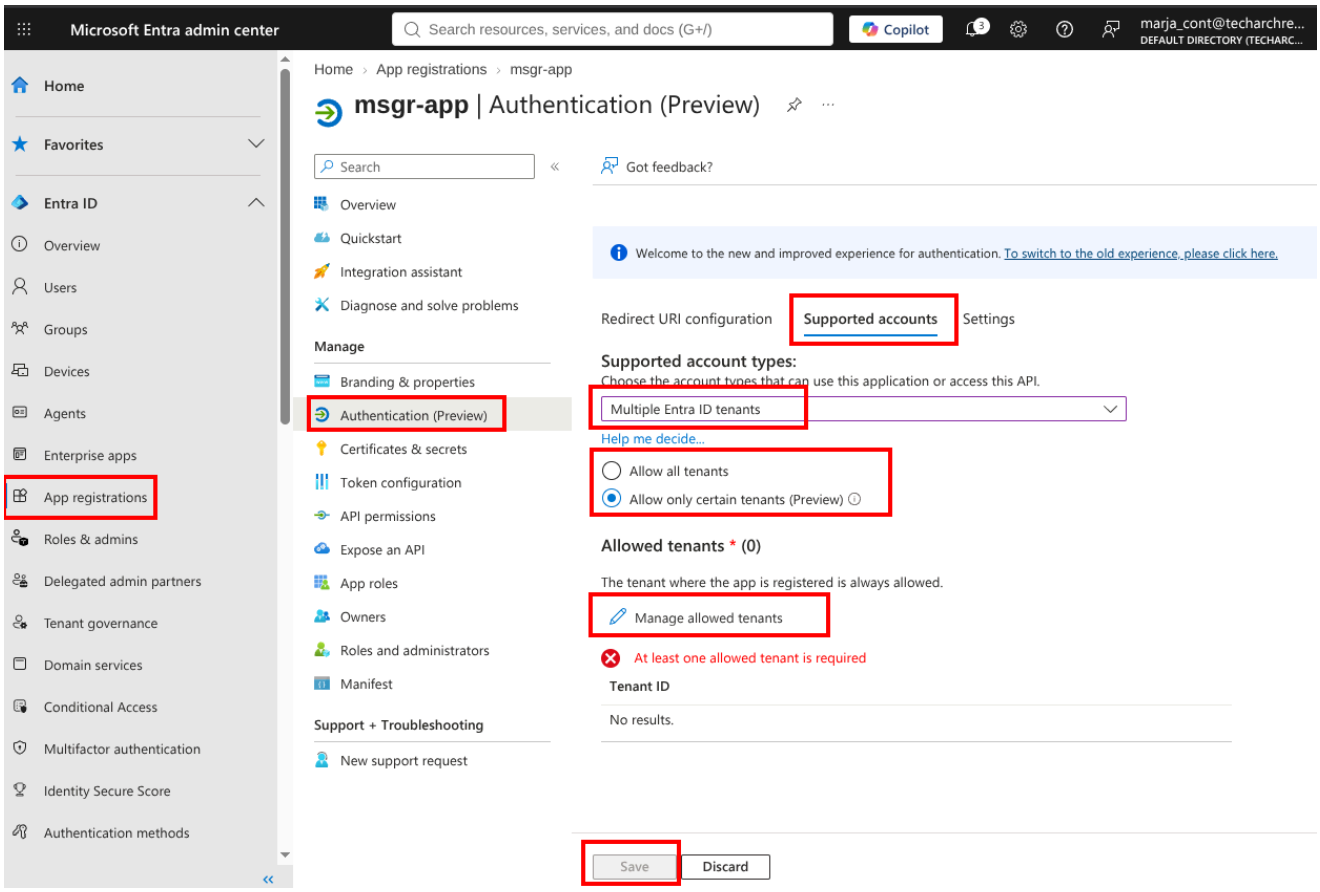
4. These permissions require an Admin grant. As with the delegated permissions, the admin consent is granted by the **Identity tenant** administrator so that the service principal in the Identity tenant receives the application permissions.

NOTE: It can take up to 60 minutes for the permissions to propagate into use.

Convert an existing single-tenant application

If you already have a working single-tenant Radiator application in the **Application tenant**, you can convert it to multi-tenant instead of registering a new one. The client ID, client secret, and API permissions are preserved in the conversion.

1. Sign in to the Microsoft Entra admin center of the **Application tenant**.
2. Browse to **App registrations** and select your existing application.
3. Select **Authentication**.
4. Under **Supported accounts**, change the selection from **Single tenant only** to **Multiple Entra ID tenants** and select either **Allow all tenants** or limit access to specific tenants with **Allow only certain tenants**. If limiting the allowed tenants, add them in the **Manage allowed tenants** view.
5. Select **Save**.



Before continuing, verify the existing application already has the client secret and Microsoft Graph permissions described in "Add credentials" and "Set permissions". Add anything that is missing. Then continue with "Grant admin consent in the Identity tenant".

Grant admin consent in the Identity tenant

A multi-tenant application registered in the **Application tenant** does not automatically appear in the **Identity tenant**. Until it is consented there is nothing for the Identity tenant administrator to browse to. The application must first be provisioned in the Identity tenant through an admin-consent action, which creates its service principal (Enterprise application) there.

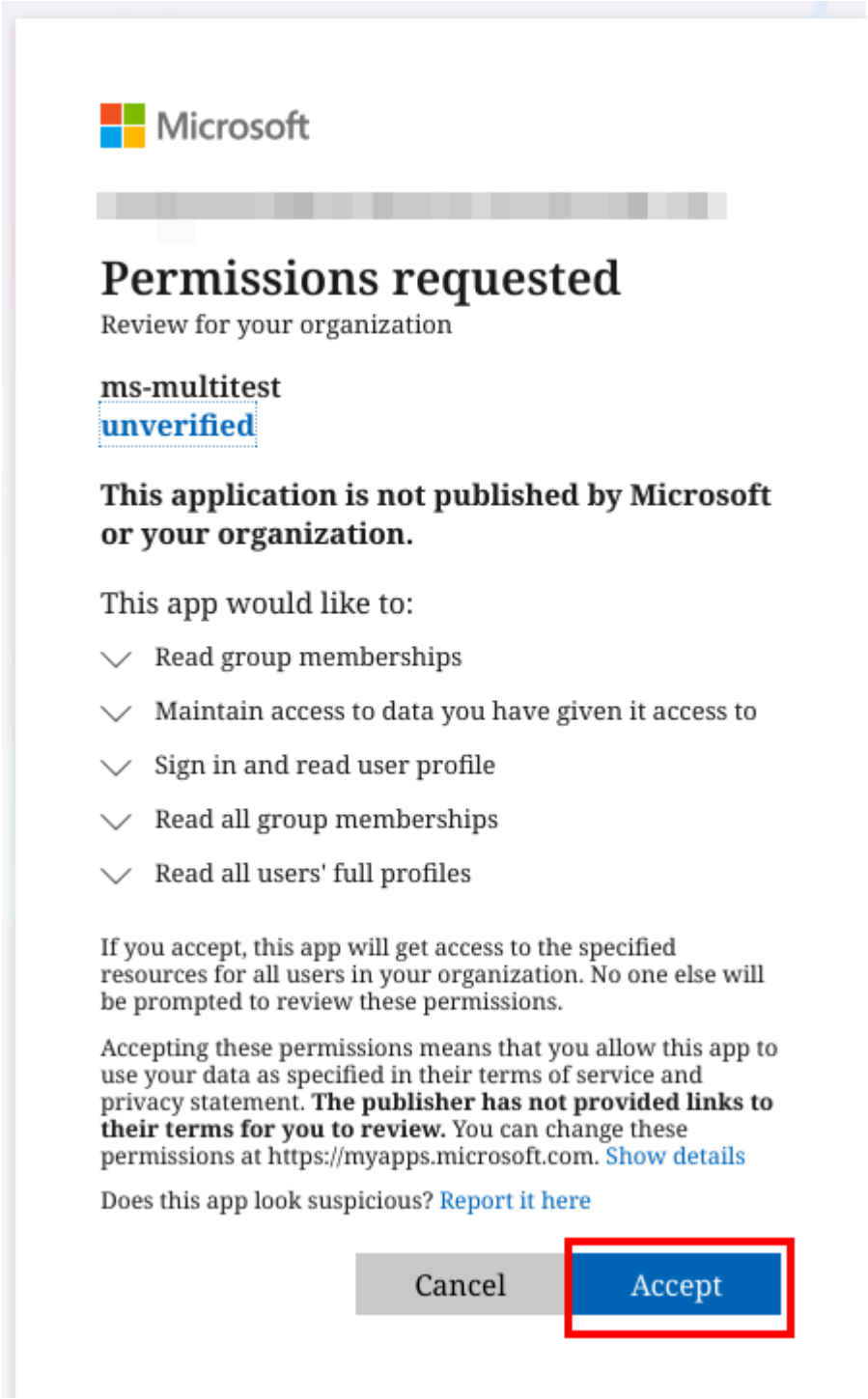
Provision the application with the admin-consent URL

The **Identity tenant** administrator provisions the application by opening an admin-consent URL that combines the Identity tenant ID with the Application-tenant application's client ID:

```
https://login.microsoftonline.com/{IDENTITY_TENANT_ID}/adminconsent?client_id=
{APPLICATION_TENANT_CLIENT_ID}
```

- `{IDENTITY_TENANT_ID}` : the Identity tenant's Directory (tenant) ID.
- `{APPLICATION_TENANT_CLIENT_ID}` : the Application (client) ID of the application you registered in the Application tenant.

The Identity tenant administrator signs in, reviews the consent prompt that shows the application name and the requested Microsoft Graph permissions, and approves it. This creates the service principal for your Application tenant application inside the Identity tenant and grants the permissions there.

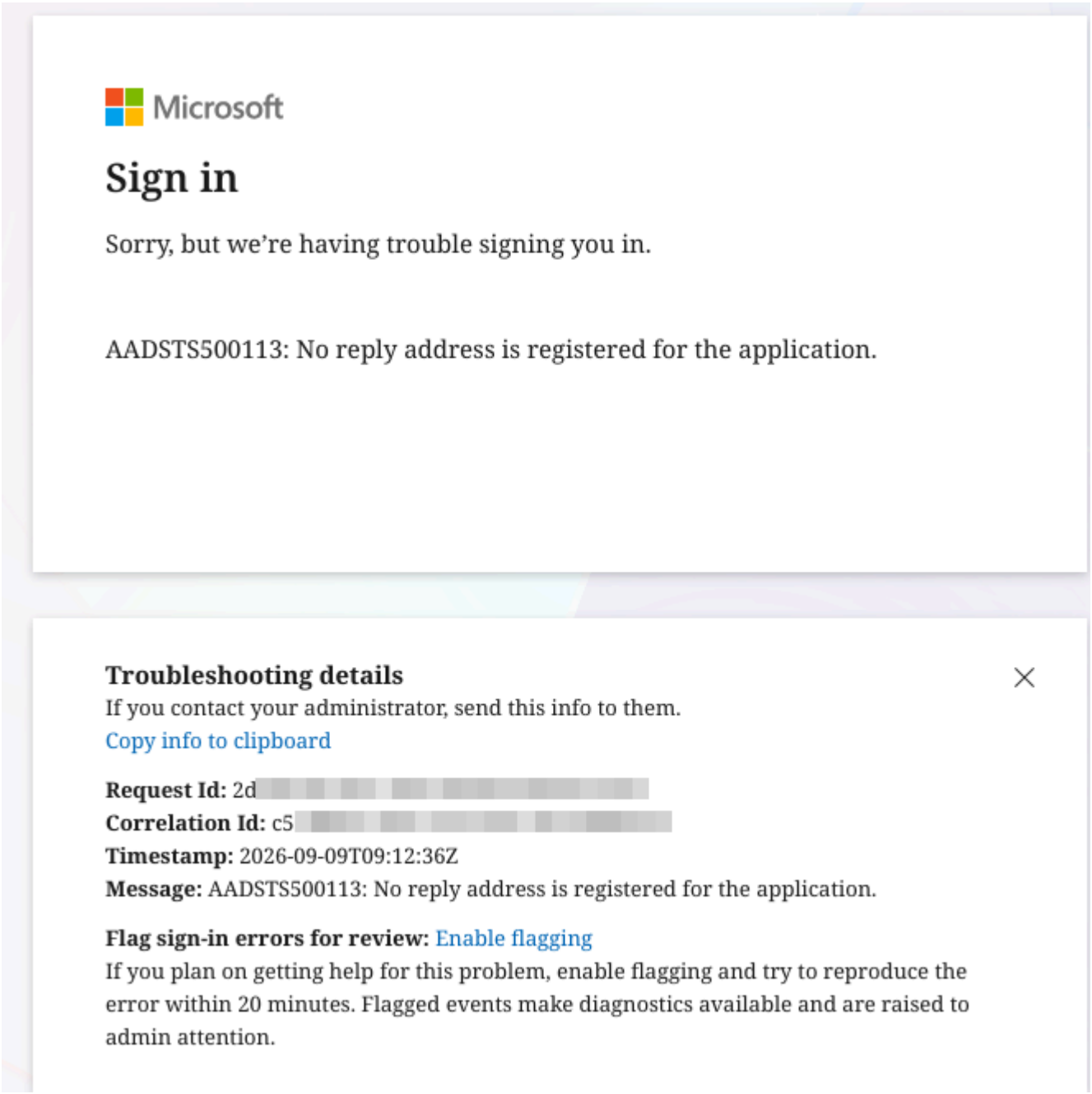


NOTE: Since the application is used with ROPC flow, it does not require configuring Redirect URI. This means that when the administrator grants admin consent, the web page will show an error at the end. This does not affect the functionality of the Service Principal, as Microsoft Entra ID executes the steps in this specific order:

1. Administrator signed in as the Identity tenant admin and clicked Accept.
2. Microsoft Entra ID immediately provisioned the Service Principal (Enterprise Application) in Identity tenant and granted the requested permissions.
3. Microsoft Entra ID attempted to redirect the admin's browser back to the application, but because the redirect URI was missing the flow threw the AADSTS500113 error at the redirection step.

Because step 2 is completed before step 3 fails, the application identity and admin consent were successfully established in Identity tenant.

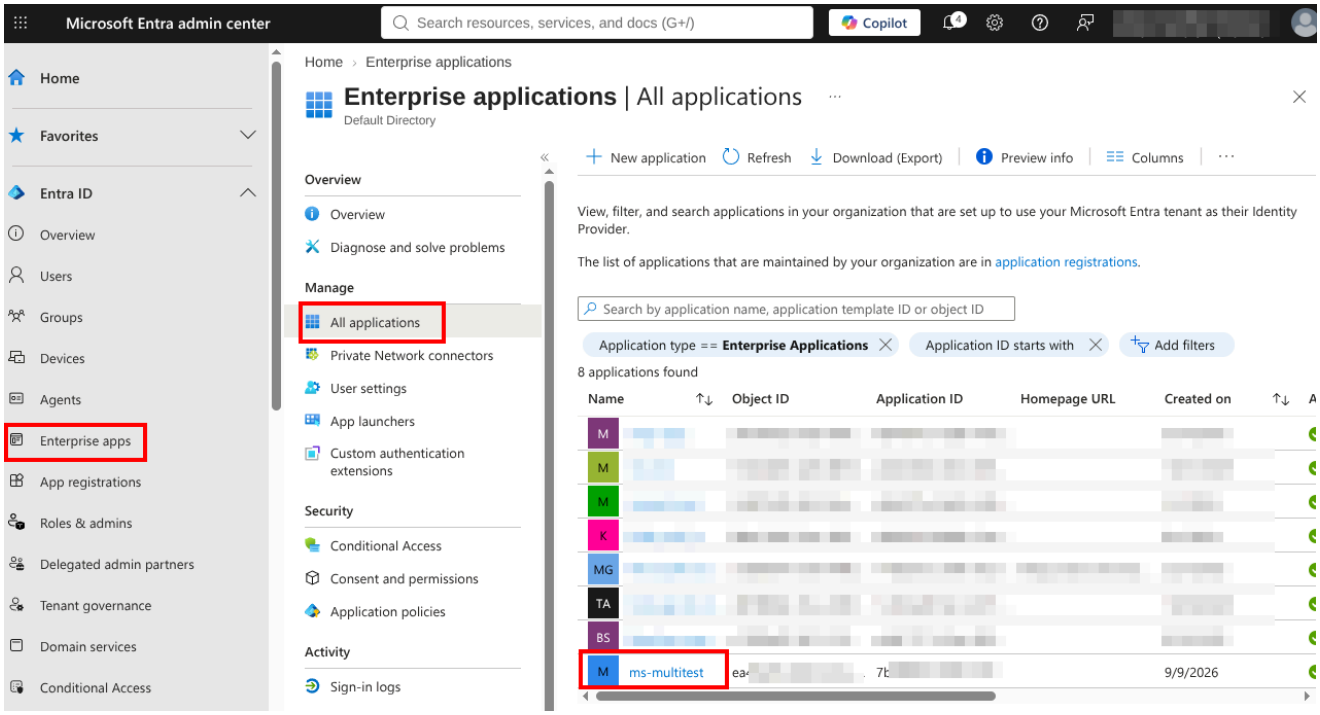
Since ROPC operates directly against the /token endpoint without requiring browser redirects or interactive consent prompts, it works as long as the Service Principal exists and permissions are granted in Identity tenant.



Find the application in the Identity tenant after consent

Once consent has been granted, the Identity tenant administrator can browse to the application in the Identity tenant under Enterprise applications:

1. Sign in to the Microsoft Entra admin center of the **Identity tenant**.
2. Browse to **Enterprise applications** > **All applications**.
3. Search by the application name or by the Application (client) ID from the Application tenant.



NOTE: The application appears under **Enterprise applications**, not under **App registrations**. In the Identity tenant, **App registrations** lists only applications whose home tenant is the Identity tenant. The home tenant of this application is the Application tenant, so in the Identity tenant it is visible only as an Enterprise application (Service Principal) after consent.

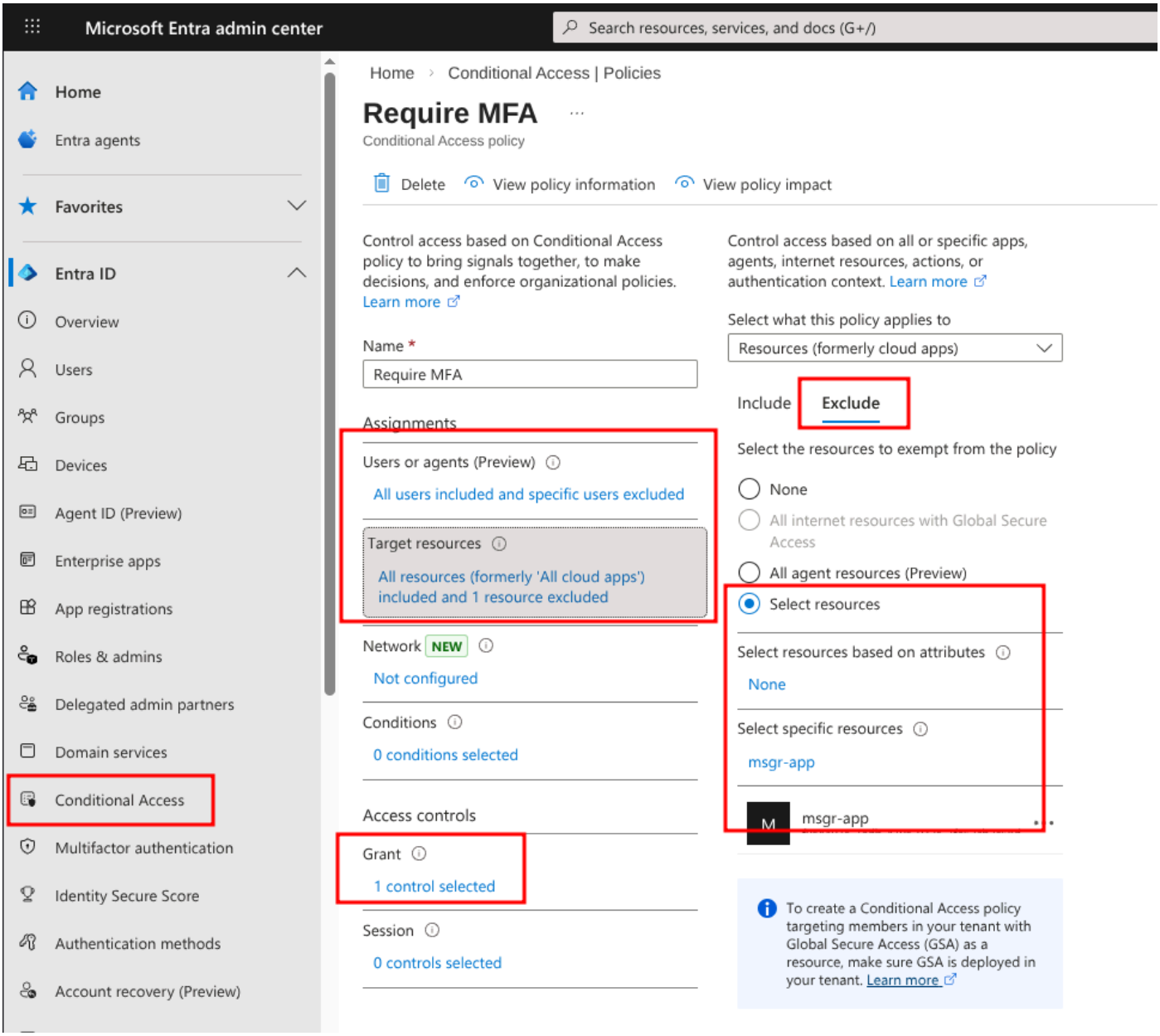
Create exception for MFA requirement for the application

When authenticating with RADIUS protocol and ROPC or Clients credentials flow it is not possible to use the automatic multi-factor authentication, instead the MFA requirement must be disabled for the Microsoft Entra ID Application and trigger separately from Radiator Policy Server configuration. In the multi-tenant scenario the Conditional Access and MFA policies that apply to the authenticating users are enforced by the tenant that authenticates the users. In the common case this is the **Identity tenant**, because that is where the accounts are members. Configure the MFA exception only in the tenant that authenticates the users and enforces MFA.

The recommended way to do this is with Conditional Access policies, as that will allow having MFA enabled for all other use cases. For example: MFA should only be disabled when the user is authenticating via the application created, not when the user is logging in to the Entra portal.

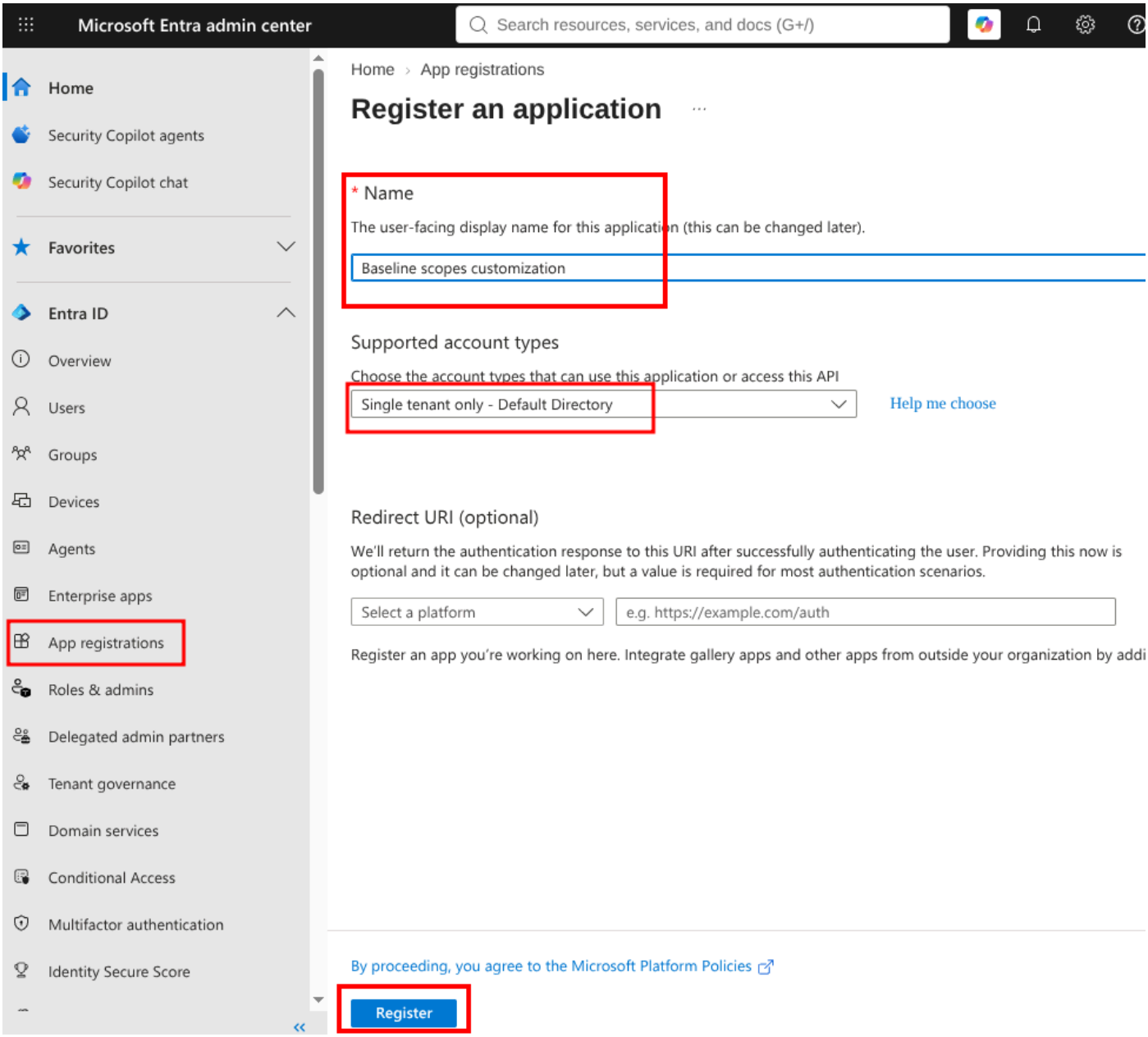
Using Conditional Access policies requires at minimum Microsoft Entra ID P1 licence and disabling organization security defaults. When disabling MFA via Conditional Access policy, users must not have Per-user MFA *enforced* or *enabled* in the Entra portal of the tenant that authenticates the users (https://entra.microsoft.com > All users > Per-user MFA), instead the MFA should be enforced via Conditional Access policies for other use cases than with Radiator Policy Server authentication. In practice this means that MFA is not disabled/bypassed via Conditional Access policy, it is just not enforced to Radiator Policy Server authentication.

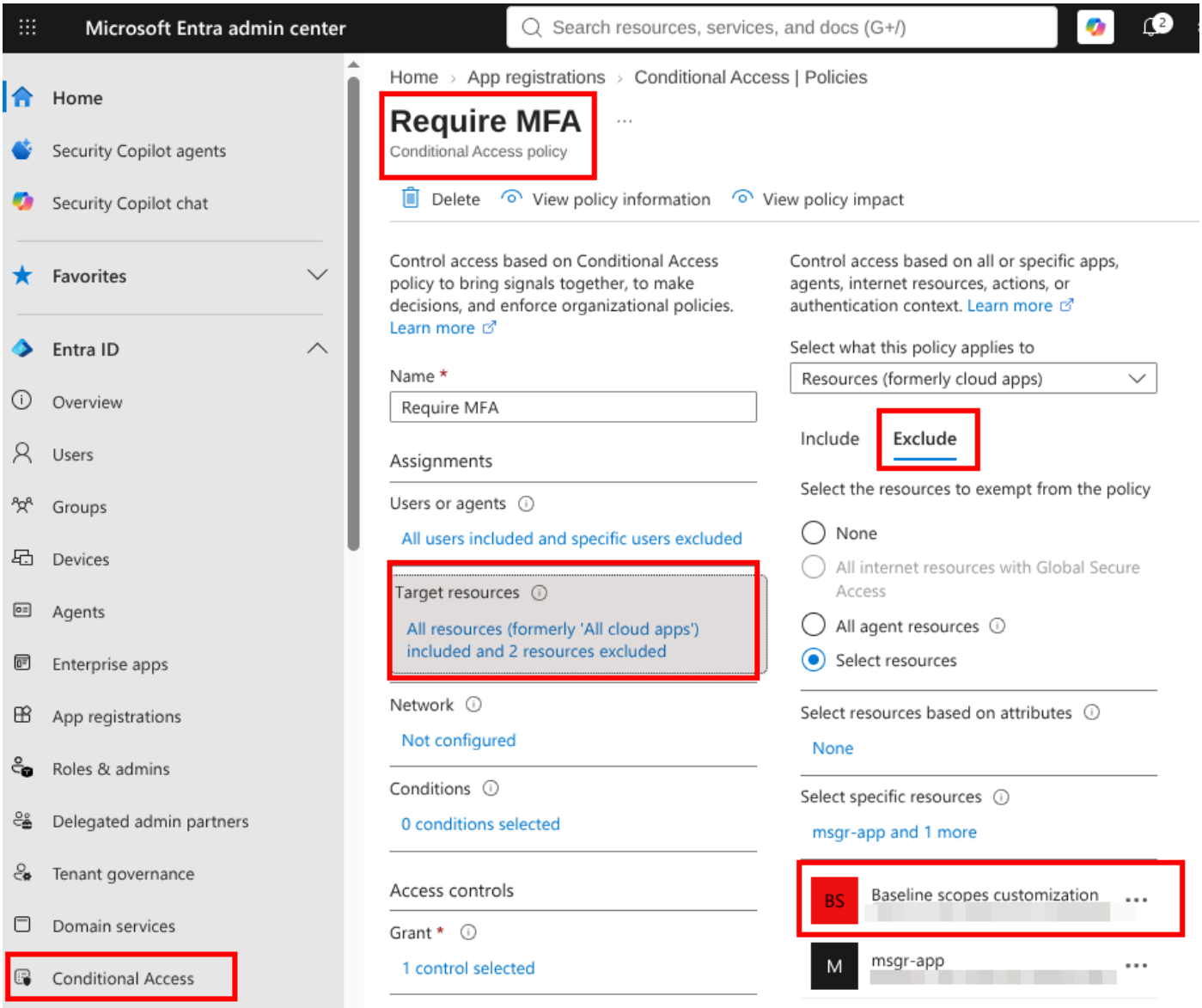
Example Conditional Access policy to require MFA except when using the application can be done for either all users or specific users, but the main thing is to exclude the created app when selecting Target resources. In the Grant section, “Require multifactor authentication” should be selected as control for granting the access:

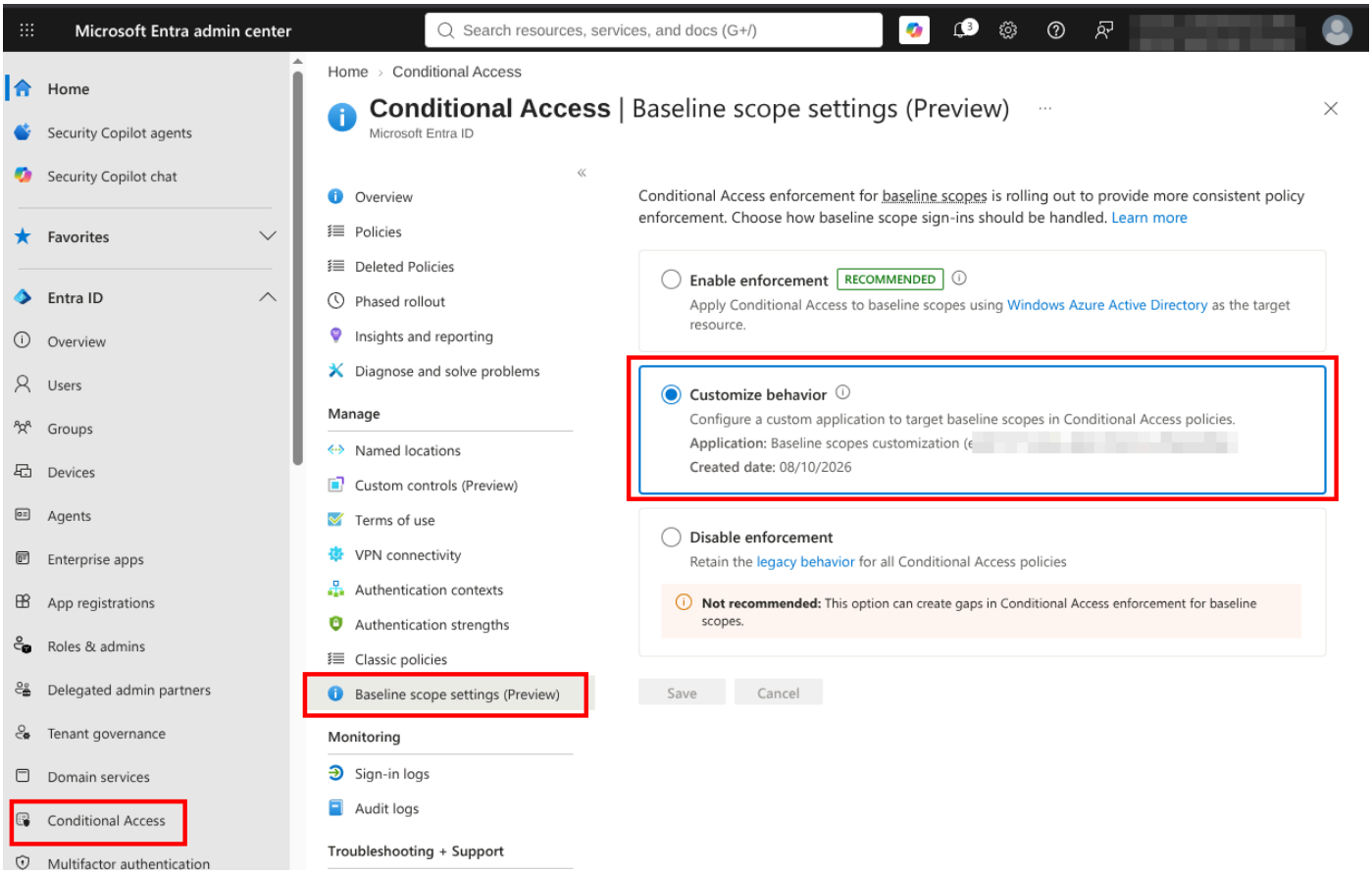


Recently, Microsoft has changed how the Conditional Access policies function when an application is excluded from a policy that otherwise targets All resources. Now the exclusion also takes into account which scopes Radiator uses with the application, and the behavior of the low-level baseline scopes has changed. All scopes are now evaluated and the Conditional Access policies are enforced regardless of the exclusion (see more from Microsoft).

To continue with the previous functionality, where baseline scopes were automatically excluded from policy enforcement, the Conditional Access Baseline scope enforcement must be changed to Customized behavior mode and another empty application must be registered so it can be excluded on the Conditional Access policy rule as shown in Microsoft instructions. In the multi-tenant scenario this empty application and the Customized behavior configuration must be registered in the tenant that authenticates the users and enforces Conditional Access.


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Security Copilot agents
Security Copilot chat
Favorites
Entra ID
Overview
Users
Groups
Devices
Agents
Enterprise apps
App registrations
Roles & admins
Delegated admin partners
Tenant governance
Domain services
Conditional Access
Multifactor authentication
Identity Secure Score
Home › App registrations
Register an application
* Name
The user-facing display name for this application (this can be changed later).
Baseline scopes customization
Supported account types
Choose the account types that can use this application or access this API
Single tenant only - Default Directory
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Select a platform
e.g. https://example.com/auth
Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by addi
By proceeding, you agree to the Microsoft Platform Policies
Register


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Security Copilot agents
Security Copilot chat
Favorites
Entra ID
Overview
Users
Groups
Devices
Agents
Enterprise apps
App registrations
Roles & admins
Delegated admin partners
Tenant governance
Domain services
Conditional Access
Home › App registrations › Conditional Access | Policies
Require MFA
Conditional Access policy
Delete
View policy information
View policy impact
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
Require MFA
Assignments
Users or agents
All users included and specific users excluded
Target resources
All resources (formerly 'All cloud apps') included and 2 resources excluded
Network
Not configured
Conditions
0 conditions selected
Access controls
Grant *
1 control selected
Control access based on all or specific apps, agents, internet resources, actions, or authentication context. Learn more
Select what this policy applies to
Resources (formerly cloud apps)
Include
Exclude
Select the resources to exempt from the policy
None
All internet resources with Global Secure Access
All agent resources
Select resources
Select resources based on attributes
None
Select specific resources
msgr-app and 1 more
BS
Baseline scopes customization
M
msgr-app



NOTE: Do not use the Radiator application on the Baseline scope customized behavior configuration as it has various permissions configured.

It is also possible to exclude Radiator from MFA requirement by excluding the users or user groups, or by selecting the other applications to the policy individually without using All resources. Excluding the users/user groups means that MFA is not required for the user at all, regardless of where they log in. Selecting all the applications except the Radiator application means the list may need to be manually updated from time to time to catch possible new Microsoft or other applications.

Radiator Policy Server configuration

After completing the previous steps you will need to update your Radiator Policy Server configuration. See Entra ID configuration guide (Radiator Entra ID configuration guide) for the full configuration steps.

The multi-tenant scenario differs from the single-tenant one only in which tenant the values come from:

- `TENANT ID` must point at the **Identity tenant**, because ROPC validates the user's password against the tenant where the account is a member. Use the Identity tenant Directory (tenant) ID.
- `APPLICATION ID` is the Application (client) ID from the application in the **Application tenant**.
- `APPLICATION SECRET` is the client secret value from the application in the **Application tenant**.

With these values, users who are members of the Identity tenant authenticate successfully through ROPC. Users who are only guests in the Identity tenant are not supported by ROPC and will not authenticate.

Optional: supporting both tenants

If you need users from both the Application tenant and the Identity tenant to authenticate at the same time (for example while accounts are being migrated), a single `TENANT ID` is not enough, because ROPC validates only members of the one tenant. To support both:

1. Grant admin consent for the multi-tenant application in both the Application tenant and the Identity tenant, so a service principal exists in each.
2. Make sure the MFA exception is configured on authenticating tenants.
3. Select the authenticating tenant's `vars.aaa.oauth2.token-url` dynamically based on the username's realm/domain, so each user is validated against the tenant where they are a member. For example, in the `entra-ad` or `entra-auth-mfa` examples available in the public radiator-radconfs repository the file 50_policies.radconf can be modified in following way before the backend call around row 57:

```
map aaa.identity.realm {
    "identitytenant.example.com" => {
        vars.aaa.oauth2.token-url =
"https://login.microsoftonline.com/<IDENTITY_TENANT_ID>/oauth2/v2.0/token";
    }
    any => {
        vars.aaa.oauth2.token-url =
"https://login.microsoftonline.com/<APPLICATION_TENANT_ID>/oauth2/v2.0/token";
    }
}
```

This works only while each user is a native member of the tenant they are routed to, as guests are not supported by ROPC. Once all accounts have moved to the Identity tenant, remove the above snippet from the 50_policies.radconf file and follow Radiator Entra ID configuration guide instructions on how to configure the Identity tenant `TENANT ID` in use.

Troubleshooting

The single-tenant Microsoft Entra ID App creation for Radiator Policy Server authentication guide lists the common access-token errors and their solutions that apply here as well. The errors below are the ones most often seen in the multi-tenant scenario.

Error: Acquiring access token failed

{"error":"invalid_grant","error_description":"AADSTS50034: The user account {EUII Hidden} does not exist in the xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx directory. To sign into this application, the account must be added to the directory

Solution

Check that the `TENANT ID` used is from the tenant in which the user is a member. In the multi-tenant scenario this usually means `TENANT ID` points at the Application tenant while the account is a member of the Identity tenant, or the reverse. Check also that `vars.aaa.oauth2.token-url` uses the tenant ID of the tenant where the account is a native member. A guest reference in the tenant is not enough, as ROPC does not support guest accounts.

Error Acquiring access token failed

{"error":"invalid_grant","error_description":"AADSTS65001: The user or administrator has not consented to use the application with ID 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx' named 'ms-multitenant'. Send an interactive authorization request for this user and resource.

Solution

The application has not been consented in the tenant that `TENANT ID` points at. Have that tenant's administrator run the admin consent URL described in "Grant admin consent in the Identity tenant". After consent, verify that the

application appears under Enterprise applications in that tenant.

Error: Acquiring access token failed

{"error":"unauthorized_client","error_description":"AADSTS700016: Application with identifier 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx' was not found in the directory

Solution

The service principal for the application does not exist in the tenant that `TENANT ID` points at, or the client ID is wrong. Confirm that admin consent has been granted in that tenant (the application must be visible under Enterprise applications) and that `APPLICATION ID` has the correct Application (client) ID from the Application tenant registration.