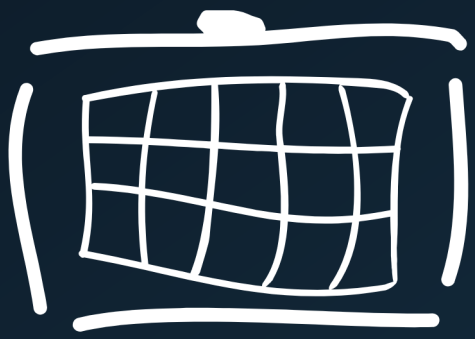


Radiator

CONFIGURATION GUIDE

Microsoft Entra ID App creation for Radiator Policy Server authentication

Date: 2026-11-16

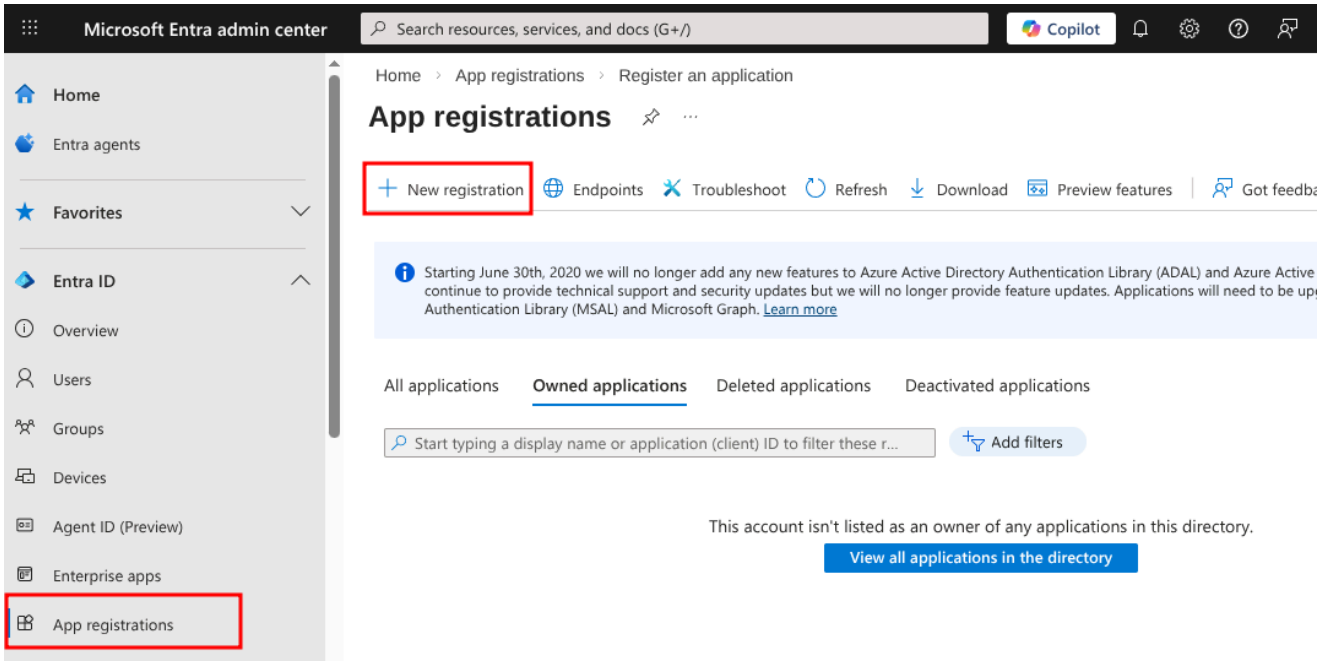
Creating an application to the Microsoft Entra ID is essential for establishing a trust relationship between Radiator Policy Server and the Microsoft identity platform. With the application you enable identity and access management (IAM) for Radiator Policy Server, allowing it to securely interact with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

Create the application

Create the app registration 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 correct tenant.
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. Select **Register** to complete the app registration.

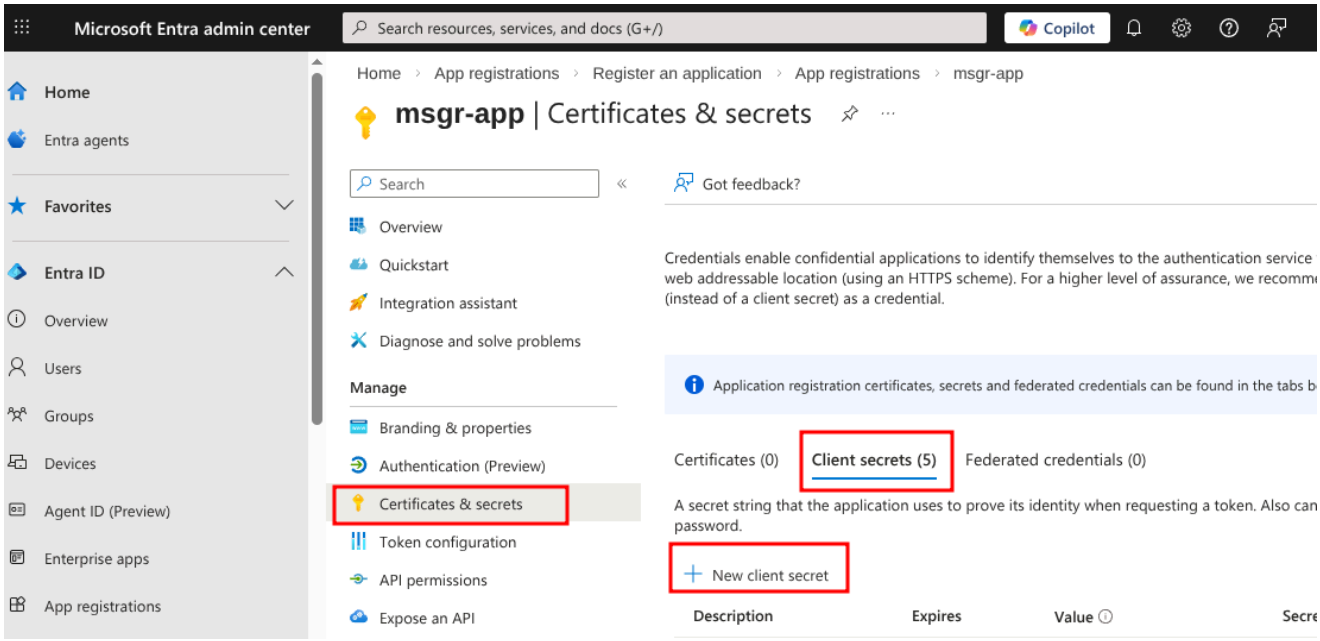


Add credentials

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.

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

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



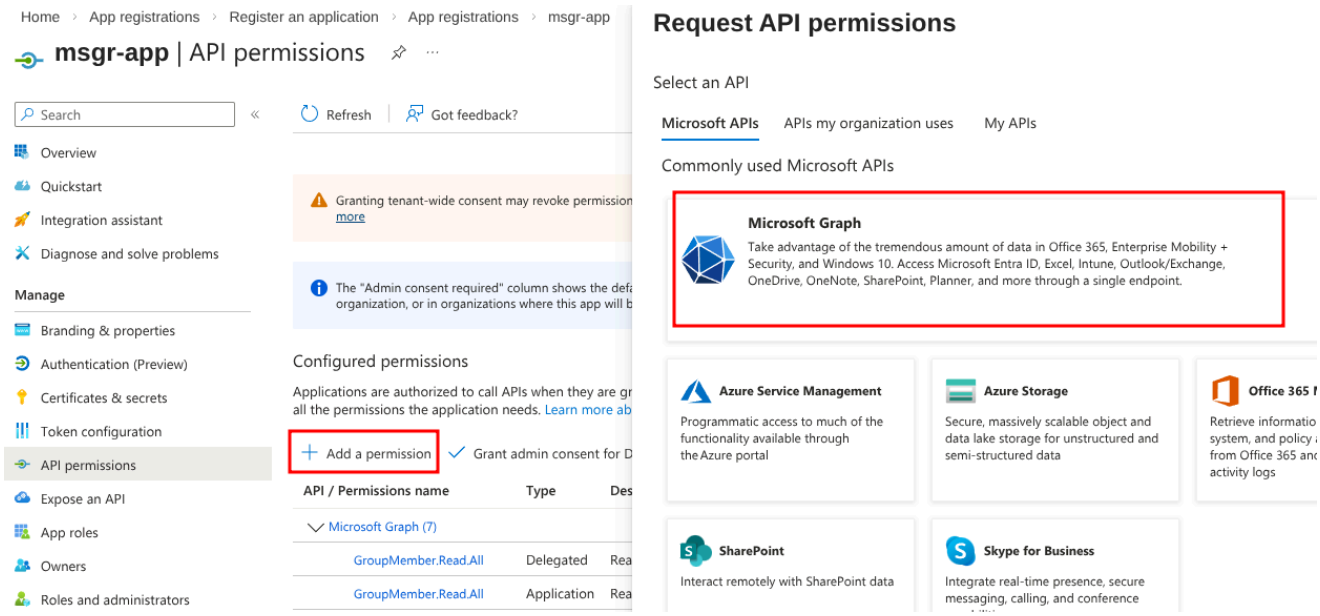
3. Add a description for your client secret.
4. Select an expiration for the secret or specify a custom lifetime.
5. Select **Add**.
6. *Record the secret's value* for use in Radiator Policy Server configuration (see Radiator Entra ID configuration guide). This secret value is *never displayed again*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

Set permissions

Resource Owner Password Credentials flow

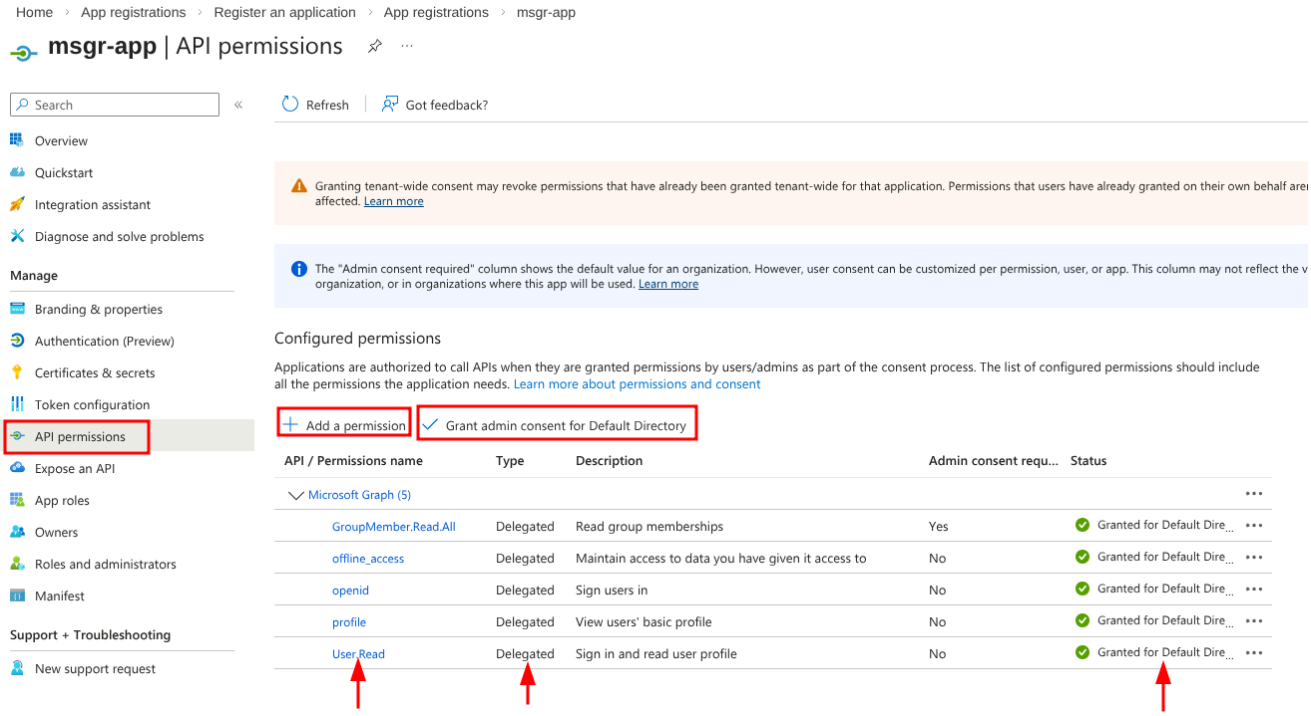
Radiator Policy Server also needs to access the data stored in Microsoft Graph. For Resource Owner Password Credentials (ROPC) flow configure delegated permission to Microsoft Graph to enable Radiator Policy Server to query the groups users belongs to as well as authenticating the user based on Microsoft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

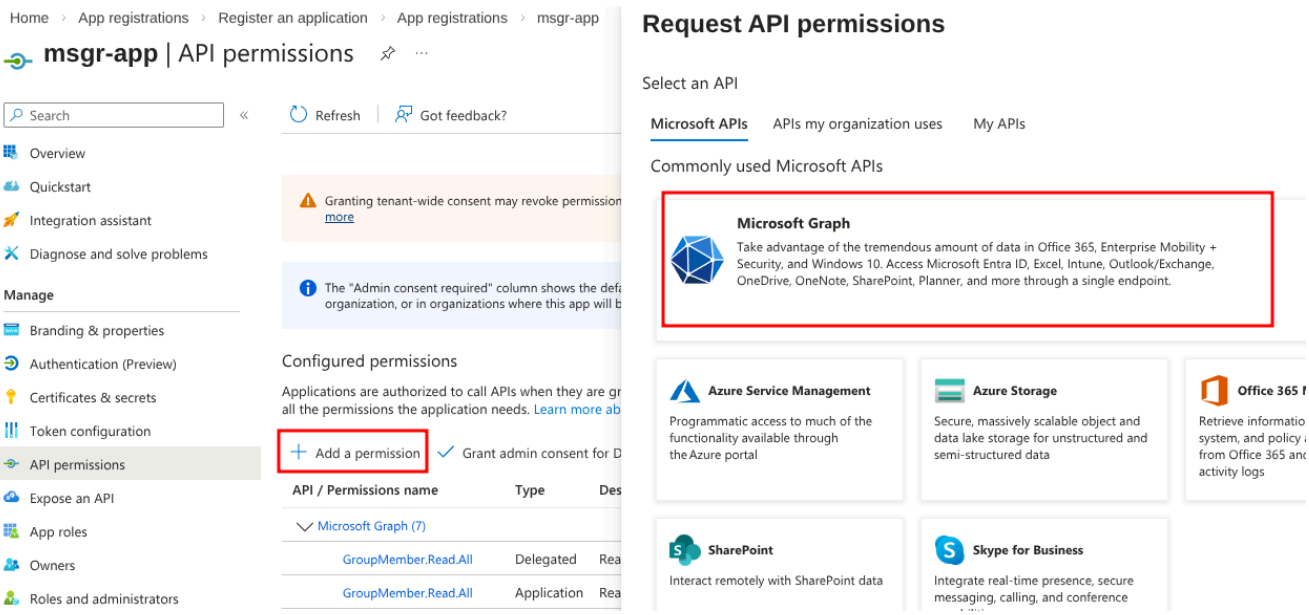


4. Some permissions require an Admin grant. The **Grant admin consent for {your tenant}** button allows an admin to grant admin consent to the permissions configured for the application. When you select the button, a dialog is shown requesting that you confirm the consent action. After granting consent, the permissions that required admin consent are shown as having consent granted.

Client credentials flow

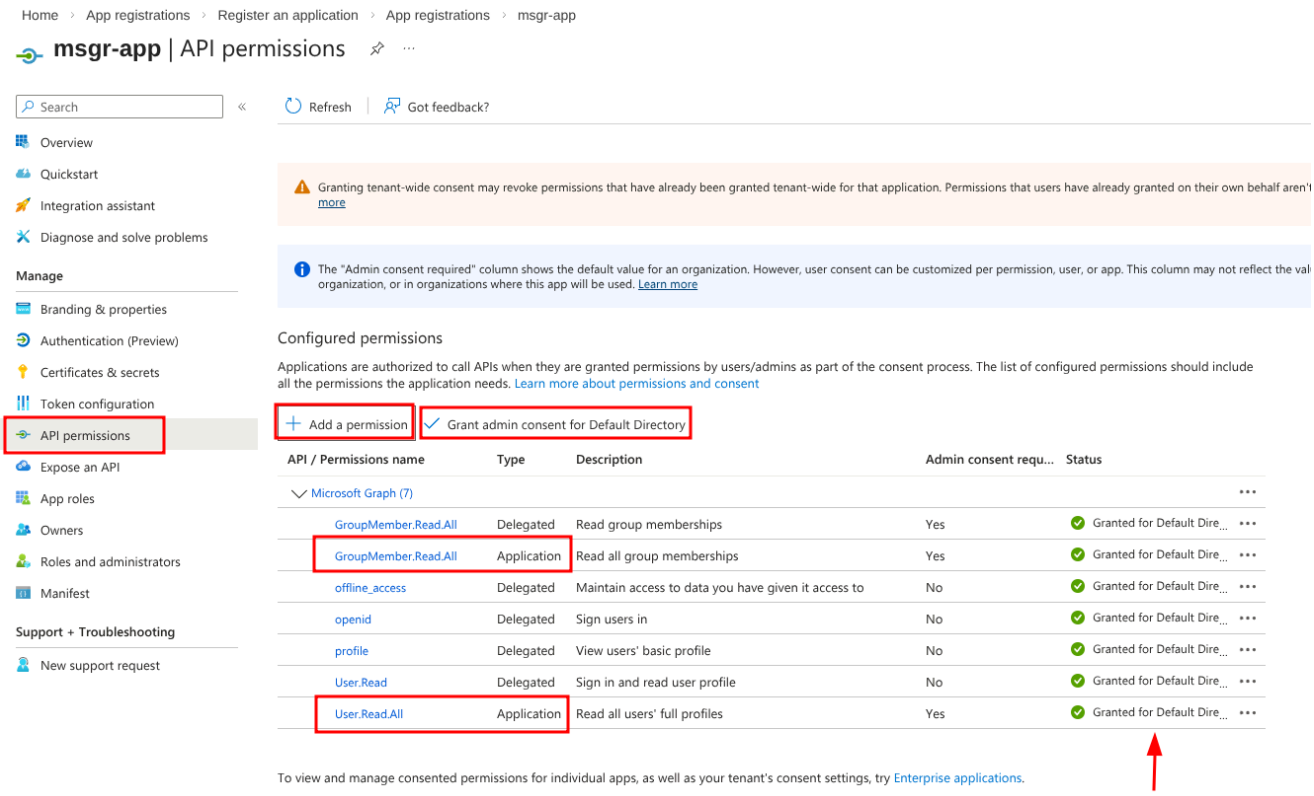
Permissions for Client credentials flow can be added to the same app used by the ROPC flow.

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. The **Grant admin consent for {your tenant}** button allows an admin to grant admin consent to the permissions configured for the application. When you select the button, a dialog is shown requesting that you confirm the consent action. After granting consent, the permissions that required admin consent are shown as having consent granted.

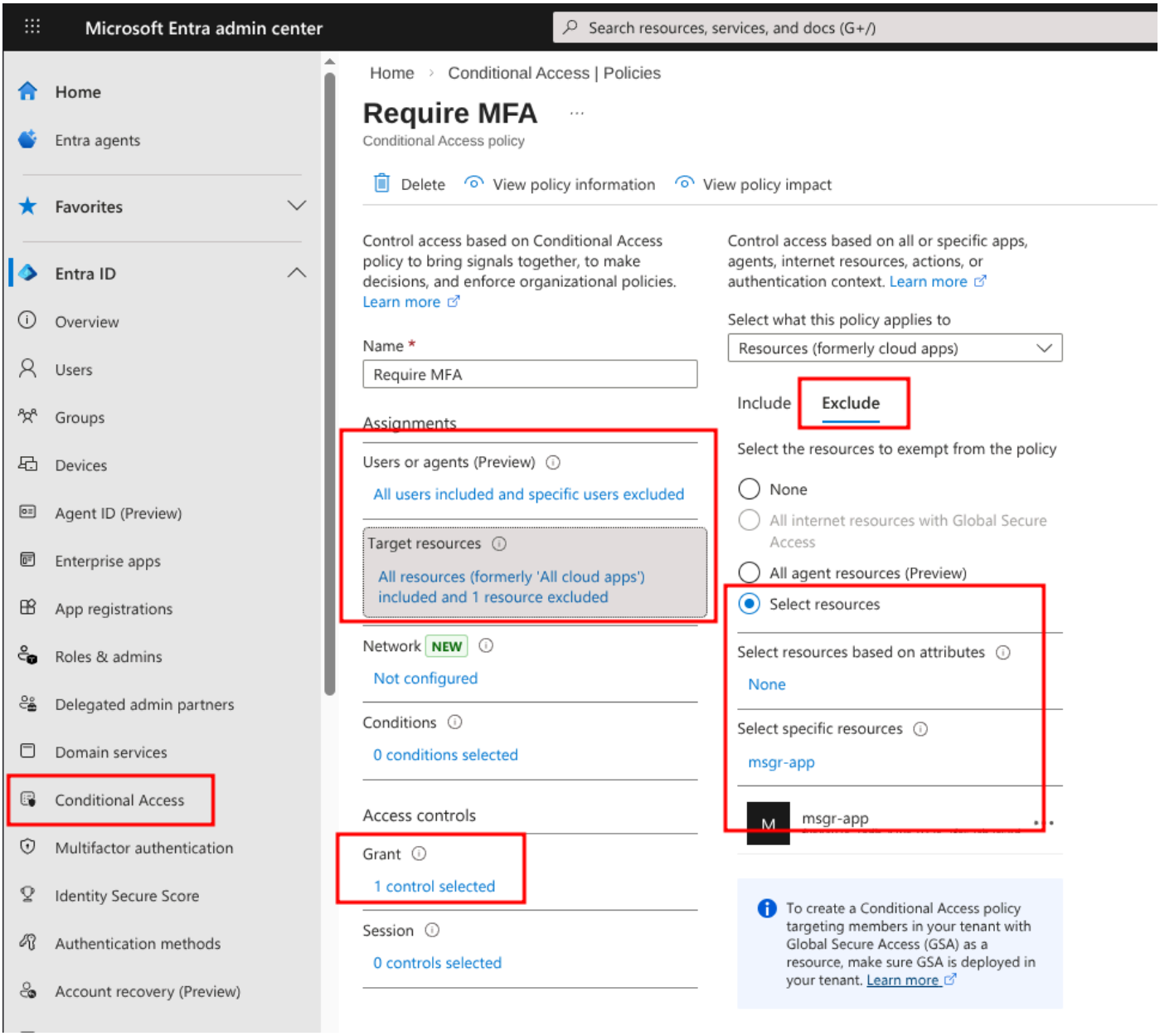
NOTE: It can take up to 60 minutes for the permissions to propagate into use.

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. 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.

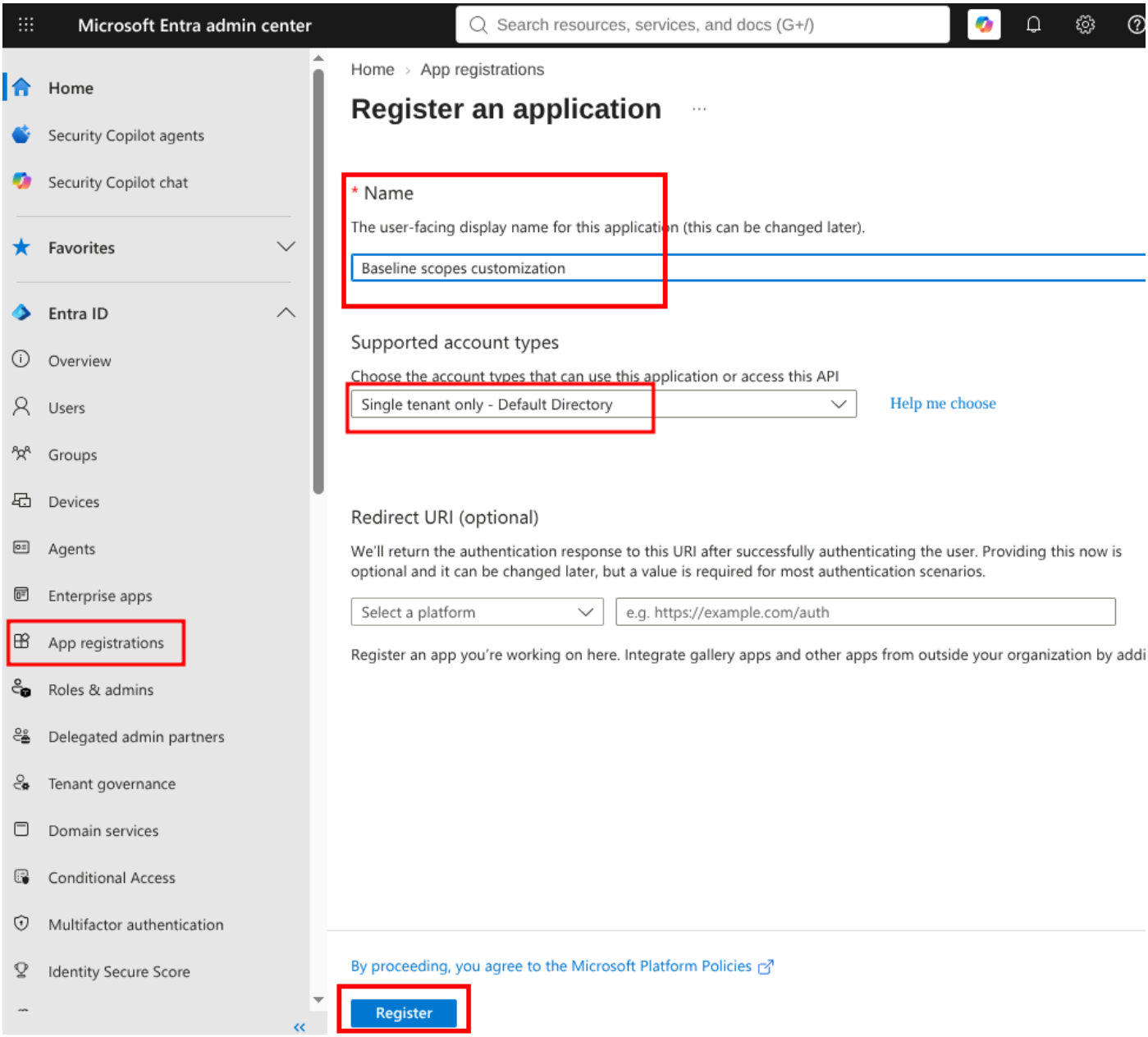
Using Conditional Access policies requires at minimum Microsoft Entra ID P1 licence and disabling organization security defaults. When disabling MFA via Conditional Access policy, users must not have Per-user MFA *enforced* or *enabled* in Entra portal (https://entra.microsoft.com > All users > Per-user 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.

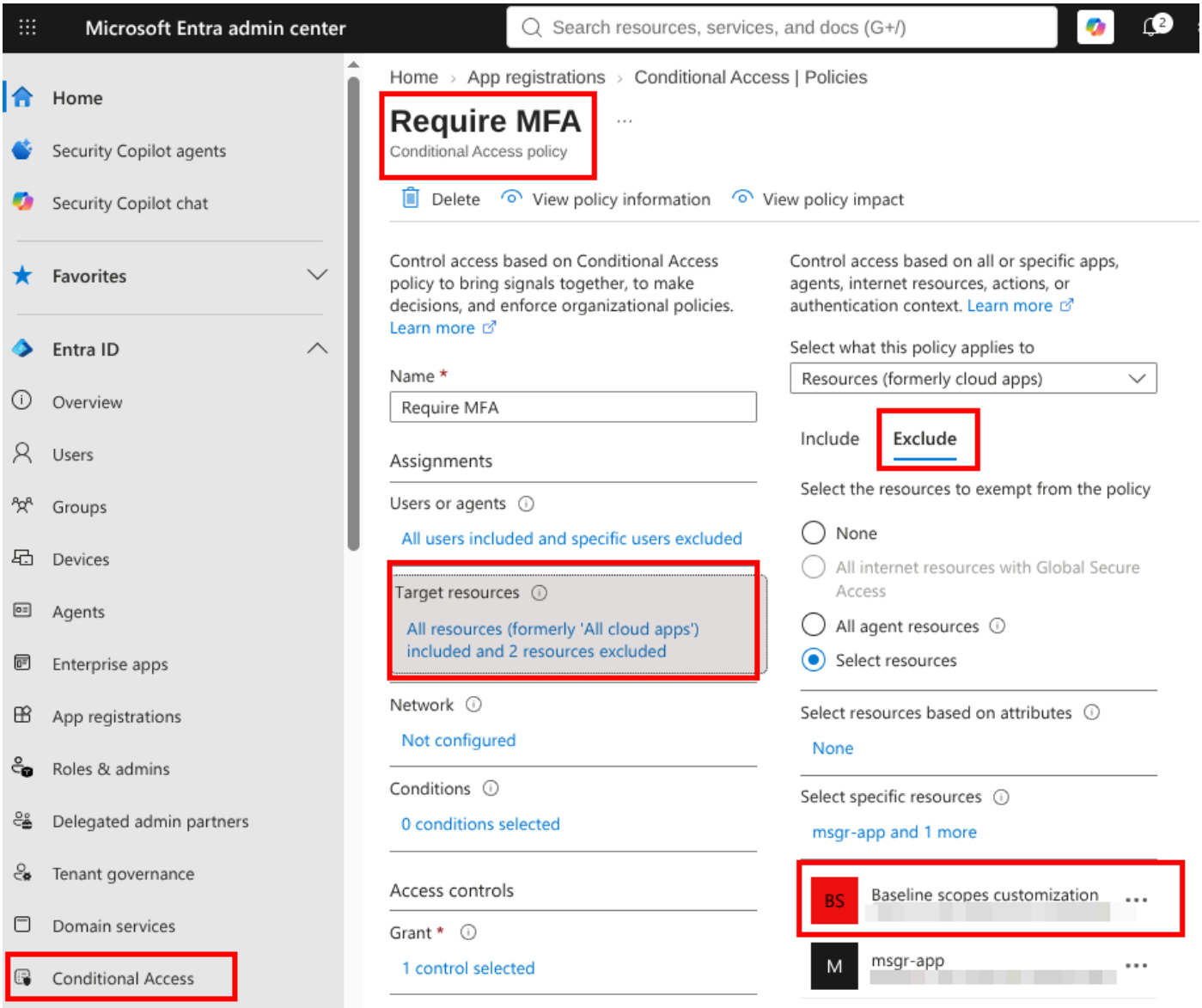
Example Conditional Access policy to require MFA except when using the application can be done for either all users or specific users, but the main thing is to exclude the created app when selecting Target resources. In the Grant section, “Require multifactor authentication” should be selected as control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

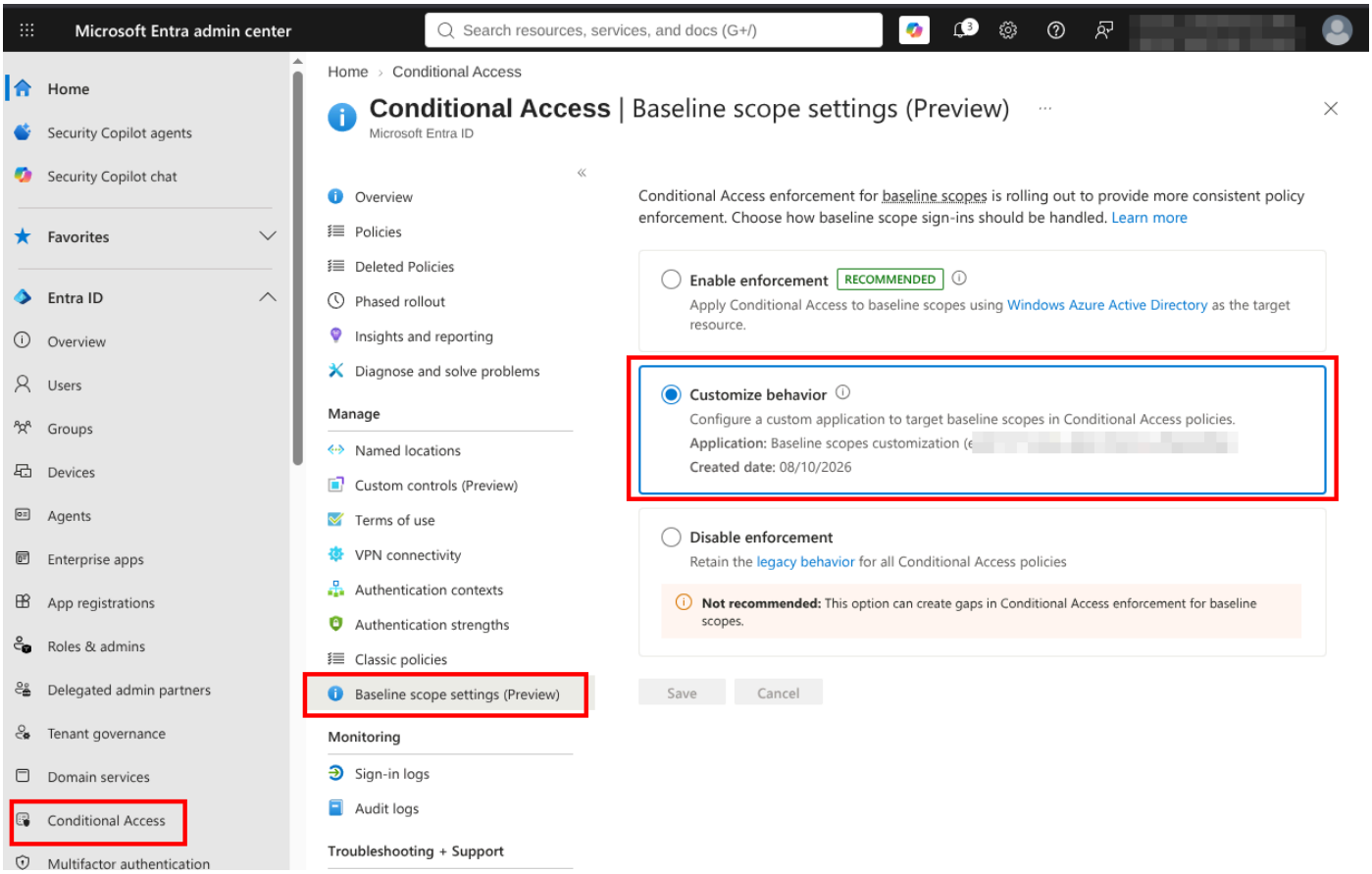


Recently, Microsoft has changed how the Conditional Access policies function when an application is excluded from a policy that otherwise targets All resources. Now the exclusion also takes into account which scopes Radiator uses with the application, and the behavior of the low-level baseline scopes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


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 more details.

Troubleshooting

Here is a collection of known errors shown on the Radiator Policy Server authentication log, and how they can be fixed either on Radiator Policy Server configuration or on Microsoft Entra ID. When Radiator Policy Server configuration is edited, remember to restart Radiator Policy Server after changes

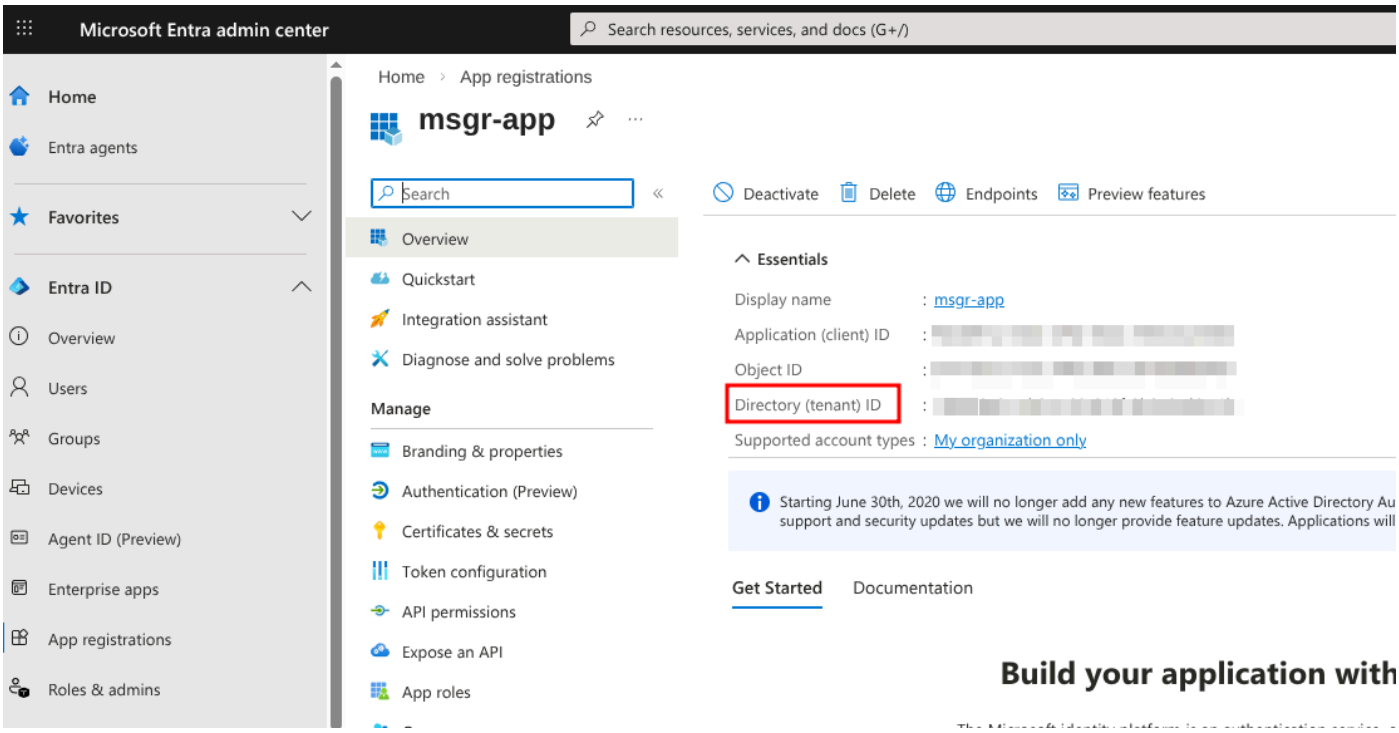
Error: Acquiring access token failed

{"error":"invalid_request","error_description":"AADSTS90002: Tenant

'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx' not found. Check to make sure you have the correct tenant ID and are signing into the correct cloud. Check with your subscription administrator, this may happen if there are no active subscriptions for the tenant.

Solution

Check that Radiator Policy Server configuration parameter *vars.aaa.oauth2.token-url* is correct, it should contain the tenant ID and not for example application ID



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-xxxxxxxxxxxx' named 'msgr-app'. Send an interactive authorization request for this user and resource.

Solution

There are multiple solutions to this error:

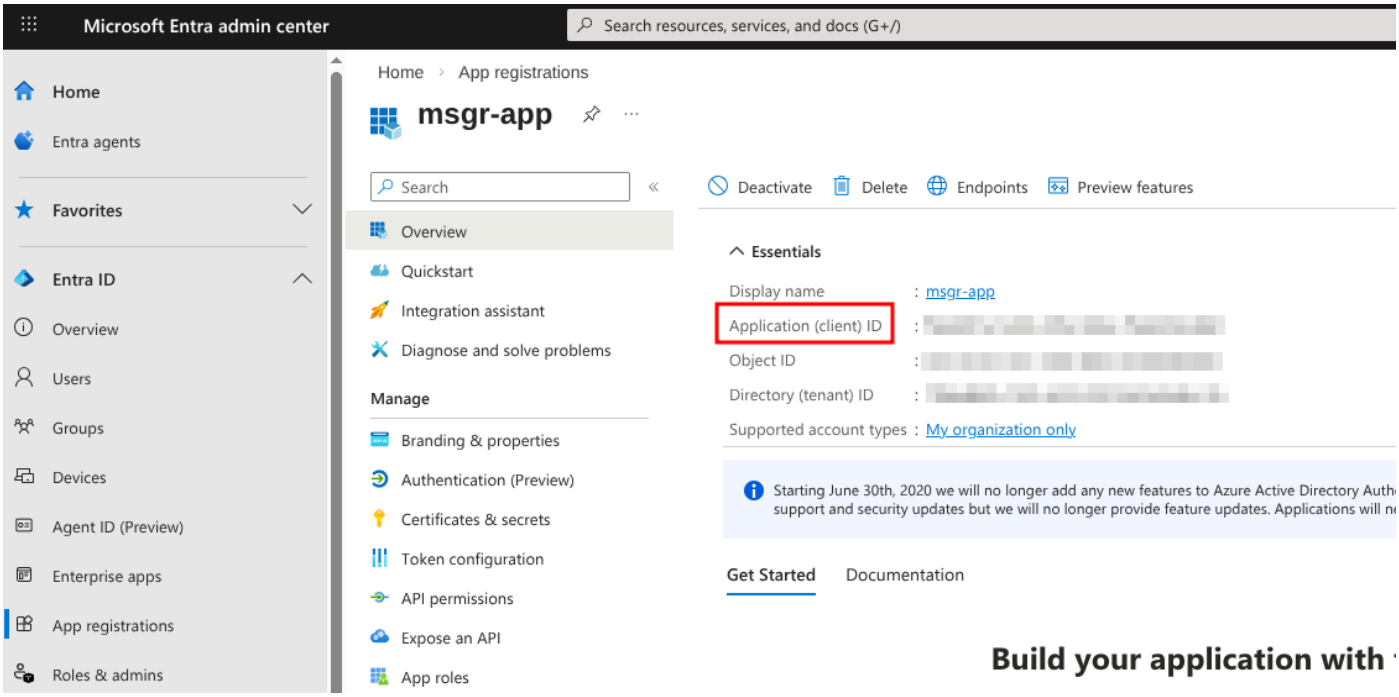
- Check the Microsoft Entra ID application permissions are as listed in "Set permissions" chapter
- Check administrator consent has been granted as shown in "Set permissions" chapter

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 'Default Directory'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant. Trace ID: 2bb28fbb-82ea-4365-b956-d88ad0d21d00

Solution

Check that Radiator Policy Server configuration and the *vars.aaa.oauth2.client* parameter has the correct application ID



Error: Acquiring access token failed

{"error":"invalid_grant","error_description":"AADSTS50126: Error validating credentials due to invalid username or password

Solution

Check the given password is correct

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 the username used is correct and exists in the Microsoft Entra ID

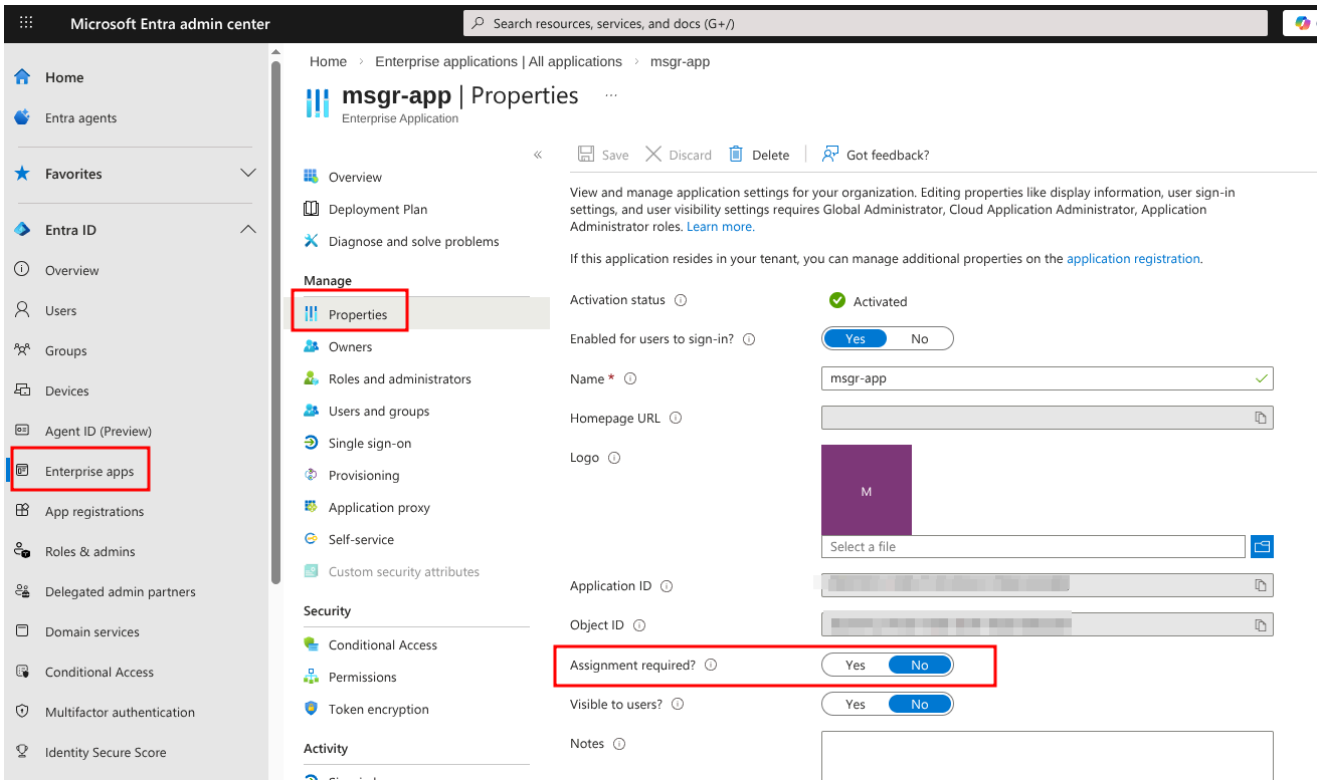
Error: Acquiring access token failed

{"error":"invalid_grant","error_description":"AADSTS50105: Your administrator has configured the application msgr-ent ('xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx') to block users unless they are specifically granted ('assigned') access to the application. The signed in user '{EUII Hidden}' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

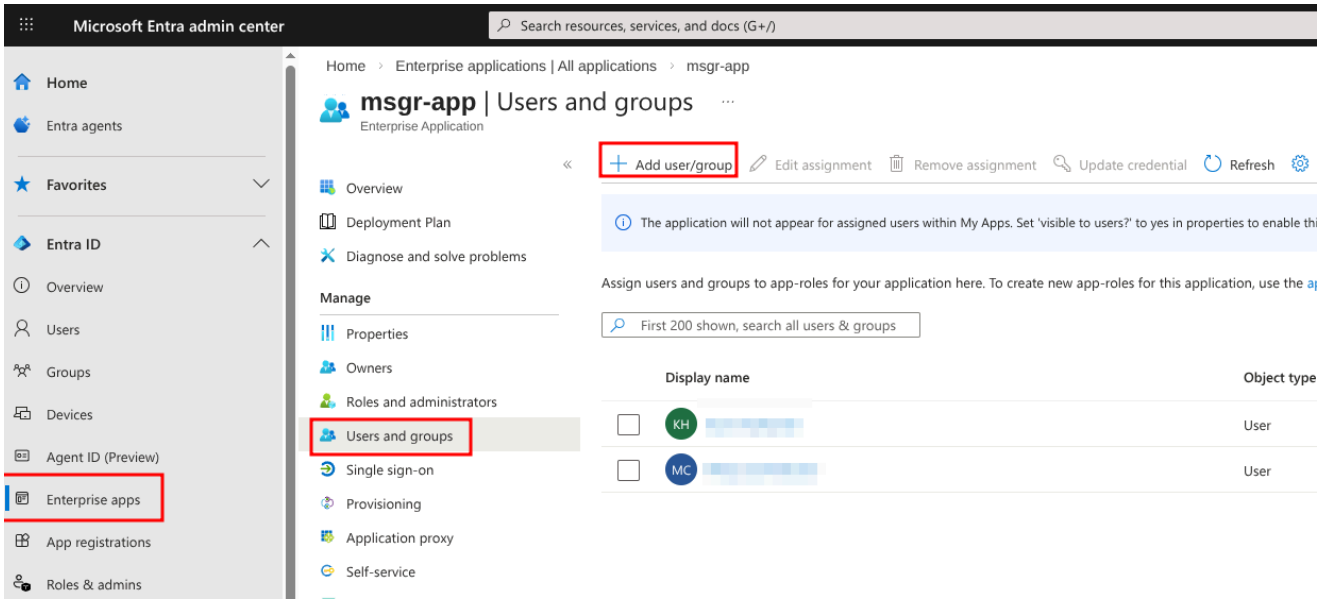
Solution

This error is usually only appearing if the application has been created as an enterprise application and the Assignment required has been set to yes. There are multiple solutions to this error:

- Check the Microsoft Entra ID application permissions are as listed in "Set permissions" chapter
- Check administrator consent has been granted as shown in "Set permissions" chapter
- Set the Assignment required option as No



- If the Assignment required cannot be set to No, then check the user has been assigned access either directly or via group

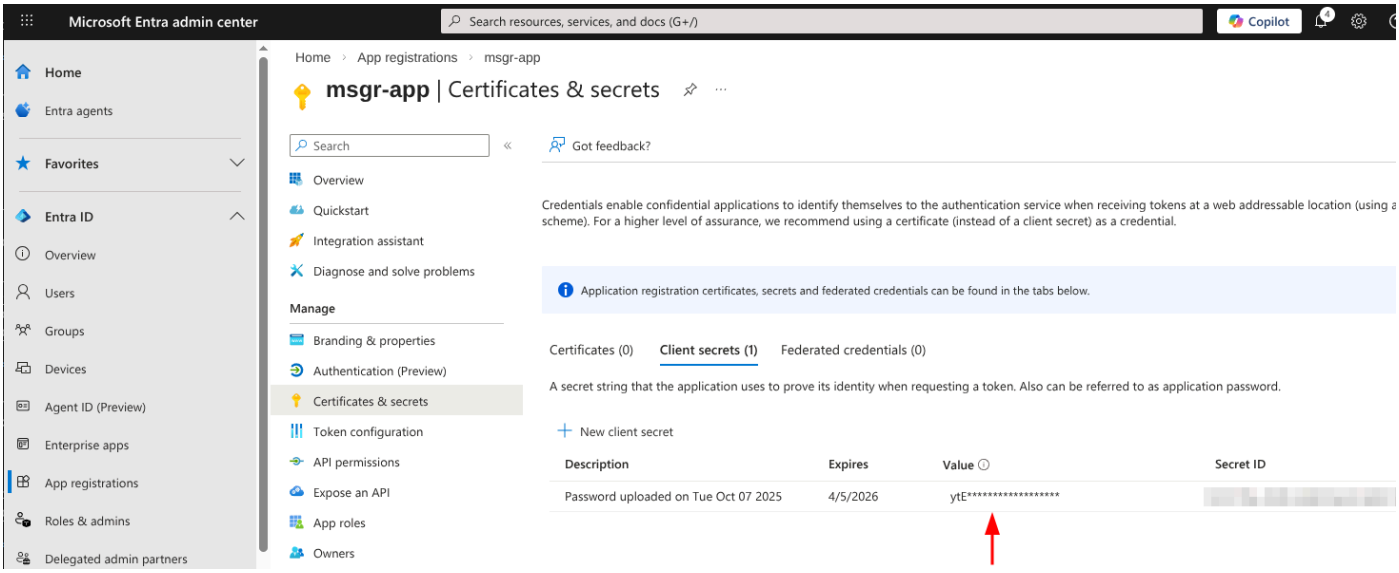


Error: Acquiring access token failed

{"error":"invalid_client","error_description":"AADSTS7000215: Invalid client secret provided. Ensure the secret being sent in the request is the client secret value, not the client secret ID, for a secret added to app 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx'

Solution

Check the Radiator Policy Server configuration and the *vars.aaa.oauth2.secret* parameter has the secret value (not secret ID) from the correct application.

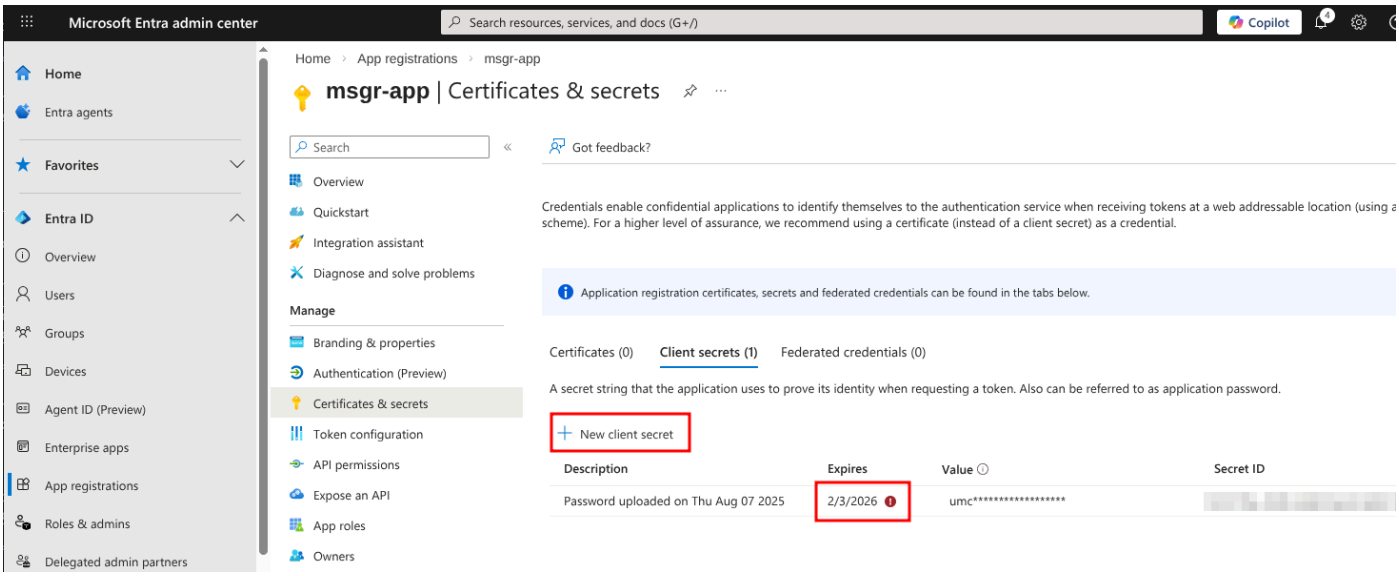


Error: Acquiring access token failed

{"error":"invalid_client","error_description":"AADSTS7000222: The provided client secret keys for app 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx' are expired. Visit the Azure portal to create new keys for your app: https://aka.ms/NewClientSecret, or consider using certificate credentials for added security: https://aka.ms/certCreds.

Solution

The secret defined on the Microsoft Entra ID has expired. Create a new secret and update it to the Radiator Policy Server configuration *vars.aaa.oauth2.secret* parameter.



Error: Acquiring access token failed

{"error":"invalid_grant","error_description":"AADSTS50079: Due to a configuration change made by your administrator, or because you moved to a new location, you must enroll in multi-factor authentication to access '00000003-0000-0000-c000-000000000000'

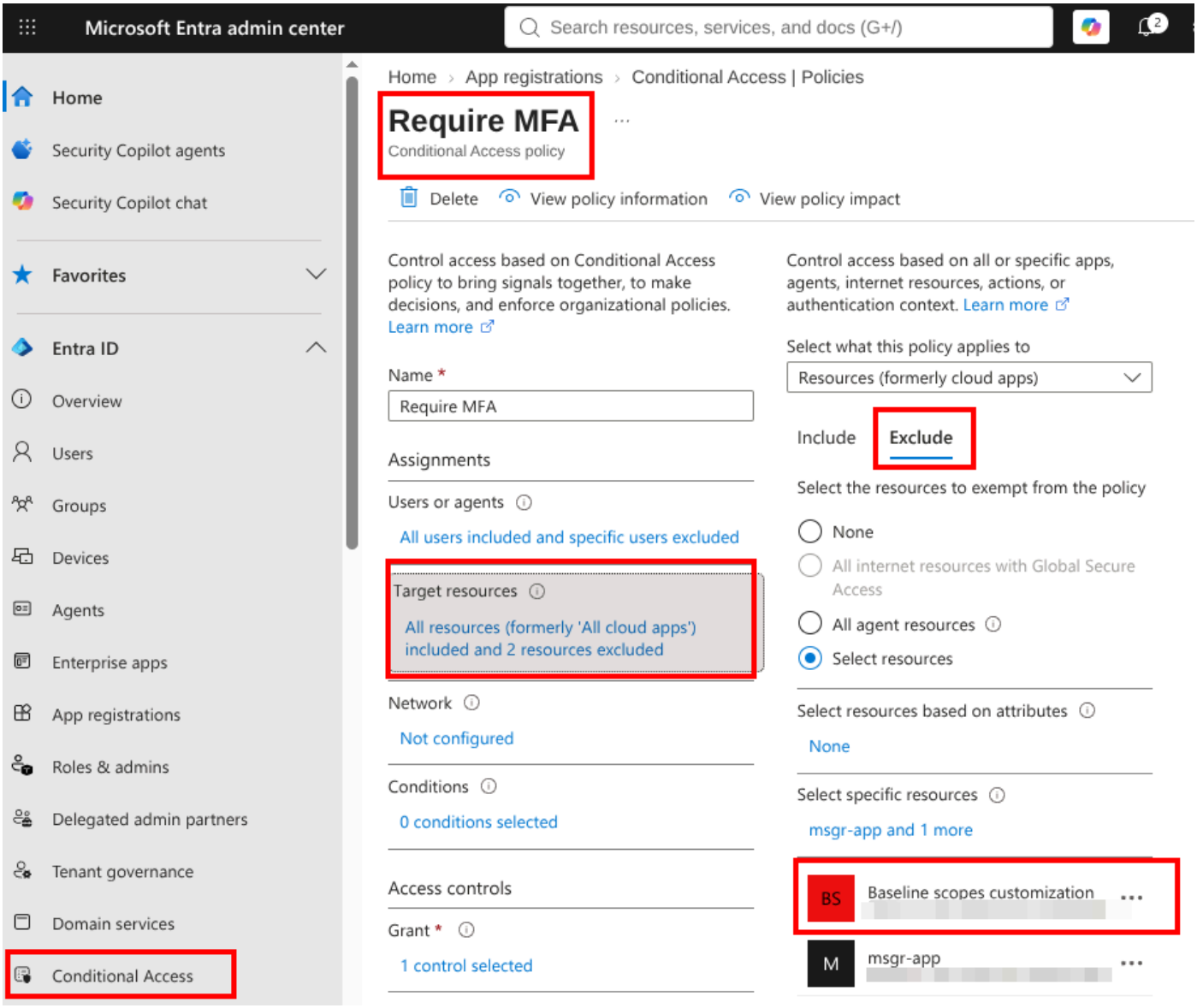
Solution

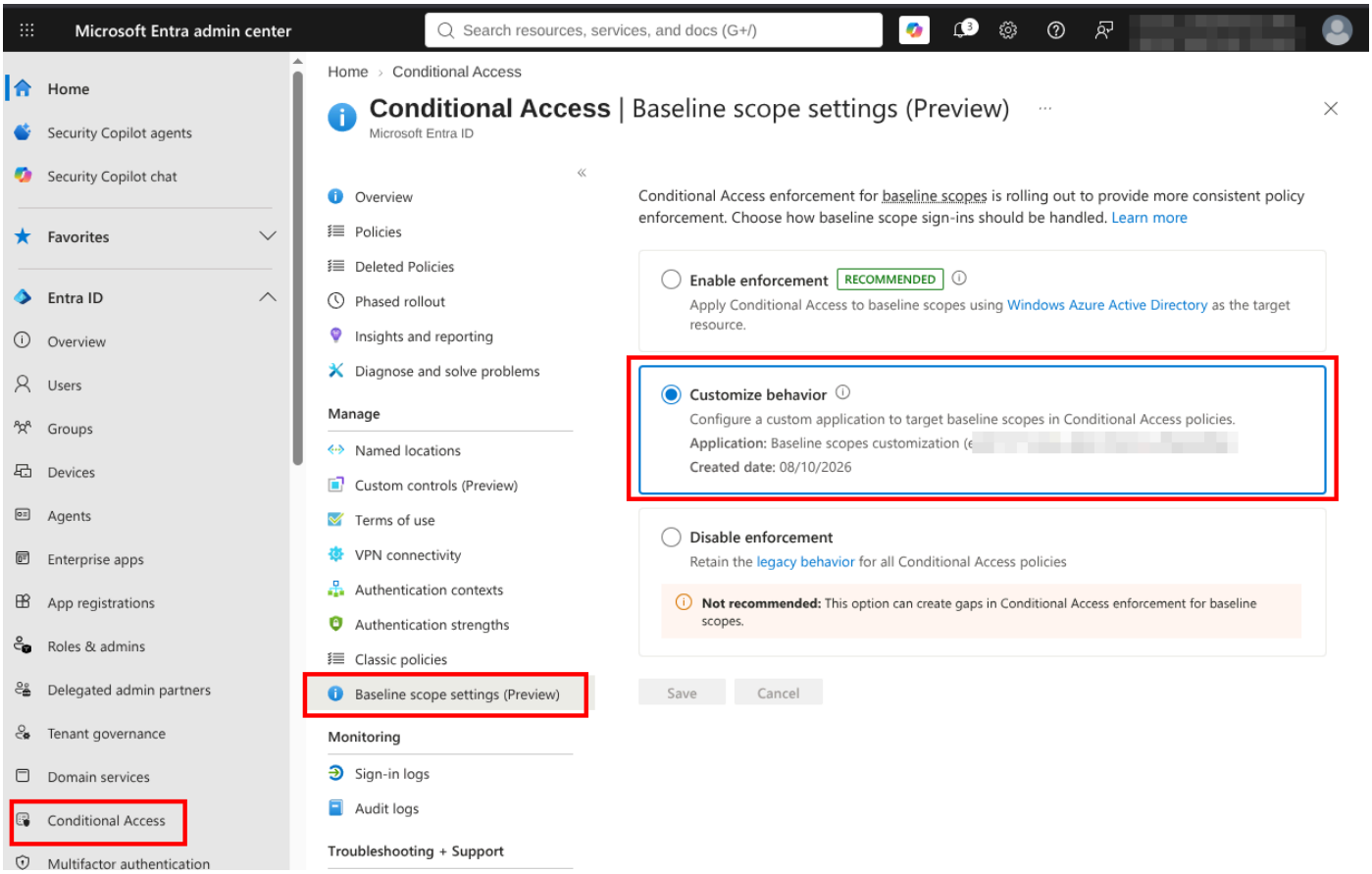
Microsoft Entra ID administrator has enforced the multi-factor authentication for the user trying to authenticate, the Security defaults are enabled or Conditional Access Baseline scope settings are not customized. Possible solutions are:

- Disable the multi-factor authentication for the user from the Entra portal https://entra.microsoft.com > All users > Per-user MFA
- Disable the multi-factor authentication from all users https://entra.microsoft.com > Overview > Properties > Security defaults and take Conditional Access Policies into use
- Disable multi-factor authentication requirement from Conditional Access policy https://entra.microsoft.com > Conditional Access or create app passwords for the user: https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-app-passwords
- Use Customized behavior on Conditional Access Baseline scope settings: https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-enforcement-resource-exclusions#customize-behavior

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 Entra portal (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. In the same policy, exclude also the application used for the Baseline scope customization.





Error: Acquiring access token failed

{"error":"invalid_grant","error_description":"AADSTS53003: Access has been blocked by Conditional Access policies. The access policy does not allow token issuance.

Solution

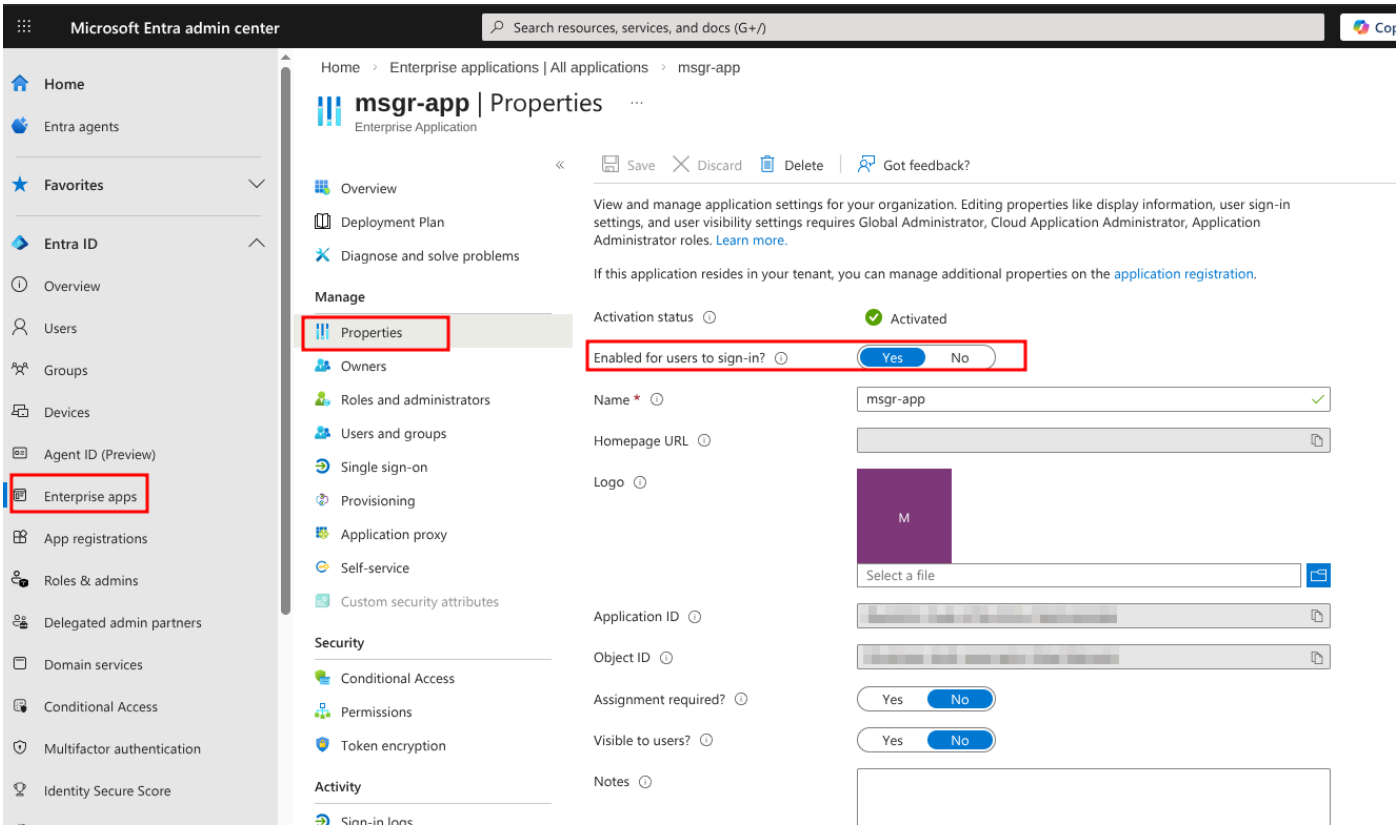
Check the Conditional Access Policies on Microsoft Entra ID and allow access for example to the target application

Error: Acquiring access token failed

{"error":"unauthorized_client","error_description":"AADSTS7000112: Application 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx'(msgr-app) is disabled

Solution

Check that the Enterprise Application Properties allow users to sign in with the app from the Microsoft Entra ID



Acquiring access token failed: error sending request for url

Acquiring access token failed: error sending request for url (https://login.microsoftonline.com/\<tenant-ID>/oauth2/v2.0/token): operation timed out

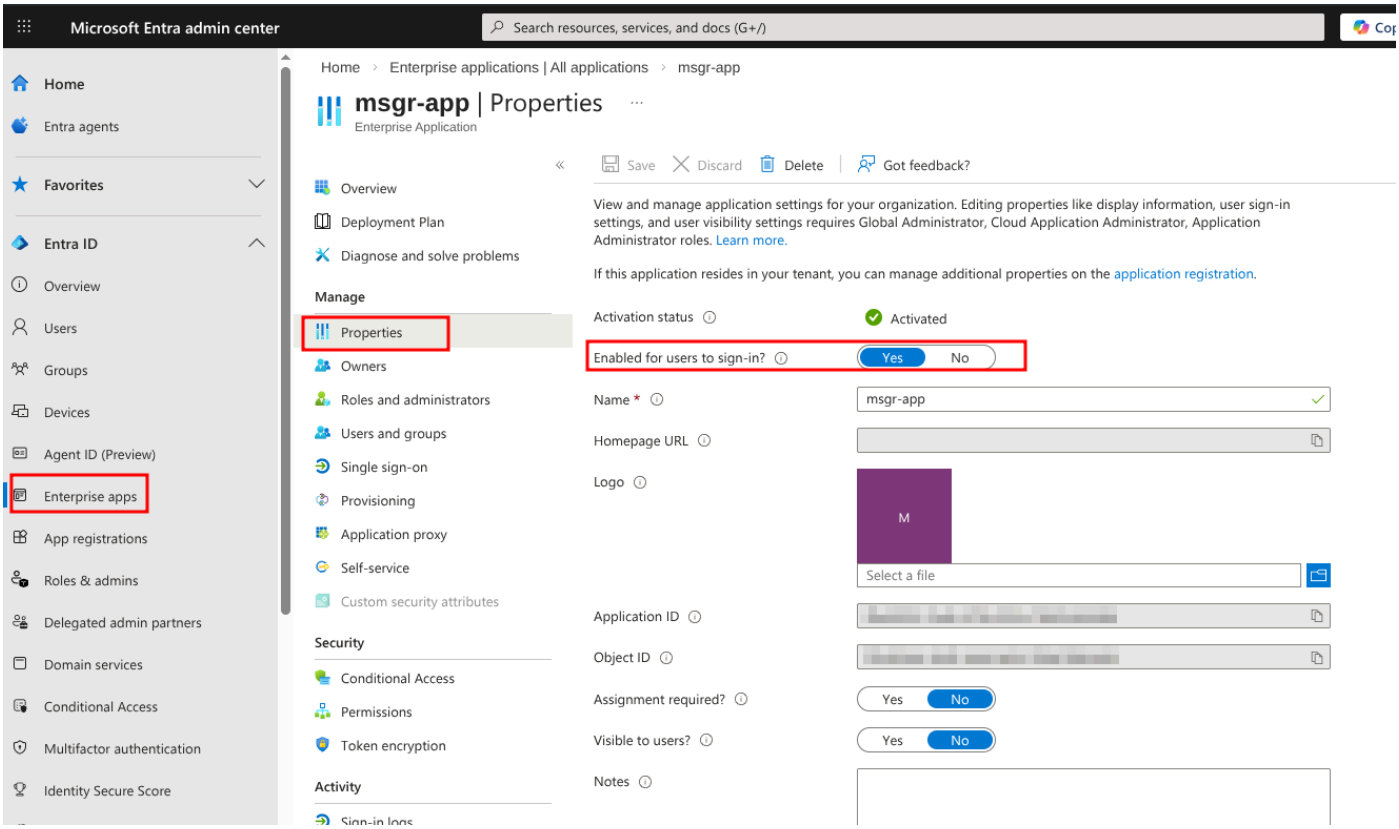
Additionally there are no sign-in tries visible on the Microsoft Entra Sign-in logs.

Solution

This error can happen for example if Microsoft Entra ID P2 license has been enabled and related to it ApplicationManagement does automatic service principal updates. These updates are visible for example on the Microsoft Entra ID directory Audit logs:

2/23/26, 2:58:00 PM	Core Directory	ApplicationManagement	Update service principal	Success
2/23/26, 2:57:57 PM	Core Directory	ApplicationManagement	Update service principal	Success
2/23/26, 2:57:56 PM	Core Directory	ApplicationManagement	Update service principal	Success

To get the application functionality back, try to disable and enable the Enterprise Application from Properties:



Error: No matching realm found

Default Handler: No matching realm found.

Solution

Check that Radiator Policy Server configuration and the username trying to authenticate have the same realm: *user@realm* and handler with condition like *aaa.identity.realm == "realm";*

Error: None of user groups matched

None of user groups matched, so the authentication is rejected

Solution

Radiator Policy Server configuration file 50_policies.conf defines groups that the user should belong to. This group membership is checked from the Microsoft Entra ID, and if the user does not belong to any of the groups listed on the Radiator Policy Server configuration, the above error is shown.