PROXY Networks

Integrating Microsoft Entra ID Authentication with PROXY Pro RAS

The PROXY Pro RAS Edition includes support for communicating directly to Microsoft Entra ID tenant services for authentication and this guide covers the steps to set this up. These instructions apply for both the on-premise and hosted versions, and we will assume your organization already has an Entra ID tenant. For instructions on how to create a new Entra ID, we recommend following Microsoft's guidelines.

To begin, log into your management portal at **portal.azure.com,** click **Entra ID**, and click **Manage** to expand so that **Groups** becomes visible.

1) Creating the two groups to be used with PROXY Pro RAS

Provide information for the following fields to create a group:

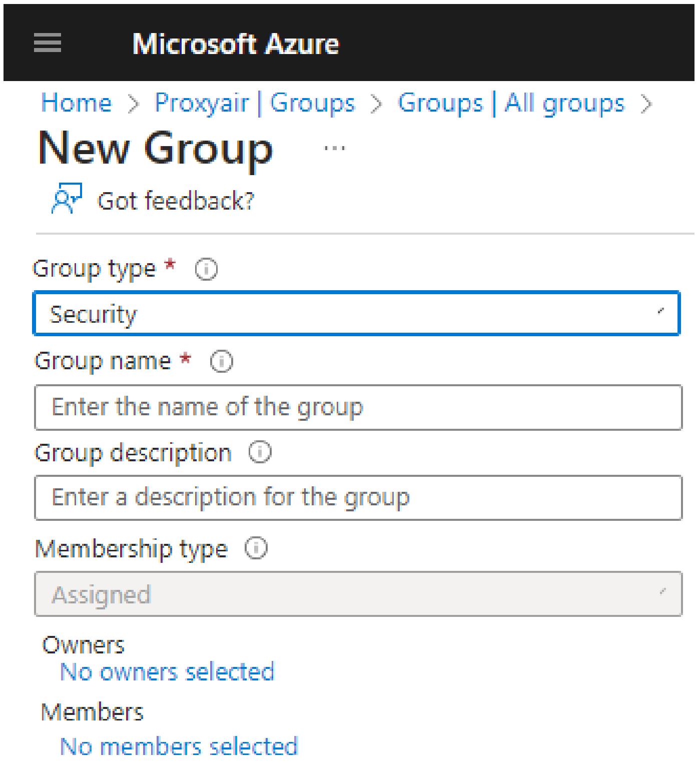
- Group type: Security
- Group name: **PROXY Pro Administrators** (or similar)
- Description: PROXY Pro Administrators group
- Membership type: Assigned (Leave alone)
- Ignore Members section at this point.

After successful group creation, close the Group panel. The Create button at the bottom will get enabled. Click to finish.

Repeat once again for the Masters group.

- Group type: Security
- Group name: **PROXY Pro Masters** (or similar)
- Description: PROXY Pro Masters group
- Membership type: Assigned (Leave alone)
- Ignore Members section at this point.

After successful group creation, close the Group panel.



New Group

Group type * Security

Group name * Enter the name of the group

Group description Enter a description for the group

Membership type Assigned

Owners No owners selected

Members No members selected

2) Adding users to the two PROXY Pro groups

When populating the two groups, we would recommend adding yourself to the PROXY Pro Administrators group. For those that utilize two accounts, a superuser account and a regular, non-admin account we typically recommend designating the superuser account as an Administrative account type in Proxy, and the day-to-day account as a Master account type. Click the **PROXY Pro Administrators Group** name, expand Manage, **Members**, click **Add members**.

a. Add yourself to this group, along with any others that should have Administrative rights within Proxy. Note that if there is a superuser version of account(s), general best practice would be to designate it as Administrative, and also, designate your day-to-day non-admin account as a Master account type in the next step. Your licensing may include a single Administrative account license, but many Master account licenses, so keep this in mind when populating groups.

b. Click **Select** to confirm.

c. Repeat the process for the **PROXY Pro Masters Group**, populating it with all other (non-admin) PROXY Pro Master users.

3) Inviting a user external to your own Entra ID tenant

a. A user external to your organization can be invited to your tenant, and then can be added to a Proxy group: https://learn.microsoft.com/en-us/entra/external-id/b2b-quickstart-add-guest-users-portal

4) App Registration (Entra ID -> Expand Manage -> App Registration)

a. Provide a **Name** for the application (PROXY Pro).

b. For Supported Account Types, use the radio button for **Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts**

c. For the **Redirect URI**, enter the address of your web console and add /pim/core/ to the end, with the trailing slash.

   a. It should look like this: https://support.yourwebsite.com/pim/core/

d. For the drop-down with the text "Select a platform", choose **Web**

e. Click **Register**.

f. Under **Authentication** hit the checkbox for **ID Tokens** and click **Save.**

5) Certificates & Secrets

a. From the **Certificates & secrets** page click **New client secret.**

b. Provide a descriptive name in the **Description** field.

c. Set the expiration to 2 years. This will need to be revisited in 2 years & updated in the PIM (step 9b).

d. **IMPORTANT:** Copy the **Value** string to Notepad or similar as this is needed for the PIM settings later. You cannot retrieve the value after this time so it's critical that this is copied to a safe place now.

6) API Permissions

a. From **API permissions**, click **Add a Permission.**

b. Click **Microsoft Graph** and click **Application Permissions.**

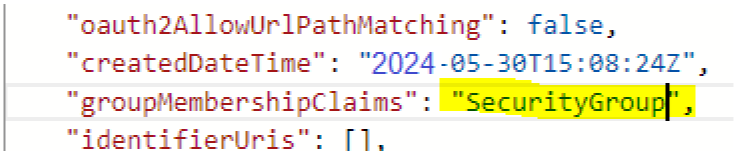
   a. Expand **Directory** and check the box for **Directory.Read.All (Read Directory Data).**

   b. Click **Add Permission**

   c. Click the **Grant admin consent for [Your Proxy Web Console]** button

7) Manifest

a. Click the **Manifest** button to edit. Replace the null with "SecurityGroup", so the line reads "groupMembershipClaims": "SecurityGroup", like in the below screen snippet:



```
    "oauth2AllowUrlPathMatching": false,
    "createdDateTime": "2024-05-30T15:08:24Z",
    "groupMembershipClaims": "SecurityGroup",
    "identifierUris": [],
```

b. Click **Save** on the top and close the Edit Manifest panel.

8) Enterprise applications (Entra ID -> Enterprise applications)

a) Click your application name.

b) Click **Permissions.**

c) Click **Grant admin consent for MyDirectory.**

d) A window appears to ask you to accept permissions on behalf of users of your organization. The two items listed underneath "This app would like to:" should be:

- Read Directory Data.
- Sign in and read user profile.

e) Click **Accept**

9) Updating Proxy Identity Manager (PIM) Settings

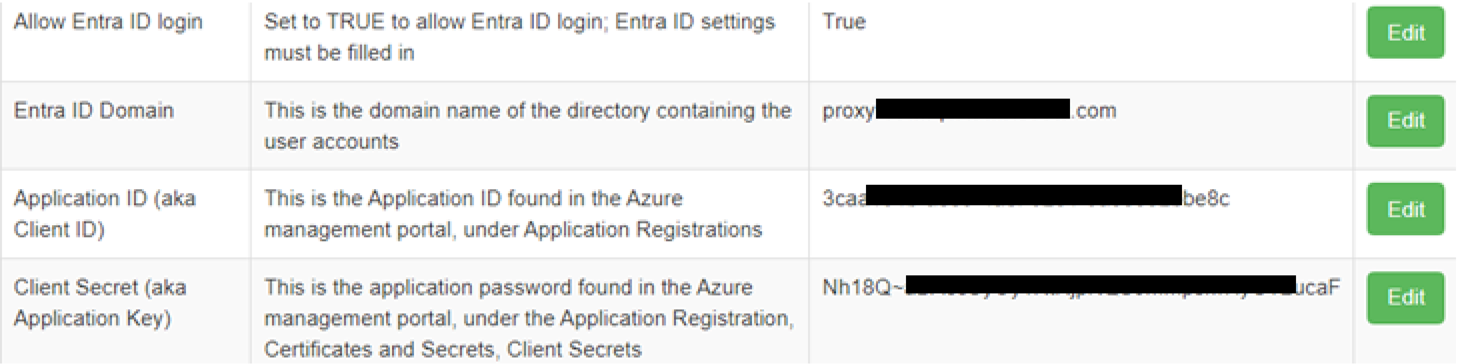
a. Visit your Proxy Identity Manager which can be accessed in either manner:

- Visit the URL directly which would look like this: https://support.yourwebsite.com/pim/settings
- Visit the PIM through the Proxy Web Console -> Gateway tab -> Network sub-tab; scroll to the bottom to find the hyperlink to the PROXY Pro Identity Manager.

b. Within the Proxy Identity Manager, edit the following:

- Allow Entra ID login: Set to True.
- Entra ID Domain: Domain name (example: MyDirectory.onmicrosoft.com).
- Entra ID Application ID (Client ID): Shown on App Registration -> All Applications; search for the PROXY Pro app.
- Entra ID Client Secret: The value from the Certificates & secret step; the value was pasted into Notepad earlier.

Below are the Entra ID values that must be plugged into the PIM. Click **Apply** and **OK** to save the changes.



Allow Entra ID login	Set to TRUE to allow Entra ID login; Entra ID settings must be filled in	True	Edit
Entra ID Domain	This is the domain name of the directory containing the user accounts	proxy[redacted].com	Edit
Application ID (aka Client ID)	This is the Application ID found in the Azure management portal, under Application Registrations	3caa[redacted]be8c	Edit
Client Secret (aka Application Key)	This is the application password found in the Azure management portal, under the Application Registration, Certificates and Secrets, Client Secrets	Nh18Q~[redacted]ucaF	Edit

10) Importing Entra ID Groups to the Proxy Web Console's "Accounts" tab

a. Log into the Proxy Web Console as an Administrative user and visit the Accounts tab.

b. Click the + button, click the Group radio button, pick the Entra ID from the Location drop-down, input the Administrative group name, click OK and Save.

c. Click the + button to add the second new group created in step 1.

d. Select the Group radio button, the Entra ID from the Location drop-down, input the Master group name in the field.

e. Select which Managed Hosts groups the Master may access, click OK and Save.

11) Logging into the Proxy Web Console with Entra ID for the First Time & Final Cleanup

a. Log out of the Proxy Web Console, if you were already logged in. Visit the landing page and click LOGIN.

b. The right-hand side of the page will now list your tenant name – click it to be prompted to authenticate. Note that if you are already logged into the computer as a user that is a member of the PROXY Pro Admins group, you will likely not be prompted and instead be immediately logged into the console.

c. Once successfully logged into the Proxy Web Console with your Entra ID identity, we recommend performing the following two minor cleanup tasks:

   i. Remove any non-Entra ID accounts from the Accounts tab (if applicable). Visit the Accounts tab, and for any users or groups listed not belonging to the Entra ID such as local accounts, click **Remove**.

   ii. Set authentication to Entra / SSO by visiting the PIM page, look for “Allow local Active Directory login” and set this to **FALSE**, then hit **Apply** to save the change. These steps ensure that logins are possible *only* with user accounts that are members of the two Entra ID groups created for this.

Additional Considerations

1) PROXY v10.4 and later: PROXY Pro Server v10.4 and later no longer use the “Azure Active Directory Graph” API provided by Microsoft, and instead uses the “Microsoft Graph” API. When configured for Azure AD integration, the PROXY Pro Identity Manager makes HTTPS requests to various Microsoft services. The URLs that it accesses are:

https://graph.microsoft.com/ and https://login.microsoftonline.com/

2) Some customers have users who are members of more than 200 AAD groups, which can lead to long processing times or login failures. We recommend following these steps to solve this problem; this requires an Azure Premium plan:

a. Click on “**Microsoft Entra ID**” in the left nav
b. Click on “**App Registrations**” under “Manage” in the left nav
c. Select the “**All Applications**” tab on that page to see the registered PROXY app, and click on the PROXY App
d. Click on “**Token configuration**” under “Manage” in the left nav
e. Click on the "**+ Add groups claim**" on the page
f. Check the box for "**Groups assigned to the application...**" (all others unchecked) and click Save
g. Click "**Manifest**" under Manage in the left navigation. Make sure the line for "groupMembershipClaims" reads: **"groupMembershipClaims": "ApplicationGroup",**
h. Dismiss that to return to the Home > directory page
i. Click on “**Enterprise Applications**” under “Manage” in the left nav
j. Click on the registered PROXY app
k. Click “**Users and Groups**” under “Manage” in the left nav
l. Click on “**Add user/group**” on top and select the Groups that are imported, or will be imported, into the PROXY Pro Web Console. Note that you will need a premium Azure subscription to be able to do this part.

Additional information can be found here:

- https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-fed-group-claims
- https://learn.microsoft.com/en-us/entra/identity-platform/optional-claims?tabs=appui#configuring-groups-optional-claims

Have questions or need help? Give us a call at 1-877-PROXY-US for Sales and Support.