# AZURE ACTIVE DIRECTORY INTEGRATION WITH PROXY PRO RAS

The on-premise PROXY Pro RAS Edition and hosted PROXY Air remote desktop service from Proxy Networks include support for communicating directly to the Microsoft Azure Active Directory (AAD) tenant service and this guide covers the steps to accomplish this. This document assumes your organization already has an AAD tenant. For instructions on how to create a new AAD, we recommend following Microsoft's guidelines.

When you are ready to get started, log into your portal at **portal.azure.com.**

## 1) Create a pair of Azure AD groups for use with PROXY

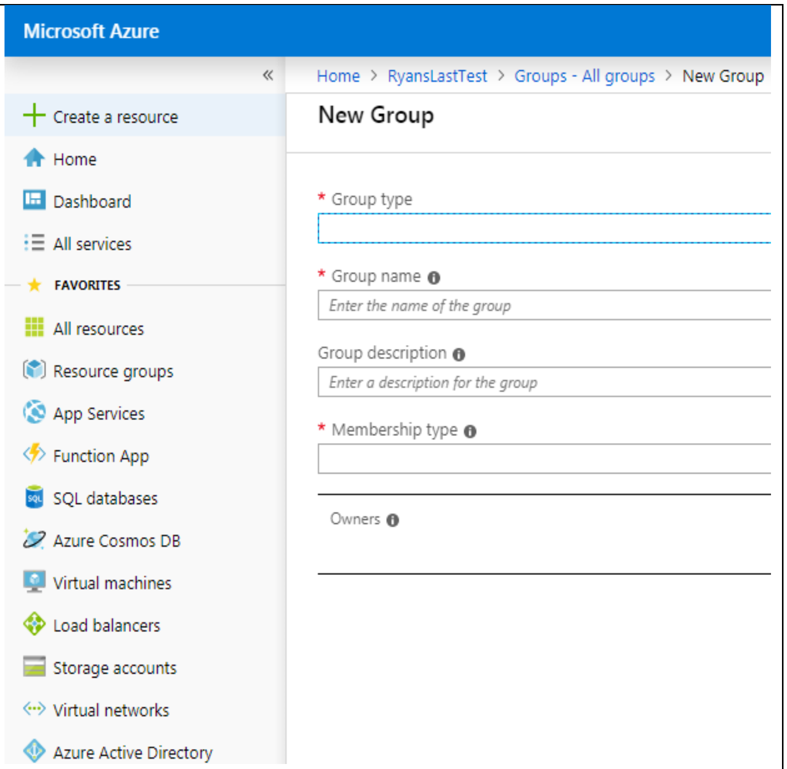
Provide information for the following fields to create a group:

- Group type: Security
- Group name: **PROXY Pro Administrators**
- 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 it to complete group creation. Repeat once again for the Masters group.

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

After successful group creation, close the Group panel.



Home > RyansLastTest > Groups - All groups > New Group

New Group

* Group type

* Group name

*Enter the name of the group*

Group description

*Enter a description for the group*

* Membership type

Owners

## 2) Adding PROXY Pro users to Azure AD Groups

a. Click the Group name, click **Members**, click **Add members.**
b. Select existing user(s) from the list or enter a user's email address.
c. Click **Select** to confirm.
d. Users must accept the invitation sent to their inbox before they can log in for the first time (after completing the rest of the steps in this guide).

## 3) Inviting a user external to your own Azure AD tenant

a. To invite an external user, click **New guest user** and the “Invite a Guest” panel opens.
b. Provide the email address of the person you would like to invite, optionally with a message.
c. Click **Invite** to send the invitation.
d. Users must accept the invitation sent to their inbox before they can log in for the first time.

## 4) App Registration

a. Provide a **Name** for the application.
b. For Supported Account Types, use the radio button for **Accounts in any organizational directory and personal Microsoft accounts.**
c. For the **Redirect URI**, enter the address of your web console and add /pim/core/ to the end.
    a. It should look like this: https://support.yourwebsite.com/pim/core/
d. Click **Register**.
e. Under **Authentication** hit the checkbox for **ID Tokens** and click **Save.**

## 5) Certificates & Secrets

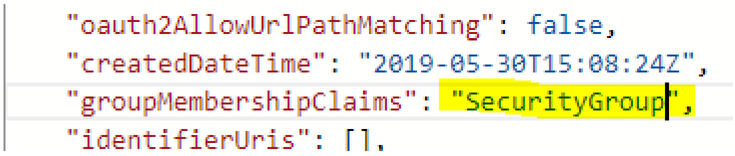
a. From the **Certificates & secrets** page click **New client secret.**
b. Provide a descriptive name in the **Description** field.
c. Set the expiration to **24 months** and note that the PIM needs to be updated in 2 years.
d. **IMPORTANT:** Copy the value to Notepad or similar as this is needed for the PIM settings later. You cannot retrieve the key 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.**
    a. If using v10.4 or later, click **Microsoft Graph** and click **Application Permissions.**
        i. Expand **Directory** and check the box for **Directory.Read.All (Read Directory Data).**
        ii. Click the **Grant admin consent for [Your Proxy Web Console]** button.
    b. If on v10.3 or earlier, click **Azure Active Directory Graph** and click **Application permissions.**
        i. Expand **Directory** and check the box for **Directory.Read.All (Read Directory Data).**
        ii. 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": "2019-05-30T15:08:24Z",
    "groupMembershipClaims": "SecurityGroup",
    "identifierUris": [],
```

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

## 8) 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:

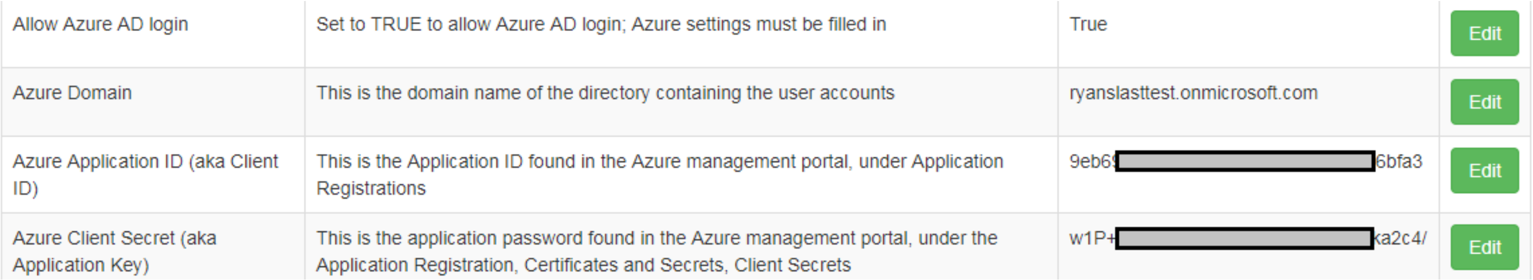
b. Visit the URL directly which would look like this: https://support.yourwebsite.com/pim/

c. 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.

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

- Allow Azure AD login: Set to True.
- Azure Domain: Domain name (example: MyDirectory.onmicrosoft.com).
- Azure Application ID (Client ID): Shown on the Overview page.
- Azure Client Secret: Supply the key from the Certificates & secret step.
- After having successfully logged in as an Administrative user for the first time with an Azure AD account, it is safe disable Local Active Directory login within the PIM (recommended).

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



| | | | |
|---|---|---|---|
| Allow Azure AD login | Set to TRUE to allow Azure AD login; Azure settings must be filled in | True | Edit |
| Azure Domain | This is the domain name of the directory containing the user accounts | ryanslasttest.onmicrosoft.com | Edit |
| Azure Application ID (aka Client ID) | This is the Application ID found in the Azure management portal, under Application Registrations | 9eb6[redacted]6bfa3 | Edit |
| Azure 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 | w1P+[redacted]ka2c4/ | Edit |

## 10) Importing Azure AD 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 to add the first new group created in step 1.

c. Select the Group radio button, input the Administrative group name, click OK and Save.

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

e. Select the Group radio button and provide the Master group name in the field.

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

## Additional Considerations

**PROXY v10.0 through v10.3**: When configured for Azure Active Directory integration, the PROXY Pro Identity Manager makes HTTPS requests to various Microsoft services (the Azure Active Directory Graph API, and Azure AD authentication services). The URLs that it accesses are:

- https://graph.windows.net/
- https://login.windows.net/
- https://login.microsoftonline.com/

**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/
- https://login.microsoftonline.com/

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:

a. Click App Registrations
b. Search for the Proxy app and click it to select it
c. Click Token Configuration
d. Click Add groups claim and choose the "Groups assigned to this application" check box
e. Select "Group ID" for both "ID" and "Access" and hit Save
f. Manifest line 13 should be changed to: "groupMembershipClaims": "ApplicationGroup",

**Have questions or need help? Give us a call at 1-877-PROXY-US.**