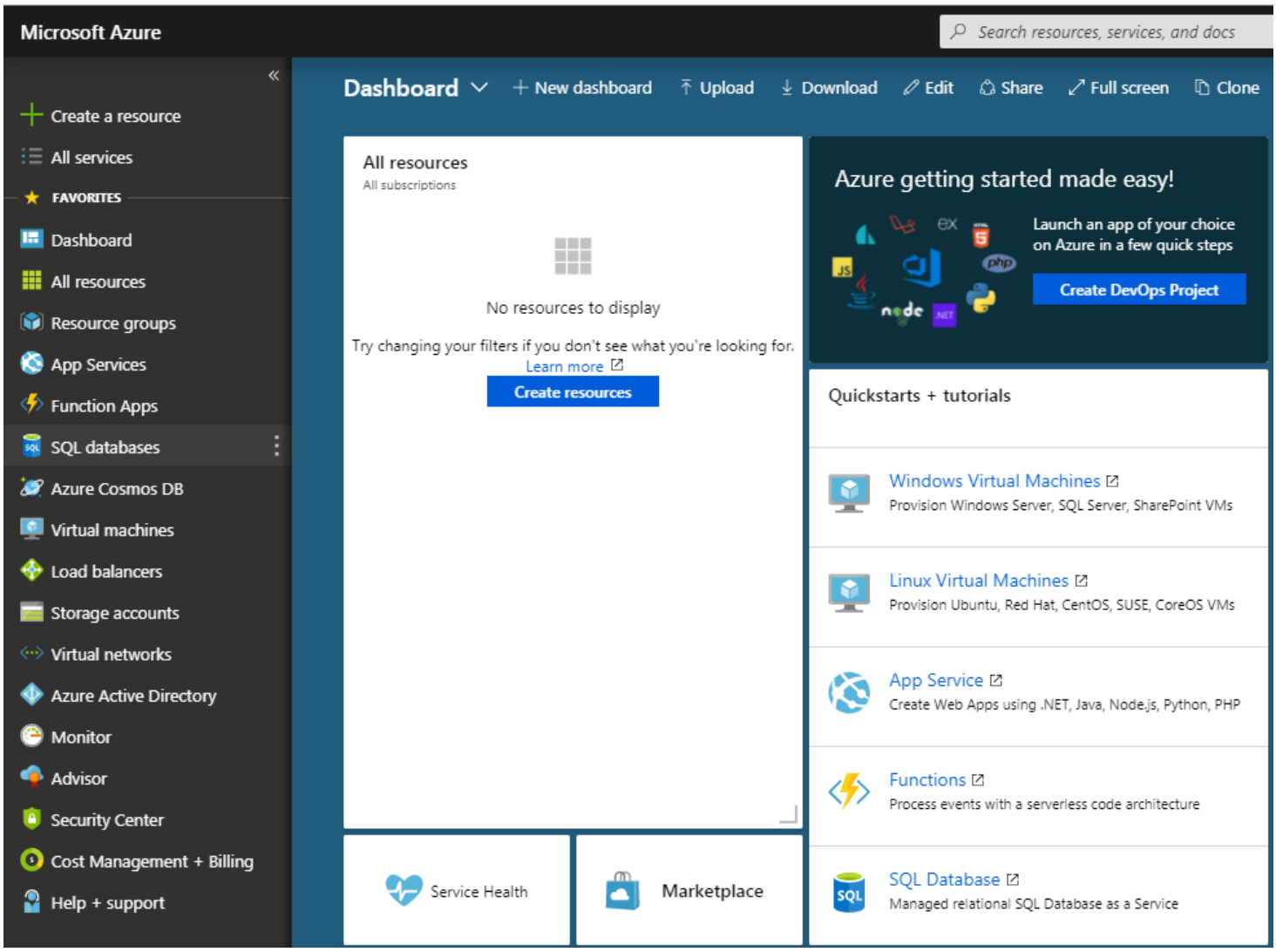
GUIDE: AZURE ACTIVE DIRECTORY INTEGRATION

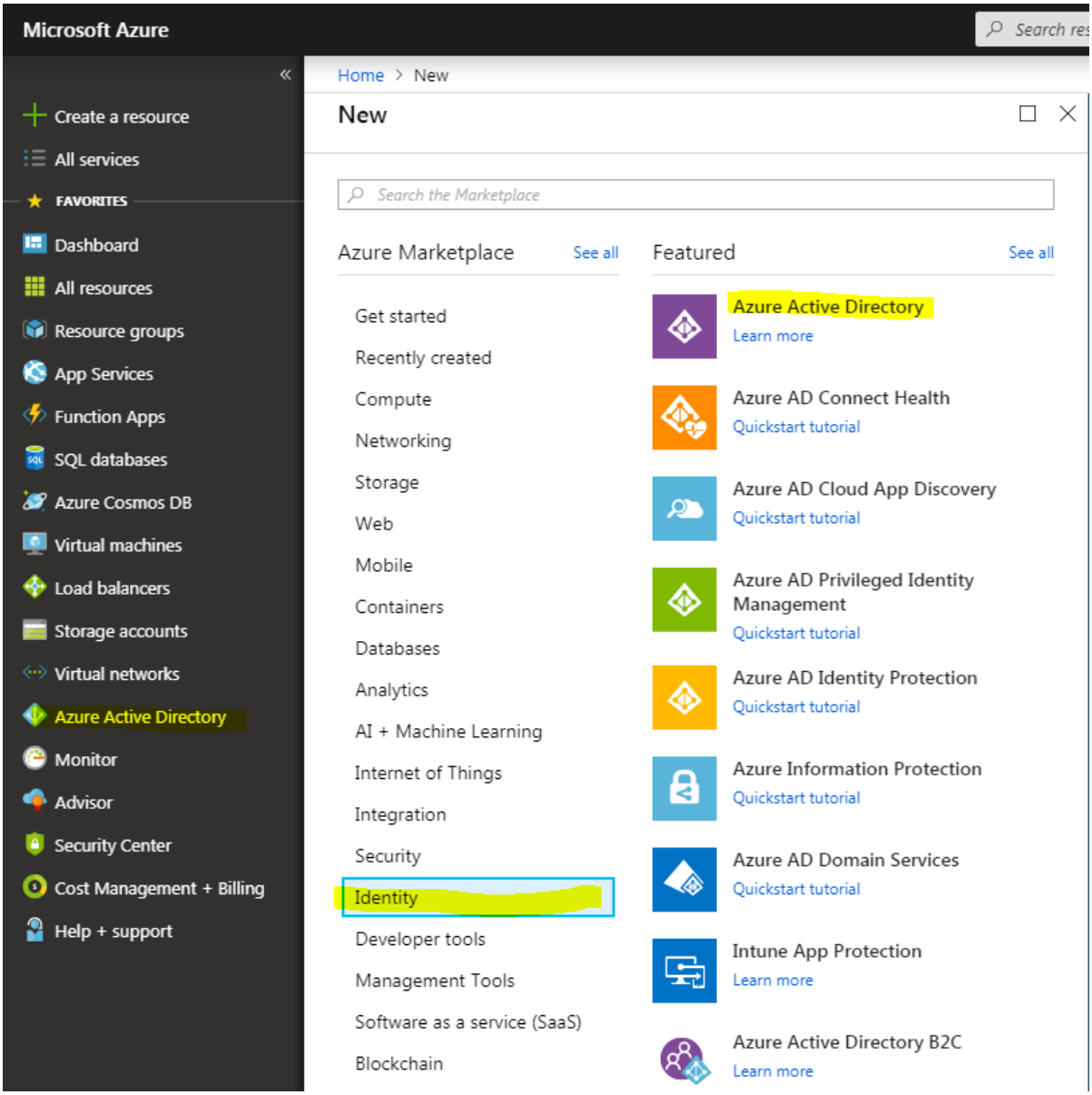
PC-Duo now includes support for communicating directly to the Microsoft Azure Active Directory (AAD) tenant service and this guide covers the steps to accomplish this. Until the last version of PC-Duo, authentication had been limited to Windows Authentication. Pc-Duo can now use alternate identity providers and provide multi-factor authentication.

When you are ready to get started, log into your portal at **portal.azure.com,** which looks like this:



Create a New Directory (Skip this step if you have an existing AAD)

1) Click "**+ Create a resource**", then click **Identity**, then click **Azure Active Directory.**



2) Provide an organization name and initial directory name. As an example, we have used this format:
   - Organization name: <Server> at <Company Name> (GWCOne at Vector Networks)
   - Initial domain name: <Company><Server> (pcduogwcone).

   Once the data input is complete, click **Create** at the bottom of the panel. The Directory creation will take a few minutes and is indicated by the message "Directory is being created now" in the

middle of the panel. At the same time, the bottom border of the bell icon in top has a busy progress bar.

3) Upon completion, the panel displays message, "Click here to manage your new directory".

4) At this point, the Azure Active Directory has been created and we'll now both create groups and users and then register the PC-Duo server as an application.

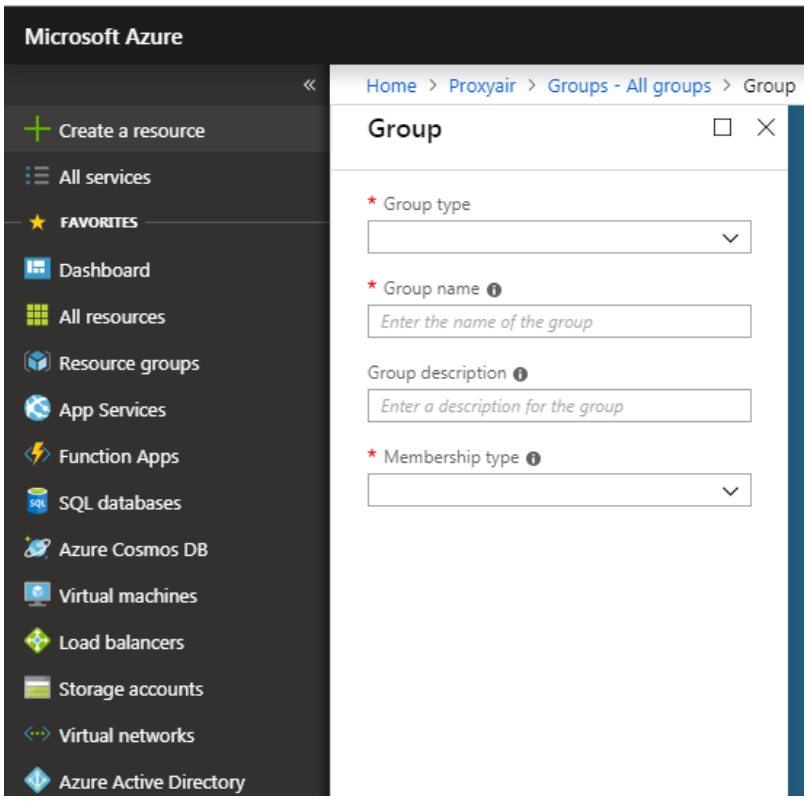
Important: Save the initial domain name (i.e. pcduogwcone.onmicrosoft.com) to be used later. At this point the Directory is created and ready to be configured. The configuration includes:

- Create groups and users.
- Register application.

Create Groups (Click Azure Active Directory -> Groups -> New Group)

Provide information for the following fields to create a group:

- Name: **PC-Duo Administrators**
- Description: PC-Duo Administrators group
- Membership type: Assigned
- Enable Office features: 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 step 6-8 with another group data:

- Name: **PC-Duo Masters**
- Description: PC-Duo Masters group
- Membership type: Assigned
- Enable Office features: Leave alone
- Ignore Members section at this point.

After successful group creation, close the Group panel.

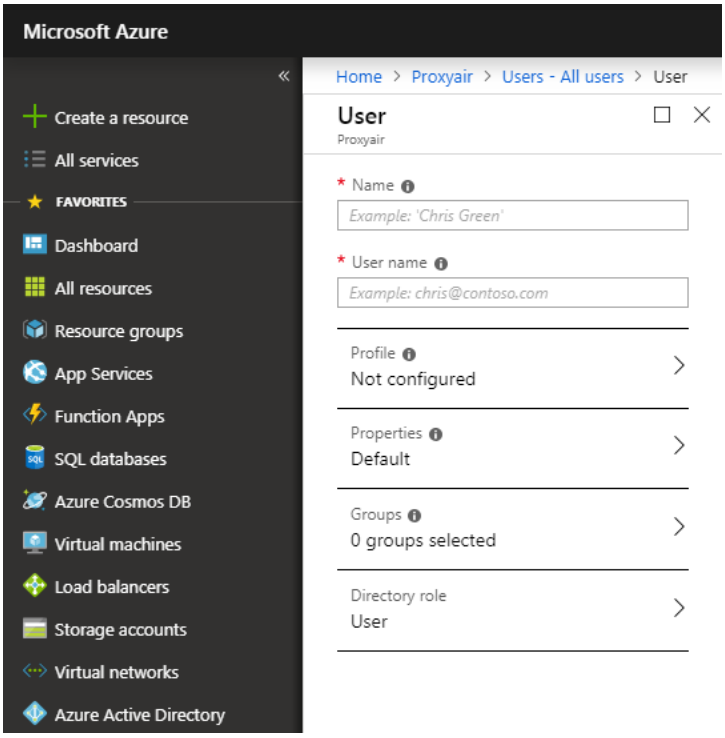
Create Users (Click Azure Active Directory -> Users -> New user)

Provide information into the following fields to create a user:

- Name: User full name (John Smith)
- User name: Fully qualified user name (jsmith@pcduogwcone.onmicrosoft.com)
- Click Profile, a new panel title Profile will open. In the Profile panel provide General information at least:
    - First Name: of the new user to be created (John)
    - Last Name: of the new user to be created (Smith)

Be sure to click **OK** at the bottom of the Profile panel after first name and last name are filled in. This will save new user profile information and close the Profile panel.

- Properties: Leave alone
- Ignore Groups section at this point.
- Leave the Directory role as User.
- Important step: Check the **Show Password** box and copy the Password from the field above it. Save the user name (jsmith@pcduogwcone.onmicrosoft.com) and corresponding password to a text file.



This password is the user's one time first password. The user will be asked to change it when they log in. If this step is missed, an admin will have to reset the user's password and perform this step again to provide the user with their first login password.

Caution: Communicate the first-time password to the user via secure channel later.

- Click **Create** to save the user. This will automatically close the User panel.
- Repeat these steps to create another user

Inviting External Users (Click Azure Active Directory -> Groups -> New user)

1) To invite an external user, click **New guest user** and the "Invite a Guest" panel opens.
2) Provide information for the fields to create a user.
3) Enter the email address of the external user and click **Invite** to send the invitation.

Adding Users to Groups (Click Azure Active Directory -> Groups)

1) Click the Group name, click **Members**, click **Add members.**
2) Select existing user(s) from the list or enter a user's email address.
3) Click **Select** to confirm.

App Registration (Click Azure Active Directory -> App Registrations)

1) Click **New Application Registration**.
2) Provide information for the following fields to create a new app registration:
   - Name: PC-Duo v13 on <server> (PC-DUO on GWCOne)
   - Application type: Web app / API
   - Sign-on-URL: https://<path to web console> (https://gwcone.eng.vectornetworks.com)

   Click **Create** at the bottom of the panel to register new application; a successful creation will close the panel also.
3) Click on the row that displays the application name.

4) Click the **Manifest** button at the top of the "Registered app" pane, opening the "Edit Manifest" panel. Look for the line "groupMembershipClaims": null (line # 7). Replace the null with SecurityGroup so the line reads "groupMembershipClaims": "SecurityGroup" like in the below screen snippet:

Click **Save** on the top and close the Edit Manifest panel. In the App Registrations panel, click the **Settings** button.

5) In the **Settings** panel, click **Properties** from the GENERAL section. Copy Contents of the Home page URL and paste it into the App ID URL. Click **Save**, then close the properties panel.

6) In the **Settings** panel, click **Reply URLs** from GENERAL section:
In the Reply URLs panel, click on the row that displays the Web Console URL path to edit. Append "/pim/core/" to the URL (including the final /). Click **Save**, then Close the Reply URLs panel. If the web console is not running on 443 the non-standard port must be specified in this URL. The Reply URL must contain the port but Home Page URL and App ID URL do not.

7) In the **Settings** panel, click **Keys** from the API ACCESS section. Provide a key description with a string that is at most 16. (PC-DUO GWCONE). Select duration as "Never Expires" and click **Save** to reveal the Application Key Value. **Very Important**: As the message displayed upon Save, please copy the Application Key Value and save it someplace since this value will never be visible once the panel is closed. After having copy/pasted the key to Notepad or similar, close the panel.

8) In the **Settings** panel, click **Required permissions** from API ACCESS section, showing "Required permissions".

9) Click **Windows Azure Active Directory** and the **Enable Access** panel opens.
Check these permissions then click **Update Permissions** afterward:
   - APPLICATION PERMISSIONS
     - Read directory data
   - DELEGATED PERMISSIONS
     - Read all groups
     - Read all users' basic profile
     - Sign in and read user profile

10) Back in the "Required permissions" panel, click **Grant Permissions**.

11) Close all panels till the "Registered App" panel is visible.

12) Before proceeding further, please collect the following information:
   - **Application ID** – displayed as property in the Essentials collapsible panel.
   - **Application Key** – was requested to be saved in an earlier step. This key was only visible when created so there is no way to access it again. If it was lost, start over with the app registration.
   - **Domain Name** – note the domain used in step 2. If you did not create a new domain, you can verify the domain name clicking the "Domain names" link from the Manage column of the Directory panel.

Updating Proxy Identity Manager (PIM) Settings

PC-Duo Identity Manager settings are accessible via two paths:

- Directly accessing the PIM web application.
- In the Web Console, click Gateway -> Network –> Network Settings. At the bottom, there is a link to navigate to the PIM settings.

Navigate to PC-Duo Identity Manager settings and edit these fields:

- Allow Azure AD login: Switch to True.
- Azure Domain: Domain name saved from the last section.
- Azure Client ID: Application id saved from the last section.
- Azure Application Key: Application key saved from the last section.

Click **Apply** that appears at the bottom of the grid. Follow the popup and click **OK**.

On the PC-Duo Identity Manager page when you see "*Modified settings have been applied, but PC-Duo Identity Manager could not be automatically restarted.* Click **PC-Duo Identity Manager** in the top navigation bar to reload the page. Click **Settings** and log in to confirm all the settings are correct. This is not a mandatory step; however, it helps to double check and forces the load of PC-Duo Identity Manager web application in IIS.

Below is a screen snippet showing the PIM's Azure fields that must be filled in.

Azure Domain	This is the domain name of the directory containing the user accounts	pcduogwv13.onmicrosoft.com	Edit
Azure Application ID	This is the Application ID found in the Azure management portal, under Application Registrations	04: d8	Edit
Azure Application Key	This is the application password found in the Azure management portal, under the application Settings, API Access, Keys	azl HY=	Edit
Allow access to Find a Desktop from External Addresses	Set to FALSE to prevent users from logging into Web Console from external addresses	True	Edit

Importing Azure AD Groups to the Proxy Web Console's "Accounts" tab

1) Log into the PC-Duo Web Console as an Administrative user and visit the "Accounts" tab.
2) Click the "+" button to add the two new Azure AD Groups.
3) Select the "Group" radio button and provide the group name in the field.
4) Add the PC-Duo Administrators group as the "Administrative" account type and then add the PC-Duo Masters group as the "Master" account type.
5) Upon completion, members of the two Azure AD groups may now log in.

HAVE QUESTIONS OR NEED HELP? GIVE US A CALL 1-800-330-5035 FOR SUPPORT!