PCDUO

AZURE ACTIVE DIRECTORY INTEGRATION

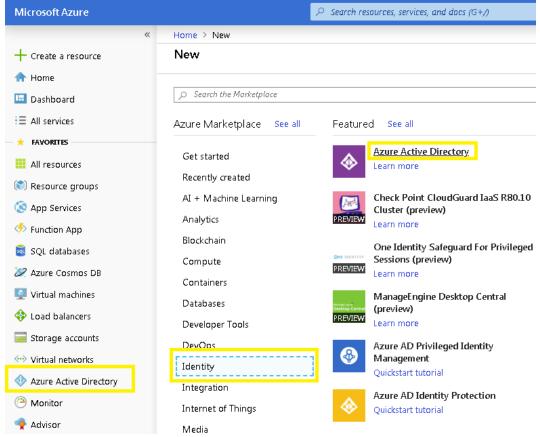
PC-Duo includes support for communicating directly to the Microsoft Azure Active Directory (AAD) tenant service and this guide covers the steps to accomplish this. Until PC-Duo v10, authentication had been limited to Windows Authentication. We have now broken free from that in order to use alternate 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:

Microsoft Azure			۶	Search resources, services, and docs	
*	Home > RyansLastTest - Overview				
+ Create a resource	RyansLastTest - Overview				
🛧 Home	Azure Active Directory	Østar i star 👼 s			
🖪 Dashboard		🧬 Switch directory 🗓 D	elete direct	tory	
∃ All services	Overview	RyansLastTest.onmicrosoft.co	om		
+ FAVORITES	💅 Getting started	RyansLastTest			
All resources	Manage	Azure AD Free			
🕅 Resource groups	🔓 Users	Sign-ins			
🔇 App Services	🗳 Groups				
🦘 Function App	🕴 Organizational relationships	To see sign-in data, your organization needs A: Premium P1 or P2. Start a free trial			
👼 SQL databases	Roles and administrators				
🞾 Azure Cosmos DB	Enterprise applications				
👰 Virtual machines	Devices				
🚸 Load balancers	App registrations				
Storage accounts	App registrations (Legacy)	What's new in Azure AD			
😔 Virtual networks	ldentity Governance	Stay up to date with the late	est release r	notes and blog posts.	
Azure Active Directory	Application proxy	25 entries since February 20, 2019. View archive 🕫			
😬 Monitor	🔓 Licenses				
🌪 Advisor	🚸 Azure AD Connect		(25)	New feature	
🧿 Security Center	🕫 Custom domain names	Collaboration	(2)	Group Management - Collaboration April 20, 2019	
Oost Management + Billing	Ø Mobility (MDM and MAM)	Monitoring & Reporting 3rd Party Integration			
Help + support	🕈 Password reset		(4) (1)	Configure a naming policy for Office 365 groups preview)	
	Company branding		(2)	F	

A. Create a New Directory (Home > New). Already have an AAD? Skip to next step.

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



- b) Provide an organization name within the "Organizational name" field.
- c) Provide an initial domain name in the "Initial domain name" field.
- d) Click **Create** at the bottom of the panel and within a couple minutes your new directory will be created.
- e) Upon completion, the panel displays message, "Click here to manage your new directory".

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

- Creating groups and users.
- Registering the application.

B. Create Groups (Home > YourAzureADHere > Groups - All groups > New Group)

Provide information for the following fields to create a group:		Microsoft Azure		
		«	Home > RyansLastTest > Groups - All groups > New Group	
		+ Create a resource	New Group	
Group type: SecurityGroup name: PC-Duo		🛧 Home		
		🛅 Dashboard	* Group type	
Administrators		I All services		
Description: PC-Duo Administrators		- 🕇 FAVORITES	* Group name 👔	
group		All resources	Group description 👔	
		(Resource groups	Enter a description for the group	
 Membership type: Assigned (Leave alone) 		Services	* Membership type 🚯	
,		Function App		
Ignore Members section at this point.		SQL databases	Owners 🚯	
		Azure Cosmos DB		
After successful group creation, close the		Virtual machines		
Group panel. The Create button at the		Load balancers		
bottom will get enabled. Click it to complete group creation.		Storage accounts		
Repeat once again for the Masters group.		Azure Active Directory		
Repeat once again for the Masters group.		V Azure Active Directory		
Group type: Security				
Group name: PC-Duo Masters				
Description: PC-Duo Masters group				
Membership type: Assigned (Leave				
alone)				
Ignore Members section at this point.				
After successful group creation, close the Group panel.				

C. Create Users (Home > YourAzureADHere > Users - All users > User)

Skip to the next step if you already have user accounts and would like to invite them via their email addresses.

Provide information into the following fields to create a user:

- Name: User full name (John Smith)
- User name: Fully qualified user name (jsmith@YourAzureADHere.onmicrosoft. com)
- Click Profile, a new panel title Profile will open. In the Profile panel provide General information at least:
 - Name: John Smith
 - o Username: <u>JSmith@company.com</u>

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

 Important: Check the Show Password box and copy the Password from the field above it. Save the user name (JSmith@YourAzureADHere.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.

Microsoft Azure	∠ Search resources, :	>_			
«	Home > YourAzureADHere > Users - All users >	User			
+ Create a resource	User YourAzureADHere				
🛧 Home	* Name 👩				
🔄 Dashboard	Example: 'Chris Green'				
E All services	* User name 👩				
🛧 FAVORITES	Example: chris@contoso.com				
📕 All resources	Durfile o				
🐑 Resource groups	Profile 💿 Not configured				
🔇 App Services	Properties 👔				
🦘 Function App	Default	>			
🧟 SQL databases	Groups 🚯				
🖉 Azure Cosmos DB	0 groups selected	>			
👰 Virtual machines	Directory role	_			
🚸 Load balancers	User				
Storage accounts					
↔ Virtual networks					
🚸 Azure Active Directory					

Repeat these steps to create another	
user.	

D. App Registration (Home > YourAzureADHere - App registrations > Register an application)

- a. Provide a **Name** for the application.
- b. For Supported Account Types, use the third 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.

E. Certificates & Secrets (Home > YourAzureADHere - App registrations > YourAzureADHere - 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 **Never** and click **Add.**
- 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.
- F. API Permissions (Home > YourAzureADHere App registrations > YourAzureADHere API permissions)
 - a. From API permissions, click Add a Permission.
 - b. Click Azure Active Directory Graph and click Application permissions.
 - c. Expand **Directory** and check the box for **Directory.Read.All (Read Directory Data).**
 - d. Click the Grant admin consent for [Your PC-Duo Web Console] button.

G. Manifest (Home > YourAzureADHere - App registrations > YourAzureADHere - Manifest)

 a. Click the **Manifest** button to edit. Change null to "groupMembershipClaims": null (line # 12). 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.

H. Enterprise applications (Home > YourAzureADHere > Enterprise applications - All 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

I. Updating PC-Duo Identity Manager (PIM) Settings

- a. Visit your PC-Duo Identity Manager which can be accessed in either manner:
- b. Visit the URL directly which would look like this: <u>https://support.yourwebsite.com/pim/</u>
- c. Visit the PIM through the PC-Duo Web Console -> Gateway tab -> Network sub-tab; scroll to the bottom to find the hyperlink to the PC-Duo Identity Manager.
- d. Within the PC-Duo 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.

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(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+ka2c4/	Edit

J. Importing Azure AD Groups to the PC-Duo Web Console's "Accounts" tab

- a. Log into the PC-Duo Web Console as an Administrative user and visit the Accounts tab.
- b. Click the + button to add the first new group created in step 3.

- 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 3.
- 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.
- K. Adding Users to Groups (Home > YourAzureADHere > Groups All groups > MyGroup Members)
 - 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.
- L. Inviting a User (Home > YourAzureADHere > Users All users > User)
 - 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.

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