MITRATECH

EXPECT SUCCESS

PolicyHub® Configuring SCIM with Azure Active Directory

PolicyHub

Approval and Publication History

Version 1.0.0.0	Initial Release. Approved and Published.	February 2022

Disclaimer of Warranty

Mitratech Holdings, Inc. (Mitratech) makes no representations or warranties, either expressed or implied, by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special or consequential damages.

Mitratech reserves the right to not support non-standard or non-default functionality and extended functionality available in third-party software, unless specifically documented as supported or certified in the Mitratech product documentation. For further information regarding third-party non-standard or non-default functionality, please contact Mitratech Support.

This test document, along with the software that it describes, is furnished under licence and may be used or copied only in accordance with the terms of such licence. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as commitment by Mitratech.

The following document is for PolicyHub™ only. Though every effort was made to ensure that the information in this document is correct and reliable, Mitratech does not assume any liability for any errors encountered in this document.

If you need support for PolicyHub™, visit https://mitratech.force.com and select your product. If this is your first time accessing the support portal, please register via the "Sign Up" option.

For more information about Mitratech, visit our web site: http://www.mitratech.com.

Government Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the applicable Mitratech licence agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013 (Feb 2012)FAR 12.212(a) (1995), FAR 52.227-19 (Dec 2007), or FAR 52.227-14, as applicable.

Contents

General

SCIM Provisioning is a great way to connect an Identity Provider directly with PolicyHub in order to provision users and groups. This can be used instead of the standard Active Directory and CSV synchronization mechanisms or to supplement these feeds. This configuration guide provides information on how to enable SCIM provisioning with Azure Active Directory.

SCIM Endpoint URL

The endpoint URL is the URL of the SCIM API specific to your PolicyHub instance. The endpoint URL is case insensitive. You will need this URL to enable provisioning with Azure.

The URL will be in following format:
https://PolicyHub Instance_URL/PolicyHubApi/ScimApi.svc/Scim/V2

If you are unsure of this value or if you are unsure if this has been configured for your PolicyHub instance, then please contact our services team or your Mitratech account manager.
NOTE: For the SCIM API to work for on-premise customers, SSL should must be enabled on the hosting server and should be accessible from public network.

Configure Azure for SCIM

Requirements

To setup SCIM provisioning with Azure Active Directory, you will need access to the Azure Administration Console.

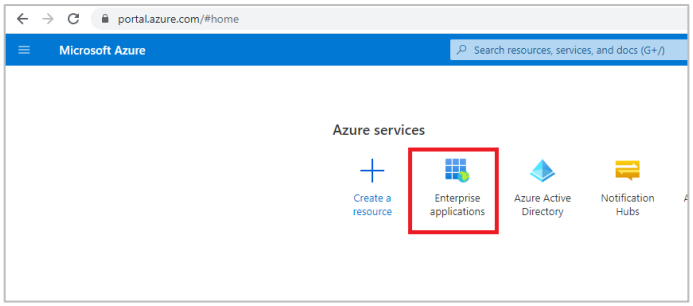
Bearer Token

Before you start integrating your Identity Provider with your PolicyHub SCIM API, you will need a secure token. It will be used to authenticate all requests coming from Azure. Please note that the PolicyHub SCIM API currently only supports **Bearer Tokens**.

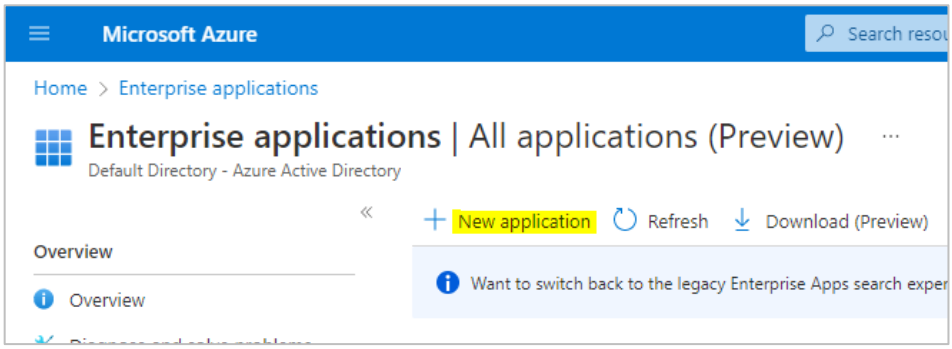
If you don't already have the authentication token for your PolicyHub instance, please contact a member of our services team or your Mitratech account manager.

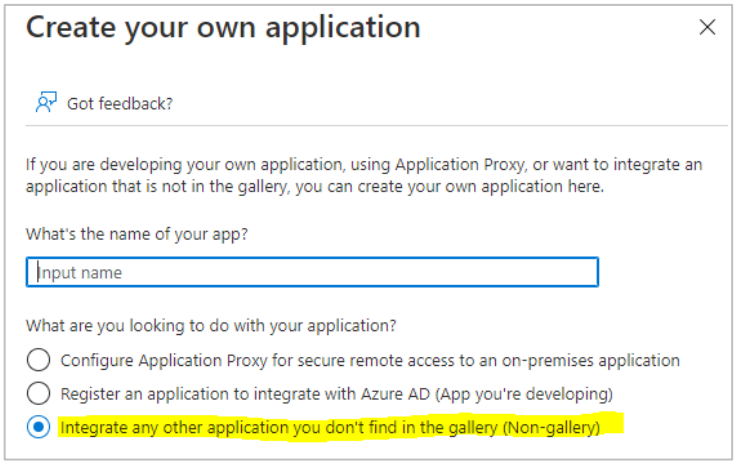
Creating the Application

Login to the Azure Administrative Console and click on **Enterprise Applications**.



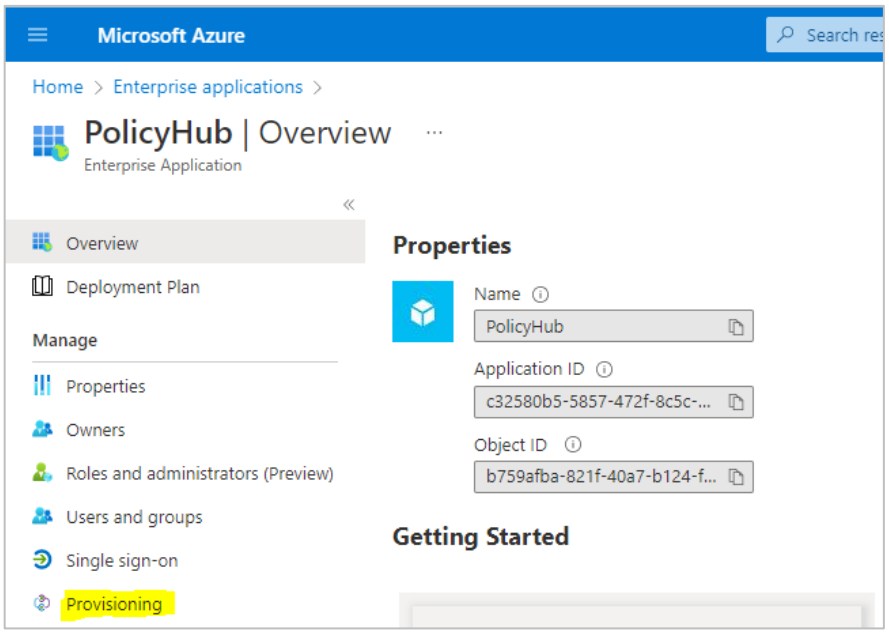
You can also use the Azure Search panel to find **Enterprise Applications**. If you already have an application ready, then select it from the list. Alternatively, you can click on **New Application**. You will be asked to enter a name for the Application. Enter a name and make sure **Integrate any other application you don't find in the gallery (Non-gallery)** is selected and click the **Create** button.





Enable SCIM Provisioning

Now go to **Provisioning** from left panel and click on **Get Started** button.

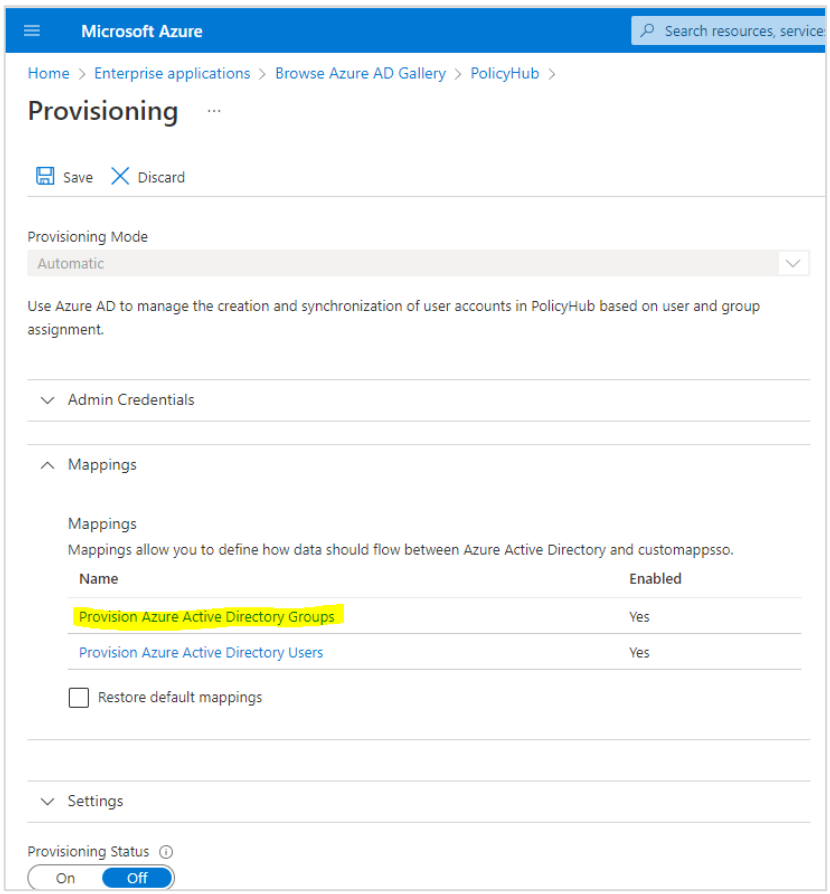


In next page, select **Automatic** from the Provisioning Mode dropdown and in **Tenant URL**, enter SCIM API endpoint URL in this format:
https://PolicyHub Instance_URL/PolicyHubApi/ScimApi.svc/Scim/V2

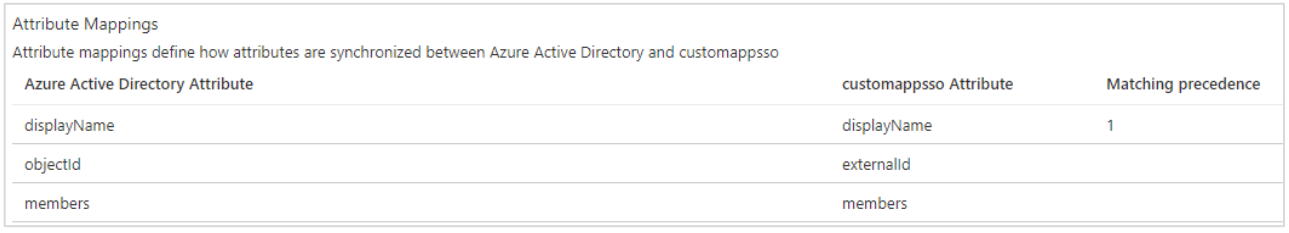
Your **Secret Token** is the bearer token that will be provided by Mitratech.
Now click on **Test Connection**. Once test connection succeeded, Click on **Save**.
This completes the basic SCIM configuration. Now we need to configure the attributes in Azure.

Configuring Group Attributes

In the Provisioning page, click on Edit Provisioning. Now click on Provision Azure Active Directory Groups.



You will see default settings as given in the screenshot.



Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute	Matching precedence
displayName	displayName	1
objectId	externalId	
members	members	

Perform the following steps to configure Group Attributes.

Step 1

- Click on **displayName**, a popup will appear.
- Select **MappingType** as **Expression** from the dropdown and in the **Expression** text box enter **Append([displayName], "|Azure")** and set the Matching Precedence value to 2 and click OK.
- Please note that there is a pipe symbol in **displayName**

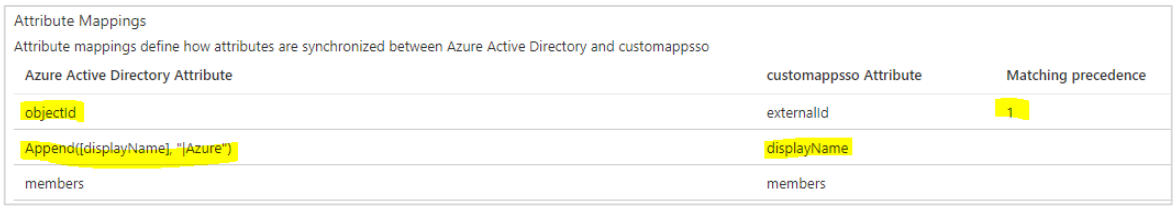
Step 2

- Click on **objectId** and select **Yes** from **Match objects using this attribute** dropdown and then set the **Matching Precedence** value to **1** and then press **OK**.

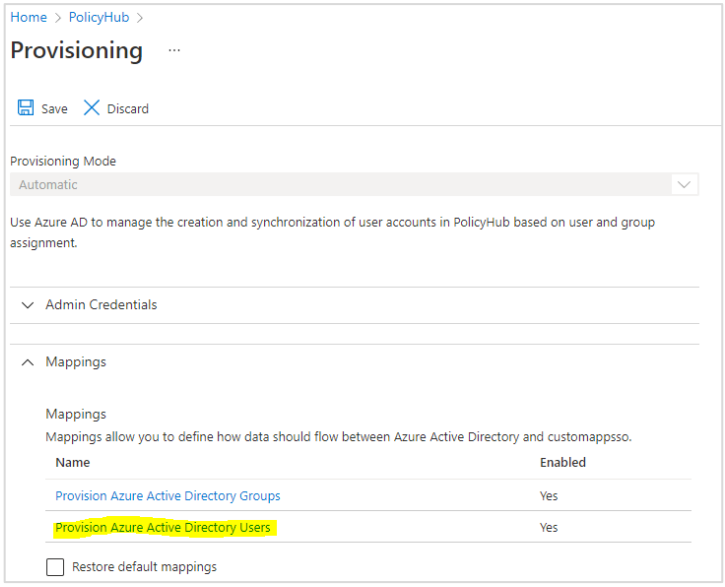
Step 3

- Click on **displayName** and select **No** from **Match objects using this attribute** dropdown. This will set Matching Precedence value to **none**. Click OK and then click Save.

Finally, the Group Attribute configuration will look like this:



Configure User Attributes



Step 1

- Click on userPrincipalName and set Matching Precedence value to 2 and press OK.

Step 2

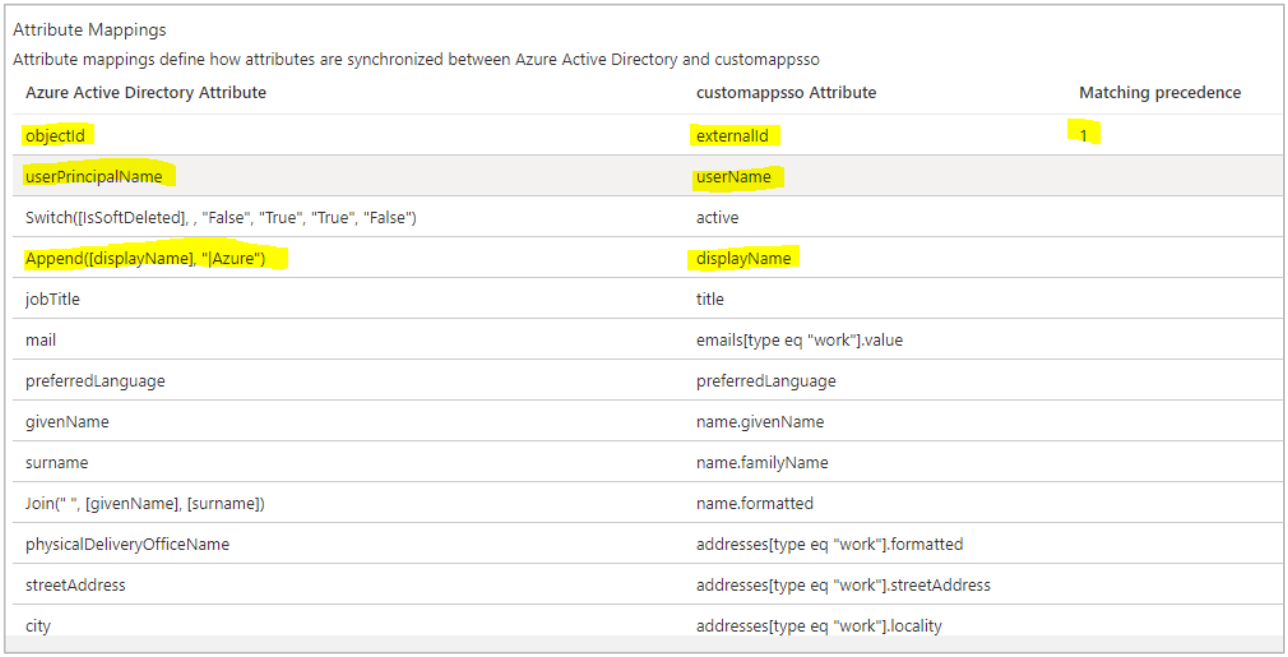
- Click on **displayName**
- Select **MappingType** as **Expression** from the dropdown and in the **Expression** text box enter **Append([displayName], "|Azure")** and set the **Matching Precedence** value to **2** and click **OK**.
- Please note that there is a pipe symbol in displayName value

Step 3

- Select **mailNickname** and change value to **objectId**.
- Select **Yes** from **Match objects using this attribute** and enter **1** as the Matching Precedence value and click **OK**.

Step 4

- Click on **userPrincipalName** and select No from the **Match objects using this attribute** dropdown. This will set the **Matching Precedence** value to none. Click **OK** and then click **Save**.



Attribute Mappings

Attribute mappings define how attributes are synchronized between Azure Active Directory and customappsso

Azure Active Directory Attribute	customappsso Attribute	Matching precedence
objectId	externalId	1
userPrincipalName	userName	
Switch([IsSoftDeleted], , "False", "True", "True", "False")	active	
Append([displayName], "|Azure")	displayName	
jobTitle	title	
mail	emails[type eq "work"].value	
preferredLanguage	preferredLanguage	
givenName	name.givenName	
surname	name.familyName	
Join(" ", [givenName], [surname])	name.formatted	
physicalDeliveryOfficeName	addresses[type eq "work"].formatted	
streetAddress	addresses[type eq "work"].streetAddress	
city	addresses[type eq "work"].locality	

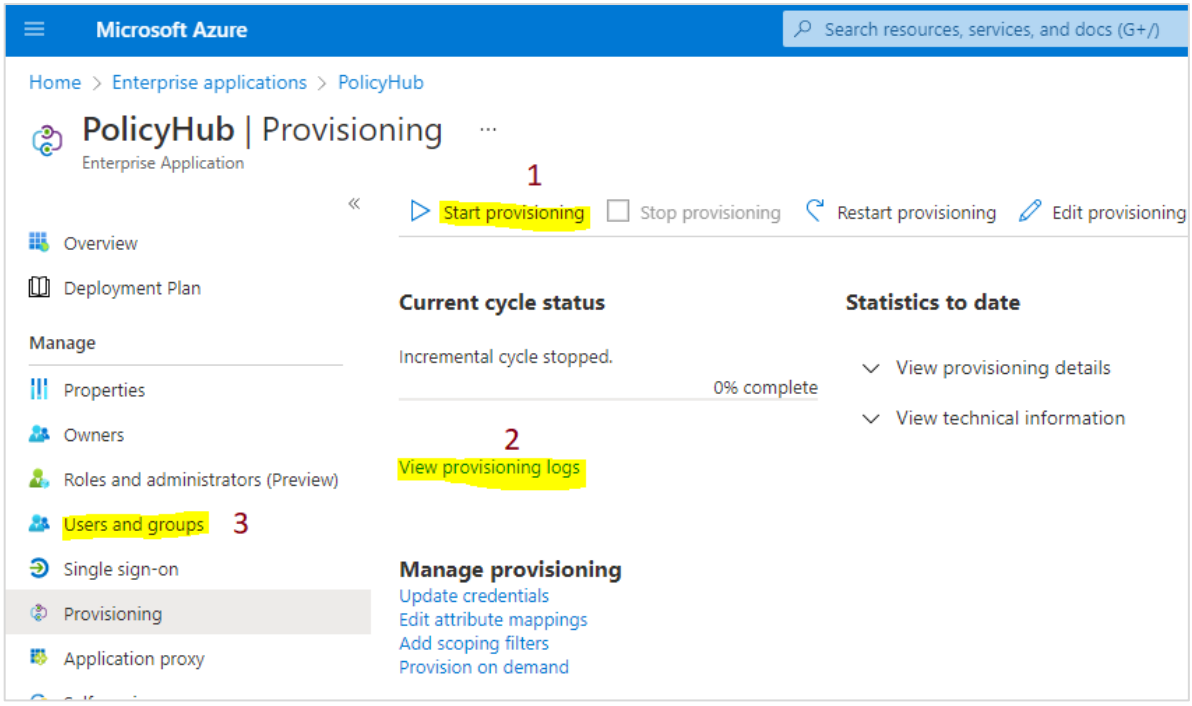
The remaining attributes can be left as they are. The 3 attributes for a User should look like this:

Azure Attribute	Custom App Attribute	Matching Precedence
objectId	externalId	1
userPrincipalName	userName	
Append([displayName], “|Azure”)	displayName	

Mapping the **externalId** to **objectId** allows the API to use the Azure Object ID for every SCIM transactions instead of userName. This enables PolicyHub to be able to differentiate between two users with the same name in cases where a user has been removed and a new user added with the same name.

Azure Provisioning Panel

Once you are finished with the configuration, you will see this panel from where you can Start/Stop provisioning and see the provisioning logs.



Start Provisioning

This button is used to start provisioning. Once it started, any user or group assigned to the application will be provisioned automatically in PolicyHub. The duration of the next provisioning can be between 45 minutes to 1 day. If you want this to happen sooner, then you can use the Restart button or you can Stop and Start the provisioning.

View Provisioning Logs

Whenever provisioning occurs, a log is generated. If you find any users or groups that are not synchronized then you can refer to this log and it will tell you the reasons for any failures.

Note: FirstName, LastName, LoginName (UserName) and Email are mandatory fields in PolicyHub and so when you are adding a user in Azure AD, please make sure you have provided these four fields.

Users and Groups

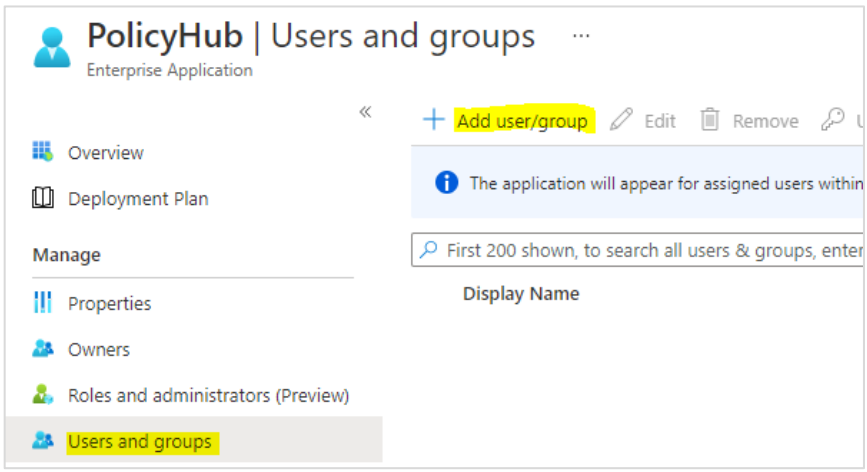
This is the area in which you can assign users and groups to application.

Import Users & Groups

Before we do any user/group related operations, please check if automatic provisioning is started or not (see above screenshot for more info).

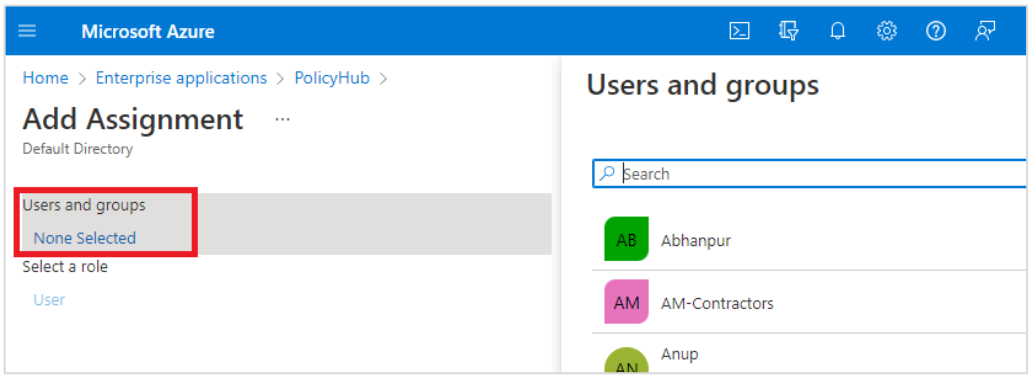
In Azure, we can add Users or Groups separately in the application.
Next in this document you will see how we can perform CRUD operations using Azure and the PolicyHub SCIM API.

Use the following screen to perform User/Group related operations.

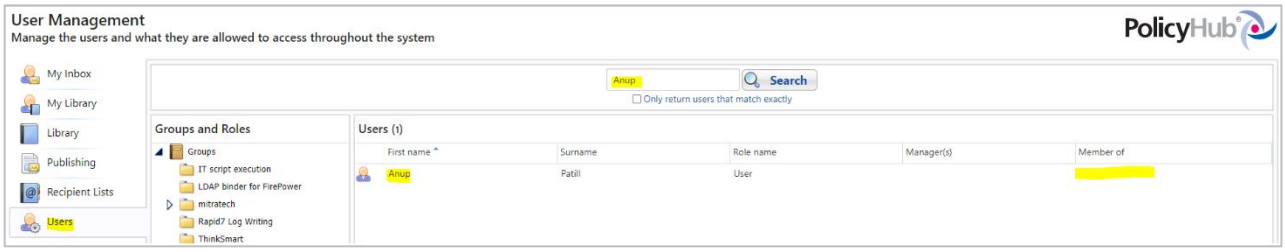


Add User

In the Add Assignment tab, click **None Selected** link, this will show you all of the available users and groups. Select a user and click the **Assign** button from the footer of the page.



As you have provisioned an individual user but not a group, in PolicyHub, you will not see the user in the Users tab under any group. Use the **Search User** option to search for the user. You will see that the user is present in PolicyHub but the **Member Of** column is empty. This means user is not a part of any group.



If you subsequently add this user to a group in Azure, this will not be reflected in PolicyHub unless you also sync the group with PolicyHub.

Edit User

To edit a user, you can go to Azure Home and select Azure Active Directory where you will find the Users tab. Click on the Users tab and select a user from the list which you want to edit and from Profile section you can edit the user's details.

Delete User

To delete a user from PolicyHub, you can un-assign the user from Azure application. Please note, deleting a user using the unassign option will work only if you have assigned the user directly to the application and it is not linked with more than 1 group.
Alternatively, delete the user permanently from Azure. This will also delete the user from PolicyHub.

Add Group

Groups can be added in the same way that users are. One important thing to note is that when we add a group, all its children (users or groups) will also get added automatically. This is applicable only for the first level. 2nd level nested Users and Groups will not be added.

Edit Group

Go to Groups tab from Azure Active Directory and select the group which you want to edit. From the Properties tab, you can edit the group details. For adding or removing a member (User/Group), you can use Members tab.

Delete Group

To delete a group from PolicyHub, either you can unassign the group from the Azure application or you can use the Delete Group option to remove the group from PolicyHub.
If you unassign a group from the application in Azure, then all its first level members (Users/Groups) will be deleted from PolicyHub.

Working with Group Hierarchy

PolicyHub supports group hierarchies. To import a group hierarchy using PolicyHub SCIM API from Azure, first create a nested group.

A group can have Users and a Subgroups, and Subgroups can also have Users and Subgroups. But at the time of import, there are some rules in Azure that must be followed.

Suppose we have a group hierarchy like this. Here **Blue** represents Groups and **Orange** represents Users.

ABC Enterprise

|

|-------- Corporate

| |---------- Anthony

| |---------- Chicago

| |---------- David

| |---------- John

|-------- Michael

|-------- Franchise

Case 1

- If you assign **ABC Enterprise** to the Azure PolicyHub application directly then all direct children (1st level) will be imported with **ABC Enterprise** **(i.e. Corporate, Franchise and Michael)** automatically.

Case 2

- If you assign **Corporate** to the Azure PolicyHub application, then along with **Corporate**, user **Anthony** and group **Chicago** will also be imported into PolicyHub automatically and group **Corporate** will become the topmost root node in PolicyHub.

Case 3

- If you just assign users to the application, then it will only import user but not linked group.

How to import the entire hierarchy into PolicyHub

- For this, we just need to assign **ABC Enterprise, Corporate** and **Chicago** to the Azure PolicyHub application. What happens behind the scenes is, when you assign **ABC Enterprise**, it will also import **Corporate**, **Franchise** and **Michael** into PolicyHub. Assigning **Corporate** will import **Anthony** and **Chicago** and assigning **Chicago** will import **David** and **John**. This way only assigning 3 groups will import the above given hierarchy at once.

It is very important to think ahead about how you are going to manage users and groups in Azure Active Directory and put sufficient processes in place to ensure future provisioning is performed automatically.

www.mitratech.com

5001 Plaza on the Lake, Suite 111, Austin, TX 78746
Tel: US (512) 382-7322.