MITRATECH
EXPECT SUCCESS

PolicyHub® Configuring SCIM with Okta

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 Okta.

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 Okta.

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 OKTA for SCIM

Requirements

To setup SCIM provisioning with OKTA, you need to have access to the OKTA Admin Console.

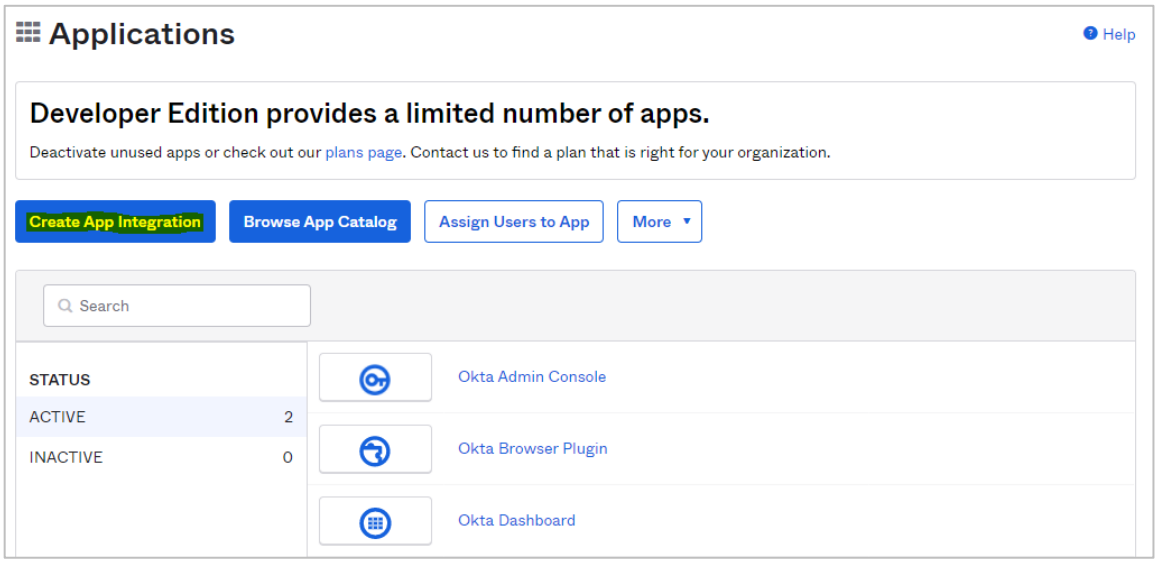
Bearer Token

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 Okta. Please note that the PolicyHub SCIM API currently only supports **Bearer Tokens**.

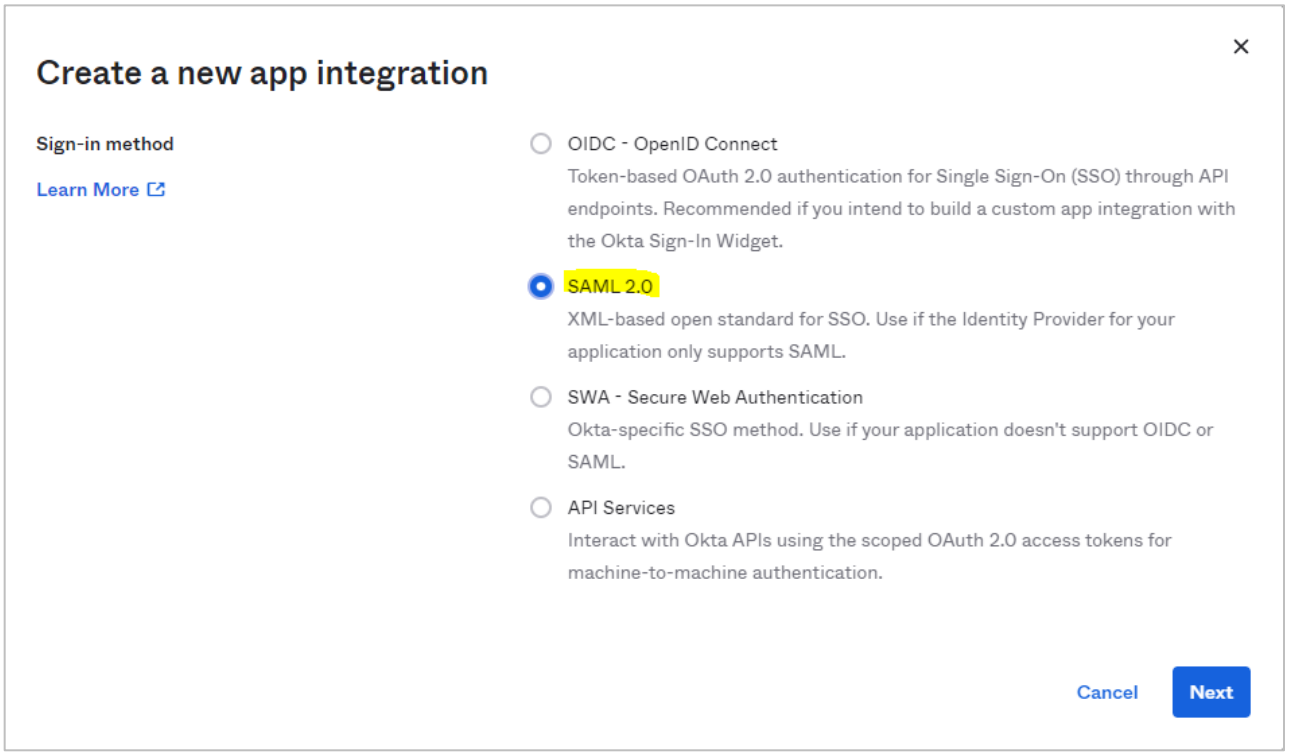
If you don't already have the authentication token for your PolicyHub instance, please contact a member of our services team or your Mitratech account manager.

Create Application

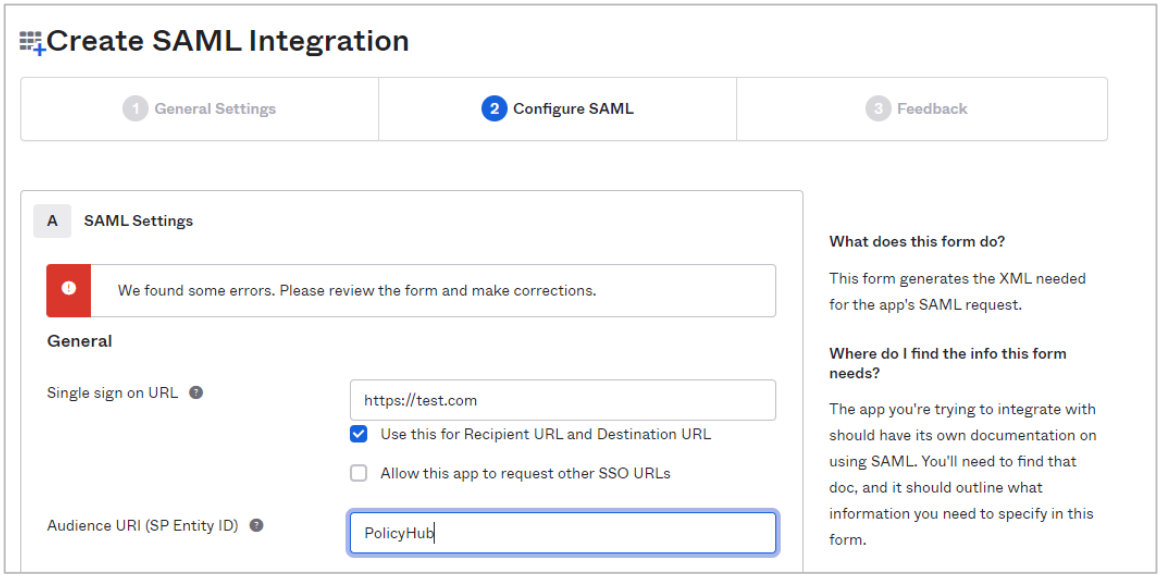
Login to the OKTA Admin console and from the sidebar menu, click on the Application menu. You will see following screen.



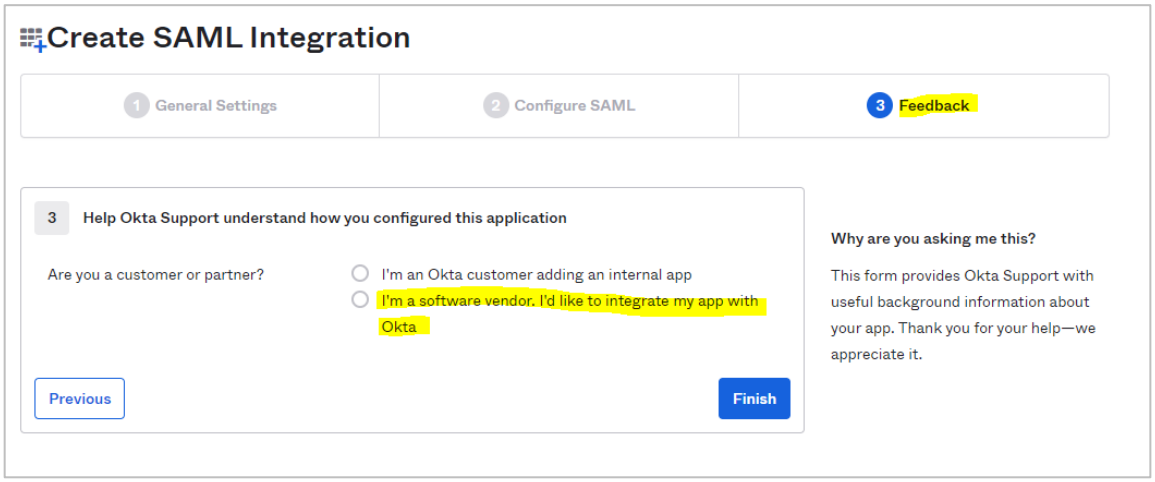
Click on **Create App Integration**. A popup will appear. Select **SAML 2.0** radio button and click Next.



In the **General Settings** tab, enter the Application Name and click Next. The next screen will ask you to integrate SAML. SAML configuration is covered in a separate document. After configuring SAML, click Next.



Next in the Feedback tab, select I'm a software vendor. I'd like to integrate my app with OKTA. And then click Finish.

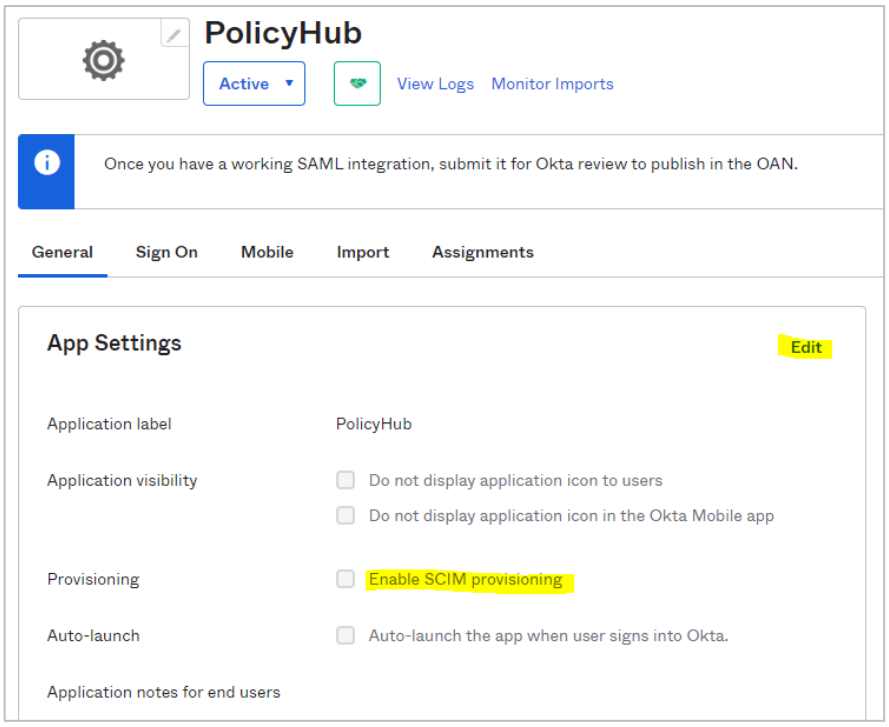


Now the application is created, we can enable SCIM provisioning.

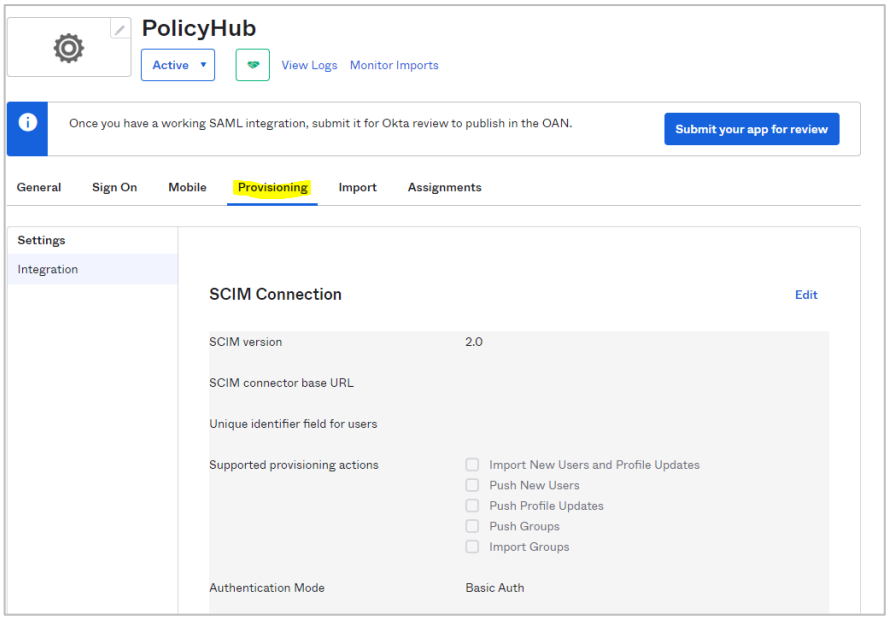
If you already have an application in OKTA, then you can jump into the Enable SCIM Provisioning section of this document.

Enable SCIM Provisioning

Once you have finished creating an application in OKTA, go to the Application menu and select PolicyHub. You will see something similar to this:



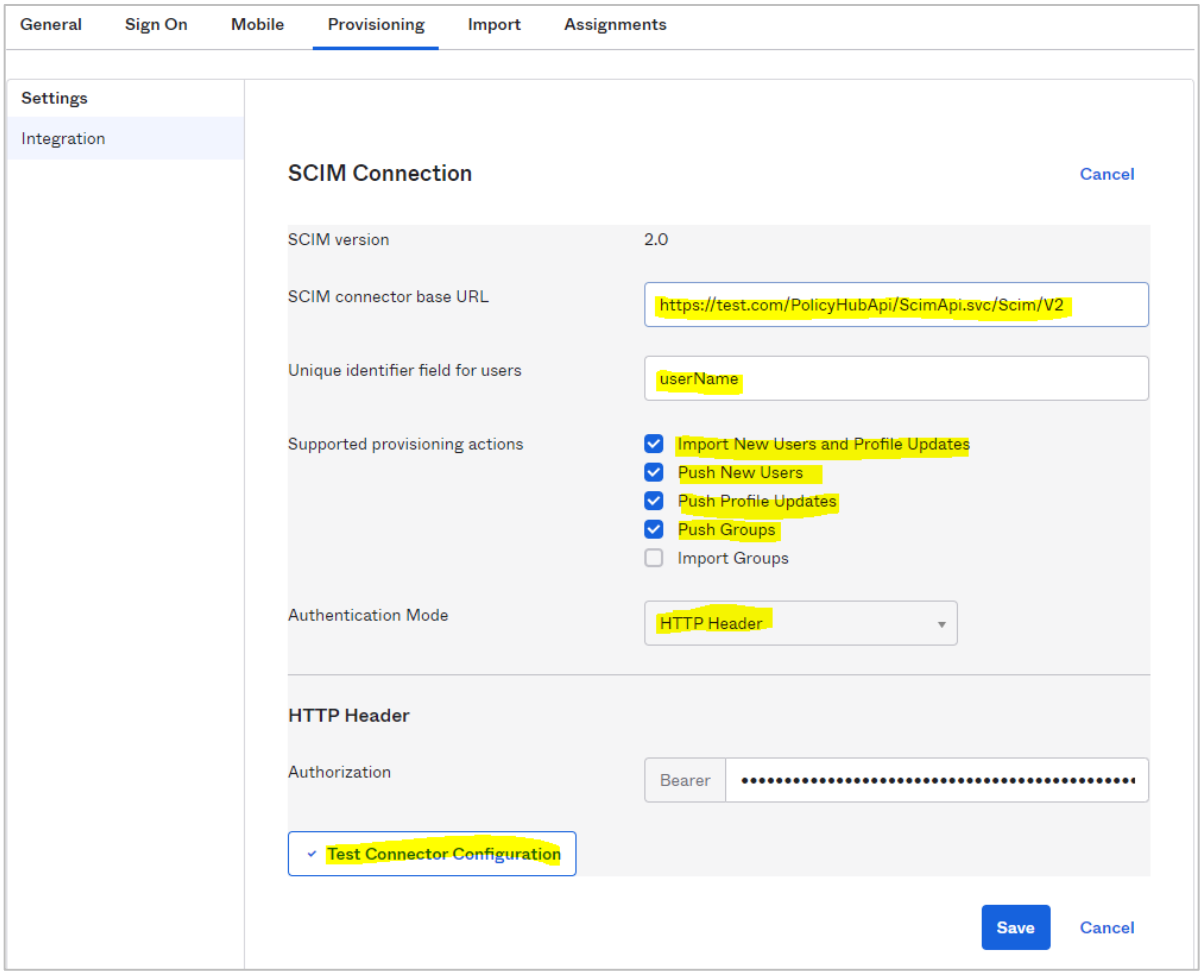
From the **General** tab, click on the Edit button and select **Enable SCIM provisioning** and click Save. Once you have saved the **General** tab changes, you will see a new tab called **Provisioning**.



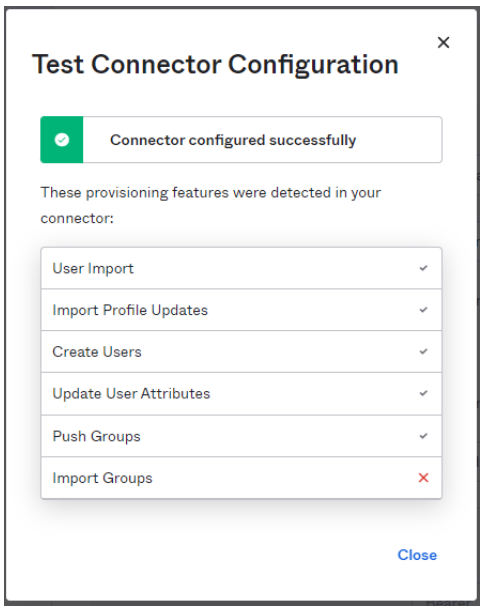
From here, you can configure the SCIM integration. Click on Edit and in the SCIM connector base URL enter the URL in this format:
https://PolicyHub Instance_URL/PolicyHubApi/ScimApi.svc/Scim/V2

In the Unique identifier field for the user text box, enter **userName**. (‘u’ should be in lower case and ‘N’ should be in upper case). In Supported provisioning actions, select the first four checkboxes.

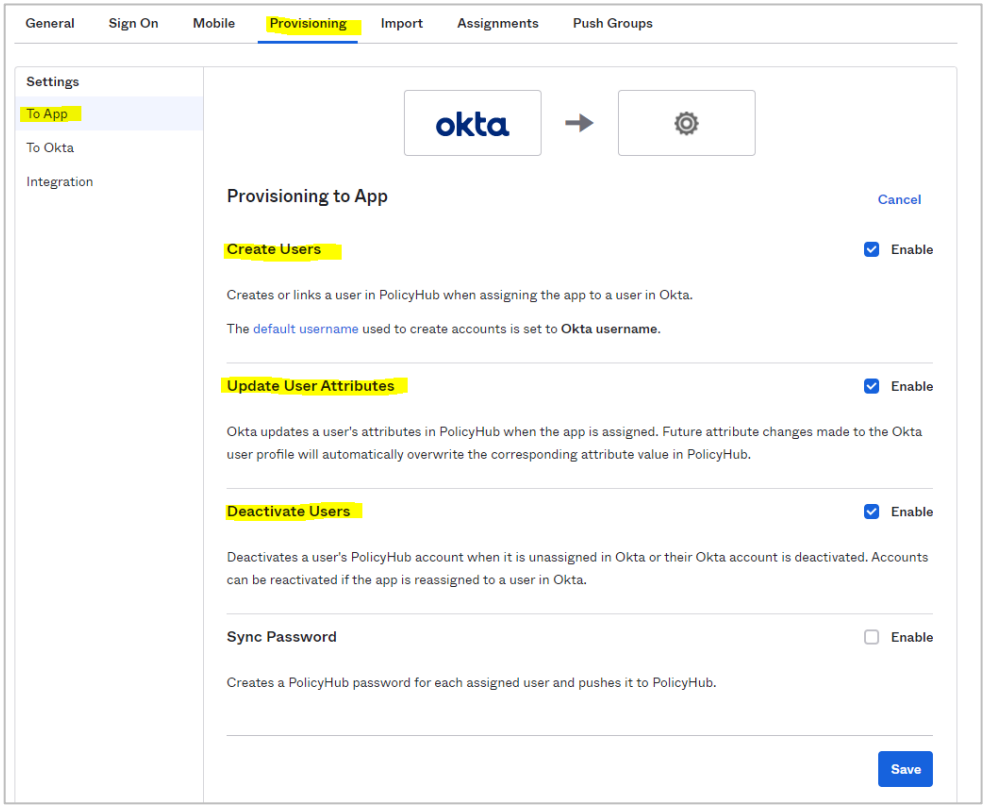
In the Authentication Mode dropdown, select HTTP Header and in the token text box enter the bearer token provided by Mitratech and then click on Test Connection.



You will see the following message once the connection test is completed.



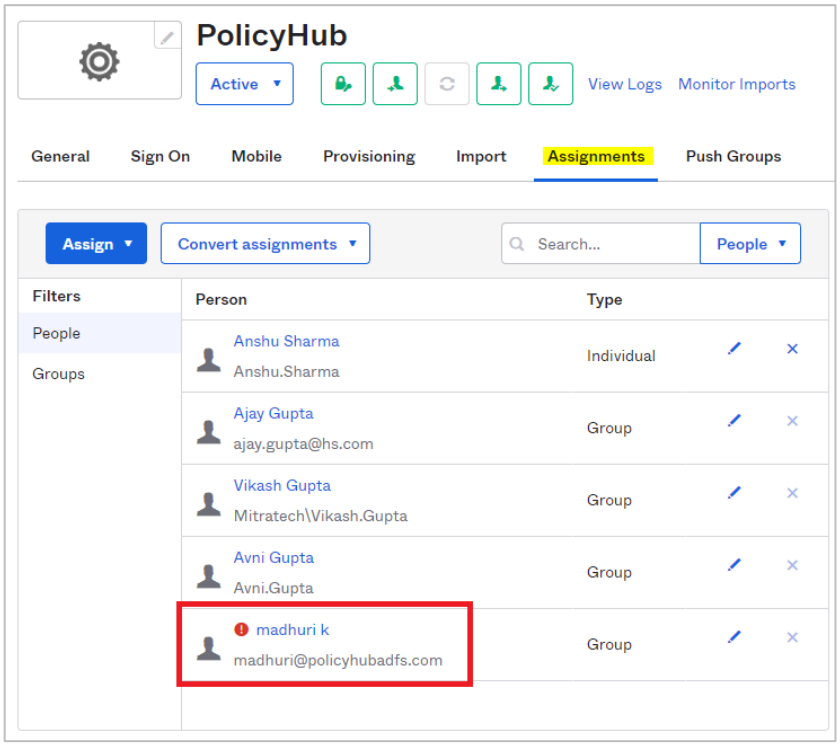
Now click on Save button. After you save you will see a new tab **To App** in panel on the left. Now you can set what operations you want to enable in SCIM. Select **Create Users**, **Update User Attributes** and **Deactivate Users** and then click **Save**.

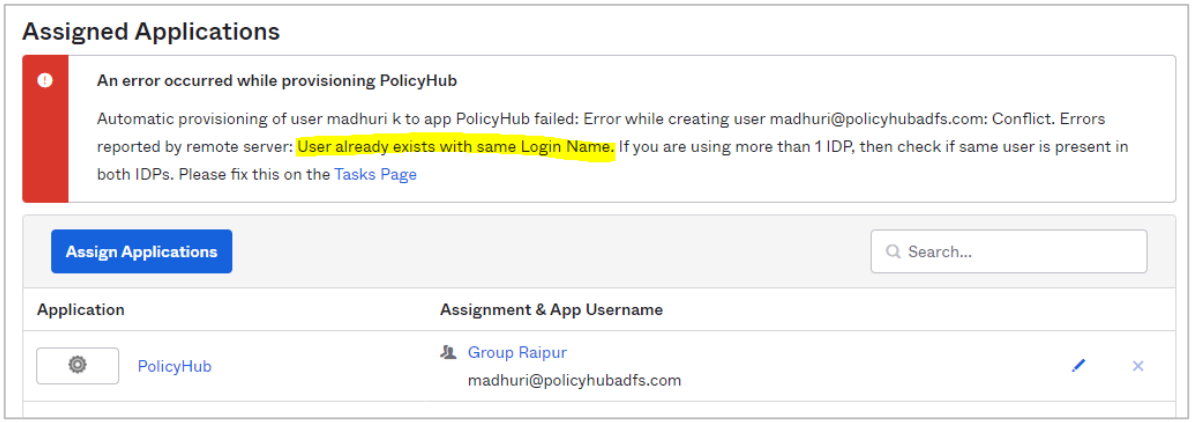


Now you have enabled SCIM Provisioning for OKTA you can start adding users and groups.

Import Users & Groups

With simple steps, you can import users and groups in OKTA. Here is the link for Getting Started: Users and Groups.
In PolicyHub, First Name, Last Name, Email and Login Name (Login ID/User ID) is mandatory. Before you assign a user to OKTA for provisioning, please make sure you have provided this 4 information in user details tab. If any user or group failed in provisioning, you can find the reason on OKTA Log. In below screenshot, you can see user **madhuri** is not added successfully. You can get exact error detail by clicking on the user from Assignments tab or from the Tasks panel from left sidebar you can see the complete error log.

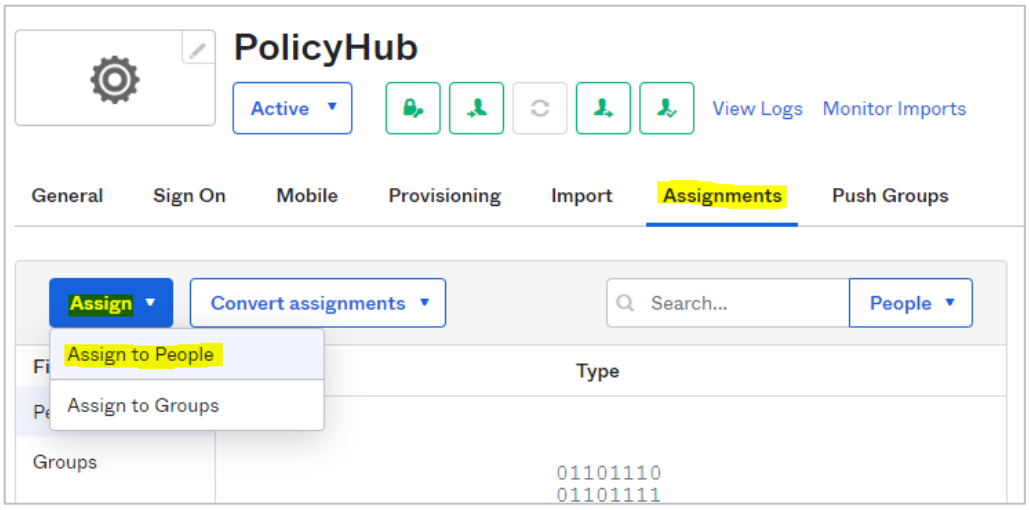




Perform User/Group Import

In OKTA, you can add Users or Groups separately in the application.

Next in this document we will cover how you can perform CRUD operations using OKTA and the PolicyHub SCIM API. Use following screen to perform User/Group related operations.



Add User

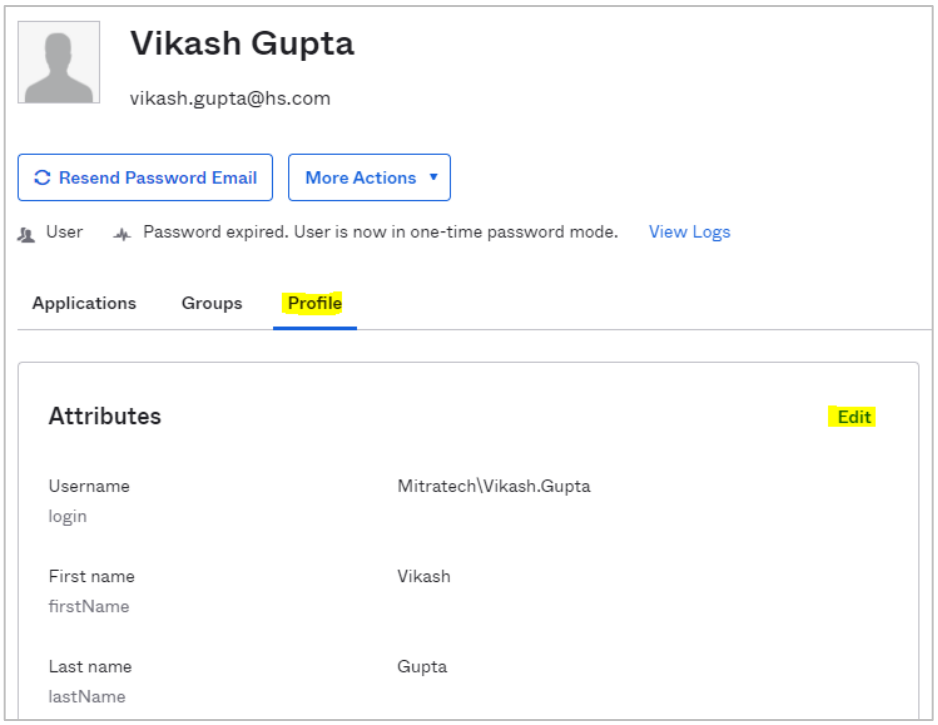
Click on the **Assign to People** dropdown item to select users that you want to assign to PolicyHub. A popup will appear from where you can select users. Make sure the user you are selecting is **Active** in OKTA and the fields First Name, Last Name, Email and Login Name (User ID / Login ID) are provided because these four fields are mandatory in PolicyHub.

From the Directory => People page you will see the list of users who are not active. These inactive users will not be included in SCIM transactions by OKTA. All users that you want to synchronize with PolicyHub should be active.

Limitation: There is no unique identifier exposed by OKTA through SCIM for a user, so if a login name gets reused, there is no way to determine if it is a new user or an existing user that was re-added. PolicyHub is configurable in how it handles this scenario, allowing the choice between always reactivating an existing user or always creating a new user, with the default being that a new user is always created. This is for safety reasons as we do not want to show the history of an old, deleted user for a new user that gets added with the same name.

Modify User

Go to Directory => People from the left sidebar menu and search for the user from the list that you want to edit. Select it and go to the Profile tab.



It's important not to edit the **Login Name** for a user. This is used to uniquely identify a user and if it is changed, then the existing user will no longer be updated with any changes from Okta and no new user will be provisioned with the same name. If this happens then the only way to continue synchronizing the user is to change the login name back again.

In many organizations the login name is consists of a combination of first name and surname and so this is a field subject to change for example when an employee gets married. In cases like this it's important to have a process around how this is handled from an IT perspective as this is beyond the control of PolicyHub and its SCIM integration with Okta.

Important: There is an issue which we've observed while editing a user. When you edit the email ID and click save then the username also get updated automatically with the email ID. In order to prevent this user from being decoupled, please make sure that after editing the email ID, that there is no change to the username. In this does change, then you will need to change it back in order to continue synchronizing the user with PolicyHub

Delete User

There are two options to remove a user from PolicyHub. Either you can unassign a user from OKTA or you can Deactivate/Delete the user from OKTA.

If you are using the unassign option, then the user will be removed from PolicyHub if the user is only in one group, but if they are in other groups as well, then they will not be removed from PolicyHub.

Add Group

There are two tabs for groups provisioning. ‘Assignment’, which can be used to assign a group to the application but will not push groups to PolicyHub.

The other option is ‘Push Groups’, which can be used to push the group to PolicyHub.

You can push groups directly to PolicyHub without using the ‘Assignment’ tab but the benefit of using the ‘Assignment’ tab is that on assigning a group, all the users assigned to the group will be created in PolicyHub automatically (but not the group itself).

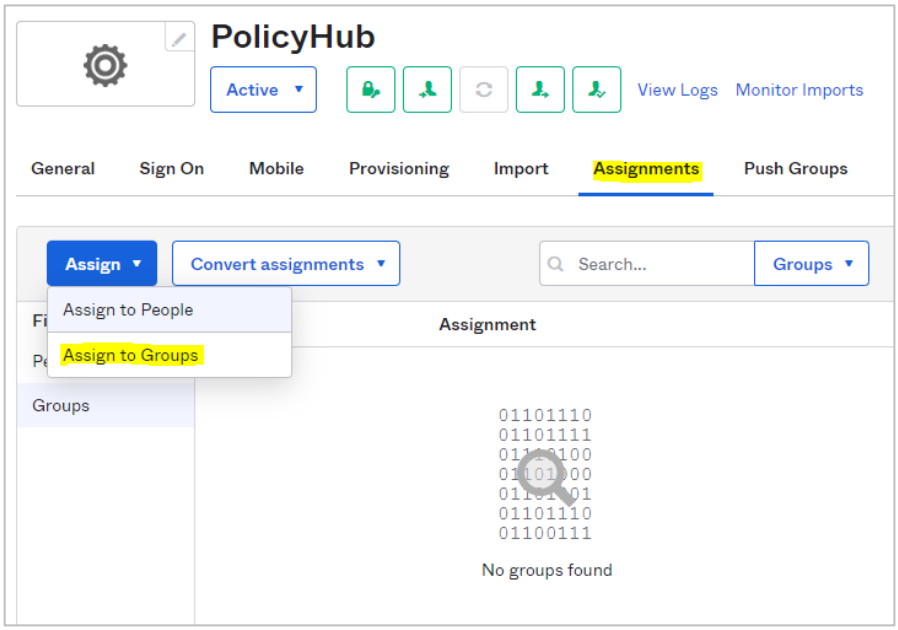
If you only use ‘Push Groups’ then the group will be created but not the users. In this scenario, you would have to link the users manually in the application.

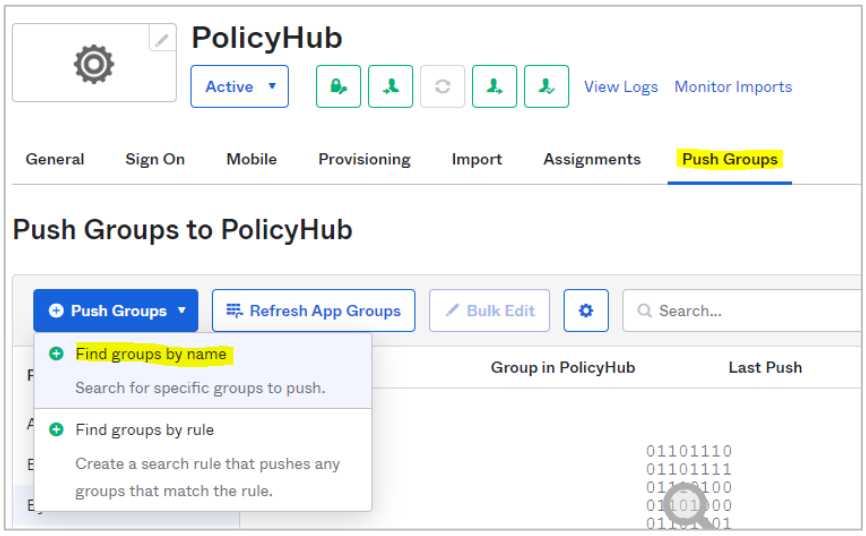
For example, if Group-A has 3 users and if you push the group then the group will be created in PolicyHub but there will be no user inside it.

If you use the Assignment tab to add the group, then first it will push all the users belonging to that group automatically to PolicyHub. Next, you just need to add the group in the Push Groups tab.

Using these 2 simple steps will import the group as well as the users. If you later add or remove a user from the group, then it will be synchronized with PolicyHub automatically.

In summary, the recommended way to synchronize groups with PolicyHub is firstly to assign the group from Assignments tab and then use the Push Groups tab to push the group.





Search for a group by name and click Save. All the users linked to the group and the group itself will be imported to PolicyHub.

LIMITATION:

- OKTA does not support group hierarchy and so all groups will appear as top-level root groups in PolicyHub. This can make it challenging when targeting specific groups during the publication process.

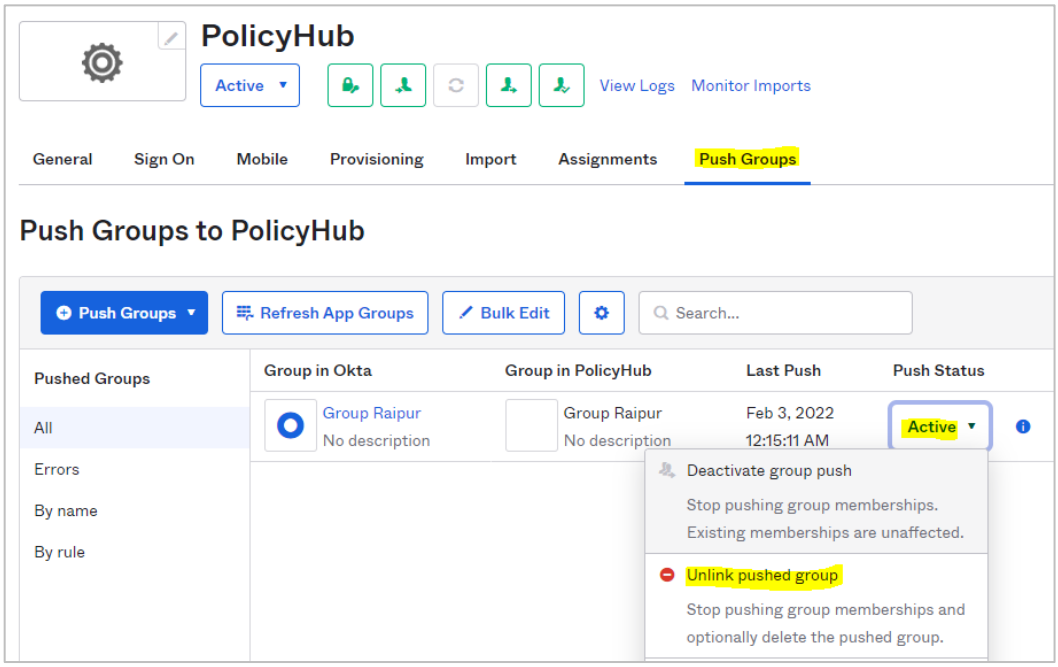
Modify Group

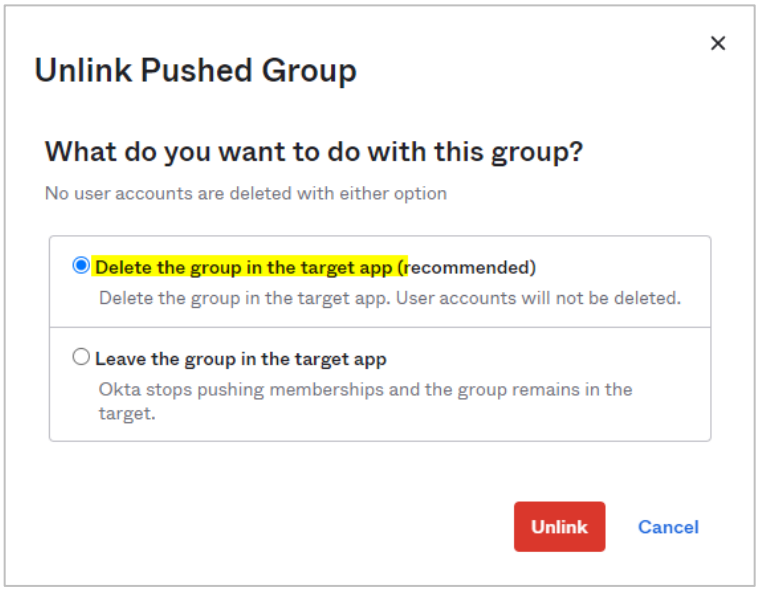
Go to Directory => Group from the left sidebar menu and search for a group from the list that you want to edit. Select it and go to the Profile tab. You can now change the group name.
From the People tab in the same page, you can add or remove members from a Group.

Delete a Group

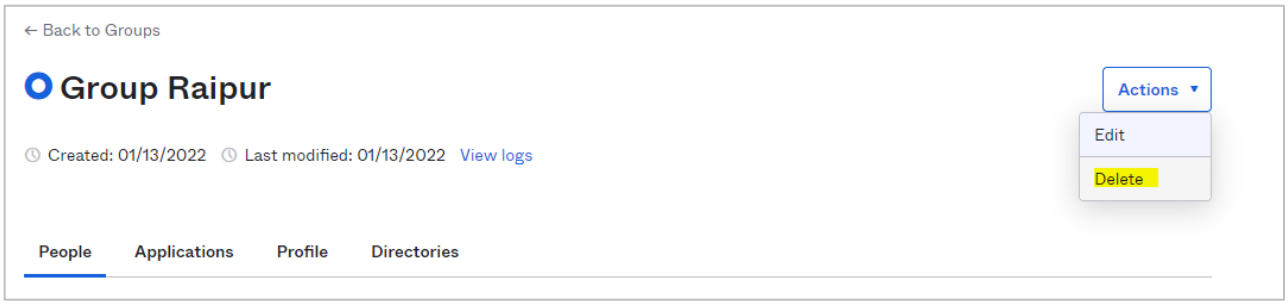
To delete a group, you have two options

1. You can go to Push Groups tab where you will find an option to remove the group from the OKTA Application. Select **Delete the group in the target app (recommended).** This will unlink the group from the application in OKTA and will remove the group from PolicyHub.





2. Go to Directory => Groups and select the group that you want to delete. From the Actions dropdown, click Delete.

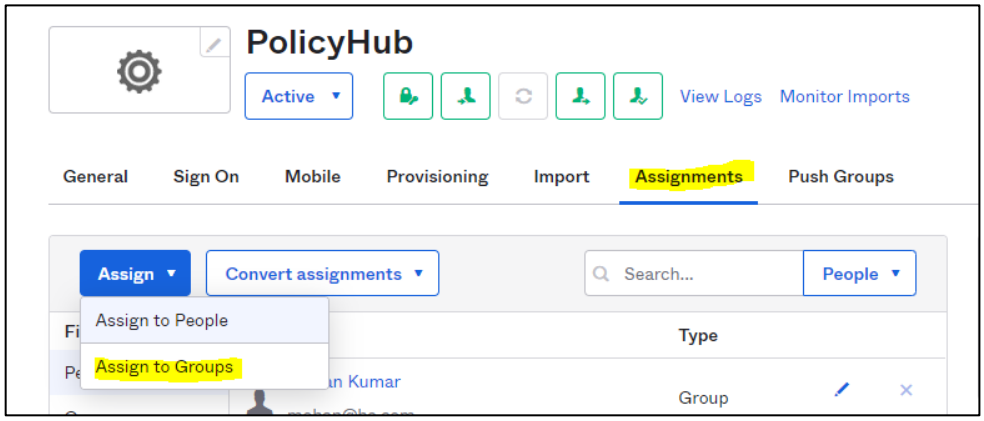


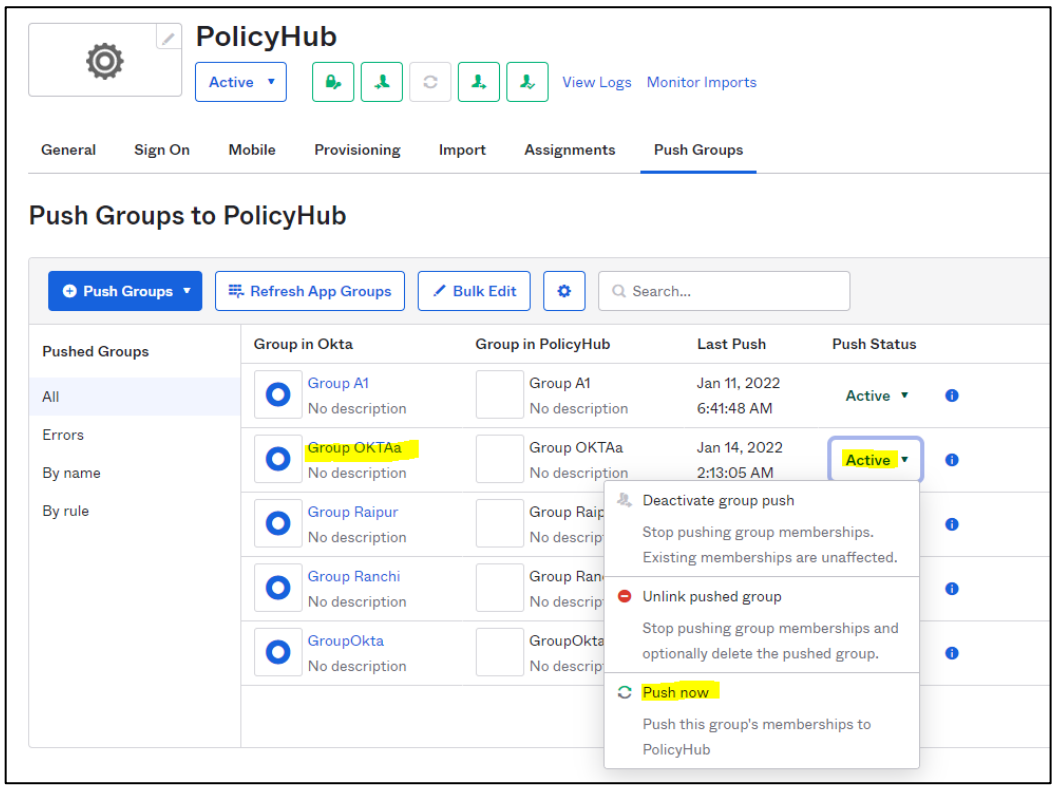
Recommendation

Always assign a group before a push. If you don't, then sometimes it will be difficult to find out why some users are not getting added to a group even though the group is active and present in PolicyHub.

Troubleshooting

In the event of any mismatch between user and group mappings, go to the 'Assignment' tab and check if the group is present or not. If not, then assign it and then got to 'Push Groups' and from the Push Status dropdown, click 'Push Now'.


PolicyHub
Active
View Logs
Monitor Imports
General
Sign On
Mobile
Provisioning
Import
Assignments
Push Groups
Assign
Convert assignments
Search...
People
Assign to People
Assign to Groups
Type
Group


PolicyHub
Active
View Logs
Monitor Imports
General
Sign On
Mobile
Provisioning
Import
Assignments
Push Groups
Push Groups to PolicyHub
Push Groups
Refresh App Groups
Bulk Edit
Search...
Pushed Groups
All
Errors
By name
By rule
Group in Okta
Group in PolicyHub
Last Push
Push Status
Group A1
No description
Jan 11, 2022
6:41:48 AM
Active
Group OKTAa
Jan 14, 2022
2:13:05 AM
Group Raipur
Group Ranchi
GroupOkta
Deactivate group push
Stop pushing group memberships.
Existing memberships are unaffected.
Unlink pushed group
Stop pushing group memberships and
optionally delete the pushed group.
Push now
Push this group's memberships to
PolicyHub

www.mitratech.com

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