



Axiad Cloud
OKTA SCIM & SAML
Configuration Guide

OKTA SCIM INTEGRATION TO AXIAD CLOUD	3
PREREQUISITES/REQUIREMENTS	3
SUPPORTED FEATURES	3
KNOWN ISSUES AND LIMITATIONS	3
OKTA & SCIM CONFIGURATIONS	4
1. CREATE APPLICATION	4
2. CONFIGURE AXIAD CLOUD APP FOR PROVISIONING	9
3. CONFIGURE ASSIGNMENTS FOR THE AXIAD CLOUD APP	14
4. TO REMOVE USERS FROM SCIM PROVISIONING	15
5. TO PROVISION GROUPS TO AXIAD CLOUD	16
6. TO MODIFY A GROUP BEING PROVISIONED – PUSH, REMOVE OR STOP	20
TROUBLESHOOTING	22

OKTA SCIM Integration to Axiad Cloud

Use case

This use case is for when you want to defer Axiad Cloud's authentication to an external IdP in this case OKTA via SAML protocol and provision users via SCIM over the Internet. The authentication will be handled by the OKTA as the IdP, and Axiad Cloud will trust the returned result. Users will be populated into Axiad Cloud vis SCIM integration.

In addition to OKTA this also supports all IdP vendors that support SAML v2.0 and SCIM 2.0, such as OKTA, Ping, etc. Refer to dedicated documentation for each.

Prerequisites/Requirements

There are a couple of things you need to do before you can provision external users into your sites and products:

1. Get the user provisioning functionality for your Okta account. See [Lifecycle Management](#) for more details.
2. Ensure that your OKTA Org is integrated to you Active Directory or other user directory source. If you need instructions for [Installing the Okta Active Directory Agent](#).

Supported Features

- Provisioning of Users and Groups through SCIM
- Single Sign On (SSO) through SAML

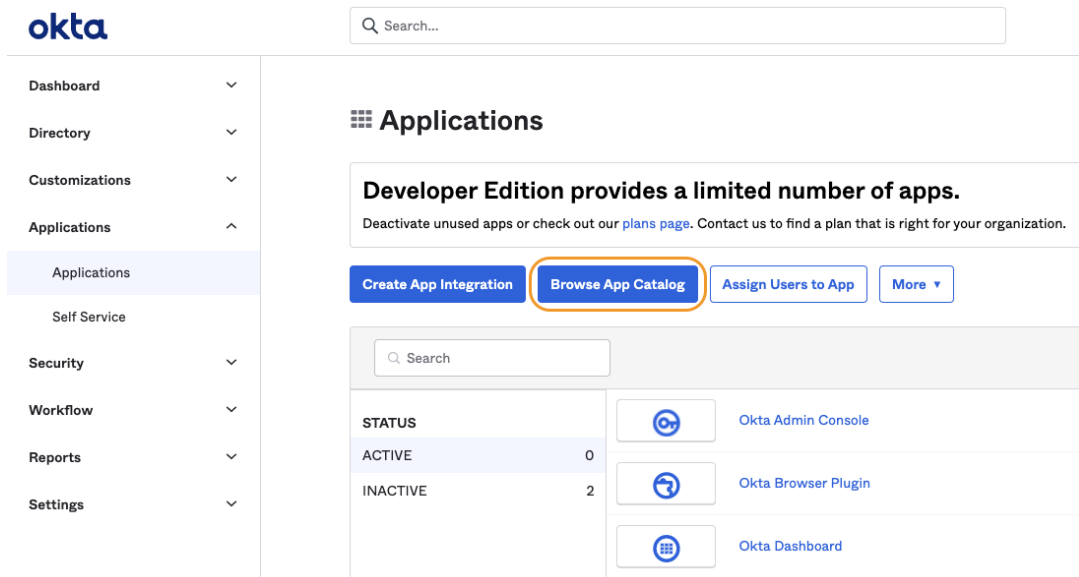
Known Issues and Limitations

- No support for Okta password provisioning through SCIM
- Only support for SCIM 2.0
- No support for case sensitive usernames
- Single Sign On (SSO) through OpenID not tested

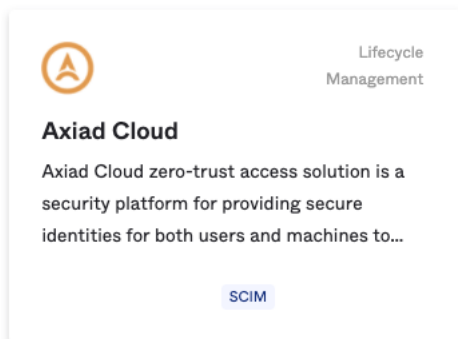
OKTA & SCIM Configurations

1. Create Application

- 1.1. Log into your OKTA org – Your URL may vary based on your configuration and/or custom domain
- 1.2. Click on ‘Applications’ on the left and then click on ‘Applications’ in the drop down submenu
- 1.3. Click the ‘Browse App Integration Catalog’ button



- 1.4. Search for the ‘Axiad Cloud’ application and click on it to open



1.5. Click on the 'Add' button

[← Back to Add Application](#)



Axiad Cloud

[Overview](#) [Capabilities](#)

Overview

Axiad Cloud zero-trust access solution is a security platform for providing secure identities for both users and machines to protect access to sensitive data for all users, devices and applications. The Okta Axiad Cloud integration allows Users and Groups to be securely provisioned to Axiad Cloud so customers can issue secure identities and realize a passwordless environment.



Use Case

[Lifecycle Management](#)

[Single Sign-On](#)

Functionality

[SAML](#)

[SWA](#)

[SCIM](#)

1.6. If you would like to change the 'Application label' you can change that now or leave it as Axiad Cloud then click the 'Done' button.

Add Axiad Cloud

1 General Settings


General Settings - Required

Application label	<input type="text" value="Axiad Cloud"/>
This label displays under the app on your home page	
Application Visibility	<input type="checkbox"/> Do not display application icon to users
	<input type="checkbox"/> Do not display application icon in the Okta Mobile App
Cancel	Done




General settings
All fields are required to add this application unless marked optional.

- 1.7. Once added it will take you to the Axiad Cloud application configuration page. Click on the 'Sign On' tab then click the 'Edit' link

[← Back to Applications](#)



Axiad Cloud

Active    [View Logs](#) [Monitor Imports](#)

General **Sign On** **Mobile** **Provisioning** **Import** **Assignments** **Push Groups**

Settings Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)


SAML 2.0

Default Relay State




Disable Force Authentication

- 1.8. Under the 'SAML 2.0' section enter the URI provided by Axiad Support in the 'Default Relay State' field

[← Back to Applications](#)



Axiad Cloud

Active ▾    [View Logs](#) [Monitor Imports](#)


[General](#) [Sign On](#) [Mobile](#) [Provisioning](#) [Import](#) [Assignments](#) [Push Groups](#)

Settings Cancel

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

 SAML 2.0 is the only sign-on option currently supported for this application.

SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState.

Attributes (Optional) [Learn More](#)

Disable Force Authentication Never prompt user to re-authenticate.

[Preview SAML](#)

- 1.9. Scroll down to the 'Advanced Sign-on Settings' section and enter the 'ACS URL' and 'Audience URI' provided by Axiad Support in their corresponding fields

Advanced Sign-on Settings

These fields may be required for a Axiad Cloud proprietary sign-on option or general setting.

ACS URL

Please enter your ACS URL. Refer to the Setup Instructions to obtain this value.

Audience URI

Please enter your Audience URI. Refer to the Setup Instructions to obtain this value.

Credentials Details

Application username format

Update application username on

Password reveal Allow users to securely see their password (Recommended)

i Password reveal is disabled, since this app is using SAML with no password.

Save

NOTE: The URLs & URIs will be provided by Axiad but below are two examples of formatting

Production Stack Default Relay State & ACS URL

<https://access-user-infinidim.cloud.axiadids.net/auth/realms/master/>

Demo/Test Stack Default Relay State & ACS URL

<https://access-access-user-infinidim.demo.axiadids.net/auth/realms/master/>

Production Stack Audience URI

<https://access-user-infinidim.cloud.axiadids.net/auth/realms/master/broker/okta-infinidim/endpoint>

Demo/Test Stack Audience URI

<https://access-user-infinidim.demo.axiadids.net/auth/realms/master/broker/okta-infinidim/endpoint>

1.10. Click on the 'Preview SAML' button and copy the URL and provide to Axiad Support

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="id19616626039614281885910243" IssueInstant="2022-03-11T22:10:53.495Z" Version="2.0">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">http://www.okta.com/Issuer</saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">userName</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2022-03-11T22:15:53.693Z"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2022-03-11T22:05:53.693Z" NotOnOrAfter="2022-03-11T22:15:53.693Z">
    <saml2:AudienceRestriction>
      <saml2:Audience/>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2022-03-11T22:10:53.495Z">
    <saml2:AuthnContext>
      <saml2:AuthnContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
</saml2:Assertion>
```

1.11. Back on the 'Sign-In Options' page click the 'Save' button at the bottom of the page.

2. Configure Axiad Cloud App for Provisioning

2.1. Click on the 'Provisioning' tab then click on the 'Configure API Integration' button

← Back to Applications

Axiad Cloud Active View Logs Monitor Imports

General Sign On Mobile **Provisioning** Import Assignments Push Groups

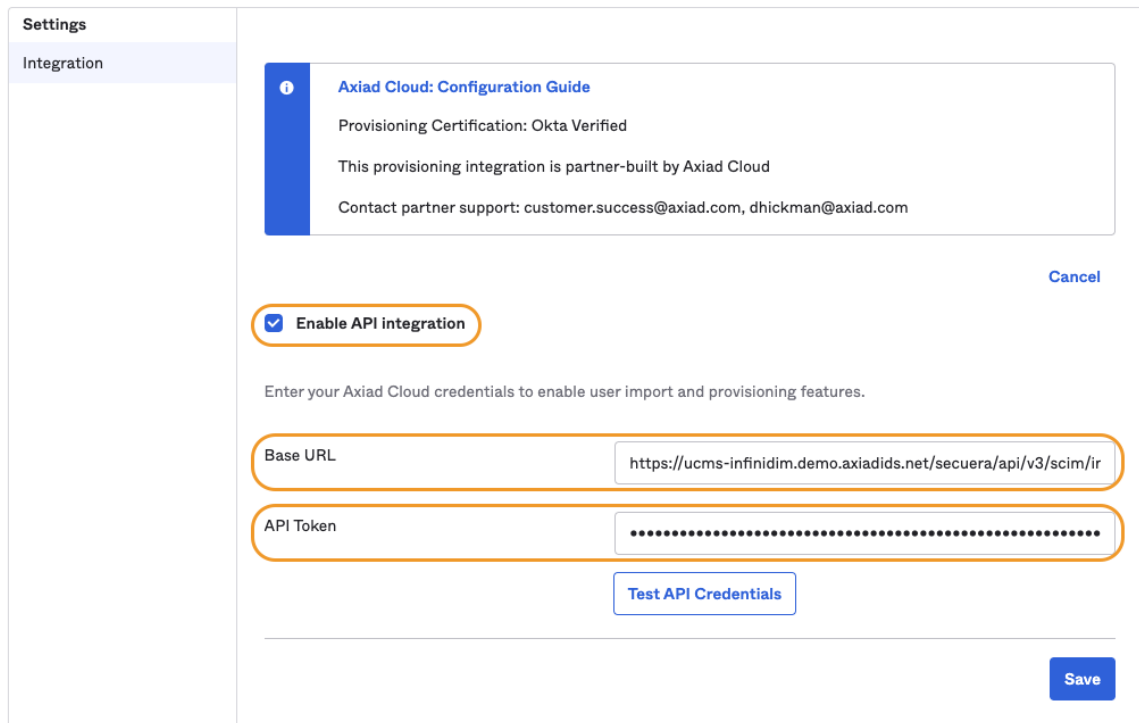
Settings
Integration

Axiad Cloud: Configuration Guide
Provisioning Certification: Okta Verified
This provisioning integration is partner-built by Axiad Cloud
Contact partner support: customer.success@axiad.com

Provisioning is not enabled
Enable provisioning to automate Axiad Cloud user account creation, deactivation, and updates.

Configure API Integration

- 2.2. Click the 'Enable API integration' check box, then enter the SCIM API URL provided by Axiad Support in the 'Base URL' field and enter the API key provided by Axiad Support in the 'API Token' field



NOTE: This URL will be provided by Axiad but below are two examples

Production Stack

<https://ucms-infinidim.cloud.axiadids.net/secuera/api/v3/scim/infinidim>

Demo/Test Stack

<https://ucms-infinidim.demo.axiadids.net/secuera/api/v3/scim/infinidim>

NOTE: This is a permanent OAuth Bearer Token API key generated by Axiad and provided via a secure file transfer method, this is not customer generated key


- 2.3. Click the 'Test API Credentials' button



- 2.4. Once you see the message that the OAuth Bearer Token was verified successfully you can click the 'Save' button at the bottom

2.5. Under the 'Provisioning' tab click the 'Edit' link

[← Back to Applications](#)





Axiad Cloud

[Active](#) [View Logs](#) [Monitor Imports](#)

[General](#) [Sign On](#) [Mobile](#) [Provisioning](#) [Import](#) [Assignments](#) [Push Groups](#)

Settings

- To App
- To Okta
- Integration

 → 

Provisioning to App [Edit](#)

Create Users Enable

Creates or links a user in Axiad Cloud when assigning the app to a user in Okta.

The [default username](#) used to create accounts is set to **Okta username**.

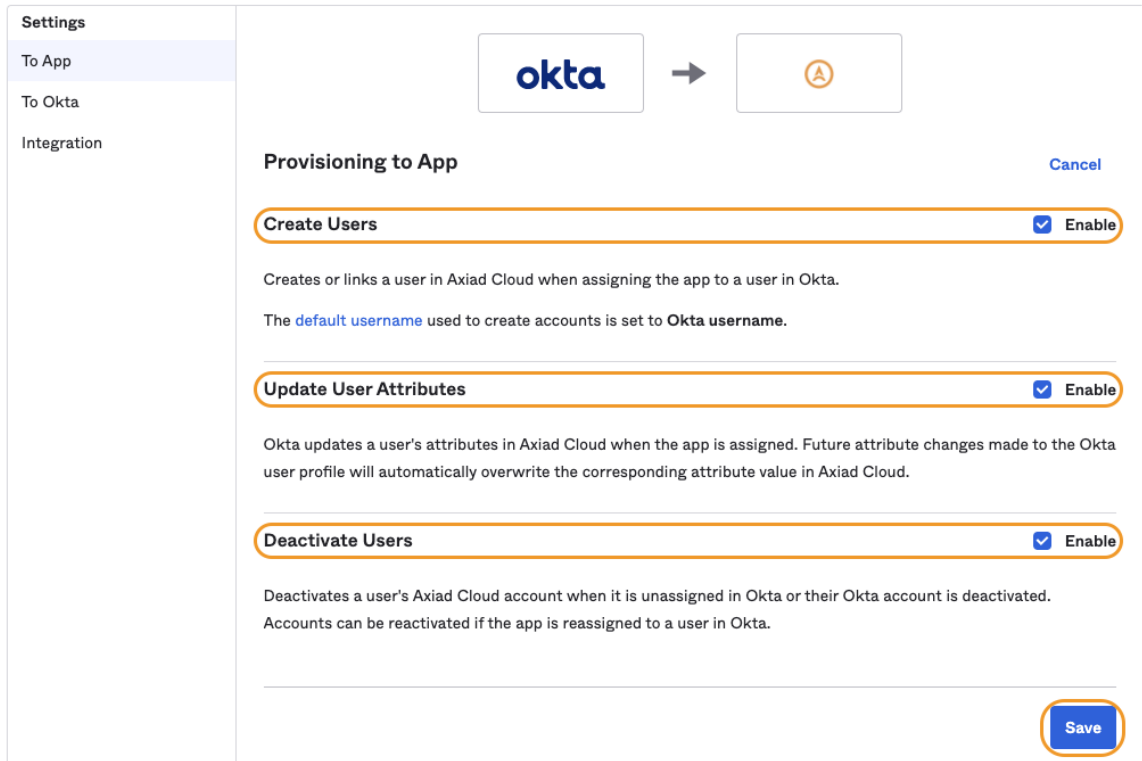
Update User Attributes Enable

Okta updates a user's attributes in Axiad Cloud when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Axiad Cloud.

Deactivate Users Enable


Deactivates a user's Axiad Cloud account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

2.6. Check the boxes to Enable 'Create Users', 'Update User Attributes' and 'Deactivate Users' then click the 'Save' button at the bottom



Settings

- To App
- To Okta
- Integration

okta → 

Provisioning to App Cancel

Create Users Enable

Creates or links a user in Axiad Cloud when assigning the app to a user in Okta.

The **default username** used to create accounts is set to **Okta username**.

Update User Attributes Enable

Okta updates a user's attributes in Axiad Cloud when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Axiad Cloud.

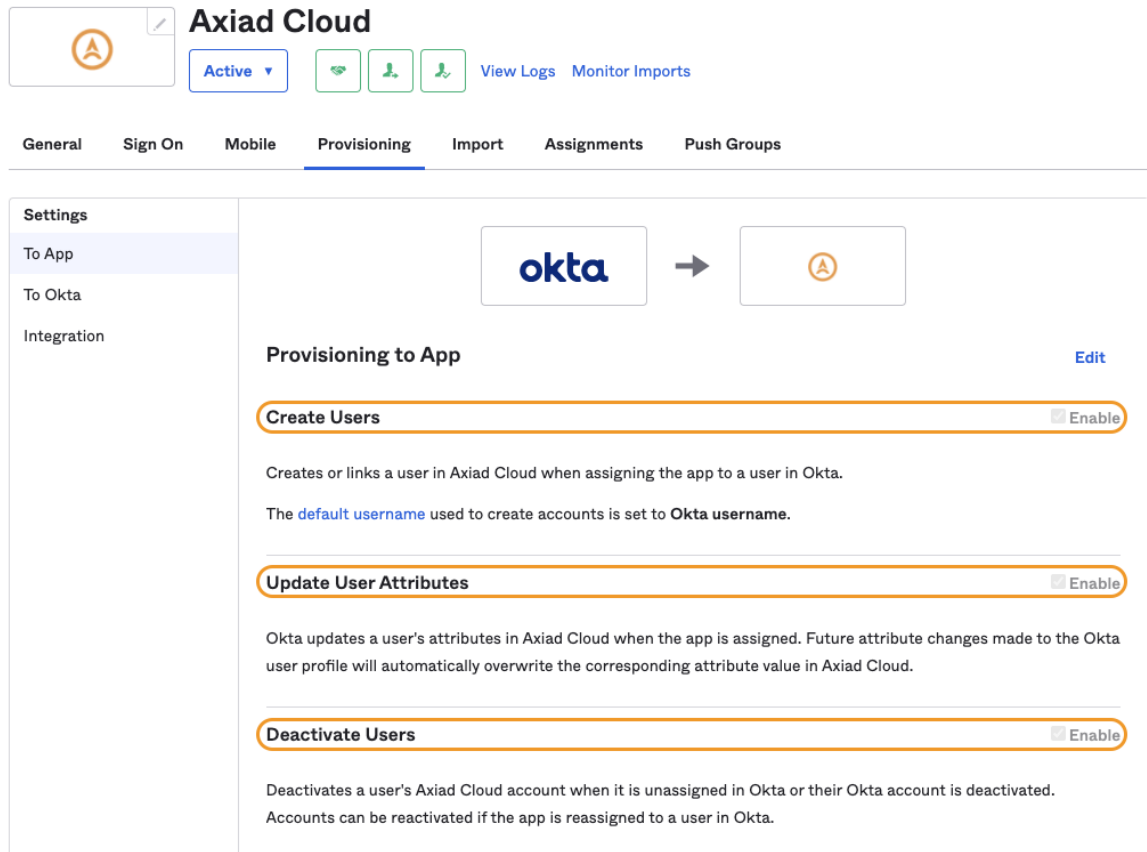
Deactivate Users Enable

Deactivates a user's Axiad Cloud account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.




Save

2.7. You should now see the 'Provisioning to App' page and it should be configured for the following options:

- Create Users
- Update Users
- Deactivate Users



Axiad Cloud

Active ▾    [View Logs](#) [Monitor Imports](#)

General Sign On Mobile **Provisioning** Import Assignments Push Groups

Settings

- To App
- To Okta
- Integration

Provisioning to App [Edit](#)

Create Users Enable

Creates or links a user in Axiad Cloud when assigning the app to a user in Okta.

The **default username** used to create accounts is set to **Okta username**.

Update User Attributes Enable

Okta updates a user's attributes in Axiad Cloud when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Axiad Cloud.

Deactivate Users Enable

Deactivates a user's Axiad Cloud account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

NOTE: Sync Password is not supported by Axiad at this time and will not be shown as an available option.

2.8. The Axiad Cloud app should be configured by default with the following Attribute Mappings:

- **userName** (In OKTA this has to be an email address and is not configurable)
- **giveName** user.lastName
- **familyName** user.lastName
- **email** user.email
- **emailType** (user.email != null && user.email != "") ? 'work' : "

Axiad Cloud Attribute Mappings

Select a(n) Axiad Cloud attribute to set its value based on values stored in Okta.

[Go to Profile Editor](#)

[Force Sync](#)

Attribute	Attribute Type	Value	Apply on
Username userName	Personal	Configured in Sign On settings	
Given name givenName	Personal	user.firstName	Create and update ✎ ✕
Family name familyName	Personal	user.lastName	Create and update ✎ ✕
Primary email email	Personal	user.email	Create and update ✎ ✕
Primary email type emailType	Personal	(user.email != null && user.email != "") ? 'work' : "	Create and update ✎ ✕

[Hide Unmapped Attributes](#)

NOTE: If you require additional attributes you can add by clicking 'Show Unmapped Attributes' but coordinate with Axiad Support to ensure they are mapped properly in Axiad Cloud.

3. Configure Assignments for the Axiad Cloud App

- 3.1. Click on the 'Assignments' tab
- 3.2. Click on the 'Assign' button then select either 'Assign to People' or 'Assign to Groups'

General Sign On Mobile Provisioning Import **Assignments** Push Groups

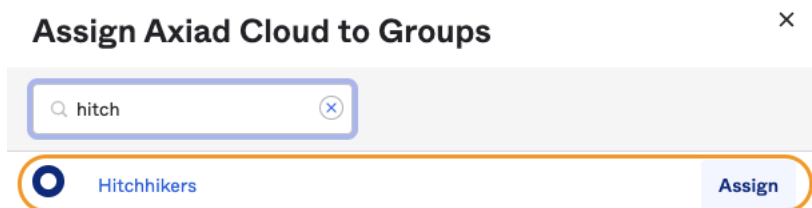
[Assign](#) [Convert assignments](#) [People](#)

Type
Groups
01101110 01101111

NOTE: Assign to Groups adds the Users in that Group but does not assign the Group to be provisioned.

Groups can be either created in OKTA or imported from conXions Active Directory or other OKTA supported directory.

- 3.3. In the pop-up window search for the User or Group you wish to add to provisioning and click 'Assign' on the right side

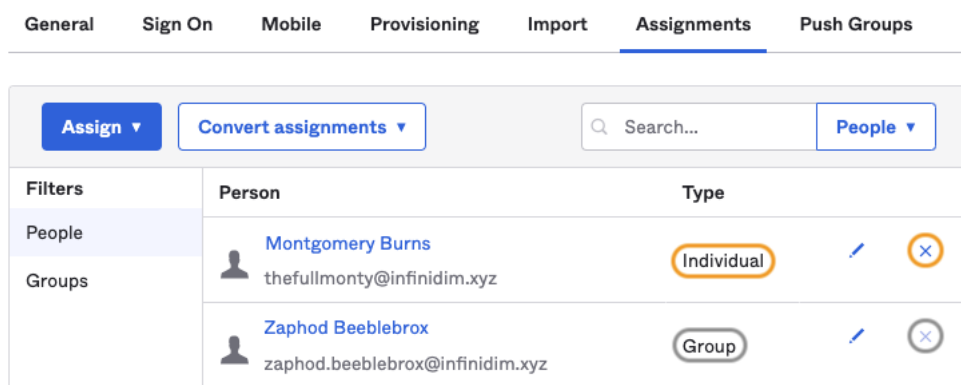


- 3.4. When you have selected all the Users or Groups you want to assign click the 'Done' button at the bottom.
- 3.5. Those Users will now be provisioned

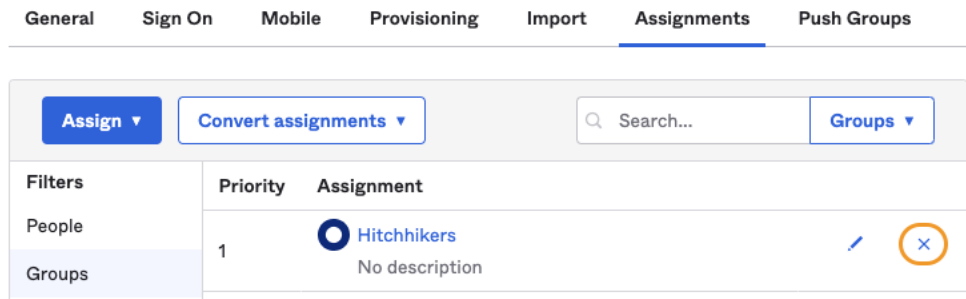
NOTE: To configure a proper sync of users and groups, both the user and the group must be assigned the SCIM application within Okta. This will enable them both be provisioned on the Axiad side and maintain proper group membership.

4. To Remove Users from SCIM Provisioning

- 4.1. Click on 'Assignments' tab
- 4.2. If you want to remove a User that was assigned, individually find the User and click on the 'X' to the right of their Name
- 4.3. If the 'X' next to the User is grayed out that means the User was assigned as part of a Group Assignment



4.4. If you want to remove a Group click on 'Groups' on the left then find the Group and click on the 'X' on the right side

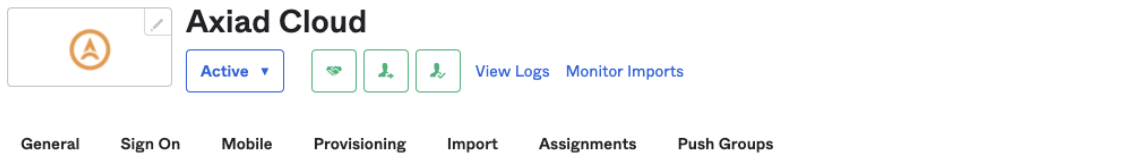


4.5. This will remove all users in that group from provisioning

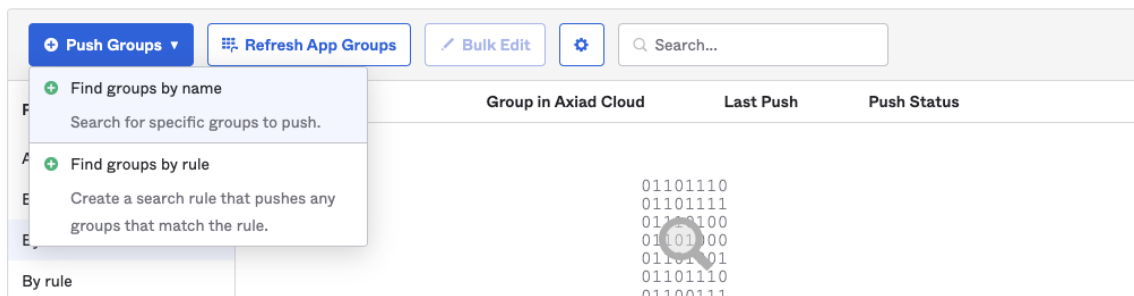
5. To Provision Groups to Axiad Cloud

5.1. Click on the 'Push Groups' tab

5.2. Click on the '+ Push Groups' button then select either '+ Find groups by name' or '+Find groups by rule'

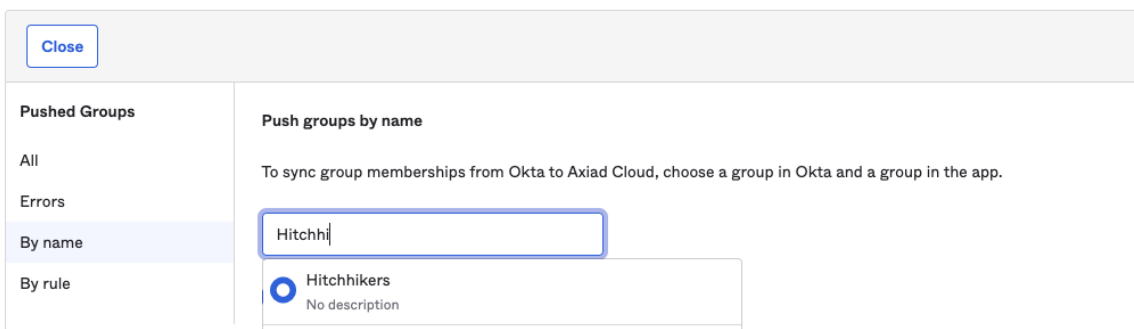


Push Groups to Axiad Cloud



5.3. If you clicked 'Find groups by name' start entering the Group name and once the predictive search finds the correct Group, click on the Group.

Push Groups to Axiad Cloud



5.4. Once you have selected the Group you plan on adding, if you want to add an additional Group click on the 'Save & Add Another' button, when done click the 'Save' button

Push Groups to Axiad Cloud

[Close](#)

Pushed Groups

- All
- Errors
- By name**
- By rule

Push groups by name

To sync group memberships from Okta to Axiad Cloud, choose a group in Okta and a group in the app.

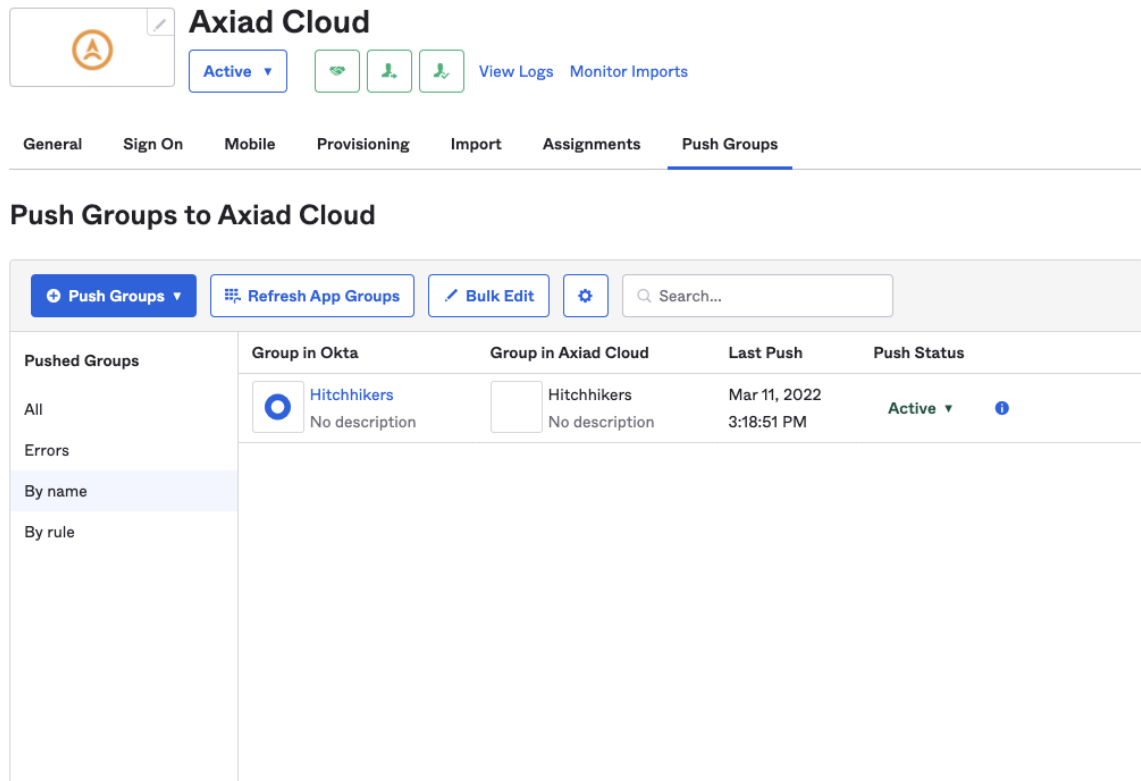
 Push group memberships immediately

Group	Match result & push action
<input checked="" type="radio"/> Hitchhikers	Match found Link Group ▼ <input type="text" value="Hitchhikers"/>




[Save](#) [Save & Add Another](#)

5.5. When you get back to the Push Groups tab it will attempt to push the Group and will transition from Pushing to Active

[← Back to Applications](#)






Axiad Cloud

Active ▾    [View Logs](#) [Monitor Imports](#)

General Sign On Mobile Provisioning Import Assignments **Push Groups**

Push Groups to Axiad Cloud

[Push Groups](#) ▾ [Refresh App Groups](#) [Bulk Edit](#) 

Pushed Groups	Group in Okta	Group in Axiad Cloud	Last Push	Push Status
All	 Hitchhikers No description	<input type="checkbox"/> Hitchhikers No description	Mar 11, 2022 3:18:51 PM	Active ▾ 
Errors				
By name				
By rule				

5.6. If you clicked 'Find groups by rule' enter a rule name to track how the rules are pushing groups.

5.7. The rules have two options to filter from, "Group name" and "Group description. Both can be filtered based on "starts with", "ends with", or "contains".

5.7.1. **Note:** Okta requires that both of these filters be filled in to create a rule.

5.8. The example screen shot below is showing a rule that will push groups that have been synchronized to Okta from Active Directory and have added "Active Directory" in the description to denote this.



Axiad Cloud SCIM & SAML

Active ▾



[View Logs](#) [Monitor Imports](#)



Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

[Submit your app for review](#)

[General](#)

[Sign On](#)

[Mobile](#)

[Provisioning](#)

[Import](#)

[Assignments](#)

[Push Groups](#)

Push Groups to Axiad Cloud SCIM & SAML

[Close](#)

Pushed Groups

All

Errors

By name

By rule

Push groups by rule

Create a search rule that pushes any matching groups to Axiad Cloud SCIM & SAML automatically.

Rule name

Push groups synchronized from AD

Group name

ends with ▾

AD

Group description

contains ▾

Active Directory

Immediately push groups found by this rule

[Create Rule](#)

[Cancel](#)

5.9. Once your rule has the filters set, select "Create Rule"

6. To Modify a Group being Provisioned – Push, Remove or Stop

6.1. Click on the 'Push Groups' tab

6.2. To push now click on the 'Active' link and from the drop down select 'Push Now'

General Sign On Mobile Provisioning Import Assignments **Push Groups**

Push Groups to Axiad Cloud

[+ Push Groups](#)
[Refresh App Groups](#)
[Bulk Edit](#)

Pushed Groups	Group in Okta	Group in Axiad Cloud	Last Push	Push Status
All	Hitchhikers No description	Hitchhikers No description	Mar 11, 2022 3:18:51 PM	Active ▼ ⓘ
Errors				<ul style="list-style-type: none"> 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 Axiad Cloud
By name				
By rule				

6.3. To remove the group from provisioning and delete the group from Axiad Cloud click on the 'Active' link then select 'Unlink pushed group'

General Sign On Mobile Provisioning Import Assignments **Push Groups**

Push Groups to Axiad Cloud

[+ Push Groups](#)
[Refresh App Groups](#)
[Bulk Edit](#)

Pushed Groups	Group in Okta	Group in Axiad Cloud	Last Push	Push Status
All	Hitchhikers No description	Hitchhikers No description	Mar 11, 2022 3:18:51 PM	Active ▼ ⓘ
Errors				<ul style="list-style-type: none"> 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 Axiad Cloud
By name				
By rule				

6.4. On the pop up window select 'Delete the group in the target app (recommended)' and click the 'Unlink' button

Unlink Pushed Group

×

What do you want to do with this group?

No user accounts are deleted with either option

- Delete the group in the target app (recommended)**
Delete the group in the target app. User accounts will not be deleted.
- Leave the group in the target app**
Okta stops pushing memberships and the group remains in the target.

Unlink

Cancel

Congratulations your OKTA Axiad Cloud integration is complete!



Troubleshooting

Please contact Axiad Support for assistance with troubleshooting

<https://axiad.com/support>

support@axiad.com

|