



# Setting Up OKTA SSO & SCIM

A step-by-step guide to configuring Single Sign-On and automated user provisioning

Questions?

Need help with setup?

**Support@wellnesscoach.live**

# KEY CONFIGURATION DETAILS

Reference these values during SSO and SCIM setup

Parameter	Value
Single Sign-On URL	<a href="https://api.meditation.live/auth/sso/callback">https://api.meditation.live/auth/sso/callback</a>
Audience URI (SP Entity ID)	<b>WellnessCoach</b>
Default Relay State	<b>Obtain from Wellness Coach Admin Portal</b>
Name ID Format	<b>EmailAddress</b>
Application Username	<b>Okta username</b>
SCIM 2.0 Base URL	<a href="https://ed.wellnesscoach.live/scim">https://ed.wellnesscoach.live/scim</a>
SCIM Unique Identifier	<b>Email</b>
SCIM Authorization Token	<b>Obtain from Wellness Coach Admin Portal</b>
Wellness Coach Portal	<a href="#">🌐 Portal   Wellness Coach</a>

Don't have Portal access? Email [Support@wellnesscoach.live](mailto:Support@wellnesscoach.live) to get access to the Portal.



# Okta SSO Setup

Technical steps to configure SAML-based Single Sign-On



**STEP 1****CREATE APP INTEGRATION**

Go to Okta Admin Console, click Applications, then Create App Integration.

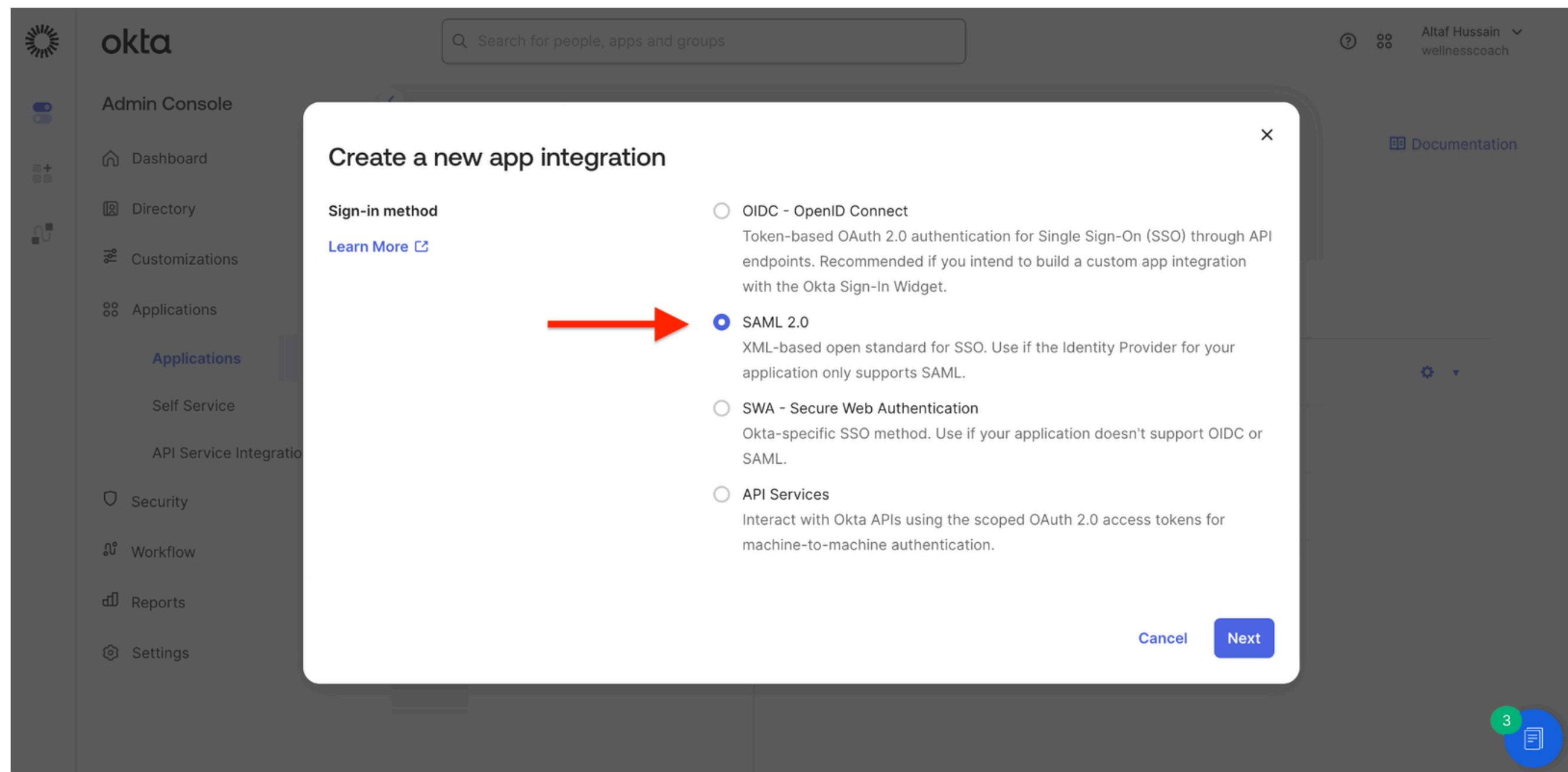
The screenshot displays the Okta Admin Console interface. The left sidebar contains the navigation menu with 'Applications' highlighted. The main content area shows the 'Applications' page with a search bar and a table of application statuses. The 'Create App Integration' button is prominently displayed at the top of the main content area.

STATUS		
ACTIVE	5	Okta Admin Console
INACTIVE	1	Okta Browser Plugin
		Okta Dashboard



**STEP 2****SELECT SAML 2.0**

Choose SAML 2.0 as the sign-in method and click Next.



The screenshot displays the Okta Admin Console interface. A modal dialog titled "Create a new app integration" is open, showing the "Sign-in method" selection screen. A red arrow points to the "SAML 2.0" option, which is selected with a blue radio button. The dialog box includes a "Learn More" link and a "Next" button.

**Sign-in method**  
[Learn More](#)

- OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel Next



# STEP 3

# CONFIGURE APP SETTINGS

Enter 'Wellness Coach' as the app name, upload the logo, and click Next.

The screenshot displays the Okta Admin Console interface for configuring a SAML integration. The left sidebar shows the navigation menu with 'Applications' selected. The main content area is titled 'Create SAML Integration' and features a progress bar with three steps: '1 General Settings', '2 Configure SAML', and '3 Feedback'. The 'General Settings' step is active and contains the following fields:

- App name:** A text input field containing 'Wellness Coach', with a red arrow pointing to it from the number '1'.
- App logo (optional):** A file upload area containing a circular logo with the text 'wellnesscoach' below it, with a red arrow pointing to it from the number '2'.
- App visibility:** A radio button option labeled 'Do not display application icon to users'.
- Buttons:** A 'Cancel' link and a blue 'Next' button, with a red arrow pointing to the 'Next' button from the number '3'.

The footer of the page includes copyright information: '© 2025 Okta, Inc. Privacy Status site OK3 Cell (US) Version 2025.09.0 E Feedback'. A notification icon with the number '3' is visible in the bottom right corner.



**STEP 4****CONFIGURE SAML SETTINGS**

Enter the Single Sign-On URL, Audience URI, Default Relay State, and configure Name ID format.

Single Sign-on URL: <https://api.meditation.live/auth/sso/callback>

Audience URI (SP Entity ID): WellnessCoach

Default Relay State: [Get from <https://portal.wellnesscoach.live/enterprises/config/sso-scim>]

The screenshot displays the 'Create SAML Integration' page in the Okta Admin Console, specifically the 'Configure SAML' step. The page is divided into three sections: 'General Settings', 'Configure SAML', and 'Feedback'. The 'Configure SAML' section is active and contains the following fields:

- Single sign-on URL:** . A red arrow points to the input field. Below the field is a checked checkbox labeled 'Use this for Recipient URL and Destination URL'.
- Audience URI (SP Entity ID):** . A red arrow points to the input field.
- Default RelayState:** . A red arrow points to the input field. Below the field is the text: 'If no value is set, a blank RelayState is sent'.
- Name ID format:** . A red arrow points to the dropdown menu.
- Application username:** . A red arrow points to the dropdown menu.
- Update application username on:** . A red arrow points to the dropdown menu.

On the right side of the page, there is a help section titled 'What does this form do?' which states: 'This form generates the XML needed for the app's SAML request.' Below this is another section titled 'Where do I find the info this form needs?' which states: 'The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.'

The left sidebar shows the Okta Admin Console navigation menu with options: Admin Console, Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The top right corner shows the user profile 'Altaf Hussain wellnesscoach'.



## STEP 5

## CONFIGURE ATTRIBUTES

On the Sign On tab, scroll to Attribute Statements, click Show Legacy Configuration, and click Edit.

The screenshot displays the Okta Admin Console interface. On the left, the navigation menu is visible with the 'Applications' section expanded. A red arrow points from the 'Self Service' option in the menu to the 'Attribute statements' section in the main content area. Below this, another red arrow points from the 'Show legacy configuration' section to the 'Profile attribute statements' section. A final red arrow points from the 'Edit' link in the 'Profile attribute statements' section to the right.

**Admin Console**

- Dashboard
- Directory
- Customizations
- Applications
- Self Service
- API Service Integrations
- Security
- Workflow
- Reports
- Settings

**Attribute statements**

Learn more about configuring [attribute statements](#)

No expressions are configured. Click **Add expression** to get started.

**Show legacy configuration**

**Profile attribute statements**

Learn more about [profile attribute statements](#)

Name	Name format	Value
------	-------------	-------

**Credentials Details**

Application username format: Okta username

Update application username on: Create and update [Update Now](#)

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

[View SAML setup instructions](#)

work until you configure the app to trust Okta as an IdP.

Altaf Hussain wellnesscoach



## STEP 6

## ATTRIBUTE STATEMENTS

Map firstName, lastName, and email attributes from Okta user profile.

The screenshot shows the Okta Admin Console interface. The left sidebar contains the navigation menu with 'Applications' selected. The main content area is titled 'Attribute statements' and includes a search bar and a user profile dropdown. Below the title, there is a message: 'No expressions are configured. Click Add expression to get started.' with an 'Add expression' button. A modal window titled 'Show legacy configuration' is open, showing 'Profile attribute statements'. This modal contains a table with three rows, each representing an attribute statement. Red arrows point to the 'Name' column of each row: 'firstName', 'lastName', and 'email'. The 'Value' column for each row contains 'user.firstName', 'user.lastName', and 'user.email' respectively. Below the table is an 'Add Another' button. At the bottom of the modal, there is a 'Save' button and a 'Cancel' button, with a red arrow pointing to the 'Save' button.

Name	Name format	Value
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName
email	Unspecified	user.email



# STEP 7

# COMPLETE SETUP

Click Save or Next, Review settings and click Finish to create the integration.

The screenshot displays the Okta Admin Console interface during the SSO setup process. On the left, the 'Admin Console' navigation menu is visible, listing options such as Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area shows a configuration step titled 'Contact app vendor'. At the top of this step, there is a search bar with the placeholder text 'Search for people, apps and groups' and a user profile for 'Altaf Hussain' with the email 'wellnesscoach'. Below the search bar, there is a radio button option: 'It's required to contact the vendor to enable SAML'. The main form contains three text input fields: 'Which app pages did you consult to configure SAML?' (with placeholder text 'Enter links, describe where the pages are, or anything else you think is helpful'), 'Did you find SAML docs for this app?' (with placeholder text 'Enter any links here'), and 'Any tips or additional comments?' (with placeholder text 'Placeholder text'). At the bottom of the form, there are two buttons: 'Previous' and 'Finish'. A red arrow points from the 'Previous' button towards the 'Finish' button. The footer of the page includes copyright information: '© 2025 Okta, Inc.', along with links for 'Privacy', 'Status site', 'OK3 Cell (US)', 'Version 2025.08.2 E', and 'Feedback'. A notification icon with the number '3' is visible in the bottom right corner.



## STEP 8

## COPY METADATA URL

On the Sign On tab, copy the metadata URL for Wellness Coach configuration in the Portal.

The screenshot displays the Okta Admin Console interface. The left sidebar shows the navigation menu with 'Applications' selected. The main content area is titled 'Settings' and has tabs for 'General', 'Sign On', 'Provisioning', 'Import', 'Assignments', and 'Push Groups'. The 'Sign On' tab is active. Under 'Sign on methods', the 'SAML 2.0' method is selected. A red arrow labeled '1' points to the 'Sign On' tab. Below, the 'Metadata details' section shows the 'Metadata URL' as `https://wellnesscoach.okta.com/app/exk1o0mrwuiELN/OcY1d8/sso/saml/metadata`. A red arrow labeled '2' points to the 'Copy' button next to this URL. Other fields include 'Default Relay State' (60c384bb157d282eb6a71b21), 'Application username format' (Okta username), and 'Update application username on' (Create and update). A 'View SAML setup instructions' button is located at the bottom right of the settings area.



**STEP 9****CONFIGURE WELLNESS COACH PORTAL**

Enable SSO in the Wellness Coach Admin Portal, enter the IdP metadata link, and click fetch to prefill the values, then save.

Alternatively, you can upload the IdP metadata XML file to prefill the values, then save.

The screenshot displays the 'Retain and Hire' admin portal interface for SSO configuration. The left sidebar contains navigation options: Home, Account Management, Plans, Advanced, SSO Configuration (highlighted), Provisioning, Challenges, Reports, and User Management. The main content area is titled 'Retain and Hire' and includes a sub-header 'Manage organization-wide settings, authentication options, and additional configurations.' Below this, there are tabs for Profile, Feature Settings, SSO (selected), and Provisioning. The 'SSO Configuration' section is active, showing a toggle for 'Enable Single Sign-On' set to 'Yes'. Below the toggle, there are two options: 'Upload IdP Metadata XML' (with a 'Choose XML File' button) and 'Fetch from Metadata URL' (with an input field and a 'Fetch' button). Red arrows point to these two options, with the word 'or' between them. To the right, the 'SSO Setup Parameters' section is visible, showing fields for 'SINGLE SIGN-ON URL OR ACS URL' (https://devopsapi.meditation.live/auth/sso/callback), 'AUDIENCE URI (ENTITY ID)' (WellnessCoach), and 'DEFAULT RELAY STATE' (67db7de974510cb3bae28104).





# Okta SCIM Setup

Technical steps to configure automated user provisioning



## STEP 1

## ENABLE SCIM

Navigate to the General tab -> Click Edit -> Select SCIM -> Click Save.

The screenshot displays the Okta Admin Console interface for the 'Wellness Coach' application. The left sidebar shows the navigation menu with 'Applications' selected. The main content area shows the application details for 'Wellness Coach', which is currently 'Active'. The 'General' tab is selected, and the 'App Settings' modal is open. The 'Provisioning' section has 'SCIM' selected, and the 'Save' button is highlighted. The 'Application label' is 'Wellness Coach'. The 'Application visibility' section has 'Do not display application icon to users' selected. The 'Provisioning' section has 'None', 'On-Premises Provisioning', and 'SCIM' options, with 'SCIM' selected. The 'Auto-launch' section has 'Auto-launch the app when user signs into Okta.' selected. The 'Application notes for end users' and 'Application notes for admins' sections are empty. The 'Save' button is highlighted with a red arrow.



**STEP 2****CONFIGURE SCIM SETTINGS**

Navigate to the Provisioning tab -> Integration -> Edit

Enter the SCIM 2.0 Base URL, unique identifier, and authorization token.

Select HTTP Header for Authentication Mode

SCIM Connector base URL: <https://ed.wellnesscoach.live/scim>

Authorization Token: [Get from <https://portal.wellnesscoach.live/enterprises/config/employee-verification-template#scim-config>]

The screenshot shows the Okta Admin Console interface. The left sidebar contains navigation options like Admin Console, Dashboard, Directory, Customizations, Applications, Self Service, and API Service Integrations. The main content area is titled 'SCIM Connection' and is part of the 'Provisioning' tab. The configuration fields are as follows:

- SCIM version: 2.0
- SCIM connector base URL: <https://ed.wellnesscoach.live/scim>
- Unique identifier field for users: email
- Supported provisioning actions:  Push New Users,  Push Profile Updates,  Push Groups,  Import New Users and Profile Updates,  Import Groups
- Authentication Mode: HTTP Header
- HTTP Header Authorization: Bearer

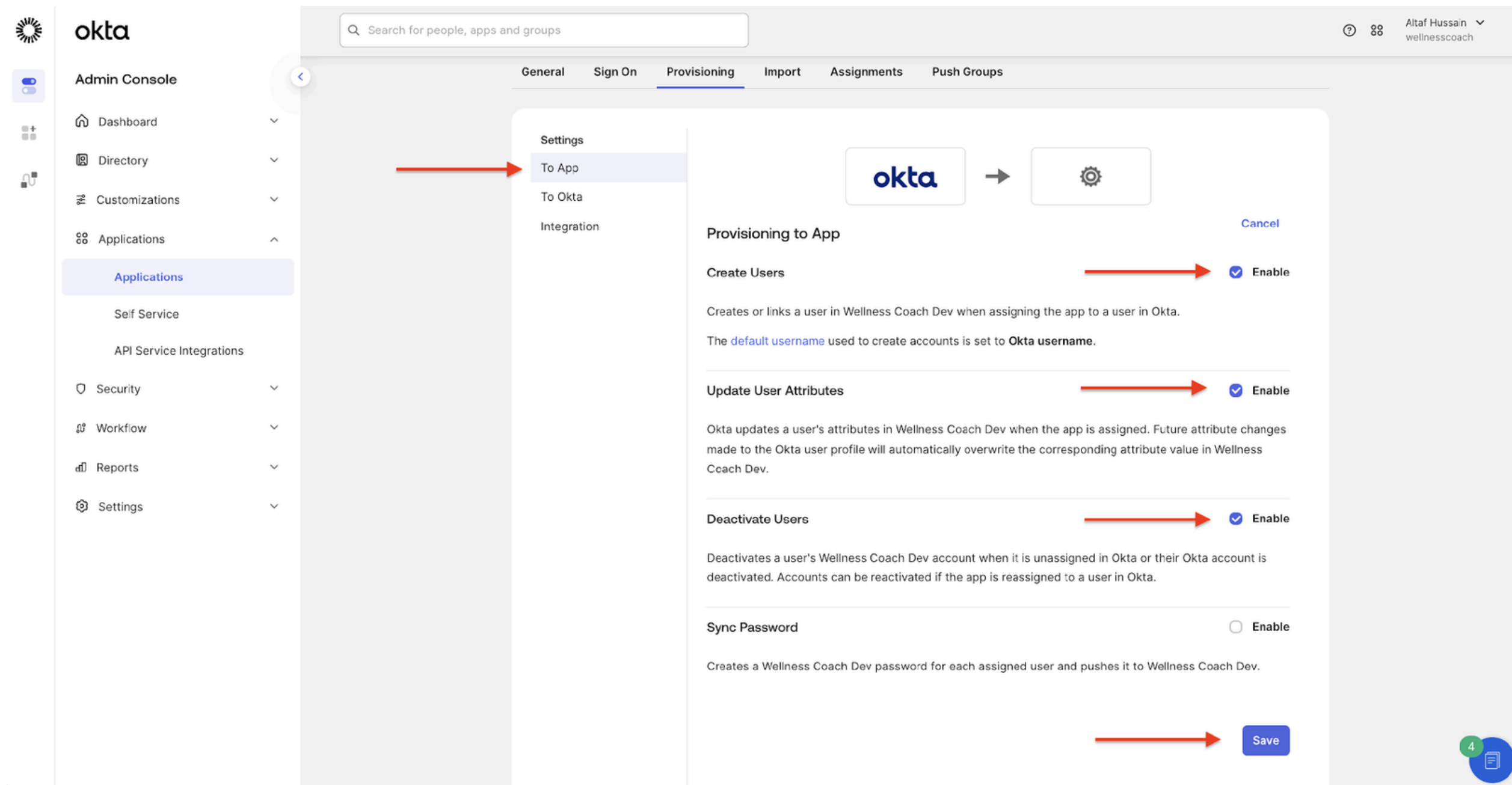
At the bottom, there is a 'Test Connector Configuration' button, a 'Save' button, and a 'Cancel' button. Red arrows in the image point to the 'Integration' tab, the SCIM connector base URL, Unique identifier field, Authentication Mode, and Authorization field.



## STEP 3

## ENABLE PROVISIONING

Navigate to Provisioning -> To App. Enable Create Users, Update User Attributes, and Deactivate Users, then click Save.



The screenshot displays the Okta Admin Console interface. On the left, the navigation menu is visible, with 'Applications' selected. The main content area shows the 'Provisioning' tab for an application, with the 'To App' sub-tab selected. The 'Settings' sidebar on the left has a red arrow pointing to 'To App'. The main content area features a diagram showing 'Okta' pointing to a gear icon, representing provisioning to the application. Below this, the 'Provisioning to App' settings are listed:

- Create Users:** Enabled (checked). A red arrow points to the 'Enable' checkbox. Description: Creates or links a user in Wellness Coach Dev when assigning the app to a user in Okta. The default username used to create accounts is set to Okta username.
- Update User Attributes:** Enabled (checked). A red arrow points to the 'Enable' checkbox. Description: Okta updates a user's attributes in Wellness Coach Dev when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in Wellness Coach Dev.
- Deactivate Users:** Enabled (checked). A red arrow points to the 'Enable' checkbox. Description: Deactivates a user's Wellness Coach Dev 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.
- Sync Password:** Disabled (unchecked). Description: Creates a Wellness Coach Dev password for each assigned user and pushes it to Wellness Coach Dev.

At the bottom right, a red arrow points to the 'Save' button. A notification badge with the number '4' is visible in the bottom right corner.



## STEP 4

## ASSIGN PEOPLE OR GROUPS

Assign People or Groups from the respective tabs. For Groups, assign the Wellness Coach app to the appropriate group.

The screenshot displays the Okta Admin Console interface for the 'Wellness Coach' application. The left sidebar shows the navigation menu with 'Applications' selected. The main content area is titled 'Wellness Coach' and includes a search bar, a back button, and a status indicator 'Active'. Below this, there are tabs for 'General', 'Sign On', 'Provisioning', 'Import', and 'Assignments'. The 'Assignments' tab is active, showing a table with columns for 'Filters', 'Person', and 'Type'. The table lists one assignment for 'Altaf Hussain' (Group). Red arrows point to the 'People' and 'Groups' filter options. On the right, there are sections for 'REPORTS' (Current Assignments, Recent Unassignments) and 'SELF SERVICE' (You need to enable self service for org managed apps before you can use self service for this app. Go to self service settings). The footer contains copyright information and version details.

Filters	Person	Type
People	Altaf Hussain	Group
Groups	altaf@retainandhire.com	



# **SSO & SCIM Overview**

Background information on Single Sign-On and SCIM



# WHAT IS SINGLE SIGN-ON (SSO)?

*One set of credentials. Every application. Seamless access.*

**SSO allows users to authenticate once and gain access to multiple applications without re-entering credentials.**

Instead of maintaining separate usernames and passwords for each app, employees log in once through an Identity Provider (IdP) like Okta and get automatic access to all connected services.



**One Login**



**More Secure**



**Less Friction**

## How SSO Works

- 1 User visits Wellness Coach
- 2 Redirected to Okta (IdP)
- 3 User authenticates once
- 4 Okta sends SAML assertion
- 5 Access granted automatically



# SSO Authentication Flow

Wellness Coach supports both IdP-Initiated and SP-Initiated SSO



## IdP-Initiated Login

---

- 1 Employee logs into Okta Dashboard
- 2 Clicks the Wellness Coach icon
- 3 *SAML request sent from Okta*
- 4 Automatically signed into Wellness Coach



## SP-Initiated Login

---

- 1 Employee opens Wellness Coach app
- 2 Redirected to Okta login page
- 3 Employee authenticates with Okta
- 4 Redirected back, access granted



# Why SSO with Wellness Coach?

## Single Sign-On



Access Wellness Coach with one set of login credentials from any device or application, whether cloud or on-premise.

## Fraud Prevention



Okta's dynamic risk engine detects and blocks fraud in real-time using Device ID, Location, and Time-based multi-factor authentication.

## Employee Access Management



New hires automatically get access on their start date. Terminated employees' access is revoked on their last day.

## Seamless Experience



Employees enjoy frictionless access to wellness resources without managing multiple passwords or separate logins.



# WHAT IS SCIM?

System for Cross-domain Identity Management

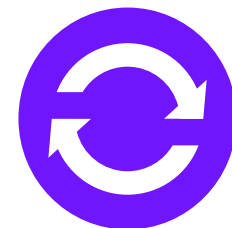
**SCIM is an open standard that automates user provisioning and de-provisioning across cloud applications.**

With SCIM, your Active Directory stays in sync with Wellness Coach. When an employee joins your organization, their Wellness Coach account is created automatically. When they leave, access is revoked instantly.



## **Auto-Provisioning**

New employees get access automatically



## **Real-Time Sync**

Real-Time Sync



## **Auto-Deprovisioning**

Access revoked on termination

