

# ProLease SCIM Setup Guide

Support Contact: TechSupport@ProLease.com

## Features

### 1. Push New Users

New users created through OKTA will also be created in ProLease.

### 2. Push Profile Updates

Updates made to the user's profile through OKTA will be pushed to ProLease.

### 3. Push User Deactivation

Deactivating the user or disabling the user's access to the application through OKTA will deactivate the user in ProLease.

**Note: In ProLease application, user account only will be deactivated but not deleted.**

## Requirements

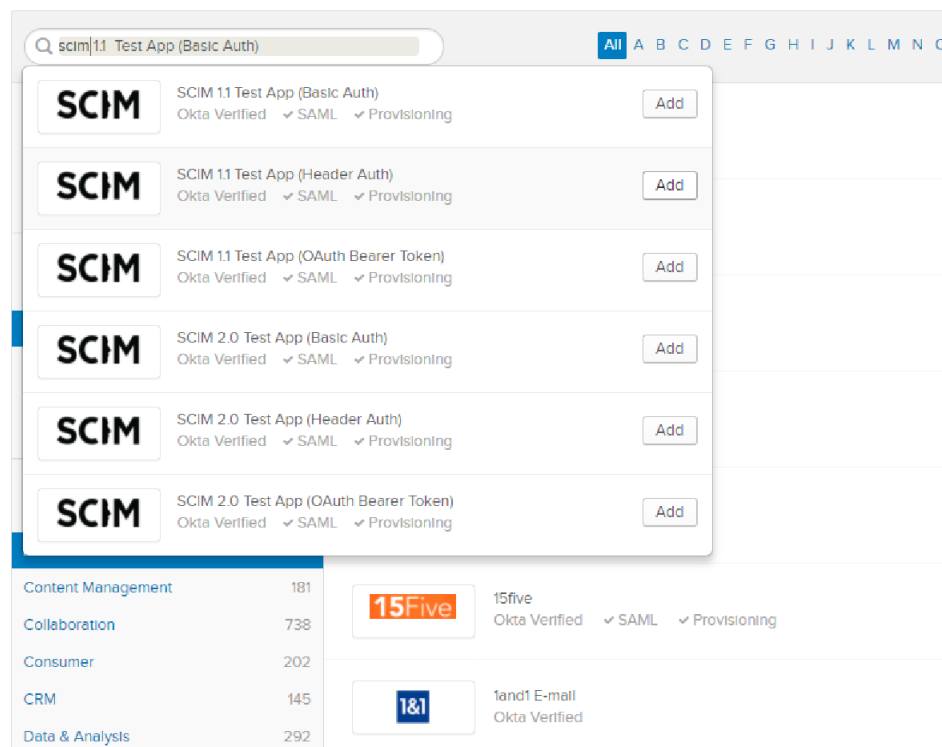
Before add SCIM application, contact ProLease for setting up SCIM credential and gain API key.

## Configuration Steps

### 1. Add application SCIM 1.1 Test App (Header Auth)

[← Back to Applications](#)

 Add Application



The screenshot displays the ProLease application configuration interface. At the top, there is a search bar containing "scim|1.1 Test App (Basic Auth)" and a navigation menu with "All" and letters A through O. Below the search bar, a list of SCIM applications is shown, each with a "SCIM" icon, a title, a list of features (Okta Verified, SAML, Provisioning), and an "Add" button. The applications listed are:

- SCIM 1.1 Test App (Basic Auth)
- SCIM 1.1 Test App (Header Auth)
- SCIM 1.1 Test App (OAuth Bearer Token)
- SCIM 2.0 Test App (Basic Auth)
- SCIM 2.0 Test App (Header Auth)
- SCIM 2.0 Test App (OAuth Bearer Token)

Below the list, there is a sidebar with navigation options and a list of other applications:


- Content Management: 181
- Collaboration: 738
- Consumer: 202
- CRM: 145
- Data & Analysis: 292

Other applications shown include:

- 15Five: 15five, Okta Verified, SAML, Provisioning
- 1&1: 1and1 E-mail, Okta Verified

## 2. Input Application label and click Next.

☰ Add SCIM 1.1 Test App (Header Auth)



1 General Settings   2 Sign-On Options   3 Provisioning

4 Assign to People

### General Settings - Required

Application label   
This label displays under the app on your home page

Application Visibility  Do not display application icon to users  
 Do not display application icon in the Okta Mobile App


Browser plugin auto-submit  Automatically log in when user lands on login page

#### General settings

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

3. Under Sign On Methods section, select SAML 2.0. Leave Default Relay State blank. Check Disabled Force Authentication. Under Credentials Details section, select Okta username as Application username format and ignore Password reveal since this app is using SAML with no password.

☰ Add SCIM 1.1 Test App (Header Auth)



1 General Settings   2 Sign-On Options   3 Provisioning

4 Assign to People

### Sign-On Options - Required

**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.

SAML 2.0

Default Relay State   
All IDP-initiated requests will include this RelayState

Disable Force Authentication   
Never prompt user to re-authenticate.

Secure Web Authentication

**CREDENTIALS DETAILS**

Application username format

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

#### About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

#### You can sync passwords to this app

If you enable provisioning and password push, you can automatically synchronize Okta passwords to SCIM 1.1 Test App (Header Auth).

#### Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

4. Check Enable provisioning features, type Base URL <https://workplace.proleaseweb.com/scim/v1/> and API Token gained from ProLease. Then click Test API Credentials to check if you are able to connect to ProLease SCIM API. Please contact ProLease when you are not.

### Provisioning Settings - Optional

Enable provisioning features

#### API CREDENTIALS

Enter your SCIM 1.1 Test App (Header Auth) credentials to enable user import and provisioning features.


Base URL

API Token

#### PROVISIONING FEATURES

5. Under User Import section, click Advanced Configure Import Matching Rules to expand. Follow the diagram below and select the corresponding options.

 **User Import** Enabled

Import users from SCIM 1.1 Test App (Header Auth) to create new Okta users. If the Okta user already exists, the two accounts will automatically be linked. Imported users are assigned SCIM 1.1 Test App (Header Auth) access when they are confirmed on the Import tab.

**Schedule import** never ▼  
Select **never** if you prefer to import manually.

**Okta username format** Email address ▼  
Select the username users should enter to log into Okta.

[Advanced: Configure Import Matching Rules](#)

---

**EXACT IMPORT MATCH**

**Imported user is exact match if**

- Their Okta username format matches an existing Okta user
- Their email address matches an existing Okta user
- Their Okta username format OR their email address matches an existing Okta user
- Their first and last name matches an existing Okta user

**When exact match found** Manually confirm match ▼

**PARTIAL IMPORT MATCH**

**Imported user is partial match if**  Their first and last name matches an existing Okta user

**When partial match found** Manually confirm match ▼


**NO IMPORT MATCH**

**When no match found** Manually confirm new user ▼

Auto-activate after confirmation.

**Max Import Unassignment**

6. Check Create Users, Update User Attributes, Deactivate Users. Uncheck Profile Master and Sync Password then click Next.




Profile Master  Enable

Profile mastering makes SCIM 1.1 Test App (Header Auth) the identity authority for assigned users. When enabled, user profiles are not editable in Okta and changes are sync'd to Okta during provisioning events.

If you have more than one profile master you can set their priority on the [Profile Masters](#) page.

---




Create Users  Enable

Creates or links a user in SCIM 1.1 Test App (Header Auth) 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 SCIM 1.1 Test App (Header Auth) when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in SCIM 1.1 Test App (Header Auth).


---



Deactivate Users  Enable

Deactivates a user's SCIM 1.1 Test App (Header Auth) 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.

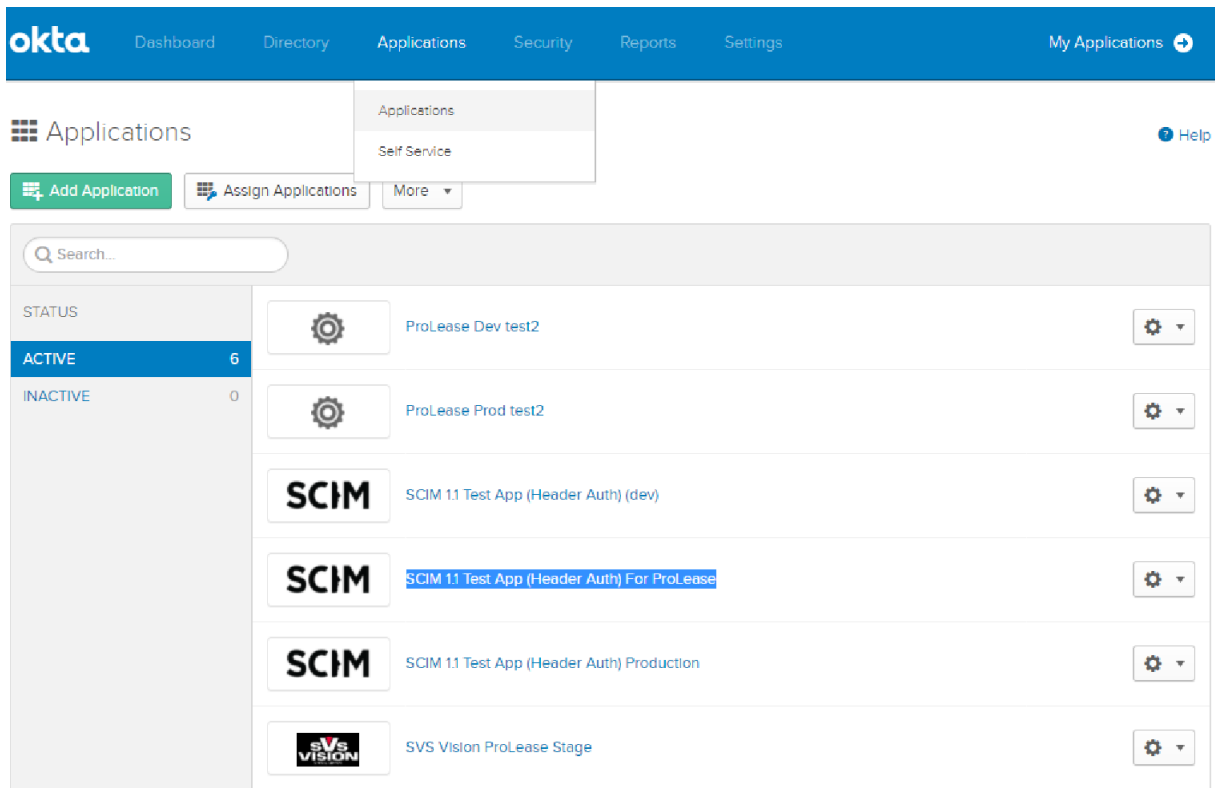
---



Sync Password  Enable

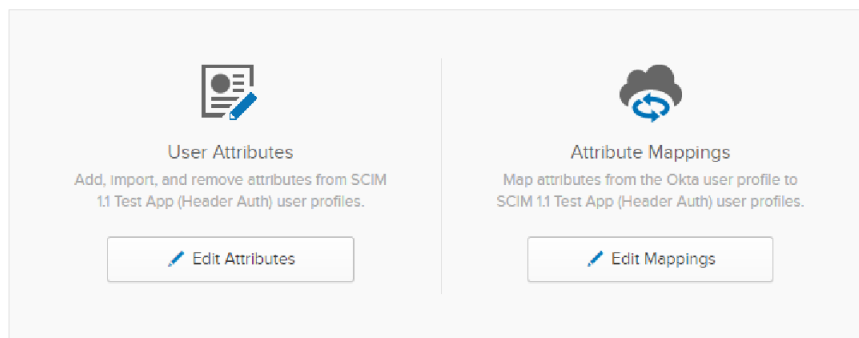
Creates a SCIM 1.1 Test App (Header Auth) password for each assigned user and pushes it to SCIM 1.1 Test App (Header Auth).

7. After the application is added, go to Applications Tab to see if your application is active. If yes, click your application.



8. Click Provisioning Tab and scroll to bottom. Under Profile Attributes & Mappings section, click Edit Mappings.

#### Profile Attributes & Mappings



9. Click Override with mapping.

The screenshot shows a dialog titled "SCIM 1.1 Test App (Header Auth) For ProLease User Profile Mappings". It features two tabs: "SCIM 1.1 Test App (Header Auth) For ProLease L..." and "Okta to SCIM 1.1 Test App (Header Auth) For Pro...". The SCIM side is labeled "SCIM" and "SCIM 1.1 Test App (Header Auth) For ProLease User Profile appuser". The Okta side is labeled "Okta" and "Okta User Profile user". A message states: "Username is set by SCIM 1.1 Test App (Header Auth) For ProLease - Override with mapping". A table below shows a mapping for the attribute "login" (string type).

10. Follow the diagram below to map SCIM application User Profile to Okta User Profile. All the attributes that are not included in the diagram are not mapped.

The screenshot displays the mapping configuration interface. On the left, there are dropdown menus for SCIM attributes: "appuser.userName", "appuser.givenName", "appuser.familyName", "appuser.middleName", "Choose an attribute or enter an expression...", "Choose an attribute or enter an expression...", "appuser.email", "Choose an attribute or enter an expression...", and "appuser.displayName". Each dropdown is followed by a mapping icon (yellow arrow with 'i' and 'o') or a "no mapping" icon (grey arrow with "/"). On the right, a list of Okta attributes is shown with their types: "login" (string), "firstName" (string), "lastName" (string), "middleName" (string), "honorificPrefix" (string), "honorificSuffix" (string), "email" (email), "title" (string), and "displayName" (string).

11. Click Save Mappings at bottom right corner.

The screenshot shows the bottom of the mapping dialog. It includes a "Preview" button, a text input field "Enter an Okta user to preview their mappings...", and two buttons: "Save Mappings" (green) and "Cancel" (grey).

12. Click apply updates now to go back Profile Editor.

The screenshot shows a confirmation dialog titled "Mappings saved!". It asks: "Do you want to apply these mappings to all users with this profile?". There are two buttons: "Apply updates now" (green) and "Don't apply updates" (grey).

### 13. Click Map Attributes to open User Profile Mappings Window again.

Okta Dashboard Directory Applications Security Reports Settings My Applications

Profile Editor [← Back to profiles](#)

SCIM 1.1 Test App (Header Auth) For ProLease User [Edit](#)

Display name SCIM 1.1 Test App (Header Auth) For ProLease User

Description

Variable name [?](#) scim1headerauth\_2

Attributes

[+ Add Attribute](#) [Map Attributes](#)

FILTERS	Display Name	Variable Name	Data Type	Attribute Type	
All	Username	user:Name	string	Base	<a href="#">?</a> <a href="#">×</a>
Base	Given name	givenName	string	Base	<a href="#">?</a> <a href="#">×</a>
Custom	Family name	familyName	string	Base	<a href="#">?</a> <a href="#">×</a>

### 14. Click Okta to <your application name> Tab

SCIM 1.1 Test App (Header Auth) For ProLease User Profile Mappings

SCIM 1.1 Test App (Header Auth) For ProLease t... [Okta to SCIM 1.1 Test App \(Header Auth\) For Pro...](#)



15. Click Override with mapping and follow the below diagram to do mapping. All the attributes that are not included in diagram are not mapped. After you finished, save and apply

Source Attribute	Target Attribute	Type
user.login	userName	string
user.firstName	givenName	string
user.lastName	familyName	string
user.middleName	middleName	string
Choose an attribute or enter an expression...	honorificPrefix	string
Choose an attribute or enter an expression...	honorificSuffix	string
user.email	email	email
Choose an attribute or enter an expression...	emailType	email
Choose an attribute or enter an expression...	title	string
user.displayName	displayName	string

mapping.

16. Go back to Profile Editor and click Custom tab on left hand side.

Attributes

+ Add Attribute    Map Attributes

FILTERS

- All
- Base
- Custom**

Display Name

Middle name







Honorific prefix

Honorific suffix

17. Remove all attributes that are not mapped by clicking the corresponding "X" button. Your application should only have the attributes listed in below diagram.

Attributes

+ Add Attribute    Map Attributes

FILTERS	Display Name	Variable Name	Data Type	Attribute Type	
All	Middle name	middleName	string	Custom	 
Base	Primary email	email	string	Custom	 
Custom	Display name	displayName	string	Custom	 

## Troubleshooting Tips

1. You should not import users from your application to create new okta users.
2. User without first name and last name cannot be created or updated via SCIM application.