Configuring Okta to Manage LaunchDarkly Users with SCIM

Features

- **Push New Users**
  Users created in Okta are also created in LaunchDarkly.

- **Push Profile Updates**
  Updates made to the user's profile through Okta will be pushed to LaunchDarkly.

- **Push User Deactivation**
  Deactivating the user or disabling the user's access to the application through Okta will deactivate the user in LaunchDarkly.

- **Push Groups**
  Okta groups and their members can be pushed as new LaunchDarkly teams.

- **Group Linking**
  Okta groups and their members can be linked to existing teams in LaunchDarkly.

Requirements

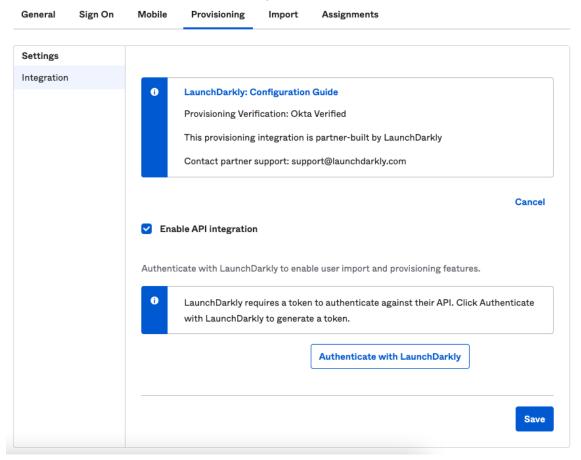In order to complete this procedure, you must have the following prerequisites:

- SCIM provisioning is only available to LaunchDarkly customers on Enterprise plans. To learn more about our Enterprise plans, contact sales@launchdarkly.com.
- You must be a LaunchDarkly Owner / Admin
- You must have added the LaunchDarkly app to Okta and have SSO enabled. To learn more about LaunchDarkly's SSO features, read Single Sign-On in LaunchDarkly's documentation.
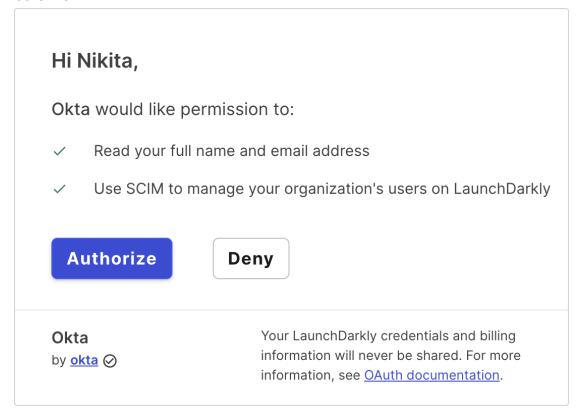
Step-by-Step Configuration Instructions

Configure your **Provisioning** settings for LaunchDarkly as follows:
1. Click the **Configure API Integration** button.

2. Check the **Enable API Integration** box.
3. Click the **Authenticate with LaunchDarkly** button. A new browser window opens.

4. The browser message describes what permissions Okta requires in LaunchDarkly. Click **Authorize.**

Hi Nikita,

Okta would like permission to:

✓ Read your full name and email address

✓ Use SCIM to manage your organization's users on LaunchDarkly

Authorize   Deny

Okta
by **okta** ⊘

Your LaunchDarkly credentials and billing information will never be shared. For more information, see OAuth documentation.

5. Return to Okta's **Provisioning** settings screen.
6. Click **Save**.
7. On the **To App** tab in **Provisioning**, click **Edit** and choose the **Provisioning Features** you want to enable.
8. Click **Save** to complete the configuration.

Provisioning to App

Create Users

☑ Enable

Creates or links a user in LaunchDarkly 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 LaunchDarkly when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in LaunchDarkly.
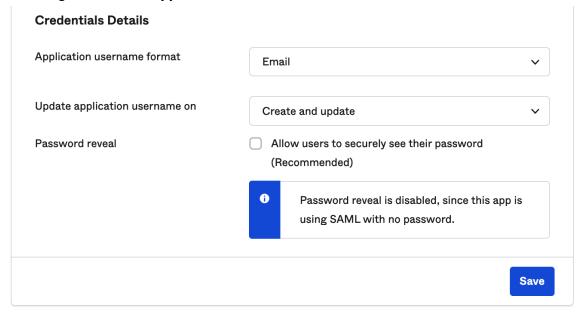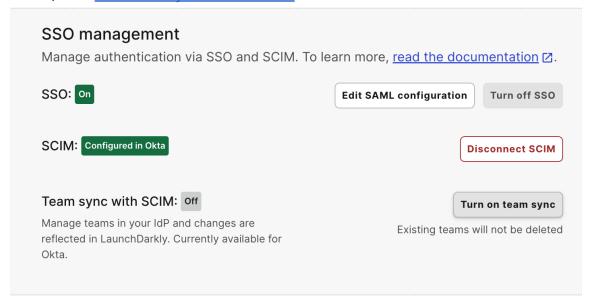
Deactivate Users

☑ Enable

Deactivates a user's LaunchDarkly 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

9. In the **Sign On** tab, set **Application username format** to **Email**. Click **Save**.

Credentials Details

Application username format

Email ⌄

Update application username on

Create and update ⌄

Password reveal

☐ Allow users to securely see their password (Recommended)

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

Save

10. To enable **Push Groups** and **Group Linking,** go to LaunchDarkly's **Account Settings**, click **Security**, then click **Turn on team sync**. To learn syncing Okta Groups with LaunchDarkly Teams, read LaunchDarkly's documentation.

SSO management

Manage authentication via SSO and SCIM. To learn more, read the documentation ↗.

SSO: On   Edit SAML configuration   Turn off SSO

SCIM: Configured in Okta   Disconnect SCIM

Team sync with SCIM: Off   Turn on team sync

Manage teams in your IdP and changes are   Existing teams will not be deleted
reflected in LaunchDarkly. Currently available for
Okta.

Schema Discovery

LaunchDarkly supports several custom attributes in addition to the standard SCIM username, given name, and family name.

Here is a table explaining LaunchDarkly's custom attributes:

Attribute	Okta attribute	Attribute type	Notes
Role	role	string	role is one of `no_access`, `reader`, `writer`, or `admin` which correspond to the built-in user roles in LaunchDarkly.
Custom Roles	customRole customRoleArray	String String array	customRole is a string containing comma-separated custom role keys, which grant custom permissions to users and user groups.

To connect LaunchDarkly's custom attributes to Okta user attributes:

1. In Okta's Admin Console, go to **Directory** > **Profile Editor**.
2. In the search field, enter "LaunchDarkly". The LaunchDarkly User profile appears.
3. Click the **LaunchDarkly User** profile to open the application's profile.
4. Click **Mappings**.
5. Select the **Okta User to LaunchDarkly** tab.
6. Choose an attribute or expression for the custom attributes you want to add.
7. Click **Save Mappings.**

Troubleshooting and Tips

- LaunchDarkly uses email addresses as SCIM usernames. It stores emails in lowercase. Emails with uppercase letters won't work as expected.

- LaunchDarkly does not store separate username and primary email fields. Changing the username updates the email and changing the email updates the username.

- Only one email address may be associated with a LaunchDarkly account at a time. If you attempt to provision the same email address into multiple accounts, it will fail.

- LaunchDarkly currently only allows one SCIM connection at a time. If you receive an error that you cannot add an additional SCIM connection, go to LaunchDarkly's **Account Settings**, click the **Security**, and then click **Disconnect SCIM**. After you do this, you will be able to make a new SCIM connection.

- If you see ConstraintViolationException errors when using **Push Groups**, go to the **Provisioning** tab, click **Integration**, and make sure that the **Import Groups** checkbox is checked. This is a known issue with Group Push.

- After you sync a LaunchDarkly team with an Okta group, you cannot unsync it. The only way to remove the team is to unlink the pushed group in Okta.

- To learn more about using LaunchDarkly's features, read [LaunchDarkly's documentation](#).