Configuring Okta to Manage LaunchDarkly Federal Users with SCIM

Features

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

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

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

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

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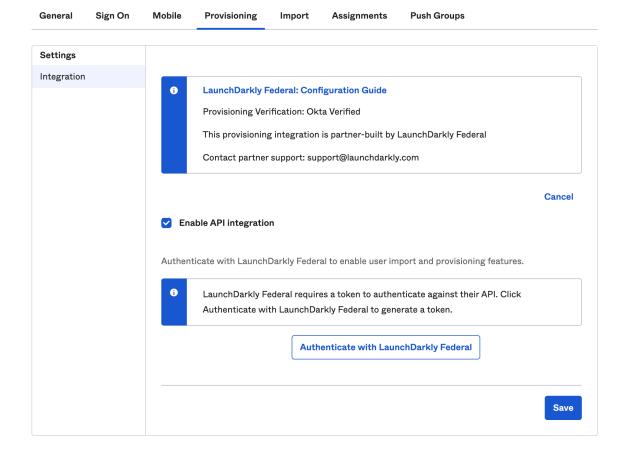
Requirements

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

- You must be a LaunchDarkly Owner / Admin
- You must have added the LaunchDarkly Federal app to Okta and have SSO enabled. To learn more about LaunchDarkly's SSO features, read Single Sign-On in LaunchDarkly's documentation.
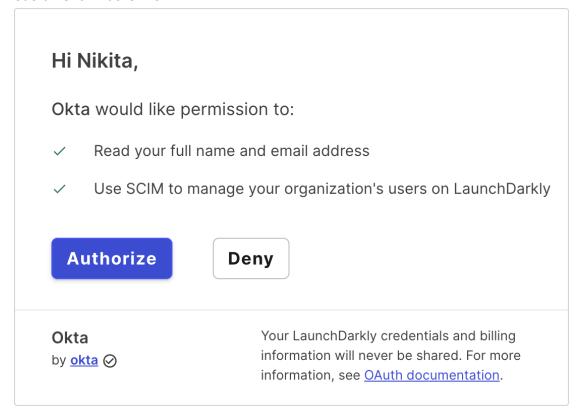
Step-by-Step Configuration Instructions

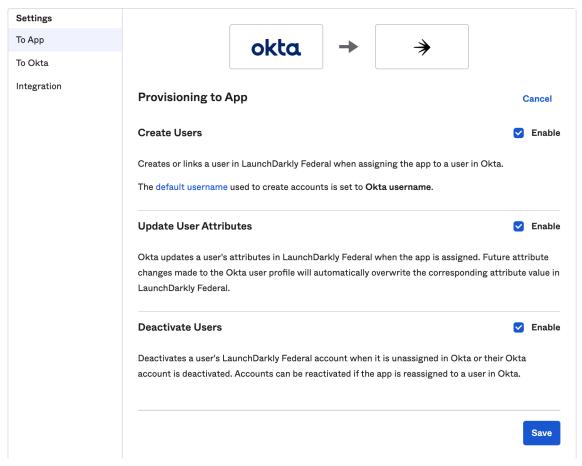Configure your **Provisioning** settings for LaunchDarkly as follows:
1. Click the **Configure API Integration** button.
2. Check the **Enable API Integration** box.
3. Click the **Authenticate with LaunchDarkly Federal** button. A new browser window opens.

Settings

Integration

LaunchDarkly Federal: Configuration Guide

Provisioning Verification: Okta Verified

This provisioning integration is partner-built by LaunchDarkly Federal

Contact partner support: support@launchdarkly.com

Cancel

☑ **Enable API integration**

Authenticate with LaunchDarkly Federal to enable user import and provisioning features.

LaunchDarkly Federal requires a token to authenticate against their API. Click Authenticate with LaunchDarkly Federal to generate a token.

Authenticate with LaunchDarkly Federal

Save

4. The browser message describes what permissions Okta requires in LaunchDarkly Federal. 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.
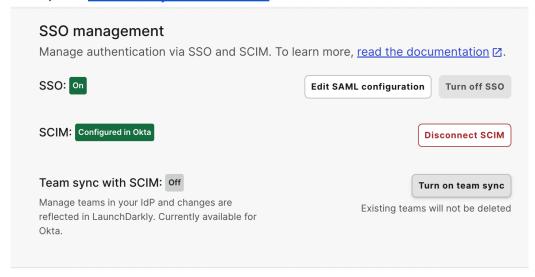
5. Return to Okta's **Provisioning** settings screen.
6. Click **Save**.
7. On the **To App** tab in **Provisions**, click **Edit** and choose the **Provisioning Features** you want to enable.
8. Click **Save** to complete the configuration.

9. In the **Sign On** tab, set **Application username format** to **Email**. Click **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
reflected in LaunchDarkly. Currently available for   Existing teams will not be deleted
Okta.

Schema Discovery

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

Here is a table explaining LaunchDarkly Federal'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 Federal"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 Federal". The LaunchDarkly Federal User profile appears.
3. Click the **LaunchDarkly Federal User** profile to open the application's profile.
4. Click **Mappings**.
5. Select the **Okta User to LaunchDarkly Federal** tab.
6. Choose an attribute or expression for the custom attributes you want to add.

7. Click **Save Mappings.**

Troubleshooting and Tips

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

- LaunchDarkly Federal 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 Federal account at a time. If you attempt to provision the same email address into multiple accounts, it will fail.

- LaunchDarkly Federal 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.

- After you sync a LaunchDarkly Federal 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](#).