bitwarden | Help Center Article

ADMIN CONSOLE > USER MANAGEMENT >

Okta SCIM Integration

View in the help center:
https://bitwarden.com/help/okta-scim-integration/

Okta SCIM Integration

System for cross-domain identity management (SCIM) can be used to automatically provision and de-provision members and groups in your Bitwarden organization.

> ⓘ **Note**
>
> SCIM Integrations are available for **Teams and Enterprise organizations**. Customers not using a SCIM-compatible identity provider may consider using Directory Connector as an alternative means of provisioning.

This article will help you configure a SCIM integration with Okta. Configuration involves working simultaneously with the Bitwarden web vault and Okta Admin Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

Supported features

The following provisioning features are supported by this integration:

- **Push Users:** Users in Okta that are assigned to Bitwarden are added as users in Bitwarden.
- **Deactivate Users:** Users with the deactivated status will no longer have access to their assigned apps. Deactivating a user in Okta will change their Bitwarden status to revoked.
- **Delete user**: Users deleted in Okta will be moved to revoked status in the Bitwarden organization.

  > ⓘ **Note**
  >
  > Choosing the suspended status for a user in Okta will **not** result in a revoked status in Bitwarden.

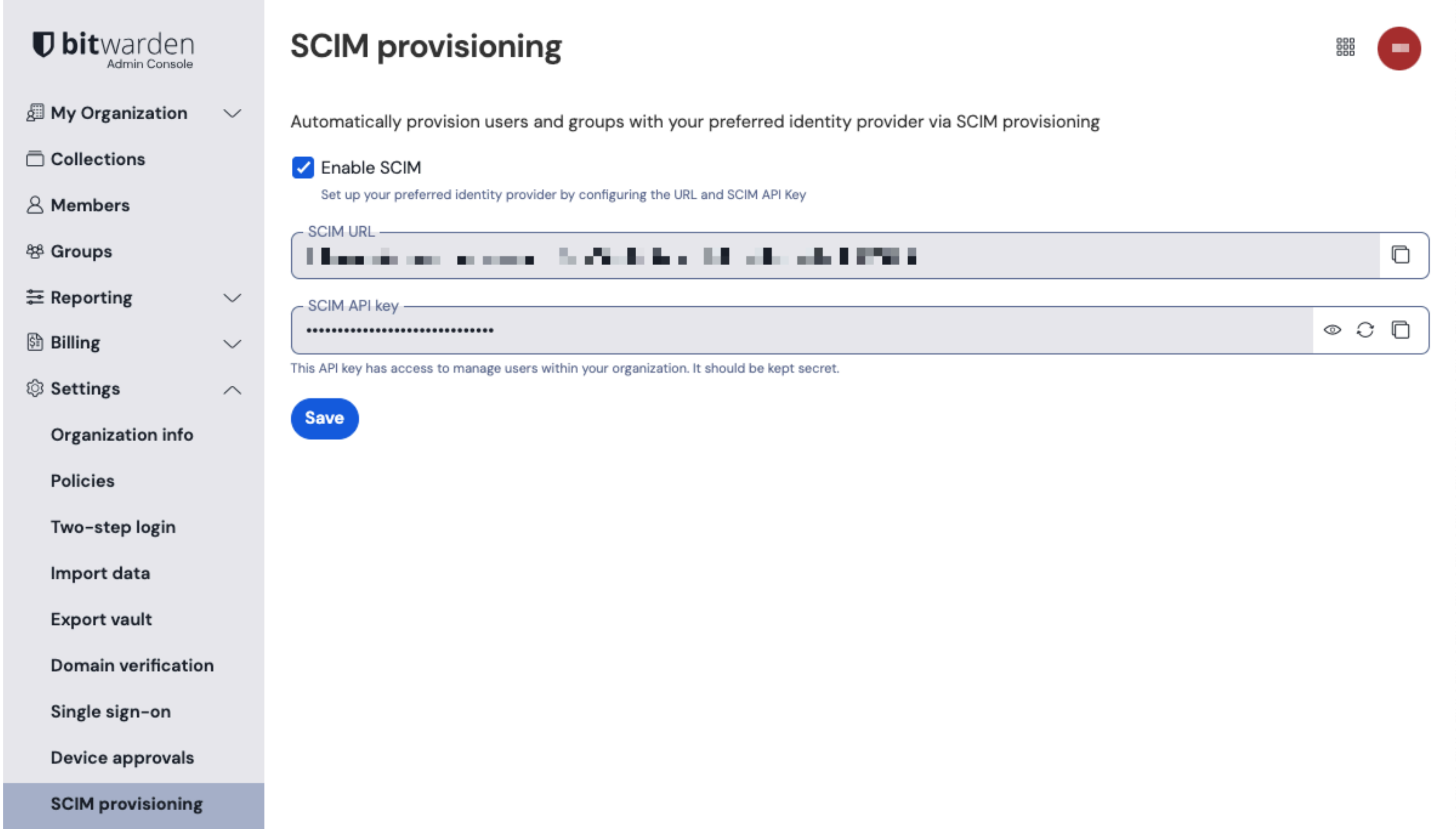
- **Push Groups:** Groups and their users in Okta can be pushed to Bitwarden.

> ⓘ **Note**
>
> Please note, Bitwarden does not support changing a user's email address once provisioned. Bitwarden also does not support changing a user's email address type, or using a type other than `primary`. The values entered for email and username should be the same. Learn more.

Enable SCIM

> ⓘ **Note**
>
> **Are you self-hosting Bitwarden?** If so, complete these steps to enable SCIM for your server before proceeding.

To start your SCIM integration, open the Admin Console and navigate to **Settings** → **SCIM provisioning**:



SCIM provisioning

Automatically provision users and groups with your preferred identity provider via SCIM provisioning

☑ Enable SCIM

Set up your preferred identity provider by configuring the URL and SCIM API Key

SCIM URL: [redacted]

SCIM API key: ••••••••••••••••••••••••••••••

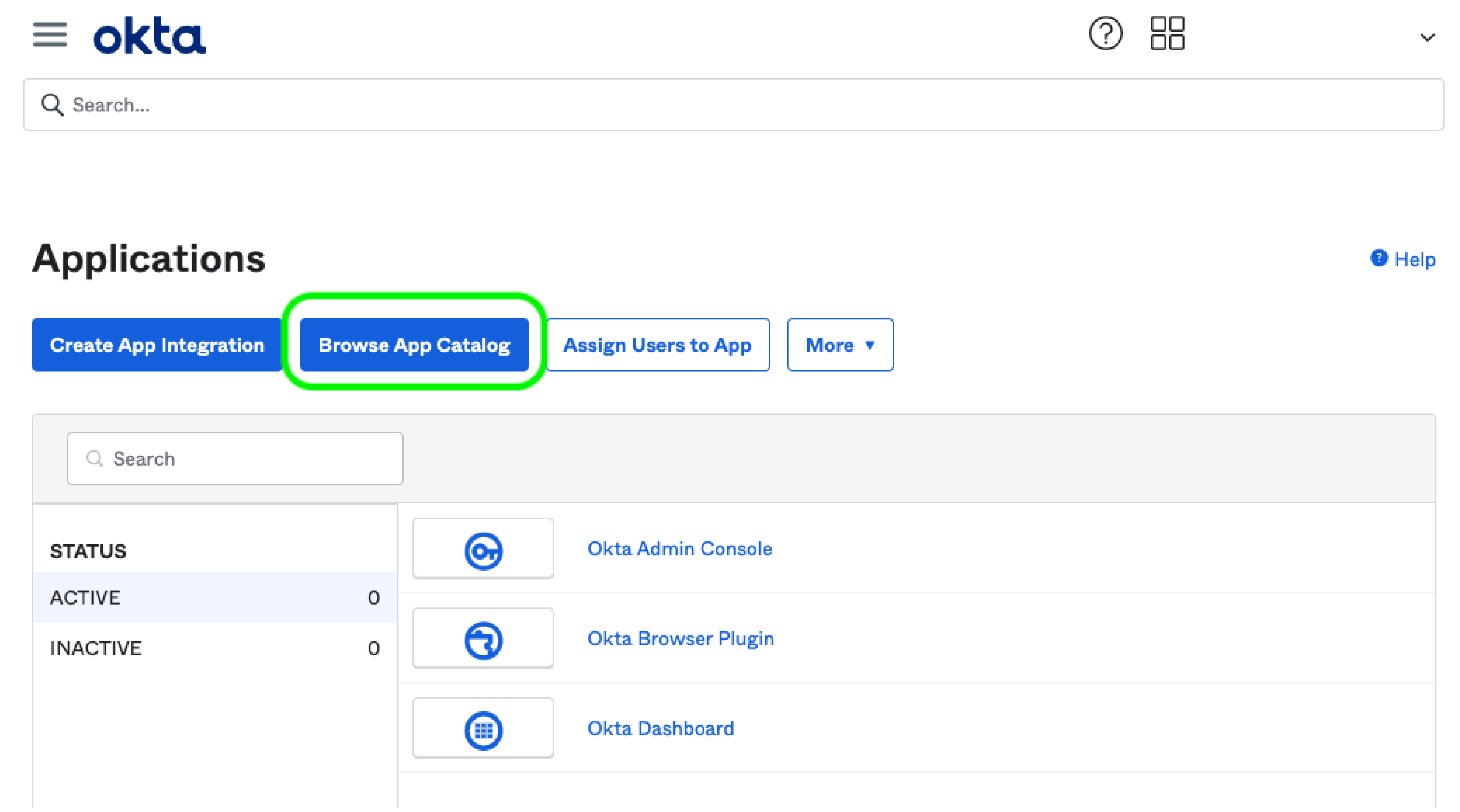
This API key has access to manage users within your organization. It should be kept secret.

SCIM provisioning

Select the **Enable SCIM** checkbox and take note of your **SCIM URL** and **SCIM API Key**. You will need to use both values in a later step.

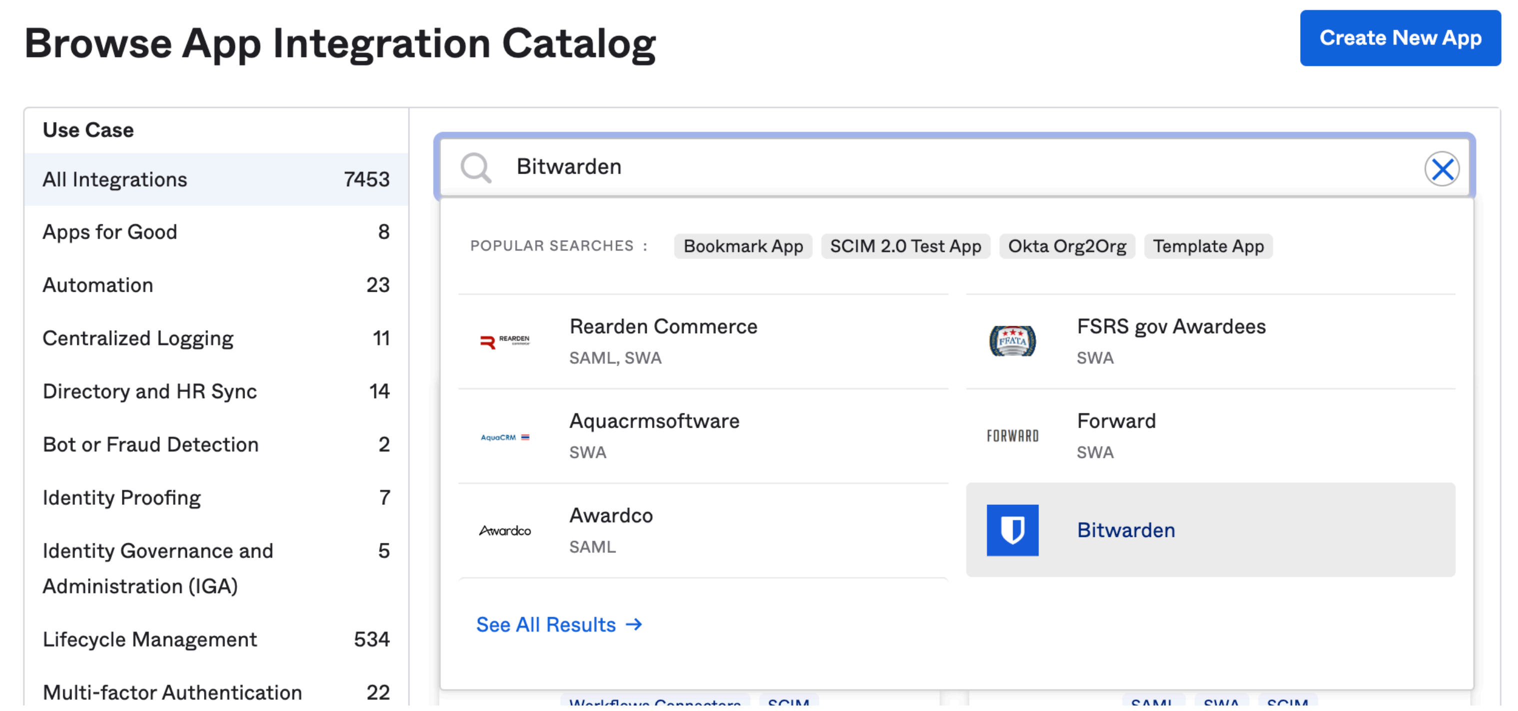
Add the Bitwarden app

In the Okta Admin Portal, select **Applications** → **Applications** from the navigation. On the Application screen, select the **Browse App Catalog** button:



Browse App Catalog

In the search bar, enter `Bitwarden` and select **Bitwarden**:



Use Case	
All Integrations	7453
Apps for Good	8
Automation	23
Centralized Logging	11
Directory and HR Sync	14
Bot or Fraud Detection	2
Identity Proofing	7
Identity Governance and Administration (IGA)	5
Lifecycle Management	534
Multi-factor Authentication	22

Bitwarden Okta App

Select the **Add Integration** button to proceed to configuration.

General settings

On the **General Settings** tab, give the application a unique, Bitwarden-specific label. Check the **Do not display application icon to users** and **Do not display application icon in Okta Mobile App** options and select **Done**.

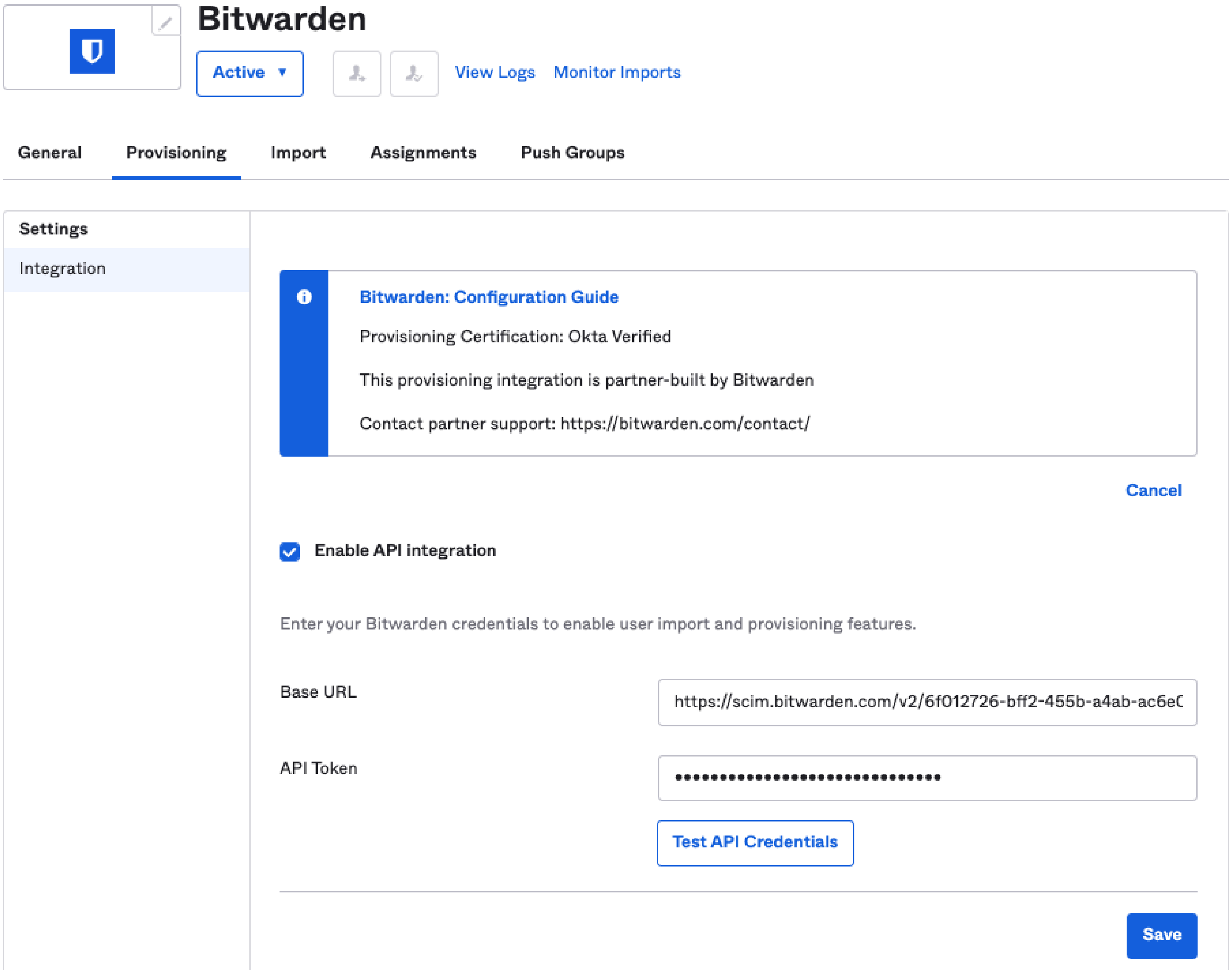
Setup provisioning

To setup provisioning, the following steps must be completed in the order presented.

Provisioning settings

Open the **Provisioning** tab and select the **Configure API Integration** button.

Once selected, Okta will list a few options for you to configure:



Bitwarden: Configuration Guide

Provisioning Certification: Okta Verified

This provisioning integration is partner-built by Bitwarden

Contact partner support: https://bitwarden.com/contact/

☑ Enable API integration

Enter your Bitwarden credentials to enable user import and provisioning features.

Base URL: https://scim.bitwarden.com/v2/6f012726-bff2-455b-a4ab-ac6e(

API Token: ••••••••••••••••••••••••••••••

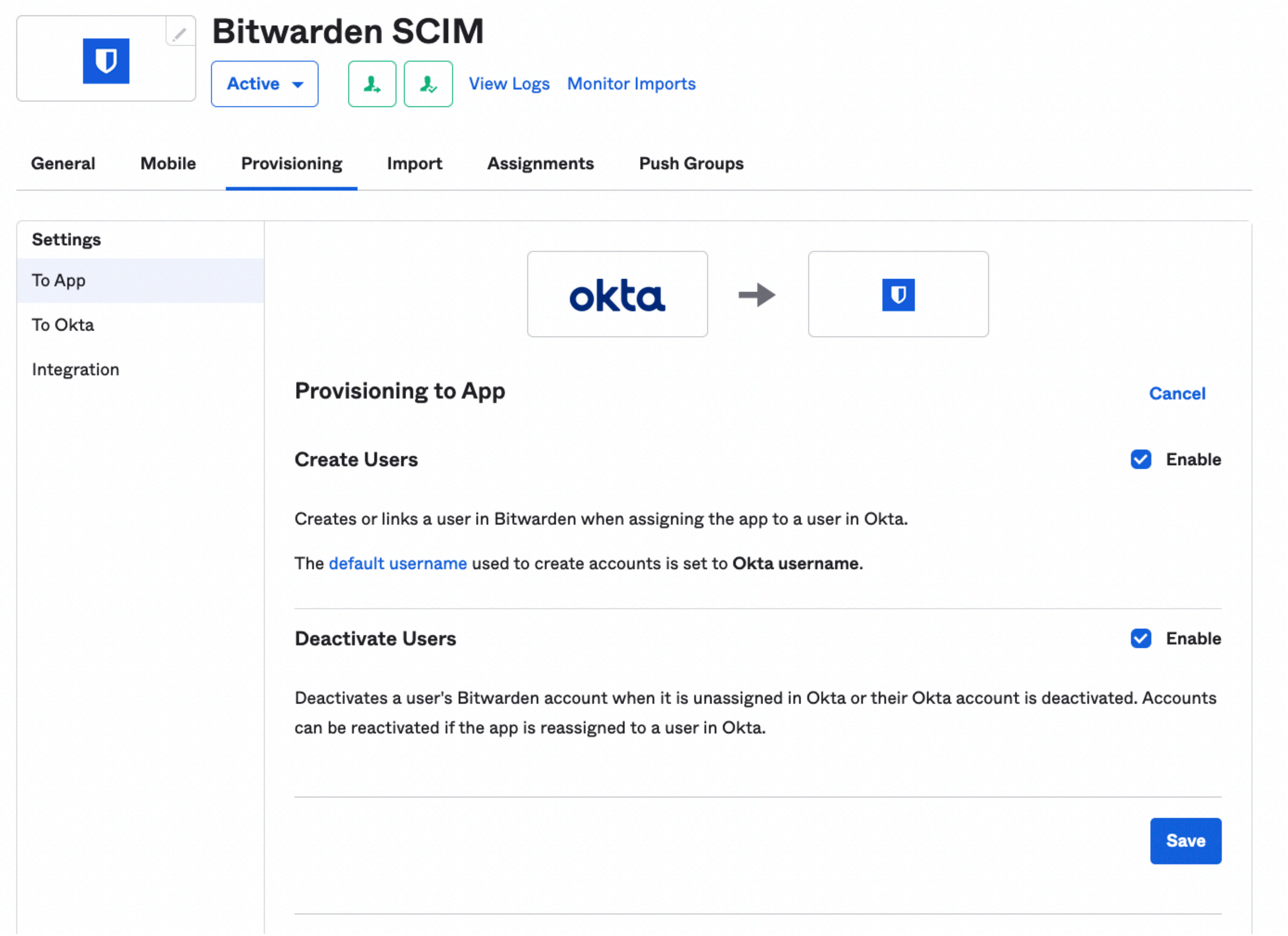
Configure API Integration

1. Check the **Enable API Integration** checkbox.
2. In the **Base URL** field, enter your SCIM URL, which can be found on the SCIM Provisioning screen (learn more).
3. In the **API Token** field, enter your SCIM API Key (learn more).

Once you are finished, use the **Test API Credentials** button to test your configuration. If it passes the test, select the **Save** button.

Set Provisioning actions

After the provisioning settings step has been completed, navigate to the **Provisioning** → **To App** screen. Then, select the **Edit** button:



Provisioning to App

Create Users ☑ Enable

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

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

Deactivate Users ☑ Enable

Deactivates a user's Bitwarden 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.

Provisioning To App

Enable, at a minimum, **Create Users** and **Deactivate Users**. Select **Save** when you are done.

Assignments

Open the **Assignments** tab and use the Assign dropdown menu to assign people or groups to the application. Assigned users and groups will be automatically issued an invitation. Depending on your workflow, you may need to use the **Push Groups** tab to trigger group provisioning once they are assigned.

Finish user onboarding

Now that your users have been provisioned, they will receive invitations to join the organization. Instruct your users to accept the invitation and, once they have, confirm them to the organization.

> ⓘ **Note**
>
> The Invite → Accept → Confirm workflow facilitates the decryption key handshake that allows users to securely access organization vault data.