

BEHEERCONSOLE > GEBRUIKERSBEHEER >

Integratie met Okta SCIM



Integratie met Okta SCIM

System for cross-domain identity management (SCIM) kan worden gebruikt om leden en groepen in uw Bitwarden-organisatie automatisch te provisioneren en de-provisioneren.

Note

SCIM-integraties zijn beschikbaar voor **Enterprise-organisaties**. Teams organisaties, of klanten die geen SCIM-compatibele identity provider gebruiken, kunnen overwegen [Directory Connector](#) te gebruiken als een alternatieve manier van provisioning.

Dit artikel helpt u bij het configureren van een SCIM-integratie met Okta. Bij de configuratie wordt tegelijkertijd gewerkt met de Bitwarden-webkuis en Okta Admin Portal. We raden u aan om beide documenten bij de hand te hebben en de stappen uit te voeren in de volgorde waarin ze zijn beschreven.

Ondersteunde functies

De volgende provisioningfuncties worden ondersteund door deze integratie:

- **Push-gebruikers:** Gebruikers in Okta die zijn toegewezen aan Bitwarden worden toegevoegd als gebruikers in Bitwarden.
- **Gebruikers deactiveren:** Wanneer gebruikers worden gedeactiveerd in Okta, worden ze ook gedeactiveerd in Bitwarden.
- **Push groepen:** Groepen en hun gebruikers in Okta kunnen worden gepusht naar 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](#).

SCIM inschakelen

Note

Host je Bitwarden zelf? Zo ja, voer dan deze stappen uit [om SCIM in te schakelen voor uw server](#) voordat u verdergaat.

Om uw SCIM-integratie te starten, opent u de beheerconsole en navigeert u naar **Instellingen** → **SCIM-provisioning**:

bitwarden
Admin Console

- My Organization
- Collections
- Members
- Groups
- Reporting
- Billing
- Settings
 - Organization info
 - Policies
 - Two-step login
 - Import data
 - Export vault
 - Domain verification
 - Single sign-on
 - Device approvals
 - 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

SCIM API key

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

Save

SCIM-voorziening

Schakel het selectievakje **Enable SCIM in** en noteer uw **SCIM URL** en **SCIM API Key**. Je zult beide waarden in een latere stap moeten gebruiken.

De Bitwarden-app toevoegen

Selecteer in het Okta Admin Portal **Applicaties** → **Applicaties** in de navigatie. Selecteer in het scherm Applicatie de knop **Bladeren door App Catalog** :

Applications

[Help](#)[Create App Integration](#)[Browse App Catalog](#)[Assign Users to App](#)[More ▾](#)

STATUS

ACTIVE 0

INACTIVE 0



Okta Admin Console



Okta Browser Plugin



Okta Dashboard

[Browse App Catalog](#)

Voer in de zoekbalk **Bitwarden** in en selecteer **Bitwarden**:

Browse App Integration Catalog

[Create New App](#)

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

POPULAR SEARCHES : [Bookmark App](#) [SCIM 2.0 Test App](#) [Okta Org2Org](#) [Template App](#)



Rearden Commerce
SAML, SWA



FSRS gov Awardees
SWA



Aquacrmsoftware
SWA



Forward
SWA



Awardco
SAML



Bitwarden

[See All Results →](#)

[Workflow Connectors](#) [SCIM](#) [SAML](#) [SWA](#) [SCIM](#)

[Bitwarden Okta App](#)

Selecteer de knop **Integratie toevoegen** om verder te gaan met de configuratie.

Algemene instellingen

Geef de applicatie op het tabblad **Algemene instellingen** een uniek, Bitwarden-specifiek label. Schakel de opties **Toepassingspictogram niet weergeven aan gebruikers** en **Toepassingspictogram niet weergeven in Okta Mobile App in** en selecteer **Gereed**.

Bepaling instellen

Instellingen voor provisioning

Open het tabblad **Provisioning** en selecteer de knop **Configureer API-integratie**.

Zodra Okta is geselecteerd, worden er enkele opties weergegeven die u kunt configureren:

The screenshot shows the Bitwarden provisioning configuration page in Okta. At the top, there is a header for 'Bitwarden' with an 'Active' dropdown, two user icons, and links for 'View Logs' and 'Monitor Imports'. Below this is a navigation bar with tabs for 'General', 'Provisioning' (selected), 'Import', 'Assignments', and 'Push Groups'. On the left, a 'Settings' sidebar has 'Integration' selected. The main content area features an information box with the title 'Bitwarden: Configuration Guide', stating 'Provisioning Certification: Okta Verified' and 'This provisioning integration is partner-built by Bitwarden', with a link to contact partner support. Below this is a checkbox labeled 'Enable API integration' which is checked. A text prompt asks to enter Bitwarden credentials. There are two input fields: 'Base URL' with the value 'https://scim.bitwarden.com/v2/6f012726-bff2-455b-a4ab-ac6eC' and 'API Token' which is masked with dots. A 'Test API Credentials' button is located below the API token field. At the bottom right, there is a 'Save' button.

Configure API Integration

1. Schakel het selectievakje **API-integratie inschakelen in**.

2. Voer in het veld **Base URL** uw SCIM URL in, die u kunt vinden op het scherm SCIM Provisioning([meer informatie](#)).

3. Voer in het veld **API Token** uw SCIM API Key in([meer informatie](#)).

Zodra je klaar bent, gebruik je de **Test API Credentials** knop om je configuratie te testen. Als de test slaagt, selecteer je de knop **Opslaan**.

Provisioning-acties instellen

Selecteer in het scherm **Provisioning** → **To App** de knop **Edit** :

The screenshot shows the Bitwarden SCIM configuration interface. At the top, there's a header for 'Bitwarden SCIM' with an 'Active' dropdown, two user icons, and links for 'View Logs' and 'Monitor Imports'. Below this is a navigation bar with tabs: 'General', 'Mobile', 'Provisioning' (selected), 'Import', 'Assignments', and 'Push Groups'. On the left, a sidebar lists 'Settings', 'To App' (selected), 'To Okta', and 'Integration'. The main content area is titled 'Provisioning to App' and features a diagram showing 'Okta' pointing to the Bitwarden logo. Below the diagram, there are two sections: 'Create Users' and 'Deactivate Users'. The 'Create Users' section has a description: '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.' and is currently 'Enable' (checked). The 'Deactivate Users' section has a description: '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.' and is also 'Enable' (checked). A 'Cancel' button is at the top right, and a 'Save' button is at the bottom right.

Provisioning To App

Schakel ten minste **Gebruikers maken** en **Gebruikers deactiveren** in. Selecteer **Opslaan** als je klaar bent.

Opdrachten

Open het tabblad **Toewijzingen** en gebruik het vervolgkeuzemenu Toewijzen om personen of groepen toe te wijzen aan de applicatie. Toegewezen gebruikers en groepen krijgen automatisch een uitnodiging. Afhankelijk van je workflow kan het nodig zijn om het **Push Groups** tabblad te gebruiken om de groep provisioning te triggeren zodra ze zijn toegewezen.

Onboarding van gebruikers voltooien

Nu je gebruikers zijn voorzien, ontvangen ze uitnodigingen om lid te worden van de organisatie. Instrueer je gebruikers om [de uitnodiging te accepteren](#) en [bevestig ze daarna aan de organisatie](#).

Note

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