

ADMIN CONSOLE > USER MANAGEMENT >

OneLogin SCIM Integration

View in the help center:
<https://bitwarden.com/help/onelogin-scim-integration/>

OneLogin 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.

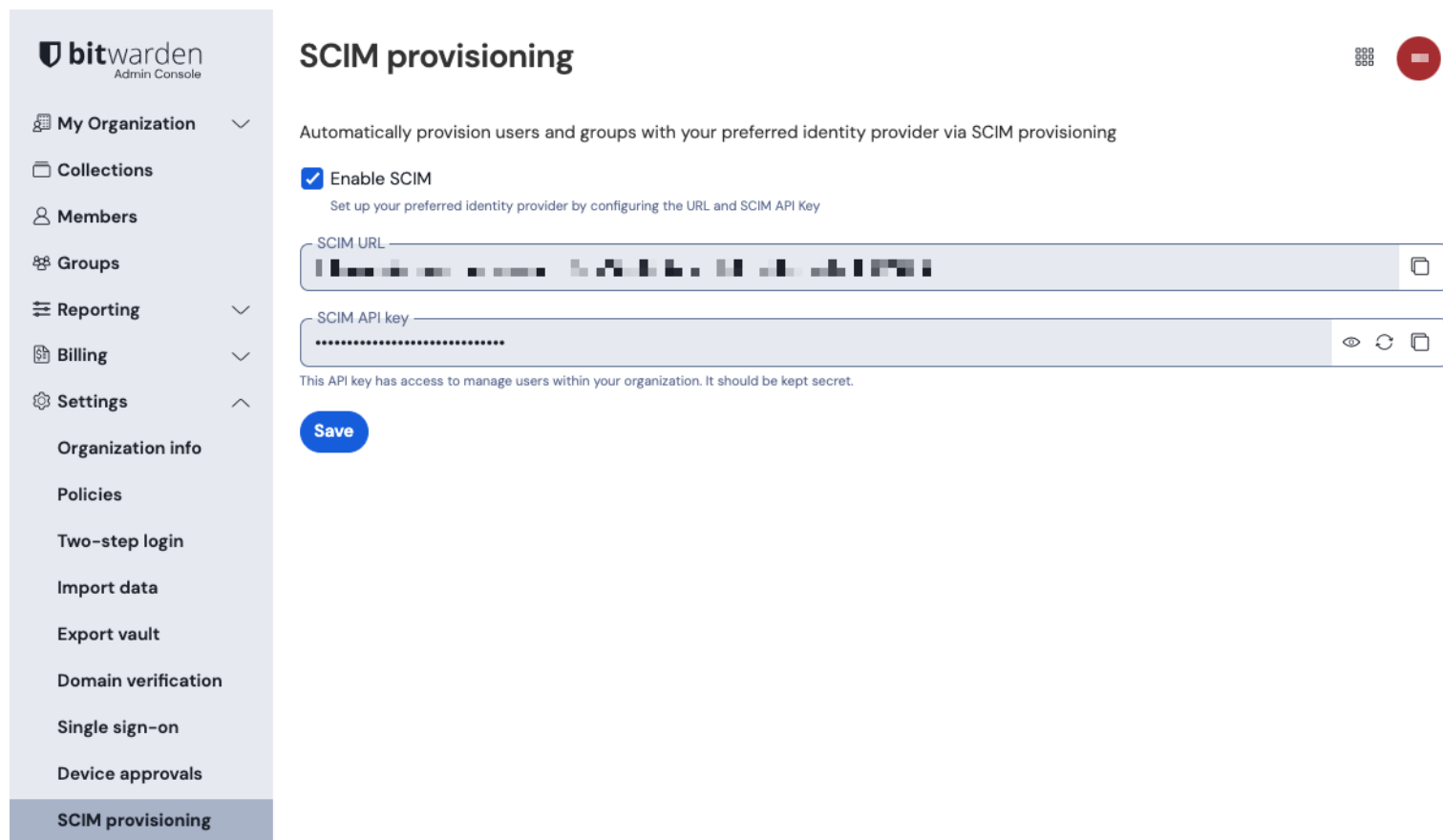
This article will help you configure a SCIM integration with OneLogin. Configuration involves working simultaneously with the Bitwarden web vault and OneLogin Admin Portal. As you proceed, we recommend having both readily available and completing steps in the order they are documented.

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**:



The screenshot shows the Bitwarden Admin Console interface. On the left is a sidebar with navigation links: My Organization, Collections, Members, Groups, Reporting, Billing, and Settings. The Settings section is expanded, showing options like Organization info, Policies, Two-step login, Import data, Export vault, Domain verification, Single sign-on, Device approvals, and SCIM provisioning (which is highlighted). The main content area is titled 'SCIM provisioning' and contains the following elements:

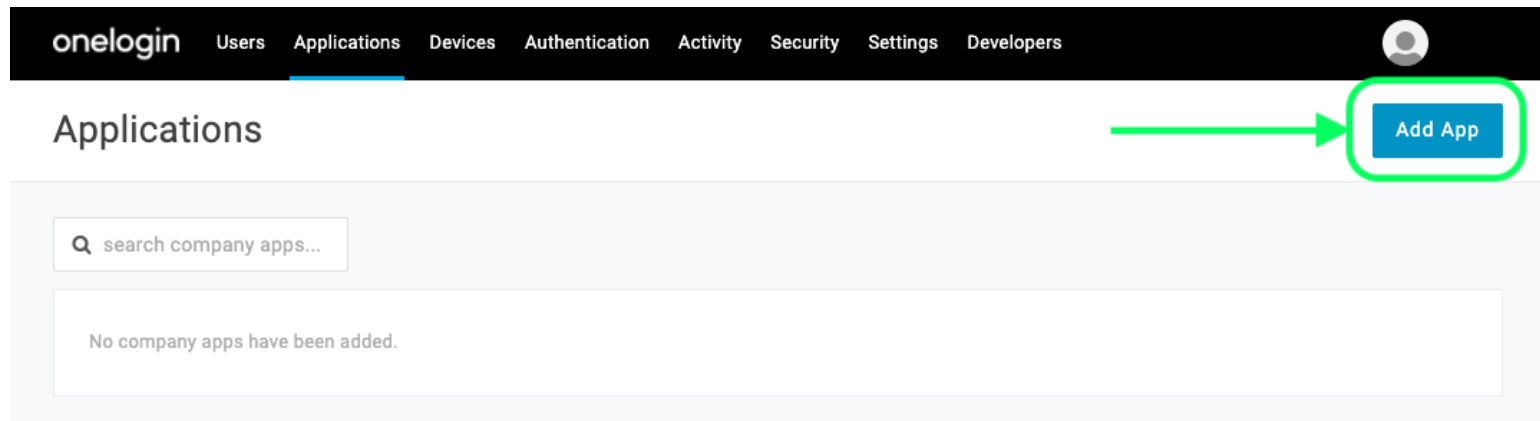
- A description: 'Automatically provision users and groups with your preferred identity provider via SCIM provisioning'.
- A checkbox labeled 'Enable SCIM' which is checked. Below it is the text: 'Set up your preferred identity provider by configuring the URL and SCIM API Key'.
- A text input field for 'SCIM URL' containing a long alphanumeric string, with a copy icon on the right.
- A text input field for 'SCIM API key' containing a series of dots, with an eye icon, a refresh icon, and a copy icon on the right.
- A warning message: 'This API key has access to manage users within your organization. It should be kept secret.'
- A blue 'Save' button.

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.

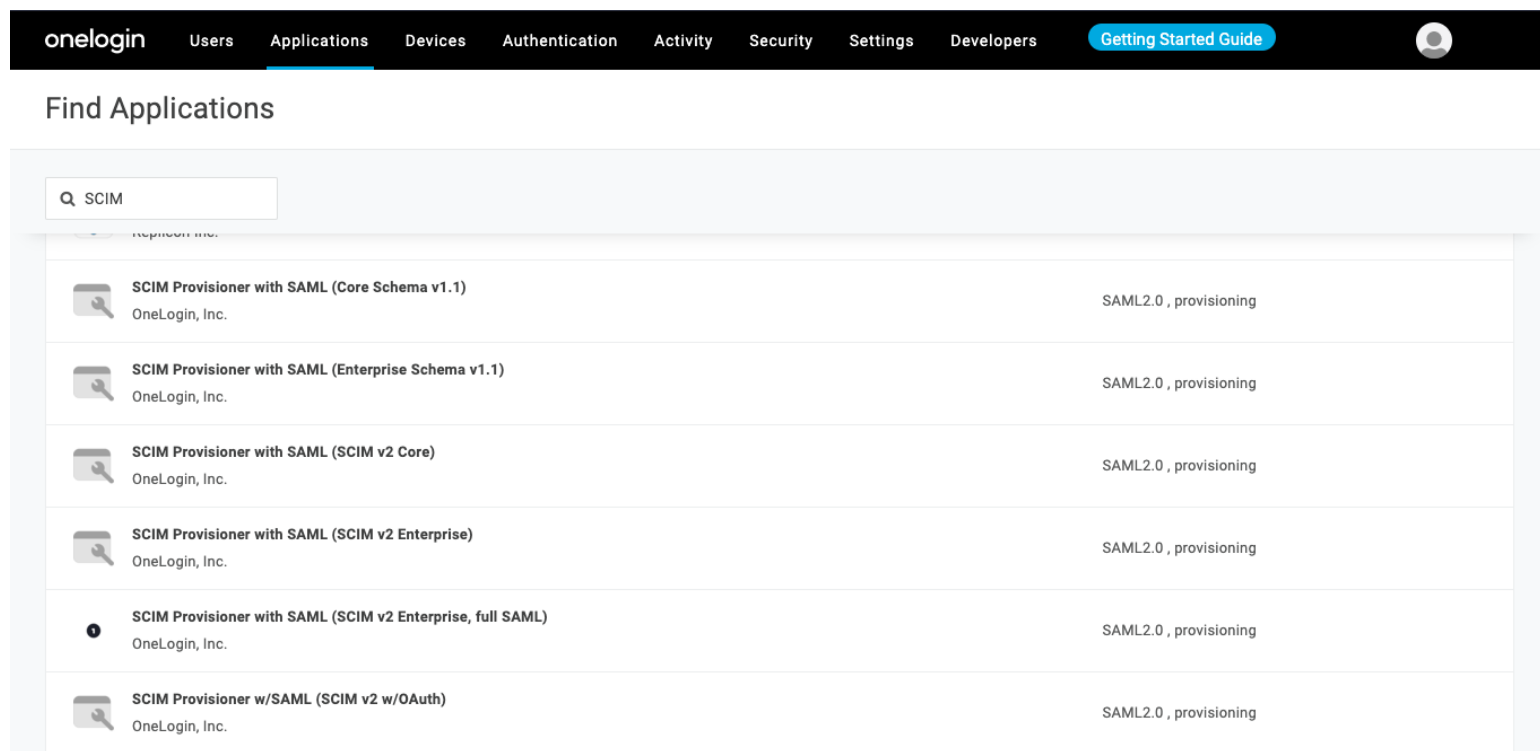
Create a OneLogin app

In the OneLogin Portal, navigate to the the **Applications** screen and select the **Add App** button:



Add an Application

In the search bar, type **SCIM** and select the **SCIM Provisioner with SAML (SCIM v2 Enterprise)** app:



SCIM Provisioner App

Give your application a Bitwarden-specific **Display Name** and select the **Save** button.

Configuration

Select **Configuration** from the left-hand navigation and configure the following information, some of which you will need to retrieve from the Single Sign-On and SCIM Provisioning screens in Bitwarden.

onelogin

Users

Applications

Devices

Authentication

Activity

Security

Settings

Developers

Getting Started Guide

Applications / SCIM Provisioner with SAML (SCIM v2 Enterprise)

More Actions

Save

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Application details

SAML Audience URL

SAML Consumer URL

API Connection

API Status

Disabled

Enable

SCIM Base URL

SCIM JSON Template

SCIM App Configuration

Application details

OneLogin will require you to fill in the **SAML Audience URL** and **SAML Consumer URL** fields even if you aren't going to use single sign-on. [Learn what to enter in these fields.](#)

API connection

Enter the following values in the **API Connection** section:

Application setting	Description
SCIM base URL	Set this field to the SCIM URL (learn more).
SCIM bearer token	Set this field to the SCIM API key (learn more).

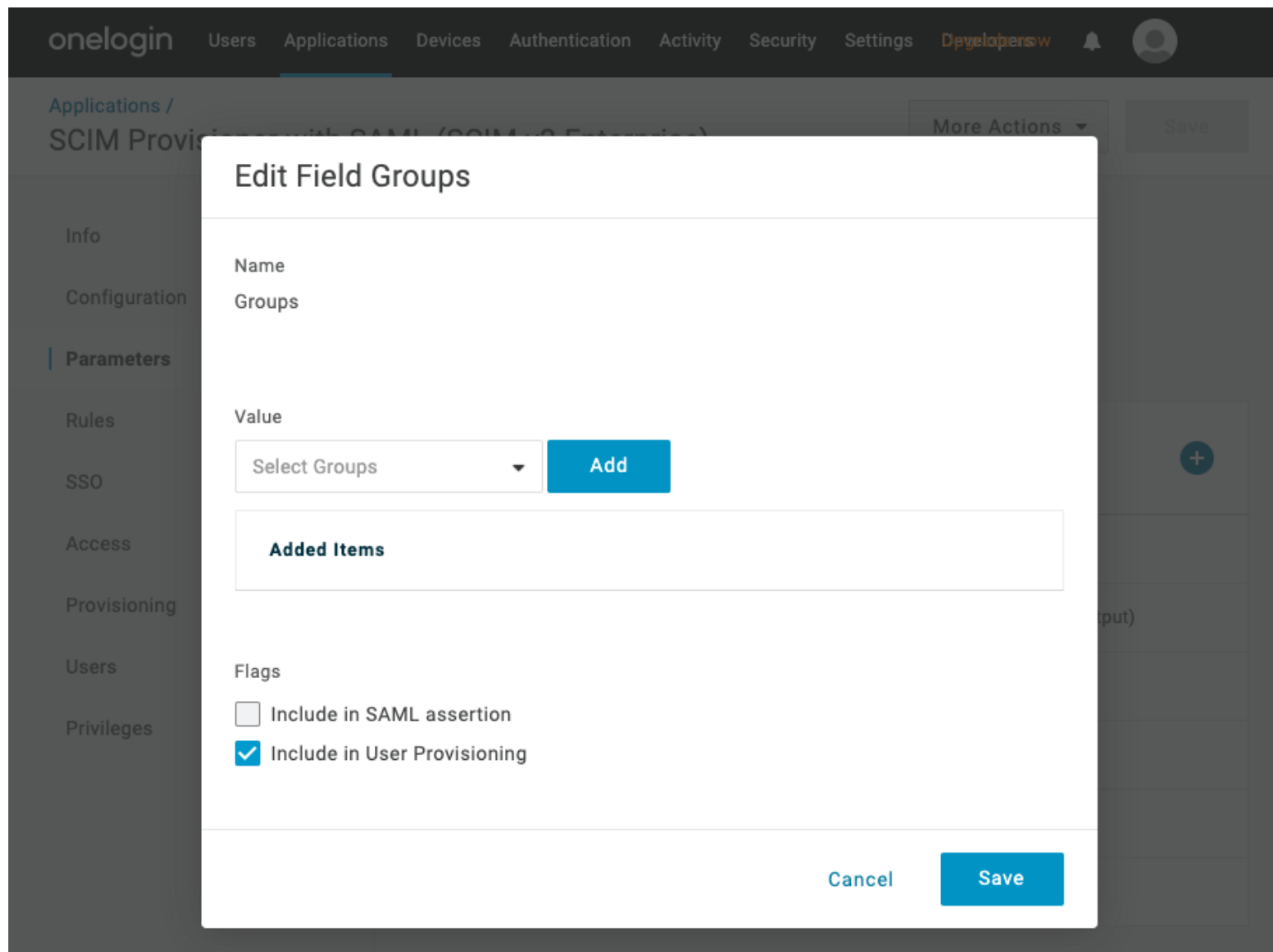
Select **Save** once you have configured these fields.

Access

Select **Access** from the left-hand navigation. In the **Roles** section, assign application access to all the roles you would like provision in Bitwarden. Each role is treated as a group in your Bitwarden organization, and users assigned to any role will be included in each group including if they are assigned multiple roles.

Parameters

Select **Parameters** from the left-hand navigation. Select **Groups** from the table, enable the **Include in User Provisioning** checkbox, and select the **Save** button:



Include Groups in User Provisioning

Rules

Create a rule to map OneLogin Roles to Bitwarden groups:

1. Select **Rules** from the left-hand navigation.
2. Select the Add Rule button to open the **New mapping** dialog:

More Actions ▾

New mapping

Name

Create Groups from Roles

Conditions

No conditions. Actions will apply to all users.

+

Actions

Set Groups in SCIM - SCIMonelogin - AJ ▾

☐ From Existing
 ☒ Map from OneLogin

For each

role ▾

with value that matches

.*

set SCIM - SCIMonelogin - AJ Groups named after **roles**.

+

Cancel

Save

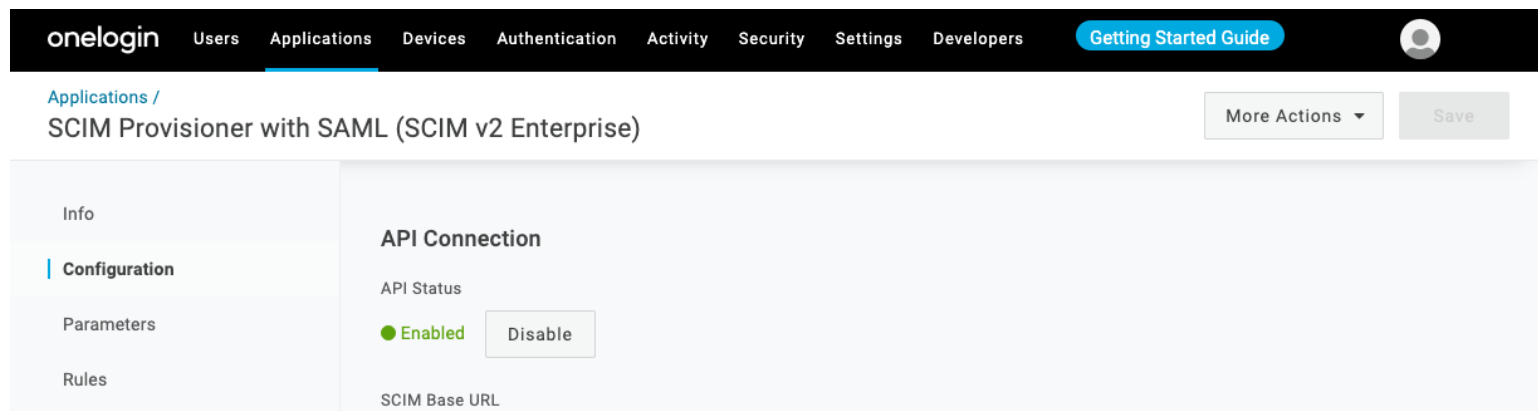
Role/Group Mapping

3. Give the rule a **Name** like Create Groups from Rules.
4. Leave **Conditions** blank.
5. In the **Actions** section:
 1. Select **Set Groups in <application_name>** from the first dropdown.
 2. Select the **Map from OneLogin** option.
 3. Select **role** from the "For each" dropdown.
 4. Enter **.*** in the "with value that matches" field to map all roles to groups, or enter a specific role name.

6. Select the **Save** button to finish creating the rule.

Test connection

Select **Configuration** from the left-hand navigation, and select the **Enable** button under **API Status**:



onelogin Users Applications Devices Authentication Activity Security Settings Developers Getting Started Guide

Applications / SCIM Provisioner with SAML (SCIM v2 Enterprise) More Actions Save

Info Configuration Parameters Rules

API Connection

API Status

● Enabled Disable

SCIM Base URL

Test API Connection

This test **will not** start provisioning, but will make a GET request to Bitwarden and display **Enabled** if the application gets a response from Bitwarden successfully.

Enable provisioning

Select **Provisioning** from the left-hand navigation:

onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers

Applications /
SCIM Provisioner with SAML (SCIM v2 Enterprise)

Info
Configuration
Parameters
Rules
SSO
Access
Provisioning
Users
Privileges

Workflow

☒ Enable provisioning

Require admin approval before this action is performed

☐ Create user
☒ Delete user
☐ Update user

When users are deleted in OneLogin, or the user's app access is removed, perform the below action

Delete

When user accounts are suspended in OneLogin, perform the following action:

Suspend

Entitlements

Refresh

Entitlements are user attributes that are usually associated with fine-grained app access, like app group, department, organization, or license level. When you click Refresh, OneLogin imports your organization's app entitlement values (such as group names or license types) so you can map them to OneLogin attribute values. Entitlement refresh can take several minutes. Check Activity > Events for completion status.

Provisioning Settings

On this screen:

1. Select the **Enable Provisioning** checkbox.
2. In the **When users are deleted in OneLogin...** dropdown, select **Delete**.
3. In the **When user accounts are suspended in OneLogin...** dropdown, select **Suspend**.

When you are done, select **Save** to trigger provisioning.

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.

Appendix

User attributes

Both Bitwarden and OneLogin's **SCIM Provisioner with SAML (SCIM v2 Enterprise)** application use standard SCIM v2 attribute names. Bitwarden will use the following attributes:

- `active`
- `emails`^a or `userName`
- `displayName`
- `externalId`

^a – Because SCIM allows users to have multiple email addresses expressed as an array of objects, Bitwarden will use the `value` of the object which contains `"primary": true`.