bitwarden | Help Center Article

MY ACCOUNT > TWO-STEP LOGIN >

Two-step Login via Duo

View in the help center:
https://bitwarden.com/help/setup-two-step-login-duo/

Two-step Login via Duo

Two-step login using Duo is unique among available two-step login methods in that it can be enabled for a personal account (like the other methods) or enabled for an entire organization by teams and enterprise organizations.

Setup Duo

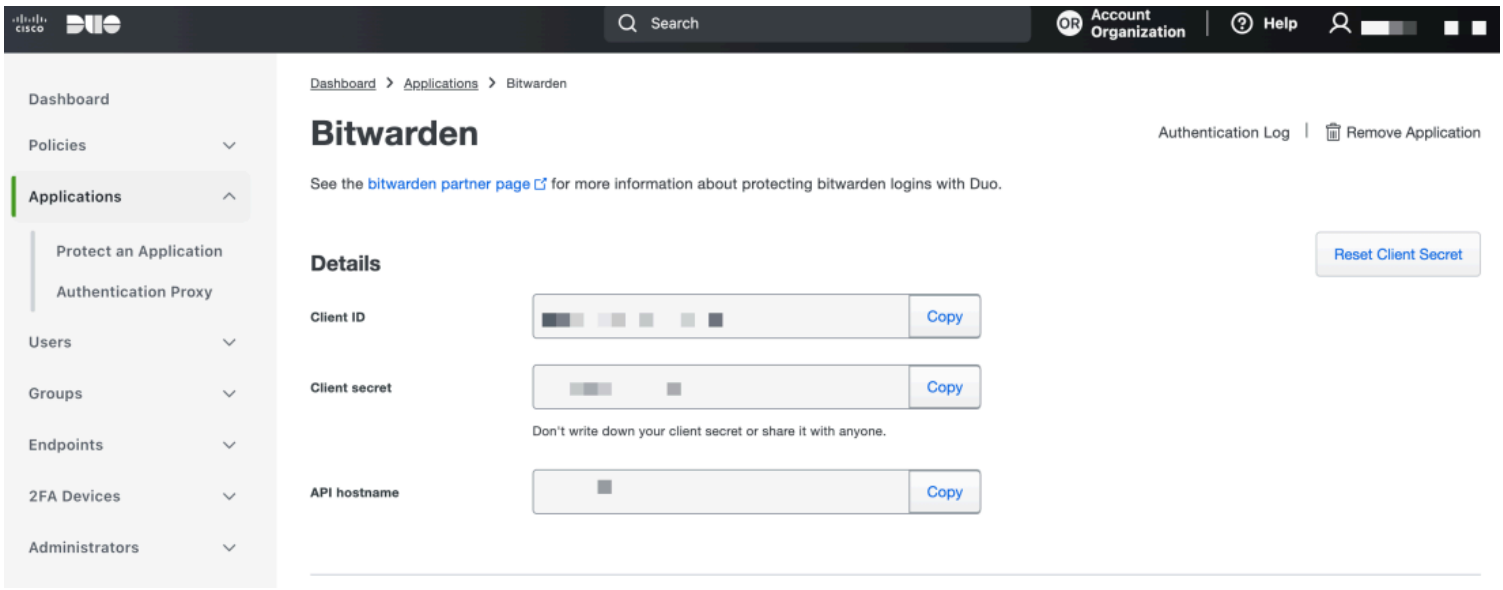
This article covers Duo setup for **Personal users**, **Organization users**, and **Organization admins**:

⇒Personal user

Retrieve Duo keys

You will need a Duo account in order to obtain some information required by Bitwarden to complete setup. Sign up for free, or log in to your existing Duo Admin Panel. To configure Duo:

1. In the left menu, navigate to **Applications**.
2. Select the **Protect an Application** button.
3. Find or search for **Bitwarden** in the applications list, and select the **Protect** button. You will be redirected to a Bitwarden application page:



Duo Bitwarden Application

Take note of the **Client ID**, **Client secret**, and **API Hostname**. You will need to reference these values when you setup Duo within Bitwarden.

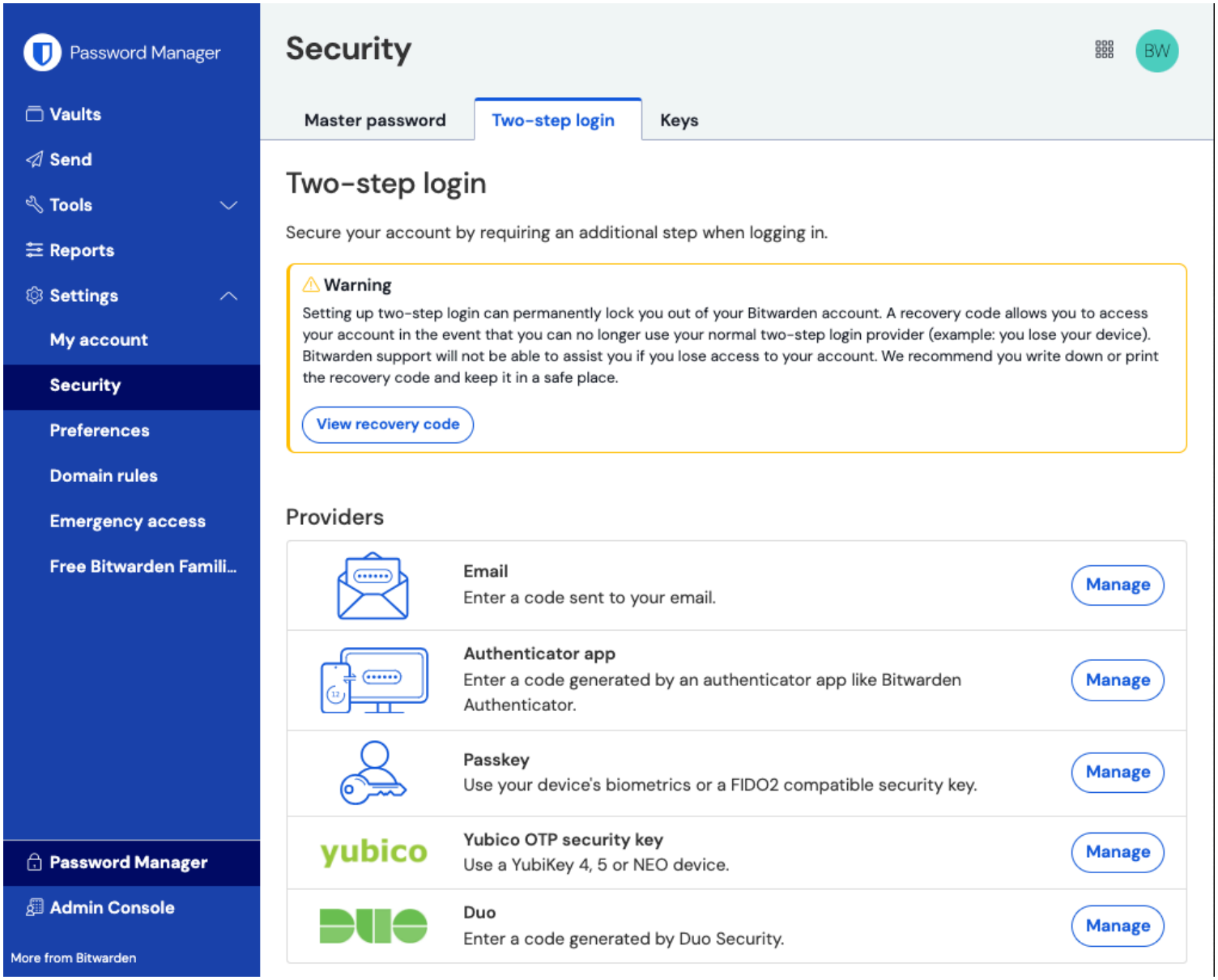
Setup Duo in Bitwarden

> ⚠ **Warning**
>
> **Losing access to your two-step login device can permanently lock you out of your vault** unless you write down and keep your two-step login recovery code in a safe place or have an alternate two-step login method enabled and available.
>
> Get your recovery code from the **Two-step login** screen immediately after enabling any method. Additionally, users may create a Bitwarden export to backup vault data.

To enable two-step login using Duo as a personal user:

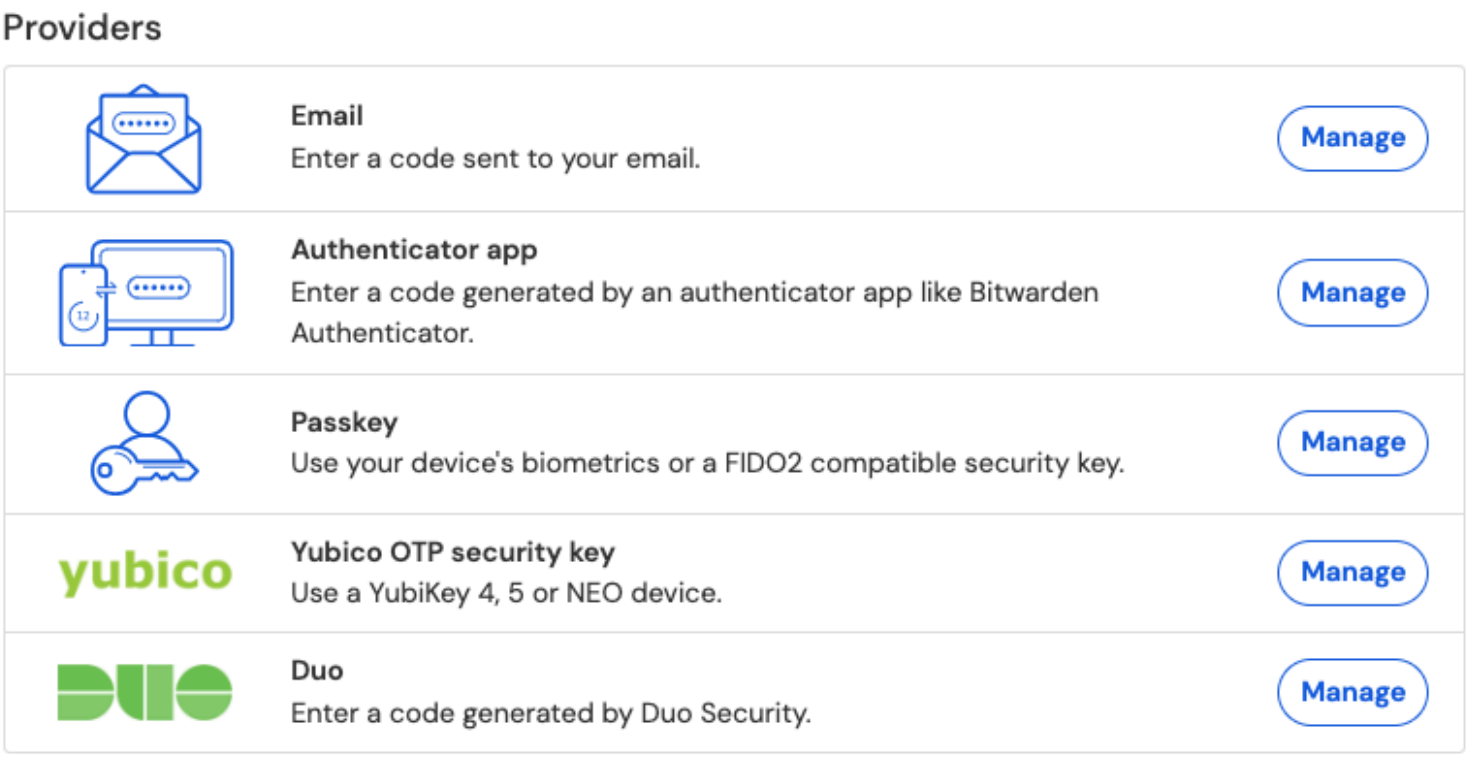
1. Log in to the Bitwarden web app.

2. Select **Settings** → **Security** → **Two-step login** from the navigation:



Two-step login

3. Locate the **Duo** option and select the **Manage** button.



Two-step login providers

You will be prompted to enter your master password to continue.

4. Enter the following values retrieved from the Duo Admin Panel (see the above section in this tab):
   - **Client ID** into the **Integration Key** field
   - **Client Secret** into the **Secret Key** field
   - Enter the **API Hostname**
5. Select the **Enable** button.

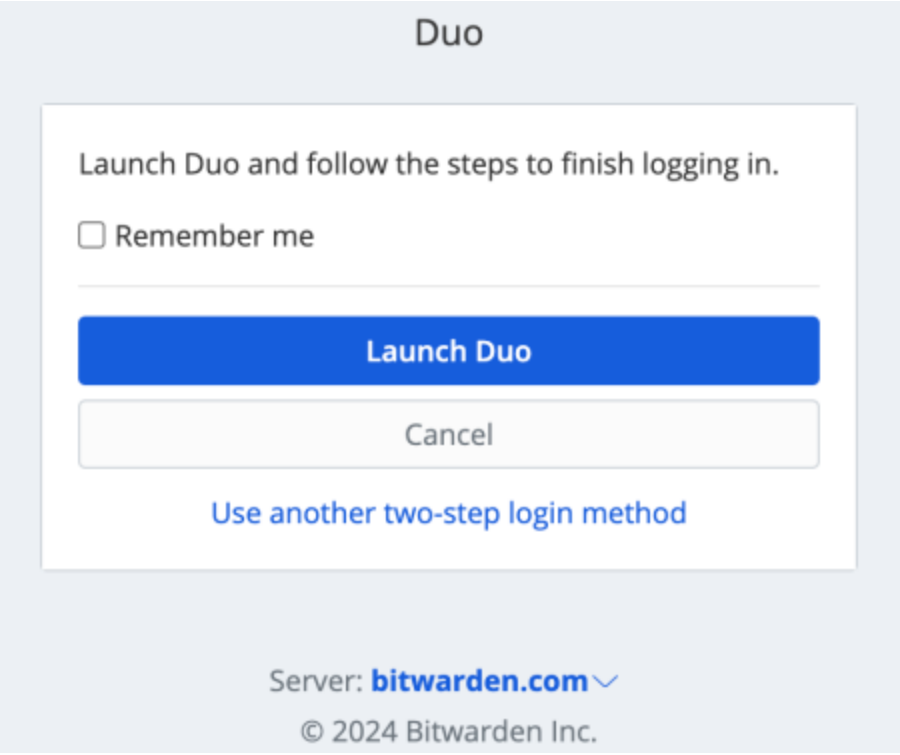
A green `Enabled` message should appear to indicate that Duo has been enabled for your vault. You can double-check by selecting the **Close** button and seeing that the **Duo** option has a green checkmark (✓) on it.

We recommend keeping your active web vault tab open before proceeding to test two-step login in case something was misconfigured. Once you have confirmed it's working, logout of all your Bitwarden apps to require two-step login for each. You will eventually be logged out automatically.

> **Note**
>
> Self-hosted instances operating on air-gapped networks may require additional setup in order to maintain server communication with Duo.

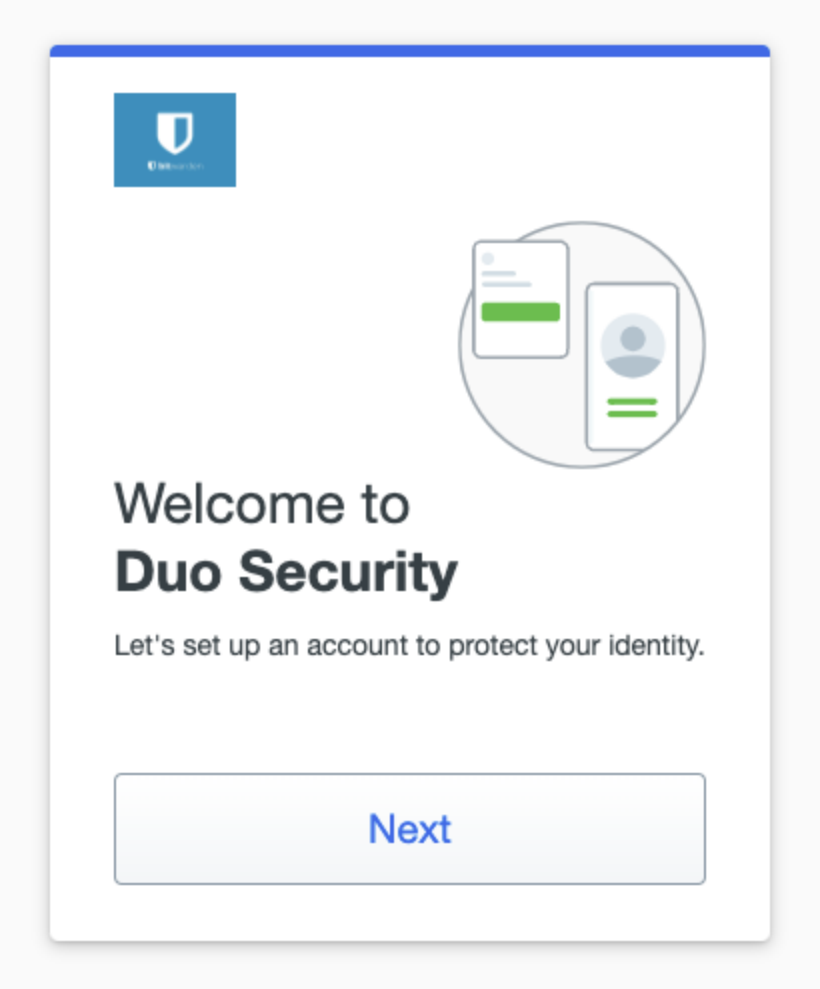
Register a device

Once Duo is setup, open the web vault. If Duo is your highest-priority enabled method, you will be prompted to **Launch Duo** the next time you log on:



Launch Duo Individual

You will be asked to register a two-step login device, follow the on-screen prompts to configure a secondary device to use Duo (for example, what type of device to register and whether to send an SMS or push notification).



Duo 2FA setup

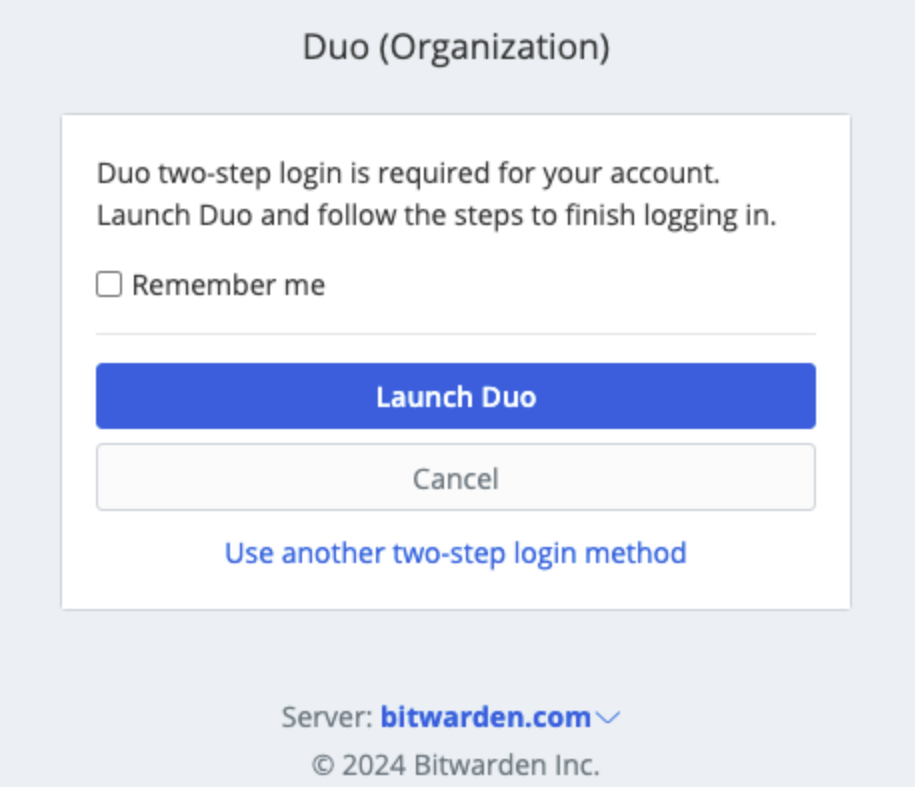
If you have not already downloaded the Duo mobile app, we recommend that you do so:

- Download for iOS
- Download for Android

⇒Organization user

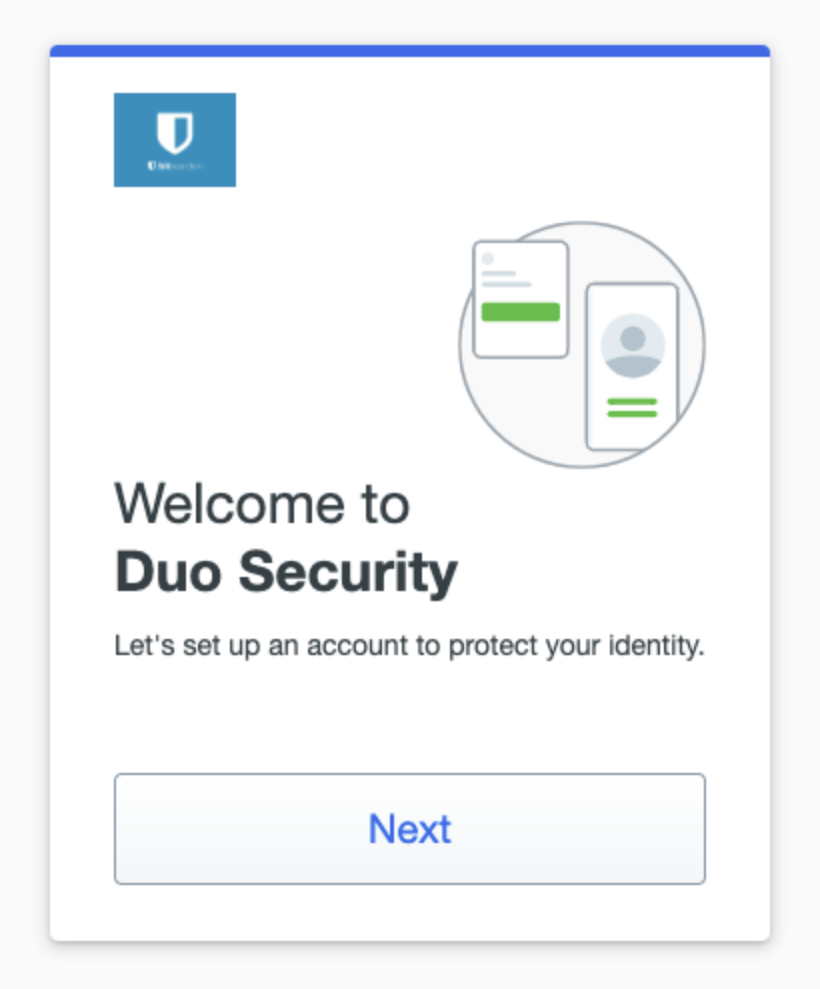
Register a device

Once your organization admin has setup Duo, you will be prompted to **Launch Duo** the next time you log on:



Launch Duo

You will be asked to register a two-step login device, follow the on-screen prompts to configure a secondary device to use Duo (for example, what type of device to register and whether to send an SMS or push notification).



Duo 2FA setup

> **Tip**
> If you don't get asked by Duo to register a device, try logging in using an incognito or private browsing window.

If you haven't already downloaded the Duo mobile app, we recommend that you do so:

- Download for iOS
- Download for Android

⇒Organization admin

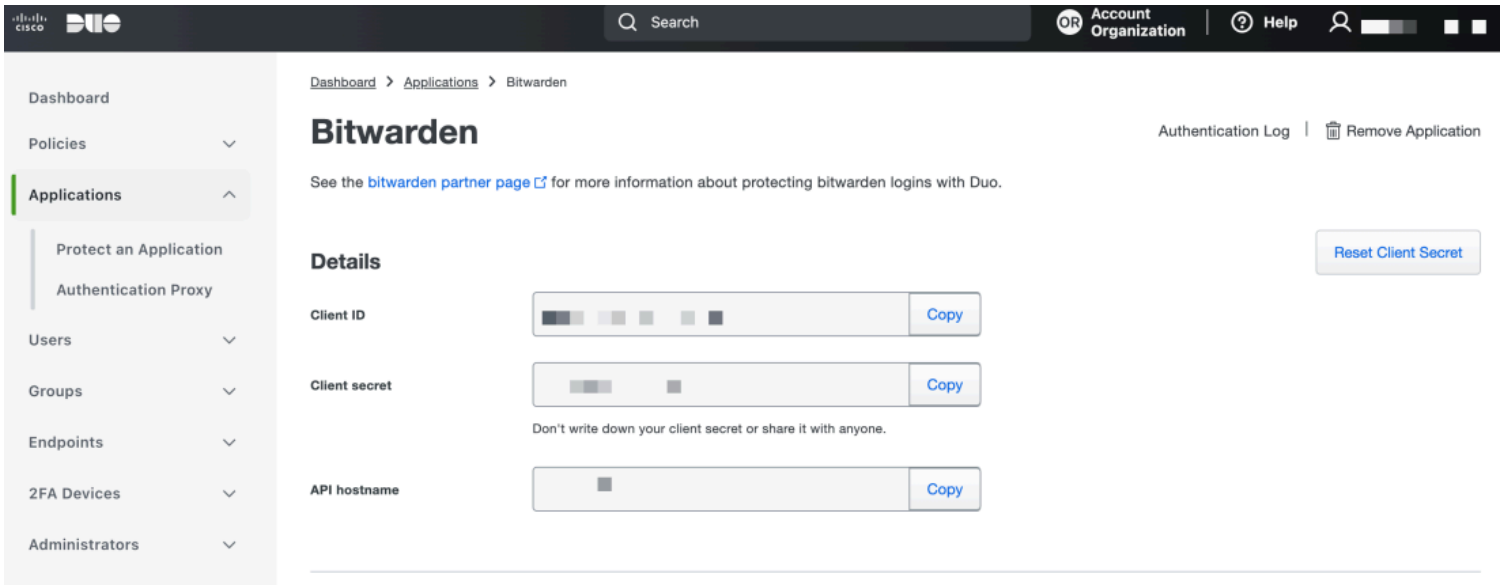
Enabling Duo for an organization will prompt all enrolled members to register a device for Duo two-step login the next time they log in to the web vault.

> **Note**
> Bitwarden will only recognize users with email address usernames. Duo users that do not have an email address as their primary username will require one. Please reference Duo Username Aliases Configuration Guide for additional information and instructions.

Retrieve Duo keys

You will need a Duo account in order to obtain some information required by Bitwarden to complete setup. Sign up for free, or log in to your existing Duo Admin Panel. To configure Duo:

1. In the left menu, navigate to **Applications**.
2. Select the **Protect an Application** button.
3. Find or search for **Bitwarden** in the Applications list, and select the **Protect** button. You will be redirected to a Bitwarden application page:



Duo Bitwarden Application

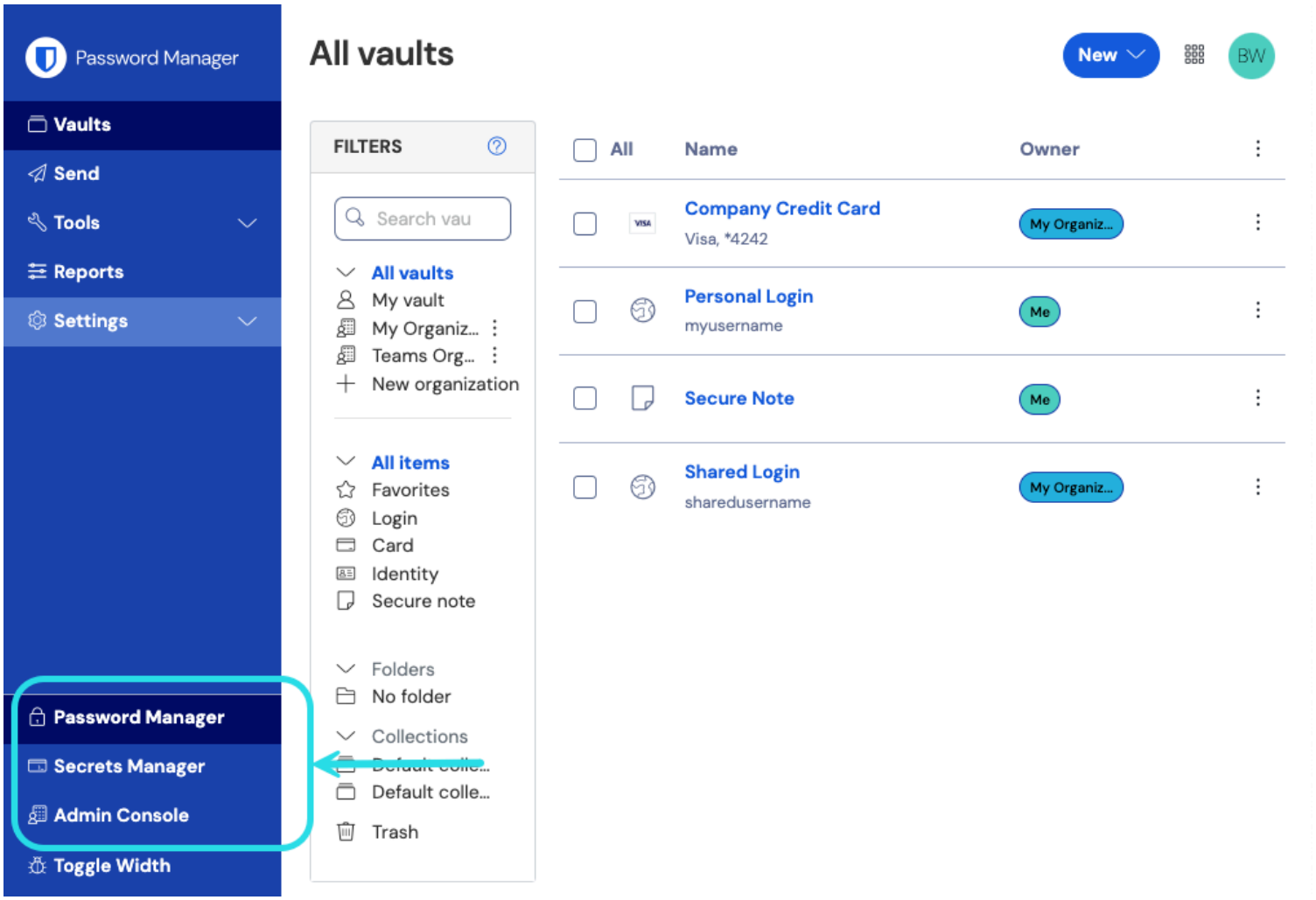
Take note of the **Client ID**, **Client secret**, and **API Hostname**. You will need to reference these values when you setup Duo within Bitwarden.

Setup Duo in Bitwarden

> **⚠ Warning**
>
> Once you initially configure and setup Duo, it is **critically important** that you disable it for the organization before making any further application configuration changes from the Duo Admin Panel. To make configuration changes; disable Duo in Bitwarden, make the required changes in the Duo Admin Panel, and re-enable Duo in Bitwarden.
>
> This is because Duo for organizations does not currently support recovery codes. Instead, you will need to rely on the Duo Admin Panel to bypass two-step login for members who lose access to Duo. Altering the application configuration from the Duo Admin Panel while Duo is active risks losing the ability to bypass two-step login for you or your organization's members.

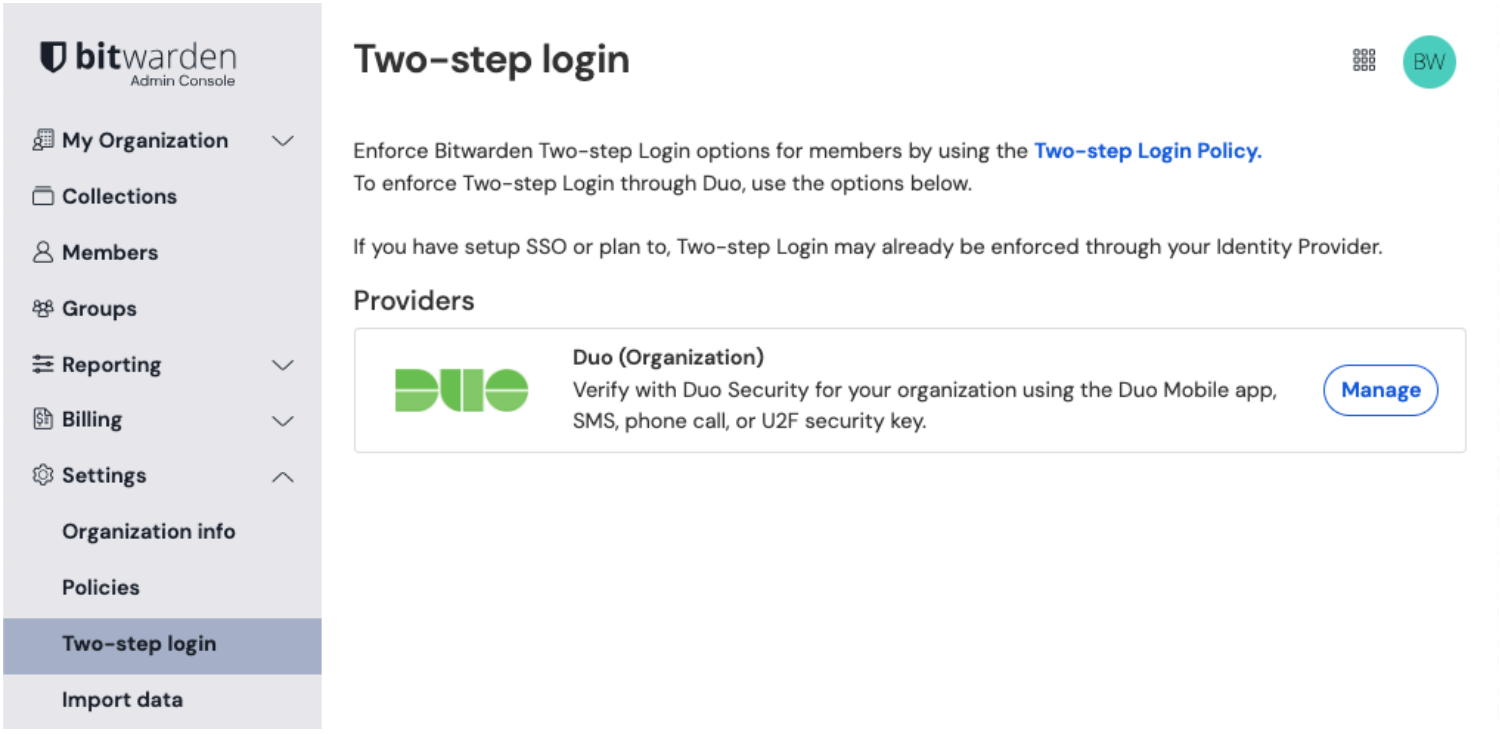
You must be an organization owner to setup Duo for your organization. To enable two-step login using Duo for your organization:

1. Log in to the Bitwarden web app.
2. Open the Admin Console using the product switcher:



Product switcher

3. Select **Settings** → **Two-step login** from the navigation:



Manage Duo for organizations

4. Locate the **Duo (Organization)** option and select the **Manage** button.

5. You will be prompted to enter your master password to continue.

6. Enter the following values retrieved from the Duo Admin Panel:

   - **Client ID** into the **Integration Key** field
   - **Client Secret** into the **Secret Key** field
   - Enter the **API Hostname**

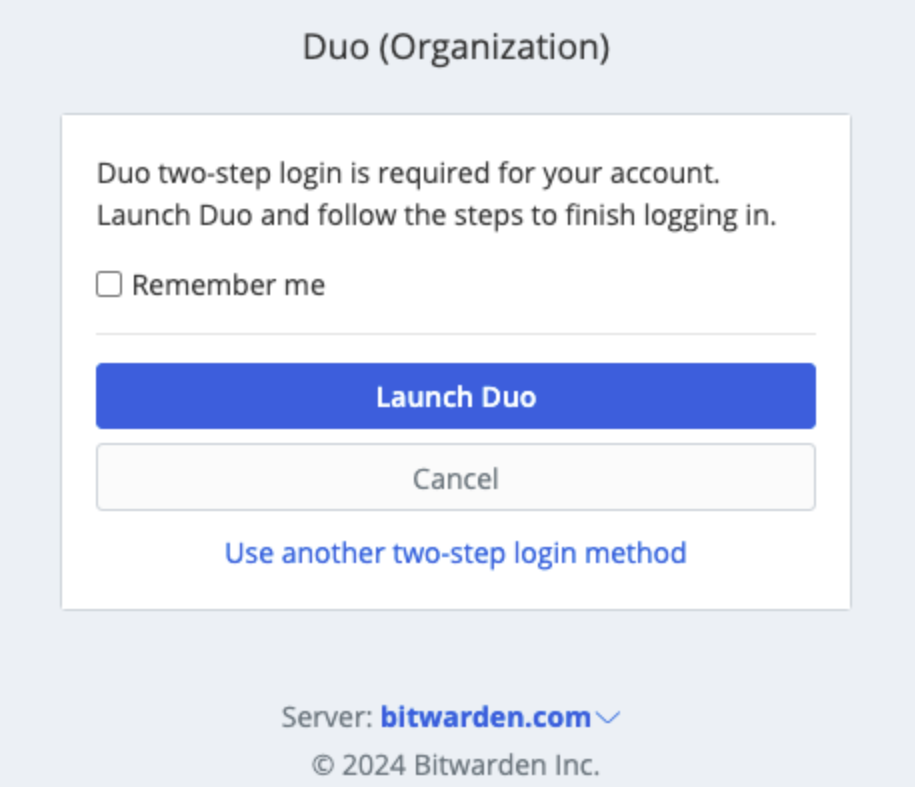
7. Select the **Enable** button.

A green `Enabled` message should appear to indicate that Duo has been enabled for your vault. You can double-check by selecting the **Close** button and seeing that the **Duo** option has a green checkmark (✓) on it.

> **Note**
>
> Self-hosted instances operating on air-gapped networks may require additional setup in order to maintain server communication with Duo.

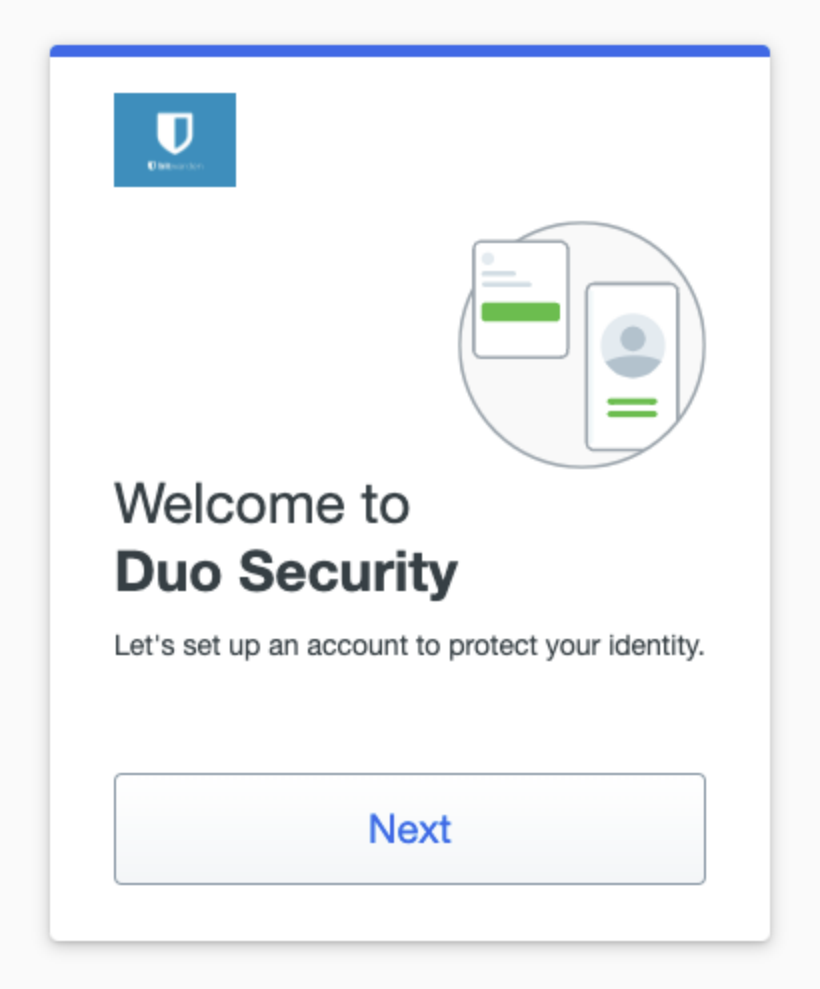
Register a device

Once Duo is setup, you and your organization members will be prompted to **Launch Duo** the next time you log on:



Launch Duo

You will be asked to register a two-step login device, follow the on-screen prompts to configure a secondary device to use Duo (for example, what type of device to register and whether to send an SMS or push notification).



Duo Setup Screen

> **Tip**
> If you don't get asked by Duo to register a device, try logging in using an incognito or private browsing window.

If you haven't already downloaded the Duo mobile app, we recommend that you do so:

- Download for iOS
- Download for Android

Use Duo

The following assumes that **Duo** is your highest-priority enabled method. For organization members, **org-wide Duo is always the highest-priority method**. To access your vault using Duo two-step login:

1. Login to your Bitwarden vault on any app and enter your email address and master password. A prompt will ask you to **Launch Duo**. Once launched, a Duo screen will appear to begin your two-step login verification.

2. Depending on how you have configured Duo, complete the authentication request by:

   - Approving the **Duo Push** request from your registered device.

- Finding the six-digit verification code in your **Duo Mobile** app or **SMS** messages, and enter the code on the vault login screen.

  > **Tip**
  > Check the **Remember Me** box to remember your device for 30 days. Remembering your device will mean you won't be required to complete your two-step login step.

You will not be required to complete your secondary two-step login step to **unlock** your vault once logged in. For help configuring log out vs. lock behavior, see vault timeout options.