

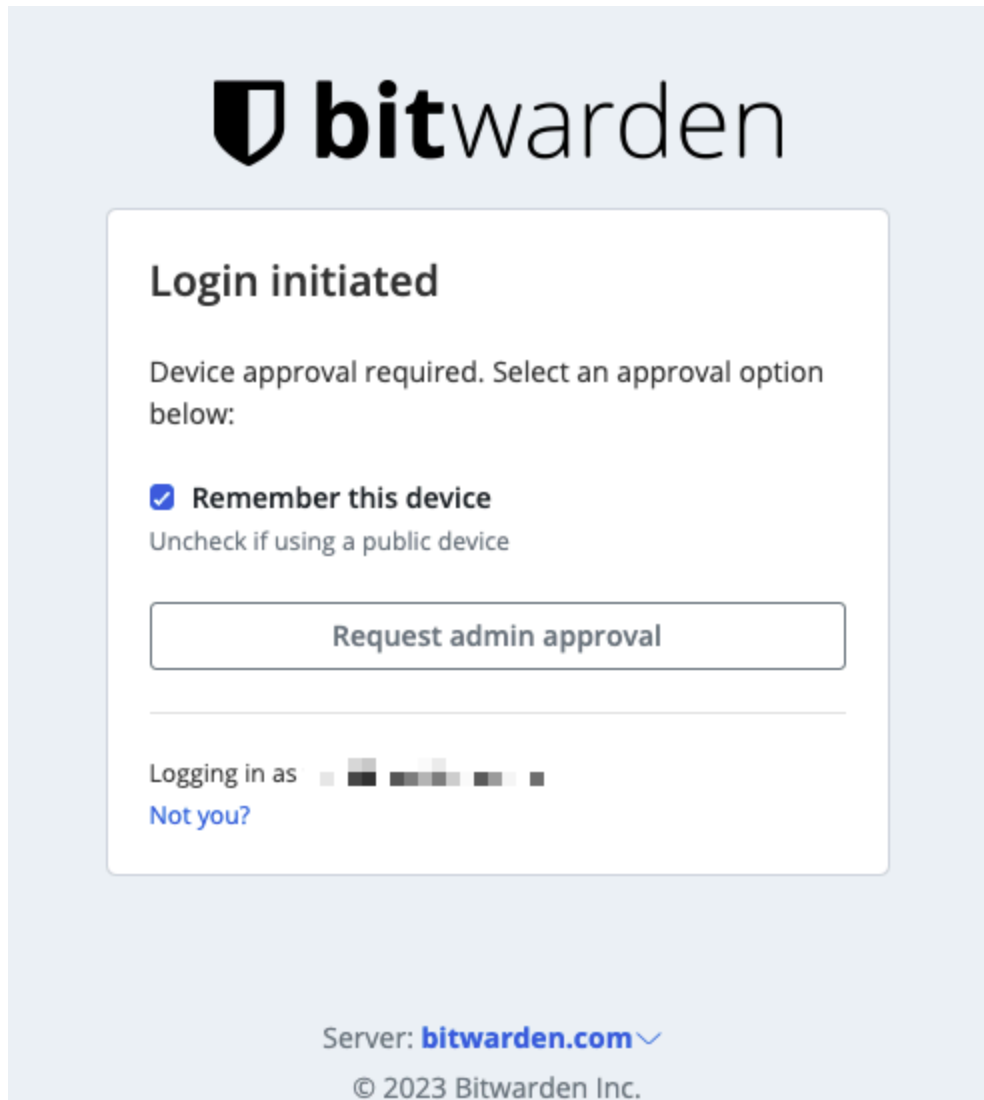
ADMIN CONSOLE > LOGIN WITH SSO >

Approve a Trusted Device

View in the help center:
<https://bitwarden.com/help/approve-a-trusted-device/>

Approve a Trusted Device

When a member of your organization logs into a new device, they'll need to [approve](#), or [trust](#), that device. One method for doing so, done by selecting the **Request admin approval** option, involves sending a device approval request to admins and owners within the organization for approval.



Request admin approval

To approve a request, as an organization admin, or owner, or [custom user](#) with the **Manage account recovery** permission:

1. Log in to the Bitwarden web app and open the Admin Console using the product switcher:

The screenshot displays the Bitwarden web interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, and Settings. The 'All vaults' page is active, showing a 'FILTERS' panel on the left with a search bar and a list of vault categories. A red box highlights the 'Password Manager' option in the sidebar, with a red arrow pointing to the 'All items' section in the filters panel. The main content area shows a table of vaults with columns for selection, name, owner, and actions.

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login sharedusername	My Organiz...	⋮

Product switcher

2. Select **Settings** → **Device approvals** from the navigation.
3. Using the options ⋮ menu, select ✓ **Approve request**.

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

Device approvals

Approve login requests below to allow the requesting member to finish logging in. Unapproved requests expire after 1 week. Verify the member's information before approving.

Member	Device info	Time	
user1@bitwarden.com phrasing-dole-preflight-console-work	Chrome 127.0.0.1	Feb 29, 2024, 10:50:36 AM	<input checked="" type="checkbox"/> Approve request <input type="checkbox"/> Deny request

Approve device request

Note

When a member requests device approval, a fingerprint phrase is displayed on the member's device. Additional verification can be performed by checking that this fingerprint phrase matches the one shown in the member column. This method is optional and **requires synchronous communication** between the requesting member and the administrator.

Bulk approve requests

Multiple device requests may be approved at one time using the top level options menu and selecting **Approve all requests**.

Approve or bulk approve device

Warning

Bulk device approval using the **Approve all requests** option may neglect verification steps that administrators can perform to ensure a request is legitimate, such as checking the user's reported fingerprint phrase.

Bitwarden recommends that significant security controls such as IdP credential standards, IdP MFA, and IdP device registration and trust be reviewed before enabling and using bulk device approval.

When a device request is approved, the requesting user is sent an email informing them they can continue logging in on that device. The user must take action by logging in to the new device within 12 hours, or the approval will expire.

Unapproved requests will expire after 1 week. You can deny a login attempt by instead selecting **Deny request**, or deny all existing requests by selecting the top-most options **Deny all requests**.

Events are logged when:

- A user requests a device approval.
- A device request is approved.
- A device request is denied.