bitwarden | Help Center Article

MITT KONTO > LOGGA IN OCH LÅS UPP >

Add a Trusted Device

View in the help center:
https://bitwarden.com/help/add-a-trusted-device/

Add a Trusted Device

When you become a member of an organization, the device you log in with for the first time will automatically be registered as a trusted device. Once this occurs, all you'll need to do to log in to Bitwarden and decrypt your data is complete your company's established single sign-on flow.

> **Tip**
>
> Devices will be trusted by default when you log in on them. It is highly recommended that you uncheck the **Remember this device** option when logging in on a public or shared device.

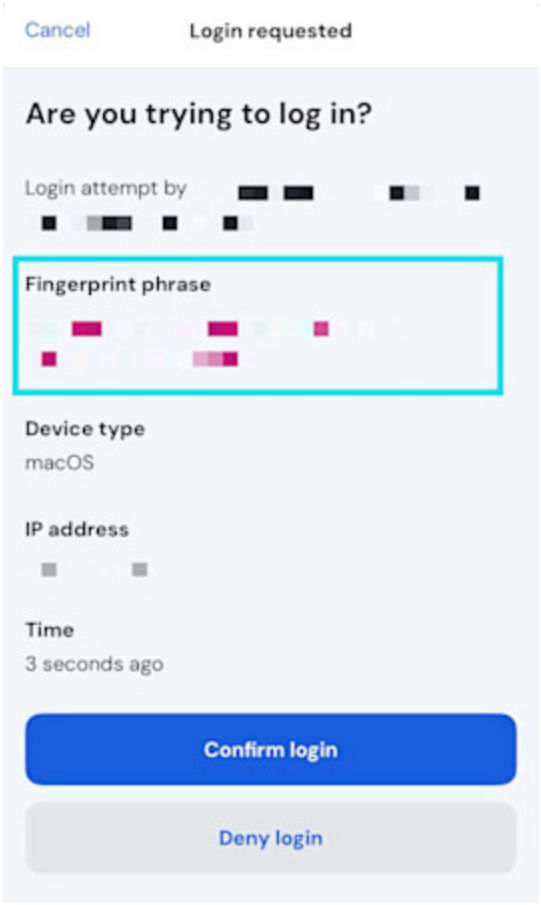
When you log into a new device however, you'll need to approve, or trust, that device. There are a few methods for doing so:

- **Approve from another device**: If you have another Bitwarden Password Manager web app, mobile app or desktop app you're currently logged in to, you can approve the new device from there. On mobile, ensure first that the the Approve login requests option is enabled.

  ### ⇒Mobilapp

  Så här godkänner du en begäran med mobilappen när du har initierat **Logga in med enheten**:

  1. Logga in på mobilappen.
  2. Navigera till **Inställningar → Kontosäkerhet → Väntande inloggningsförfrågningar**.
  3. Leta upp och välj den aktiva enhetsbegäran.
  4. Verifiera fingeravtrycksfrasen och välj **Bekräfta inloggning**.



Mobile device approval

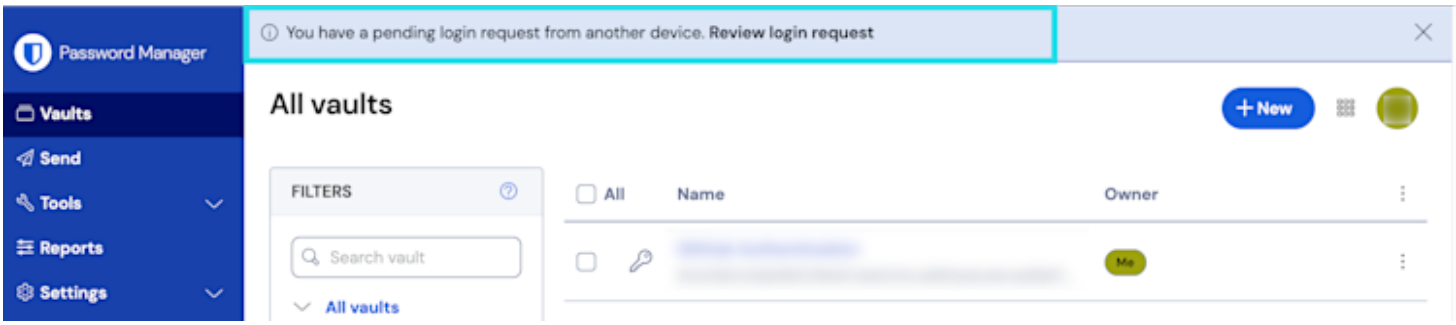
⇒Webbapp

Så här godkänner du en begäran med webbappen när du har initierat **Logga in med enhet**:

1. Logga in på webbappen.

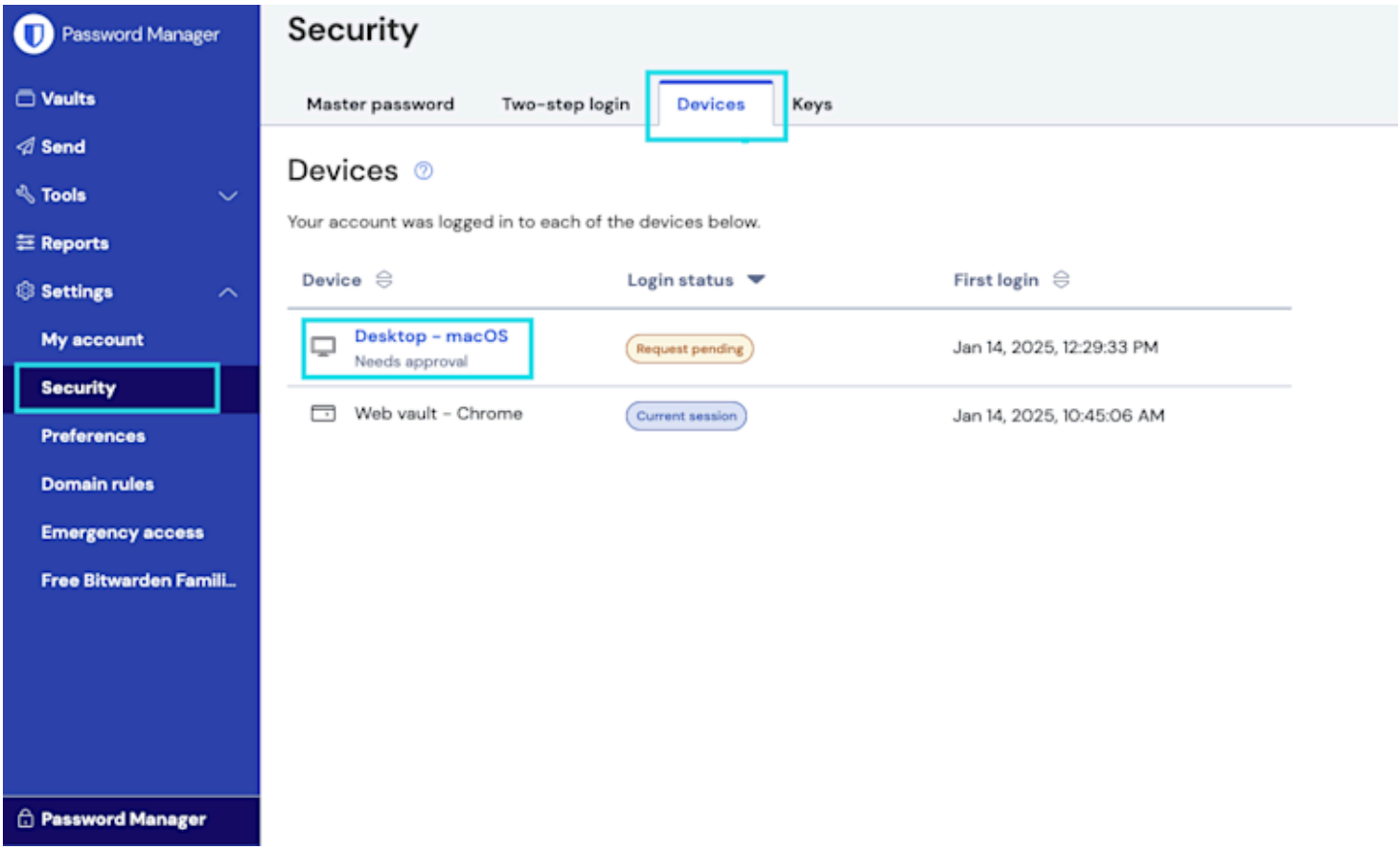
> **Note**
> När du begär godkännande för en inloggning av webbläsartillägget, väntar tillägget i upp till två minuter för godkännande även om du klickar ut eller minimerar tilläggsfönstret för att godkänna begäran med hjälp av webbappen.

2. Navigera till **Inställningar → Säkerhet → Enheter**, eller välj länken på banneraviseringen:



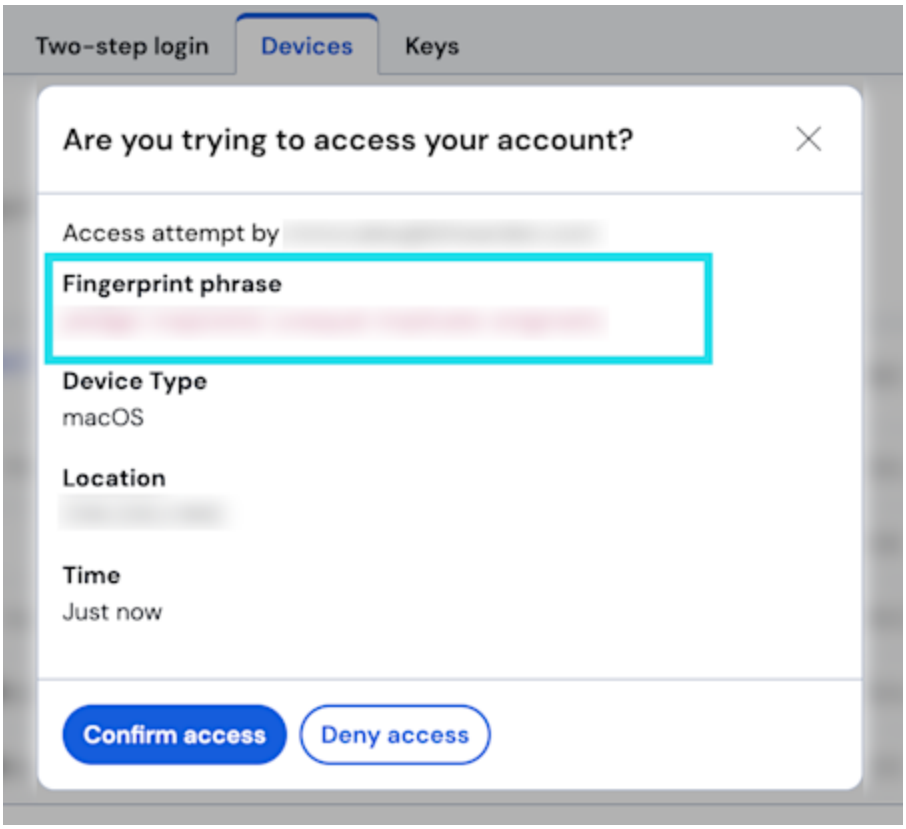
Login with Device Notification

3. Leta upp och välj den aktiva enhetsbegäran:



Web app approve device login

4. Verifiera fingeravtrycksfrasen och välj **Bekräfta inloggning**.

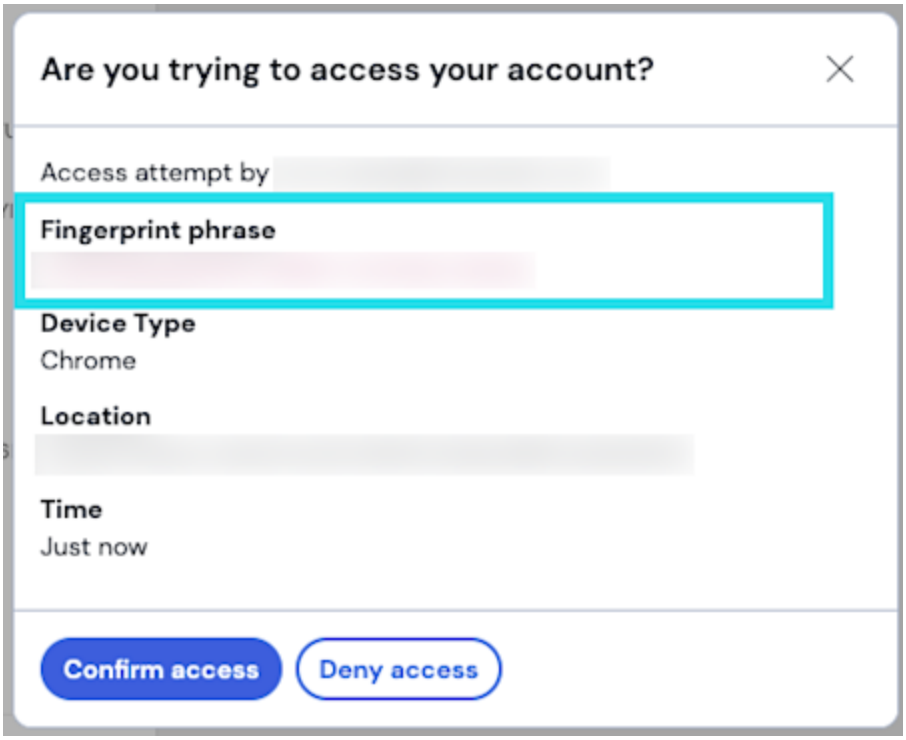


Confirm fingerprint web app

⇒Skrivbordsapp

Så här godkänner du en begäran med skrivbordsappen när du har initierat **Logga in med enheten**:

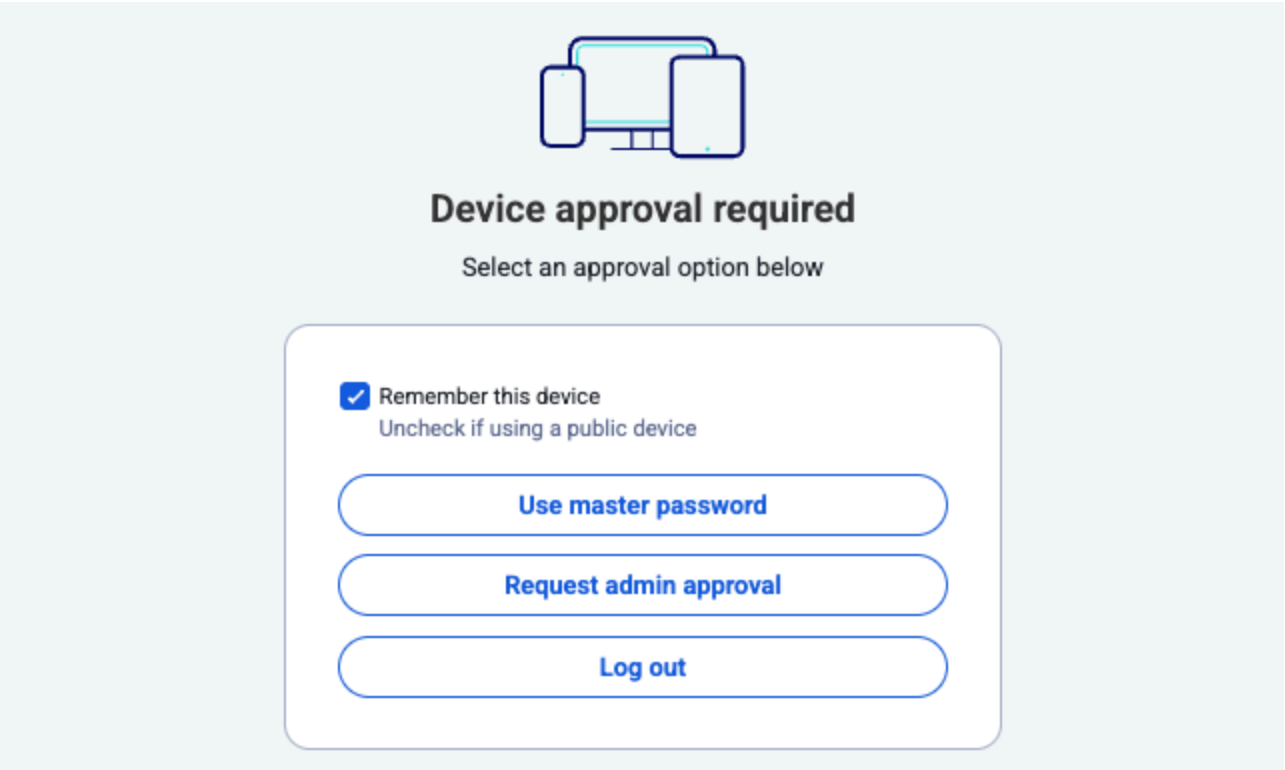
1. Logga in på skrivbordsappen.
2. En autentiseringsbegäran kommer att skickas till din skrivbordsapp:



Approve device desktop

3. Verifiera fingeravtrycksfrasen och välj **Bekräfta inloggning**.

- **Use master password**: If you are an admin or owner, or joined your organization before SSO with trusted devices was implemented, and therefore still have a master password associated with your account, you can enter it to approve the device.



Request admin approval

- **Request admin approval**: You can send a device approval request to admins and owners within your organization for approval. You **must** be enrolled in account recovery to request admin approval, though you may have been automatically enrolled when you joined the organization. In many cases, this will be the only option available to you (learn more).

> **Note**
>
> If you use this option, you'll get an email informing you to continue logging in on the new device when you're approved. You must take action by logging in to the new device within 12 hours, or the approval will expire.

Once the new device becomes trusted, all you'll need to do to log in to Bitwarden and decrypt your vault data is complete your company's established single sign-on flow.

Adding your first trusted device

The initial client used to access Bitwarden for users who were invited with Just in Time (JIT) provisioning using login with SSO will become their first trusted device. If the initial client accessed is the Bitwarden desktop or mobile app, this device can be used to approve additional devices.

For the desktop or mobile app to become the first trusted device, the user should not use the organization invite link. Instead, open the mobile or desktop app and select the **Enterprise single sign-on** option to begin the JIT process.

Remove a trusted device

Devices will remain trusted until:

- The application or extension is uninstalled.
- The web browser's memory is cleared (web app only).
- The user's encryption key is rotated.

> **Note**
>
> Only users who have a master password can rotate their account encryption key. Learn more.

Troubleshooting

If you're having trouble establishing device trust:

- On Chrome, check that **Allow sites to save data on your device** is turned on (**Settings → Privacy and security → Site settings → Additional content settings → On-device site data → Allow sites to save data on your device**).