ADMIN CONSOLE \rightarrow LOGGA IN MED SSO \rightarrow

Approve a Trusted Device

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

D bit warden

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.

Device approval required	
Select an approval option below	
Remember this device Uncheck if using a public device Use master password	
Request admin approval	
Log out	\supset

Request admin approval

As an admin, you'll receive an email any time an organization member submits a device approval request. 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:

D bitwarden

Password Manager	All vaults			New 🗸	BW
🗇 Vaults			Nama	Owner	
🖉 Send			Name	Owner	:
\ll Tools \sim	Q Search vau	AZEV	Company Credit Card Visa, *4242	My Organiz	:
₩ Reports	✓ All vaults		Personal Login		
🕸 Settings 🛛 🗸 🗸	My Organiz	0 9	myusername	Me	1
	 Teams Org : + New organization 		Secure Note	Ме	:
	 ✓ All items ☆ Favorites ③ Login □ Card □ Identity □ Secure note 		Shared Login sharedusername	My Organiz	÷
C Password Manager	 ✓ Folders ➡ No folder 				
Secrets Manager					
Admin Console	Default colle				
Administre	🔟 Trash				
🛱 Toggle Width					

Product switcher

2. Select **Settings** \rightarrow **Device approvals** from the navigation.

3. Using the options \vdots menu, select \checkmark Approve request.

D bit warden

Säker och pålitlig lösenordshanterare med öppen källkod för företag

D bit warden		Device approvals			
🖉 My Organization	\sim	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.			
Collections		Member	Device info	Time	:
A Members			Channe	5-6-20-2024 40-50-26 AM	
뿅 Groups		user/@bluwarden.com phrasing-dole-preflight-console-work	127.0.0.1	Feb 29, 2024, 10:50:36 AM	· · · · · · · · · · · · · · · · · · ·
\equiv Reporting	\sim				✓ Approve request
Billing	\sim				> Deny request
Settings	\sim				
Organization info					
Policies					
Two-step login					
Import data					
Export vault					
Domain verification	n				
Single sign-on					
Device approvals					
SCIM provisioning	_				
		Approve device re	quest		

(i) 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 \checkmark Approve all requests.

D bit warden

Säker och pålitlig lösenordshanterare med öppen källkod för företag

D bit warden	Device approvals				
${\ensuremath{\it B}}$ My Organization $\ {\ensuremath{\sim}}$	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.				
Collections	Member	Device info	Time	:	
A Members	@bitwarden.com	macOS	lun 20. 2024. 3:56:35 PM	✓ Approve all requests	
器 Groups	oversleep-respect-remember-knoll-granddad		jan 20, 202 i, ciccico i in	× Deny all requests	
\equiv Reporting \lor	@bitwarden.com	macOS	Jun 20, 2024, 3:58:03 PM	:	
Settings	numerous-knapsack-lunar-thumb-unaudited			•	
Policies	@bitwarden.com	macOS	Jun 20, 2024, 3:59:46 PM	:	
Import data	over cast-buctisin-parsinip-subtet-mait				
Export vault					
Domain verification					
Single sign-on					
Device approvals					
SCIM provisioning					
🖯 Password Manager					
🗐 Admin Console					
More from Bitwarden					
Secrets Manager Secure your infrastructure					

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 \times **Deny request**, or deny all existing requests by selecting the top-most options : menu and selecting \times **Deny all requests**.

Events are logged when:

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