

Howwe IT requirements

Version 2026-10-22 · Last updated 22 October 2026

This page is for the IT department of an organisation that starts using Howwe. It lists what needs to be open in your network and email, and how single sign-on is set up. Howwe runs in the browser, so nothing needs to be installed.

1. Domains to allow

Howwe uses the domains below. All traffic is HTTPS on port 443. The simplest setup is to allow `*.howwe.io` , which also covers domains we add later.

Domain	Used for
<code>app.howwe.io</code>	The Howwe application
<code>graphql.howwe.io</code>	Reading and saving data in Howwe
<code>ai-api.howwe.io</code>	Howwe's AI features, dictation and document upload
<code>login.howwe.io</code>	Sign-in and single sign-on
<code>terms.howwe.io</code>	The terms notice shown at first sign-in
<code>analytics.howwe.io</code>	Product analytics
<code>help.howwe.io</code>	Help center
<code>*.intercom.io</code> , <code>*.intercomcdn.com</code>	Support chat and help in the app

If a domain is blocked, the part of Howwe that uses it stops working. For example, blocking `ai-api.howwe.io` turns off the AI features, and blocking the Intercom domains turns off the support chat.

2. Single sign-on

Users can sign in with your organisation's own identity provider, such as Microsoft Entra ID, Google Workspace or another SAML 2.0 provider. Single sign-on runs through `login.howwe.io` .

1. Contact us at help@howwe.io and tell us which identity provider you use.
2. We send you the values your identity provider needs, such as the entity ID, the reply (ACS) URL and the signing certificate. You send us your provider's metadata.
3. You add Howwe as an application in your identity provider and assign the users or groups that should have access.
4. We test the sign-in together with a test user before it is turned on for everyone.
5. Single sign-on can be turned on for the whole organisation or for some groups first, so that you can roll it out step by step.

Who has access, and with which roles, is decided in Howwe by your organisation's administrators.

3. Email

Howwe sends account emails, such as invitations and notifications, from addresses at howwe.io. Replies from our support come through Intercom. Our emails are signed with SPF and DKIM.

Make sure your email filter accepts email from howwe.io and from Intercom, so that invitations and notifications reach your users.

4. AI assistants (MCP)

Your users can connect AI assistants, such as Microsoft Copilot, Claude, ChatGPT and Gemini, to Howwe through our MCP server. The calls to Howwe come from the AI provider's servers, not from your network, so nothing needs to be opened for them.

Your organisation decides whether AI assistants may be used and which ones. An administrator can ask us at contact@howwe.io to turn off access through AI assistants for the whole organisation, and we do so within two business days. Read more at howwe.io/mcp.

5. Security

All traffic to Howwe is encrypted with TLS 1.2 or higher. Customer data is stored in the EU. Read more in our [security overview](#) and our [list of sub-processors](#).

6. Contact

Questions about setup, single sign-on or network requirements: help@howwe.io.