CyberArmor.AI Partner Portal — User Guide

Last verified: 2026-11-21, against the Partner Console's code on `main` at commit 3310fef64; the protection level on the customer card and in the panel, and the region link on the sign-in page, were added then. The screenshots predate them.

Earlier: 2026-10-29, every section was checked against the Partner Console's code (`msp-console/`) on `main` at commit 1f4497db6. The screenshots were taken on 2026-10-24 on the live Singapore Partner Console (am-msp.cyberarmor.ai); customer organizations shown in them are CyberArmor.AI demo organizations, and cards for other partners' customers were hidden from the pictures.

The **Partner Portal** (also called the **Partner Console**) is for resellers, distributors and managed security service providers (MSPs/MSSPs). It lists every customer organization you manage, so you can invite each customer's administrator, set how many devices each customer may enroll, and open any customer's portal to help them.

Which address do I use?

Region	Partner Portal address
Asia and Middle East (including Pakistan)	**https://am-msp.cyberarmor.ai**
United States	**https://msp.cyberarmor.ai**

When you open a customer from the Partner Portal, you work inside the normal Customer Portal. Everything in the **Customer Portal User Guide** applies there.

Prefer to watch? The training video *Partner Console walkthrough* (6 minutes) shows every step of this guide. It is on the documentation site at **https://docs.cyberarmor.ai/training/partner-console/** and on **https://cyberarmor.ai/training**.

Contents

1. Sign in
2. Your customers at a glance
3. Invite a customer's administrator and set their device limit
4. Work inside a customer's portal
5. Protect your account and manage your team (Security)

---

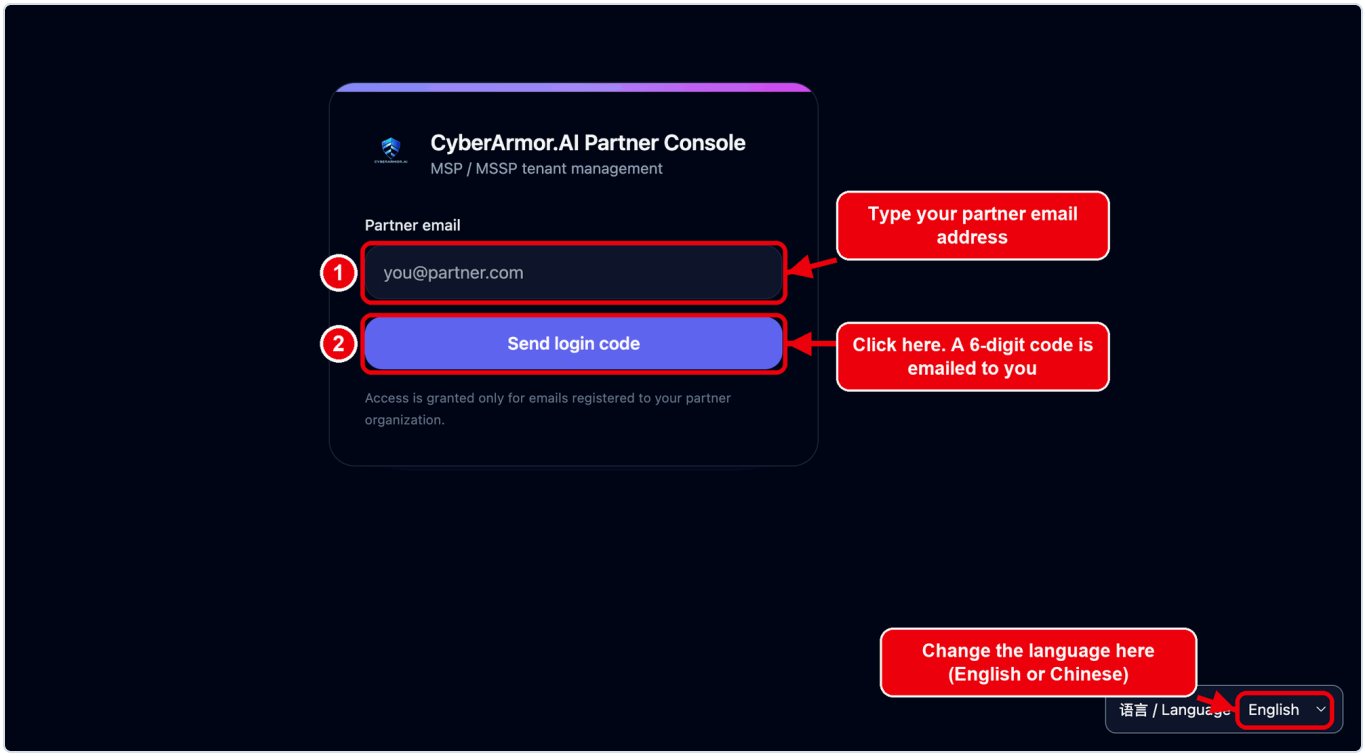
1. Sign in

Step 1. Open **https://am-msp.cyberarmor.ai**.

Step 2. Type your partner email address (1) and click **Send login code** (2). Type the 6-digit code from the email and click **Verify and enter**. There is no password to remember. (**Resend code** sends another; **Use a different email** starts again.) If you opened the wrong region's console, click **Not your region? Choose again** at the bottom of the page.

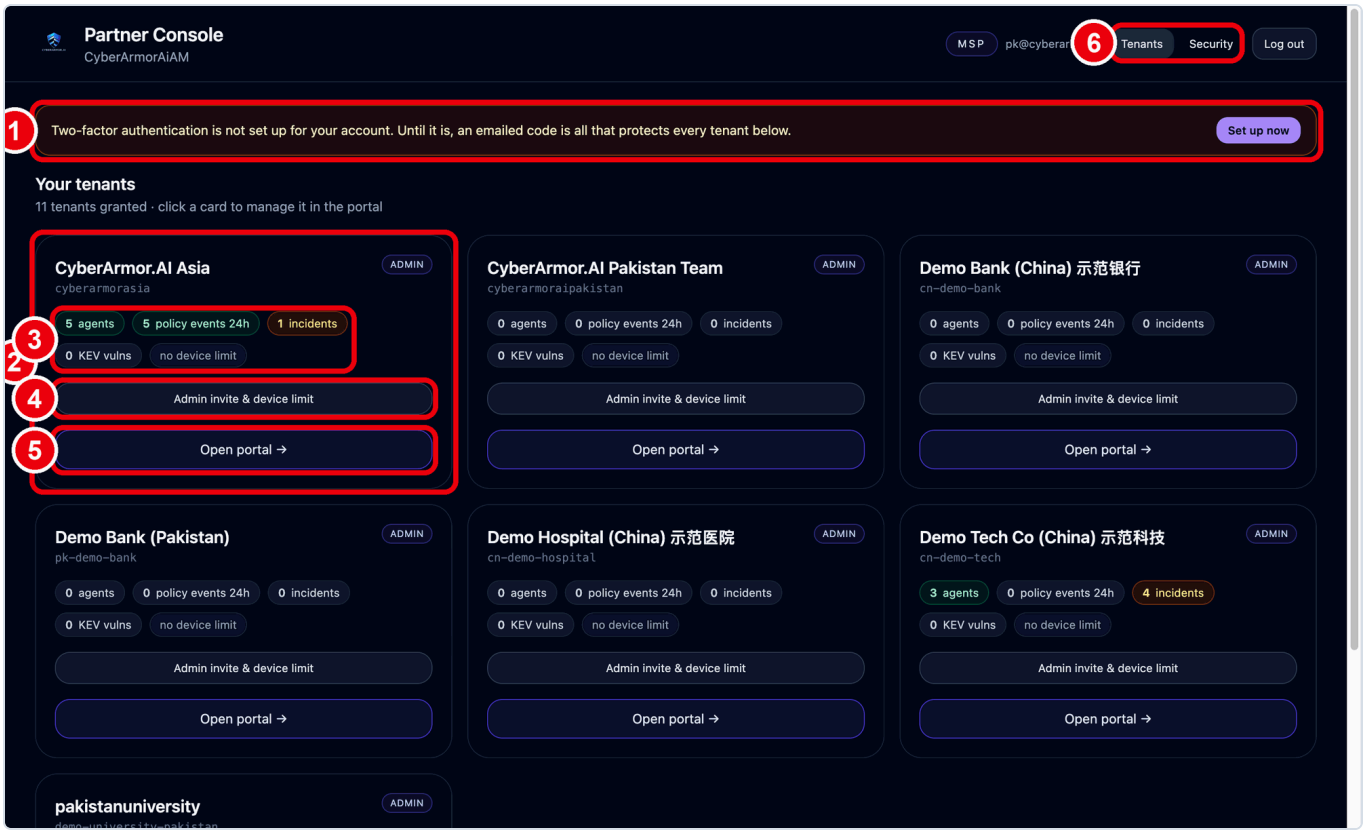
Step 3 (only for some people). If your address belongs to more than one partner organization, the console asks which one; each has its own sign-in and its own authenticator. Pick it and click **Continue**. **Start over** returns to the email step.

Step 4 (once you have set up an authenticator app). Type the **Authenticator code** from your app, or one of your backup codes, and click **Verify**.



2. Your customers at a glance

After signing in you see **Your tenants**: one card for each customer organization granted to your partner organization.

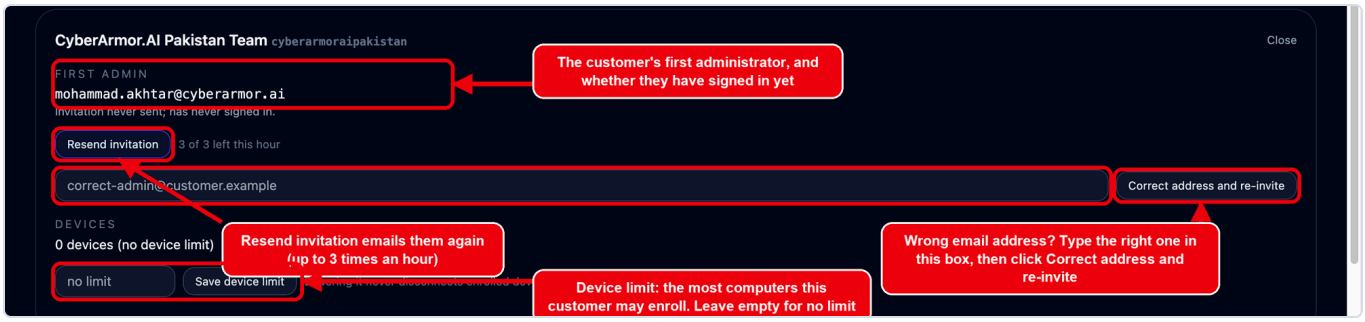


#	What it is	What it tells you or does
1	**Two-factor reminder**	"Two-factor authentication is not set up for your account", shown until you set up an authenticator app. **Set up now** takes you to the Security page (section 5). Do this first: your account can open every customer you manage. If your partner organization requires two-factor sign-in, the console opens on Security until you have set it up.
2	**A customer card**	The customer's name and organization ID, and your role for it (for example ADMIN). If CyberArmor.AI has suspended the organization, the card says so: partner access is paused, and your grant is kept.
3	**Health at a glance**	The customer's **protection level** first (green when it holds; amber when settings have been changed away from it, with "N of M changed"; grey when no level has been chosen). Then agents, policy events in the last 24 hours, incidents, known-exploited vulnerabilities (KEV vulns) on their devices, and devices used against the device limit. Green means activity, amber means incidents to look at, and red means known-exploited vulnerabilities or a customer at its device limit. A count the server could not take reads **not checked**, never zero.
4	**Admin invite & device limit**	Invite the customer's administrator and set their device limit (section 3). Shown to partner admins, on customers where your role is admin.
5	**Open portal →**	Opens this customer's portal (section 4).
6	**Tenants / Security / Log out**	Switch between your customer list and your account security, or sign out. **Switch partner** appears if your address belongs to more than one partner organization.

---

3. Invite a customer's administrator and set their device limit

Step 1. On the customer's card, click **Admin invite & device limit**. A panel opens at the top of the page.



Protection level. At the top of the panel you see the level the customer is on and whether its settings still match it; any setting that has been changed is listed. To put the customer on a level, choose it from the list and click **Apply level**. This is recorded in the customer's audit log under your partner organization's name. Only a partner admin with admin access to the customer can change it.

Step 2. Check the **First admin**. The panel shows the customer administrator's email, what happened to the invitation (for example "accepted by the mail server (not proof of delivery)" or "NOT SENT"), and whether they have signed in yet. If the invitation was never received:

- click **Resend invitation** to email it again. The panel says how many resends are left this hour (3 an hour by default); or
- if the address is wrong and the administrator has never signed in, type the correct one in the box and click **Correct address and re-invite**. If they have already signed in, the button reads **Request change (new address confirms)**: the change waits until the new address confirms it.

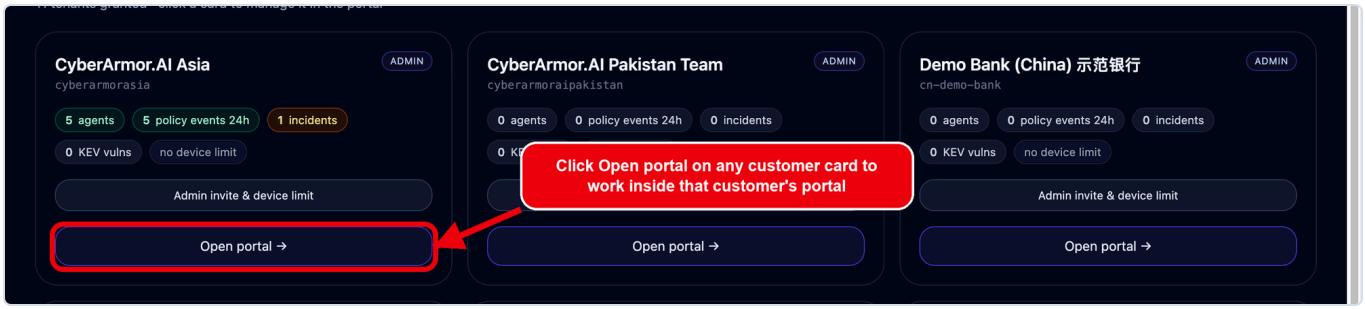
The administrator signs in to the Customer Portal with an emailed code, then adds their own colleagues from **Users**.

Step 3. Set the **device limit**: the most computers and browsers this customer may enroll. Type a number and click **Save device limit**. Leave it empty for no limit. Lowering the limit never disconnects devices that are already enrolled; it only stops new ones. The panel also shows how many devices are counted now, and how many new devices were refused at the limit in the last 7 days. If CyberArmor.AI or the customer's plan set the limit, the panel says so and you cannot change it here.

Click **Close** when you are done.

4. Work inside a customer's portal

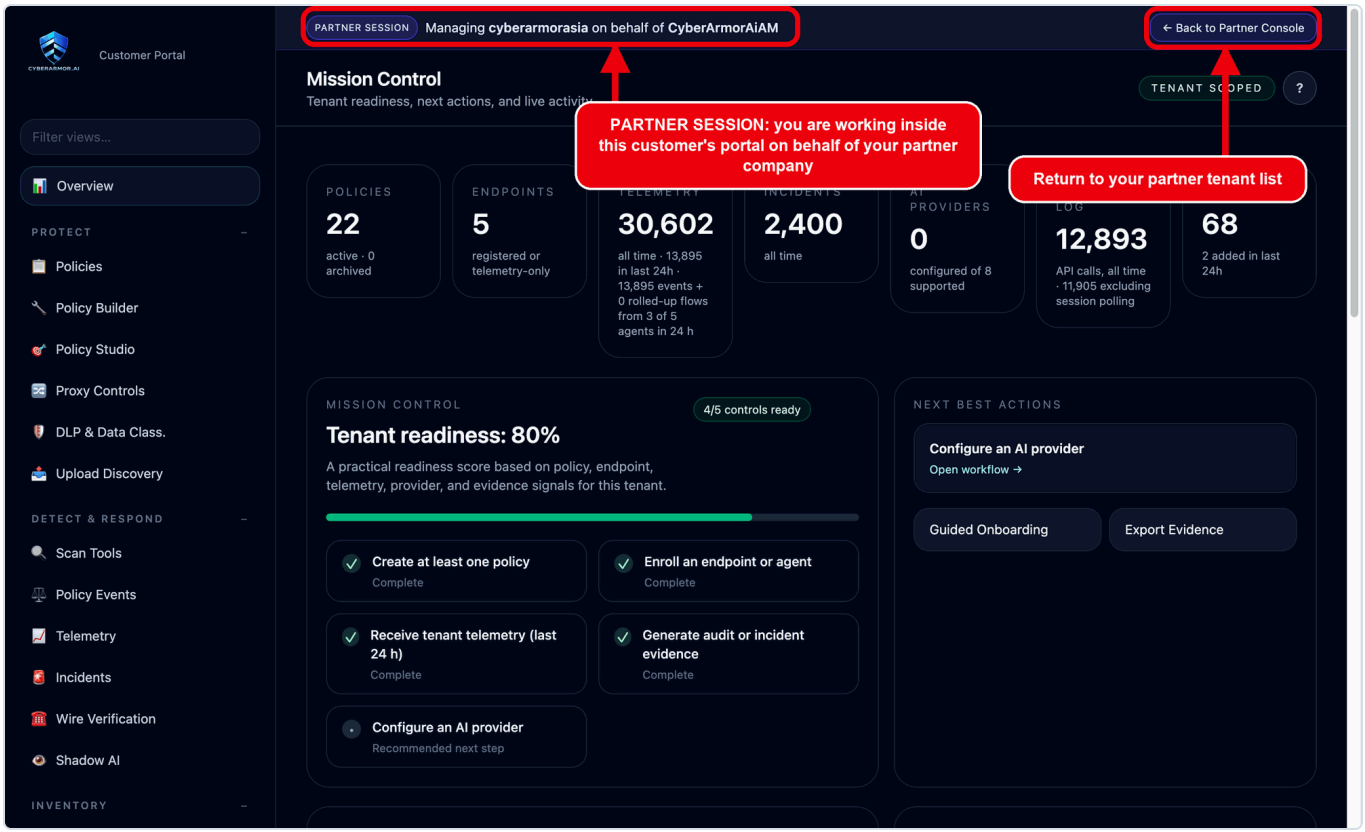
Step 1. On the customer's card, click **Open portal →**.



Step 2. The customer's portal opens, in the language you were using in the console. A **Partner session** banner at the top shows which customer you are managing and on behalf of which partner. You act under your own partner email address, not as the customer.

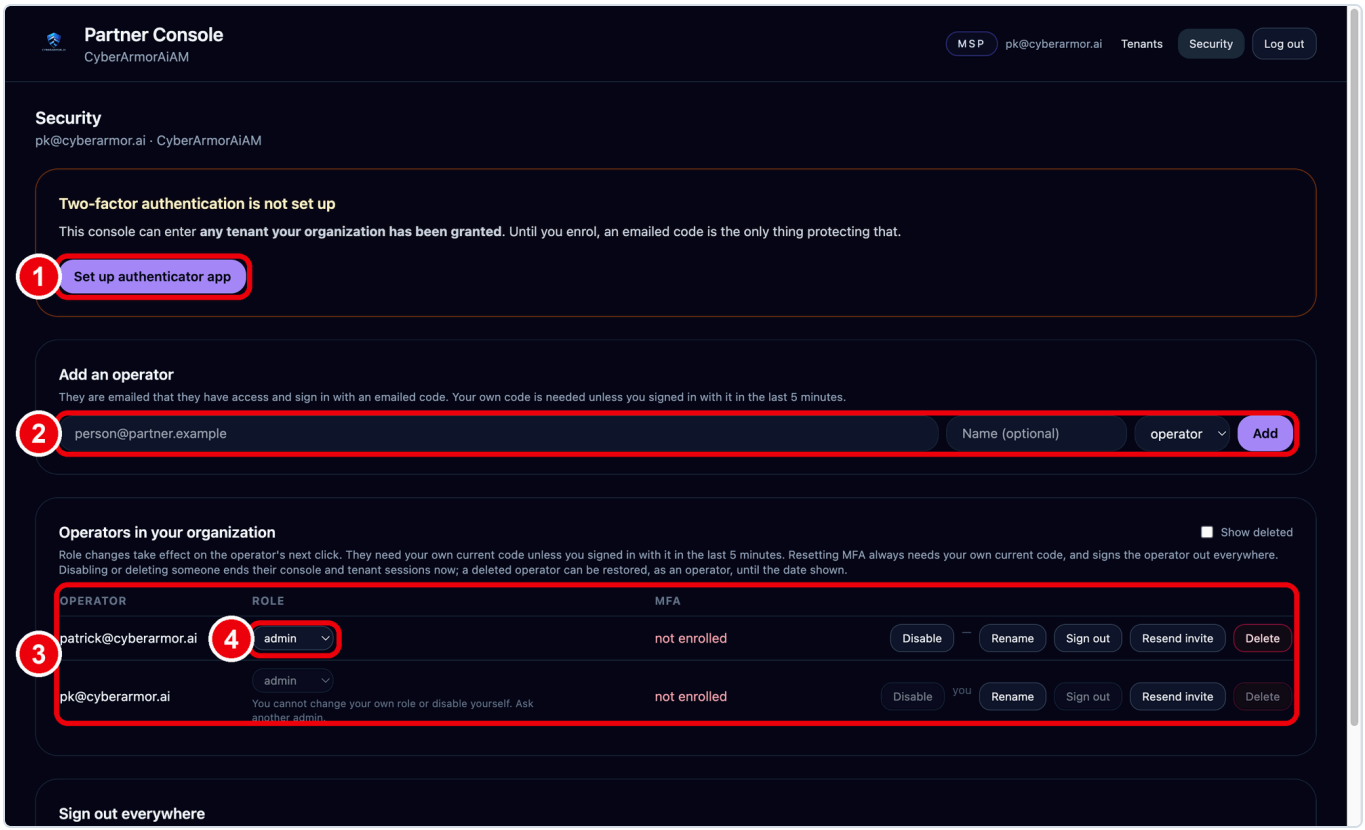
From here, follow the **Customer Portal User Guide**: download installers and issue tokens, apply compliance policy packs, create policies, check devices and incidents.

Click ← **Back to Partner Console** (top right) to return to your customer list.



5. Protect your account and manage your team (Security)

Click **Security** at the top of the page.



1. **Set up authenticator app.** Turn on two-factor sign-in with an app such as Microsoft Authenticator or Google Authenticator: scan the QR code, type the code it shows, and save the backup codes, which are shown once. Your account can enter every customer you manage, so this is strongly recommended. Once it is on, the card offers **Regenerate backup codes**, **Move to a new device** and **Turn off** (not offered if your partner organization requires two-factor sign-in).
2. **Add an operator** (partner admins only). Give a colleague access to the Partner Portal: type their email, an optional name, choose **operator** or **admin**, and click **Add**. They receive an email and sign in with an emailed code. Your own authenticator code is needed unless you signed in with it in the last 5 minutes.
3. **Operators in your organization.** Everyone on your team, their role, and whether they have set up two-factor sign-in (**enrolled**, **in progress** or **not enrolled**). The buttons on each row: **Disable** (or **Enable**), **Reset MFA**, **Rename**, **Sign out** (ends their console and customer-portal sessions), **Resend invite** and **Delete**. Disabling or deleting someone ends their sessions at once. Tick **Show deleted** to see deleted operators; a deleted operator can be restored, as an operator, until the date shown, and API keys they created in a customer organization stay revoked.
4. **Role.** Change someone between **operator** and **admin**; the change takes effect on their next click and needs your own current code unless you signed in with it in the last 5 minutes. You cannot change your own role or disable yourself, and the only active admin cannot be demoted or disabled: make another operator an admin first.

At the bottom of the page, **Sign out everywhere** ends all your sessions, including any customer portals you opened from the Partner Portal.