CyberArmor.AI 合作伙伴门户 — 用户指南

最后核验时间：2026-10-29。全文已对照 `main` 分支提交 1f4497db6 的合作伙伴控制台代码（`msp-console/`）逐节核对。截图拍摄于 2026-10-24，环境为新加坡生产环境合作伙伴控制台（am-msp.cyberarmor.ai）；截图中显示的客户组织均为 CyberArmor.AI 演示组织，其他合作伙伴的客户卡片已从图中隐去。

合作伙伴门户（也称为**合作伙伴控制台**）面向经销商、分销商以及托管安全服务提供商（MSP/MSSP）。该门户列出您所管理的每一个客户组织，您可以在此邀请各客户的管理员、设定各客户可注册的设备数量上限，并打开任意客户的门户为其提供支持。

我应使用哪个访问地址？

区域	合作伙伴门户地址
亚洲及中东地区（含巴基斯坦）	**https://am-msp.cyberarmor.ai**
美国	**https://msp.cyberarmor.ai**

当您从合作伙伴门户打开某个客户时，您实际进入的是常规的客户门户。**客户门户用户指南**中的全部内容在此同样适用。

想看视频？ 培训视频《合作伙伴控制台演练》（约 6 分钟）演示了本指南的每一个步骤。视频位于文档站点 **https://docs.cyberarmor.ai/zh/training/partner-console/** 和 **https://cyberarmor.ai/training**。视频目前为英语（巴基斯坦）版。

目录

1. 登录
2. 客户概览
3. 邀请客户管理员并设定设备数量上限
4. 在客户门户内开展工作
5. 保护您的账户并管理团队（安全）

---

1. 登录

步骤 1. 打开 **https://am-msp.cyberarmor.ai**。

步骤 2. 输入您的合作伙伴邮箱地址（1），然后点击**发送登录验证码**（2）。输入邮件中收到的 6 位验证码，再点击**验证并进入**。无需记忆任何密码。（**重新发送验证码**会再发一封；**使用其他邮箱**可重新开始。）

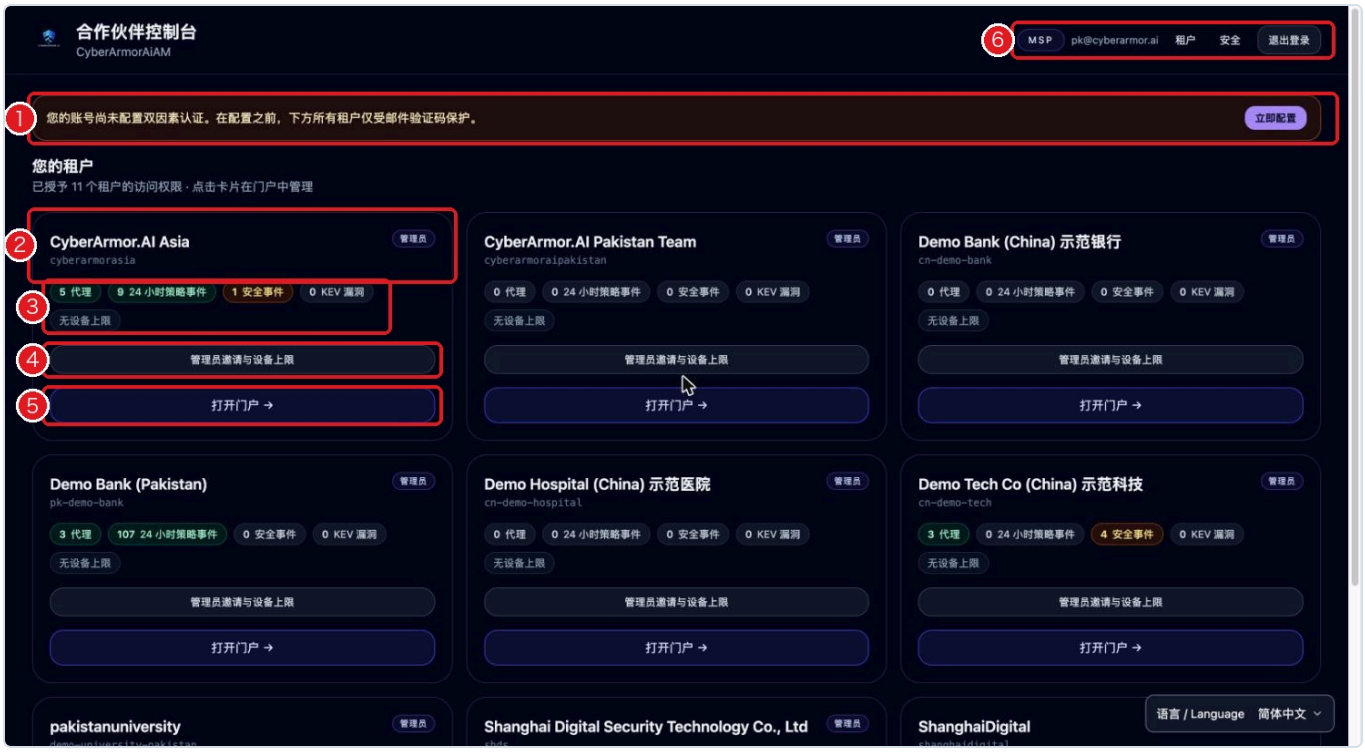
步骤 3（仅部分用户需要）。 如果您的邮箱地址隶属于多个合作伙伴组织，控制台会询问您要进入哪一个；每个组织都有各自的登录和各自的身份验证器。选择后点击**继续**。

步骤 4（已设置身份验证器应用时）。 输入应用中显示的**身份验证器验证码**或一个备用码，然后点击**验证**。



2. 客户概览

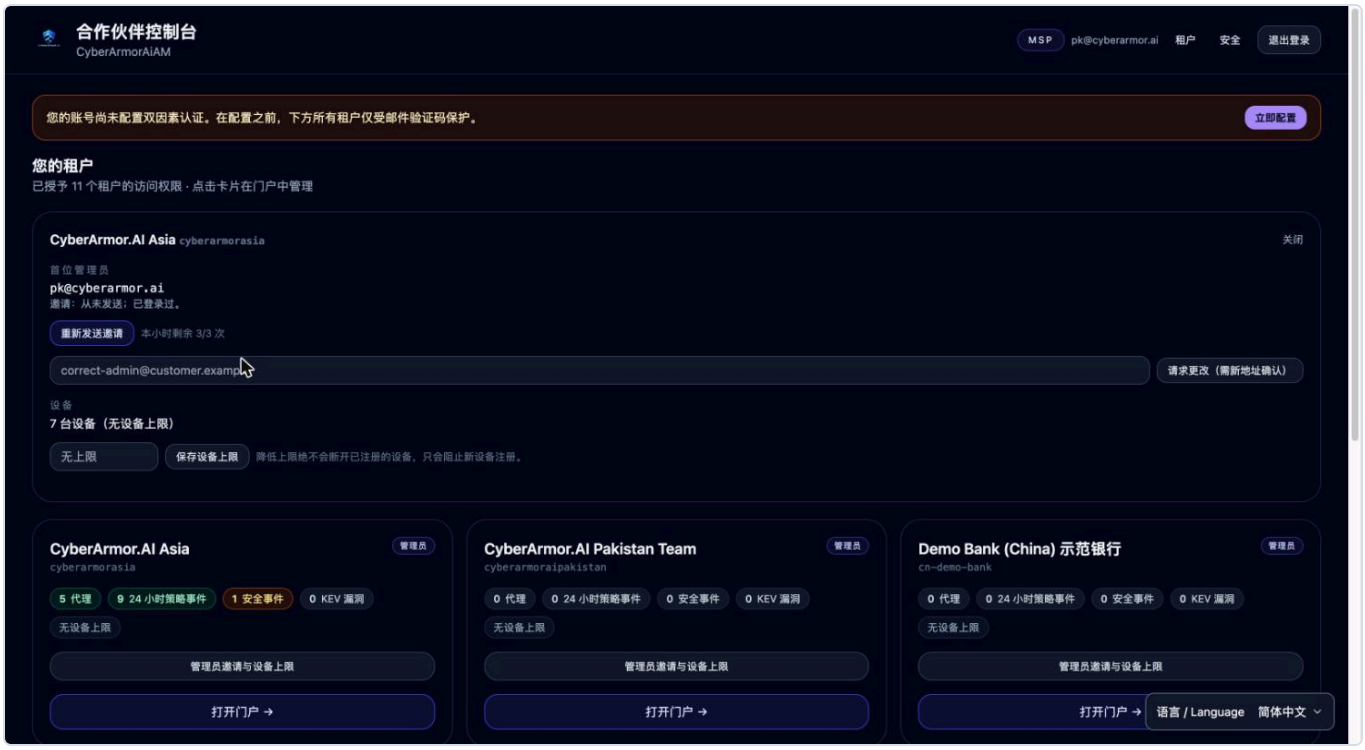
登录后，您会看到**您的租户**列表：已授权给贵合作伙伴组织的每一个客户组织对应一张卡片。



序号	名称	含义与用途
1	**双因素认证提醒**	提示您的账户尚未设置双因素认证，在您完成身份验证器应用设置之前会一直显示。点击**立即配置**可前往安全页面（第 5 节）。请优先完成此项：您的账户可以进入您所管理的每一个客户环境。如果贵合作伙伴组织要求双因素登录，在您完成设置之前，控制台会一直停留在安全页面。
2	**客户卡片**	显示客户名称、组织 ID，以及您在该组织中的角色（例如 ADMIN）。如果 CyberArmor.AI 已暂停该组织，卡片会如实说明：合作伙伴访问暂停，但您的授权会保留。
3	**健康状况速览**	代理程序数量、最近 24 小时的策略事件数、安全事件数、设备上已知可利用漏洞（KEV vulns）的数量，以及已用设备数与设备上限的对比。绿色表示有活动，琥珀色表示有需要查看的安全事件，红色表示存在已知可利用漏洞或客户已达到设备上限。服务器未能统计的数字显示为**未检查**，绝不显示为零。
4	**管理员邀请与设备上限**	邀请该客户的管理员并设定其设备数量上限（第 3 节）。仅向合作伙伴管理员显示，且仅出现在您角色为管理员的客户卡片上。
5	**打开门户 →**	打开该客户的门户（第 4 节）。
6	**租户 / 安全 / 退出登录**	在客户列表与账户安全设置之间切换，或退出登录。如果您的邮箱地址隶属于多个合作伙伴组织，还会显示**切换合作伙伴**。

3. 邀请客户管理员并设定设备数量上限

步骤 1. 在客户卡片上点击**管理员邀请与设备上限**。页面顶部会展开一个面板。



步骤 2. 检查**首位管理员**信息。该面板会显示客户管理员的邮箱地址、邀请邮件的实际状态（例如"已被邮件服务器接受（不代表已送达）"或"未发送"），以及其是否已完成登录。如果对方始终未收到邀请：

- 点击**重新发送邀请**以再次发送邮件。面板会显示本小时内还可重发几次（默认每小时 3 次）；或

- 如果邮箱地址有误且该管理员从未登录过，请在输入框中填写正确地址，然后点击**更正地址并重新邀请**。如果对方已经登录过，按钮会显示为**请求更改（需新地址确认）**：更改要等到新地址确认后才生效。

该管理员将使用邮件验证码登录客户门户，随后可在**用户**页面中自行添加其同事。

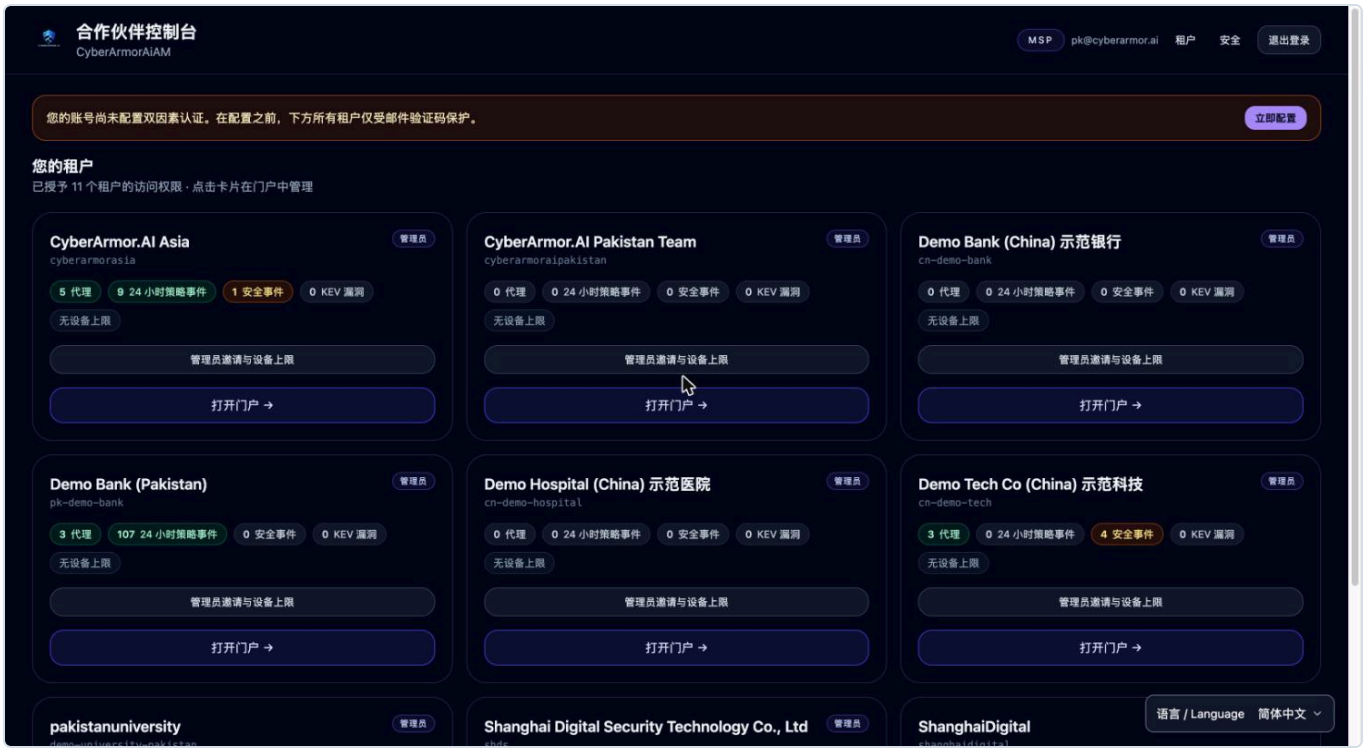
步骤 3. 设定**设备数量上限**：即该客户最多可注册的计算机与浏览器数量。输入数字后点击**保存设备上限**。留空则表示不限制数量。调低上限不会断开已注册设备的连接，仅会阻止新设备注册。面板还会显示当前统计到的设备数量，以及最近 7 天内因达到上限而被拒绝的新设备数量。如果该上限由 CyberArmor.AI 或客户的套餐设定，面板会说明这一点，且您无法在此更改。

完成后点击**关闭**。

---

4. 在客户门户内开展工作

步骤 1. 在客户卡片上点击**打开门户 →**。



步骤 2. 该客户的门户随即打开，并沿用您在控制台中使用的语言。页面顶部的**合作伙伴会话**横幅会显示您当前正在管理哪一位客户，以及您代表哪一家合作伙伴。您是以自己的合作伙伴邮箱身份进行操作，而非以客户身份。

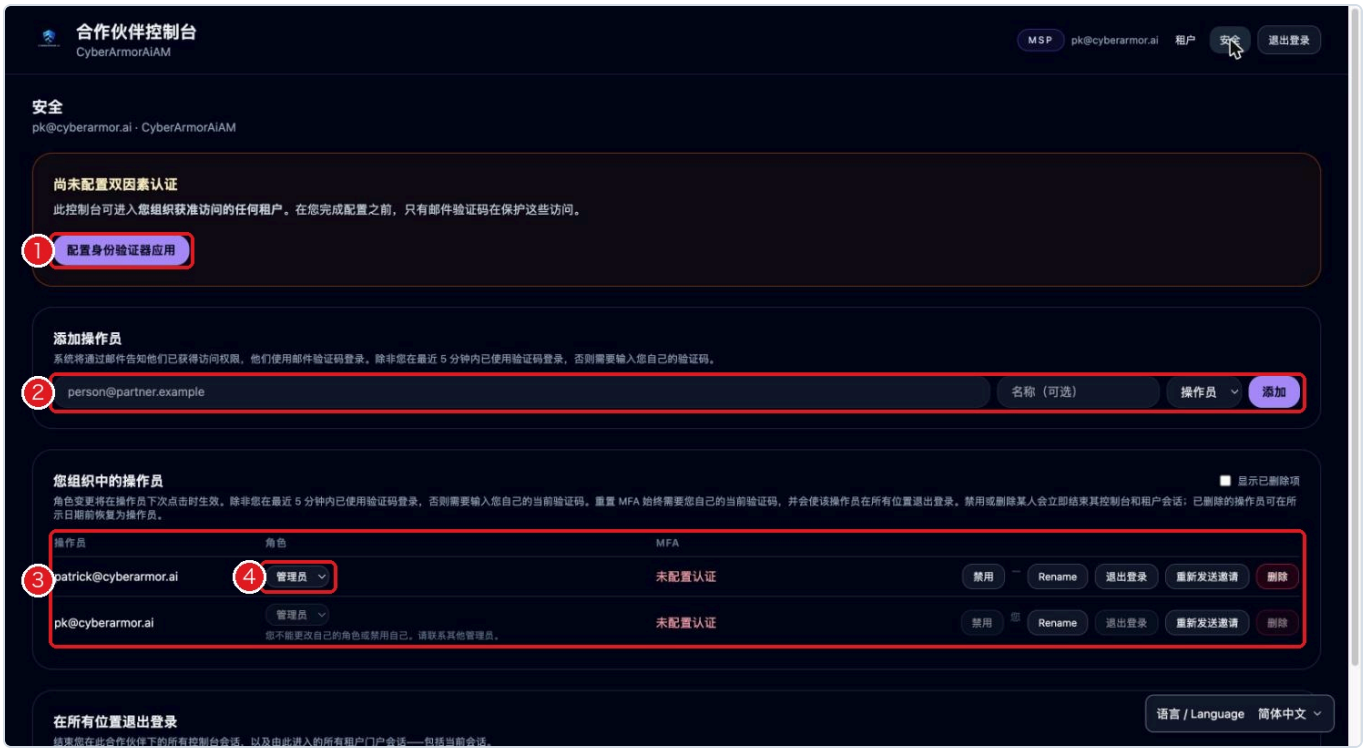
从此处开始，请遵循**客户门户用户指南**进行操作：下载安装程序并签发令牌、应用合规策略包、创建策略、查看设备与安全事件。

点击右上角的 ← **返回合作伙伴控制台** 即可回到您的客户列表。



5. 保护您的账户并管理团队（安全）

点击页面顶部的**安全**。



1. **配置身份验证器应用。** 使用 Microsoft Authenticator 或 Google Authenticator 等应用启用双因素登录：扫描二维码，输入应用显示的验证码，并保存仅显示一次的备用码。您的账户能够进入您所管理的每一个客户环境，因此强烈建议启用此功能。启用后，卡片会提供**重新生成备用码**、**迁移到新设备**和**关闭**（如果贵合作伙伴组织要求双因素登录，则不提供关闭）。
2. **添加操作员**（仅限合作伙伴管理员）。为同事开通合作伙伴门户访问权限：输入其邮箱地址、可选的姓名，选择**操作员**或**管理员**，然后点击**添加**。对方将收到邮件，并使用邮件验证码登录。除非您在最近 5 分钟内使用身份验证器验证码登录过，否则需要输入您本人的验证码。
3. **您组织中的操作员。** 显示团队中的所有成员、其角色，以及双因素登录的状态（**已配置认证**、**进行中**或**未配置认证**）。每一行的操作按钮包括：**禁用**（或**启用**）、**重置 MFA**、**重命名**、**退出登录**（结束其控制台与客户门户会话）、**重新发送邀请**和**删除**。禁用或删除某人会立即结束其会话。勾选**显示已删除**可查看已删除的操作员；已删除的操作员在所示日期之前可以作为操作员恢复，而其在客户组织中创建的 API 密钥会保持吊销状态。
4. **角色。** 在**操作员**与**管理员**之间调整成员角色；更改在对方下一次点击时生效，并且除非您在最近 5 分钟内使用身份验证器验证码登录过，否则需要输入您本人的验证码。您无法更改自己的角色或禁用自己；唯一的在用管理员也无法被降级或禁用：请先把另一位操作员设为管理员。

在页面底部，**在所有位置退出登录**将终止您的所有会话，包括您从合作伙伴门户打开的任何客户门户。