Network policies

- Select policies for a sandbox
- How policies combine
- Policy rules
- Create a policy
- Understand blocked access

Use network policies to control which hosts and services your sandbox can reach. For tools and authentication, configure MCP and Secrets separately.

There are two types of network policy:

- Kit policies are the read-only network rules defined by the selected kit. They apply automatically when you create a sandbox, including when you use a custom kit. Review curated kit rules under **Kit policies** on the **Policies** page. The launcher's policy picker also shows the selected kit's policy when the kit includes network rules.
- User policies are policies that you can select when you create a sandbox. Choose the read-only **Open** or **Balanced** presets, or create a custom policy. **Open** allows outbound access to any host. **Balanced** allows access to a curated set of hosts and services.

Select policies for a sandbox

The launcher remembers your policy selections from the previous launch in the same browser. Without saved selections, it selects the account's policies marked **Always applied**. These policies can't be deselected in the launcher. You can select zero, one, or several additional user policies. By default, **Open** is marked **Always applied**, unlike local sandboxes where you choose a network preset.

On **Policies**, use the **Always applied** switch in the user-policy table to change this account setting, including for read-only presets. The setting is saved and controls which policies are required for future sandbox launches. Turning it off makes the policy optional in the launcher. Review your saved selections before launching.

To use a preset as an editable starting point, select **Duplicate** on its row, edit the copied name and rules, and save the custom policy.

How policies combine

Allow rules from all applicable user policies and the kit are combined. A destination allowed by any of these rules is permitted unless an explicit deny rule blocks it. Deny rules take precedence over allow rules.

For example, selecting both **Open** and **Balanced** permits all outbound destinations except those explicitly denied. Open's `**` rule already allows all destinations, so Balanced's allow list doesn't narrow access. To restrict access with an allow list, deselect **Open** if it is selected and can be removed, and review the allow rules in the remaining policies and kit.

If the combined allow list contains any rules, destinations outside that list are blocked. This default behavior isn't an explicit deny rule: adding an allow rule in another policy permits the matching destinations. If the combined allow list is empty or absent, the sandbox can reach any destination except those blocked by deny rules.

Policy rules

Policy rules allow or deny network destinations. Use the following hostname patterns:

Pattern	Example	Matches
Exact hostname	`example.com`	`example.com` only, not subdomains
Single-level wildcard	`*.example.com`	One subdomain level, such as `api.example.com`
Multi-level wildcard	`**.example.com`	Any depth: `api.example.com`, `v2.api.example.com`
Hostname with port	`example.com:443`	`example.com` on port 443 only

`example.com` does not match subdomains, and `*.example.com` does not match the root domain. Add each pattern required by your destinations.

You can also match IPv4 and IPv6 CIDR ranges, such as `10.0.0.0/8`, `192.168.1.0/24`, and `2001:db8::/32`.

Include the hosts your agent needs both during setup and while it runs, such as source control services, package registries, and model providers.

Create a policy

1. Open **Policies** and select **New policy**.
2. Enter a **Name** that describes what the policy is for.
3. For each rule, enter a **Rule name**, choose **allow** or **deny**, and select **TCP**, **UDP**, or both. TCP is selected by default. To create a UDP-only rule, select **UDP** and deselect **TCP**.
4. Enter the destination patterns under **Targets**. Select **Add rule** to configure another rule.
5. Review the rules and save the policy.

To apply the policy, select it under **Egress policy for this sandbox** when you create a sandbox.

You can edit, copy, or delete a custom policy. You can't edit or delete the built-in presets or kit policies.

Understand blocked access

If a policy blocks a service, your agent or tool might report an HTTP 403 response, a connection failure, or another service error. Check the error message for the host it tried to reach.

Check that your allow rules cover the host and port, along with any supporting APIs the service needs. Add the narrowest rule that permits the required access. Use **Open** if your task needs broad outbound access.

□□□ #2
□ □□□ □□□ 2026-10-31 18:53:11 UTC
□ □□□ □□□ 2026-10-31 18:53:12 UTC