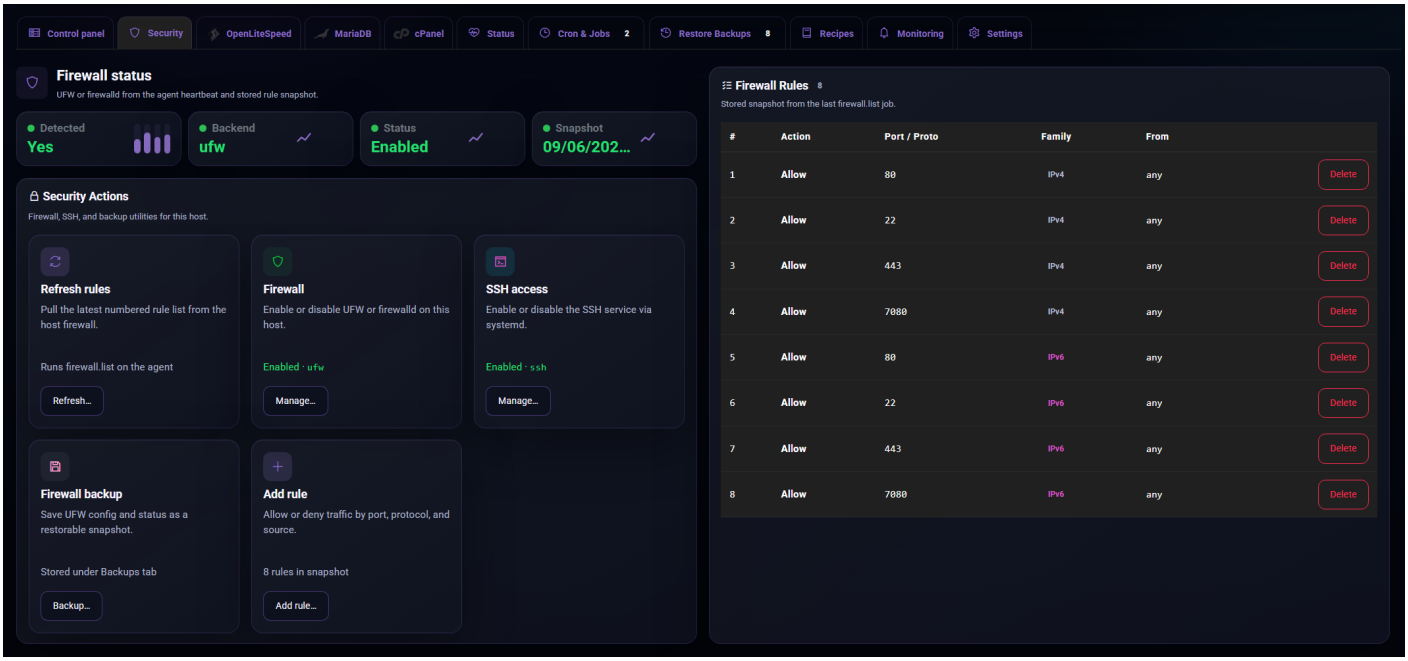
Security Tab

Member Security

Tab: Security.

Use the **Security** tab to check and manage host-level firewall and SSH access for one server in a hosting pool. It is for server access control, not website, database, or cPanel account security.



What you can do

Area	What it is for
Firewall status	See whether a supported firewall backend is detected, which backend is in use, whether it is enabled, and when the rule list was last refreshed.
Security actions	Refresh firewall rules, enable or disable the firewall, manage SSH access, back up firewall rules, and add firewall rules.
Firewall rules	Review the latest stored rule snapshot and delete rules when needed.

Supported firewall views are based on what the member reports, commonly UFW or firewalld.

Free and Pro

Feature	Community	Pro
View firewall status from the latest member report	Included	Included
View SSH status from the latest member report	Included	Included
View stored firewall rule snapshots	Included	Included
Refresh firewall rules	Upgrade required	Included
Enable or disable firewall	Upgrade required	Included
Add firewall rules	Upgrade required	Included
Delete firewall rules	Upgrade required	Included
Enable or disable SSH service	Upgrade required	Included
Back up firewall rules	Upgrade required	Included

Community gives visibility. Pro gives controlled action: rule changes, firewall state changes, SSH access control, and firewall backups before risky changes.

Firewall status

Open **Pool**, choose the member, then select **Security**.

The firewall status area shows:

- Whether a supported firewall was detected.
- The firewall backend, such as UFW or firewalld.
- Whether the firewall is enabled or disabled.
- When the rule snapshot was last refreshed.

If the firewall is not detected, the member may not have a supported firewall installed or the agent may not have enough information yet. Refresh rules after fixing the host.

Refreshing rules

Use **Refresh rules** to pull a fresh firewall rule list from the host.

Refresh is useful after:

- You changed firewall rules outside ServersCTL.

- A backup or restore changed host security files.
- The rules table is empty or stale.
- You want to confirm the current live state before editing.

The rules table updates after the job completes. Check **Cron & Jobs** if the refresh does not appear to finish.

Managing the firewall

Use **Firewall** to enable or disable the detected firewall backend.

Before enabling the firewall:

- Make sure SSH is allowed from your access IP or management network.
- Make sure required web, database, control panel, and monitoring ports are allowed.
- Refresh the rule list so you can see what will apply.

Before disabling the firewall:

- Understand that inbound filtering is reduced or stopped until it is enabled again.
- Use this only for controlled troubleshooting or planned maintenance.

Existing rules are preserved. Refresh rules after the job completes so the table reflects the new state.

Adding rules

Use **Add rule** to allow, deny, or reject traffic by protocol, port, and source.

The form asks for:

Field	Meaning
Action	Allow, deny, or reject matching traffic.
Protocol	TCP or UDP.
Port	A single port or a valid range.
Source	`any` or an IPv4 CIDR range.
Comment	Optional note to make the rule easier to identify later.

Use narrow sources where possible. For example, allow SSH from your office or VPN range instead of allowing it from anywhere.

Deleting rules

Use **Delete** from the firewall rules table when a rule is no longer needed.

Deleting a rule can immediately change live traffic. Check the action, port, protocol, source, and comment before confirming.

SSH access

Use **SSH access** to enable or disable the SSH service on the host.

Disabling SSH may close current sessions and block new SSH logins. The balctl agent should continue running, so you can turn SSH back on from the Security tab when the member is still checking in.

Use this carefully. If the agent stops checking in and SSH is disabled, you may need console access from your server provider.

Firewall backup

Use **Firewall backup** before large firewall changes, migrations, or security cleanups.

Firewall backups are stored with the member's backups so they can be found from the backup and restore areas. Keep a backup before removing broad rules or changing access to production services.

What this tab does not manage

The Security tab is host-level only.

Not managed here	Where to manage it
cPanel users, packages, and account access	cPanel tab or WHM
AutoSSL and website certificates	cPanel or OpenLiteSpeed tools, depending on the server
Database users and grants	MariaDB / MySQL tab or database tools
DNS provider security	Managed DNS or provider settings

Revision #1
Created 2026-07-08 19:25:11 UTC by ServersCTL
Updated 2026-07-08 19:25:38 UTC by ServersCTL