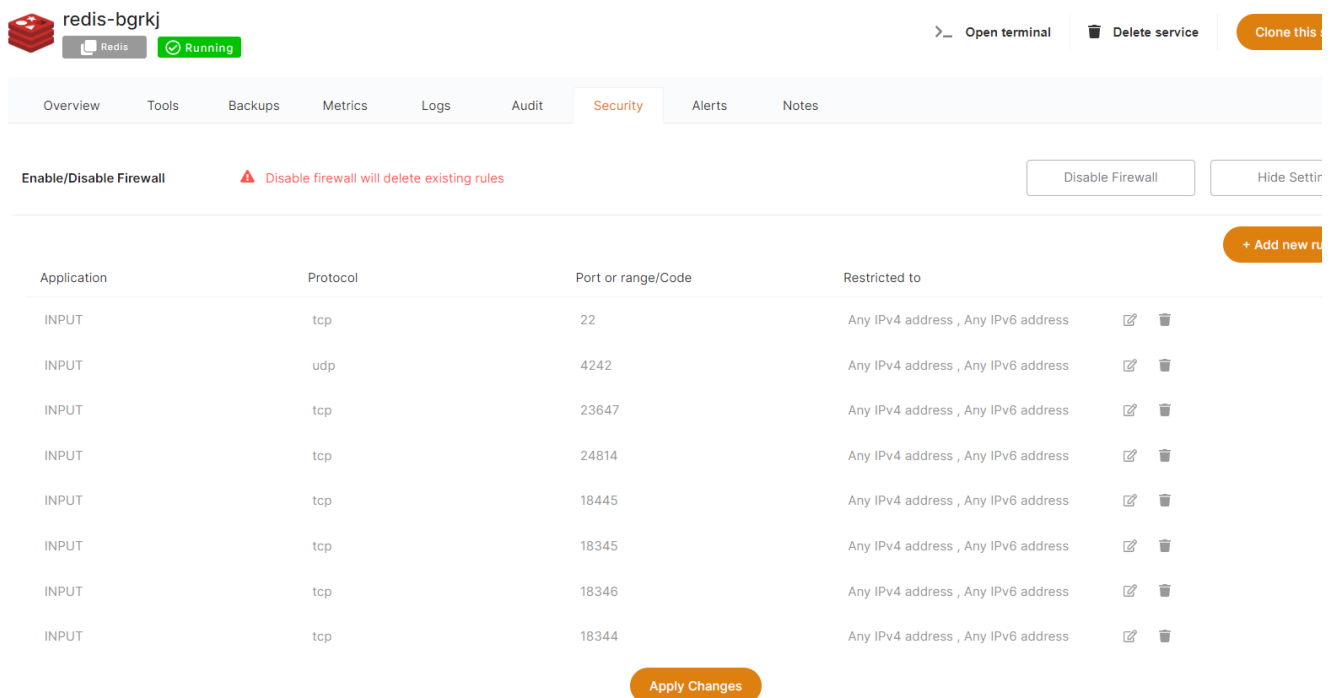


Network Firewall

By default, we only open the ports necessary for the application you have deployed.

How can I restrict access to my service by IP address?

From the Dashboard, select "**Security**", then "**Show Settings**" on the Firewall row



The screenshot shows the Redis dashboard for a service named 'redis-bgrkj'. The 'Security' tab is selected, displaying a table of firewall rules. The table has four columns: Application, Protocol, Port or range/Code, and Restricted to. There are eight rules listed, all for 'INPUT' applications. The 'Restricted to' column shows 'Any IPv4 address , Any IPv6 address' for each rule. At the bottom of the table is an 'Apply Changes' button. Above the table, there are buttons for 'Disable Firewall' and 'Hide Settings', and a warning message: 'Disable firewall will delete existing rules'.

Application	Protocol	Port or range/Code	Restricted to
INPUT	tcp	22	Any IPv4 address , Any IPv6 address
INPUT	udp	4242	Any IPv4 address , Any IPv6 address
INPUT	tcp	23647	Any IPv4 address , Any IPv6 address
INPUT	tcp	24814	Any IPv4 address , Any IPv6 address
INPUT	tcp	18445	Any IPv4 address , Any IPv6 address
INPUT	tcp	18345	Any IPv4 address , Any IPv6 address
INPUT	tcp	18346	Any IPv4 address , Any IPv6 address
INPUT	tcp	18344	Any IPv4 address , Any IPv6 address

From there you can modify, remove, or add new rules to open a port from your service to the internet (or just to a specific target IP).

All services come preconfigured with firewall rules that match the software you are deploying.

“ You have to keep port 80 open to any ipv4/ipv6 or else Letsencrypt won't be able to generate an SSL certificate.

Here is a compilation of the ports necessary for Elestio Automation:

Mandatory	Application	Protocol	Port	Usage
✔	Input	TCP	22	Automation SSH
☐	Input	UDP	4242	Nebula/ Global IP
☐	Input	TCP	18345	VS Code
☐	Input	TCP	18374	Open Terminal
☐	Input	TCP	18346	File Explorer
☐	Input	TCP	18445	Tail Logs
☐	Input	TCP	18344	Terminal

☐ => Ports are necessary only if you are utilizing specific tools and activating global private IP functionality.