interweb

Generated on 15/11/2026 00:15

KNOWLEDGE BASE · PUBLIC DOCUMENT

How to change the SSH port without locking yourself out

Security & Access

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-1390	v2026.10.10	Angola · English

Interweb Angola
RLX Angola, Lda. · Group RLX Holdings
Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/1390

How to change the SSH port without locking yourself out

Security & Access Created on **October 10, 2026** 3 min read



The rule for changing the SSH port is a single one: **open the new port before you close the old one, and test in a second connection before closing the first**. You edit `/etc/ssh/sshd_config`, add a `Port 2222` line (an example), open that port in the firewall, restart SSH and connect through it. Only when it works do you remove port 22. Changing the port is not real security: it clears the noise of automatic probes that only look at 22 and keeps the logs readable. Security comes from keys (**creating an SSH key** and **keeping your VPS secure**).

Step by step

1. **Pick the port and write it down.** A free number (above 1024) you do not use. Write it where you keep the credentials: whoever inherits the server or forgets the number cannot get in (**I have lost SSH access**).

2. **Open the new port in the firewall first.** With ufw: `sudo ufw allow 2222/tcp`. With firewalld: `sudo firewall-cmd --permanent --add-port=2222/tcp` and `sudo firewall-cmd --reload`. On AlmaLinux and Rocky, SELinux has to know about it too: `sudo semanage port -a -t ssh_port_t -p tcp 2222` (see **SELinux and AppArmor**).

3. **Edit the configuration keeping both ports.** `sudo nano /etc/ssh/sshd_config` and leave the lines `Port 22` and `Port 2222`. That way, if something goes wrong, 22 still lets you in.

4. **Test the configuration before restarting.** `sudo sshd -t` should print nothing. If it prints something, it is a syntax error: fix it before going on.

5. **Restart SSH, with your current session still open.** `sudo systemctl restart ssh` on Debian and Ubuntu; `sudo systemctl restart sshd` on AlmaLinux and Rocky. On recent Ubuntu releases SSH may be started by a socket (`ssh.socket`): see the warning below.

6. **Confirm it listens on both ports.** `sudo ss -tlnp | grep sshd` should show 22 and 2222.

7. **Connect through the new one, in a new window,** without closing the old one: `ssh -p 2222 user@server-IP`. Carry on only if you get in.

8. **Remove the old port.** Delete the `Port 22` line, `sudo sshd -t`, restart, and close 22 in the firewall (`sudo ufw delete allow 22/tcp`). Test once more in a third window.

What changes afterwards

Tool	How to give the port
`ssh`	`ssh -p 2222 user@IP`
`scp`	`scp -P 2222 file user@IP:/destination` (capital P)
`sftp` and graphical clients	`sftp -P 2222 ...`; in a graphical client, the "Port" field
`rsync`	`rsync -e "ssh -p 2222" ...` (**copying with rsync**)
Tunnels and automatic backups	The port must be updated in every script and configuration file that connects to the server.

On recent Ubuntu releases, SSH may be started by a socket.
In that case the port the system listens on can come from the `ssh.socket` unit and not only from `sshd_config`. That is why the `ss -tlnp` confirmation step is mandatory: if the new port does not show up, look at `systemctl status ssh.socket` and Ubuntu's documentation for your release, and only then close the old one. Depending on your system, the mechanics can vary.

Never close the session where you made the change until you have tested in another.
It is the most common cause of being locked out. If it happens, the panel console gets in without the network and undoes it: **I have lost SSH access to my server**.

Other services need to know the new port too.
If you run fail2ban (**installing fail2ban**), tell it the new port, or it stops protecting SSH. And if you run SSH on another port because of networks that only let web traffic through, that is a different question: **ports and firewall**.

NEED A HAND?

Locked yourself out after touching SSH? Tell us the service name and what you did, and we will give you the console.

Open a support ticket →

SEE ALSO

- **I have lost SSH access to my server** →
- **Keeping your VPS secure** →
- **Ports and firewall on a VPS** →
- **Why your IP gets blocked by the firewall** →

interweb

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF)	500 260 5724
COMMERCIAL REGISTRATION NO.	26464-25/250724
REGISTERED OFFICE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACT	info@interweb.ao · +244 942 011 191 · www.interweb.ao
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-AO-KB-1390 · v2026.10.10 · Generated on 15/11/2026 00:15