SSH Commands Cheat Sheet

OpenSSH quick reference for Linux & Unix system administrators

computingforgeeks.com

Tested: **OpenSSH 9.9p1** / Rocky Linux 10 & **9.6p1** / Ubuntu 24.04

CONNECT

`ssh host`	Connect as current user
`ssh user@host`	Connect as a specific user
`ssh -p 2222 user@host`	Non-standard port
`ssh -i key user@host`	Use a specific private key
`ssh -A user@host`	Forward the SSH agent
`ssh -X user@host`	X11 (GUI) forwarding
`ssh -v / -vv / -vvv`	Verbose debug output

KEYS & COPY-ID

`ssh-keygen -t ed25519`	Generate Ed25519 key (best)
`ssh-keygen -t rsa -b 4096`	Generate RSA 4096 key
`ssh-keygen -f file -N ""`	Custom name, no passphrase
`ssh-keygen -p -f key`	Change a key passphrase
`ssh-keygen -lf key.pub`	Show key fingerprint
`ssh-copy-id user@host`	Install public key on server
`ssh-copy-id -p 2222 ...`	Copy key on custom port

SSH-AGENT

`eval $(ssh-agent)`	Start the agent
`ssh-add`	Add the default key
`ssh-add key`	Add a specific key
`ssh-add -t 3600 key`	Add with a timeout
`ssh-add -l`	List loaded keys
`ssh-add -D`	Remove all keys

CONFIG (~/.SSH/CONFIG)

`Host alias`	Define a host shortcut
`HostName ip`	Real address of the host
`User name`	Default login user
`Port n`	Default port
`IdentityFile key`	Default key for this host
`ProxyJump bastion`	Route through a jump host
`ServerAliveInterval 60`	Keep-alive (no timeouts)

REMOTE COMMANDS

`ssh host 'cmd'`	Run one command
`ssh host 'a && b'`	Run multiple commands
`ssh -t host 'sudo ...'`	Force a TTY (sudo, top)
`ssh host 'bash -s' < f.sh`	Run a local script remotely

FILE TRANSFER

`scp f user@host:/path`	Copy file to remote
`scp user@host:/f .`	Copy file from remote
`scp -r dir host:/path`	Copy directory recursively
`scp -P 2222 ...`	SCP on custom port (-P)
`sftp user@host`	Interactive transfer session
`rsync -avz -e ssh s/ h:d/`	Incremental sync over SSH
`sshfs host:/dir /mnt`	Mount remote dir locally
`fusermount -u /mnt`	Unmount an SSHFS mount

PORT FORWARDING & TUNNELS

`ssh -L 8080:host:80 gw`	Local forward (reach remote svc)
`ssh -R 9000:localhost:3000 h`	Reverse forward (expose local svc)
`ssh -D 9999 host`	Dynamic SOCKS5 proxy
`ssh -f -N -L ...`	Background, no shell (-fN)
`ssh -O check host`	Check a shared connection
`ssh -O exit host`	Close a shared connection

JUMP HOSTS

`ssh -J bastion host`	Hop via a bastion
`ssh -J b1,b2 host`	Chain multiple jumps
`ssh -J user@b:2222 host`	Jump with user & port

MULTIPLEXING

`ControlMaster auto`	Reuse one TCP connection
`ControlPath ~/.ssh/s/%r@%h-%p`	Shared socket path
`ControlPersist 600`	Keep master open (sec)

ESCAPE SEQUENCES (AFTER ENTER)

`~.`	Kill a frozen session
`~^Z`	Suspend the SSH session
`~#`	List forwarded connections
`~C`	Open SSH command line
`~?`	Show all escape sequences

KNOWN HOSTS

`ssh-keygen -R host`	Remove a host entry
`ssh-keyscan host`	Fetch a host's keys
`ssh-keyscan -H h >> known_hosts`	Add host without connecting

CERTIFICATES (CA)

`ssh-keygen -s ca -I id -n u k.pub`	Sign a user key with the CA
`ssh-keygen -Lf cert.pub`	Inspect a certificate
`TrustedUserCAKeys /etc/ssh/ca.pub`	Trust a CA (sshd_config)

HARDENING (SSHD_CONFIG)

`PasswordAuthentication no`	Keys only, no passwords
`PermitRootLogin no`	Block direct root login
`AllowUsers admin deploy`	Allowlist specific users
`MaxAuthTries 3`	Limit auth attempts
`Port 33000`	Change the default port
`sshd -t`	Validate config before restart

DEBUG & TROUBLESHOOT

`ssh -vvv user@host`	Max-verbosity connection trace
`ss -tlnp | grep sshd`	Is sshd listening?
`systemctl status sshd`	Service status
`journalctl -u sshd -f`	Auth log (RHEL/Rocky)
`tail -f /var/log/auth.log`	Auth log (Debian/Ubuntu)
`chmod 700 ~/.ssh; 600 keys`	Fix permission failures