

SSH Cheatsheet

By Dejan Panovski • Updated on Jan 26, 2026 •

Quick reference for SSH commands and configuration

SSH (Secure Shell) is a protocol for securely connecting to remote systems. This cheatsheet covers common SSH commands for connecting, file transfer, tunneling, and key management.

Basic Connection

Connect to remote servers.

<code>ssh user@host</code>	Connect to host
<code>ssh host</code>	Connect with current username
<code>ssh -p 2222 user@host</code>	Connect on custom port
<code>ssh user@host command</code>	Run command on remote host
<code>ssh -v user@host</code>	Verbose mode (debug)
<code>ssh -q user@host</code>	Quiet mode

SSH Keys

Generate and manage SSH keys.

<code>ssh-keygen</code>	Generate SSH key pair
<code>ssh-keygen -t ed25519</code>	Generate Ed25519 key
<code>ssh-keygen -t rsa -b 4096</code>	Generate 4096-bit RSA key
<code>ssh-keygen -p -f ~/.ssh/id_ed25519</code>	Change key passphrase
<code>ssh-keygen -y -f ~/.ssh/id_ed25519</code>	Show public key
<code>ssh-keygen -R hostname</code>	Remove host from known_hosts

Copy SSH Key

Set up passwordless authentication.

<code>ssh-copy-id user@host</code>	Copy key to remote host
<code>ssh-copy-id -i ~/.ssh/key.pub user@host</code>	Copy specific key
<code>ssh-copy-id -p 2222 user@host</code>	Copy key on custom port

SSH Agent

Manage SSH keys in memory.

<code>eval "\$(ssh-agent -s)"</code>	Start SSH agent
<code>ssh-add</code>	Add default key to agent
<code>ssh-add ~/.ssh/id_ed25519</code>	Add specific key
<code>ssh-add -l</code>	List keys in agent
<code>ssh-add -d ~/.ssh/id_ed25519</code>	Remove key from agent
<code>ssh-add -D</code>	Remove all keys

SCP (Secure Copy)

Copy files over SSH.

<code>scp file user@host:/path</code>	Copy file to remote
<code>scp user@host:/path/file .</code>	Copy file from remote
<code>scp -r dir user@host:/path</code>	Copy directory recursively
<code>scp -P 2222 file user@host:/path</code>	Copy on custom port
<code>scp -C file user@host:/path</code>	Copy with compression
<code>scp -p file user@host:/path</code>	Preserve timestamps

SFTP

Interactive file transfer.

<code>sftp user@host</code>	Connect to host
<code>sftp -P 2222 user@host</code>	Connect on custom port
<code>get file</code>	Download file (in sftp)
<code>put file</code>	Upload file (in sftp)
<code>ls, cd, pwd</code>	Navigate remote (in sftp)
<code>lls, lcd, lpwd</code>	Navigate local (in sftp)

SSH Tunneling

Create secure tunnels.

<code>ssh -L 8080:localhost:80 user@host</code>	Local port forwarding
<code>ssh -R 8080:localhost:80 user@host</code>	Remote port forwarding
<code>ssh -D 1080 user@host</code>	SOCKS proxy (dynamic)
<code>ssh -N -L 8080:localhost:80 user@host</code>	Tunnel only (no shell)
<code>ssh -f -N -L 8080:localhost:80 user@host</code>	Background tunnel

SSH Config File

Simplify connections with config.

<code>~/.ssh/config</code>	User config file
<code>Host myserver</code>	Define host alias
<code>HostName 192.168.1.100</code>	Server address
<code>User admin</code>	Username
<code>Port 2222</code>	Custom port
<code>IdentityFile ~/.ssh/mykey</code>	Private key path

Connection Options

Common SSH options.

<code>-p port</code>	Custom port
<code>-i keyfile</code>	Identity file (private key)
<code>-o option=value</code>	Set config option
<code>-F configfile</code>	Custom config file
<code>-J jumphost</code>	Jump through host (ProxyJump)
<code>-X</code>	Enable X11 forwarding
<code>-A</code>	Enable agent forwarding

Security Options

Harden SSH connections.

<code>-o StrictHostKeyChecking=yes</code>	Strict host key check
<code>-o UserKnownHostsFile=/dev/null</code>	Ignore known hosts
<code>-o PasswordAuthentication=no</code>	Disable password auth
<code>-o PubkeyAuthentication=yes</code>	Enable key auth
<code>-o ConnectTimeout=10</code>	Connection timeout

Multiplexing

Reuse SSH connections.

<code>ControlMaster auto</code>	Enable multiplexing
<code>ControlPath ~/.ssh/sockets/%r@%h-%p</code>	Socket path
<code>ControlPersist 600</code>	Keep connection for 10 min
<code>ssh -O check user@host</code>	Check connection status
<code>ssh -O exit user@host</code>	Close master connection

Common Patterns

Frequently used combinations.

<code>ssh -t user@host 'sudo command'</code>	Run sudo command
<code>ssh user@host 'cat file' > local</code>	Copy output to local
<code>tar czf - dir ssh user@host 'tar xzf -'</code>	Copy dir via tar
<code>ssh -J jump user@dest</code>	Connect via jump host
<code>ssh user@host -L 3306:localhost:3306</code>	MySQL tunnel