

# 🔒 SSH (Secure Shell) Quick Reference - Same Network 🖥️

---

## Secure Shell Protocol



⌚ Secure • 🔑 Encrypted • 🌐 Remote Access

---

### ▀ What is SSH?

SSH (Secure Shell) is a cryptographic network protocol that provides a secure way to:

- 🔒 Access remote systems on the same network
- 💻 Execute commands on remote machines
- 🔗 Forward ports and applications
- ⚙️ Manage remote services

### ⌚ Key Features

- 🔒 **Encryption:** All traffic is encrypted, preventing eavesdropping
- 🔑 **Authentication:** Supports both password and public key authentication
- ☑️ **Integrity:** Ensures data hasn't been tampered with during transit
- 🔗 **Port Forwarding:** Tunnel other protocols through SSH

### 💼 Common Use Cases

- 💻 Remote server administration on same network
- 📅 Database management
- 🌐 Web development
- ☁️ Cloud computing (AWS, GCP, Azure)

## Purpose

Practical, Ubuntu-focused commands and examples for key generation, authentication, remote access on same network, and common troubleshooting.

---

### Prerequisites (Ubuntu)

```
sudo apt update  
sudo apt install -y openssh-client openssh-server
```

Check SSH server status (remote/server machine):

```
sudo systemctl status ssh  
# enable/start if needed:  
sudo systemctl enable --now ssh
```

```
ujjwaltyagi@ujjwaltyagi:~$ sudo systemctl status ssh  
[sudo] password for ujjwaltyagi:  
● ssh.service - OpenBSD Secure Shell server  
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)  
  Active: inactive (dead)  
TriggeredBy: ● ssh.socket  
    Docs: man:sshd(8)  
          man:sshd_config(5)  
ujjwaltyagi@ujjwaltyagi:~$
```

### 1) Generate an SSH keypair (ed25519 recommended)

```
ssh-keygen -t ed25519 -C "ujjwaltyagi458@gmail.com"  
# Generated key fingerprint:  
# SHA256:0j2KZRBekWKnJEPGS2m0h2lxJk3hxioPI9115X93ev4 ujjwaltyagi458@gmail.com
```

After generating:

```
ls -l ~/.ssh  
# Verify your keys:  
id_ed25519 id_ed25519.pub  
  
# Start the SSH agent:  
eval "$(ssh-agent -s)"  
Agent pid 4677  
  
# Add your private key:  
ssh-add ~/.ssh/id_ed25519  
Identity added: /home/ujjwaltyagi/.ssh/id_ed25519 (ujjwaltyagi458@gmail.com)
```

```
# View your public key:
cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIN74CRUJB/1CpEZQD1gDhFAEeRM/syD4c20dZ0+CQzCR
ujjwaltyagi458@gmail.com
```

```
ujjwaltyagi@ujjwaltyagi: $ ssh-keygen -t ed25519 -C "ujjwaltyagi458@gmail.com"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/ujjwaltyagi/.ssh/id_ed25519):
Created directory '/home/ujjwaltyagi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ujjwaltyagi/.ssh/id_ed25519
Your public key has been saved in /home/ujjwaltyagi/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:0j2kZRBeWwKnJEP6S2mOh2ixJk3hxioPI9115X93ev4 ujjwaltyagi458@gmail.com
The key's randomart image is:
+--[ED25519 256]--+
|    .+ =+ . |
|    . = +   |
|    . o *   |
| o . . o 0   |
| *   B S +   |
| * = B +   o |
|B B + +   . . o|
|oB   .       .oo|
| .           .oE|
+---[SHA256]----+
ujjwaltyagi@ujjwaltyagi: $ ls ~/.ssh
id_ed25519  id_ed25519.pub
ujjwaltyagi@ujjwaltyagi: $ eval "$(ssh-agent -s)"
Agent pid 4677
ujjwaltyagi@ujjwaltyagi: $ ssh-add ~/.ssh/id_ed25519
Identity added: /home/ujjwaltyagi/.ssh/id_ed25519 (ujjwaltyagi458@gmail.com)
ujjwaltyagi@ujjwaltyagi: $ cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIN74CRUJB/1CpEZQD1gDhrAEeRM7syD4c20dZ0+CQzCR ujjwaltyagi458@gmail.com
ujjwaltyagi@ujjwaltyagi: $
```

## 2) Install public key on the remote host

Preferred:

```
ssh-copy-id -i ~/.ssh/id_ed25519.pub user@remote.host
```

Manual (if ssh-copy-id absent):

```
cat ~/.ssh/id_ed25519.pub | ssh user@remote.host 'mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys'
```

```
ujjwaltyagi@ujjwaltyagi: $ ssh-copy-id -i ~/.ssh/id_ed25519.pub ujjwaltyagi@10.0.2.15
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/ujjwaltyagi/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
ujjwaltyagi@10.0.2.15's password:
```

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'ujjwaltyagi@10.0.2.15'"  
and check to make sure that only the key(s) you wanted were added.

## 3) Connect and run commands

Interactive (same network):

```
ssh user@192.168.1.100
```

Single command (same network):

```
ssh user@192.168.1.100 'uname -a && uptime'
```

```
ujjwaltyagi@ujjwaltyagi:~$ ssh ujjwaltyagi@10.0.2.15
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-29-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is enabled.

118 updates can be applied immediately.
69 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

#### 4) SSH agent (avoid repeated passphrases)

```
eval "$(ssh-agent -s)"
ssh-add ~/.ssh/id_ed25519
# List loaded keys:
ssh-add -l
```

```
ujjwaltyagi@ujjwaltyagi:~$ eval "$(ssh-agent -s)"
Agent pid 4677
ujjwaltyagi@ujjwaltyagi:~$ ssh-add ~/.ssh/id_ed25519
Identity added: /home/ujjwaltyagi/.ssh/id_ed25519 (ujjwaltyagi458@gmail.com)
```

#### 5) SSH config for shortcuts (~/.ssh/config)

Create/edit [~/.ssh/config](#):

```
Host local-server
  HostName 192.168.1.100
  User youruser
  Port 22
  IdentityFile ~/.ssh/id_ed25519
  IdentitiesOnly yes
```

```
ujjwaltyagi@ujjwaltyagi:~$ nano ~/.ssh/config
ujjwaltyagi@ujjwaltyagi:~$ cat ~/.ssh/config
Host uni
  HostName 10.0.2.15
  User ujjwaltyagi
  Port 22
  IdentityFile ~/.ssh/id_ed25519
  IdentitiesOnly yes
ujjwaltyagi@ujjwaltyagi:~$ chmod 700 ~/.ssh
ujjwaltyagi@ujjwaltyagi:~$ chmod 600 ~/.ssh/config
```

Connect with:

```
ssh local-server
```

```
ujjwaltyagi@ujjwaltyagi:~$ ssh uni
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-29-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is enabled.

118 updates can be applied immediately.
69 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Tue Oct 28 13:21:11 2025 from 10.0.2.15
```

---

## 6) Port forwarding (local → remote)

Local forward (access remote web app locally on same network):

```
ssh -L 8080:localhost:8000 user@192.168.1.100
# browse http://localhost:8080
```

```
ujjwaltyagi@ujjwaltyagi:~$ ssh -L 8080:localhost:8080 ujjwaltyagi@10.0.2.15
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-29-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is enabled.

118 updates can be applied immediately.
69 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Tue Oct 28 13:35:04 2025 from 10.0.2.15
ujjwaltyagi@ujjwaltyagi:~$ █
```

## 7) File transfer: scp & sftp

SCP (single file on same network):

```
scp localfile.txt user@192.168.1.100:/home/user/
```

```
ujjwaltyagi@ujjwaltyagi:~$ scp modify1.txt ujjwaltyagi@10.0.2.15:/home/ujjwaltyagi/
modify1.txt                                                 100%   378      61.5KB/s   00:00
ujjwaltyagi@ujjwaltyagi:~$ █
```

SCP (directory on same network):

```
scp -r project/ user@192.168.1.100:/home/user/project_backup/
```

```
ujjwaltyagi@ujjwaltyagi:~$ scp -r unit_8/ ujjwaltyagi@10.0.2.15:/home/ujjwaltyagi/scripts/
check_file_permission.sh                               100%    30      17.6KB/s   00:00
ujjwaltyagi@ujjwaltyagi:~$ █
```

```
ujjwaltyagi@ujjwaltyagi:~$ ls scripts
unit_8
```

SFTP interactive (same network):

```
sftp user@192.168.1.100
sftp> put localfile
```

```
ujjwaltyagi@ujjwaltyagi:~$ sftp ujjwaltyagi@10.0.2.15
Connected to 10.0.2.15.
sftp> pwd
Remote working directory: /home/ujjwaltyagi
sftp> put modify1.txt
Uploading modify1.txt to /home/ujjwaltyagi/modify1.txt
modify1.txt                                0%   0      0.0KB/s  --::-- ETA
sftp> put floatint.txt
Uploading floatint.txt to /home/ujjwaltyagi/floatint.txt
floatint.txt                                0%   0      0.0KB/s  --::-- ETA
sftp> bye
ujjwaltyagi@ujjwaltyagi:~$
```

## 8) Troubleshooting checklist

- Permissions: `chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys`
  - Verbose SSH: `ssh -vvv user@host`
  - Confirm key present: `ssh-add -l`
  - Check server logs: `sudo journalctl -u ssh -e`
- 

## 9) Best practices

- Prefer `ed25519` keys with passphrase.
  - Use `~/.ssh/config` for convenience.
  - Keep private keys private; remove unused keys on servers.
- 

## 10) Quick commands

```
ssh-keygen -t ed25519
ssh-copy-id user@192.168.1.100
ssh user@192.168.1.100
scp file user@192.168.1.100:/path/
ssh -L 8080:localhost:8000 user@192.168.1.100
```