SSH Key Authentication Create and Share

Why SSH Keys are Important? SSH keys use asymmetric encryption—a public key is placed on the server, and a private key stays on your device.

Benefits over Passwords

- Security: Keys are far more resistant to brute-force attacks than passwords
- Convenience: No need to type passwords every time
- Automation: Ideal for scripts and remote tasks
- Granular Access: You can assign different keys to different users or devices

Pre requisite- Needs OpenSSH if not already installed.

Generating SSH Keys

1. On your local computer that will be used to establish connection with a server
2. In terminal type following command

```
ssh-keygen -t rsa -b 4096 -C "key name"
```

"-t rsa" - specifies the type of key RSA

"b 4096" - Sets the key length to 4096 bits

"-C" - Adds a comment, optional

or use ed25519 for stronger encryption

```
ssh-keygen -t rsa -t ed25519 -C "key name"
```

3. Copy Public Key to Server

```
ssh-copy-id username@server_ip
```

Or if you make multiple different keys

```
ssh-copy-id -i ~/.ssh/id_rsa_work.pub 'name of the key you want to copy' username@server_ip
```

To See the public key

```
cat ~/.ssh/id_rsa.pub
```

More Info on managing multiple keys check Managing Multiple SSH Keys

When using Passphrase, it would be a good idea to have SSH Agent to manege them. More info at SSH Agent Management

---

Revision #8
Created 2025-08-03 11:47:28 UTC by overseer
Updated 2026-03-13 01:30:13 UTC by lumxux