Managing Multiple SSH Keys

If you use different keys for different servers or services (e.g., GitHub, work, personal), here’s how to keep it organized. Using different keys for different services makes things way more organized and secure. This way if one key gets compromised, you only need to change it for that service or server.

Creating Multiple Keys

1. Login to machine you want to have access to server or services
2. Open Terminal and Create Keys

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa_work
ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa_personal   'adding path will make the key unique
and wont override the previous one'
```

3. Send each key to it's designated server

```
ssh-copy-id -i ~/.ssh/id_rsa_work.pub username@server_ip
```

Using SSH Config File

For easier access adjust config file. This will tell which key goes to which session

```
# Work server
Host work-server
    HostName work.example.com
    User yourusername
    IdentityFile ~/.ssh/id_rsa_work
    IdentitiesOnly yes

# Personal server
Host personal-server
    HostName personal.example.com
    User yourusername
    IdentityFile ~/.ssh/id_rsa_personal
```

```
    IdentitiesOnly yes
```

Using SSH Agent is a good idea if using passphrase for each one, check out SSH Agent Management

---

Revision #5
Created 2025-08-03 13:57:34 UTC by overseer
Updated 2026-03-13 01:30:02 UTC by lumxux