OpenSSH

OpenSSH (also known as OpenBSD Secure Shell) is a suite of secure networking utilities based on the Secure Shell (SSH) protocol, which provides a secure channel over an unsecured network in a client–server architecture.

OpenSSH started as a fork of the free SSH program developed by Tatu Ylönen; later versions of Ylönen's SSH were proprietary software offered by SSH Communications Security. OpenSSH was first released in 1999 and is currently developed as part of the OpenBSD operating system.

OpenSSH is not a single computer program, but rather a suite of programs that serve as alternatives to unencrypted protocols like Telnet and FTP. OpenSSH is integrated into several operating systems, namely Microsoft Windows, macOS and most Linux operating systems, while the portable version is available as a package in other systems.

Package

```
pacman -S openssh
```

Start/restart

```
systemctl enable --now sshd.service
```

Any change to `/etc/ssh/sshd_config` requires a restart of the service. Keep that in mind.

```
systemctl restart sshd.service
```

Allow root and password authentication

If you need quick access, for example to set up your server.

```
nano /etc/ssh/sshd_config
```

```
Port 22
PermitRootLogin yes
PasswordAuthentication yes
```

SSH key

This is not only more secure, it also simplifies the connection to the server without having to enter the password every time.

Config - server

```
nano /etc/ssh/sshd_config
```

```
Port 22
HostKey /etc/ssh/ssh_host_ed25519_key
PermitRootLogin no
PubkeyAuthentication yes
PasswordAuthentication no
PermitEmptyPasswords no
```

Create key - desktop

Whether you want to use a passphrase or not, depends on how you want to use your infrastructure and whether you want/need an additional layer of security. For example, keepassxc can handle passphrases and add the key to the ssh agent for automatic connections.

```
ssh-keygen -t ed25519
```

Copy the content of `id_ed25519.pub` for your server.

```
cat ~/.ssh/id_ed25519.pub
```

Add host - desktop

Change `$USER` and `$SERVERIP`.

```
nano .ssh/config
```

```
Host server
    HostName $SERVERIP
    Port 22
    User $USER
    IdentitiesOnly yes
    IdentityFile "~/.ssh/id_ed25519"
```

Add pub key - server

Paste the content of `id_ed25519.pub` in `authorized_keys`.

```
cd
mkdir .ssh
chmod 700 .ssh
touch .ssh/authorized_keys
chmod 600 .ssh/authorized_keys
```

```
nano .ssh/authorized_keys
```

SSH-agent - desktop

```
mkdir -p ~/.config/systemd/user/
nano ~/.config/systemd/user/ssh-agent.service
```

```
[Unit]
Description=SSH key agent

[Service]
Type=simple
Environment=SSH_AUTH_SOCK=%t/ssh-agent.socket
ExecStart=/usr/bin/ssh-agent -D -a $SSH_AUTH_SOCK

[Install]
WantedBy=default.target
```

```
systemctl --user enable ~/.config/systemd/user/ssh-agent.service
systemctl --user start ssh-agent.service
```

Reboot might be necessary if Keepassxc get's an error like “No agent running, cannot add identity”.