

Enable SSH Key based authentication and Disable Password Authentication in ssh

302 admin August 28, 2024 [General](#), [Installation](#) 7474

Set Up SSH Key Authentication and Turn Off Password Login

Overview: This article covers hardening SSH authentication by **enabling SSH key-based authentication** and **disabling password authentication**. It involves modifying the `/etc/ssh/sshd_config` file to set **PubkeyAuthentication yes** and **PasswordAuthentication no**, followed by restarting the SSH service to apply the changes.

Hardening Authentication in SSH

Step 1: Enable SSH Key based authentication and disable Password Authentication in **sshd configuration file**.

```
:~# vi /etc/ssh/sshd_config
```

```
PubkeyAuthentication yes
```

```
# To disable tunneled clear text passwords, change to no here!
```

```
PasswordAuthentication no
```

Step 2: After making changes in the SSHD configuration file save it and restart SSHD

```
:~# service sshd restart
```

Related Articles

[Different types of SSH authentication keys](#)

[Enable/Disable password or key based authentication](#)

[Set SSH Key Expiry for the gateway users](#)

[Add a Linux server or a Linux instance into the Ezeelogin ssh jumphost?](#)

Online URL:

<https://www.ezeelogin.com/kb/article/enable-ssh-key-based-authentication-and-disable-password-authentication-in-ssh-302.html>