How to enable or disable public key authentication in SSH

SSH server in most systems is by default configured to allow public-key authentication. The method will enable you to use your public and private key pair to log in to an SSH server without using a username and password.

You can disable public key authentication if your private key is compromised or for any other reason by configuring your SSH server

Public key authentication method for SSH could be enabled or disabled by configuring PubkeyAuthentication directive in sshd_config file on the server.

Steps to enable or disable public key authentication in SSH:

Launch your preferred terminal application.
Open SSHd configuration file with your favourite text editor.

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

Search for **PubkeyAuthentication** and set the option to **yes** or **no**.

To disable **PubkeyAuthentication** then set to **no** and you will login with username and password.

To enable **PubkeyAuthentication** then set to **yes** and you will login with Public Key Authentication.

Ins0mniA

Revision #3
Created 2025-05-04 03:30:12 EEST by Green
Updated 2025-09-04 02:04:07 EEST by Green