SSH in most system by default allow login using public key. While this is convenient, it is a security risk when unauthorized person manage to get the private key, especially when the key is not protected by any passphrase. The option to allow public key authentication is PubkeyAuthentication in the /etc/sshd_config configuration file. If it is not set, SSH daemon will allow public key authentication.
Edit configuration file

To disable it, add the following line (or change the option to no if the option already exist) in the configuration file, /etc/ssh/sshd_config;

PubkeyAuthentication no

Reload SSH service

To have the changes take effect, the SSH daemon need to reload the edited configuration file with the following command;

$ sudo /etc/init.d/ssh reload

In some Linux distribution, the command is as the following;

$ sudo /etc/init.d/sshd reload

SSH in most system by default allow login using public key. While this is convenient, it is a security risk when unauthorized person manage to get the private key, especially when the key is not protected by any passphrase. The option to allow public key authentication is PubkeyAuthentication in the /etc/sshd_config configuration file. If it is not set, SSH daemon will allow public key authentication.

Edit configuration file

To disable it, add the following line (or change the option to no if the option already exist) in the configuration file, /etc/ssh/sshd_config;

PubkeyAuthentication no **Reload SSH service**

To have the changes take effect, the SSH daemon need to reload the edited configuration file with the following command;

```
$ sudo /etc/init.d/ssh reload
```

In some Linux distribution, the command is as the following;

```
$ sudo /etc/init.d/sshd reload
```

- See more at: https://docs.oseems.com/general/application/ssh/disable-public-key-authentication#sthash.bbHMmyzw.dpuf

SSH in most system by default allow login using public key. While this is convenient, it is a security risk when unauthorized person manage to get the private key, especially when the key is not protected by any passphrase. The option to allow public key authentication is PubkeyAuthentication in the /etc/sshd_config configuration file. If it is not set, SSH daemon will allow public key authentication.

Edit configuration file

To disable it, add the following line (or change the option to no if the option already exist) in the configuration file, /etc/ssh/sshd_config;

```
PubkeyAuthentication no
```

Reload SSH service

To have the changes take effect, the SSH daemon need to reload the edited configuration file with the following command;

```
$ sudo /etc/init.d/ssh reload
```

In some Linux distribution, the command is as the following;

```
$ sudo /etc/init.d/sshd reload
```

- See more at: https://docs.oseems.com/general/application/ssh/disable-public-key-authentication#sthash.bbHMmyzw.dpuf

SSH in most system by default allow login using public key. While this is convenient, it is a security risk when unauthorized person manage to get the private key, especially when the key is not protected by any passphrase. The option to allow public key authentication is PubkeyAuthentication in the /etc/sshd_config configuration file. If it is not set, SSH daemon will allow public key authentication.

Edit configuration file

To disable it, add the following line (or change the option to no if the option already exist) in the configuration file, /etc/ssh/sshd_config;

PubkeyAuthentication no

Reload SSH service

To have the changes take effect, the SSH daemon need to reload the edited configuration file with the following command;

```
$ sudo /etc/init.d/ssh reload
```

In some Linux distribution, the command is as the following;

```
$ sudo /etc/init.d/sshd reload
```

- See more at: https://docs.oseems.com/general/application/ssh/disable-public-key-authentication#sthash.bbHMmyzw.dpuf

SSH in most system by default allow login using public key. While this is convenient, it is a security risk when unauthorized person manage to get the private key, especially when the key is not protected by any passphrase. The option to allow public key authentication is PubkeyAuthentication in the /etc/sshd_config configuration file. If it is not set, SSH daemon will allow public key authentication.

Edit configuration file

To disable it, add the following line (or change the option to no if the option already exist) in the configuration file, /etc/ssh/sshd_config;

PubkeyAuthentication no

Reload SSH service

To have the changes take effect, the SSH daemon need to reload the edited configuration file with the following command;

```
$ sudo /etc/init.d/ssh reload
```

In some Linux distribution, the command is as the following;

```
$ sudo /etc/init.d/sshd reload
```

- See more at: https://docs.oseems.com/general/application/ssh/disable-public-key-authentication#sthash.bbHMmyzw.dpuf

SSH in most system by default allow login using public key. While this is convenient, it is a security risk when unauthorized person manage to get the private key, especially when the key is not protected by any passphrase. The option to allow public key authentication is PubkeyAuthentication in the /etc/sshd_config configuration file. If it is not set, SSH daemon will allow public key authentication.

Edit configuration file

To disable it, add the following line (or change the option to no if the option already exist) in the configuration file, /etc/ssh/sshd_config;

```
PubkeyAuthentication no
```

Reload SSH service

To have the changes take effect, the SSH daemon need to reload the edited configuration file with the following command;

```
$ sudo /etc/init.d/ssh reload
```

In some Linux distribution, the command is as the following;

```
$ sudo /etc/init.d/sshd reload
```

- See more at: https://docs.oseems.com/general/application/ssh/disable-public-key-authentication#sthash.bbHMmyzw.dpuf