**What is Causing SSH Permission Denied (publickey,gssapi-keyex,gssapi-with-mic)?**

The SSH Permission denied error appears when trying to SSH into a server:

Permission denied (publickey,gssapi-keyex,gssapi-with-mic)

The SSH Permission denied error appearing after a login attempt

Following the Permission denied statement, the bracket contains the attempted authentication methods that failed at the initiation of the connection. The error suggests that the public key is the issue, which is misleading.

One reason for the error may be **sshd\_config**, the file that contains SSH server configuration. The other possibility is that the **authorized\_keys** file has insufficient permissions. This file contains the list of public keys for the clients allowed to SSH into the server. Consequently, the system’s inability to read from the file results in the Permission denied error.

**How to fix SSH Permission denied**

Both solutions contain steps you need to perform on the server-side. Start by opening the terminal on your server and proceed with one of the solutions below.

**Solution 1: Enable Password Authentication**

If you want to use a password to access the SSH server, a solution for fixing the Permission denied error is to enable password login in the **sshd\_config** file.

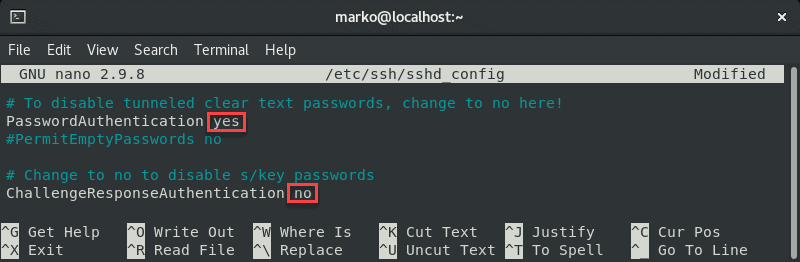
To do this, open the file in a text editor.  This example uses the nano editor:

sudo nano /etc/ssh/sshd\_config

In the file, find the **PasswordAuthentication** line and make sure it ends with **yes**.

Find the **ChallengeResponseAuthentication** option and disable it by adding **no**.

If lines are commented out, remove the hash sign **#** to uncomment them.



Save the file and exit.

Restart the SSH service by typing the following command:

sudo systemctl restart sshd

**Solution 2: Change File System Permissions**

Using the password-based login as the SSH authentication method is not recommended due to [security concerns](https://phoenixnap.com/kb/linux-ssh-security). Therefore, the following solution may be preferable since it troubleshoots [the public key authentication method](https://phoenixnap.com/kb/setup-passwordless-ssh).

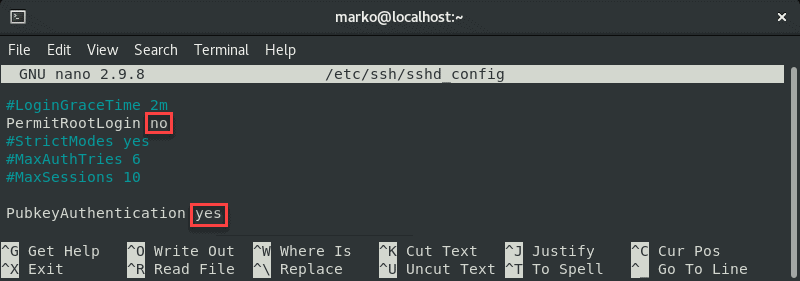
First, open the **sshd\_config** file using a text editor:

sudo nano /etc/ssh/sshd\_config

In the file, make sure the following options are set as follows:

PermitRootLogin no

PubkeyAuthentication yes

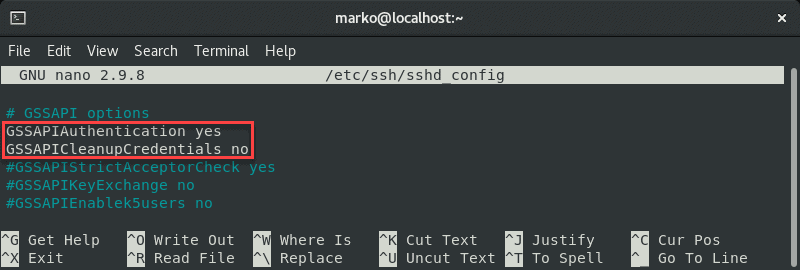


**Note:** The steps above are considered best security practices. If you need to use root login, set the relevant line to **yes**.

Comment out the GSSAPI-related options by adding the hash sign at the beginning of the line:

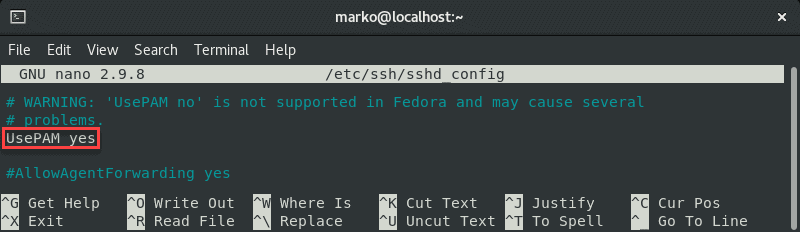
#GSSAPIAuthentication yes

#GSSAPICleanupCredentials no



Also, make sure the **UsePAM** line is set to **yes**:

UsePAM yes



Save the file and restart the sshd service:

systemctl restart sshd

Now navigate to your home folder and check the permissions:

ls -ld

Checking home folder permissions

If your owner permissions are not set to read, write, and execute (**drwx------**), use [the chmod command](https://phoenixnap.com/kb/chmod-recursive) to change them:

chmod 0700 /home/[your-username]

Now go to the **.ssh** folder and recheck the permissions:

ls -ld

Checking the .ssh folder permissions

This directory should also have read, write, and execute permissions for the file owner. To enforce them, use **chmod** again:

chmod 0700 /home/your\_home/.ssh

The **.ssh** folder contains the **authorized\_keys** file. Check its permissions with:

ls -ld authorized\_keys

Checking the permissions of the authorized_keys file

The file owner should have read and write permissions. To set them, use:

chmod 0600 /home/[username]/.ssh/authorized\_keys

Now try logging in with the key pair again. The output below shows a successful login attempt.

