[You can check if the authorized\_keys file has been set up correctly by following these steps1](https://askubuntu.com/questions/881353/test-that-i-have-correctly-added-someones-public-key-to-authorized-keys)[2](https://www.howtouselinux.com/post/ssh-authorized_keys-file):

1. Open a terminal window on your Ubuntu server.
2. Navigate to the .ssh directory using the following command:
3. cd ~/.ssh
4. [Type the following command to view the content of the authorized\_keys file:](https://www.howtouselinux.com/post/ssh-authorized_keys-file" \t "_blank)
5. [cat authorized\_keys](https://www.howtouselinux.com/post/ssh-authorized_keys-file" \t "_blank)

[This will display the content of the file in the terminal](https://www.howtouselinux.com/post/ssh-authorized_keys-file" \t "_blank)[2](https://www.howtouselinux.com/post/ssh-authorized_keys-file).

[You should see output similar to the following1](https://askubuntu.com/questions/881353/test-that-i-have-correctly-added-someones-public-key-to-authorized-keys):

-rw------- 1 example.com example.com 398 Jul 15 10:32 authorized\_keys

[Note that the directory needs to include the file called authorized\_keys with -rw------- (600) permissions1](https://askubuntu.com/questions/881353/test-that-i-have-correctly-added-someones-public-key-to-authorized-keys).

[Finally, run this command to check the permissions on your .ssh directory1](https://askubuntu.com/questions/881353/test-that-i-have-correctly-added-someones-public-key-to-authorized-keys):

ls -ld ~/.ssh

[You should have a folder called .ssh with drwx------ (700) permissions1](https://askubuntu.com/questions/881353/test-that-i-have-correctly-added-someones-public-key-to-authorized-keys).

[If for either of these tests, you get blank output, or a message similar to the following1](https://askubuntu.com/questions/881353/test-that-i-have-correctly-added-someones-public-key-to-authorized-keys):

ls: /root/.ssh: No such file or directory

[Please repeat the steps above1](https://askubuntu.com/questions/881353/test-that-i-have-correctly-added-someones-public-key-to-authorized-keys).

Remember, these are general steps and might need to be adjusted based on your specific environment. If you’re still facing issues, please provide more details about your environment. It would help in providing a more accurate guidance. Also, make sure that your GitLab runner has the necessary permissions to execute SSH commands. If it doesn’t, you might need to add the runner’s public SSH key to the authorized\_keys file on your server. If you’re not sure how to do this, I can guide you through the process. Just let me know!

Learn more

[1askubuntu.com](https://askubuntu.com/questions/881353/test-that-i-have-correctly-added-someones-public-key-to-authorized-keys)[2howtouselinux.com](https://www.howtouselinux.com/post/ssh-authorized_keys-file)[3askubuntu.com](https://askubuntu.com/questions/46424/how-do-i-add-ssh-keys-to-authorized-keys-file)[4systranbox.com](https://www.systranbox.com/where-is-my-authorized_keys-file-in-linux/)

You

i dont get any output so maby have to set it from first.

Copilot

If you don’t see any output when you run cat ~/.ssh/authorized\_keys, it means the authorized\_keys file is either empty or doesn’t exist. [You can set it up by following these steps1](https://askubuntu.com/questions/46424/how-do-i-add-ssh-keys-to-authorized-keys-file)[2](https://hostingultraso.com/help/ubuntu/how-set-public-key-authentication-ubuntu):

1. **Generate a new SSH key pair** on your local machine (the machine running the GitLab runner):
2. ssh-keygen -t rsa

This command generates a new SSH key pair. You’ll be asked to enter a file in which to save the key. You can press enter to use the default location (~/.ssh/id\_rsa). [You’ll also be asked to optionally enter a secure passphrase, which is recommended for additional security1](https://askubuntu.com/questions/46424/how-do-i-add-ssh-keys-to-authorized-keys-file).

1. **Display your public SSH key** with the following command:
2. cat ~/.ssh/id\_rsa.pub

This command will print your public SSH key to the terminal. [It should start with ssh-rsa](https://askubuntu.com/questions/46424/how-do-i-add-ssh-keys-to-authorized-keys-file)[1](https://askubuntu.com/questions/46424/how-do-i-add-ssh-keys-to-authorized-keys-file).

1. **Copy your public SSH key**. [You’ll need to add this key to the authorized\_keys file on your Ubuntu server1](https://askubuntu.com/questions/46424/how-do-i-add-ssh-keys-to-authorized-keys-file).
2. [**Log in to your Ubuntu server** and navigate to the .ssh directory in your home directory2](https://hostingultraso.com/help/ubuntu/how-set-public-key-authentication-ubuntu):
3. cd ~/.ssh
4. [**Open the**authorized\_keys**file** in a text editor2](https://hostingultraso.com/help/ubuntu/how-set-public-key-authentication-ubuntu):
5. nano authorized\_keys
6. [**Paste your public SSH key** into the authorized\_keys file2](https://hostingultraso.com/help/ubuntu/how-set-public-key-authentication-ubuntu). Save and close the file.
7. [**Set the correct permissions** for the .ssh directory and authorized\_keys file2](https://hostingultraso.com/help/ubuntu/how-set-public-key-authentication-ubuntu):
8. chmod 700 ~/.ssh
9. chmod 600 ~/.ssh/authorized\_keys

Now your GitLab runner should be able to execute SSH commands on your Ubuntu server using the SSH key pair. If you’re still facing issues, please provide more details about your environment. It would help in providing a more accurate guidance. Just let me know!

Learn more

[1askubuntu.com](https://askubuntu.com/questions/46424/how-do-i-add-ssh-keys-to-authorized-keys-file)[2hostingultraso.com](https://hostingultraso.com/help/ubuntu/how-set-public-key-authentication-ubuntu)[3digitalocean.com](https://www.digitalocean.com/community/tutorials/how-to-set-up-ssh-keys-on-ubuntu-20-04)[4linuxstart.com](https://www.linuxstart.com/ubuntu-authorized-keys/)[5linuxize.com](https://linuxize.com/post/how-to-set-up-ssh-keys-on-ubuntu-1804/)

You

how to Note that the directory needs to include the file called authorized\_keys with -rw------- (600) permissions.

Copilot

[To set the authorized\_keys file with -rw------- (600) permissions, you can use the chmod command in your terminal1](https://superuser.com/questions/677996/permission-denied-on-authorized-key-file). Here are the steps:

1. Open a terminal window.
2. Navigate to the .ssh directory in your home directory:
3. cd ~/.ssh
4. Set the permissions for the authorized\_keys file to 600:
5. chmod 600 authorized\_keys

[This command sets the permissions of the authorized\_keys file to -rw-------, which means the owner can read and write the file, but no other user can access the file](https://superuser.com/questions/677996/permission-denied-on-authorized-key-file)[1](https://superuser.com/questions/677996/permission-denied-on-authorized-key-file).

Remember, these are general steps and might need to be adjusted based on your specific environment. If you’re still facing issues, please provide more details about your environment. It would help in providing a more accurate guidance. Just let me know!

Learn more

[1superuser.com](https://superuser.com/questions/677996/permission-denied-on-authorized-key-file)[2askubuntu.com](https://askubuntu.com/questions/46424/how-do-i-add-ssh-keys-to-authorized-keys-file)[3stackoverflow.com](https://stackoverflow.com/questions/6377009/adding-a-public-key-to-ssh-authorized-keys-does-not-log-me-in-automatically)[4askubuntu.com](https://askubuntu.com/questions/466549/bash-home-user-ssh-authorized-keys-no-such-file-or-directory)

You

You should have a folder called .ssh with drwx------ (700) permissions1.

Copilot

Yes, that’s correct. The .ssh directory should have drwx------ (700) permissions. [This means the owner of the directory has read, write, and execute permissions, and no other user can access the directory](https://superuser.com/questions/215504/permissions-on-private-key-in-ssh-folder)[1](https://superuser.com/questions/215504/permissions-on-private-key-in-ssh-folder).

[You can set the permissions for the .ssh directory to 700 using the chmod command](https://superuser.com/questions/215504/permissions-on-private-key-in-ssh-folder)[2](https://www.tecmint.com/set-ssh-directory-permissions-in-linux/). Here’s how:

1. Open a terminal window.
2. Navigate to your home directory:
3. cd ~
4. Set the permissions for the .ssh directory:

chmod 700 .ssh