Why Key Authorization is not working?

596 Rakhi March 26, 2025 Common Errors & Troubleshooting 1991

Why key authorization is not working in a remote server through the gateway?

Overview: This article describes troubleshooting steps to resolve key authorization issues in a remote server accessed through a gateway. It covers enabling PubKeyAuthentication, verifying SSH configurations, resetting fingerprints, checking logs, and ensuring SSH key types are correctly configured.

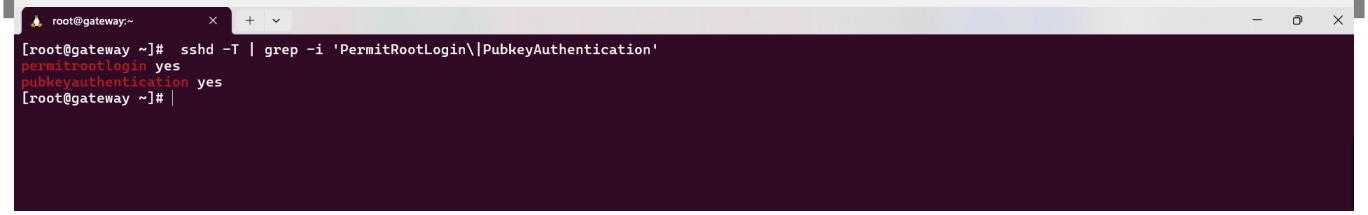
Even after setting up the remote server in the gateway machine and appending the public key to /root/.ssh/authorized_keys, you may still be prompted for a password when trying to log in. Below are possible reasons and solutions.

Troubleshooting steps:

Step 1: Check whether the PubKeyAuthentication is enabled on the sshd conf of the remote server.

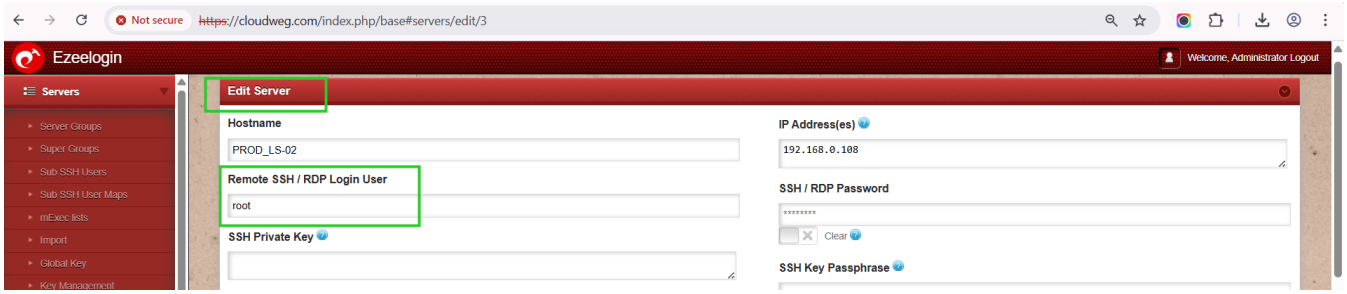
Ensure that public key authentication is enabled in the SSH daemon configuration on the remote server. Modify the configuration and restart the SSH service:

```
root@gateway:~# echo "PermitRootLogin  yes|PubkeyAuthentication  yes"
>> /etc/ssh/sshd_config

root@gateway:~# systemctl restart sshd

root@gateway:~# sshd -T | grep -i
'PermitRootLogin|PubkeyAuthentication'
```



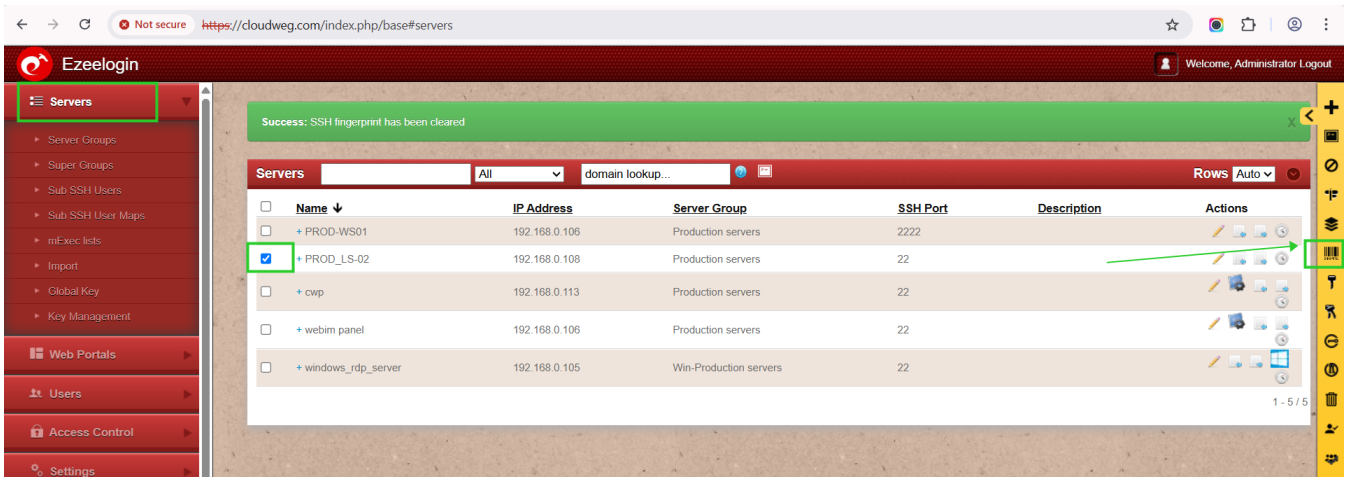
Step 2: Confirm that the remote server is added with the remote username "root".

Ensure that the remote server is configured with the correct username, typically "root" for administrative access.



Step 3: Reset the fingerprint of the remote Server.

If there is a fingerprint mismatch, reset the fingerprint and attempt to reconnect.



Step 4: Restart sshd service After resetting try to reset sshd and try to re-login to ezsh.

After resetting the fingerprint, restart the SSH service and attempt to log in again using the ezsh (ezeelogin shell):

```
root@gateway:~# systemctl restart sshd
```

Step 5: Check the latest SSH logs for any errors.

Examine the authentication logs for potential errors that could be causing authentication failures.

```
root@remote_server:~# tail -f /var/log/auth.log  //If the remote server is Ubuntu

root@remote_server:~# tail -f /var/log/secure  //If the remote server is CentOS
```

Step 6: Verify the enabled keys.

Run the following command to confirm the accepted key types. The output should list the supported

public key algorithms. If certain keys are missing, additional configurations may be needed.

```
root@gateway:~# sshd -T|grep -i key

pubkeyacceptedalgorithms ssh-ed25519-cert-v01@openssh.com,ecdsa-sha
2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openss
h.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-
v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha
2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed
25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,s
k-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-
sha2-512,rsa-sha2-256
```

Step 7: Add ssh-rsa to sshd conf in the remote server.

In Ubuntu 22, ssh-rsa is disabled by default, so you need to enter it manually.

```
root@gateway:~# echo "PubkeyAcceptedKeyTypes ssh-rsa" >>
/etc/ssh/sshd_config
```

(8) Re-run the below command and confirm that ssh-rsa has been enabled.

```
root@gateway:~# sshd -T | grep -i key

pubkeyacceptedalgorithms ssh-ed25519-cert-v01@openssh.com,ecdsa-sha
2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openss
h.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-
v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha
2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed
25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,s
k-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-
sha2-512,rsa-sha2-256,ssh-rsa
```

Related Articles:

Add ssh pubkey for passwordless authentication in ssh.

Authentication by ssh key failed.

Error log file and config file to troubleshoot.

Online URL: https://www.ezeelogin.com/kb/article/why-key-authorization-is-not-working-596.html