

Error: User modify failed. Cannot modify user on this node: Authentication by SSH key failed!

24 admin September 26, 2024 [Common Errors & Troubleshooting](#) 10391

How to solve Error: User modify failed. Cannot modify user on this node: Authentication by SSH key failed!?

Overview: This article provides step-by-step instructions for troubleshooting the error "Error: User modify failed. Cannot modify user on this node: Authentication by SSH key failed!" encountered when modifying the gateway user.

The screenshot shows the Ezeelogin web interface. At the top, there is a red banner with the error message: "Error: User modify failed. Cannot modify user on this node: Authentication by SSH key failed!". Below the banner, there is a form titled "Change password and/or security code - John". The form has several input fields: "New Password", "Confirm Password", "New Security Code", "Confirm Security Code", "Clear Two-Factor Authentication Secret", and "Authorization Password". There are also "Generate" buttons for the password and security code fields, and "Cancel" and "Save" buttons at the bottom. Below the form, there is a table of users. The table has columns: Username, First Name, Last Name, Email, Status, Expiry, User Group, and Actions. The table contains two rows: "John" (Active, Dummy group) and "admin" (Active, Admins group). The "John" row is selected.

Username	First Name	Last Name	Email	Status	Expiry	User Group	Actions
John	John		john@gmail.com	Active		Dummy	[Icons]
admin	Administrator			Active		Admins	[Icons]

Step 1: Check if the Gateway server (Ezeelogin installed server) is missing its public key from `/root/.ssh/authorized_keys` file. If the key is missing, run the following command to add it:

```
root@gateway:~# cat /usr/local/etc/ezlogin/id_clkey.pub >> /root/.ssh/authorized_keys
```

Step 1(A): Run the below command to check if the key is back in the file.

```
root@gateway:~# cat /root/.ssh/authorized_keys
```

Step 2: Run the following command to verify if the recommended SSHD settings are enabled in the `/etc/ssh/sshd_config` file.

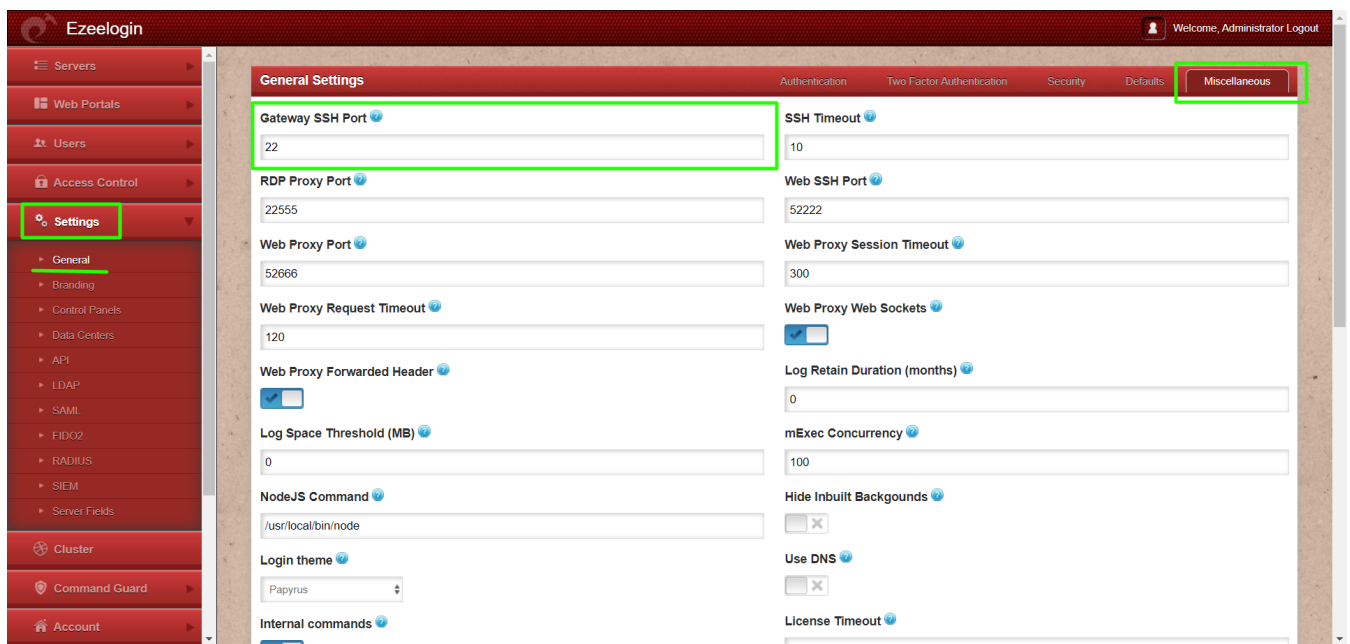
```
root@gateway:~# sshd -T | grep -i 'AllowTcpForwarding|PermitRootLogin
|PubkeyAuthentication|PasswordAuthentication|pubkeyacceptedalgorithms
|Port'

port 22
permitrootlogin yes
pubkeyauthentication yes
passwordauthentication yes
gatewayports no
allowtcpforwarding no
pubkeyacceptedalgorithms ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-
nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.co
m,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@op
enssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-ce
rt-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecds
a-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-
ed25519@openssh.com,sk-ecdsa-
sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-rsa
```

Step 3: Verify the SSH port used on the gateway server with the following command.

```
root@gateway:~# cat /etc/ssh/sshd_config | grep Port
Port 22
#Gateway Ports no
```

Step 3(A): If a [custom SSHD port](#) is being used on the gateway server, ensure it is updated under **Settings -> General -> Miscellaneous -> Gateway SSH Port** to match the current SSHD listening port on the SSH gateway server.



Step 4: Make sure **PubkeyAuthentication** is set to 'YES' in the **SSHD** configuration file.

```
root@gateway:~# vi /etc/ssh/sshd_config

#set PubkeyAuthentication to yes

PubkeyAuthentication yes
```

Stepp 4(A): After making changes restart SSHD

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

Step 5: Ensure that **root login** is permitted on the gateway server. You can check this by running the command:

```
root@gateway:~# ssh root@localhost
```

Step 5(A): If it does not log you in, edit **/etc/ssh/sshd_config** and set **PermitRootLogin** to **yes** and restart SSHD.

```
root@gateway:~# vi /etc/ssh/sshd_config
```

#Add the following lines to the end of /etc/ssh/sshd_config to allow root login from localhost only

```
Match Address 127.0.0.1
```

```
PermitRootLogin yes
```

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

Step 5(B): After making the changes, ensure that you can log in as root by using the following command and entering the password:

```
ssh root@localhost:~#
```

Step 6: Ensure that the **web user** (such as Apache or nobody) that the web server (Apache/Nginx) runs has **read** access to the keys in the directory **/usr/local/etc/ezlogin** by granting **read privileges** with the following command:

```
root@gateway:~# chmod o+r /usr/local/etc/ezlogin/id_clkey
root@gateway:~# chmod o+r /usr/local/etc/ezlogin/id_clkey.pub
or
root@gateway:~# usermod -G <current_groupname_of_id_clkey_files>
<webserver_user>
```

Step 7: Find out which key type is used by the gateway server by running the below command.

```
root@gateway:~# ssh-keygen -l -f
/usr/local/etc/ezlogin/id_key.pub
```

```
4096 SHA256:n4lmX53/gwkKB4+nSQ30hZXxXK+DRG1LPc7NlKN/1Ag ezlogin (RSA)
```

Step 7(A): Open `/etc/ssh/sshd_config` file and append the below line to **enable RSA** key type and restart SSHD.

```
root@gateway:~# vi /etc/ssh/sshd_config
```

```
PubkeyAcceptedKeyTypes +ssh-rsa
```

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

Step 8: Check for the SSHD error logs of the gateway server.

For CentOS

```
root@gateway:~# /var/log/secure
```

For Ubuntu

```
root@gateway:~# /var/log/auth.log
```

Refer to the below article if you get "**userauth_pubkey: signature algorithm ssh-rsa not in PubkeyAcceptedAlgorithms**"

[userauth_pubkey: signature algorithm ssh-rsa not in PubkeyAcceptedAlgorithms](#)

Related Articles:

[Error: User modify failed. Cannot modify user on other node: Authentication by SSH key failed!](#)

[Error: User modify failed Cannot modify user on this node: OS=FreeBSD: Command not found. OS: Undefined](#)

[Reset Ezeelogin keys used for privilege escalation.](#)

Online URL:

<https://www.ezeelogin.com/kb/article/error-user-modify-failed-cannot-modify-user-on-this-node-authentication-by-ssh-key-failed-24.html>