

## userauth\_pubkey: signature algorithm ssh-rsa not in PubkeyAcceptedAlgorithms

518 Nesvin KN March 3, 2023 [Common Errors & Troubleshooting](#) 13885



**EZEELOGIN**

**Record, monitor and track SSH sessions of your employees**

**30 Days Free Trial**

## userauth\_pubkey: signature algorithm ssh-rsa not in PubkeyAcceptedAlgorithms

1. Login to server and tail `/var/log/secure` to check errors. Refer below example.

```
root@gateway ~]# tail -f /var/log/secure  
userauth_pubkey: signature algorithm ssh-rsa not in
```

```
PubkeyAcceptedAlgorithms
```

2. Find which key type is used in the server by running the below command.

```
root@gateway ~]# ssh-keygen -l -f /usr/local/etc/ezlogin/id_key.pub
4096 SHA256:n4lmX53/gwkKB4+nSQ30hZXxXK+DRG1LPc7N1KN/1Ag ezlogin (RSA)
```

In the above example, the RSA key type is used.

3. Run the following command to see which all key types are enabled on the server.

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

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-ed2551
9@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-
sha2-256
```

4. Open `/etc/ssh/sshd_config` and append the below line to enable ssh-rsa.

```
root@gateway ~]# vim /etc/ssh/sshd_config

PubkeyAcceptedKeyTypes +ssh-rsa

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

5. 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-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
```

6. Try to modify the user now and confirm it's working fine.

## How to view the list of KEX and Keys in the Linux server?

- How to list **keys** in the Linux server?

```
root@linux ~]# ssh -Q key  
  
ssh-ed25519  
ssh-ed25519-cert-v01@openssh.com  
ssh-rsa  
ssh-dss  
ecdsa-sha2-nistp256  
ecdsa-sha2-nistp384  
ecdsa-sha2-nistp521  
ssh-rsa-cert-v01@openssh.com  
ssh-dss-cert-v01@openssh.com  
ecdsa-sha2-nistp256-cert-v01@openssh.com  
ecdsa-sha2-nistp384-cert-v01@openssh.com  
ecdsa-sha2-nistp521-cert-v01@openssh.com
```

- How to list **KEX** in the Linux server?

```
root@linux ~]# ssh -Q kex  
  
diffie-hellman-group1-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group14-sha256  
diffie-hellman-group16-sha512  
diffie-hellman-group18-sha512  
diffie-hellman-group-exchange-sha1  
diffie-hellman-group-exchange-sha256  
ecdh-sha2-nistp256  
ecdh-sha2-nistp384  
ecdh-sha2-nistp521  
curve25519-sha256  
curve25519-sha256@libssh.org
```

## Related Articles

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

Online URL:

[https://www.ezeelogin.com/kb/article/userauth\\_pubkey-signature-algorithm-ssh-rsa-not-in-pubkeyacceptedalgorithms-518.html](https://www.ezeelogin.com/kb/article/userauth_pubkey-signature-algorithm-ssh-rsa-not-in-pubkeyacceptedalgorithms-518.html)