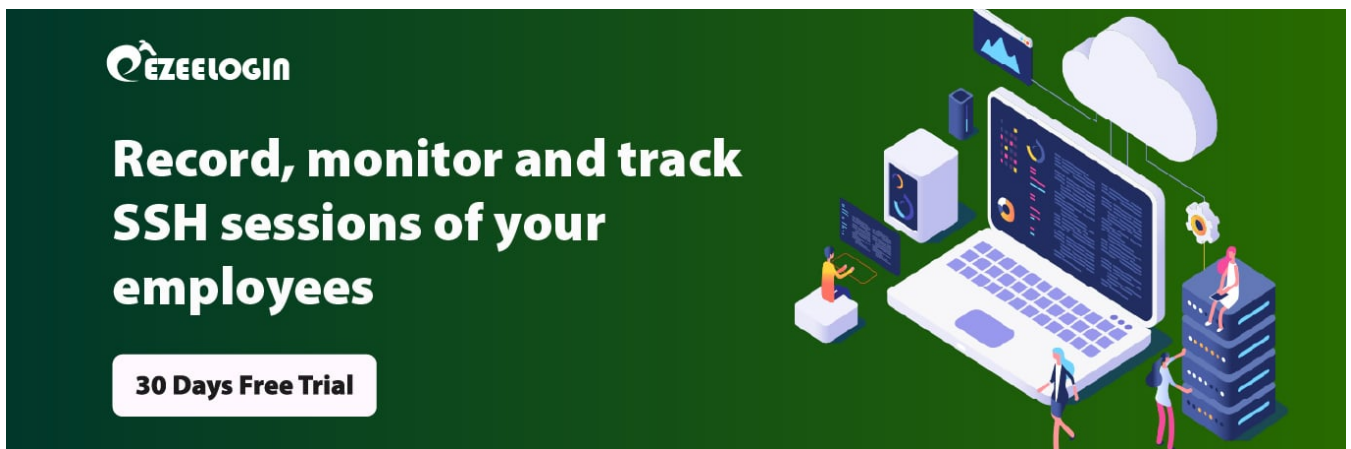


signature algorithm ssh-dss not in PubkeyAcceptedAlgorithms

554 admin April 4, 2024 [Common Errors & Troubleshooting](#) 5632



How to fix "userauth_pubkey: signature algorithm ssh-dss not in PubkeyAcceptedAlgorithms"

In order to change ssh-dss key to ssh-rsa, follow below article.

[How to reset cluster keys in Ezeelogin?](#)

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

```
root@gateway ~]# tail -f /var/log/auth.log  
  
userauth_pubkey: key type ssh-dss not in PubkeyAcceptedKeyTypes [preauth]
```

2. Run the following command to see the key types enabled on the server.

```
root@locker:~# sshd -T | grep -i key  
  
pubkeyacceptedkeytypes ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-  
-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@open  
ssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,ssh-ed25519-cert-  
v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,rsa-sha2-512-cert
```

```
-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ecdsa-sha2-nistp256@openssh.com,ssh-ed25519,sk-ssh-ed25519@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-rsa
```

3. Open `/etc/ssh/sshd_config` and append the below line to **enable ssh-dss**.

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

PubkeyAcceptedKeyTypes +ssh-dss

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

4. Re-run the below command and confirm that **ssh-dss** has been enabled.

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

pubkeyacceptedkeytypes ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ecdsa-sha2-nistp256@openssh.com,ssh-ed25519,sk-ssh-ed25519@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-rsa,ssh-dss
```

5. 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

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

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/signature-algorithm-ssh-dss-not-in->

