signature algorithm ssh-dss not in PubkeyAcceptedAlgorithms

554 admin January 14, 2026 Common Errors & Troubleshooting 13339



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

Overview: This article describes how to fix the **"userauth_pubkey: signature algorithm ssh-dss not in PubkeyAcceptedAlgorithms"** error by enabling ssh-dss in the SSH configuration and restarting the service.

Step 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]
```

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

```
root@gateway :~# 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
```

Step 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
```

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

```
root@gateway :~# 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**

Step 5: Try to modify the user now and confirm it's working fine.

We highly recommend regenerating the cluster keys, as the new keys support modern and secure key types such as ed25519 and ecdsa, since ssh-dss key type is deprecated and no longer supported by recent OpenSSH versions due to security concerns.

Refer article to regenerate cluster key: **https://www.ezeelogin.com/kb/article/how-to-reset-cluster-keys-in-ezeelogin-master-slave-configuration-219.html**

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

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

```
root@gateway :~# 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@gateway :~# 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-pubkeyacceptedalgorithms-554.html