List of supported SSH Keys & Algorithms

573 Nesvin KN October 27, 2025 General, Technical 9903

What are the supported PubkeyAcceptedKeyTypes, KEX, and HostKeyAlgorithms in the ezsh shell?

Overview: This article outlines the supported **PubkeyAcceptedKeyTypes, KEX(Key Exchange Algorithms), and HostKeyAlgorithms** in the **ezsh shell** (Ezeelogin backend shell) and their compatibility details.

Refer to the article below for guidance on finding and modifying the KEX and HostKeyAlgorithms used by the SSHD server:

KEX and Host Key Algorithms in SSH

Supported PubkeyAcceptedKeyType in Ezeelogin

PubkeyAcceptedKeyType supported from **Ezeelogin version 7.30.0**

Key Compatibility Notes:

1. The ed25519 key generated with the passphrase on Centos 7 is not supported.

2. The PHP version should be 7.3 and above in Almalinux 8, RHEL8, CentOS8, and RockyLinux to save the key in the Ezeelogin GUI.

3. Refer below articles to resolve the DSA key-based authentications.
DSA key-based authentication is not working
signature algorithm ssh-dss not in PubkeyAcceptedAlgorithms

Supported Pubkey Types:

1. rsa
2. dsa
3. ed25519
4. ecdsa
5. OpenSSH

Supported KEX and HostKeyAlgorithms in Ezeelogin

Below are the supported and unsupported KEX (Key Exchange) and HostKeyAlgorithms on **Ezeelogin version 7.29.11**

Supported KEX algorithms:

curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha256
diffie-hellman-group14-sha1
diffie-hellman-group1-sha1

Supported HostKeyAlgorithms:

ecdsa-sha2-nistp256
ssh-ed25519
ssh-rsa
ssh-dss
rsa-sha2-512
rsa-sha2-256

Unsupported HostKeyAlgorithms:

ecdsa-sha2-nistp256-cert-v01@openssh.com
ecdsa-sha2-nistp384-cert-v01@openssh.com
ecdsa-sha2-nistp521-cert-v01@openssh.com
ssh-ed25519-cert-v01@openssh.com
ssh-rsa-cert-v01@openssh.com
ssh-dss-cert-v01@openssh.com
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
sk-ecdsa-sha2-nistp256-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
sk-ecdsa-sha2-nistp256@openssh.com
sk-ssh-ed25519@openssh.com

Related Articles:

Upgrade Ezeelogin Jump server to the latest version

KEX and Host Key Algorithms in SSH

Failure establishing SSH session: Unable to exchange encryption keys

Convert existing key format to PEM format

DSA key based authentication is not working

userauth_pubkey: signature algorithm ssh-rsa not in PubkeyAcceptedAlgorithms

signature algorithm ssh-dss not in PubkeyAcceptedAlgorithms

Encryption Technologies used in Ezeelogin

Online URL: https://www.ezeelogin.com/kb/article/list-of-supported-ssh-keys-algorithms-573.html