# HACPE EE FTP/VT SSH Support List

Secure Shell (SSH) is a widely used Transport Layer Protocol to secure connections between clients and servers. The SSH handshake is a process in the SSH protocol responsible for negotiating initial trust factors to establish a secure channel between an SSH client and an SSH server for an SSH connection. The ciphers, algorithms, and key format supported by HACP EE - FTP/VT SSH protocols are listed below.

## FTP/VT SSH Support List

## Ciphers:

*Default list (in order from most to least preferable):*

chacha20-poly1305@openssh.com (priority of chacha20-poly1305 may vary depending upon CPU and/or optional binding availability)

aes128-gcm

aes128-gcm@openssh.com

aes256-gcm

aes256-gcm@openssh.com

aes128-ctr

aes192-ctr

aes256-ctr

3des-cbc

aes256-cbc

aes192-cbc

aes128-cbc

## Compression algorithms:

*Default list (in order from most to least preferable):*

none

zlib@openssh.com

zlib

## (H)MAC algorithms:

*Default list (in order from most to least preferable):*

hmac-sha2-256-etm@openssh.com

hmac-sha2-512-etm@openssh.com

hmac-sha1-etm@openssh.com

hmac-sha2-256

hmac-sha2-512

hmac-sha1

hmac-md5

hmac-sha2-256-96

hmac-sha2-512-96

hmac-ripemd160

hmac-sha1-96

hmac-md5-96

## Key exchange algorithms:

*Default list (in order from most to least preferable):*

curve25519-sha256 (node v14.0.0+)

curve25519-sha256@libssh.org (node v14.0.0+)

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256

diffie-hellman-group14-sha256

diffie-hellman-group15-sha512

diffie-hellman-group16-sha512

diffie-hellman-group17-sha512

diffie-hellman-group18-sha512

diffie-hellman-group-exchange-sha1

diffie-hellman-group14-sha1

diffie-hellman-group1-sha1

## Server host key formats:

*Default list (in order from most to least preferable):*

ssh-ed25519 (node v12.0.0+)

ecdsa-sha2-nistp256

ecdsa-sha2-nistp384

ecdsa-sha2-nistp521

rsa-sha2-512

rsa-sha2-256

ssh-rsa

ssh-dss