Supported SSH cryptography

Please note we have updated our SSH client starting with Unimus 2.2.3. The table below applies to version 2.2.3 or newer.

Default Unimus cryptography configuration

Unimus contains its own built-in SSH client. Please note when running on Linux, configuration of your OpenSSH client ("~/.ssh") is NOT applied to Unimus' SSH client.
Currently the Unimus SSH client supports the following cryptography for outbound device connections:

Supported KEX:

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

Supported ciphers:

```
3des-cbc, 3des-ctr, aes128-cbc, aes128-ctr, aes128-gcm@openssh.com,
aes192-cbc, aes192-ctr,
aes256-cbc, aes256-ctr, aes256-gcm@openssh.com, blowfish-cbc
```

Supported MAC:

```
hmac-md5, hmac-md5-96, hmac-sha1, hmac-sha1-96, hmac-sha1-etm@openssh.com,
hmac-sha2-256,
hmac-sha2-256-etm@openssh.com, hmac-sha2-512, hmac-sha2-512-etm@openssh.com
```

Supported DH size:

```
DH min: 1024
DH max: 8192
```

Adjusting supported crypto algorithms

In some environments, you might have requirements on which SSH crypto algos you can use. In this case, you can adjust which algorithms Unimus accepts when connecting to a server.

You can set configuration options in the service config files to achieve this.

On Linux these are located in:

- "**/etc/default/unimus**" for Unimus Server
- "**/etc/default/unimus-core**" for Unimus Core

On Windows:

- "**C:\Program Files\Unimus\Unimus.l4j.ini**" for Unimus Server
- "**C:\Program Files\Unimus Core\Unimus Core.l4j.ini**" for Unimus Core

The options you can set are:

```
-Dunimus.core.ssh.kex=kex1,kex2,kex3,kex4,...kexX
-Dunimus.core.ssh.cipher=cipher1,cipher2,cipher3,cipher4,...cipherX
-Dunimus.core.ssh.mac=mac1,mac2,mac3,mac4,...macX
-Dunimus.core.ssh.dh-min=1024
-Dunimus.core.ssh.dh-preferred=2048
-Dunimus.core.ssh.dh-max=8192
```