

Troubleshoot PQC PPK Manual Key Hexadecimal Format Parser Rejection

Contents

Issue

When [configuring IPsec](#) (IP Security) on Cisco IOS XE with PQC (Post-Quantum Cryptography) and manual PPK (Post-Quantum Pre-shared Keys) in hex format, the device can reject the hex format PPK with either of these errors:

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5
```

```
% Invalid input detected at '^' marker.
```

```
Device(config-ikev2-keyring-peer)#
```

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c88
```

```
% Invalid hex key.All characters in hex string must be ASCII.
```

```
Device(config-ikev2-keyring-peer)#
```

Environment

- Cisco routers running Cisco IOS XE software
- IPsec using Post-Quantum Cryptography implementation with manual PPK keys

Resolution

The router validates decoded byte values with hexadecimal strings for the PPK manual key configuration. The decoded value must meet these two requirements:

- The hexadecimal encoded PPK must represent a valid ASCII string. Since each ASCII character is encoded using 8 bits, and each hex character represents 4 bits of information, the input hex string must consist of an even number of characters. For example, the hex string **3a4b5** is an invalid input since it has an odd number (5) of hexadecimal characters.
- The parser accepts hex values only if the decoded bytes remain within the standard ASCII byte range (0x00-0x7F). The problematic key **3a4b5c88** was rejected because:

```
0x3a = 58 (ascii ":") valid
0x4b = 75 (ascii "K") valid
0x5c = 92 (ascii "\") valid
0x88 = 136 invalid - outside of standard ASCII range
```

To resolve this error, use hexadecimal values where each byte remains within the standard ASCII range (0x00-0x7F), for example:

```
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c88
% Invalid hex key.All characters in hex string must be ASCII.
Device(config-ikev2-keyring-peer)#ppk manual id peer1 key hex 3a4b5c78
Device(config-ikev2-keyring-peer)#
```

Cause

Invalid PPK key input in hexadecimal format because it is outside of the [standard ASCII character](#) range (0x00-0x7F).

Related Content

- [Configuring Quantum-Safe Encryption Using Postquantum Preshared Keys](#)
- 'Cisco bug ID [CSCwn32983](#)'(Cisco internal bug to make parser error more clear)
- [Cisco Technical Support & Downloads](#)