

Problemen oplossen PQC PPK Handmatige Sleutel Hexadecimaal Formaat Parser Afwijzing

Inhoud

uitgifte

Bij het [configureren van IPsec](#) (IP-beveiliging) op Cisco IOS XE met PQC (Post-Quantum Cryptography) en handmatige PPK (Post-Quantum Pre-shared Keys) in hex-indeling, kan het apparaat de hex-indeling PPK weigeren met een van deze fouten:

```
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)#
```

milieu

- Cisco-routers met Cisco IOS XE-software
- IPsec met Post-Quantum Cryptography-implementatie met handmatige PPK-sleutels

resolutie

De router valideert gedecodeerde bytewaarden met hexadecimale tekenreeksen voor de

configuratie van de handmatige PPK-sleutel. De gedecodeerde waarde moet aan deze twee vereisten voldoen:

- De hexadecimale gecodeerde PPK moet een geldige ASCII-tekenreeks vertegenwoordigen. Aangezien elk ASCII-teken wordt gecodeerd met 8 bits en elk hexateken 4 bits informatie vertegenwoordigt, moet de invoerhexareeks uit een even aantal tekens bestaan. De hexadecimale tekenreeks 3a4b5 is bijvoorbeeld een ongeldige invoer omdat deze een oneven aantal (5) hexadecimale tekens heeft.
- De parser accepteert hex-waarden alleen als de gedecodeerde bytes binnen het standaard ASCII-bytebereik blijven (0x00-0x7F). De problematische sleutel 3a4b5c88 werd afgewezen omdat:

```
0x3a = 58 (ascii ":") valid
0x4b = 75 (ascii "K") valid
0x5C = 92 (ascii "\") valid
0x88 = 136 invalid - outside of standard ASCII range
```

Om deze fout op te lossen, gebruikt u hexadecimale waarden waarbij elke byte binnen het standaard ASCII-bereik blijft (0x00-0x7F), bijvoorbeeld:

```
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)#
```

Oorzaak

Ongeldige PPK-sleutel invoer in hexadecimale indeling omdat deze buiten het [standaard ASCII-tekenbereik](#) valt (0x00-0x7F).

Gerelateerde inhoud

- [Quantum-veilige codering configureren met behulp van vooraf gedeelde postquantum-sleutels](#)

- 'Cisco bug ID [CSCwn32983](#)'(Cisco interne bug om parser fout duidelijker te maken)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.