

Troubleshooting de PQC PPK Manual Key Hexadecimal Format Parser Reject

Contenido

Problema

Al [configurar IPsec](#) (IP Security) en Cisco IOS XE con PQC (Post-Quantum Cryptography) y PPK manual (Post-Quantum Pre-shared Keys) en formato hexadecimal, el dispositivo puede rechazar el formato hexadecimal PPK con cualquiera de estos errores:

```
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)#
```

Entorno

- Routers Cisco que ejecutan el software Cisco IOS XE
- IPSec con implementación de criptografía poscuántica con claves PPK manuales

Resolución

El router valida los valores de bytes decodificados con cadenas hexadecimales para la

configuración manual de claves PPK. El valor descodificado debe cumplir estos dos requisitos:

- El PPK codificado en hexadecimal debe representar una cadena ASCII válida. Dado que cada carácter ASCII se codifica con 8 bits y que cada carácter hexadecimal representa 4 bits de información, la cadena hexadecimal de entrada debe constar de un número par de caracteres. Por ejemplo, la cadena hexadecimal 3a4b5 es una entrada no válida, ya que tiene un número impar (5) de caracteres hexadecimales.
- El analizador acepta valores hexadecimales sólo si los bytes descodificados permanecen dentro del intervalo de bytes ASCII estándar (0x00-0x7F). La clave problemática 3a4b5c88 fue rechazada porque:

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

Para resolver este error, utilice valores hexadecimales en los que cada byte permanezca dentro del rango ASCII estándar (0x00-0x7F), por ejemplo:

```
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)#
```

Causa

Entrada de clave PPK no válida en formato hexadecimal porque está fuera del intervalo de [caracteres ASCII estándar](#) (0x00-0x7F).

Contenido relacionado

- [Configuración del cifrado Quantum-Safe con claves previamente compartidas poscuánticas](#)
- 'Id. de error de Cisco [CSCwn32983](#)'(error interno de Cisco para aclarar más el error del analizador)

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).