

Dépannage du rejet de l'analyseur de format hexadécimal de clé manuelle PQC PPK

Table des matières

Problème

Lors de la [configuration d'IPsec](#) (IP Security) sur Cisco IOS XE avec PQC (Post-Quantum Cryptography) et PPK manuel (Post-Quantum Pre-shared Keys) au format hexadécimal, le périphérique peut rejeter le format hexadécimal PPK avec l'une de ces erreurs :

```
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)#
```

Environnement

- Routeurs Cisco exécutant le logiciel Cisco IOS XE
- IPsec avec implémentation de cryptographie post-quantique avec clés PPK manuelles

Résolution

Le routeur valide les valeurs d'octets décodées à l'aide de chaînes hexadécimales pour la

configuration manuelle de la clé PPK. La valeur décodée doit répondre à ces deux exigences :

- Le code PPK hexadécimal doit représenter une chaîne ASCII valide. Étant donné que chaque caractère ASCII est codé à l'aide de 8 bits et que chaque caractère hexadécimal représente 4 bits d'information, la chaîne hexadécimale d'entrée doit être composée d'un nombre pair de caractères. Par exemple, la chaîne hexadécimale 3a4b5 est une entrée non valide car elle a un nombre impair (5) de caractères hexadécimaux.
- L'analyseur accepte les valeurs hexadécimales uniquement si les octets décodés restent dans la plage d'octets ASCII standard (0x00-0x7F). La clé problématique 3a4b5c88 a été rejetée pour les raisons suivantes :

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

Pour résoudre cette erreur, utilisez des valeurs hexadécimales où chaque octet reste dans la plage ASCII standard (0x00-0x7F), par exemple :

```
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)#
```

Motif

Entrée de clé PPK non valide au format hexadécimal, car elle se trouve en dehors de la plage de [caractères ASCII standard](#) (0x00-0x7F).

Autres informations utiles

- [Configuration du chiffrement Quantum Safe à l'aide de clés pré-partagées postquantum](#)
- 'ID de bogue Cisco [CSCwn32983](#)'(bugue interne Cisco pour clarifier l'erreur de l'analyseur)

- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.