

# Dépannage de l'échec de mise à jour des définitions TETRA avec erreur 3000

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit les étapes pour dépanner l'échec des définitions TETRA avec l'erreur 3000.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Terminaux sécurisés Cisco

### Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Connecteur Cisco Secure Endpoint (toute version)
- Wireshark (toute version)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

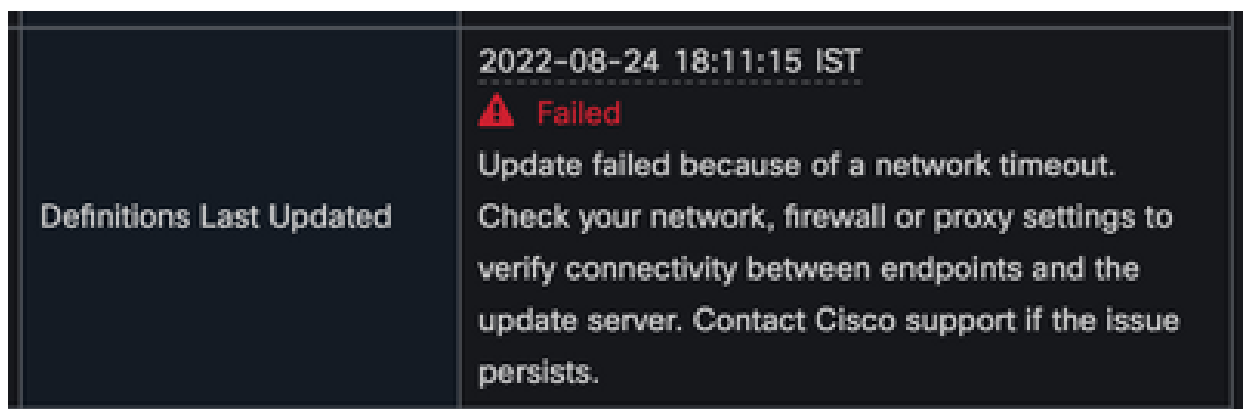
## Problème

1. Sur le terminal, la mise à jour des définitions TETRA échoue avec le message d'erreur « Impossible d'installer les mises à jour. Veuillez réessayer ultérieurement ».



2. Sur Cisco Secure Endpoint Console, l'erreur d'échec mentionnée est observée :

"La mise à jour a échoué en raison d'un délai réseau. Vérifiez les paramètres de votre réseau, de votre pare-feu ou de votre proxy pour vérifier la connectivité entre les terminaux et le serveur de mise à jour. Contactez l'assistance Cisco si le problème persiste. »



3. Dans debug sfc.exe.log, les définitions mises à jour ont échoué avec l'erreur 3000 error is observed, qui signifie Unknown\_Error comme documenté.

<#root>

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdateInterface::update updateDir: C:\Progr
(978223515, +0 ms) Aug 04 07:30:23 [11944]: ERROR: TETRAUpdateInterface::update
```

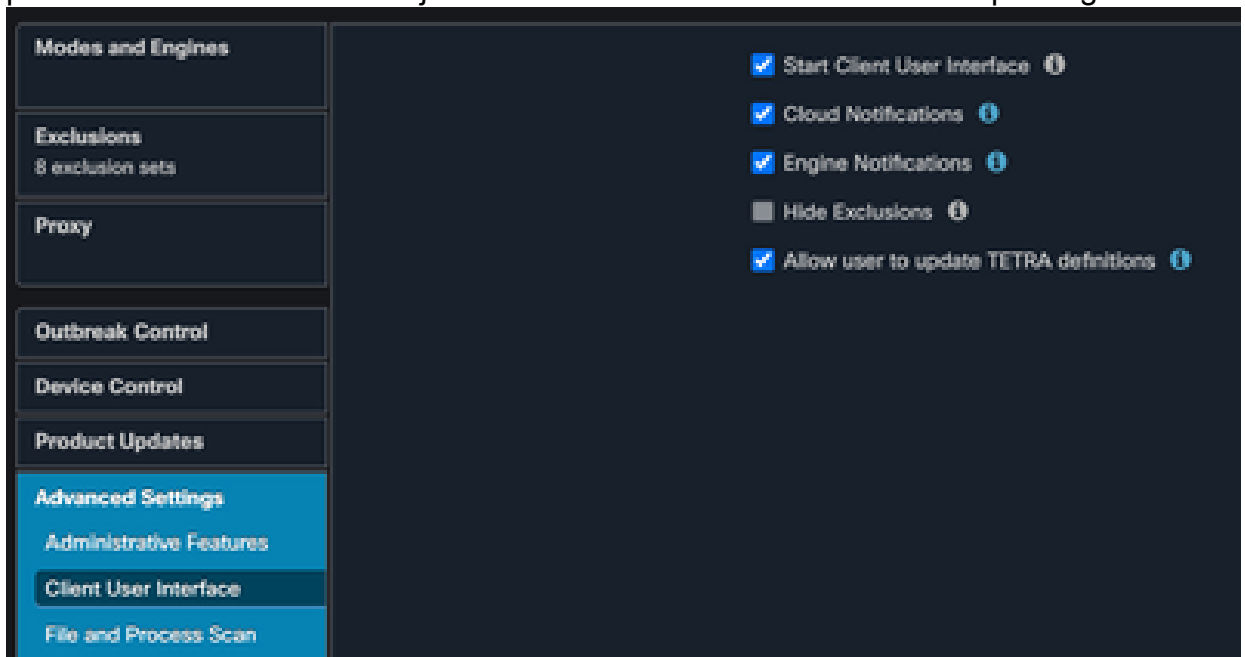
Update failed with error -3000

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PipeSend: sending message to user interface: 26,
(978223515, +0 ms) Aug 04 07:30:23 [860]: PipeWrite: waiting on pipe event handle
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit defInit: 0, bUpdate: 0
```

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit bUpdate: 0, bReload: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: FASharedPtr<class TETRAUpdateInterface>::Release
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: bUpdated = FALSE, state: 20,
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: sig count: 0, version: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: Config::IsUploadEventEnabled: returns 1, 1
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
```

## Solution

1. Activez l'option Autoriser l'utilisateur à mettre à jour les définitions TETRA dans Stratégie AMP > Interface utilisateur client sur la console. Avec ce paramètre, vous pouvez déclencher la mise à jour TETRA selon les besoins lors du dépannage.



2. Activez également la commande debug Connector et Tray-level log sur le terminal ou via AMP Policy.
3. Effectuez des captures de paquets sur le point de terminaison de la mise à jour TETRA réussie et échouée pour les définitions TETRA pendant que vous cliquez sur Mettre à jour TETRA sur le point de terminaison.
4. Sur le terminal de mise à jour TETRA réussie, dans la capture de paquets, filtrez les paquets avec `http.host == "tetra-defs.amp.cisco.com:443"` et ensuite "suivez le `tcp.stream`" de chaque paquet pour analyser le trafic associé.
5. Dans le paquet Server Hello, vous pouvez voir que le serveur accepte le chiffrement `"TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"` dans le paquet Server Hello.

No.	Time	Source	Destination	Protocol	Length	Info
169	17:54:13.501878			TCP	68	60649 → 6050 [SYN, ECN, CWR] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
170	17:54:13.501885			TCP	68	6050 → 60649 [SYN, ACK, ECN] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
171	17:54:13.501321			TCP	62	60649 → 6050 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
172	17:54:13.501438			HTTP	141	CONNECT tetra-defs.amp.cisco.com:443 HTTP/1.1
173	17:54:13.501449			TCP	56	6050 → 60649 [ACK] Seq=1 Ack=86 Win=29312 Len=0
174	17:54:13.519661			HTTP	155	HTTP/1.1 200 Connection established
175	17:54:13.520100			TLSv1..	255	Client Hello
176	17:54:13.559831			TCP	56	6050 → 60649 [ACK] Seq=100 Ack=285 Win=30336 Len=0
181	17:54:17.326736			TLSv1..	7356	Server Hello
182	17:54:17.326748			TLSv1..	1343	Certificate, Server Key Exchange, Server Hello Done
183	17:54:17.327138			TCP	62	60649 → 6050 [ACK] Seq=285 Ack=8687 Win=2102272 Len=0
184	17:54:17.329911			TLSv1..	182	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
185	17:54:17.329925			TCP	56	6050 → 60649 [ACK] Seq=8687 Ack=411 Win=30336 Len=0
186	17:54:17.784930			TLSv1..	346	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
187	17:54:17.785908			TLSv1..	355	Application Data
188	17:54:17.785921			TCP	56	6050 → 60649 [ACK] Seq=8977 Ack=710 Win=31360 Len=0
189	17:54:18.134677			TLSv1..	7356	Application Data
190	17:54:18.134689			TCP	6924	6050 → 60649 [PSH, ACK] Seq=16277 Ack=710 Win=31360 Len=6868 [TCP segment of a reassembled PDU]
191	17:54:18.135276			TCP	62	60649 → 6050 [ACK] Seq=710 Ack=23145 Win=2102272 Len=0
192	17:54:18.370829			TLSv1..	9680	Application Data [TCP segment of a reassembled PDU]
193	17:54:18.370461			TCP	62	60649 → 6050 [ACK] Seq=710 Ack=32769 Win=2102272 Len=0
194	17:54:18.370471			TCP	4600	6050 → 60649 [PSH, ACK] Seq=32769 Ack=710 Win=31360 Len=4544 [TCP segment of a reassembled PDU]
195	17:54:18.370783			TCP	62	60649 → 6050 [ACK] Seq=710 Ack=35689 Win=2102272 Len=0
196	17:54:18.370839			TCP	62	60649 → 6050 [ACK] Seq=710 Ack=37313 Win=2102272 Len=0
197	17:54:18.640187			TLSv1..	2799	Application Data, Encrypted Alert
198	17:54:18.640464			TCP	62	60649 → 6050 [ACK] Seq=710 Ack=40056 Win=2102272 Len=0

```

[Proxy-Connect-Port: 443]
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 65
    Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 61
      Version: TLS 1.2 (0x0303)
      Random: d19d47a9913f35df7270c3acee595422552881e62044737e9ee4e5fe776255
      Session ID Length: 0
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Compression Method: null (0)
      Subsequent Length: 31
  
```

6. Le serveur Cisco Secure Endpoint TETRA accepte uniquement les chiffrements mentionnés :

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_AES\_128\_GCM\_SHA256

7. Sur le point d'extrémité en échec de la mise à jour TETRA, dans la capture de paquets, une erreur fatale dans la connexion SSL est observée après le paquet Hello du client.

8. Dans le paquet Client Hello, vous pouvez voir les chiffrements proposés à partir du

No.	Time	Source	Destination	Protocol	Length	Info
245	16:57:17.390368			TCP	68	51771 → 6050 [SYN, ECN, CWR] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
246	16:57:17.390400			TCP	68	6050 → 51771 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
247	16:57:17.390587			TCP	62	51771 → 6050 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
248	16:57:17.390766			HTTP	141	CONNECT tetra-defs.amp.cisco.com:443 HTTP/1.1
249	16:57:17.390785			TCP	56	6050 → 51771 [ACK] Seq=1 Ack=86 Win=29312 Len=0
250	16:57:17.396776			HTTP	155	HTTP/1.1 200 Connection established
251	16:57:17.397250			TLSv1..	233	Client Hello
252	16:57:17.436829			TCP	56	6050 → 51771 [ACK] Seq=100 Ack=263 Win=30336 Len=0
257	16:57:17.984309			TLSv1..	63	Alert (Level: Fatal, Description: Handshake Failure)
258	16:57:17.984759			TCP	62	51771 → 6050 [FIN, ACK] Seq=263 Ack=187 Win=2102272 Len=0
268	16:57:18.023820			TCP	56	6050 → 51771 [ACK] Seq=187 Ack=264 Win=30336 Len=0
269	16:57:18.033241			TCP	56	6050 → 51771 [FIN, ACK] Seq=187 Ack=264 Win=30336 Len=0
270	16:57:18.033509			TCP	62	51771 → 6050 [ACK] Seq=264 Ack=180 Win=2102272 Len=0

```

Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 172
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 168
      Version: TLS 1.2 (0x0303)
      Random: 63060b138818b0d4fe9acf2138b0b3645b993402f5ebe9375cad8cd74d24259
      Session ID Length: 0
      Cipher Suites Length: 32
      Cipher Suites (16 suites)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
        Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
        Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)
        Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
      Compression Methods Length: 1
      Compression Methods (1 method)
  
```

point d'extrémité.

9. En outre, vous pouvez effectuer une vérification croisée des chiffrements activés sur le terminal avec la Get-TlsCipherSuite | ft name Commande PowerShell.

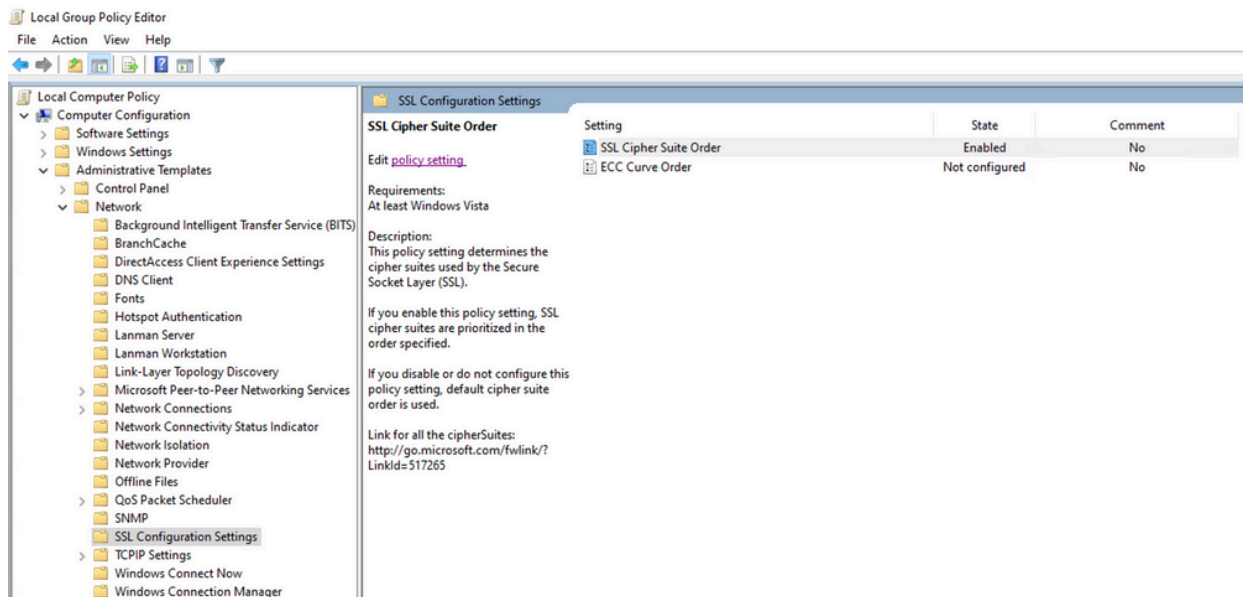
 Select Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> Get-TlsCipherSuite | ft name

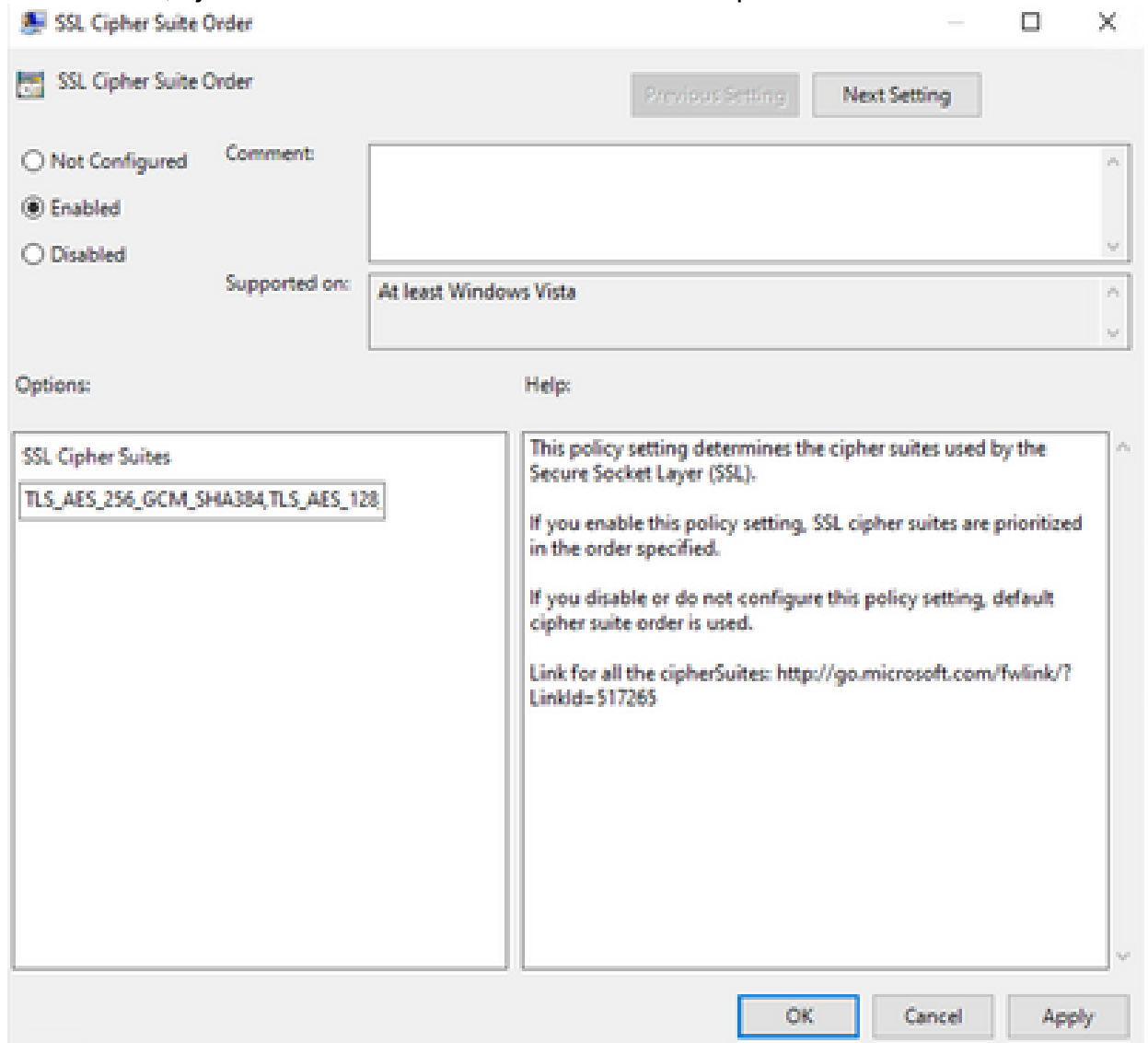
Name
----
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
TLS_PSK_WITH_AES_256_GCM_SHA384
TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_PSK_WITH_AES_256_CBC_SHA384
TLS_PSK_WITH_AES_128_CBC_SHA256
TLS_PSK_WITH_NULL_SHA384
TLS_PSK_WITH_NULL_SHA256
```

10. Si les chiffrements mentionnés à l'étape 6 ne sont pas répertoriés ici, c'est la raison de l'échec de la connexion SSL.
11. Pour résoudre ce problème, vérifiez l'ordre de la suite de chiffrement SSL dans la stratégie de groupe :

Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Temp1



12. L'ordre de la suite de chiffrement doit être Not Configured ou Disabled et, s'il est défini sur Enabled, ajoutez les chiffrements mentionnés à l'étape 6 dans la liste.



13. Appliquez ces modifications et redémarrez le terminal pour que ces modifications soient disponibles pour les applications.

14. Réessayez de mettre à jour TETRA une fois le redémarrage terminé.
15. Si le problème des définitions TETRA persiste, analysez les journaux et effectuez de nouveau les captures.

## Informations connexes

- [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.