

# Cisco Secure Endpoint - fout in Tetra Definitions Update met 3000-fout

## Inhoud

[Inleiding](#)

[Probleembeschrijving](#)

[Oplossing](#)

## Inleiding

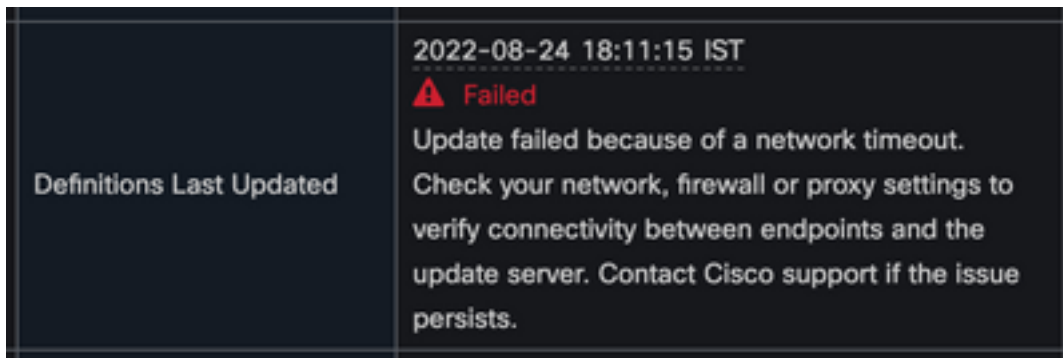
Dit document beschrijft stappen voor het oplossen van fouten in Tetra-definities met fout 3000-fout.

## Probleembeschrijving

1. Voor endpoint, tetra definities update mislukt met 'Kan geen updates installeren. Probeer het later opnieuw.' fout.



2. Op AMP-console wordt de vermelde fout waargenomen: **MisluktUpdate** mislukt vanwege een netwerk timeout. Controleer uw netwerk-, firewall- of proxyinstellingen om de connectiviteit tussen endpoints en de updateserver te verifiëren. Neem contact op met Cisco ondersteuning als het probleem zich blijft voordoen.

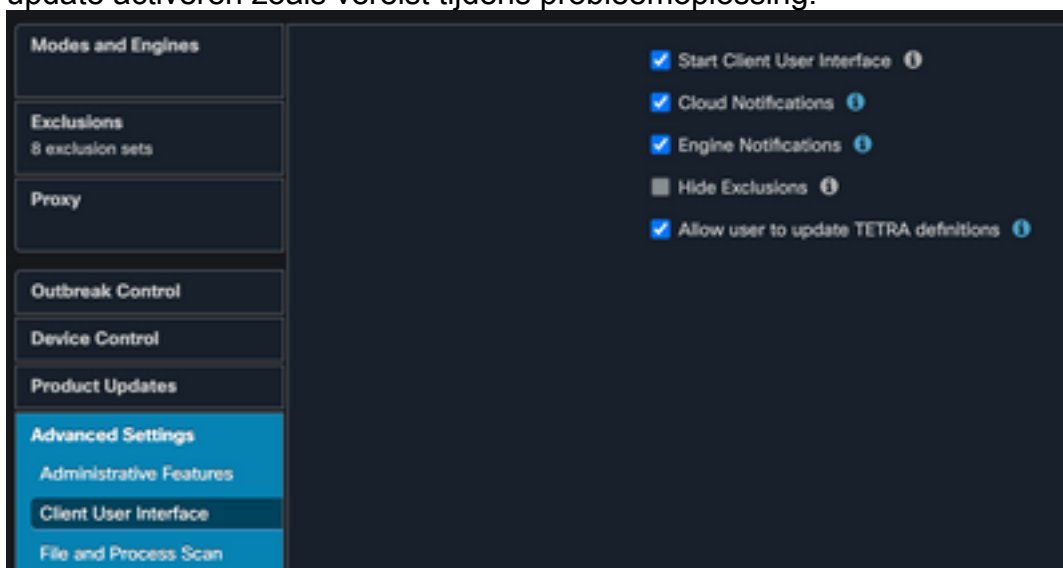


3. In debug sfc.exe.log, definities bijgewerkt mislukt met fout 3000 fout is waargenomen, wat staat voor '*Unknown\_Error*' zoals gedocumenteerd.

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TetraUpdateInterface::update updateDir:
C:\Program Files\Cisco\AMP\tetra, 20, -3000, -3000, 0, 0, 0
(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, id: 0
(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>::ReleaseInstance count: 1
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTetraUpdate: bUpdated = FALSE, state:
20, status: -3000
(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,
first failure - never, last err code - 4294964296, last upd success - never
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0,
first failure - Thu Aug 4 06:35:16 2022, last err code - 4294964296, last upd success -
never
```

## Oplossing

1. Schakel de optie 'Gebruiker toestaan om Tetra-definities bij te werken' in onder AMP Policy -> Clientgebruikersinterface op console. Met deze parameter kunnen we Tetra-update activeren zoals vereist tijdens probleemoplossing.



2. Schakel ook debug Connector en log op trayniveau in op het eindpunt of via AMP Policy.
3. Neem pakketopnamen op zowel de succesvolle Tetra-update als het mislukte eindpunt

voor Tetra-definities terwijl u op 'Tetra bijwerken' op het eindpunt klikt.

- OnTetra update succesvol endpoint, in pakketopnamefilter de pakketten met `http.host == "tetra-defs.amp.cisco.com:443"` en volg dan de `tcp.stream` van elke pakketten om het gerelateerde verkeer te analyseren.
- In 'Server Hello' pakket, kunt u zien Server accepteert 'TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384' algoritme in Server Hello pakket.

| No. | Time            | Source | Destination | Protocol | Length | Info  |
|-----|-----------------|--------|-------------|----------|--------|---|
| 169 | 17:54:13.501078 |        |             | TCP      | 68     | 60649 → 6050 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1                   |
| 170 | 17:54:13.501105 |        |             | 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 | 17:54:18.378029 |        |             | TLSv1..  | 9680   | Application Data [TCP segment of a reassembled PDU]   |
| 193 | 17:54:18.378461 |        |             | TCP      | 62     | 60649 → 6050 [ACK] Seq=710 Ack=32769 Win=2102272 Len=0  |
| 194 | 17:54:18.378471 |        |             | TCP      | 4680   | 6050 → 60649 [PSH, ACK] Seq=32769 Ack=710 Win=31360 Len=4544 [TCP segment of a reassembled PDU] |
| 195 | 17:54:18.378703 |        |             | TCP      | 62     | 60649 → 6050 [ACK] Seq=710 Ack=35689 Win=2102272 Len=0  |
| 196 | 17:54:18.378839 |        |             | TCP      | 62     | 60649 → 6050 [ACK] Seq=710 Ack=37313 Win=2102272 Len=0  |
| 197 | 17:54:18.640107 |        |             | 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: d19d47a9913f35df7270c3acebbe595422552881e62044737e9ee4e5fe776255
    - Session ID Length: 0
    - Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)
    - Compression Method: null (0)

- AMP Tetra-server accepteert alleen genoemde coderingen:

```
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
```

- Op Tetra update mislukte eindpunt, in pakketopname, wordt een fatale fout in SSL handdruk gezien na het pakket van de Klant Hello.

| No. | Time            | Source | Destination | Protocol | Length | Info  |
|-----|-----------------|--------|-------------|----------|--------|---|
| 245 | 16:57:17.390368 |        |             | TCP      | 68     | 51771 → 6050 [SYN, ECN, CWR] Seq=0 Win=8192 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=107 Win=2102272 Len=0                       |
| 268 | 16:57:18.023820 |        |             | TCP      | 56     | 6050 → 51771 [ACK] Seq=107 Ack=264 Win=30336 Len=0                              |
| 269 | 16:57:18.033241 |        |             | TCP      | 56     | 6050 → 51771 [FIN, ACK] Seq=107 Ack=264 Win=30336 Len=0                         |
| 270 | 16:57:18.033509 |        |             | TCP      | 62     | 51771 → 6050 [ACK] Seq=264 Ack=108 Win=2102272 Len=0                            |

> Frame 257: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)  
 > Linux cooked capture v1  
 > Internet Protocol Version 4, [redacted]  
 > Transmission Control Protocol [redacted]  
 > Hypertext Transfer Protocol  
 [Proxy-Connect-Hostname: tetra-defs.amp.cisco.com]  
 [Proxy-Connect-Port: 443]  
 > Transport Layer Security  
 > TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Handshake Failure)  
 Content Type: Alert (21)  
 Version: TLS 1.2 (0x0303)  
 Length: 2  
 > Alert Message  
 Level: Fatal (2)  
 Description: Handshake Failure (40)

8. In het Client Hello-pakket kunt u de aangeboden coderingen vanaf het eindpunt zien.

| No. | Time            | Source | Destination | Protocol | Length | Info  |
|-----|-----------------|--------|-------------|----------|--------|---|
| 245 | 16:57:17.390368 |        |             | TCP      | 68     | 51771 → 6050 [SYN, ECN, CWR] Seq=0 Win=8192 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=107 Win=2102272 Len=0                       |
| 268 | 16:57:18.023820 |        |             | TCP      | 56     | 6050 → 51771 [ACK] Seq=107 Ack=264 Win=30336 Len=0                              |
| 269 | 16:57:18.033241 |        |             | TCP      | 56     | 6050 → 51771 [FIN, ACK] Seq=107 Ack=264 Win=30336 Len=0                         |
| 270 | 16:57:18.033509 |        |             | TCP      | 62     | 51771 → 6050 [ACK] Seq=264 Ack=108 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: 63060b138818b0d4fe9acf2138b0b3645bb903402f5ebe9375cad8cd74d24259  
 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)

9. Daarnaast kunt u de ingeschakelde algoritmen op eindpunt controleren met 'Get-TlsCipherSuite' | Ft name' PowerShell commando.

```

Select Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-TlsCipherSuite | ft name

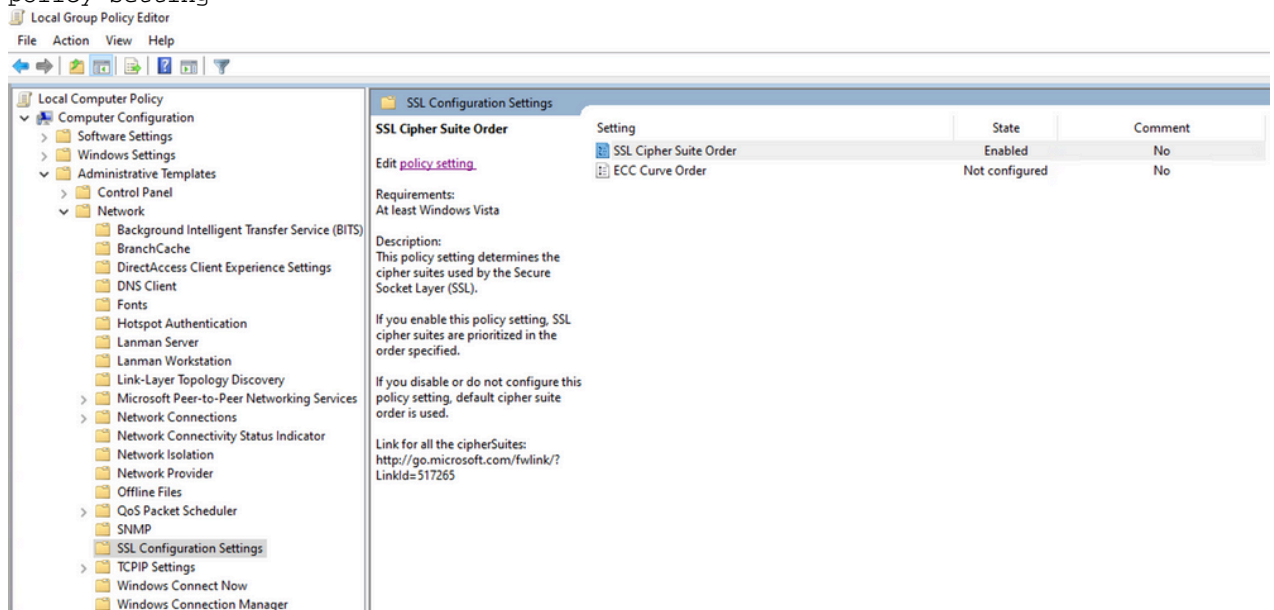
Name
----
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
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

```

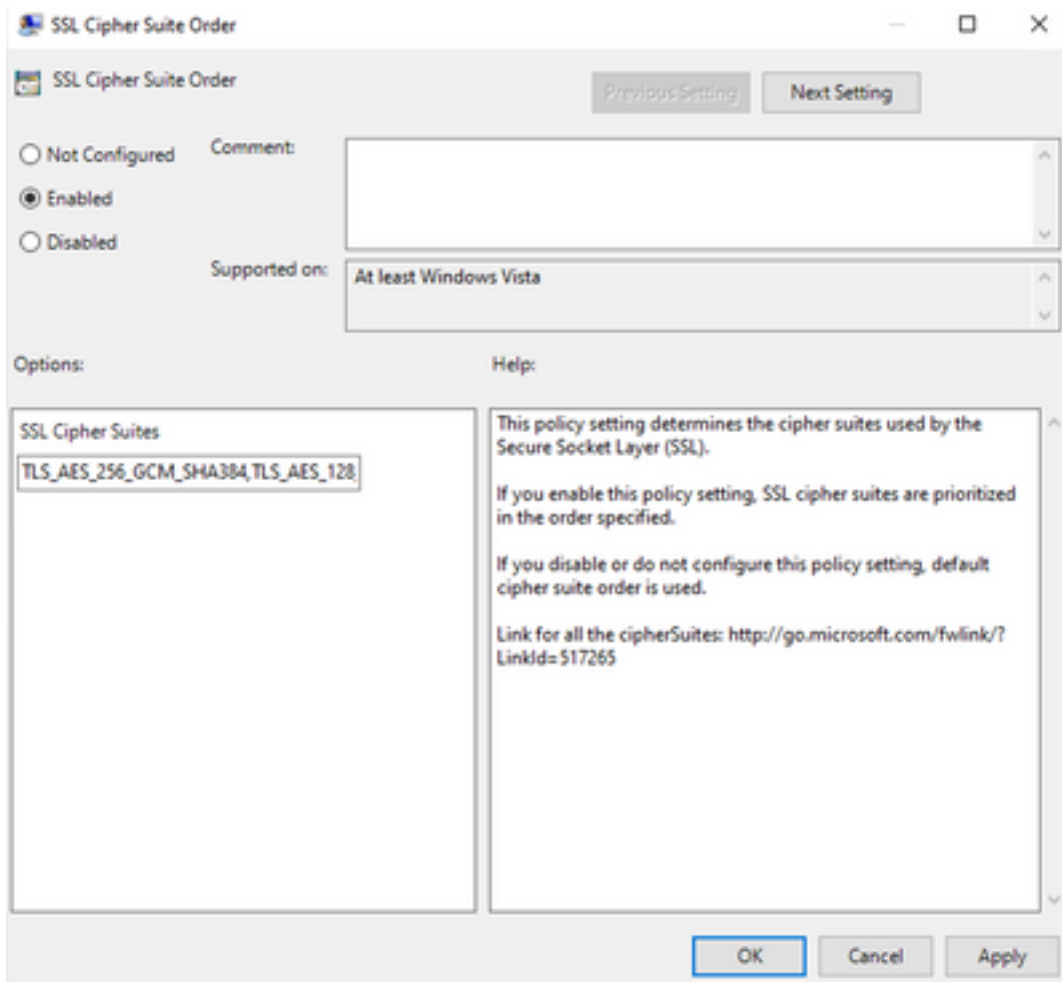
10. Als de in Stap 6 genoemde algoritmen niet hier worden vermeld, is dat de reden voor de SSL handshake mislukking.

11. Om dit op te lossen, verifieert u de 'SSL Cipher Suite Order' in het groepsbeleid:

Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Templates -> Network -> SSL Configuration Settings -> SSL Cipher Suite Order -> Edit policy setting



12. De volgorde van de Cipher Suite moet 'Niet geconfigureerd' of 'Uitgeschakeld' zijn en als dit item is ingesteld op 'Ingeschakeld', voegt u de in stap 6 vermelde algoritmen toe in de lijst.



13. Pas deze wijzigingen toe en start het eindpunt opnieuw om deze wijzigingen beschikbaar te maken voor toepassingen.
14. Probeer 'Update Tetra' opnieuw als de herstart is voltooid.
15. Als het probleem met de Tetra-definities blijft bestaan, analyseer dan de logbestanden en leg ze opnieuw vast.

## 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.