

Resolución de Problemas de Actualización de Definiciones TETRA con Error 3000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Solución](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos para resolver el error de definiciones de TETRA con el error 3000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Endpoint

Componentes Utilizados

La información de este documento se basa en:

- Cisco Secure Endpoint Connector (cualquier versión)
- Wireshark (cualquier versión)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

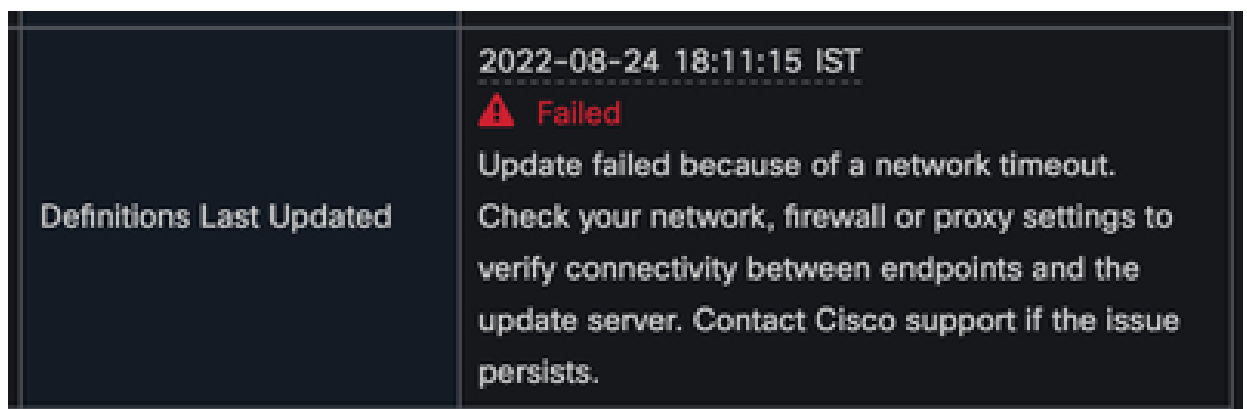
Problema

1. En el terminal, la actualización de las definiciones de TETRA falla con el mensaje de error "No se pueden instalar las actualizaciones. Inténtelo de nuevo más tarde".



2. En Cisco Secure Endpoint Console, se observa el error de falla mencionado:

"La actualización ha fallado debido a un tiempo de espera de la red. Compruebe la configuración de la red, el firewall o el proxy para verificar la conectividad entre los terminales y el servidor de actualización. Póngase en contacto con el servicio de asistencia de Cisco si el problema continúa."



3. En debug sfc.exe.log, las definiciones actualizadas fallaron con el error 3000 que se observa, que significa Unknown_Error como se documentó.

<#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
```

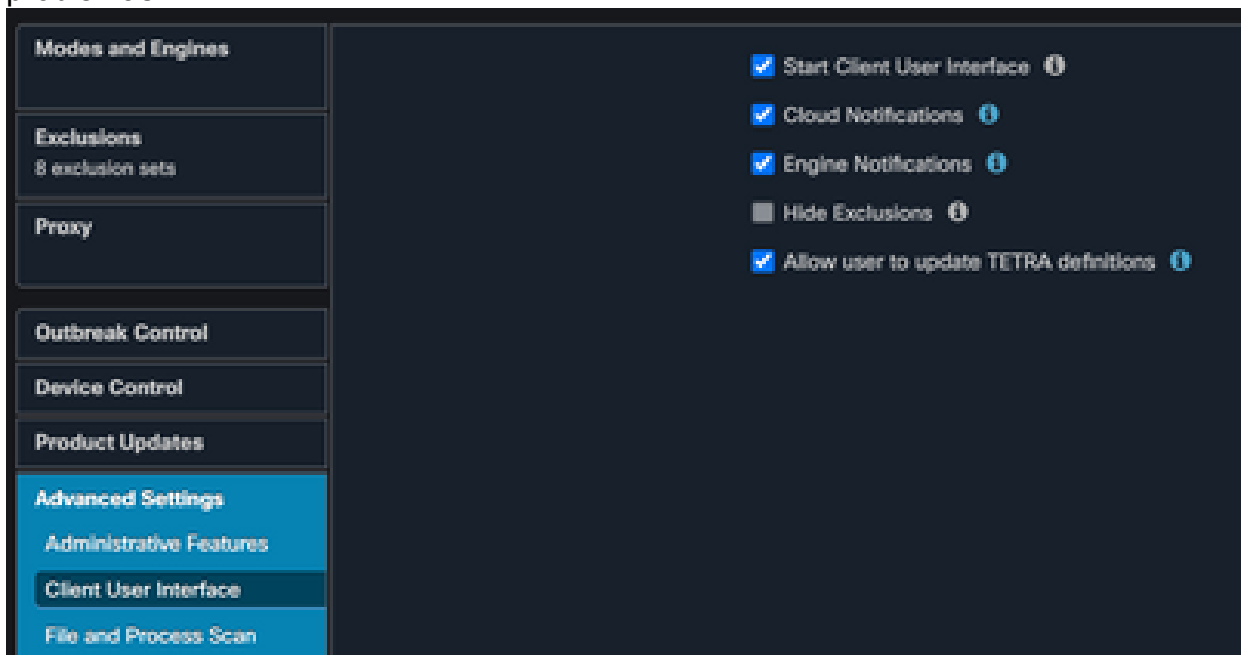
Update failed with error -3000

```
(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
```

Solución

1. Habilite la opción Permitir que el usuario actualice las definiciones de TETRA en Política de AMP > Interfaz de usuario cliente en la Consola. Con este parámetro puede activar la actualización de TETRA según sea necesario durante la resolución de problemas.



2. Además, habilite debug Connector y el registro de nivel de bandeja en el terminal o a través de la política AMP.
3. Por favor tome capturas de paquetes en los terminales exitosos y fallidos de actualización de TETRA para las definiciones de TETRA mientras hace clic en Update TETRA en el terminal.
4. En el punto final exitoso de la actualización de TETRA, en el filtro de captura de paquetes los paquetes con `http.host == "tetra-defs.amp.cisco.com:443"` y luego "siga el tcp.stream" de cada paquete para analizar el tráfico relacionado.
5. En Server Hello packet, puede ver que el servidor acepta el cifrado "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" en Server Hello packet.

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	17:54:13.501105			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	17:54:13.501430			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	17:54:13.528100			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	17:54:18.370703			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: d19d47a9913f35df7270c3acee595422552881e62044737e9ee45fe776255
 - Session ID Length: 0
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - Compression Method: null (0)
 - Extensions Length: 31

6. El servidor Cisco Secure Endpoint TETRA acepta solo los cifrados mencionados:

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. En el punto final fallido de la actualización de TETRA, en la captura de paquetes, se observa un error fatal en el intercambio de señales SSL después del paquete Hello del

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

> 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)

Cliente.

8. En el paquete de saludo del cliente, puede ver los cifrados ofrecidos desde el punto final.

```

tcp.stream eq 11
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. Además, puede realizar una verificación cruzada de los Ciphers habilitados en el punto final con `Get-TlsCipherSuite` | `ft name` Comando de PowerShell.

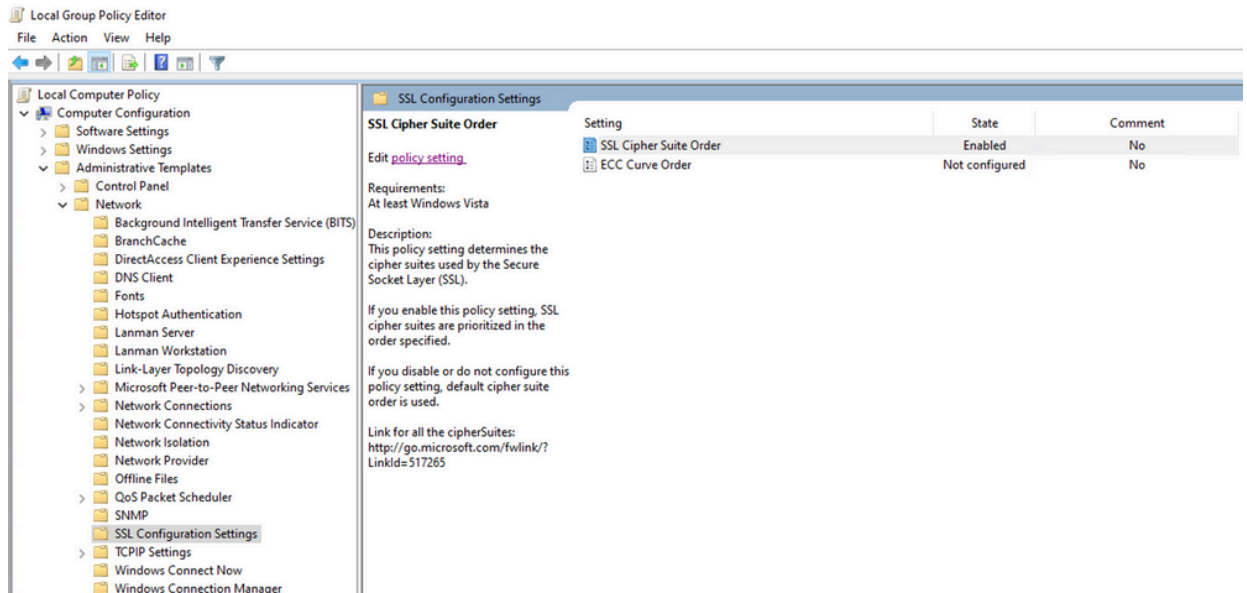
 Select Administrator: Windows PowerShell

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

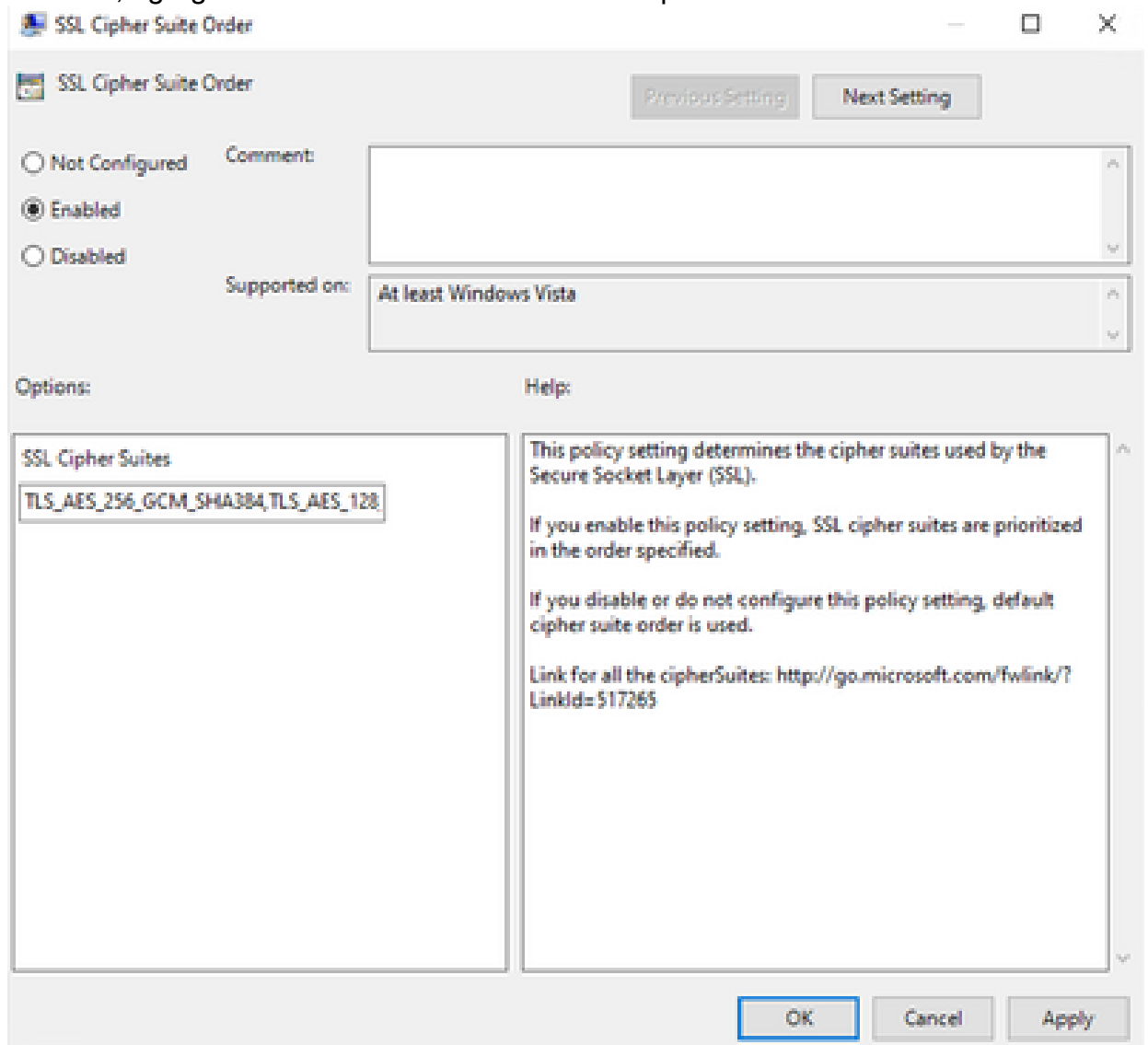
Name
----
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
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. En caso de que los cifrados mencionados en el Paso 6 no aparezcan aquí, esa es la razón del fallo del protocolo de enlace SSL.
11. Para solucionar esto, verifique el pedido de SSL Cipher Suite en la política de grupo:

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



12. El pedido de Cipher Suite debe ser Not Configured o Disabled y, si se establece en Enabled, agregue los cifrados mencionados en el paso 6 de la lista.



13. Aplique estos cambios y reinicie el terminal para que estos cambios estén disponibles para las aplicaciones.
14. Vuelva a intentar actualizar TETRA una vez que se haya completado el reinicio.

15. En caso de que el problema de las definiciones de TETRA persista, analice los registros y las capturas de nuevo.

Información Relacionada

- [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).