

Risoluzione dei problemi relativi all'aggiornamento delle definizioni TETRA con errore 3000

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alle definizioni TETRA. Errore 3000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Endpoint

Componenti usati

Le informazioni fornite in questo documento si basano su:

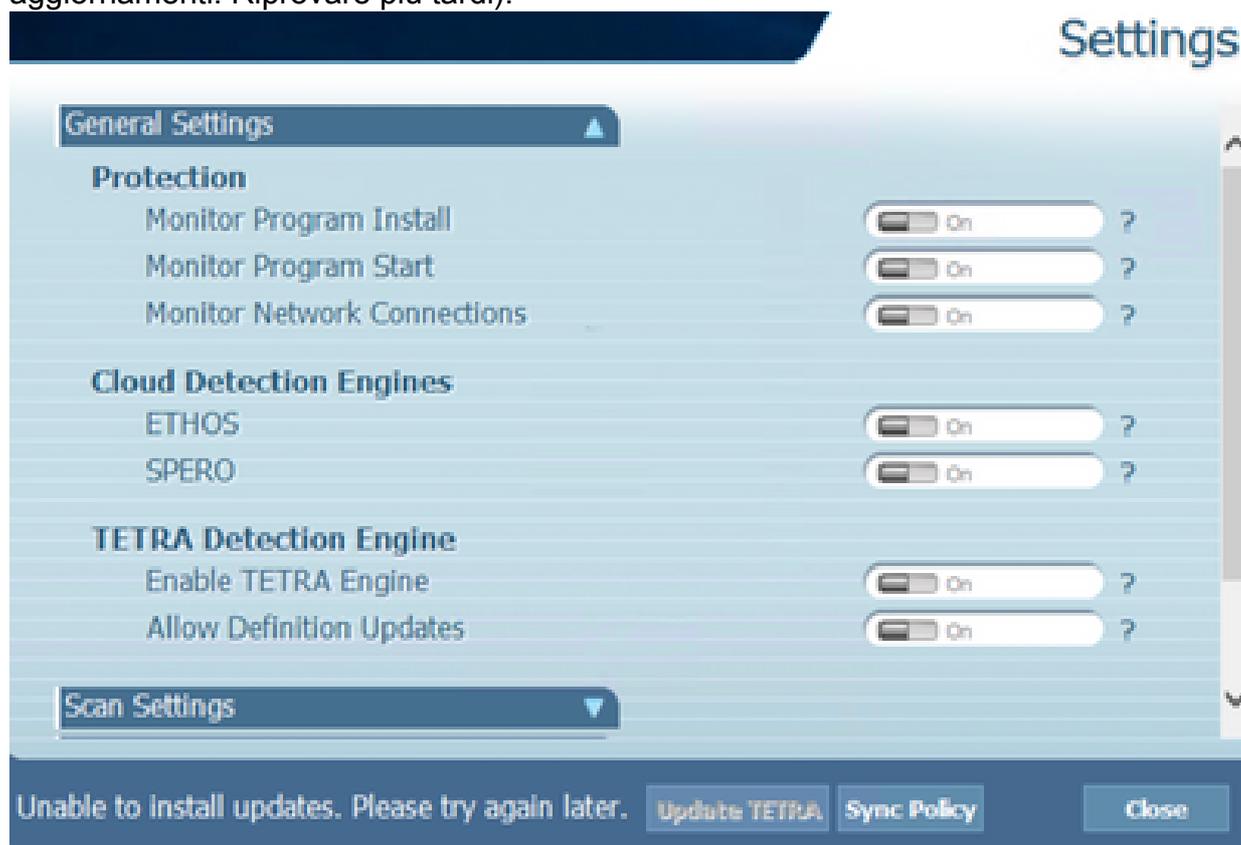
- Cisco Secure Endpoint connector (qualsiasi versione)
- Wireshark (qualsiasi versione)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

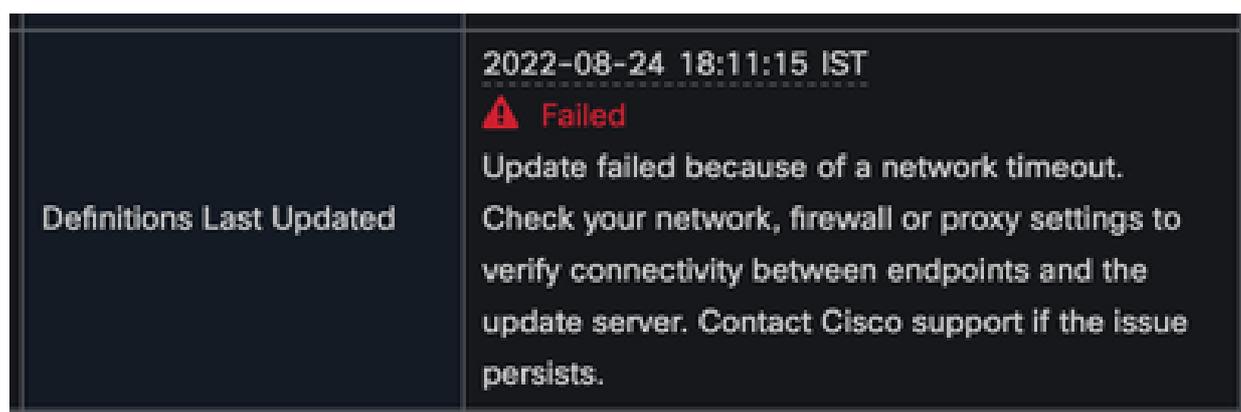
1. Sull'endpoint, l'aggiornamento delle definizioni TETRA non riesce con il messaggio di

errore "Unable to install updates.Please try again later" (Impossibile installare gli aggiornamenti. Riprovare più tardi).



2. In Cisco Secure Endpoint Console viene osservato un errore menzionato:

"Aggiornamento non riuscito a causa di un timeout di rete. Controllare le impostazioni di rete, firewall o proxy per verificare la connettività tra gli endpoint e il server di aggiornamento. Se il problema persiste, contattare il supporto Cisco."



3. In debug sfc.exe.log, le definizioni aggiornate non sono riuscite e viene rilevato l'errore 3000, che sta per Unknown_Error come documentato.

<#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
```

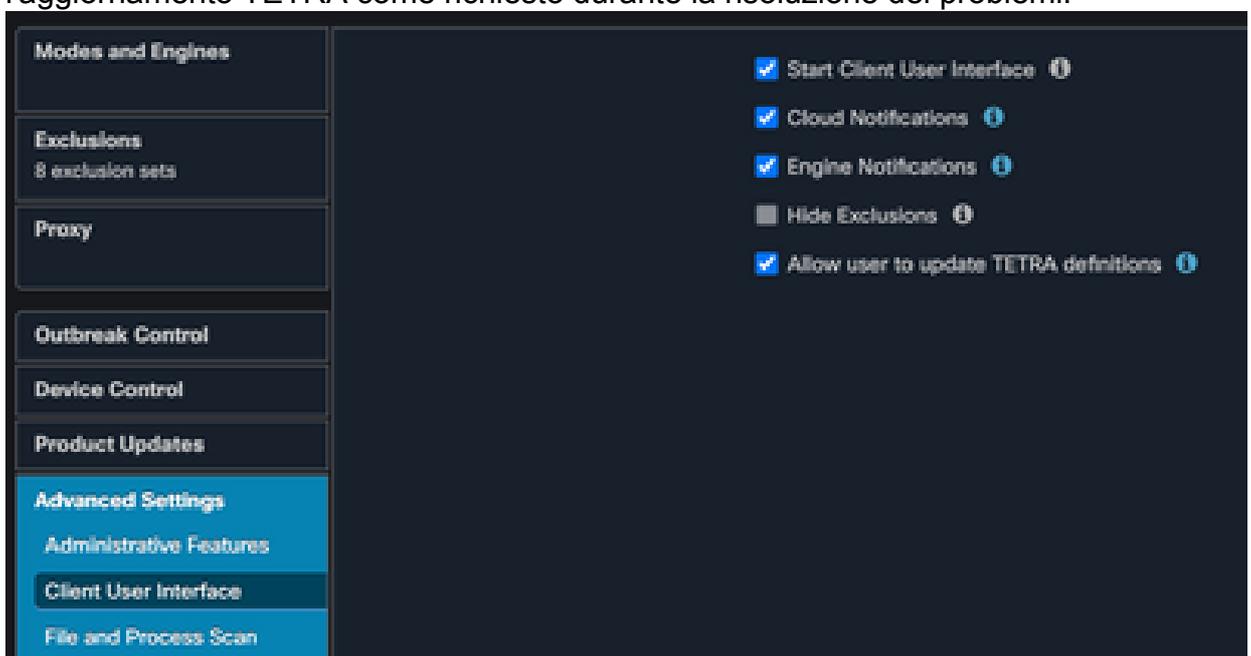
```
Update failed with error -3000
```

```
(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
```

Soluzione

1. Abilitare l'opzione Consenti all'utente di aggiornare le definizioni TETRA in Criteri AMP > Interfaccia utente client sulla console. Con questo parametro è possibile attivare l'aggiornamento TETRA come richiesto durante la risoluzione dei problemi.



2. Abilitare inoltre il connettore di debug e il registro a livello di cassetto sull'endpoint o tramite criteri AMP.
3. Acquisire le acquisizioni di pacchetti sull'endpoint con aggiornamenti TETRA riusciti e non riusciti per le definizioni TETRA mentre si fa clic su Aggiorna TETRA sull'endpoint.
4. In caso di aggiornamento TETRA dell'endpoint riuscito, filtrare i pacchetti con `http.host == "tetra-defs.amp.cisco.com:443"` e quindi "seguire il flusso `tcp.stream`" di ciascun pacchetto per analizzare il traffico correlato.
5. Nel pacchetto Server Hello, è possibile vedere il server accetta la cifratura "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" nel pacchetto 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	17:54:13.528100			TLSv1..	255	Client Hello
176	17:54:13.559031			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	17:54:18.370029			TLSv1..	9600	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	17:54:18.640107			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: d19d47a9913f35df7270c3acee595422552881e62044737e9ee4e5fe776255
      Session ID Length: 0
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Compression Method: null (0)
      Extension Length: 31
  
```

6. Il server Cisco Secure Endpoint TETRA accetta solo i seguenti tipi di crittografia:

```

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. Nell'endpoint con errore di aggiornamento TETRA, nell'acquisizione dei pacchetti viene rilevato un errore irreversibile nell'handshake SSL dopo il pacchetto Hello del client.

8. Nel pacchetto Client Hello, è possibile visualizzare le cifrature offerte dall'endpoint.

9. È inoltre possibile eseguire la verifica incrociata dei cifrari abilitati sull'endpoint con `Get-TlsCipherSuite | ft name` comando PowerShell.

 Select Administrator: Windows PowerShell

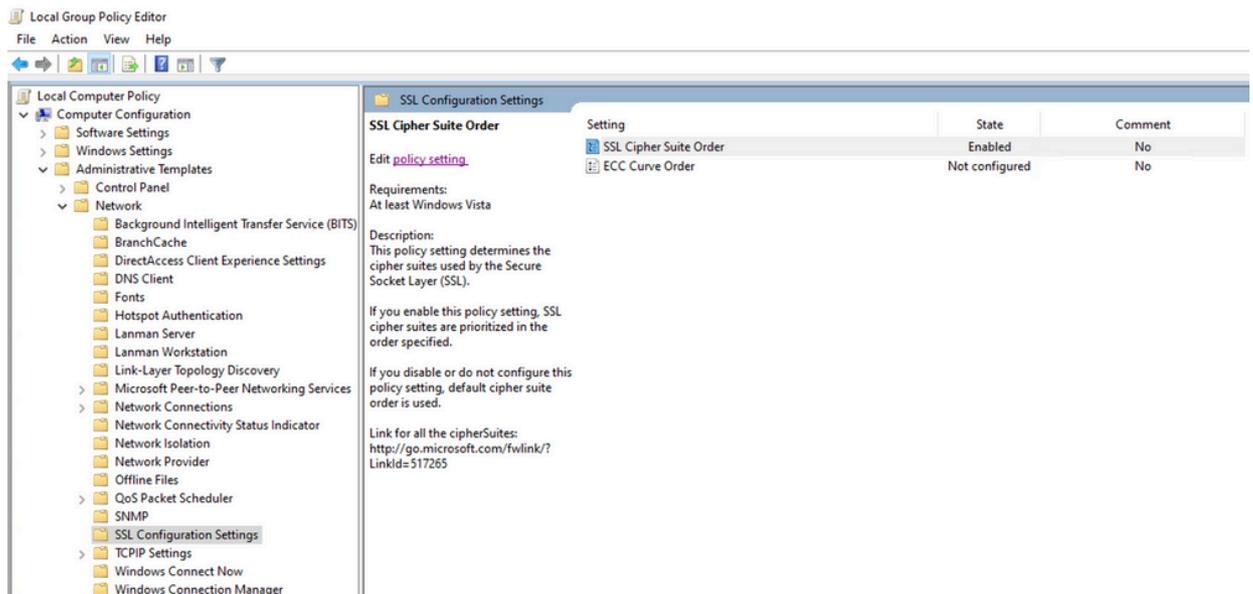
```
PS C:\WINDOWS\system32> Get-TlsCipherSuite | ft name

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
```

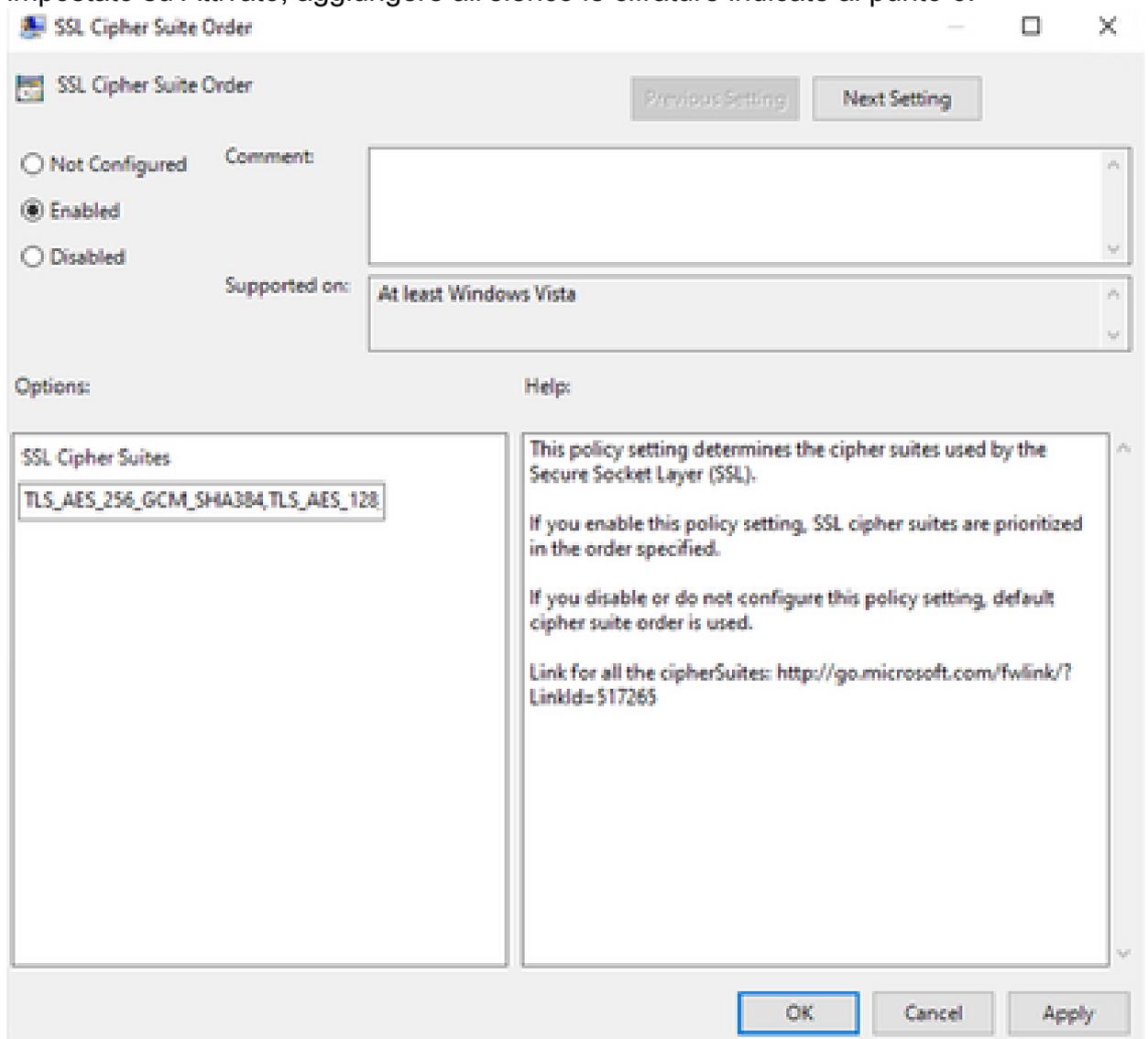
10. Nel caso in cui le cifrature menzionate nel passo 6 non siano elencate qui, è la causa dell'errore dell'handshake SSL.

11. Per risolvere il problema, verificare l'ordine della suite di crittografia SSL in Criteri di gruppo:

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



12. L'ordine della suite di cifratura deve essere Non configurato o Disattivato e, se impostato su Attivato, aggiungere all'elenco le cifrature indicate al punto 6.



13. Applicare le modifiche e riavviare l'endpoint per rendere le modifiche disponibili per le applicazioni.

14. Riprovare ad aggiornare TETRA al termine del riavvio.
15. Se il problema relativo alle definizioni TETRA persiste, analizzare nuovamente i registri e le acquisizioni.

Informazioni correlate

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).