排除TETRA定義更新失敗和3000錯誤故障

目錄

簡介

本文描述排除TETRA定義故障（出現錯誤3000）的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全端點

採用元件

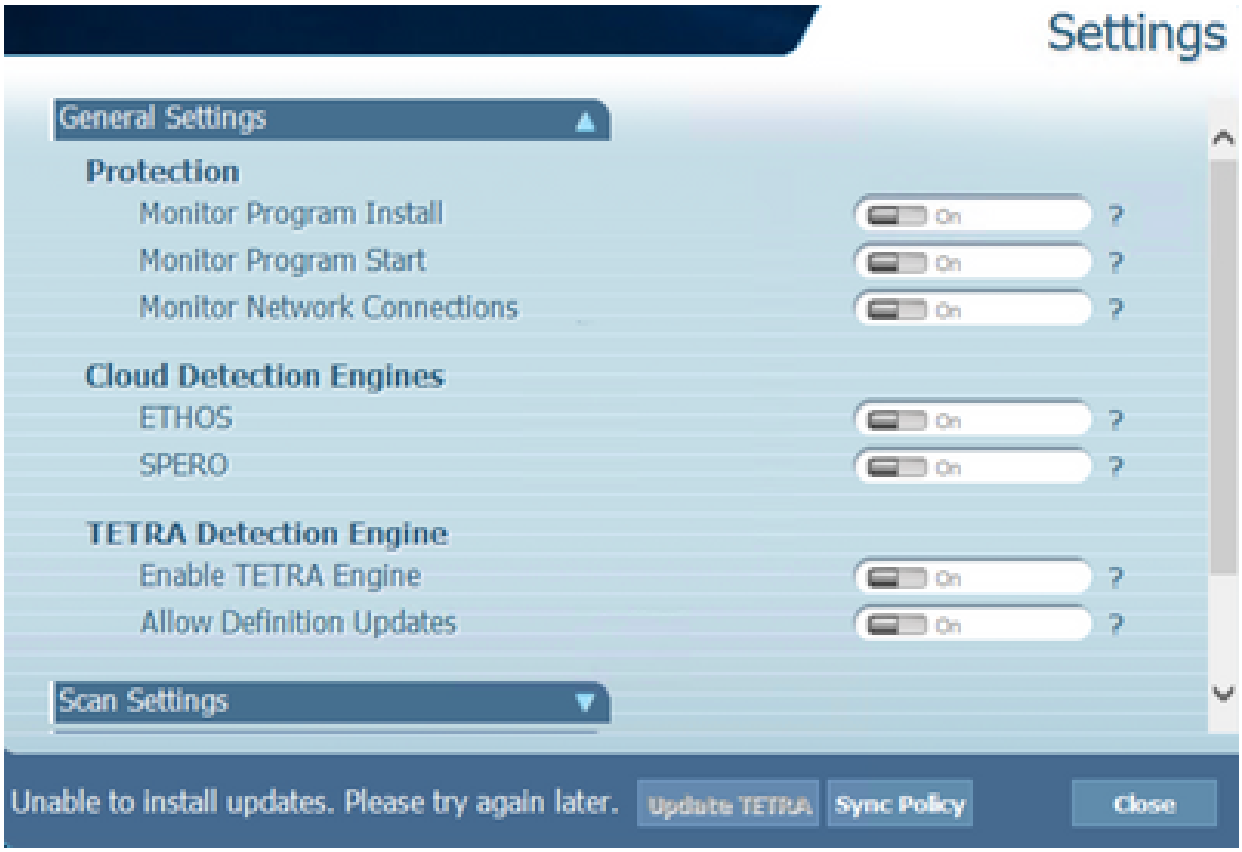
本檔案中的資訊是根據：

- 思科安全終端聯結器（任何版本）
- Wireshark（任何版本）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

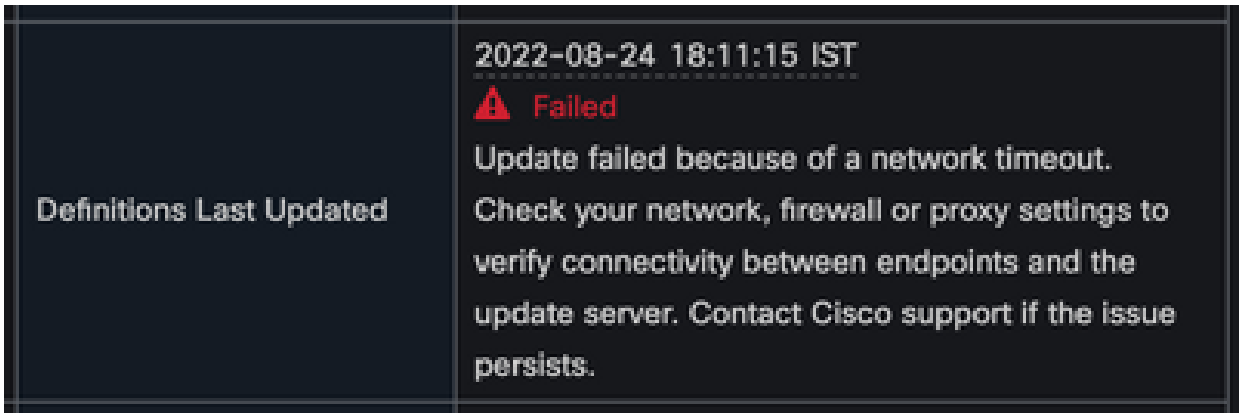
問題

1. 在終端上，TETRA定義更新失敗，出現「無法安裝更新。請稍後重試」錯誤消息。



2. 在Cisco Secure Endpoint Console上，觀察到上述故障錯誤：

「由於網路超時，更新失敗。檢查您的網路、防火牆或代理設定以驗證終端與更新伺服器之間的連線。如果問題仍然存在，請與思科支援部門聯絡。」



3. 在debug sfc.exe.log中，定義更新失敗，並觀察到錯誤3000，表示如記錄的Unknown_Error。

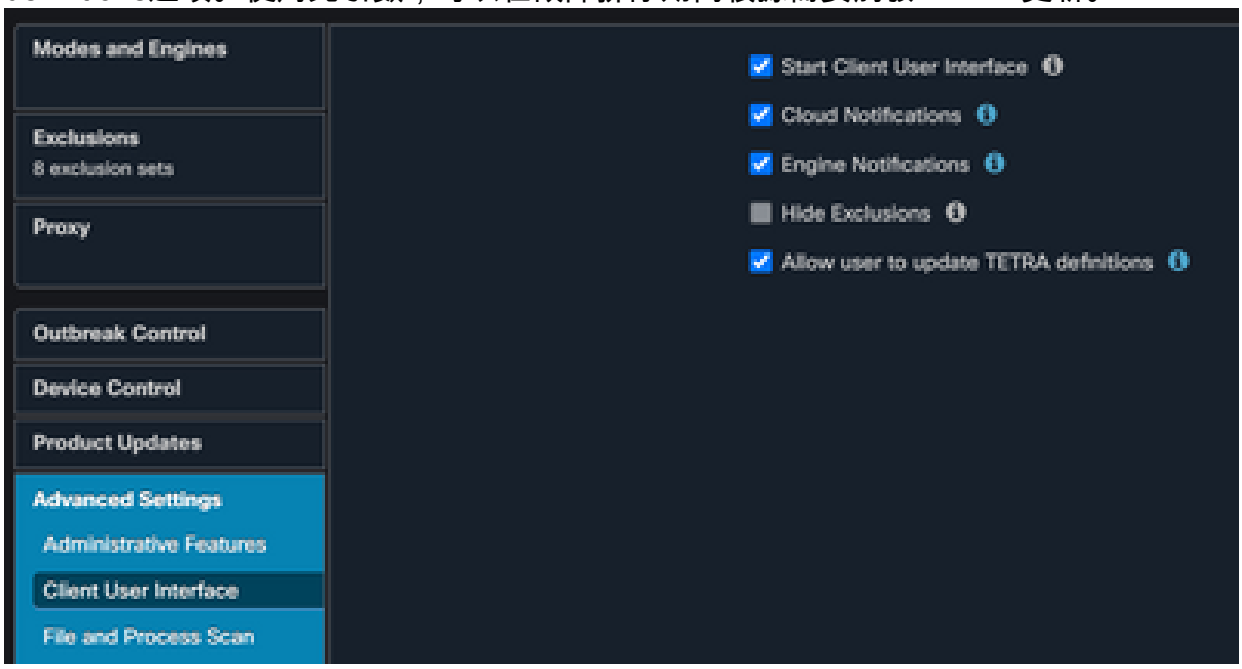
<#root>

```
(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
```

解決方案

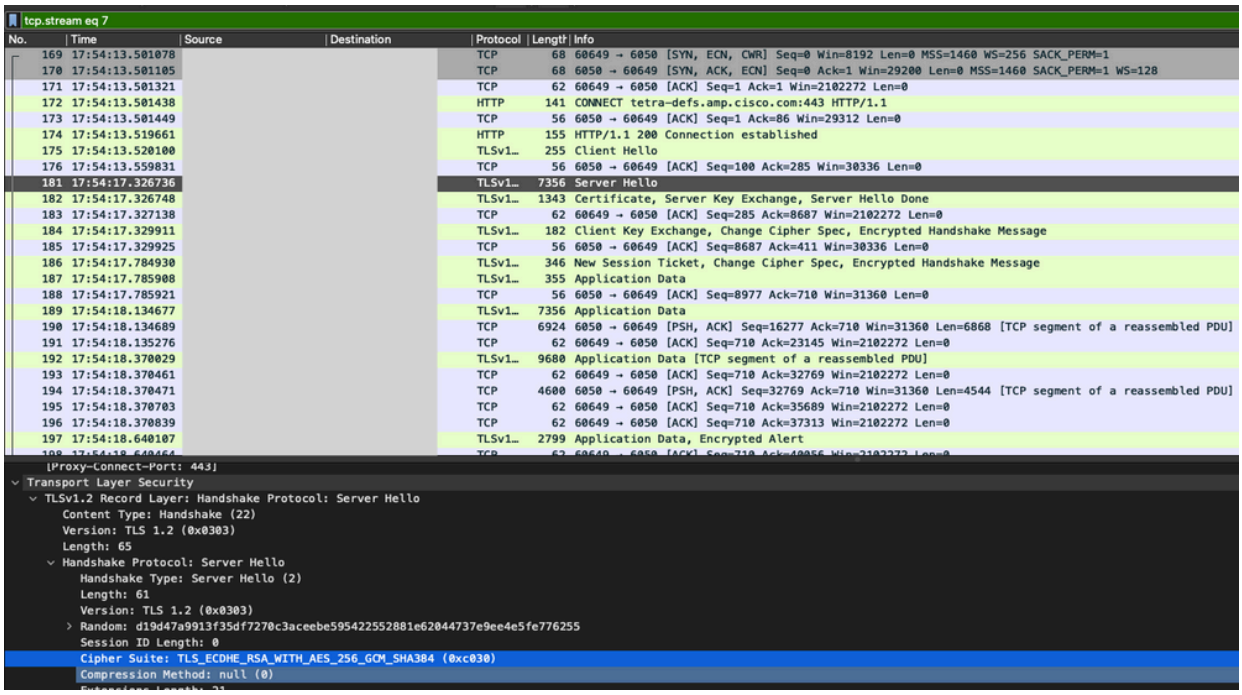
1. 請在控制檯上的AMP Policy > Client User Interface中啟用Allow user to update TETRA definitions選項。使用此引數，可以在故障排除期間根據需要觸發TETRA更新。



2. 此外，在終端上或通過AMP策略啟用調試聯結器和托盤級日誌。

3. 按一下更新TETRA端點時，請在TETRA更新成功和失敗的端點上捕獲TETRA定義的資料包捕獲。

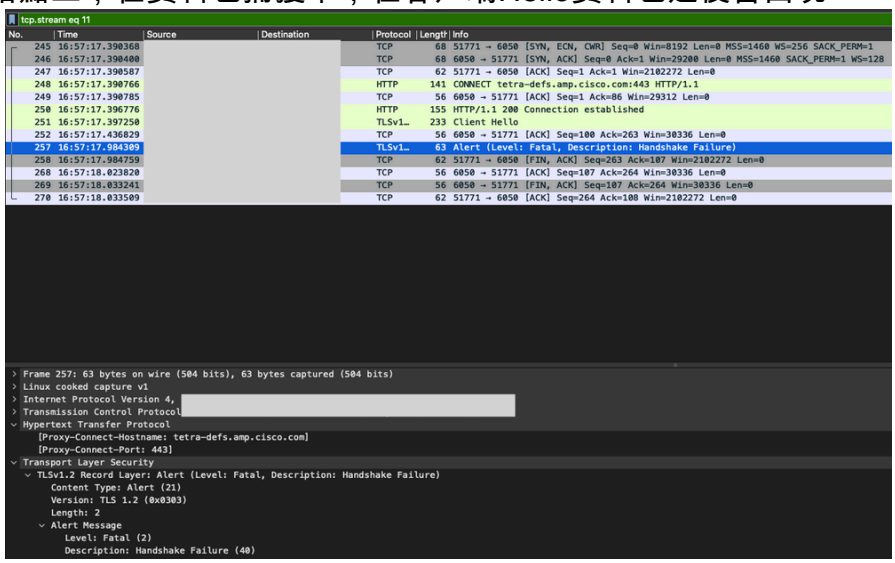
4. 在TETRA更新成功端點上，在封包擷取中，使用http.host == "tetra-defs.amp.cisco.com:443"篩選封包，然後「follow the tcp.stream」每個封包以分析相關流量。
5. 在Server Hello資料包中，可以看到伺服器接受Server Hello資料包中的「TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384」密碼。

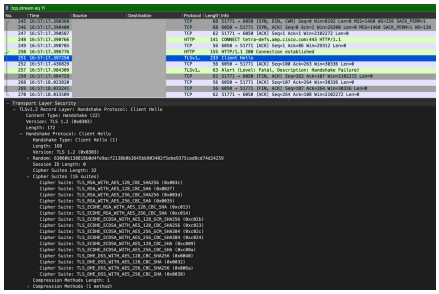


6. 思科安全終端TETRA伺服器只接受提及的密碼：

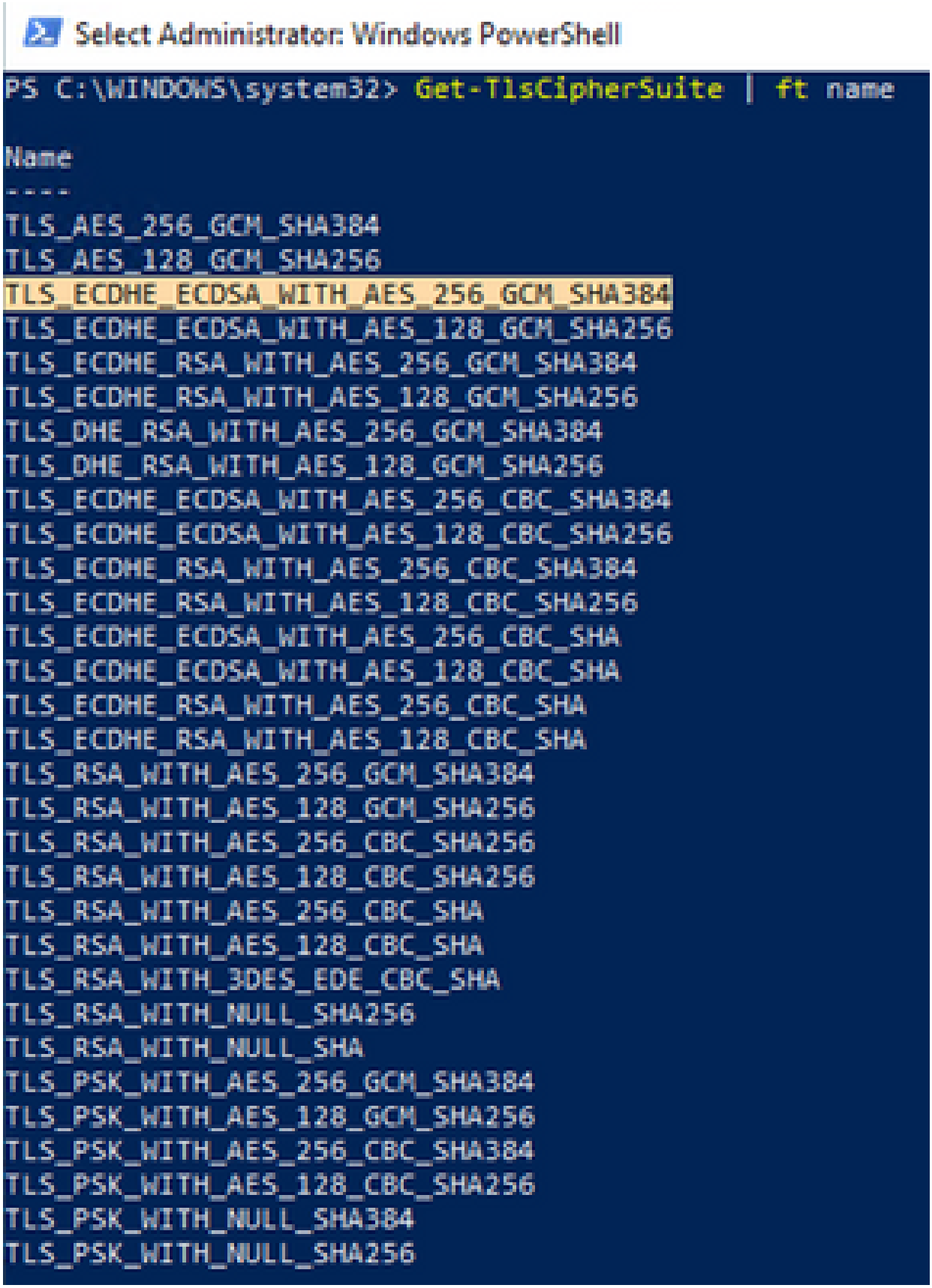
```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_AES_128_GCM_SHA256
```

7. 在TETRA更新失敗的終結點上，在資料包捕獲中，在客戶端Hello資料包之後會出現SSL握手中的致命錯誤。



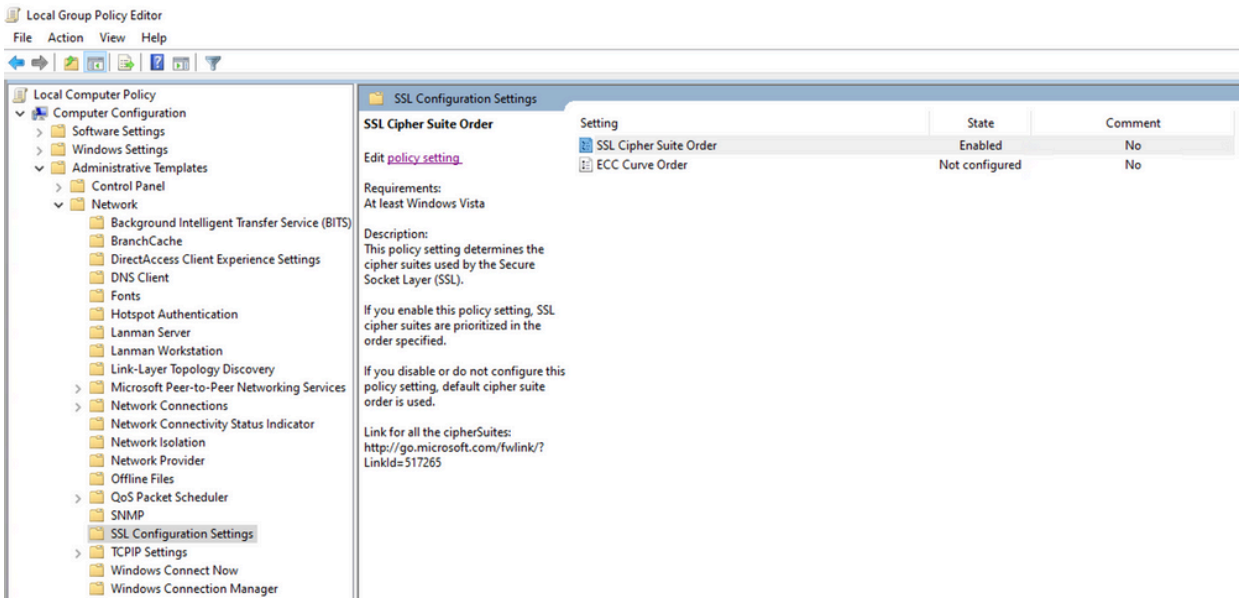


8. 在Client Hello資料包中，您可以從終端檢視提供的密碼。
9. 此外，您還可以使用Get-TlsCipherSuite交叉驗證終端上已啟用的密碼 | ft name PowerShell命令。

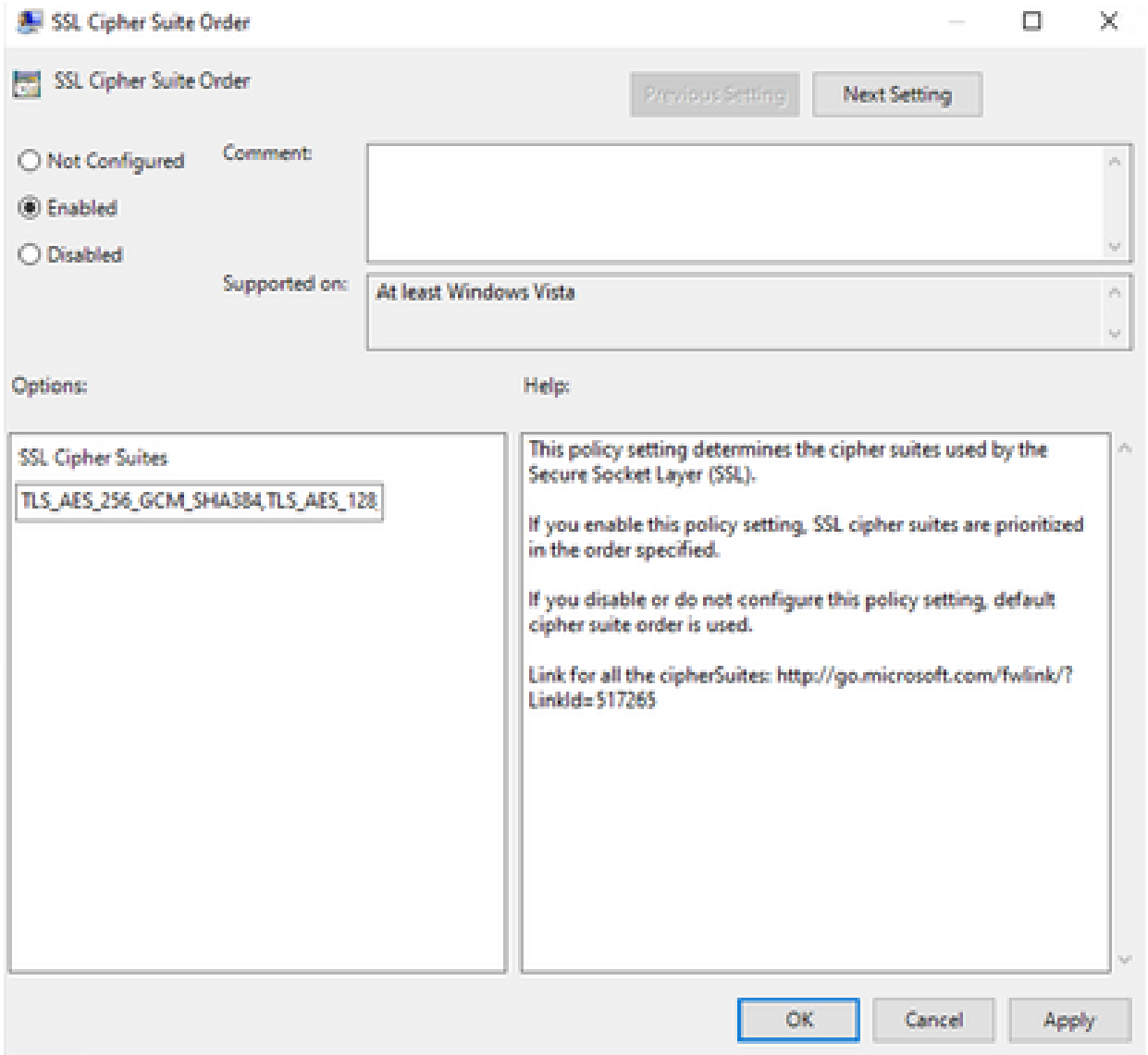


10. 如果此處未列出步驟6中提到的密碼，則這是SSL交握失敗的原因。
11. 要解決此問題，請驗證組策略中的SSL密碼套件順序:

```
Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Templ
```



12. 密碼套件順序必須是Not Configured或Disabled，如果設定為Enabled，請在清單中新增步驟6中提到的密碼。



13. 應用這些更改並重新啟動終端，以使這些更改可用於應用程式。
14. 重新引導完成後，請重試更新TETRA。
15. 如果TETRA定義問題仍然存在，請分析日誌並再次捕獲。

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。