3000エラーによるTETRA定義の更新エラーのトラブルシューティング

内容

はじめに

このドキュメントでは、エラー3000エラーでTETRA定義の障害をトラブルシューティングする手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Endpoint

使用するコンポーネント

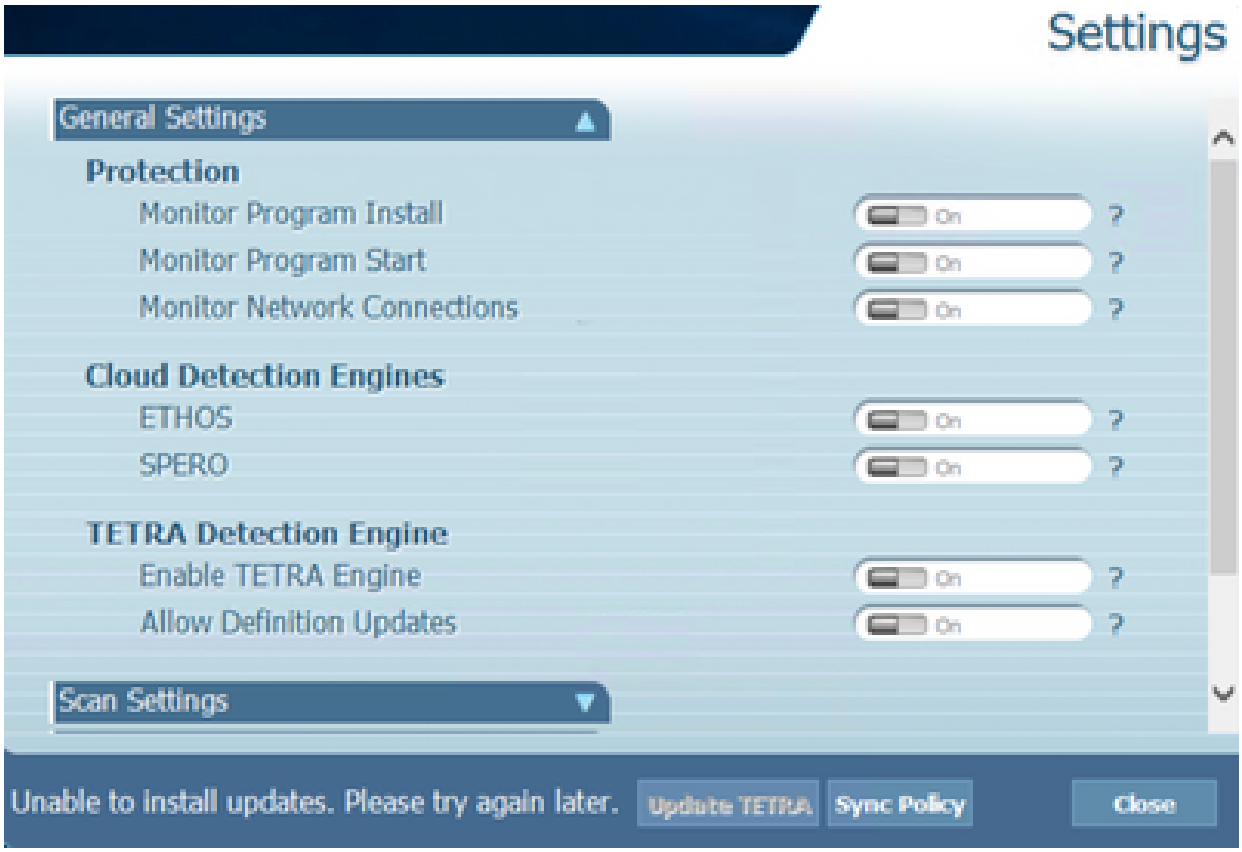
このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco Secure Endpointコネクタ（任意のバージョン）
- Wireshark（任意のバージョン）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

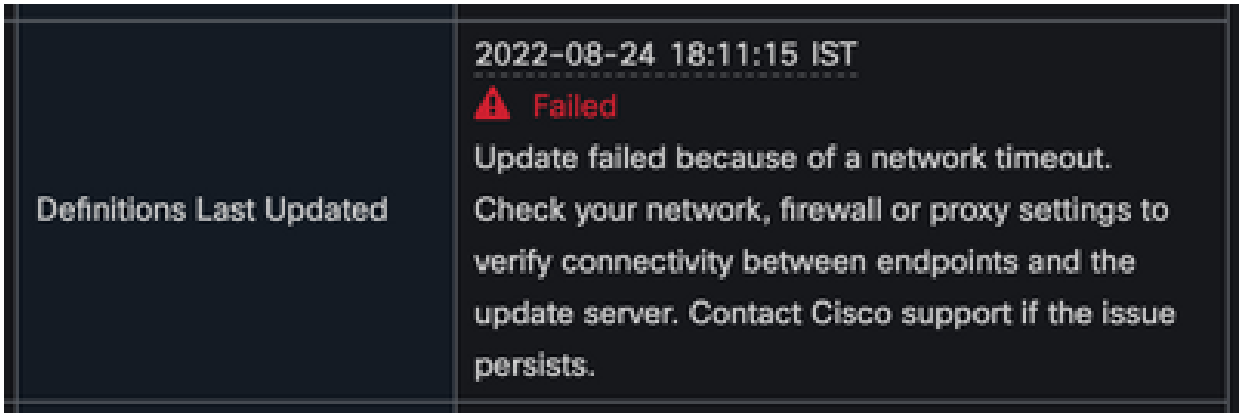
問題

1. エンドポイントで、TETRA定義の更新が「Unable to install updates.Please try again later」というエラーメッセージで失敗します。



2. Cisco Secure Endpoint Consoleで、前述の障害エラーが表示されます。

“ネットワークのタイムアウトのため、更新に失敗しました。ネットワーク、ファイアウォール、またはプロキシの設定を確認して、エンドポイントと更新サーバー間の接続を確認してください。問題が解決しない場合は、Ciscoサポートにお問い合わせください」



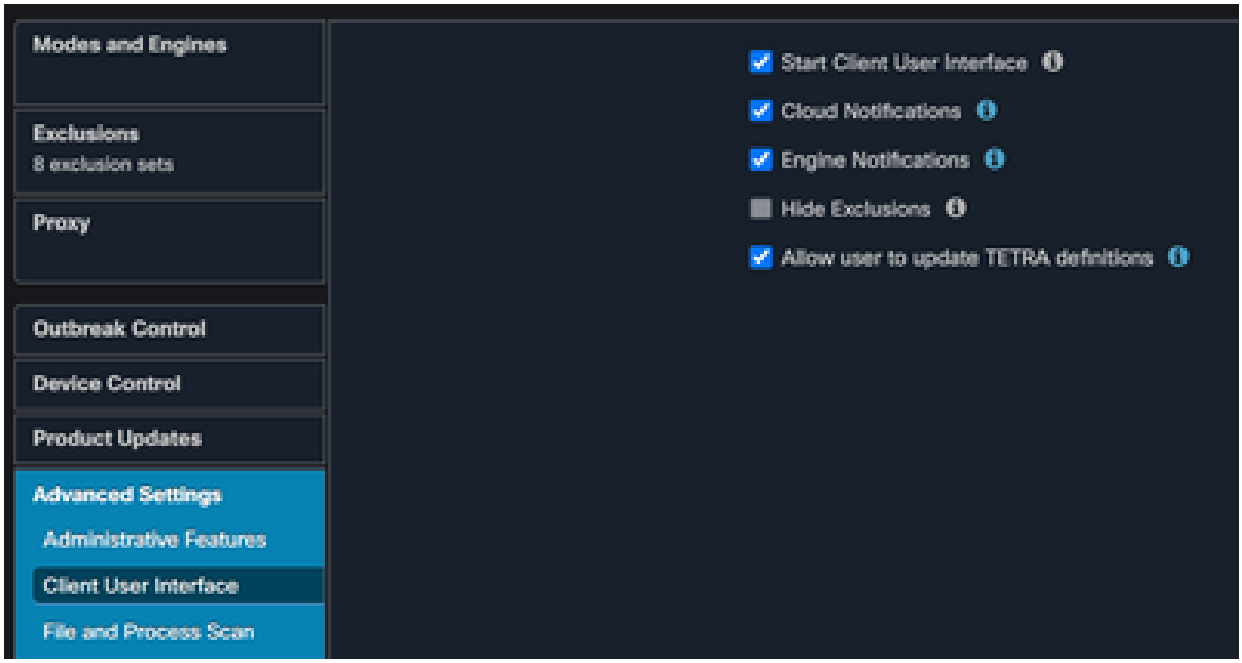
3. debug sfc.exe.logで、「definitions updated failed with error 3000」エラーが表示されます。これは、文書化されているUnknown_Errorを意味します。
<#root>

```
(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
```

解決方法

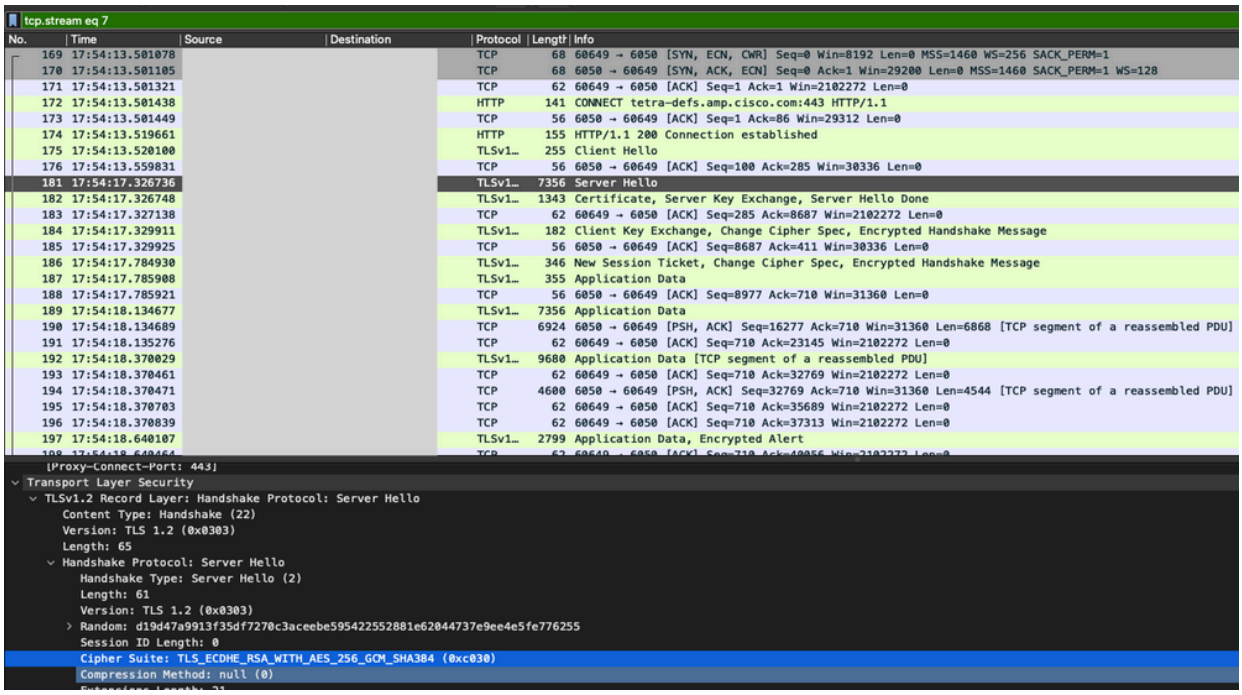
1. コンソールでAMP Policy > Client User Interfaceの順に選択し、Allow user to update TETRA definitionsオプションを有効にしてください。このパラメータを使用すると、トラブルシューティング中に必要に応じてTETRAアップデートをトリガーできます。



2. また、エンドポイントで、またはAMPポリシーを介して、コネクタとトレイレベルのデバッグログを有効にします。

3. エンドポイントでUpdate TETRAをクリックしながら、TETRA DefinitionsのTETRA更新の成功と失敗したエンドポイントの両方でパケットキャプチャを取得してください。

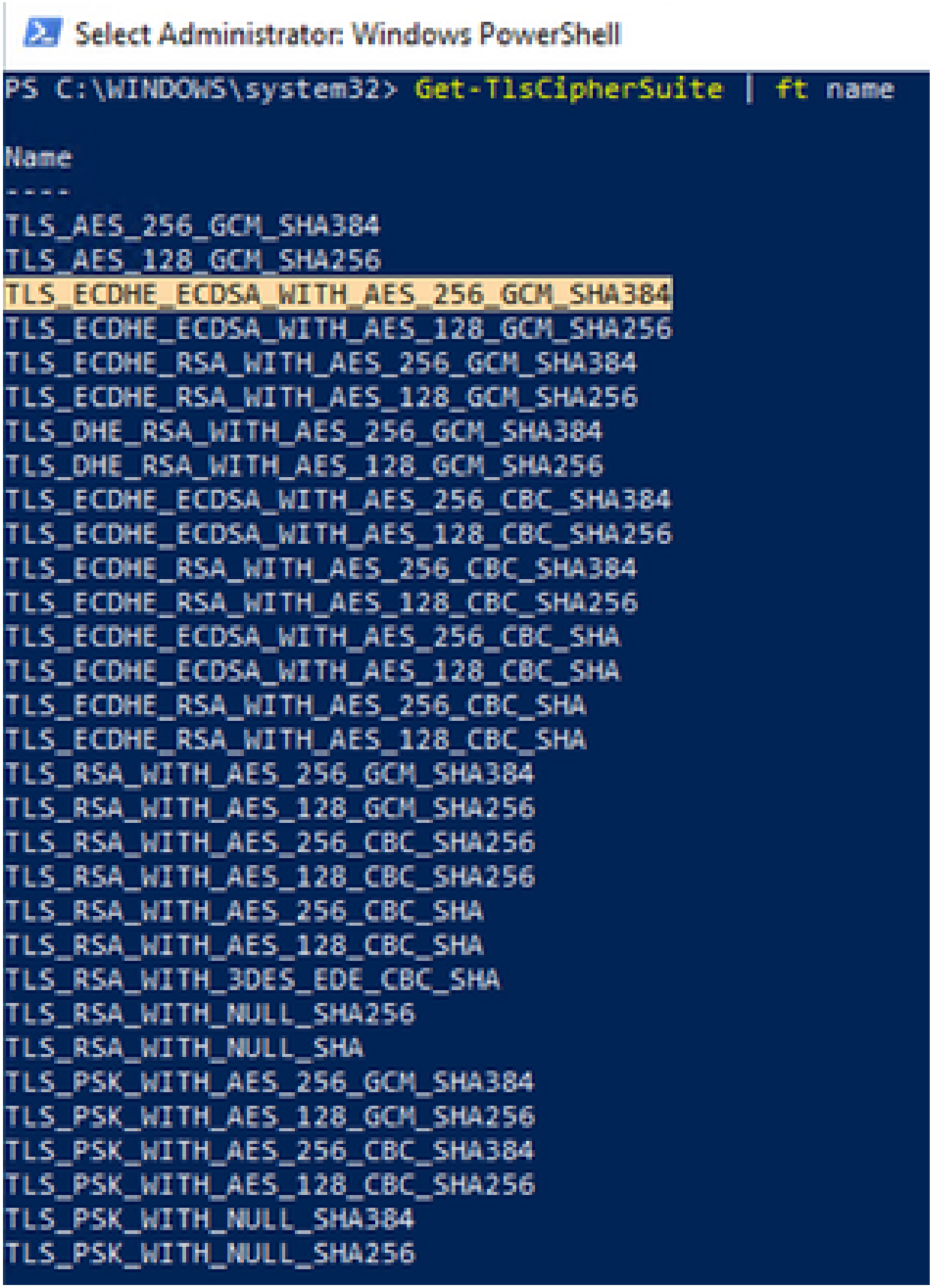
4. TETRAアップデートが成功したエンドポイントでは、パケットキャプチャでhttp.host == "tetra-defs.amp.cisco.com:443"を含むパケットをフィルタリングし、次に各パケットの"tcp.stream"を追跡して、関連するトラフィックを分析します。
5. Server Helloパケットで、Server accepts "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"という暗号がServer Helloパケットで確認できます。



6. Cisco Secure Endpoint TETRAサーバは、言及された暗号のみを受け入れます。

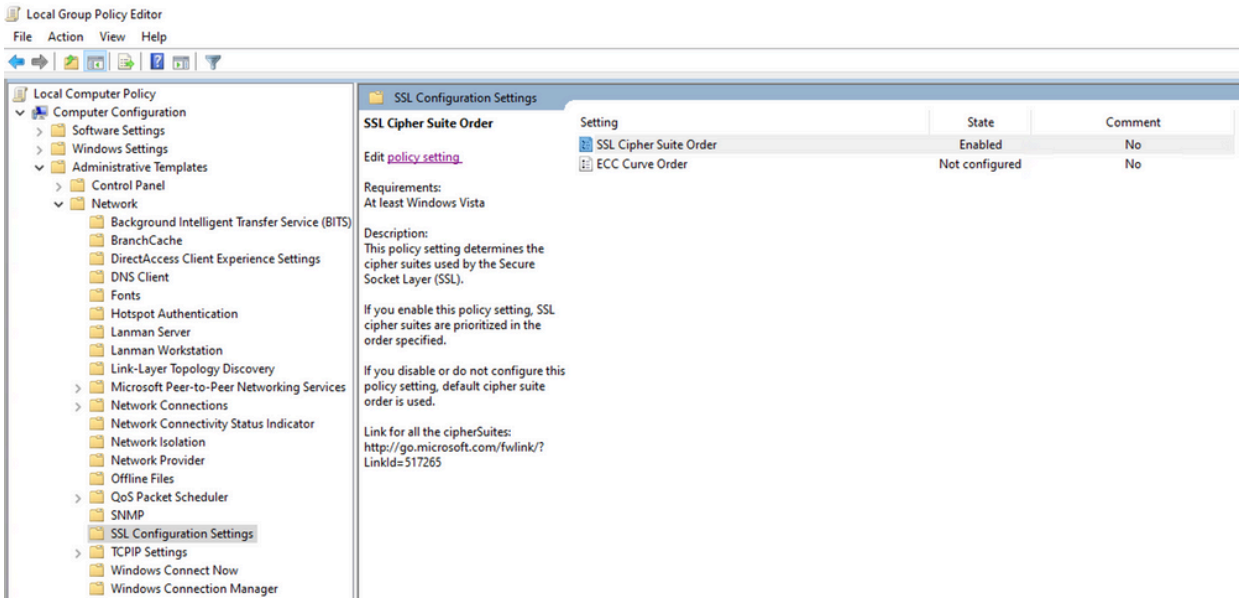
```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_AES_128_GCM_SHA256
```

7. TETRAアップデートが失敗したエンドポイントでは、パケットキャプチャで、Client Helloパケットの後にSSLハンドシェイクの致命的なエラーが表示されます。 
8. Client Helloパケットでは、エンドポイントから提供される暗号を確認できます。 
9. また、エンドポイントで有効になっている暗号をGet-TlsCipherSuiteで相互検証できます | ft name PowerShellコマンドを使用します。

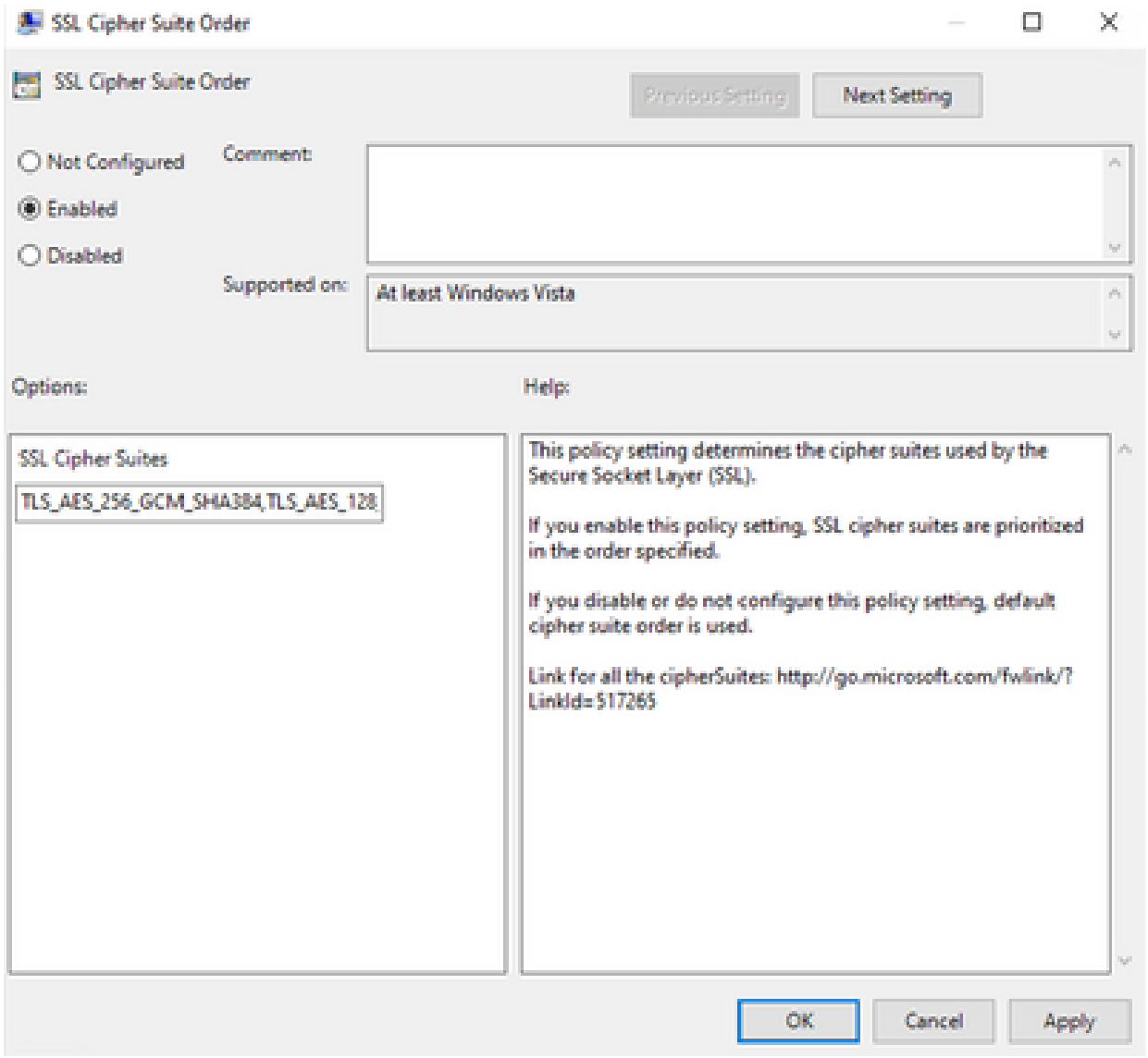


10. ステップ6で説明した暗号がここにリストされていない場合は、SSLハンドシェイクが失敗する理由です。
11. これを修正するには、グループポリシーでSSL暗号スイートの順序を確認してください。

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



12. 暗号スイートの順序はNot ConfiguredまたはDisabledである必要があります。Enabledに設定されている場合は、ステップ6で説明した暗号をリストに追加します。



13. これらの変更を適用し、エンドポイントを再起動して、アプリケーションで使用できるようにします。

14. 再起動が完了したら、Update TETRAを再試行してください。
15. TETRA定義の問題が解決しない場合は、ログを分析して再度キャプチャしてください。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。