Troubleshooting de Falha de Atualização de Definições TETRA com Erro 3000

Contents

Introdução

Este documento descreve as etapas para resolver problemas de falha de definições TETRA com erro 3000.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Endpoint seguro da Cisco

Componentes Utilizados

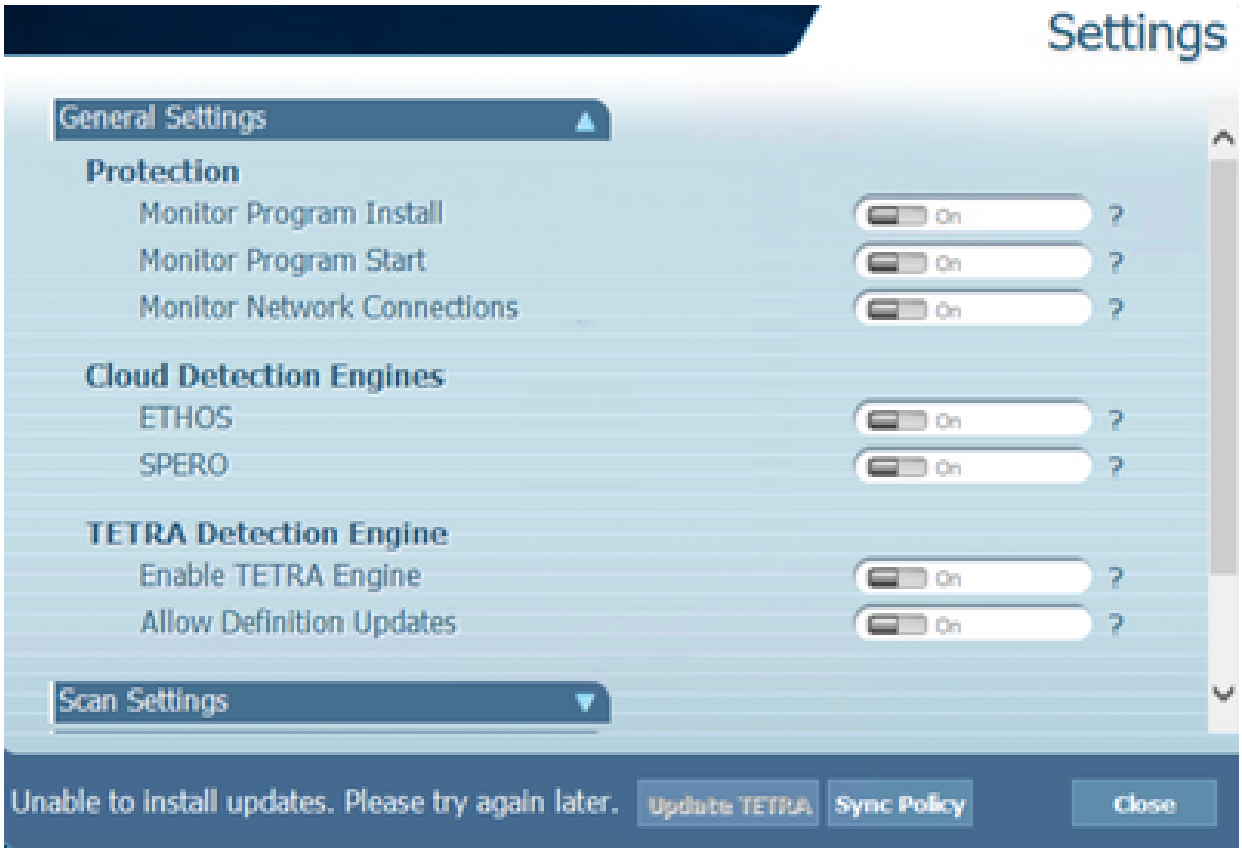
As informações neste documento são baseadas em:

- Conector Cisco Secure Endpoint (qualquer versão)
- Wireshark (qualquer versão)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

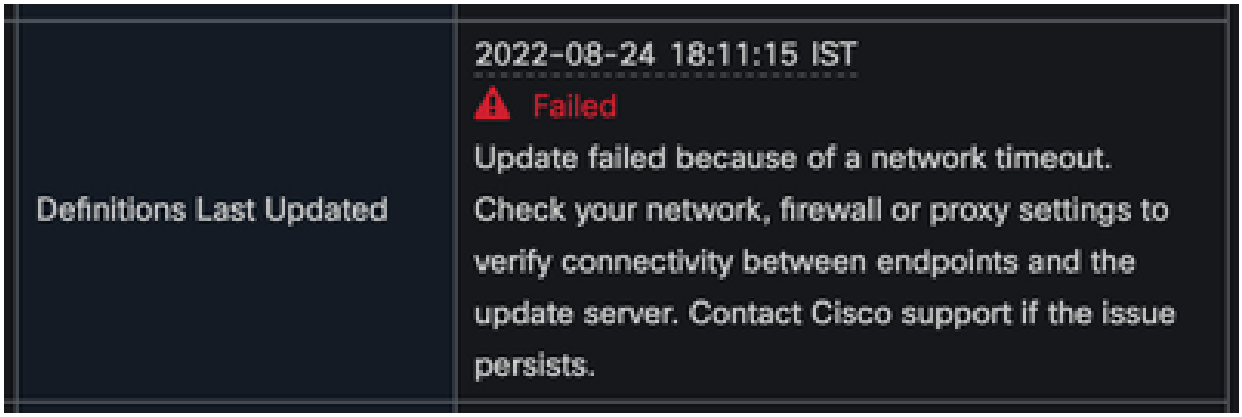
Problema

1. No endpoint, a atualização das Definições TETRA falha com a mensagem de erro "Não é possível instalar atualizações.Tente novamente mais tarde".



2. No Cisco Secure Endpoint Console, é observado o erro de falha mencionado:

   "Falha na atualização devido a um tempo limite da rede. Verifique suas configurações de rede, firewall ou proxy para verificar a conectividade entre os pontos de extremidade e o servidor de atualização. Entre em contato com o suporte da Cisco se o problema persistir."



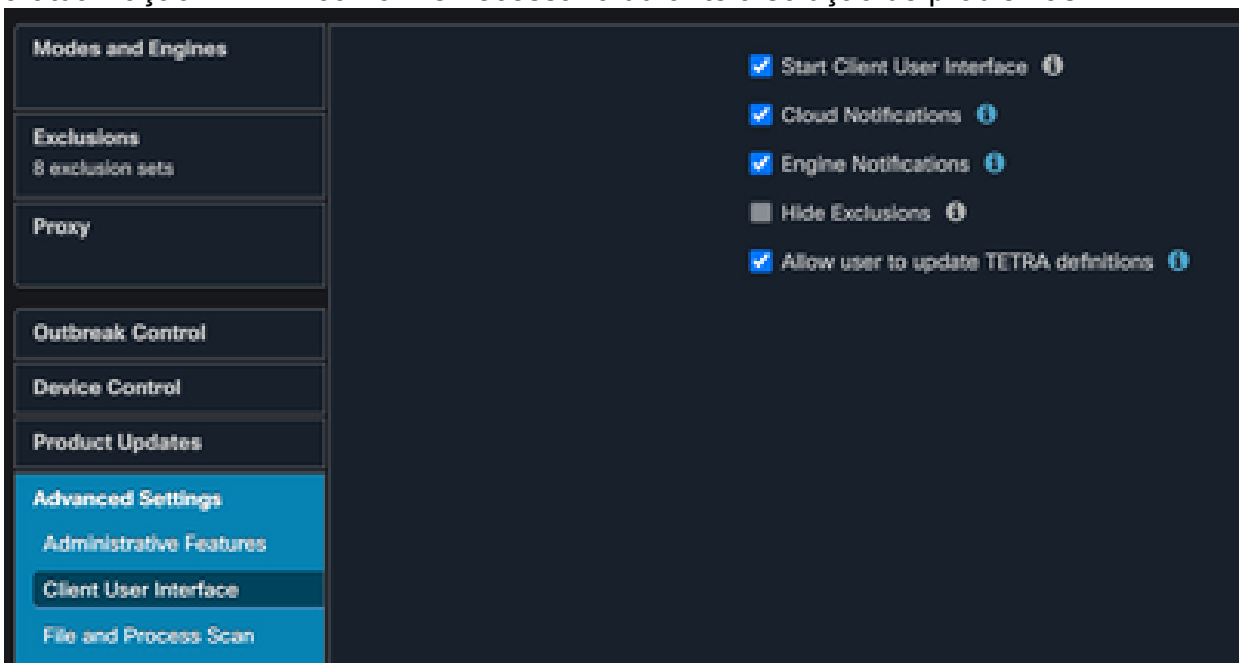
3. No debug sfc.exe.log, as definições atualizadas falharam com o erro 3000, que significa Unknown_Error como documentado.
   <#root>

```
(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
```

Solução

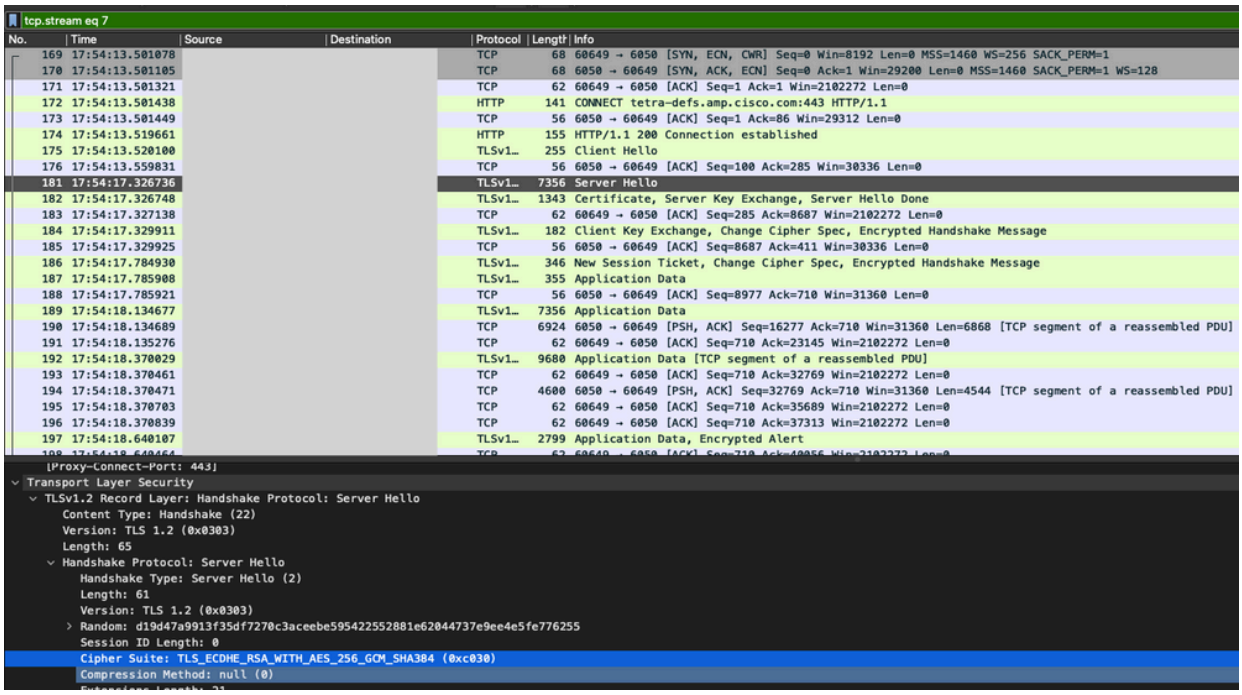
1. Habilite a opção Permitir que o usuário atualize as definições TETRA na Política AMP > Interface de usuário do cliente no Console. Com esse parâmetro, você pode acionar a atualização TETRA conforme necessário durante a solução de problemas.



2. Além disso, habilite o debug Connector e o log no nível da bandeja no endpoint ou através da política AMP.

3. Retire as capturas de pacotes tanto na atualização TETRA bem-sucedida como no ponto final com falha para Definições TETRA enquanto clica em Atualizar TETRA no ponto final.

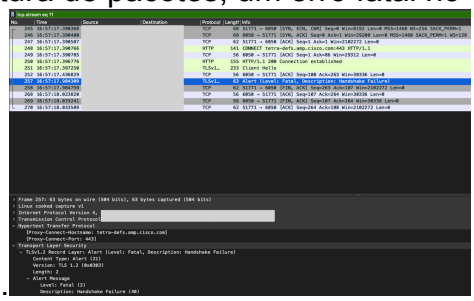
4. No endpoint bem-sucedido de atualização de TETRA, na captura de pacotes, filtre os pacotes com http.host == "tetra-defs.amp.cisco.com:443" e depois "siga o tcp.stream" de cada pacote para analisar o tráfego relacionado.
5. No pacote Server Hello, você pode ver que o servidor aceita a cifra "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" no pacote Server Hello.



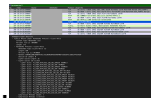
6. O servidor TETRA do Cisco Secure Endpoint aceita apenas cifras mencionadas:

```
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
```

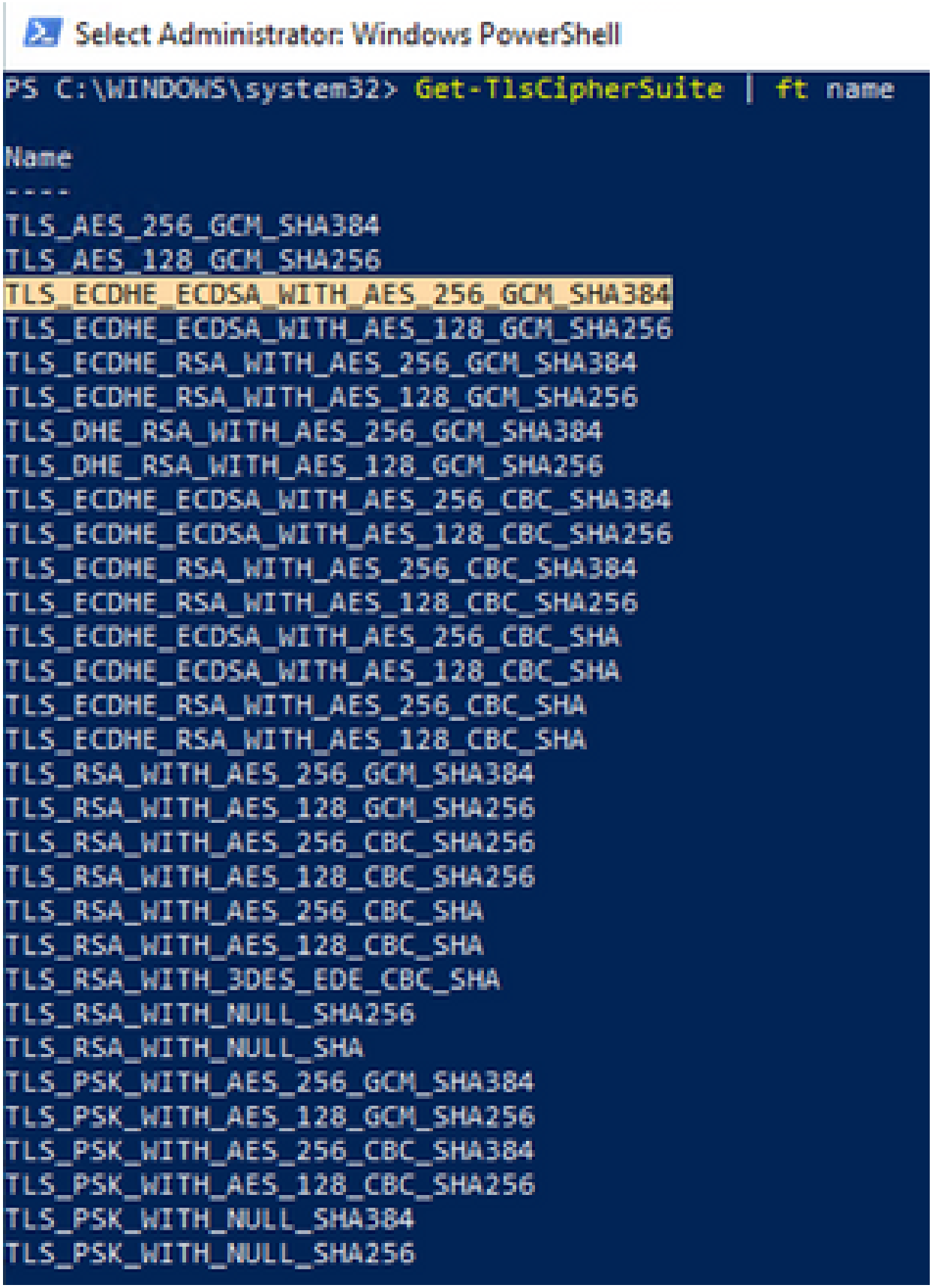
7. No endpoint com falha de atualização TETRA, na captura de pacotes, um erro fatal no handshake SSL é visto após o pacote Hello do cliente.



8. No pacote Hello do cliente, você pode ver as Cifras oferecidas do ponto final.

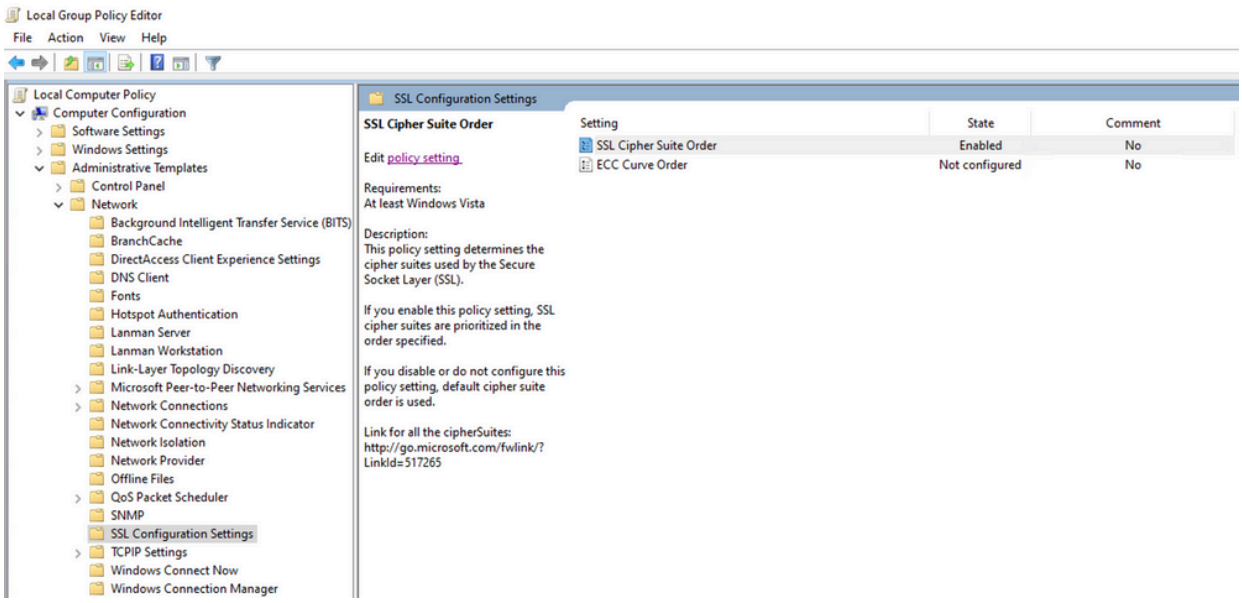


9. Além disso, você pode verificar as Cifras habilitadas no endpoint com o Get-TlsCipherSuite | ft name Comando do PowerShell.

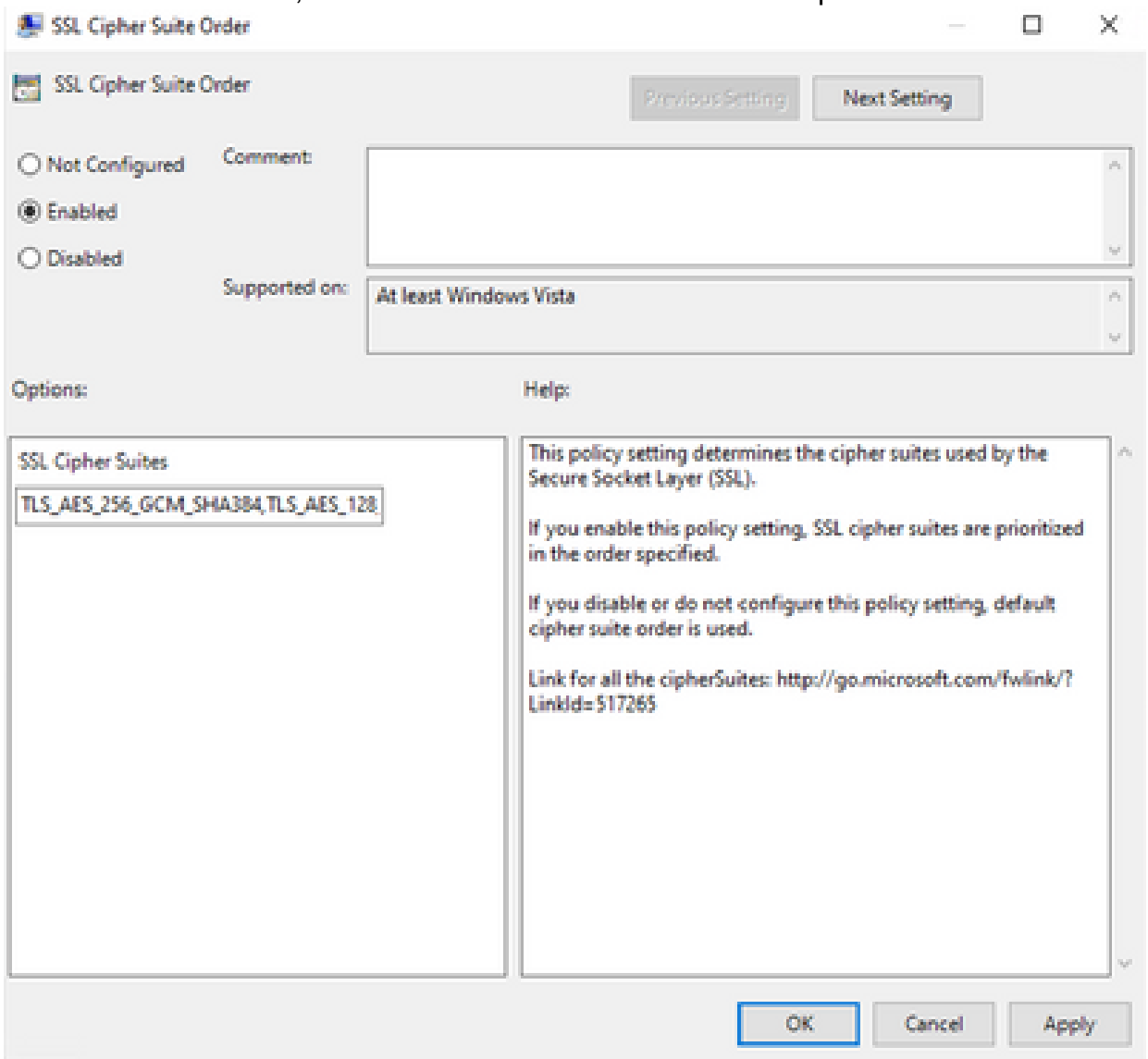


10. Caso as cifras mencionadas na Etapa 6 não estejam listadas aqui, esse é o motivo da falha de handshake SSL.
11. Para corrigir isso, verifique a Ordem do Conjunto de Cifras SSL na Política de Grupo:

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



12. A ordem do conjunto de cifras deve ser Não configurado ou Desativado e, se estiver definida como Ativado, adicione as cifras mencionadas na Etapa 6 na lista.



13. Aplique essas alterações e reinicie o endpoint para disponibilizar essas alterações para os aplicativos.
14. Tente novamente Atualizar TETRA quando a reinicialização estiver concluída.

15. Caso o problema das definições TETRA persista, analise os registros e as capturas novamente.

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.