Cisco Secure Endpoint - Fehler beim Update der Tetradefinitionen mit Fehler 3000

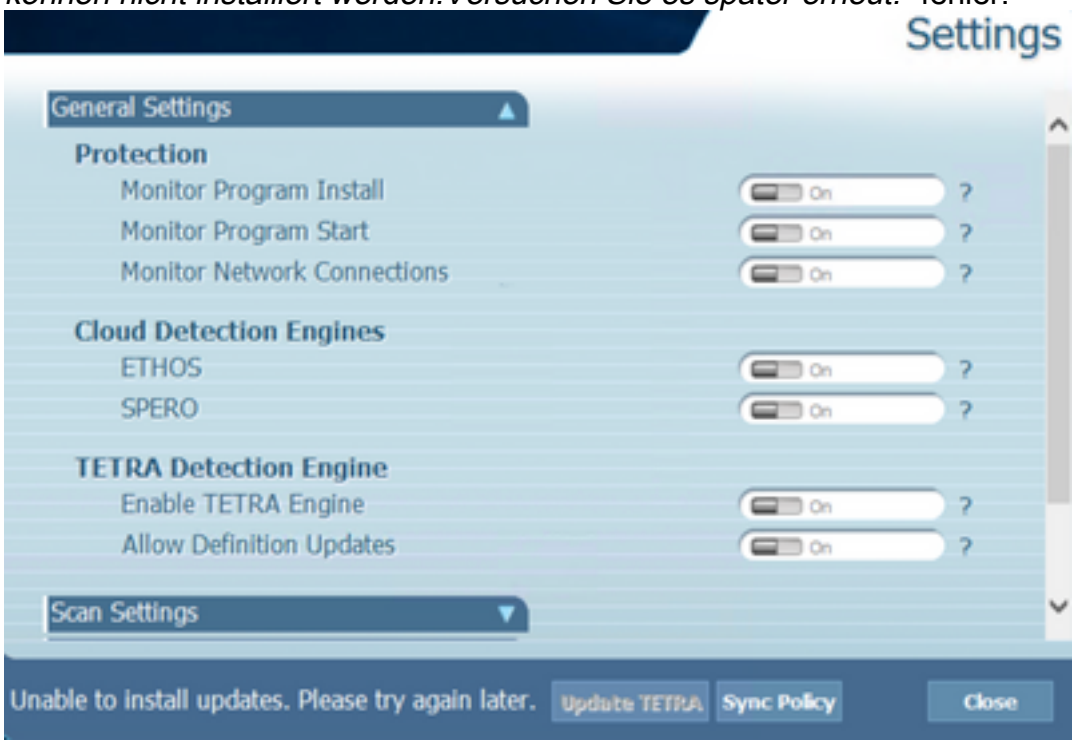
Inhalt

Einleitung

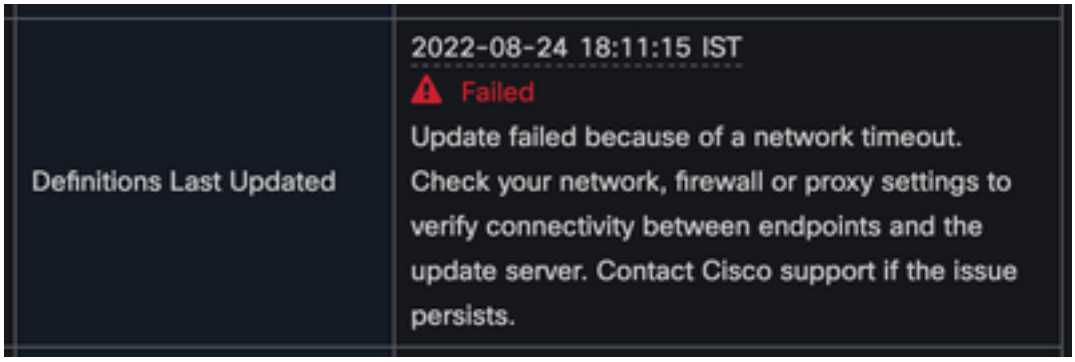
In diesem Dokument werden die Schritte zur Fehlerbehebung bei Tetra-Definitionen mit Fehler 3000 beschrieben.

Problembeschreibung

1. Auf dem Endpunkt schlägt die Aktualisierung der Tetradefinitionen fehl mit "*Updates können nicht installiert werden.Versuchen Sie es später erneut.*" fehler.



2. Auf der AMP-Konsole wird der erwähnte Fehlerfehler festgestellt: ***Fehlgeschlagen****Aktualisierung aufgrund eines Netzwerk-Timeouts fehlgeschlagen. Überprüfen Sie Ihre Netzwerk-, Firewall- oder Proxy-Einstellungen, um die Verbindung zwischen den Endpunkten und dem Update-Server zu überprüfen. Wenden Sie sich an den Cisco Support, wenn das Problem weiterhin besteht.*

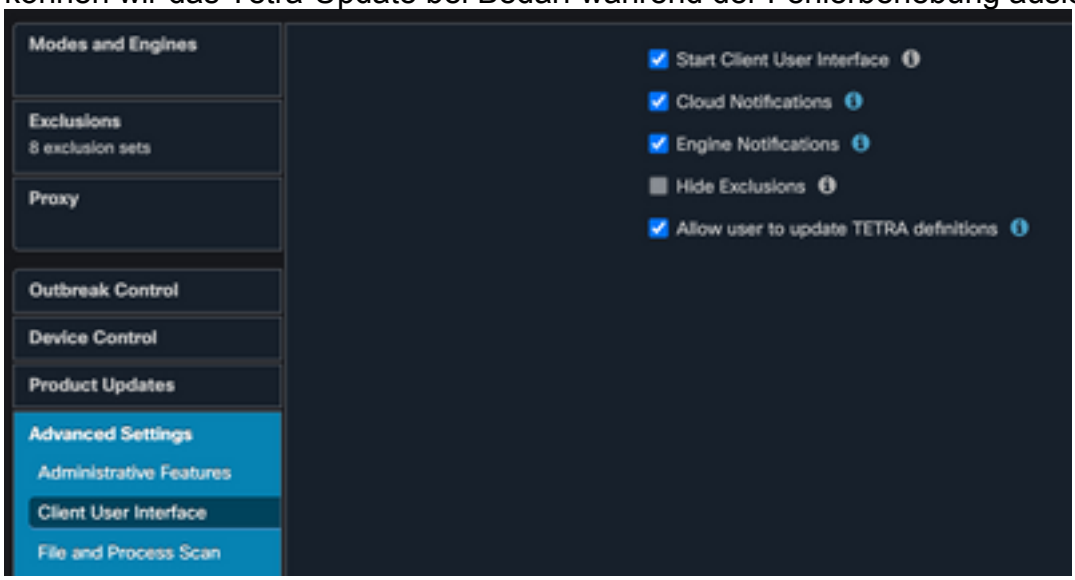


3. Im debug sfc.exe.log wurden Definitionen aktualisiert, die mit Fehler 3000 fehlschlugen. Dieser Fehler steht für "*Unknown_Error*", wie dokumentiert.

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TetraUpdateInterface::update updateDir:
C:\Program Files\Cisco\AMP\tetra, 20, -3000, -3000, 0, 0, 0
(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, id: 0
(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>::ReleaseInstance count: 1
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTetraUpdate: bUpdated = FALSE, state:
20, status: -3000
(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,
first failure - never, last err code - 4294964296, last upd success - never
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0,
first failure - Thu Aug 4 06:35:16 2022, last err code - 4294964296, last upd success -
never
```

Lösung

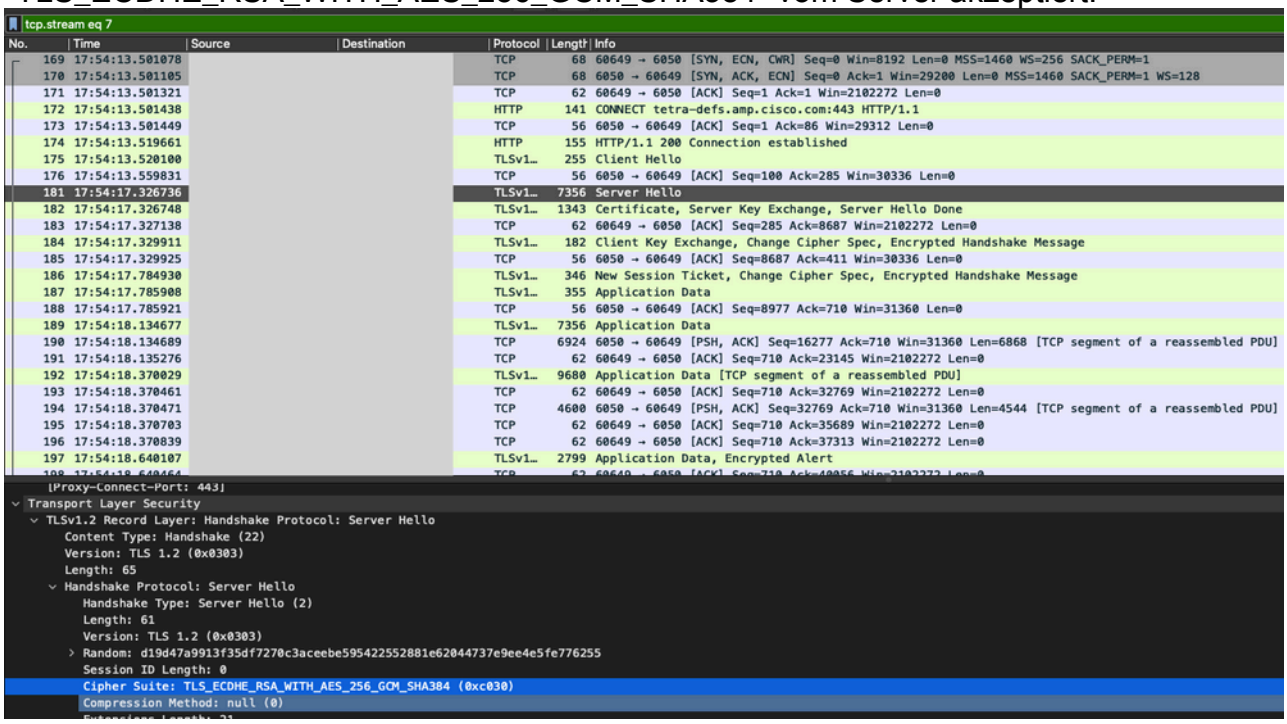
1. Aktivieren Sie die Option "Aktualisierung der Tetra-Definitionen durch Benutzer zulassen" in AMP-Richtlinie -> Client-Benutzeroberfläche auf der Konsole. Mit diesem Parameter können wir das Tetra-Update bei Bedarf während der Fehlerbehebung auslösen.



2. Aktivieren Sie außerdem die Option debug Connector and Tray-level log on the endpoint or via AMP Policy.

3. Bitte nehmen Sie die Paketerfassung sowohl auf dem erfolgreichen als auch auf dem fehlgeschlagenen Tetra-Endpunkt für Tetra-Definitionen vor, während Sie auf dem Endpunkt auf 'Tetra aktualisieren' klicken.

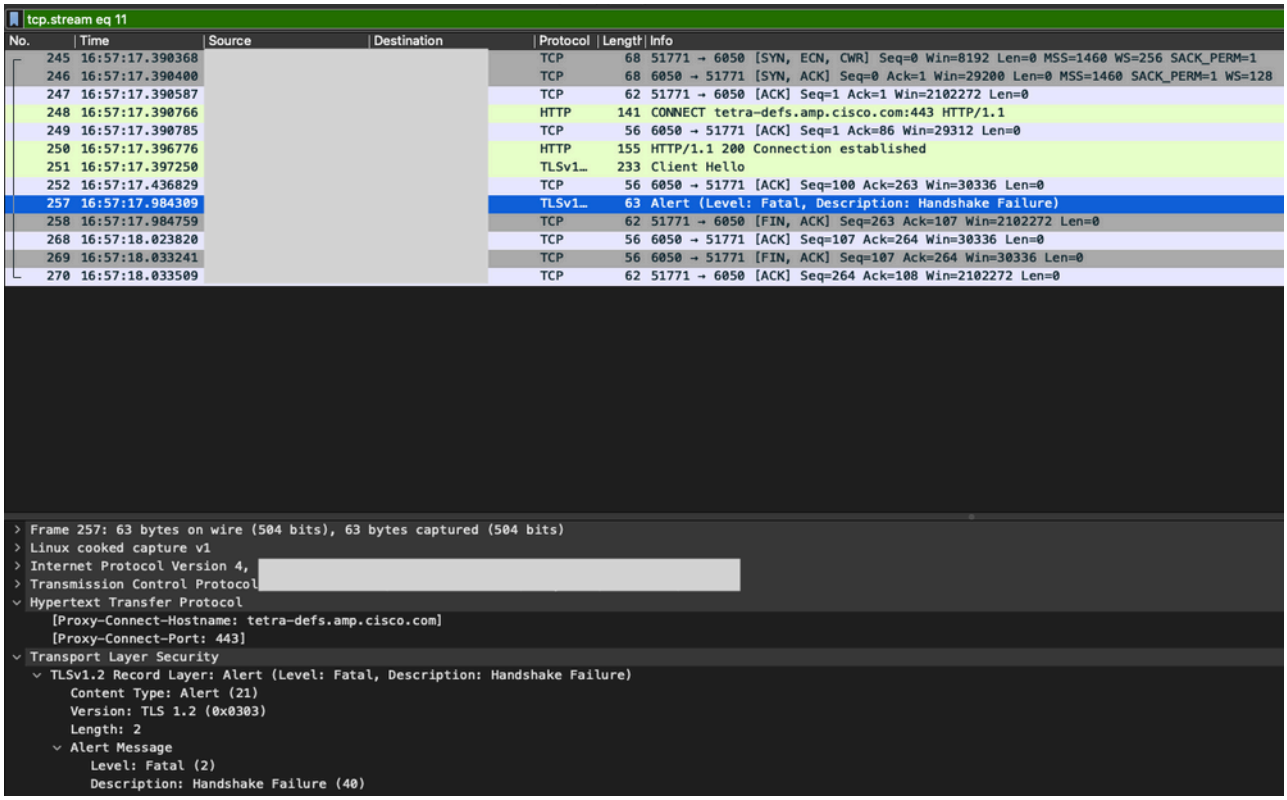
4. AufTetra Update erfolgreichen Endpunkt, in Paket-Capture-Filter die Pakete mit **http.host == "tetra-defs.amp.cisco.com:443"** und dann folgen Sie der tcp.stream jedes Pakets, um den zugehörigen Datenverkehr zu analysieren.
5. Im Paket "Server Hello" wird der Schlüssel "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" vom Server akzeptiert.



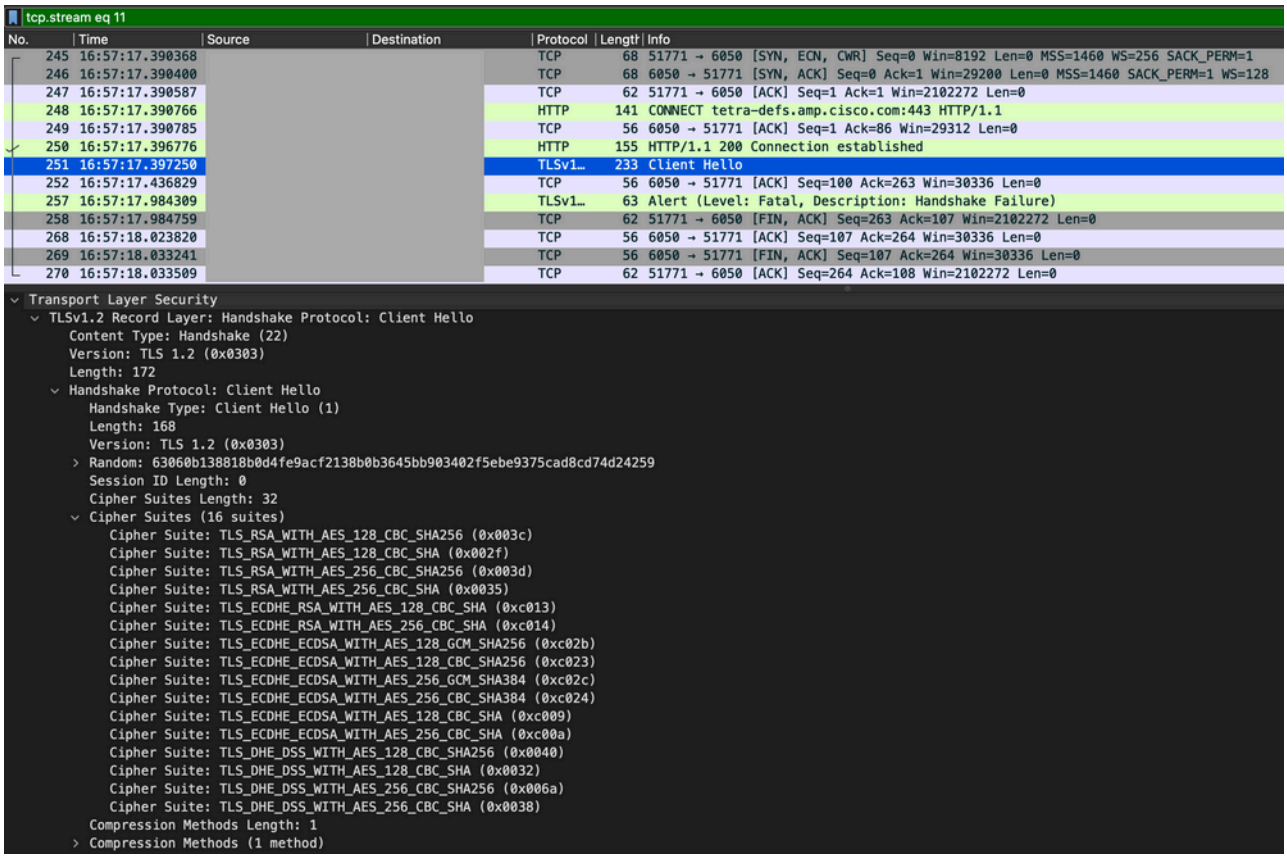
6. Der AMP Tetra-Server akzeptiert nur die folgenden Ciphers:

```
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
```

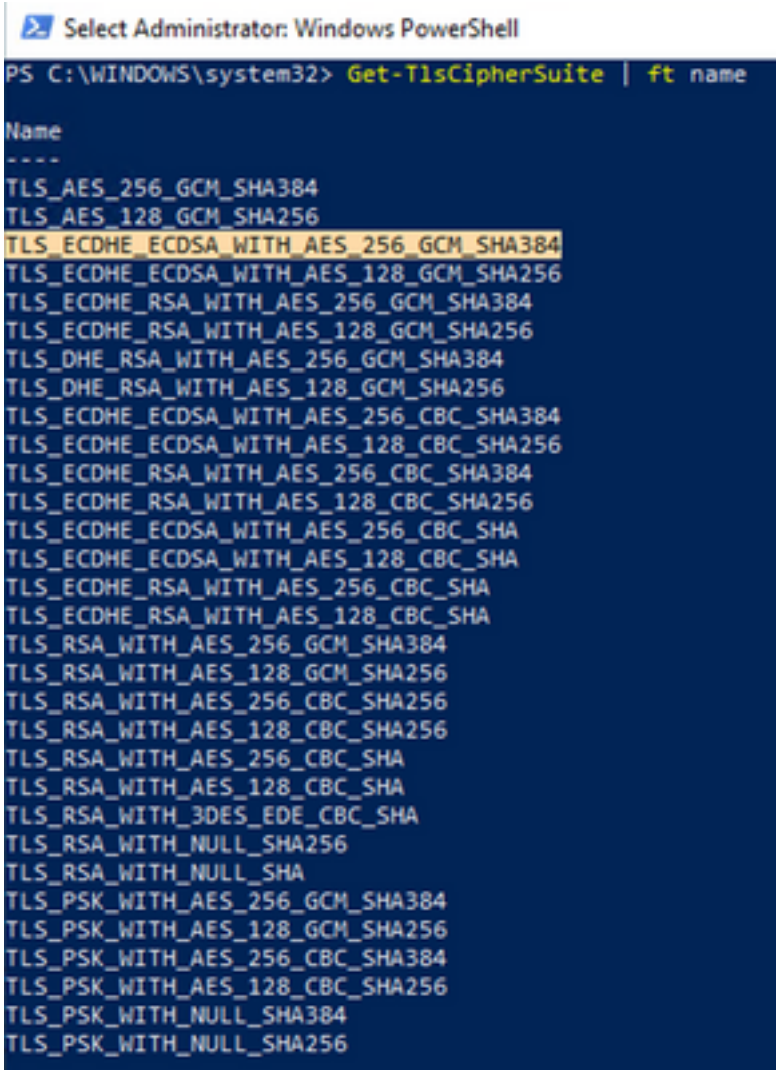
7. Bei einem Tetra-Update-Endpunkt, der bei der Paketerfassung fehlschlug, tritt nach dem Client Hello-Paket ein schwerwiegender Fehler beim SSL-Handshake auf.



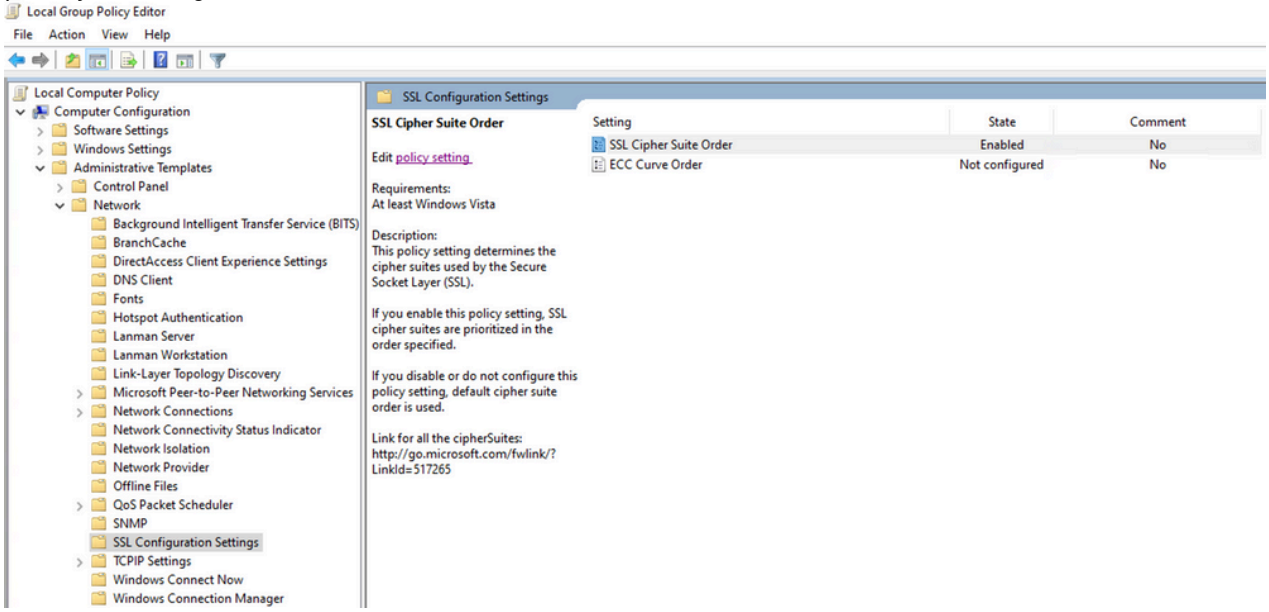
8. Im Paket "Client Hello" können Sie die angebotenen Ciphers vom Endpunkt aus sehen.



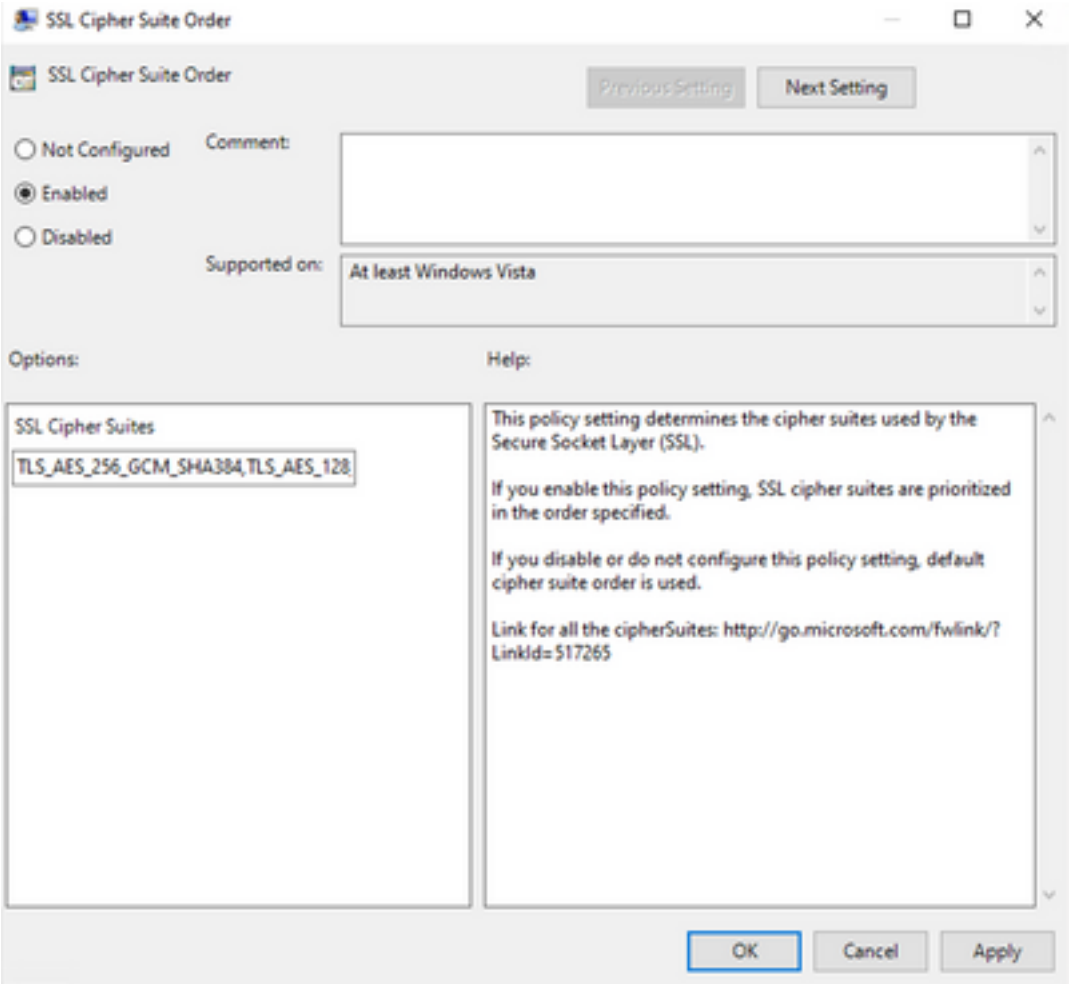
9. Darüber hinaus können Sie die aktivierten Ciphers auf dem Endpunkt mit "Get-TlsCipherSuite" überprüfen | ft name' PowerShell-Befehl.



10. Falls die in Schritt 6. erwähnten Chiffren hier nicht aufgeführt sind, ist dies der Grund für den SSL-Handshake-Fehler.
11. Um dies zu beheben, überprüfen Sie die "SSL Cipher Suite Order" in der Gruppenrichtlinie:
    `Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Templates -> Network -> SSL Configuration Settings -> SSL Cipher Suite Order -> Edit policy setting`



12. Die Cipher Suite Order muss 'Not Configured' oder 'Disabled' sein, und wenn sie auf 'Enabled' gesetzt ist, fügen Sie die in Schritt 6 erwähnten Chiffren in der Liste hinzu.



13. Wenden Sie diese Änderungen an, und starten Sie den Endpunkt neu, um diese Änderungen für Anwendungen verfügbar zu machen.
14. Versuchen Sie erneut, "Tetra aktualisieren", sobald der Neustart abgeschlossen ist.
15. Falls das Problem mit den Tetra-Definitionen weiterhin besteht, analysieren Sie die Protokolle und erfassen sie erneut.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.