# Troubleshoot TETRA Definitions Update Failure with 3000 Error

## Contents



## Introduction

This document describes steps to troubleshoot TETRA Definitions failure with error 3000 error.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Endpoint

### Components Used

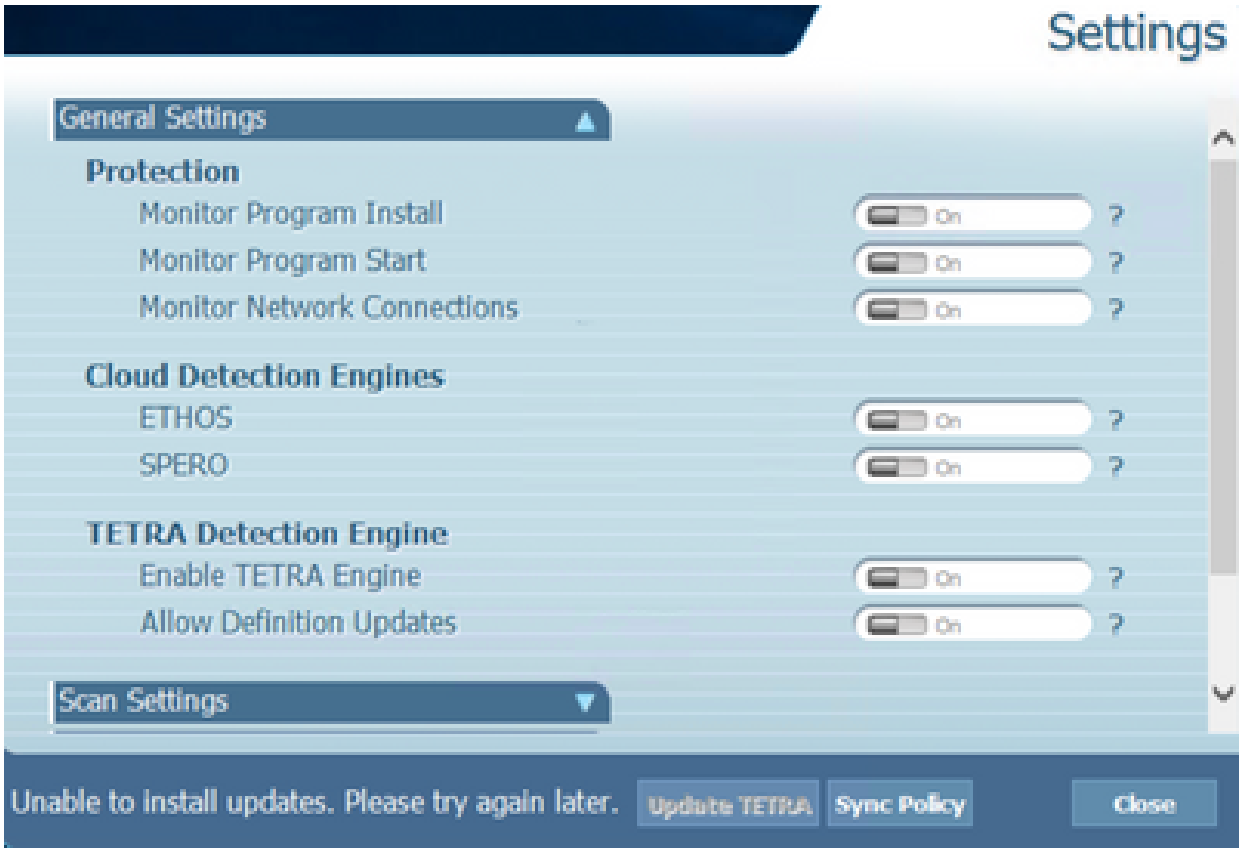
The information in this document is based on:

- Cisco Secure Endpoint connector (any version)
- Wireshark (any version)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

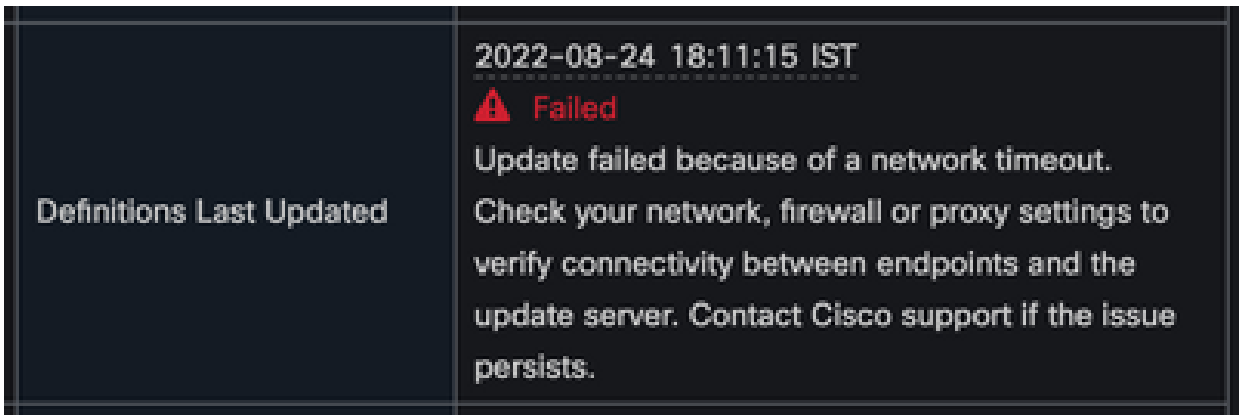
## Problem

1. On endpoint, TETRA Definitions update fail with "Unable to install updates.Please try again later" error message.




2. On Cisco Secure Endpoint Console, mentioned failure error is observed:

   "Update failed because of a network timeout. Check your network, firewall or proxy settings to verify connectivity between endpoints and the update server. Contact Cisco support if the issue persists."



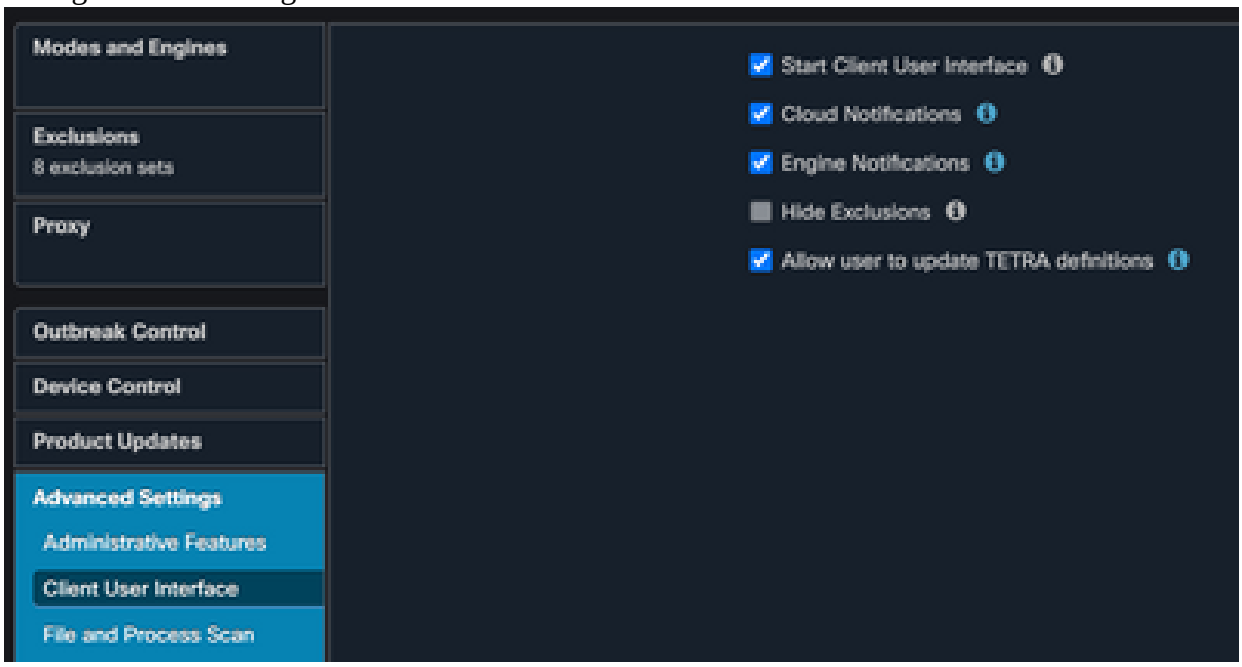

3. In **debug** sfc.exe.log, definitions updated failed with error 3000 error is observed, which stands for Unknown_Error as documented.
   <#root>

```
(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
```

# Solution

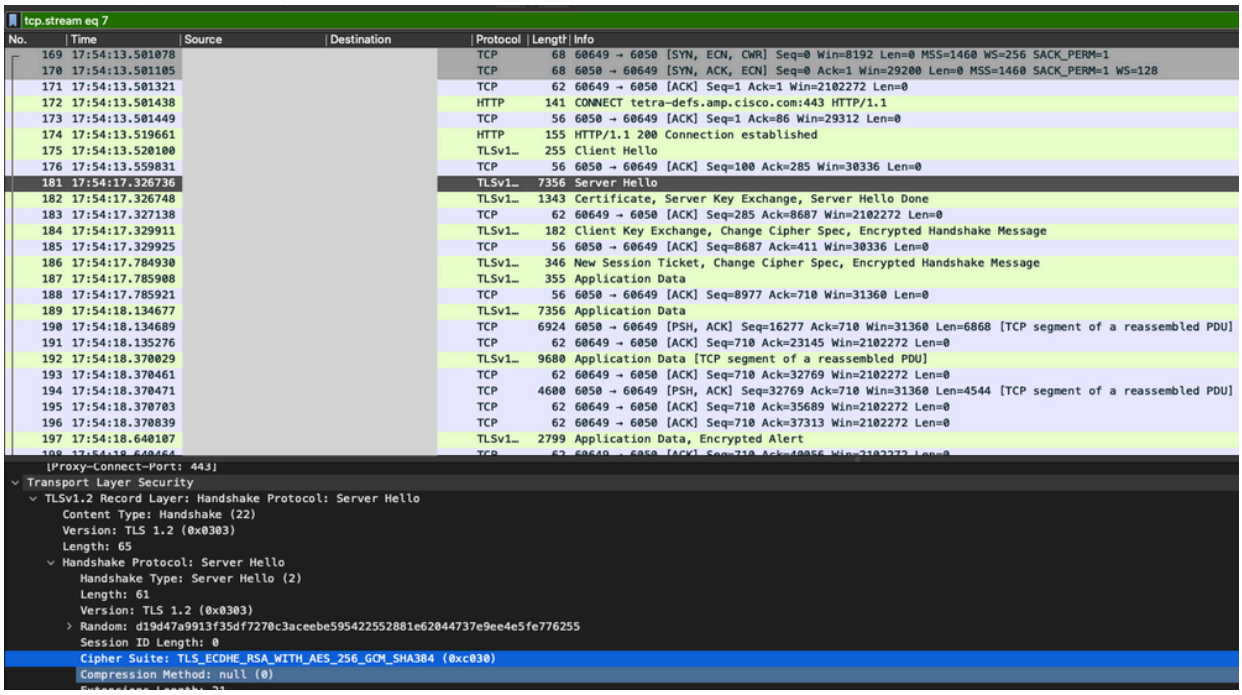
1. Please enable **Allow user to update TETRA definitions** option in **AMP Policy > Client User Interface** on the Console. With this parameter you can trigger TETRA update as required during troubleshooting.




2. Also, enable debug Connector and Tray-level log on the endpoint or via AMP Policy.

3. Please take packet captures on both TETRA update successful and failed endpoint for TETRA Definitions while you click **Update TETRA** on endpoint.

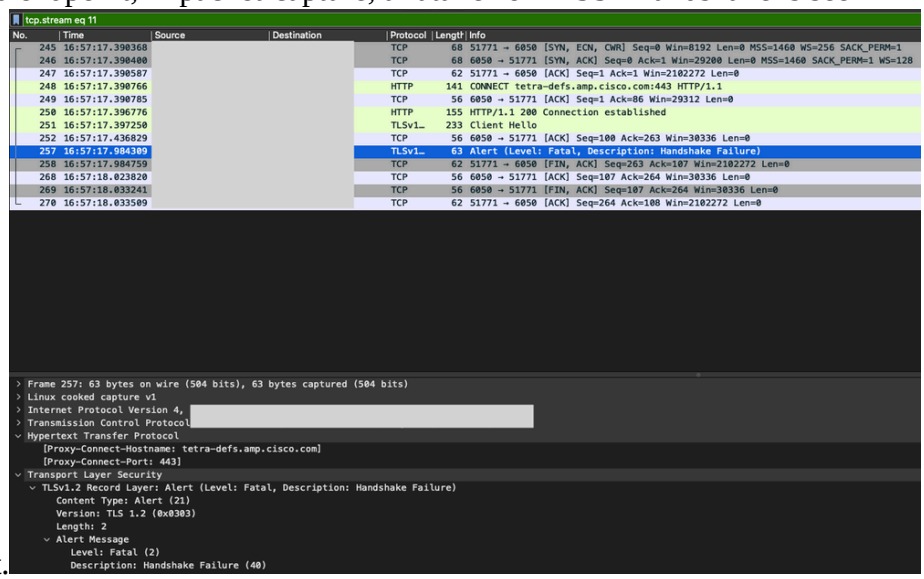
4. On TETRA update successful endpoint, in packet-capture filter the packets with **http.host == "tetra-defs.amp.cisco.com:443"** and then **"follow the tcp.stream"** of each packets to analyse the related traffic.
5. In **Server Hello** packet, you can see the Server accepts "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" cipher in Server Hello packet.

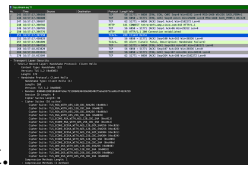



6. Cisco Secure Endpoint TETRA server accepts only mentioned Ciphers:

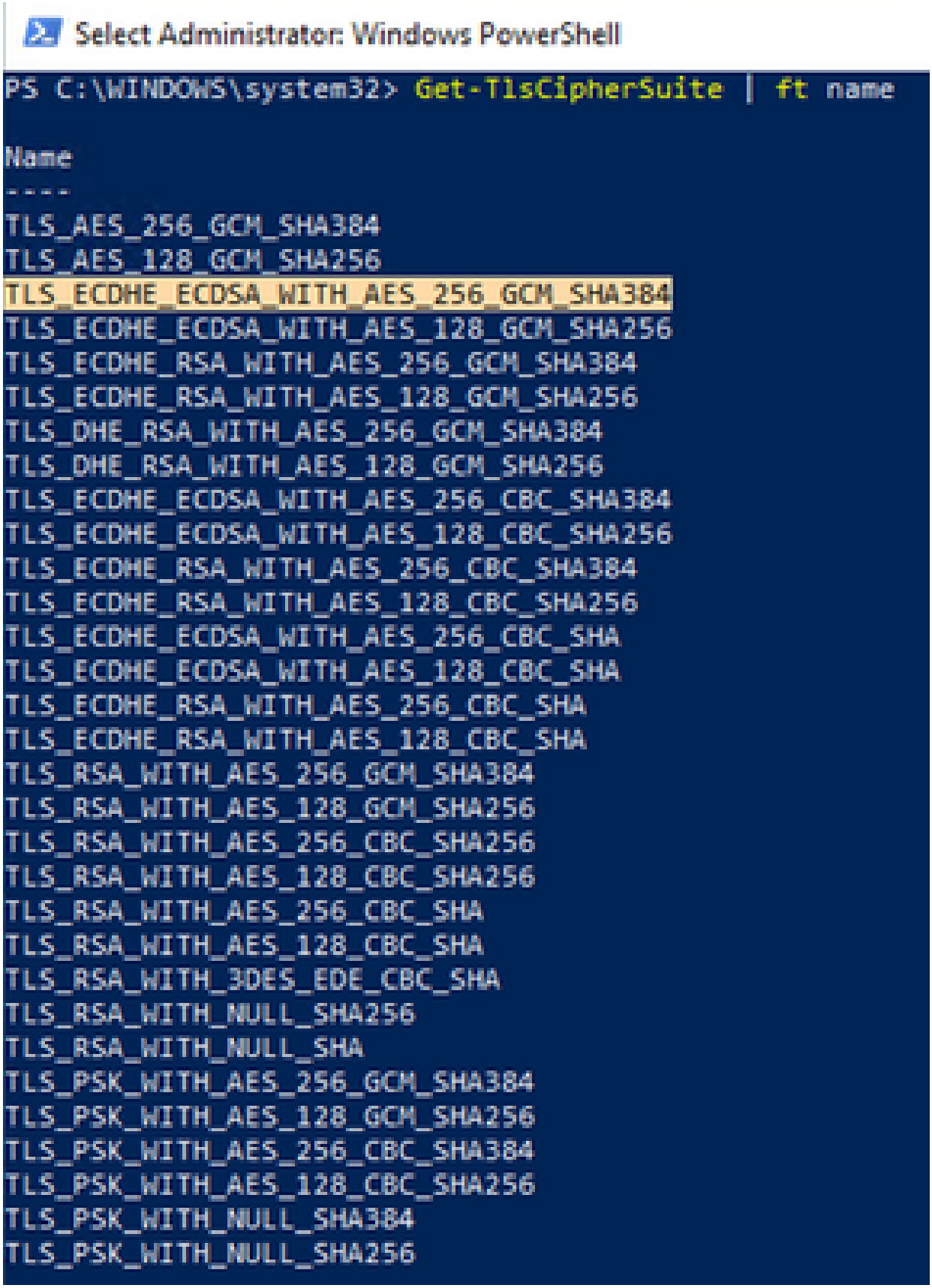
```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_AES_128_GCM_SHA256
```

7. On TETRA update failed endpoint, in packet-capture, a fatal error in SSL handshake is seen after Client Hello packet.



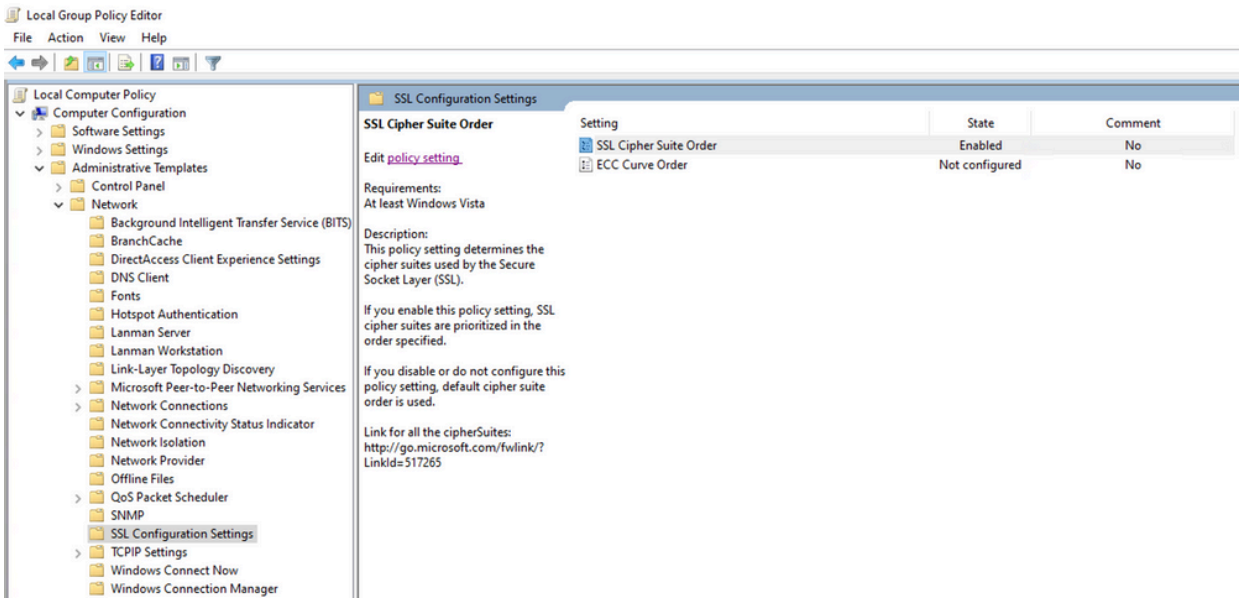



8. In the Client Hello packet, you can see the offered Ciphers from the endpoint.
9. In addition, you can cross-verify the enabled Ciphers on endpoint with the **Get-TlsCipherSuite | ft name** PowerShell command.

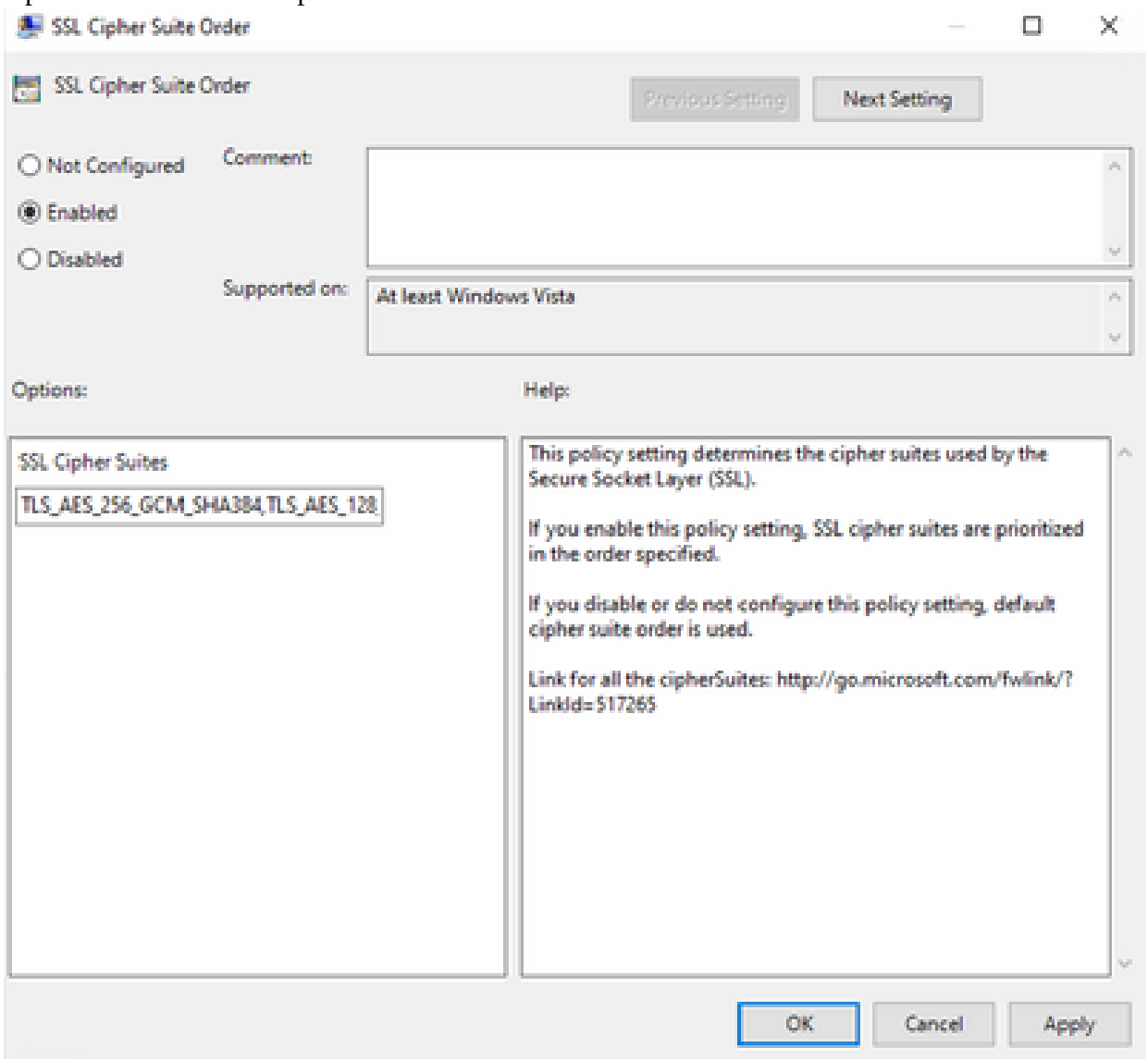



10. In case the ciphers mentioned in Step 6 are not listed here, that is the reason for the SSL handshake failure.
11. To fix this, please verify the **SSL Cipher Suite Order** in the Group Policy:

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




12. The Cipher Suite Order must be **Not Configured** or **Disabled** and if set to **Enabled**, add the ciphers mentioned in Step 6 in the list.




13. Apply these changes and reboot the endpoint to bring these changes available for applications.
14. Please retry **Update TETRA** once the reboot is completed.
15. In case the TETRA Definitions issue persists, please analyze the logs and captures again.

## Related Information

- **Cisco Technical Support & Downloads**