# Troubleshoot TETRA Definitions Update Failure with 3000 Error

#### **Contents**

**Introduction** 

**Prerequisites** 

Requirements

Components Used

**Problem** 

**Solution** 

**Related Information** 

## 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.

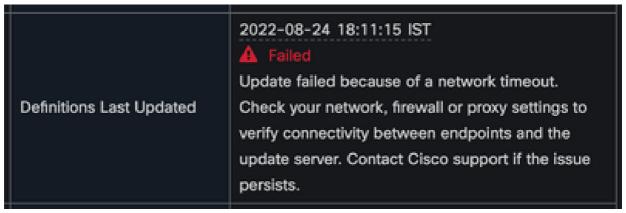
## **Problem**

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]: TETRAUpdaterInit bUpdate: 0, bReload: 0

```
(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

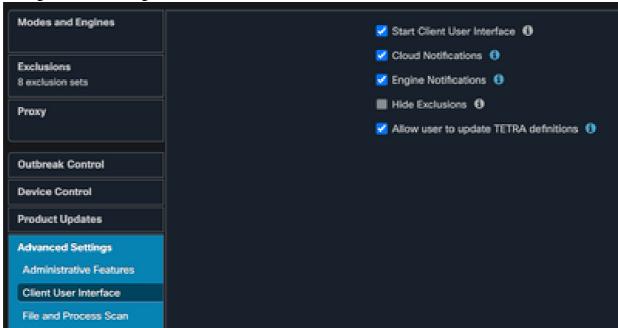
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PipeSend: sending message to user interface: 26, (978223515, +0 ms) Aug 04 07:30:23 [860]: PipeWrite: waiting on pipe event handle (978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit defInit: 0, bUpdate: 0
```

(978223515, +0 ms) Aug 04 07:30:23 [11944]: 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.

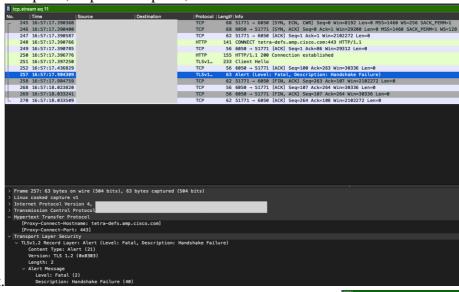
```
174 17:54:13.519661
                                                                                                                                                                                                                                                                                                                                                                                                                              255 Client Hello
56 6050 - 60649 [ACK] Seq=100 Ack=285 Win=30336 Len=0
   175 17:54:13.520100
                                                                                                                                                                                                                                                                                                                                                                          TLSv1...
   176 17:54:13.559831
                                                                                                                                                                                                                                                                                                                                                                                                                       356 Server Hello

1343 Certificate, Server Key Exchange, Server Hello Done
62 60649 - 6050 (ACK) Seq=285 Ack=8687 Win=2102272 Len=0
                                                                                                                                                                                                                                                                                                                                                                         TLSv1_ 1343 Certificate, Server Try 62 60649 - 6050 [ACK] Seq=285 Ack=8687 Win=21022/2 Lene Try 62 60649 - 6050 [ACK] Seq=285 Ack=8687 Win=21022/2 Lene Try 62 6050 - 60649 [ACK] Seq=8687 Ack=411 Win=30336 Lene Try 6650 - 60649 [ACK] Seq=8687 Ack=411 Win=30336 Lene Try 6650 - 60649 [ACK] Seq=8687 Ack=411 Win=30336 Lene Try 6650 - 60649 [ACK] Seq=8687 Ack=411 Win=30336 Lene Try 6650 - 60649 [ACK] Seq=8687 Ack=411 Win=30336 Lene Try 6650 - 60649 [ACK] Seq=8687 Ack=411 Win=30336 Lene Try 6650 - 60649 [ACK] Seq=8687 Ack=411 Win=30336 Lene Try 6650 - 60649 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=2102222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=210222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=210222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=210222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=210222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=210222 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=21022 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=21022 Lene Try 6650 - 6050 [ACK] Seq=8687 Ack=8687 Win=21022 Lene Try 6650 - 6050 [ACK] Seq=8687 Win
   185 17:54:17.329925
                                                                                                                                                                                                                                                                                                                                                                         186 17:54:17.784930
   187 17:54:17.785908
   188 17:54:17.785921
189 17:54:18.134677
190 17:54:18.134689
191 17:54:18.135276
   192 17:54:18.370029
                                                                                                                                                                                                                                                                                                                                                                         | Martin | M
   193 17:54:18.370461
 194 17:54:18.370471
195 17:54:18.370703
196 17:54:18.370839
197 17:54:18.640107
   IND. ATTEMATE CONTROL
| Proxy-Connect-Port: 443|
ansport Layer Security
TLSV1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x8383)
Length: 65
                   Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
                                 Handshake Type: Server Hello (2)
Length: 61
Version: TL5 1.2 (0x0303)
Randon: d19d47a9913f33df7770c3aceebe595422552881e62044737e9ee4e5fe776255
Session ID Length: 0
Cipher Suite: TL5_ECDHE_RSA_WITH_AES_256_GOW_SHA384 (0xc030)
```

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.

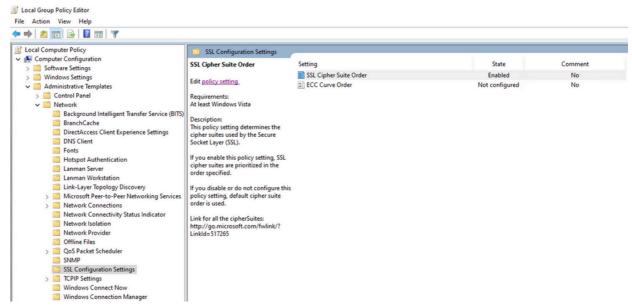
8. In the Client Hello packet, you can see the offered Ciphers from the endpoint.

9. In addition, you can cross-verify the enabled Ciphers on endpoint with the **Get-TlsCipherSuite** | **ft name** PowerShell command.

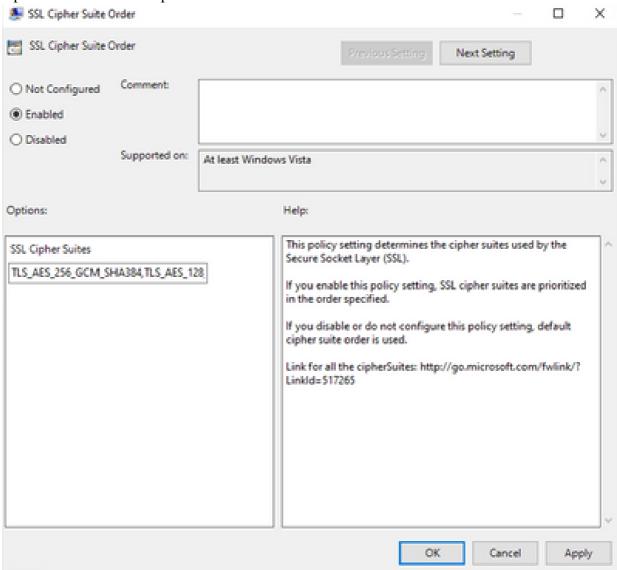
## Select Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> Get-TlsCipherSuite | ft name
Name
TLS AES 256 GCM SHA384
TLS_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS ECDHE ECDSA WITH AES 128 GCM SHA256
TLS ECDHE RSA WITH AES 256 GCM SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS DHE RSA WITH AES 128 GCM SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS ECDHE RSA WITH AES 256 CBC SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS ECDHE ECDSA WITH AES 128 CBC SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS RSA WITH AES 256 GCM SHA384
TLS RSA WITH AES 128 GCM SHA256
TLS RSA WITH AES 256 CBC SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS RSA WITH AES 256 CBC SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS RSA WITH 3DES EDE CBC SHA
TLS RSA WITH NULL SHA256
TLS_RSA_WITH_NULL_SHA
TLS_PSK_WITH_AES_256_GCM_SHA384
TLS_PSK_WITH_AES_128_GCM_SHA256
TLS_PSK_WITH_AES_256_CBC_SHA384
TLS_PSK_WITH_AES_128_CBC_SHA256
TLS_PSK_WITH_NULL_SHA384
TLS_PSK_WITH_NULL_SHA256
```

- 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:



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