

Cisco Secure Endpoint - Tetra 정의 업데이트 실패(3000 오류)

목차

[소개](#)

[문제 설명](#)

[솔루션](#)

소개

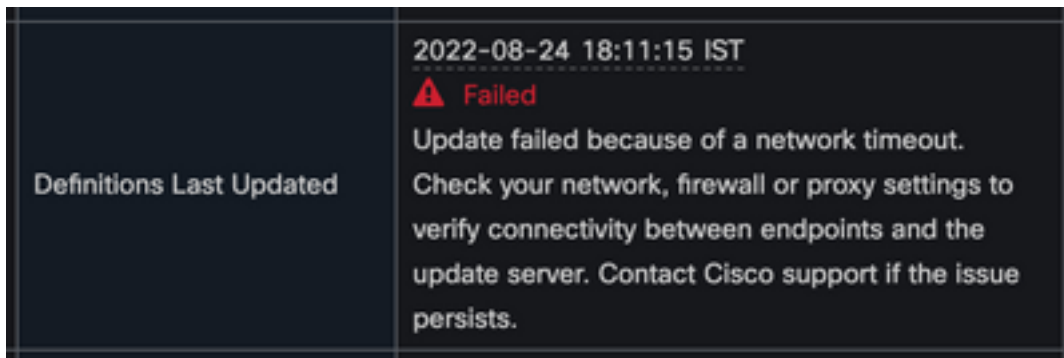
이 문서에서는 오류 3000 오류와 함께 Tetra 정의 오류를 해결하는 단계를 설명합니다.

문제 설명

1. 엔드포인트에서 tetra 정의 업데이트가 실패하고 '업데이트를 설치할 수 없습니다. 나중에 다시 시도하십시오.' 오류.



2. AMP Console에서 언급된 오류 메시지가 관찰됩니다. **실패** 네트워크 시간 초과로 인해 업데이트하지 못했습니다. 네트워크, 방화벽 또는 프록시 설정을 확인하여 엔드포인트와 업데이트 서버 간의 연결을 확인합니다. 문제가 계속되면 Cisco 지원에 문의하십시오.

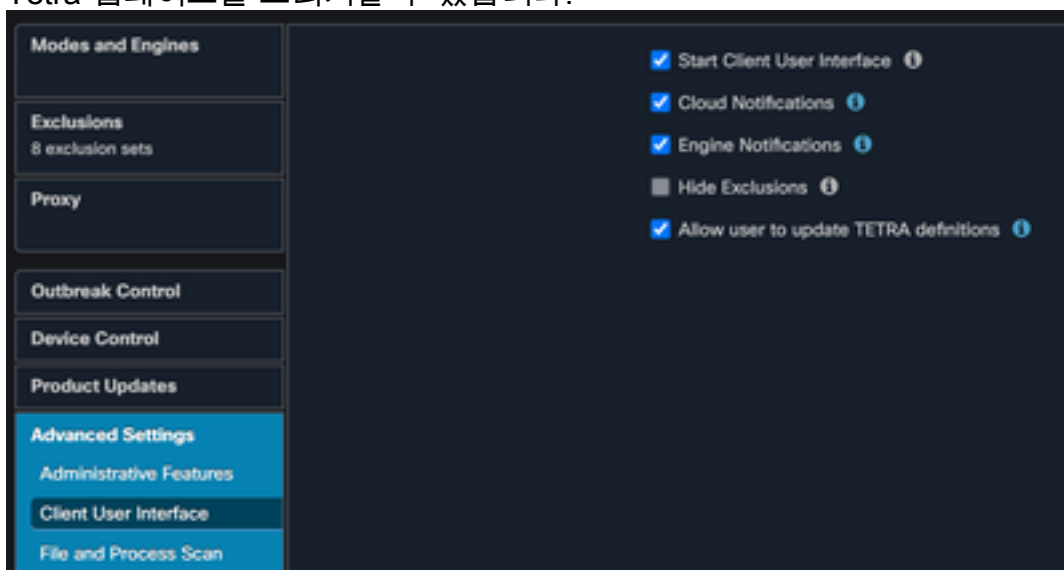


3. debug sfc.exe.log에서는 오류 3000 오류와 함께 업데이트된 정의가 관찰되며, 이는 문서화된 'Unknown_Error'를 나타냅니다.

```
(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
```

솔루션

1. 콘솔의 AMP 정책 -> 클라이언트 사용자 인터페이스에서 'Allow user to update Tetra definitions' 옵션을 활성화하십시오. 이 매개변수를 사용하면 문제 해결 중에 필요에 따라 Tetra 업데이트를 트리거할 수 있습니다.



2. 또한 엔드포인트에서 또는 AMP 정책을 통해 디버그 커넥터 및 트레이 레벨 로그를 활성화합니다.

- 엔드포인트에서 'Update Tetra'를 클릭하는 동안 Tetra 업데이트에 성공하거나 실패한 엔드포인트 모두에서 패킷 캡처를 받으십시오.
- OnTetra에서 성공한 엔드포인트를 업데이트하면 패킷 캡처에서 패킷을 `http.host == "tetra-defs.amp.cisco.com:443"`으로 필터링한 다음 각 패킷의 `tcp.stream`을 따라 관련 트래픽을 분석합니다.
- 'Server Hello' 패킷에서는 Server가 Server Hello 패킷의 'TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384' 암호를 수락하는 것을 볼 수 있습니다.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|--------|-------------|----------|--------|-------------------------------------------------------------------------------------------------|
| 169 | 17:54:13.501078 | | | TCP | 68 | 60649 → 6050 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 170 | 17:54:13.501105 | | | TCP | 68 | 6050 → 60649 [SYN, ACK, ECN] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 171 | 17:54:13.501321 | | | TCP | 62 | 60649 → 6050 [ACK] Seq=1 Ack=1 Win=2102272 Len=0 |
| 172 | 17:54:13.501438 | | | HTTP | 141 | CONNECT tetra-defs.amp.cisco.com:443 HTTP/1.1 |
| 173 | 17:54:13.501449 | | | TCP | 56 | 6050 → 60649 [ACK] Seq=1 Ack=86 Win=29312 Len=0 |
| 174 | 17:54:13.519661 | | | HTTP | 155 | HTTP/1.1 200 Connection established |
| 175 | 17:54:13.520100 | | | TLSv1.. | 255 | Client Hello |
| 176 | 17:54:13.559831 | | | TCP | 56 | 6050 → 60649 [ACK] Seq=100 Ack=285 Win=30336 Len=0 |
| 181 | 17:54:17.326736 | | | TLSv1.. | 7356 | Server Hello |
| 182 | 17:54:17.326748 | | | TLSv1.. | 1343 | Certificate, Server Key Exchange, Server Hello Done |
| 183 | 17:54:17.327138 | | | TCP | 62 | 60649 → 6050 [ACK] Seq=285 Ack=8687 Win=2102272 Len=0 |
| 184 | 17:54:17.329911 | | | TLSv1.. | 182 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 185 | 17:54:17.329925 | | | TCP | 56 | 6050 → 60649 [ACK] Seq=8687 Ack=411 Win=30336 Len=0 |
| 186 | 17:54:17.784930 | | | TLSv1.. | 346 | New Session Ticket, Change Cipher Spec, Encrypted Handshake Message |
| 187 | 17:54:17.785908 | | | TLSv1.. | 355 | Application Data |
| 188 | 17:54:17.785921 | | | TCP | 56 | 6050 → 60649 [ACK] Seq=8977 Ack=710 Win=31360 Len=0 |
| 189 | 17:54:18.134677 | | | TLSv1.. | 7356 | Application Data |
| 190 | 17:54:18.134689 | | | TCP | 6924 | 6050 → 60649 [PSH, ACK] Seq=16277 Ack=710 Win=31360 Len=6868 [TCP segment of a reassembled PDU] |
| 191 | 17:54:18.135276 | | | TCP | 62 | 60649 → 6050 [ACK] Seq=710 Ack=23145 Win=2102272 Len=0 |
| 192 | 17:54:18.370029 | | | TLSv1.. | 9680 | Application Data [TCP segment of a reassembled PDU] |
| 193 | 17:54:18.370461 | | | TCP | 62 | 60649 → 6050 [ACK] Seq=710 Ack=32769 Win=2102272 Len=0 |
| 194 | 17:54:18.370471 | | | TCP | 4600 | 6050 → 60649 [PSH, ACK] Seq=32769 Ack=710 Win=31360 Len=4544 [TCP segment of a reassembled PDU] |
| 195 | 17:54:18.370703 | | | TCP | 62 | 60649 → 6050 [ACK] Seq=710 Ack=35689 Win=2102272 Len=0 |
| 196 | 17:54:18.370839 | | | TCP | 62 | 60649 → 6050 [ACK] Seq=710 Ack=37313 Win=2102272 Len=0 |
| 197 | 17:54:18.640107 | | | TLSv1.. | 2799 | Application Data, Encrypted Alert |
| 198 | 17:54:18.640117 | | | TCP | 62 | 60649 → 6050 [ACK] Seq=710 Ack=40056 Win=2102272 Len=0 |

```

[Proxy-Connect-Port: 443]
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 65
    Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 61
      Version: TLS 1.2 (0x0303)
      Random: d19d47a9913f35df7270c3acebe595422552881e62044737e9ee4e5fe776255
      Session ID Length: 0
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Compression Method: null (0)
      Extension Length: 21
  
```

- AMP Tetra 서버는 다음 암호만 허용합니다.

```

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

```

- Tetra 업데이트 실패 엔드포인트에서 패킷 캡처의 경우 Client Hello 패킷 이후에 SSL 핸드셰이크에 치명적인 오류가 발생합니다

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|--------|-------------|----------|--------|---------------------------------------------------------------------------------|
| 245 | 16:57:17.390368 | | | TCP | 68 | 51771 → 6050 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 246 | 16:57:17.390400 | | | TCP | 68 | 6050 → 51771 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 247 | 16:57:17.390587 | | | TCP | 62 | 51771 → 6050 [ACK] Seq=1 Ack=1 Win=2102272 Len=0 |
| 248 | 16:57:17.390766 | | | HTTP | 141 | CONNECT tetra-defs.amp.cisco.com:443 HTTP/1.1 |
| 249 | 16:57:17.390785 | | | TCP | 56 | 6050 → 51771 [ACK] Seq=1 Ack=86 Win=29312 Len=0 |
| 250 | 16:57:17.396776 | | | HTTP | 155 | HTTP/1.1 200 Connection established |
| 251 | 16:57:17.397250 | | | TLSv1.. | 233 | Client Hello |
| 252 | 16:57:17.436829 | | | TCP | 56 | 6050 → 51771 [ACK] Seq=100 Ack=263 Win=30336 Len=0 |
| 257 | 16:57:17.984309 | | | TLSv1.. | 63 | Alert (Level: Fatal, Description: Handshake Failure) |
| 258 | 16:57:17.984759 | | | TCP | 62 | 51771 → 6050 [FIN, ACK] Seq=263 Ack=107 Win=2102272 Len=0 |
| 268 | 16:57:18.023820 | | | TCP | 56 | 6050 → 51771 [ACK] Seq=107 Ack=264 Win=30336 Len=0 |
| 269 | 16:57:18.033241 | | | TCP | 56 | 6050 → 51771 [FIN, ACK] Seq=107 Ack=264 Win=30336 Len=0 |
| 270 | 16:57:18.033509 | | | TCP | 62 | 51771 → 6050 [ACK] Seq=264 Ack=108 Win=2102272 Len=0 |

```

> Frame 257: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, [redacted]
> Transmission Control Protocol [redacted]
  Hypertext Transfer Protocol
    [Proxy-Connect-Hostname: tetra-defs.amp.cisco.com]
    [Proxy-Connect-Port: 443]
  Transport Layer Security
    TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Handshake Failure)
      Content Type: Alert (21)
      Version: TLS 1.2 (0x0303)
      Length: 2
      Alert Message
        Level: Fatal (2)
        Description: Handshake Failure (40)

```

8. Client Hello 패킷에서는 엔드포인트에서 제공된 암호를 볼 수 있습니다

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|--------|-------------|----------|--------|---------------------------------------------------------------------------------|
| 245 | 16:57:17.390368 | | | TCP | 68 | 51771 → 6050 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 246 | 16:57:17.390400 | | | TCP | 68 | 6050 → 51771 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 247 | 16:57:17.390587 | | | TCP | 62 | 51771 → 6050 [ACK] Seq=1 Ack=1 Win=2102272 Len=0 |
| 248 | 16:57:17.390766 | | | HTTP | 141 | CONNECT tetra-defs.amp.cisco.com:443 HTTP/1.1 |
| 249 | 16:57:17.390785 | | | TCP | 56 | 6050 → 51771 [ACK] Seq=1 Ack=86 Win=29312 Len=0 |
| 250 | 16:57:17.396776 | | | HTTP | 155 | HTTP/1.1 200 Connection established |
| 251 | 16:57:17.397250 | | | TLSv1.. | 233 | Client Hello |
| 252 | 16:57:17.436829 | | | TCP | 56 | 6050 → 51771 [ACK] Seq=100 Ack=263 Win=30336 Len=0 |
| 257 | 16:57:17.984309 | | | TLSv1.. | 63 | Alert (Level: Fatal, Description: Handshake Failure) |
| 258 | 16:57:17.984759 | | | TCP | 62 | 51771 → 6050 [FIN, ACK] Seq=263 Ack=107 Win=2102272 Len=0 |
| 268 | 16:57:18.023820 | | | TCP | 56 | 6050 → 51771 [ACK] Seq=107 Ack=264 Win=30336 Len=0 |
| 269 | 16:57:18.033241 | | | TCP | 56 | 6050 → 51771 [FIN, ACK] Seq=107 Ack=264 Win=30336 Len=0 |
| 270 | 16:57:18.033509 | | | TCP | 62 | 51771 → 6050 [ACK] Seq=264 Ack=108 Win=2102272 Len=0 |

```

  Transport Layer Security
    TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 172
      Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 168
        Version: TLS 1.2 (0x0303)
        Random: 63060b138818b0d4fe9acf2138b0b3645bb903402f5ebe9375cad8cd74d24259
        Session ID Length: 0
        Cipher Suites Length: 32
        Cipher Suites (16 suites)
          Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
          Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
          Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
          Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)
          Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
        Compression Methods Length: 1
        Compression Methods (1 method)

```

9. 또한 'Get-TlsCipherSuite'를 사용하여 엔드포인트에서 활성화된 암호를 교차 확인할 수 있습니다 | ft name' PowerShell 명령입니다.

```

Select Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-TlsCipherSuite | ft name

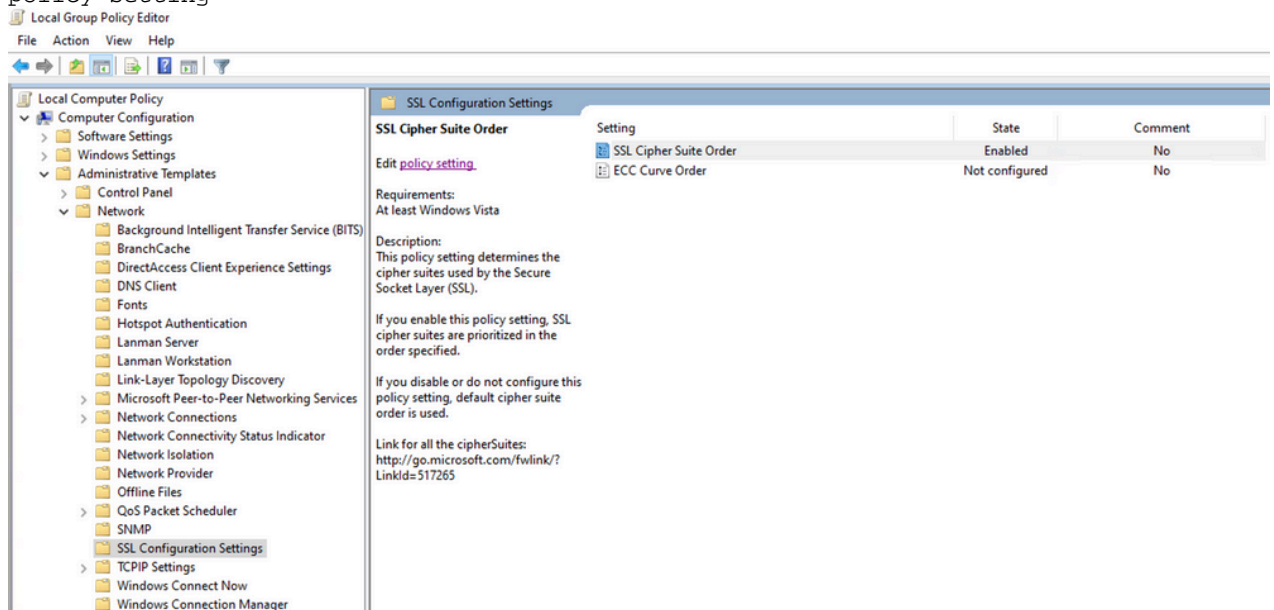
Name
----
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
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

```

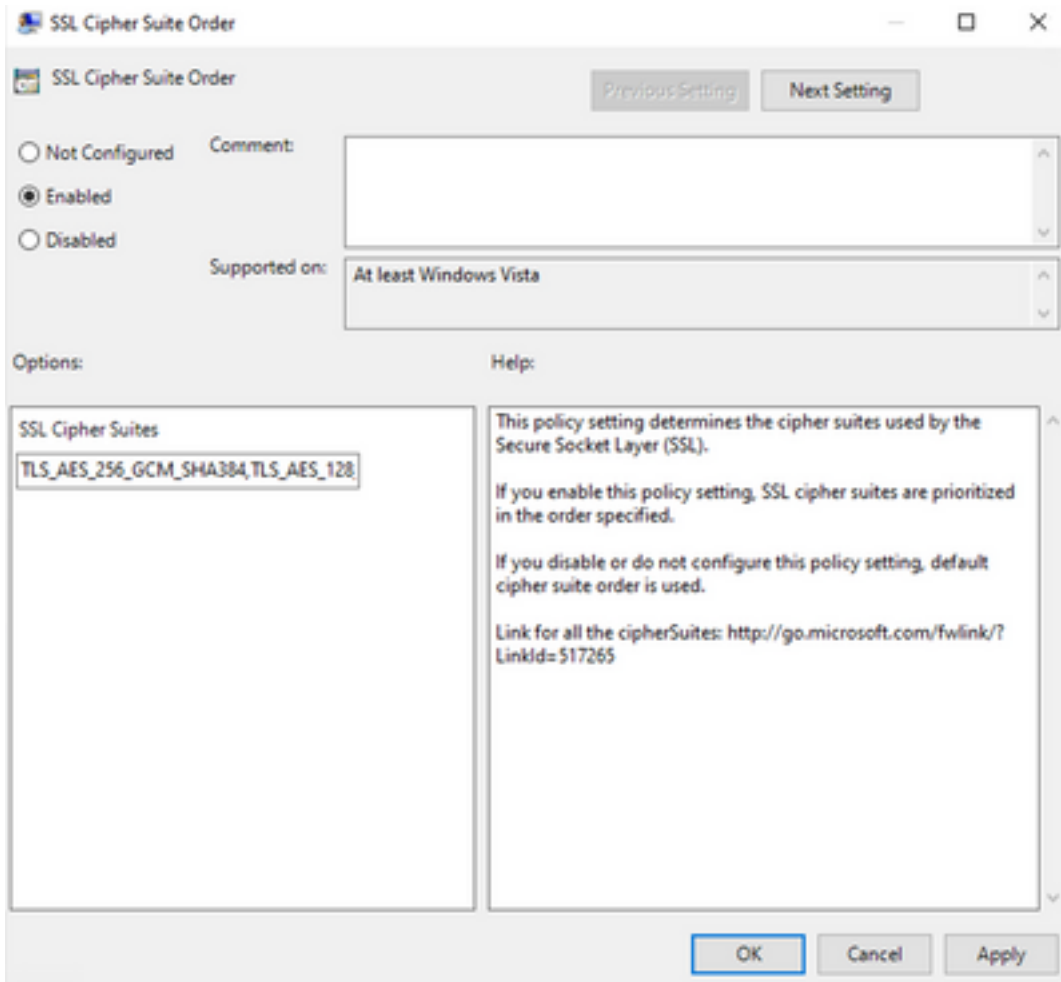
10. 6단계에서 언급한 암호가 여기에 나열되지 않은 경우 SSL 핸드셰이크 실패의 원인이 됩니다.

11. 이 문제를 해결하려면 그룹 정책에서 'SSL 암호 그룹 순서'를 확인하십시오.

Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Templates -> Network -> SSL Configuration Settings -> SSL Cipher Suite Order -> Edit policy setting



12. 암호 그룹 순서는 '구성되지 않음' 또는 '사용 안 함'이어야 하며, '사용'으로 설정된 경우 6단계에서 언급한 암호를 목록에 추가하십시오.



13. 이러한 변경 사항을 적용하고 엔드포인트를 재부팅하여 애플리케이션에서 이러한 변경 사항을 사용할 수 있도록 합니다.
14. 재부팅이 완료되면 'Update Tetra'를 다시 시도하십시오.
15. Tetra 정의 문제가 지속될 경우 로그를 분석하고 다시 캡처하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.