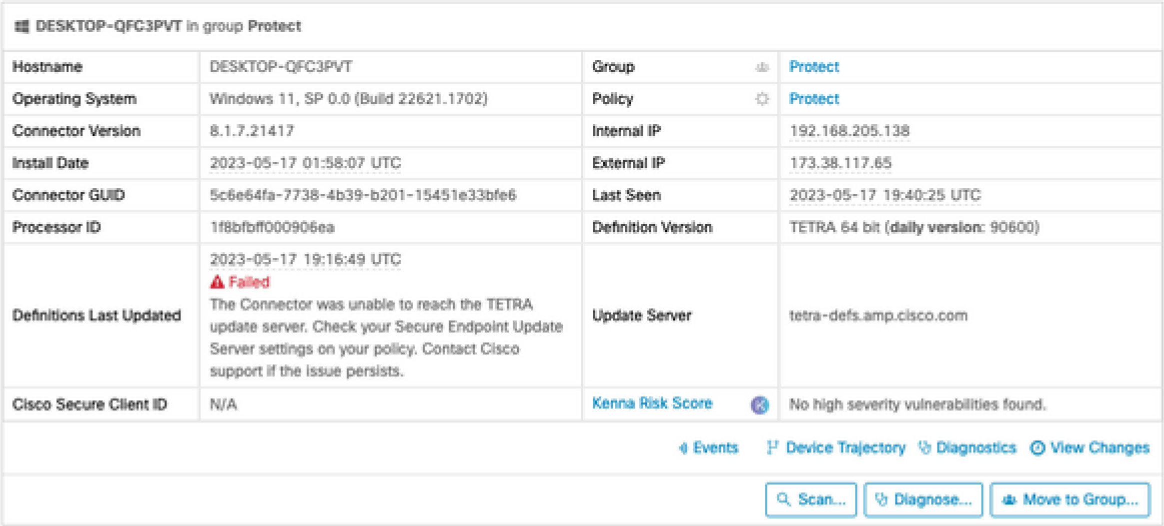
æŽ’é™¤TETRAå®šç¾©æ›´æ–°æ•…éšœ

ç›®éŒ„

ç°¡ä»‹

æœ¬æ–‡æª”æ��è¿°äº†ç‚ºèª¿æŸ¥çµ‚ç«¯ç‚ºä½•ç„¡æ³•å¾žCisco TETRAå®šç¾©æ›´æ–°ä¼ºæœ�å™¨æ›´æ–°TETRAå®šç¾©è€Œæ‡‰é�µå¾ªçš„æ¥é©Ÿã€‚

ã€Œé›»è…¦ã€�è©³ç´°è³‡è¨Šä¸‹é�¢æœƒé¡¯ç¤ºã€Œå®‰å…¨çµ‚ç«¯æŽ§åˆ¶æª¯ä¸Šå‡ºç�¾çš„ã€Œå®šç



DESKTOP-QFC3PVT in group Protect

Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-17 19:40:25 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (**daily version**: 90600)
Definitions Last Updated	2023-05-17 19:16:49 UTC ⚠ Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

â€ƒ

ç–‘é›£æŽ’è§£

æ€�ç§‘Windowså®‰å…¨çµ‚ç«¯éœ€è¦�æŒ�çºŒé€£ç·šåˆ°TETRAå®šç¾©ä¼ºæœ�å™¨æ‰�èƒ½ä

ä¸‹è¼‰TETRAå®šç¾©çš„å¸¸è¦‹éŒ¯èª¤åŒ…æ‹¬ï¼š

- ç„¡æ³•è§£æž�ä¼ºæœ�å™¨åœ°å�€
- é©—è‰SSLè‰æ›¸å¤±æ•—ï¼ˆåŒ…æ‹¬è‰æ›¸å�ŠéŠ·æ¸…å–®æª¢æŸ¥ï¼‰
- ä¸‹è¼‰é�Žç¨‹ä¸æ–·

- ç„¡æ³•é€£ç·šåˆ°ä»£ç�†ä¼ºæœ�å™¨
- ç„¡æ³•å�‘ä»£ç�†ä¼ºæœ�å™¨é€²è¡Œèº«ä»½é©—è‰

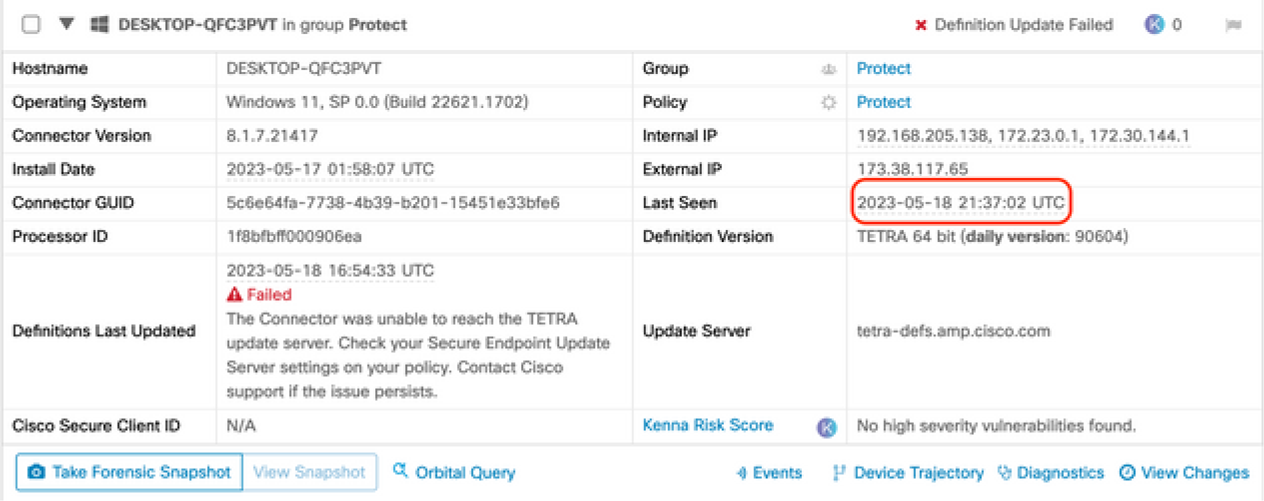
å¦‚æžœåœ¨å˜—è©¦ä¸‹è¼‰TETRAå®šç¾©æ™‚å‡ºç�¾æ•…éšœï¼Œå‰‡ä¸‹æ¬¡å˜—è©¦å°‡åœ¨ä¸‹æ¬¡æ›´æ

åœ¨å®‰å…¨çµç«¯æŽ§åˆ¶æª¯ä¸Šæª¢æŸ¥çµç«¯å ±å‘Šçš„é€£ç·š

å®‰å…¨ç«¯é»žæŽ§åˆ¶æª¯é¡¯ç¤ºç«¯é»žæ˜¯å�¦å®šæœŸé€£ç·šã€‚ ç¢ºä¿�æ‚¨çš„çµ‚ç«¯è™•æ–¼æ´»å‹•ç‹€æ

æ€�ç§‘å¹³å�‡æ¯�å¤©ç™¼ä½ˆ4å€‹å®šç¾©æ›´æ–°ï¼Œå¦‚æžœçµ‚ç«¯åœ¨ç•¶å¤©çš„ä»»ä½•æ™‚å€™

ã€Œä¸Šæ¬¡æª¢è¦–æ™‚é–“ã€�ç‹€æ…‹ä½�æ–¼ã€Œé›»è…¦è©³ç´°è³‡è¨Šã€�é �é�¢ä¸Šï¼Œå¦‚ä¸‹åœ–æ



DESKTOP-QFC3PVT in group Protect

Definition Update Failed

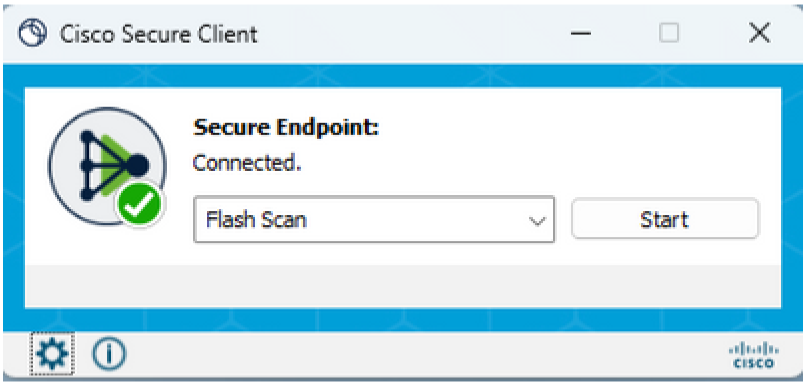
Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138, 172.23.0.1, 172.30.144.1
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-18 21:37:02 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (**daily version:** 90604)
Definitions Last Updated	2023-05-18 16:54:33 UTC ⚠ Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

å¦‚æžœçµç«¯æ£åœ¨é€£ç·šï¼Œä¸¦ä¸”å ±å‘Šå®šç¾©æœªä¸‹è¼‰ä½†æŽ§åˆ¶æª¯çœ‹åˆ°éŒ¯èª¤ï¼Œå‰‡å�é¡Œå�¯è
å¦‚æžœã€Œä¸Šæ¬¡æª¢è¦–æ™‚é–“ã€�å’Œã€Œä¸Šæ¬¡æ›´æ–°å®šç¾©ã€�ä¹‹é–“çš„æ™‚é–“å·®ç•°è¼ƒå¤

æª¢æŸ¥çµç«¯ä¸Šçš„é€£ç·š

çµç«¯ä½¿ç”¨è€…å�¯ä»¥ä½¿ç”¨UIä»‹é�¢æª¢æŸ¥é€£ç·šã€‚

é–‹å•ŸCisco Secure Clientæœƒé¡¯ç¤ºé€£ç·šç‹€æ…‹ã€‚



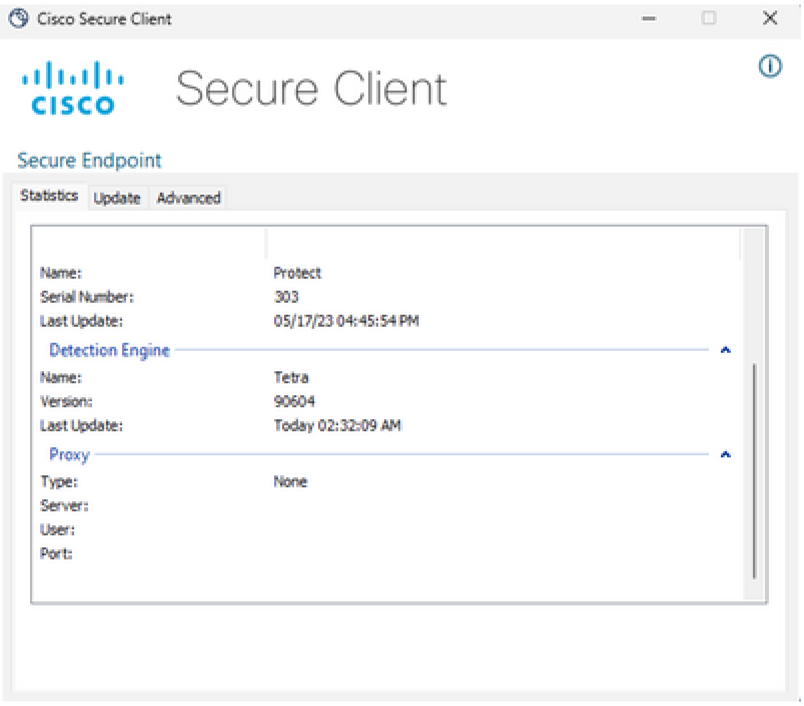
Secure Endpoint:
Connected.

Flash Scan

çµç«¯æœªé€£ç·šä¸¦å ±å‘Šé€£ç·šå�é¡Œæ™‚ï¼Œå�¯ä½¿ç”¨ConnectivityToolã€‚
é€™åŒ…å�«åœ¨ç”Ÿæˆ�æ”¯æ�´åŒ…çš„IPSupportToolä¸ã€‚

æª¢æŸ¥çµç«¯ä¸Šçš„TETRAå®šç¾©

æ€�ç§'å®‰å…¨å®¢æˆ¶ç«¯æ��ä¾›æœ‰é—œçµ‚ç«¯è�¯çµ�å™¨è¼‰å…¥çš„ç•¶å‰�TETRAå®
åœ¨ã€Œçµ±è¨ˆè³‡è¨Šã€�é �ç±¤ä¸Šï¼ŒTETRAçš„ç•¶å‰�å®šç¾©å�¯ç”¨ã€‚



Name: Protect
Serial Number: 303
Last Update: 05/17/23 04:45:54 PM

Name: Tetra
Version: 90604
Last Update: Today 02:32:09 AM

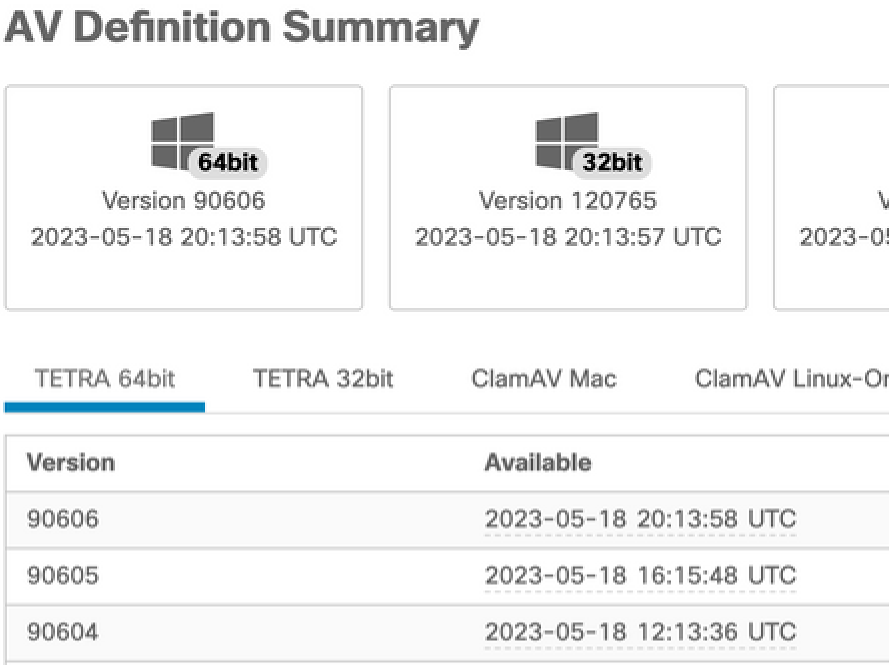
Type: None
Server:
User:
Port:

â€ƒ

æ¤å¤–ï¼Œç•¶å‰�çš„TETRAå®šç¾©è©³ç´°è³‡è¨Šç”±AmpCLIå·¥å…·åœ¨çµ‚ç«¯ä¸Šå ±å'Šã€‚
è©²å'½ä»¤ç¤ºä¾‹å¦‚ä¸‹ï¼š

```
PS C:\Program Files\Cisco\AMP\8.1.7.21417> .\AmpCLI.exe posture
{"agent_uuid":"5c6e64fa-7738-4b39-b201-15451e33bfe6","connected":true,"connector_version":"8.1.7","engin
```

å°‡é¡¯ç¤ºæ¯�å€‹å¼•æ“Žçš„å®šç¾©ç‰ˆæœ¬ï¼ŒåŒ…æ‹¬TETRAã€‚
åœ¨ä¸Šé�¢çš„è¼¸å‡ºä¸ï¼Œé€™æ˜¯ç‰ˆæœ¬90604ã€‚
é€™å�¯ä»¥èˆ‡**ç®¡ç�†>AVå®šç¾©æ'˜è¦�**ä¸‹çš„å®‰å…¨çµ‚ç«¯æŽ§åˆ¶æª¯é€²è¡Œæ¯”è¼ƒã€‚
è©²é �çš„ç¤ºä¾‹å¦‚ä¸‹æ‰€ç¤ºã€‚


AV Definition Summary

Version	Available
90606	2023-05-18 20:13:58 UTC
90605	2023-05-18 16:15:48 UTC
90604	2023-05-18 12:13:36 UTC

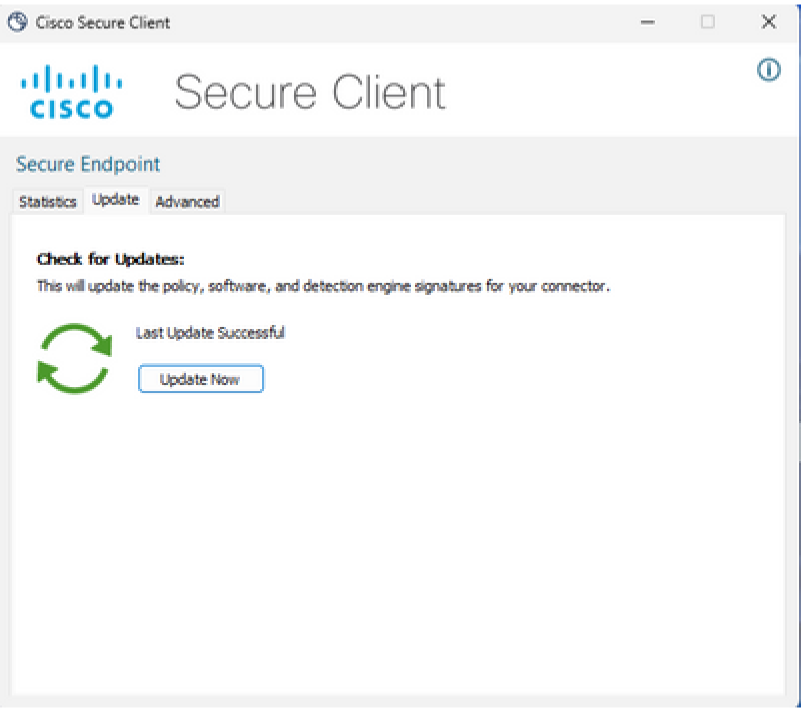
â€ƒ

å¦‚æžœç‰ˆæœ¬ä»»�è�½å¾Œä¸¦ä¸”è�¯çµ�å™¨ç‹€æ…‹å·²é€£ç·šï¼Œå‰‡å�¯ä»¥åŸ·è¡Œå®šç¾©çš„æ›

åœ¨ç«¯é»žä¸Šå¼·åˆ¶TETRAå®šç¾©æ›´æ–°

çµ‚ç«¯ä½¿ç”¨è€…å�¯ä»¥æ¨¡æ“¬å’Œæª¢æŸ¥TETRAä¸‹è¼‰é€²åº¦ã€‚ ä½¿ç”¨è€…è¦�è§¸ç™¼æ›´æ–°ï¼Œéœ€è¦�åœ¨ç–ç•¥ä¸è¨å®šé€²é�¸é …ã€‚ åœ¨**Advanced Settings > Client User Interface**ç–ç•¥è¨å®šé �é�¢ä¸‹ï¼Œéœ€è¦�ç‚ºä½¿ç”¨è€…è§¸ç™¼çš„å®šç¾©å•Ÿç”¨**Allow user to update TETRA definitions**è¨å®šã€‚

åœ¨Cisco Secure Clientä¸ï¼Œçµ‚ç«¯ä½¿ç”¨è€…å�¯ä»¥é–‹å•Ÿå®¢æˆ¶ç«¯ä¸¦æª¢æŸ¥å®‰å…¨çµ‚ç«¯çš„è¨å®šã€‚ ä½¿ç”¨è€…å�¯ä»¥é»žé�¸ã€Œç«‹å�³æ›´æ–°ã€�ä»¥è§¸ç™¼å¦‚ä¸‹æ‰€ç¤ºçš„TETRAå®šç¾©æ›´æ–°ï¼



Check for Updates:

This will update the policy, software, and detection engine signatures for your connector.

Last Update Successful

å¦‚æžœæ‚¨é�‹è¡Œçš„æ˜¯é�¢å�‘çµ‚ç«¯çš„AMPè�¯çµ�å™¨ç‰ˆæœ¬7.2.7å�Šæ›´é«˜ç‰ˆæœ¬ï¼Œæ‚
â€” forceupdateã€�å¼·åˆ¶è�¯çµ�å™¨ä¸‹è¼‰TETRAå®šç¾©ã€‚

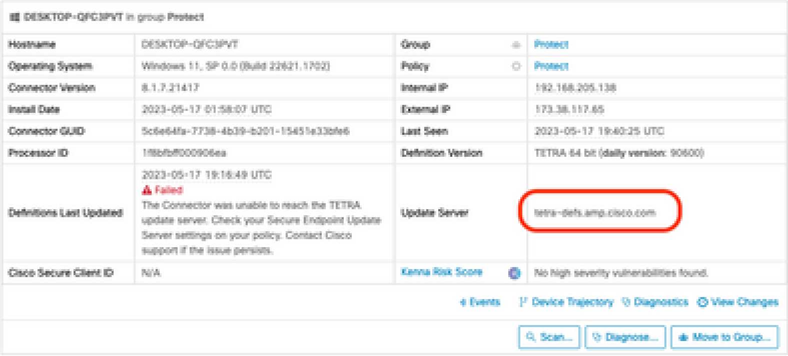
```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

å¼·åˆ¶åŸ·è¡Œæ›´æ–°å¾Œï¼Œå�¯ä»¥å†�æ¬¡æª¢æŸ¥TETRAå®šç¾©ä»¥æª¢è¦–æ˜¯å�¦ç™¼ç”Ÿæ›´æ–°
å¦‚æžœä»�ç„¶æ²’æœ‰é€²è¡Œæ›´æ–°ï¼Œå‰‡éœ€è¦�æª¢æŸ¥èˆ‡TETRAä¼ºæœ�å™¨çš„é€£ç·šã€

æª¢æŸ¥çµ‚ç«¯ä¸Šçš„TETRAå®šç¾©ä¼ºæœ�å™¨é€£ç·š

çµ‚ç«¯ç–ç•¥åŒ…æ‹¬çµ‚ç«¯è�¯çµ¡ä»¥ä¸‹è¼‰å®šç¾©çš„å®šç¾©ä¼ºæœ�å™¨ã€‚

é›»è…¦è©³ç´°è³‡è¨Šé �é�¢åŒ…æ‹¬æ›´æ–°ä¼ºæœ�å™¨ã€‚
ä¸‹åœ–é¡¯ç¤ºäº†æ›´æ–°ä¼ºæœ�å™¨çš„é¡¯ç¤ºä½�ç½®ï¼š



DESKTOP-QFC3PVT in group Protect

Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-17 19:40:25 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (daily version: 90600)
Definitions Last Updated	2023-05-17 19:16:49 UTC ⚠ Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

â€ƒ

åœ¨å…¬å…±é›²ä¸Šï¼Œçµ‚ç«¯å�¯ä»¥é€£ç·šåˆ°çš„æ‰€éœ€ä¼ºæœ�å™¨å��ç¨±åˆ—åœ¨Required

Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operationsä¸‹

ç›´æŽ¥é€£ç·šé©—è‰

åœ¨çµ‚ç«¯æ©Ÿä¸Šï¼Œå�¯ä»¥é�‹è¡Œä»¥ä¸‹å‘½ä»¤ä»¥æª¢æŸ¥å°�æ›´æ–°ä¼ºæœ�å™¨çš„DNSæŸ¥è©¢ï¼š

```
PS C:\Program Files\Cisco\AMP> Resolve-DnsName -Name tetra-defs.amp.cisco.com
Name                        Type TTL Section IPAddress
----                        ---- --- ------- ---------
tetra-defs.amp.cisco.com    A    5   Answer  192.XXX.X.XX
tetra-defs.amp.cisco.com    A    5   Answer  192.XXX.X.X
tetra-defs.amp.cisco.com    A    5   Answer  192.XXX.X.X
```

å¦‚æžœè§£æž�äº†IPï¼Œå‰‡å�¯ä»¥æ¸¬è©¦è‡³ä¼ºæœ�å™¨çš„é€£ç·šã€‚
æœ‰æ•ˆçš„éŸ¿æ‡‰å°‡å¦‚ä¸‹æ‰€ç¤ºï¼š

<#root>

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
* Trying 192.XXX.X.X:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.X) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* ALPN: server did not agree on a protocol. Uses default.
* using HTTP/1.x
> GET / HTTP/1.1
> Host: tetra-defs.amp.cisco.com
> User-Agent: curl/8.0.1
> Accept: */*
>
* schannel: server closed the connection

< HTTP/1.1 200 OK


< Date: Fri, 19 May 2023 19:13:35 GMT
< Server:
< Last-Modified: Mon, 17 Apr 2023 15:48:54 GMT
< ETag: "0-5f98a20ced9e3"
< Accept-Ranges: bytes
< Content-Length: 0
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
```

å¦‚æžœç„¡æ³•å»ºç«‹é€£ç·šä¾†é©—è‰è‡³CRLä¼ºæœ�å™¨çš„æ†‘è‰(ä¾‹å¦‚commercial.ocsp.identrust.comæˆ

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
```

```
* Trying 192.XXX.X.XX:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.XX) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation function
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
curl: (35) schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation
```

ä»£ç�†é©—è‰

å¦‚æžœçµ‚ç«¯é…�ç½®ç‚ºä½¿ç”¨ä»£ç�†ï¼Œå‰‡å�¯ä»¥æª¢æŸ¥æœ€å¾Œä¸€å€‹éŒ¯èª¤ç‹€æ…‹ã€‚ é�‹è¡Œä¸‹é�¢çš„PowerShellå�¯èƒ½æœƒè¿”å›žTETRAæ›´æ–°å˜—è©¦çš„æœ€å¾Œä¸€å€‹éŒ¯èª¤ã€‚

```
PS C:\Program Files\Cisco\AMP> (Select-Xml -Path local.xml -XPath '//tetra/lasterror').Node.InnerText
```

ä¸Šä¸€å€‹éŒ¯èª¤ä»£ç¢¼	å•�é¡Œ	å‹•ä½œ
4294965193	ç„¡æ³•å»ºç«‹èˆ‡ä»£ç�†çš„é€£ç·š	æª¢æŸ¥èˆ‡ä»£ç�†çš„ç¶²è·¯é€£ç·š
4294965196	ç„¡æ³•é€šé�Žä»£ç�†é€²è¡Œèº«ä»½é©—è‰	æª¢æŸ¥ä»£ç�†çš„èº«ä»½é©—è
4294965187	å·²é€£ç·šä»£ç�†ä¸”ä¸‹è¼‰å¤±æ•—	æª¢æŸ¥ä»£ç�†æ—¥èªŒä»¥çžè§£

å…¶ä»–è³‡è¨Š

- å¦‚æžœæ‚¨çœ‹åˆ°çµ‚ç«¯å§‹çµ‚ç„¡æ³•ä¸‹è¼‰TETRAå®šç¾©ï¼Œå„˜ç®¡å®Œæˆ�äº†ä¸Šè¿°æª¢æŸ¥ï¼Œè«‹å TACæ¡ˆä¾‹ä»¥é€²è¡Œé€²ä¸€æ¥èª¿æŸ¥ã€‚

[å¾žAMP for Windowsè�¯çµ�å™¨æ”¶é›†è¨ºæ–·è³‡æ–™]

關於此翻譯