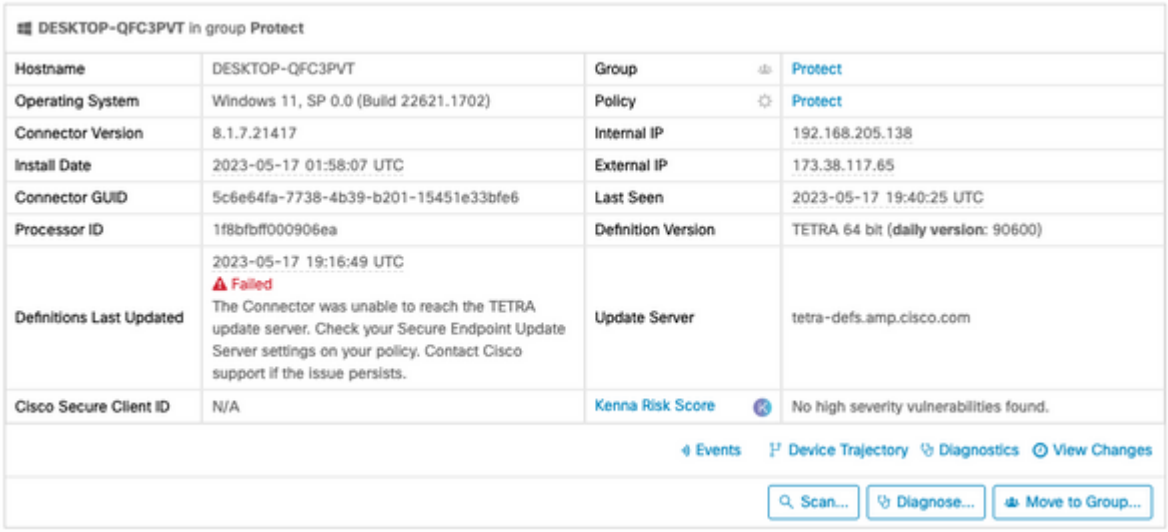
Fehlerbehebung bei Aktualisierungsfehlern von TETRA-Definitionen

Inhalt

Einleitung

In diesem Dokument werden die Schritte beschrieben, die zur Ermittlung des Grundes befolgt werden sollten, warum Endpunkte die TETRA-Definitionen von Cisco TETRA-Definitionen-Aktualisierungsservern nicht aktualisieren.

Definitionen Letzter aktualisierter Fehler, der in der Konsole für sichere Endgeräte angezeigt wird, wird unter den Computerdetails angezeigt (siehe unten).



â€ƒ

Fehlerbehebung

Cisco Secure Endpoint für Windows benötigt eine dauerhafte Verbindung zum TETRA-Definitions-Server, um Updates herunterzuladen.

Häufige Fehler beim Herunterladen der TETRA-Definitionen sind:

- Fehler beim Auflösen der Serveradresse.
- Fehler beim Überprüfen des SSL-Zertifikats (einschließlich Überprüfung der Zertifikatsperrliste).
- Unterbrechung beim Download
- Fehler beim Herstellen der Verbindung zum Proxyserver.
- Fehler bei der Authentifizierung am Proxyserver

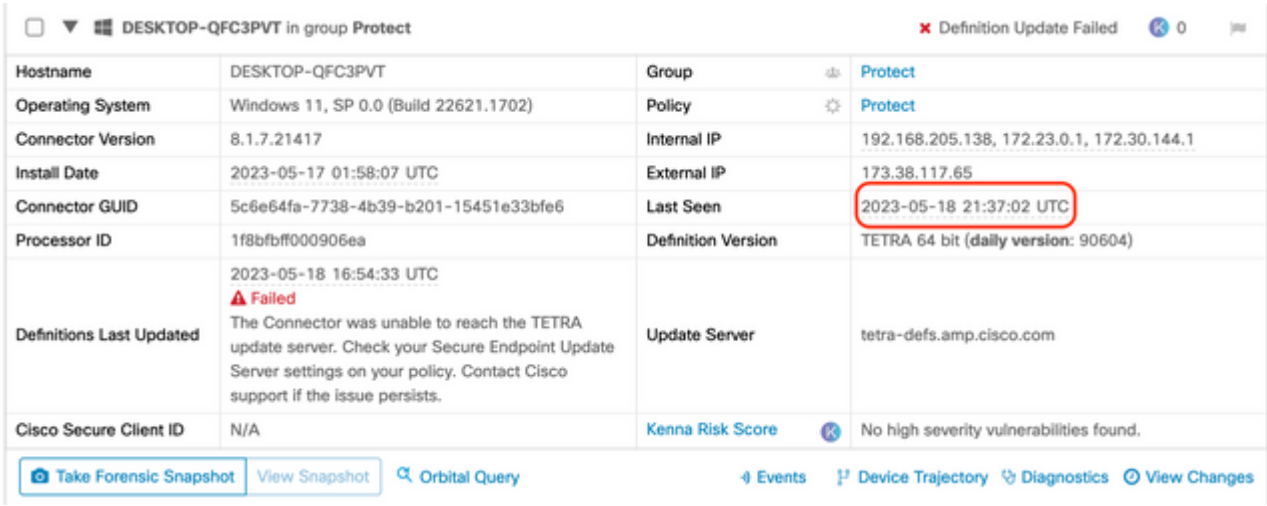
Wenn beim Versuch, die TETRA-Definitionen herunterzuladen, ein Fehler auftritt, erfolgt der nächste Versuch im nächsten Aktualisierungsintervall oder wenn ein manuelles Update vom Benutzer initiiert wurde.

Überprüfen der von Endgeräten gemeldeten Verbindungen auf der Konsole für sichere Endgeräte

Die Konsole für sichere Endgeräte zeigt an, ob sich das Endgerät regelmäßig verbindet. Stellen Sie sicher, dass Ihre Endgeräte aktiv sind und den Status "Zuletzt gesehen" haben. Wenn sich die Endpunkte nicht bei der Konsole für sichere Endpunkte anmelden, weist dies darauf hin, dass der Endpunkt nicht aktiv ist oder Verbindungsprobleme aufweist.

Cisco veröffentlicht täglich durchschnittlich 4 Definitions-Updates. Wenn das Update nicht vom Endgerät heruntergeladen werden kann, zeigt der Connector einen Fehler an. In Anbetracht dieser Häufigkeit werden die Endpunkte nur dann als "Innerhalb der Richtlinie" gemeldet, wenn sie ständig verbunden sind und durchgehend über eine stabile Netzwerkverbindung zum TETRA-Server verfügen.

Der Status "Zuletzt gesehen" wird auf der Seite mit den Computerdetails angezeigt, wie unten gezeigt:

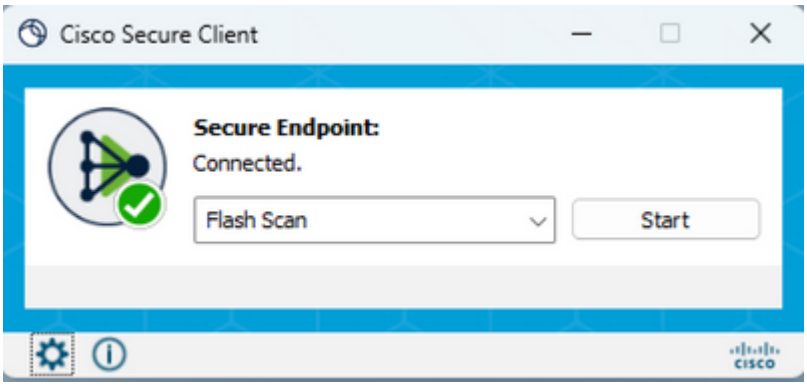


Wenn der Endpunkt eine Verbindung herstellt und ein Fehler gemeldet wird, dass die Definitionen nicht heruntergeladen werden, sondern von der Konsole angezeigt werden, kann das Problem gelegentlich auftreten. Weitere Untersuchungen können durchgeführt werden, wenn die Zeitunterschiede zwischen "Last Seen" und "Definitions Last Updated" groß sind.

Überprüfen der Verbindung am Endpunkt

Endbenutzer können die Verbindung über die Benutzeroberfläche überprüfen.

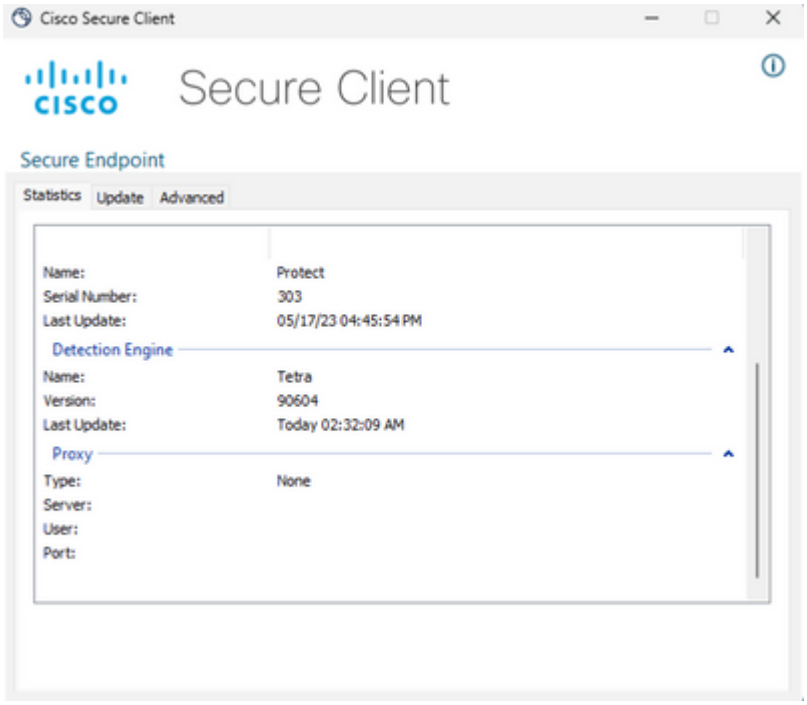
Beim Öffnen des Cisco Secure Client wird der Verbindungsstatus angezeigt.



Das ConnectivityTool kann verwendet werden, wenn der Endpunkt nicht verbunden ist, und meldet Verbindungsprobleme. Diese ist im IPSupportTool enthalten, das das Support-Paket generiert.

TETRA-Definitionen auf dem Endpunkt überprüfen

Cisco Secure Client liefert Informationen zu den aktuellen TETRA-Definitionen, die vom Endgeräteanschluss geladen werden. Der Endbenutzer kann den Client öffnen und die Einstellungen für Secure Endpoint überprüfen. Auf der Registerkarte Statistik ist die aktuelle TETRA-Definition verfügbar.

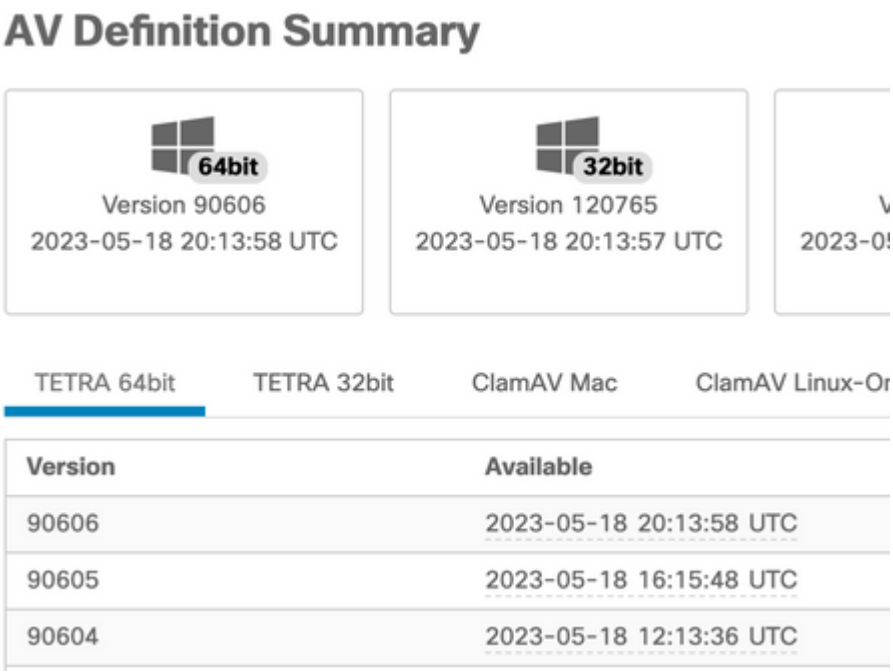


â€f

Außerdem werden die aktuellen TETRA-Definitionsdetails vom AmpCLI-Tool am Endpunkt gemeldet. Ein Beispiel für diesen Befehl:

```
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","engir
```

Die Definitionsversionen werden für jede der Motoren einschließlich TETRA angezeigt. In dieser Ausgabe oben ist dies Version 90604. Dies kann mit der Konsole für sichere Endgeräte verglichen werden unter: **Management > AV Definition Summary**. Ein Beispiel für die Seite ist wie folgt.



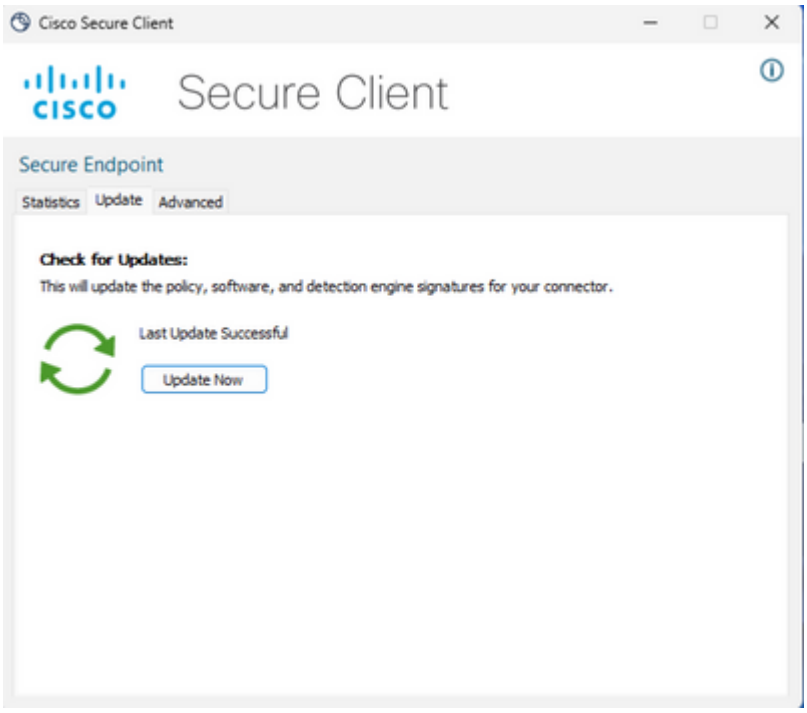
â€ƒ

Wenn die Version noch nicht verfügbar ist und der Steckverbinderstatus verbunden ist, kann entweder eine Aktualisierung der Definitionen oder eine Überprüfung der Endpunktverbindung zum TETRA-Server durchgeführt werden.

Erzwingen einer Aktualisierung der TETRA-Definitionen auf dem Endpunkt

Endbenutzer können den Fortschritt des TETRA-Downloads initiieren und überprüfen. Damit der Benutzer das Update auslösen kann, muss die Option in der Richtlinie festgelegt werden. Unter **Erweiterte Einstellungen > Client User Interface** policy settings (**Erweiterte Einstellungen > Client-Benutzeroberflächen-**Richtlinieneinstellungen) müssen die Einstellungen **Allow user to update TETRA definitions (TETRA-Definitionen aktualisieren)** aktiviert sein, damit die Definitionen vom Benutzer ausgelöst werden.

Im Cisco Secure Client kann der Endbenutzer den Client öffnen und die Einstellungen für Secure Endpoint überprüfen. Der Benutzer kann auf "Jetzt aktualisieren" klicken, um die TETRA-Definitionsupdate wie unten dargestellt auszulösen:



Wenn Sie AMP für Endpoints Connector Version 7.2.7 und höher ausführen, können Sie einen neuen Schalter "-forceupdate" verwenden, um den Connector zu zwingen, die TETRA-Definitionen herunterzuladen.

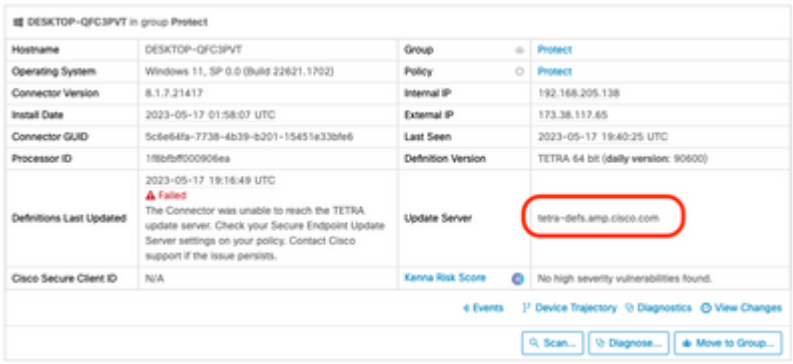
```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

Nachdem die Aktualisierung erzwungen wurde, kann die TETRA-Definition erneut überprüft werden, um festzustellen, ob eine Aktualisierung erfolgt. Wenn noch keine Aktualisierung erfolgt, muss die Verbindung zum TETRA-Server überprüft werden.

Überprüfen der TETRA Definition Server-Konnektivität auf dem Endpunkt

Die Endpunktrichtlinie enthält den Definitionsserver, an den sich der Endpunkt wendet, um die Definitionen herunterzuladen.

Die Seite mit den Computerdetails enthält den Aktualisierungsserver. Das nachfolgende Bild zeigt, wo der Aktualisierungsserver angezeigt wird:



â€ƒ

In der Public Cloud wird der erforderliche Servername, mit dem das Endgerät eine Verbindung herstellen kann, unter: Erforderliche Serveradressen für den ordnungsgemäßen Betrieb von Cisco Secure Endpoint und Malware Analytics aufgeführt.

Prüfung direkter Verbindungen

Vom Endpunkt aus kann der folgende Befehl ausgeführt werden, um die DNS-Suche beim Aktualisierungsserver zu überprüfen:

```
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
```

Wenn die IP aufgelöst ist, kann die Verbindung zum Server getestet werden. Eine gültige Antwort sieht wie folgt aus:

<#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
```

Wenn die Verbindung nicht hergestellt werden kann, um das Zertifikat mit dem Zertifikatsperrlisten-Server zu überprüfen (z. B. commercial.ocsp.identrust.com oder validation.identrust.com), wird ein Fehler wie folgt angezeigt:

```
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
```

Proxy-Validierung

Wenn der Endpunkt für die Verwendung eines Proxys konfiguriert ist, kann der letzte Fehlerstatus überprüft werden. Wenn Sie PowerShell unten ausführen, kann der letzte Fehler des TETRA-Aktualisierungsversuchs zurückgegeben werden.

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

Letzter Fehlercode	Problem	Aktionen
4294965193	Verbindung zum Proxy konnte nicht hergestellt werden	Netzwerkverbindung zum Proxy überprüfen
4294965196	Authentifizierung über Proxy nicht möglich	Authentifizierungsinformationen für den Proxy überprüfen
4294965187	Verbindung zum Proxy hergestellt und Download fehlgeschlagen	Proxyprotokolle auf Downloadprobleme überprüfen

Zusätzliche Informationen

- Wenn Sie Endpunkte sehen, die trotz der oben genannten Prüfungen ständig nicht die TETRA-Definitionen herunterladen können, aktivieren Sie Connector im Debugmodus für ein Zeitintervall, das dem in Ihrer Richtlinie definierten Aktualisierungsintervall entspricht, und generieren Sie das Support-Paket. Wenn sich der Connector im Debug-Modus befindet, beachten Sie, dass die Wireshark-Paketerfassung ebenfalls durchgeführt werden muss. Die Paketerfassung muss außerdem für ein Zeitintervall ausgeführt werden, das dem in der Richtlinie definierten Aktualisierungsintervall entspricht. Sobald diese Informationen erfasst wurden, öffnen Sie ein Cisco TAC-Ticket mit diesen Informationen, um weitere Untersuchungen anzustellen.

Sammlung von Diagnosedaten von AMP für Windows Connector

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.