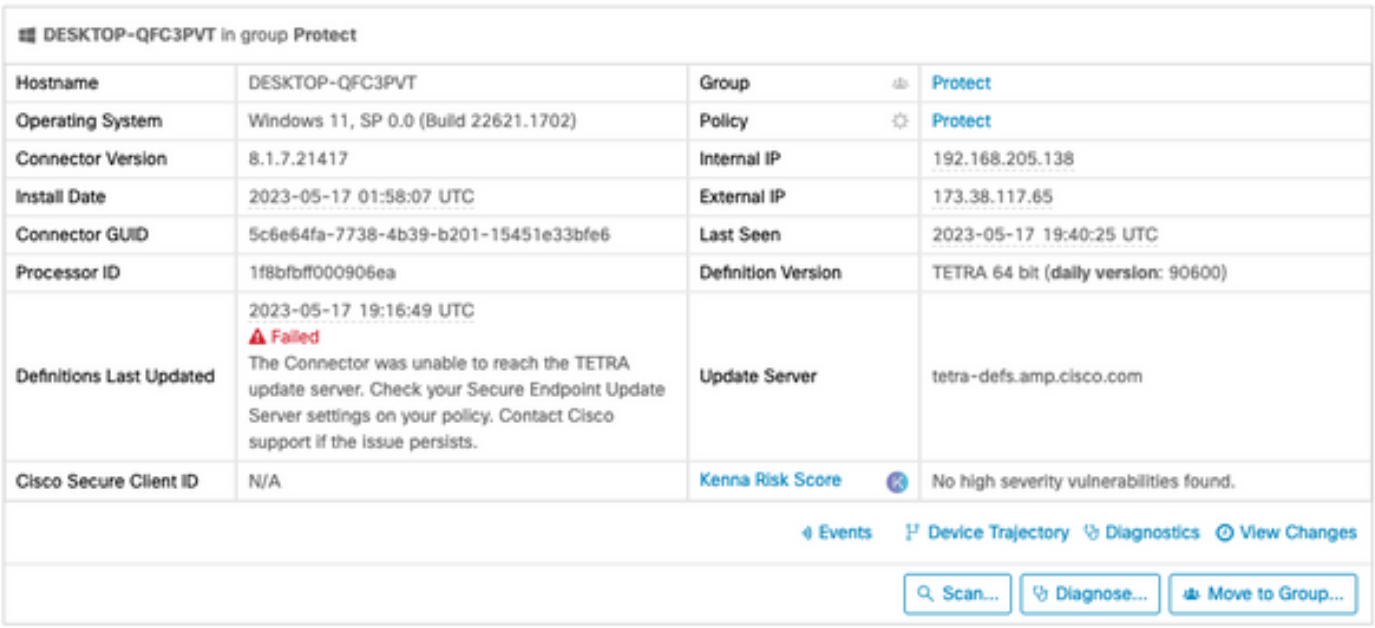
TETRA定義の更新失敗のトラブルシューティング

内容

はじめに

このドキュメントでは、エンドポイントがCisco TETRA定義更新サーバからTETRA定義を更新できない理由を調査するために実行する必要がある手順について説明します。

定義セキュアエンドポイントコンソールに表示されるLast Updated failureは、次に示すようにComputer detailsの下に表示されます。



（「トラブルシューティング」）

Cisco Secure Endpoint for Windowsでは、更新をダウンロードするために、TETRA定義サーバへの持続的な接続が必要です。

TETRA定義をダウンロードする際の一般的なエラーには、次のものがあります。

- サーバアドレスを解決できない
- SSL証明書の検証に失敗しました（証明書失効リストの確認を含む）
- ダウンロード中の中断
- プロキシサーバーに接続できません
- プロキシサーバーへの認証に失敗しました

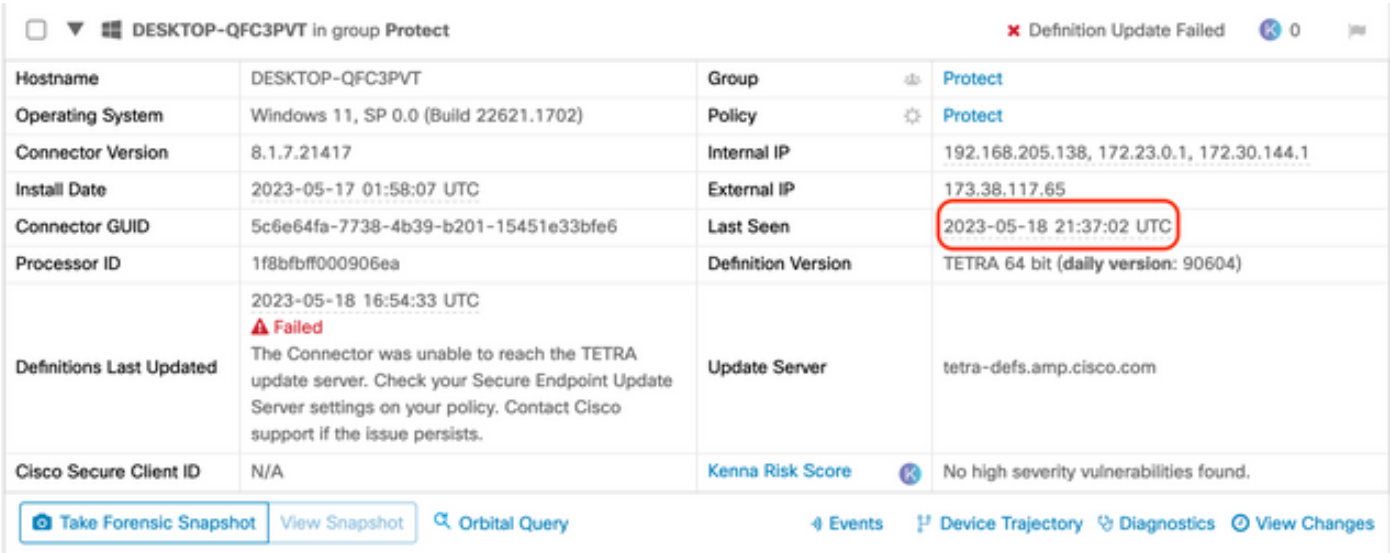
TETRA定義のダウンロード中に障害が発生した場合、次の更新間隔またはユーザが手動で更新を開始すると、次の更新が行われます。

セキュアエンドポイントコンソールで報告されたエンドポイント接続の確認

セキュアなエンドポイントコンソールに、エンドポイントが定期的に接続しているかどうかが表示されます。 エンドポイントがアクティブで、最新の「Last Seen」ステータスであることを確認します。エンドポイントがSecure Endpoint Consoleでチェックインしない場合は、エンドポイントがアクティブでないか、接続に問題があることを示します。

シスコでは1日に平均4件の定義更新をリリースしていますが、その日のいずれかの時点でエンドポイントが更新のダウンロードに失敗すると、コネクタで障害エラーが発生します。この頻度を考慮すると、エンドポイントが常に接続され、TETRAサーバへの安定したネットワーク接続が確立されている場合にのみ、エンドポイントは「ポリシー内」として報告されます。

「Last Seen」ステータスは、次の丸で囲まれたコンピュータの詳細ページにあります。

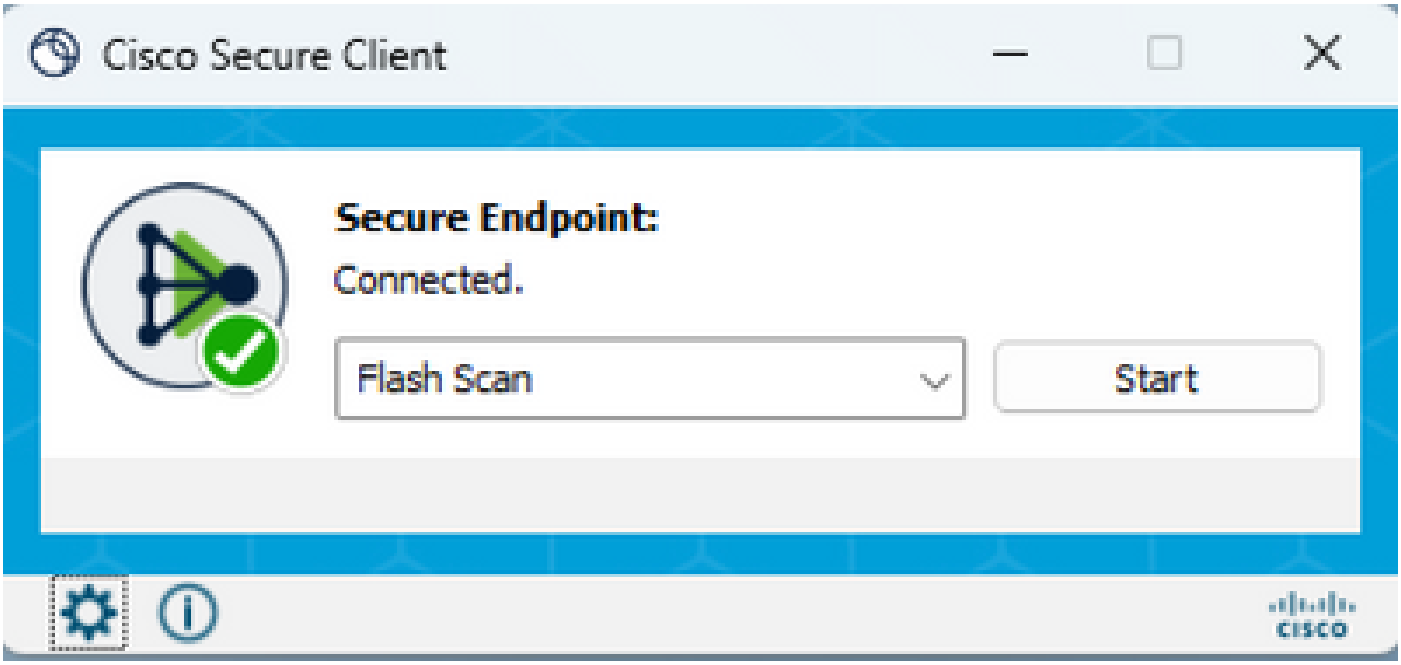


エンドポイントが接続中で、定義がダウンロードされていないがコンソールに表示されるエラーが報告された場合は、問題が断続的に発生している可能性があります。 「Last Seen」と「Definitions Last Updated」の時間差が大きい場合は、詳細な調査を実施できます。

エンドポイントの接続の確認

エンドユーザは、UIインターフェイスを使用して接続を確認できます。

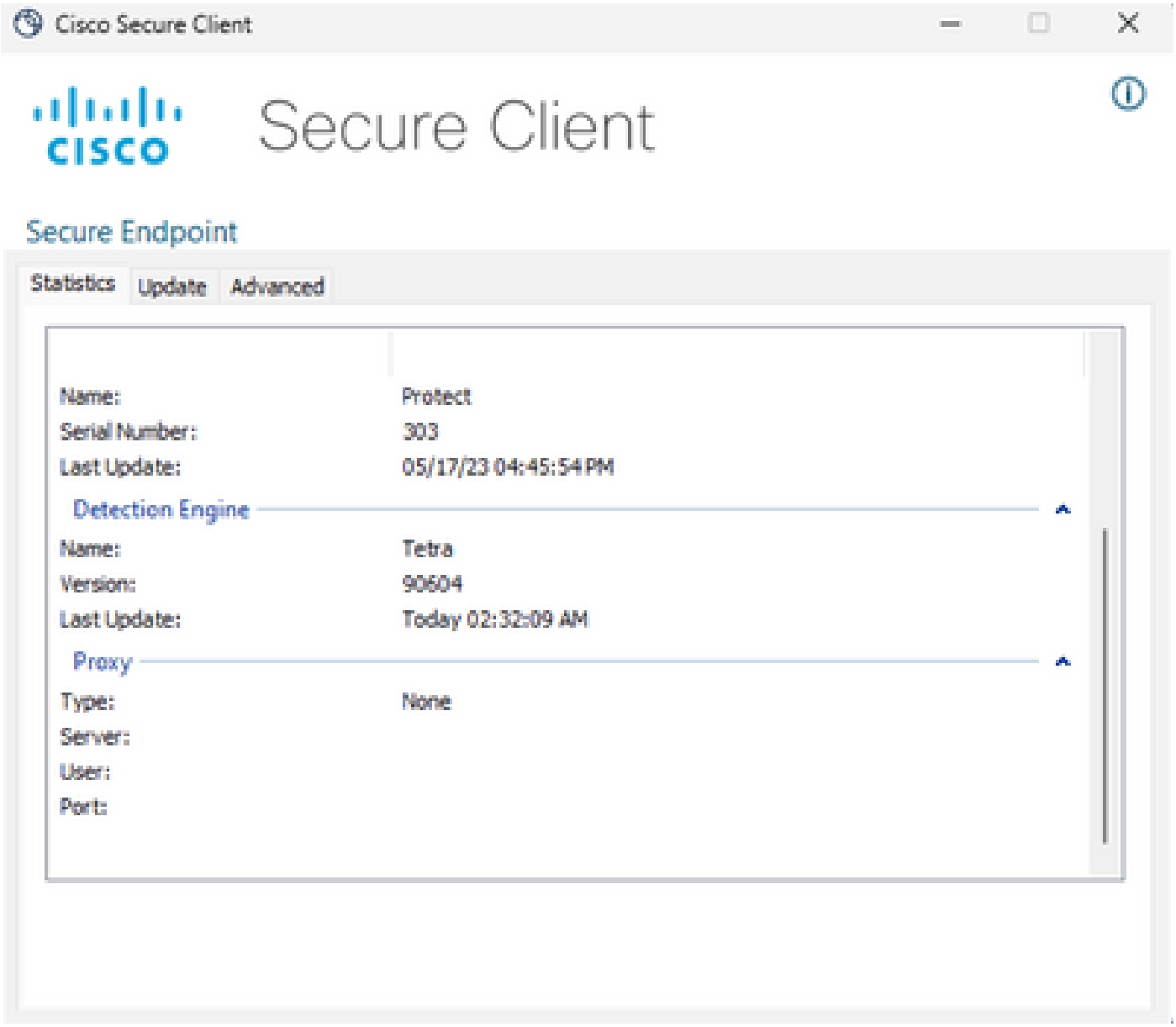
Cisco Secure Clientを開くと、接続ステータスが表示されます。



ConnectivityToolは、エンドポイントが接続されておらず、接続の問題を報告する場合に使用できます。 これは、サポートパッケージを生成するIPSupportToolに含まれています。

エンドポイントでのTETRA定義の確認

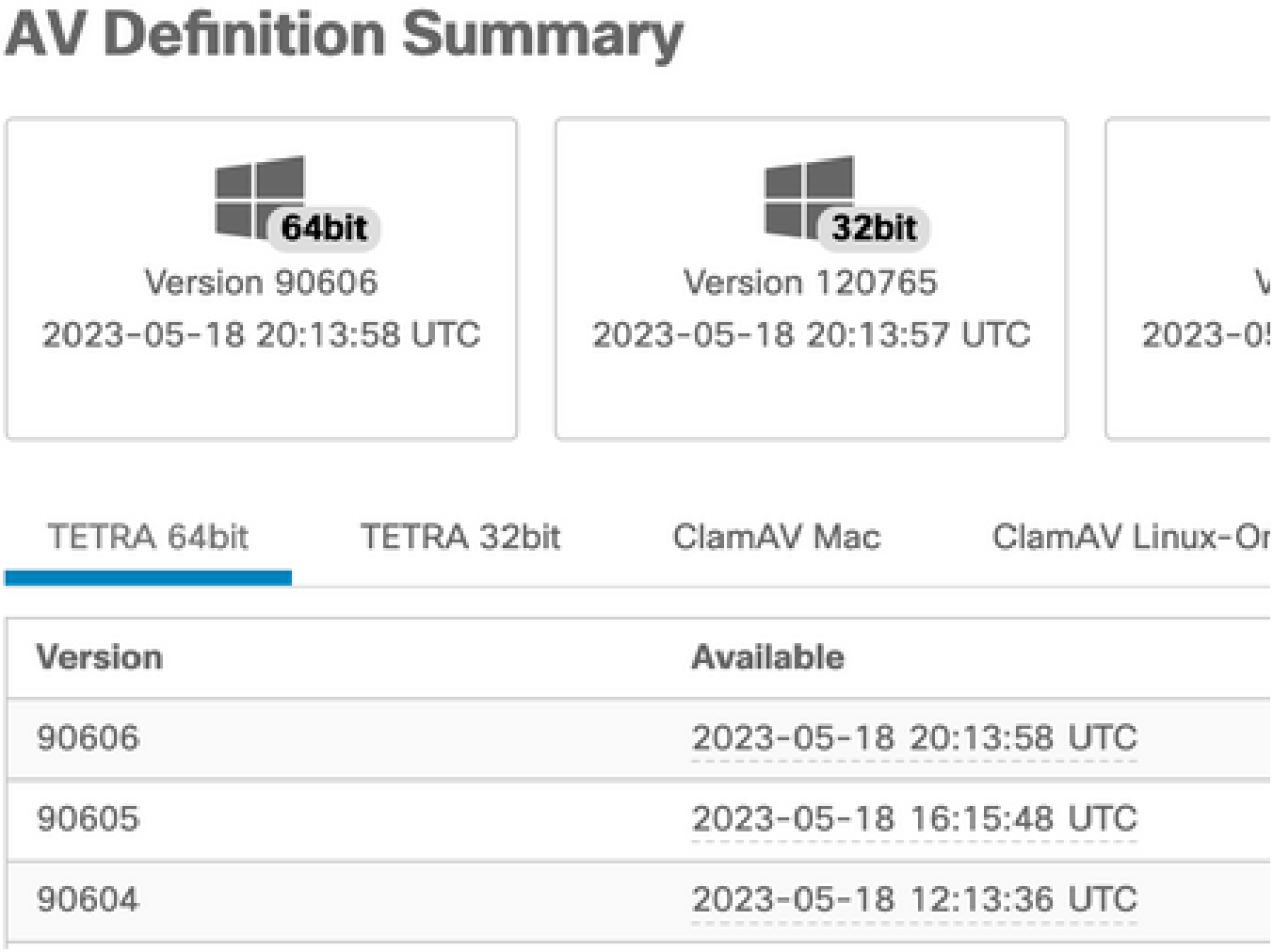
Cisco Secure Clientは、エンドポイントコネクタによってロードされた現在のTETRA定義に関する情報を提供します。 エンドユーザはクライアントを開き、セキュアエンドポイントの設定を確認できます。 「統計」タブで、TETRAの現在の定義を使用できます。



また、現在のTETRA定義の詳細は、エンドポイントのAmpCLIツールによって報告されます。 コマンドの例を次に示します。

```
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","engi
```

TETRAを含む各エンジンの定義バージョンが表示されます。上記の出力では、バージョン90604になっています。これは、Management > AV Definition Summaryの下のSecure Endpoint Consoleと比較できます。 ページの例を次に示します。

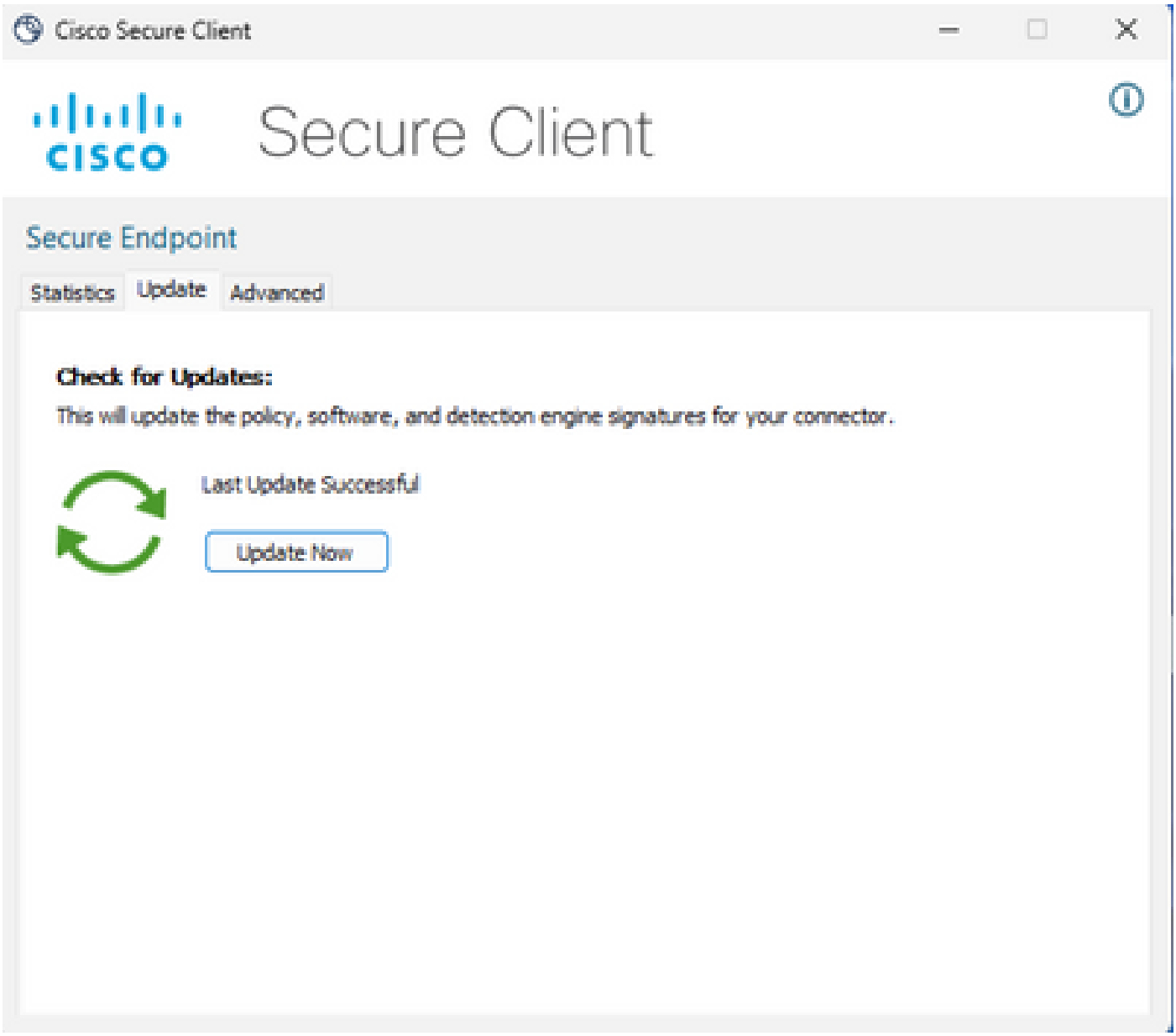


バージョンがまだ遅れており、コネクタステータスがconnectedの場合は、定義の更新またはTETRAサーバへのエンドポイント接続の確認のいずれかを実行できます。

エンドポイントでTETRA定義を強制的に更新する

エンドユーザは、TETRAダウンロードの進捗状況を確認できます。 ユーザがアップデートをトリガーするには、ポリシーでオプションを設定する必要があります。 Advanced Settings > Client User Interfaceポリシー設定ページで、定義がユーザによってトリガーされるように、Allow user to update TETRA definitions設定を有効にする必要があります。

Cisco Secure Clientでは、エンドユーザがクライアントを開き、セキュアエンドポイントの設定を確認できます。 次に示すように、「今すぐ更新」をクリックしてTETRA定義の更新をトリガーできます。



AMP for Endpointsコネクタバージョン7.2.7以降を実行している場合は、新しいスイッチ「–forceupdate」を使用して、コネクタにTETRA定義をダウンロードさせることができます。

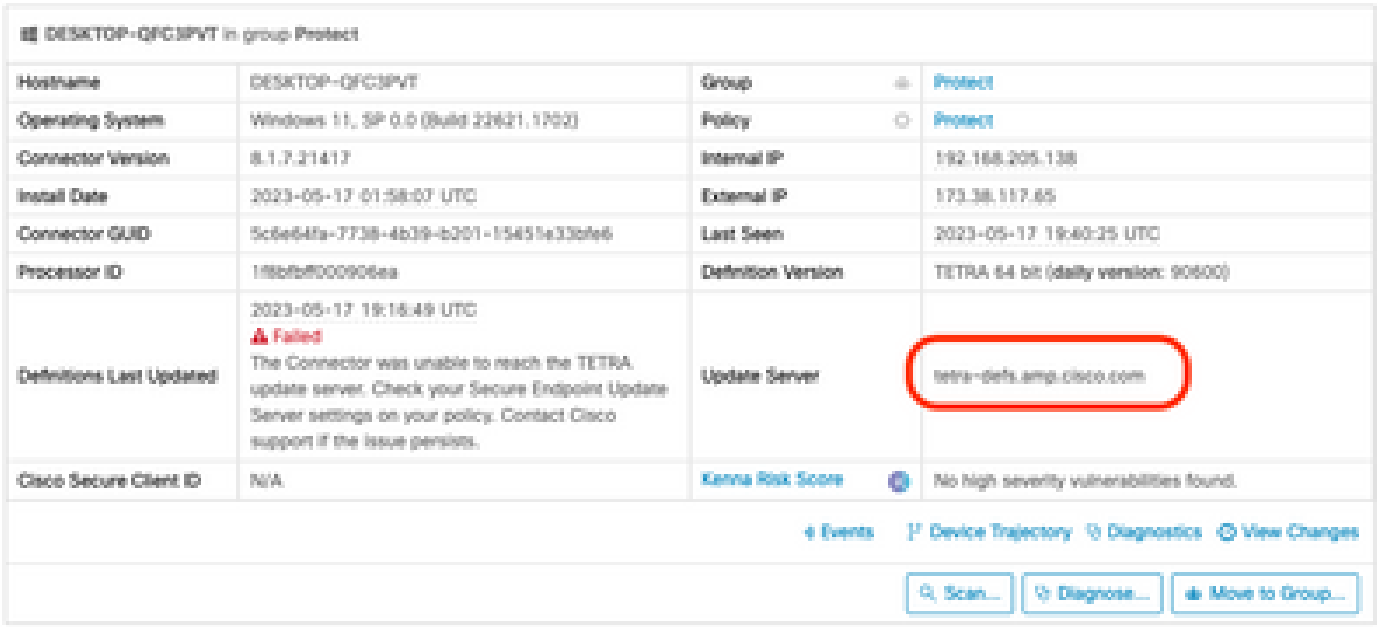
```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

更新が強制された後、更新が発生するかどうかを確認するためにTETRA定義を再びチェックできます。 それでもアップデートが行われていない場合は、TETRAサーバへの接続を確認する必要があります。

エンドポイントでのTETRA Definition Server接続の確認

エンドポイントポリシーには、定義をダウンロードするためにエンドポイントが接続する定義サーバが含まれます。

コンピュータの詳細ページに更新サーバが表示されます。 次の図は、アップデートサーバが表示されている場所を示しています。



パブリッククラウドでは、エンドポイントが接続できる必須のサーバ名は、「Cisco Secure Endpointおよびマルウェア分析を適切に運用するために必要なサーバアドレス」に記載されています。

直接接続の検証

エンドポイントから次のコマンドを実行して、更新サーバへのDNSルックアップを確認できます。

```
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
```

IPアドレスが解決されると、サーバへの接続をテストできます。 有効な応答は次のようになります。

<#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
```

CRLサーバで証明書を検証するための接続(commercial.ocsp.identrust.comまたはvalidation.identrust.comなど)を確立できない場合は、次のような エラーが表示されます。

```
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
```

プロキシの検証

エンドポイントがプロキシを使用するように設定されている場合は、最後のエラーステータスを確認できます。 下記のPowerShellを実行すると、TETRA更新の試行で最後のエラーが返される場合があります。

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

最後のエラーコー	問題	[アクション（Actions）]

ド		
4294965193	プロキシへの接続を確立できませんでした	プロキシへのネットワーク接続を確認する
4294965196	プロキシで認証できませんでした	プロキシの認証資格情報を確認します
4294965187	プロキシに接続し、ダウンロードできませんでした	ダウンロードの問題についてプロキシログを確認する

追加情報

- 上記のチェックが完了したにもかかわらず、エンドポイントでTETRA定義のダウンロードが繰り返し失敗する場合は、ポリシーで定義された更新間隔と同じ間隔でデバッグモードのコネクタを有効にし、サポートバンドルを生成してください。コネクタがデバッグモードの場合は、Wiresharkのパケットキャプチャも取得することに注意してください。また、パケットキャプチャは、ポリシーで定義されている更新間隔と同じ時間間隔で実行する必要があります。この情報を収集したら、詳細な調査のために、この情報とともにCisco TACケースをオープンしてください。

AMP for Windowsコネクタからの診断データの収集

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。