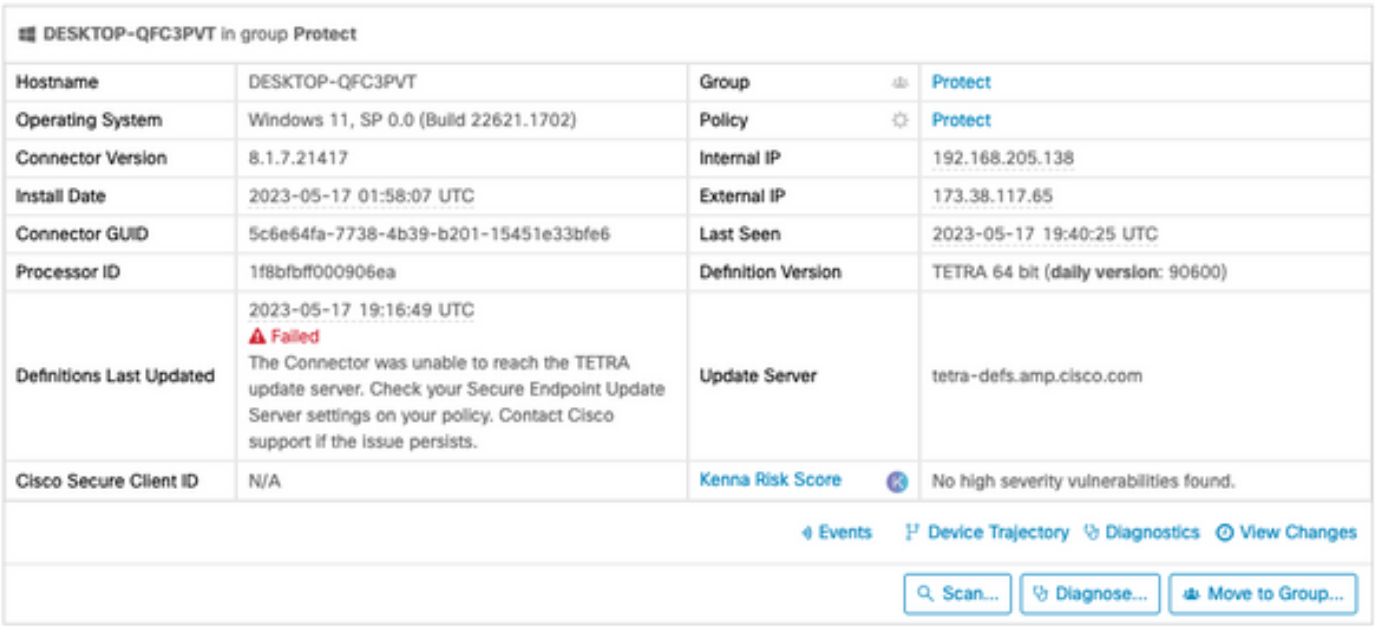
TETRA 정의 업데이트 실패 문제 해결

목차

소개

이 문서에서는 엔드포인트가 Cisco TETRA 정의 업데이트 서버에서 TETRA 정의를 업데이트하지 못하는 이유를 조사하기 위해 수행해야 할 단계에 대해 설명합니다.

Secure Endpoint Console에 표시된 정의 Last Updated 실패가 아래와 같이 Computer details(컴퓨터 세부사항) 아래에 나타납니다.



문제 해결

Windows용 Cisco Secure Endpoint에서 업데이트를 다운로드하려면 TETRA 정의 서버에 대한 지

속적인 연결이 필요합니다.

TETRA 정의를 다운로드할 때 흔히 발생하는 오류는 다음과 같습니다.

- 서버 주소를 확인하지 못했습니다.
- SSL 인증서 검증 실패(Certificate Revocation List 검사 포함)
- 다운로드 중 중단
- 프록시 서버에 연결하지 못했습니다.
- 프록시 서버에 대한 인증 실패

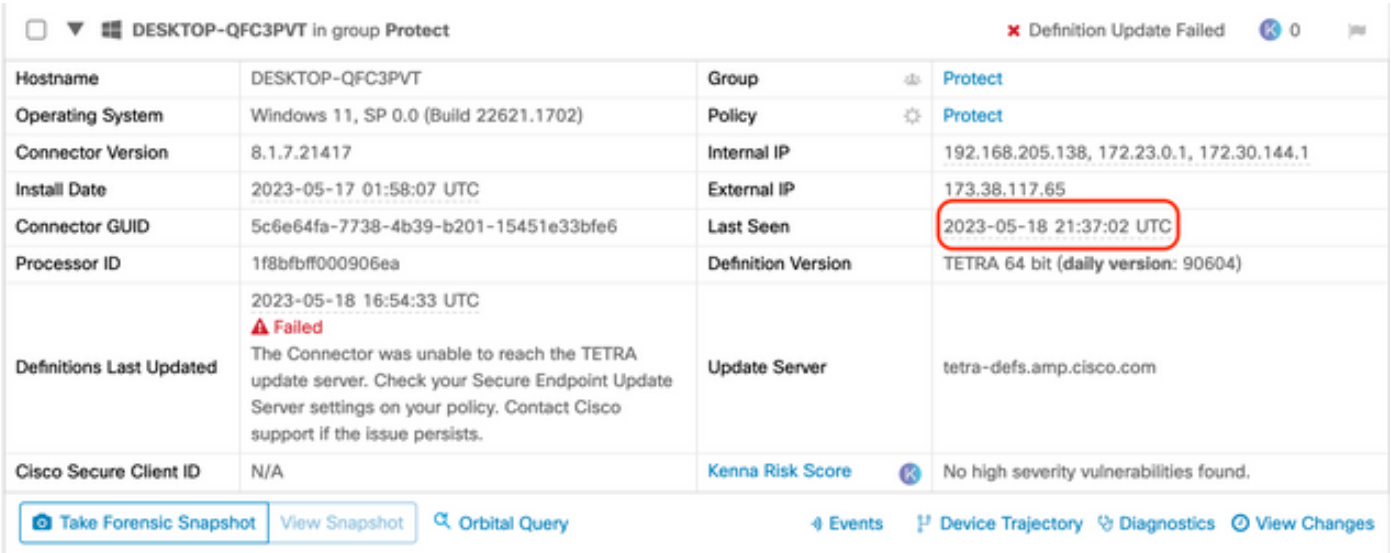
TETRA 정의를 다운로드하는 동안 오류가 발생하면 다음 업데이트 간격 또는 사용자가 수동 업데이트를 시작하는 경우 다음 시도가 이루어집니다.

보안 엔드포인트 콘솔에서 엔드포인트가 보고한 연결 확인

Secure Endpoint Console(보안 엔드포인트 콘솔)은 엔드포인트가 정기적으로 연결 중인지 여부를 표시합니다. 엔드포인트가 활성 상태이고 최근 "Last Seen" 상태인지 확인합니다. 엔드포인트가 Secure Endpoint Console에서 체크 인하지 않는 경우, 이는 엔드포인트가 활성 상태가 아니거나 일부 연결 문제가 있음을 나타냅니다.

Cisco는 매일 평균 4개의 정의 업데이트를 릴리스하며, 하루 중 어느 시점에서든 엔드포인트에서 업데이트를 다운로드하지 못하면 커넥터에서 오류 메시지를 게시합니다. 이러한 빈도를 고려할 때, 엔드포인트가 지속적으로 연결되어 있고 TETRA 서버에 대한 안정적인 네트워크 연결이 지속되는 경우에만 엔드포인트가 "Within Policy(정책 내)"로 보고됩니다.

"Last Seen(마지막 확인)" 상태는 아래에 표시된 대로 Computer details(컴퓨터 세부사항) 페이지에 있습니다.

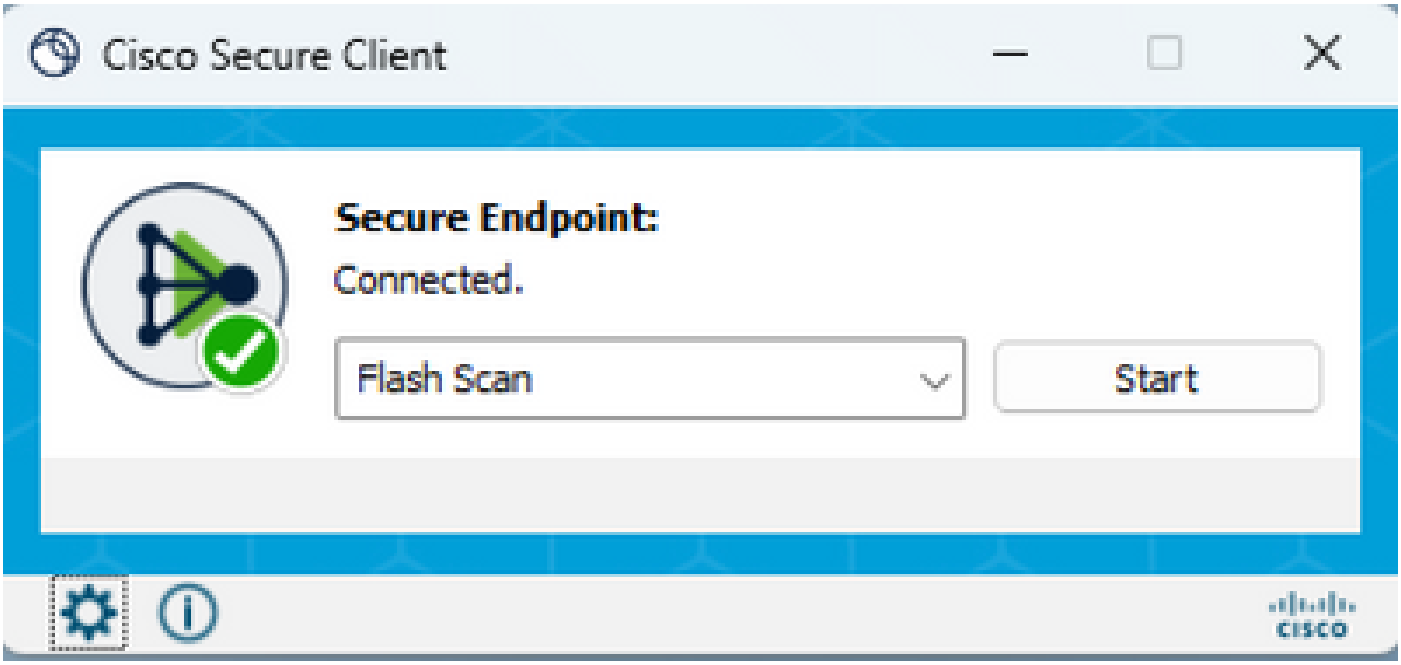


엔드포인트가 연결 중이고 정의가 다운로드되지 않았지만 콘솔에 표시되는 오류가 보고되면 문제가 간헐적으로 발생할 수 있습니다. 'Last Seen'과 'Definitions Last Updated' 간 시간 차이가 클 경우 추가 조사를 진행할 수 있다.

엔드포인트에서 연결 확인

최종 사용자는 UI 인터페이스를 사용하여 연결을 확인할 수 있습니다.

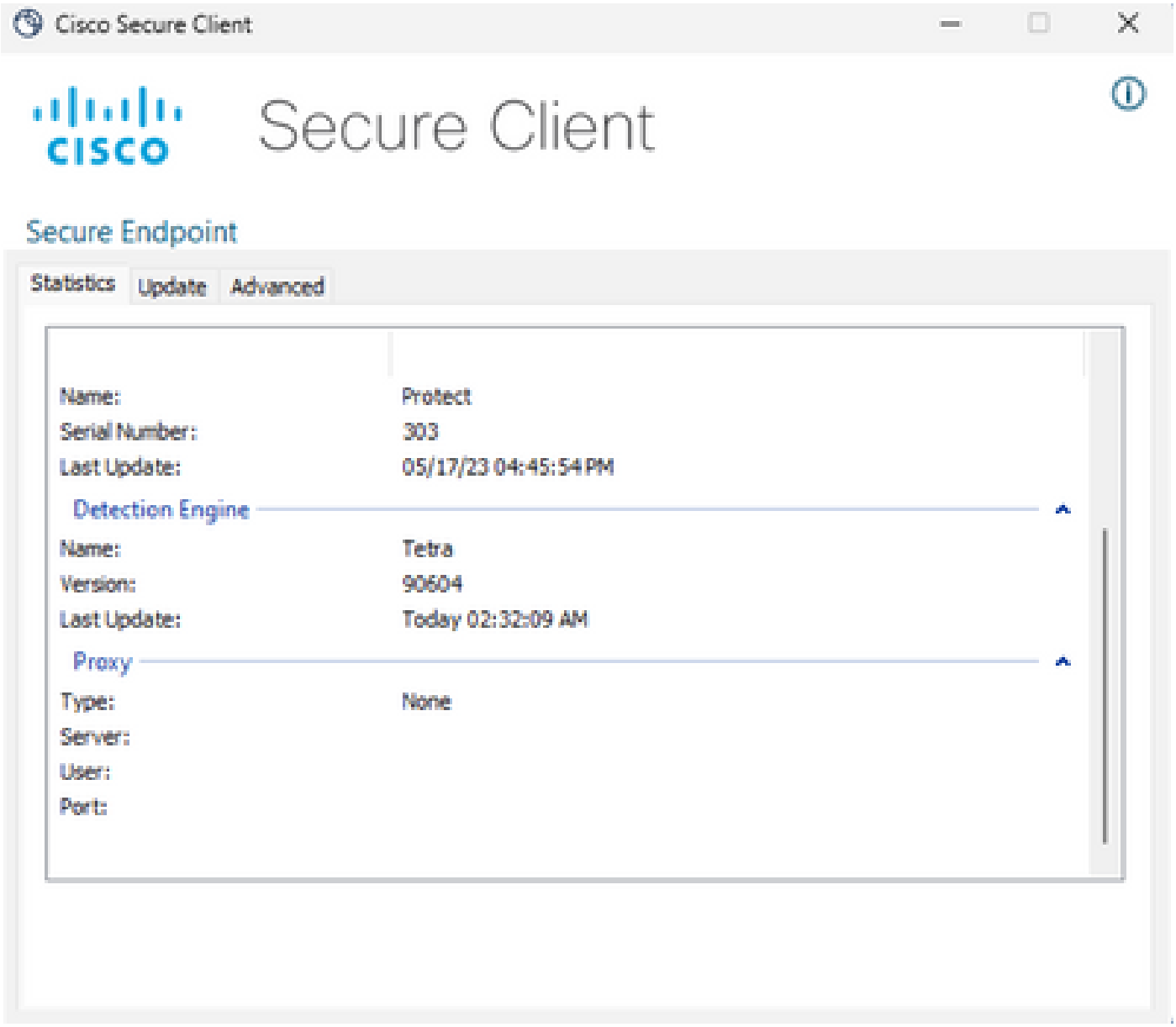
Cisco Secure Client를 열면 연결 상태가 표시됩니다.



ConnectivityTool은 엔드포인트가 연결되지 않았고 연결 문제를 보고할 때 사용할 수 있습니다. 이는 지원 패키지를 생성하는 IPSupportTool에 포함되어 있습니다.

엔드포인트에서 TETRA 정의 확인

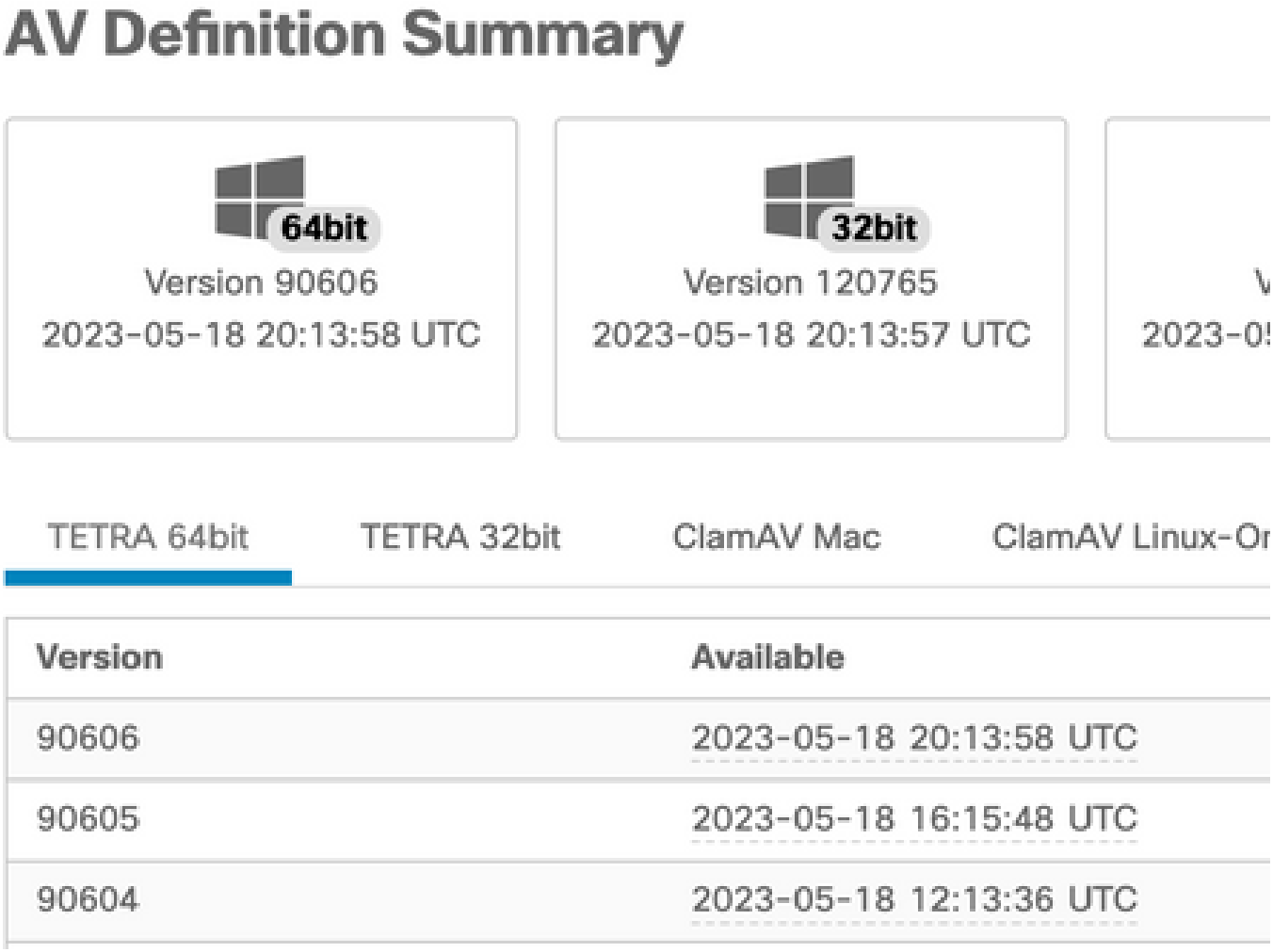
Cisco Secure Client는 엔드포인트 커넥터가 로드한 현재 TETRA 정의에 대한 정보를 제공합니다. 최종 사용자는 클라이언트를 열고 보안 엔드포인트에 대한 설정을 확인할 수 있습니다. Statistics(통계) 탭에서 TETRA의 현재 정의를 사용할 수 있습니다.



또한 현재 TETRA 정의 세부사항은 엔드포인트의 AmpCLI 툴에서 보고합니다. 명령의 예는 다음과 같습니다.

```
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
```

정의 버전은 TETRA를 포함한 각 엔진에 대해 표시됩니다. 위의 이 출력에서는 버전 90604입니다. 이는 Secure Endpoint Console의 Management(관리) > AV Definition Summary(AV 정의 요약)와 비교할 수 있습니다. 페이지의 예는 아래와 같습니다.

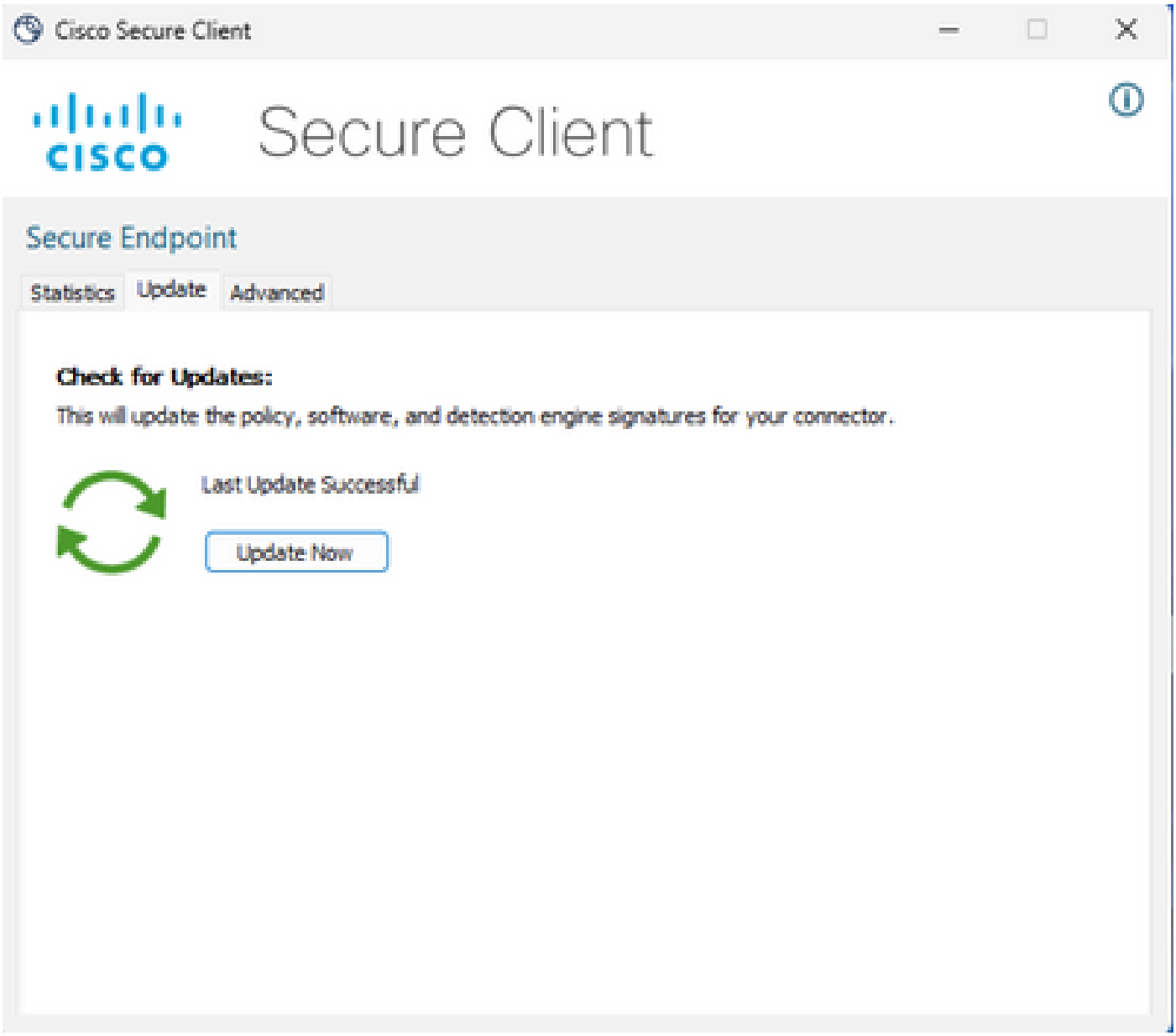


버전이 아직 이전 버전이고 커넥터 상태가 연결된 경우 정의를 업데이트하거나 TETRA 서버에 대한 엔드포인트 연결을 확인할 수 있습니다.

엔드포인트에서 TETRA 정의 업데이트 강제 수행

최종 사용자는 TETRA 다운로드 진행률을 입력하고 확인할 수 있습니다. 사용자가 업데이트를 트리거하려면 정책에서 옵션을 설정해야 합니다. Advanced Settings(고급 설정) > Client User Interface policy settings(클라이언트 사용자 인터페이스 정책 설정) 페이지에서 사용자에 의해 트리거되는 정의에 대해 Allow user to update TETRA definitions(사용자가 TETRA 정의를 업데이트할 수 있도록 허용) 설정을 활성화해야 합니다.

Cisco Secure Client에서 최종 사용자는 클라이언트를 열고 Secure Endpoint에 대한 설정을 확인할 수 있습니다. 사용자는 "Update Now(지금 업데이트)"를 클릭하여 아래에 표시된 대로 TETRA 정의 업데이트를 트리거할 수 있습니다.



AMP for Endpoints Connector 버전 7.2.7 이상을 실행 중인 경우 새 스위치 "-forceupdate"를 사용하여 커넥터가 TETRA 정의를 다운로드하도록 강제할 수 있습니다.

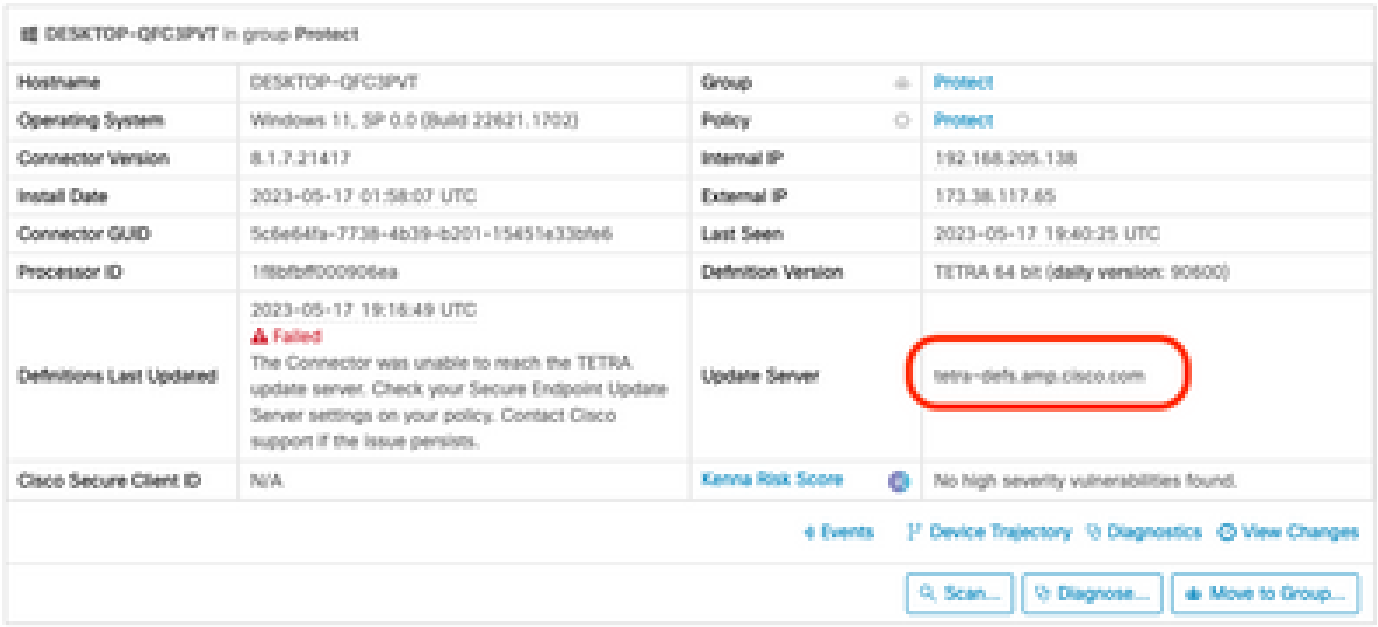
```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

업데이트가 강제 수행된 후 TETRA 정의를 다시 확인하여 업데이트가 발생하는지 확인할 수 있습니다. 업데이트가 아직 진행되지 않은 경우 TETRA 서버에 대한 연결을 확인해야 합니다.

엔드포인트에서 TETRA 정의 서버 연결 확인

엔드포인트 정책에는 엔드포인트가 정의를 다운로드하기 위해 연결하는 정의 서버가 포함됩니다.

컴퓨터 세부사항 페이지에는 업데이트 서버가 포함되어 있습니다. 아래 그림에는 업데이트 서버가 표시되는 위치가 나와 있습니다.



퍼블릭 클라우드의 경우 엔드포인트가 연결할 수 있는 필수 서버 이름이 아래에 나열됩니다.
[Required Server Addresses for Appropriate Cisco Secure Endpoint & Malware Analytics Operations(올바른 Cisco Secure Endpoint & Malware Analytics 작업에 필요한 서버 주소)]

직접 연결 유효성 검사

엔드포인트에서 다음 명령을 실행하여 업데이트 서버에 대한 DNS 조회를 확인할 수 있습니다.

```
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
```

IP가 확인되면 서버에 대한 연결 연결을 테스트할 수 있습니다. 유효한 응답은 다음과 같습니다.

<#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 서버(예: commercial.ocsp.identrust.com 또는 validation.identrust.com)로 인증서를 검증하기 위해 연결할 수 없는 경우, 다음과 같은 오류가 표시됩니다.

```
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
```

프록시 유효성 검사

엔드포인트가 프록시를 사용하도록 구성된 경우 마지막 오류 상태를 확인할 수 있습니다. 아래의 PowerShell을 실행하면 TETRA 업데이트 시도의 마지막 오류를 반환할 수 있습니다.

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

마지막 오류 코드	문제	작업
4294965193	프록시에 대한 연결을 설정할 수 없음	프록시에 대한 네트워크 연결 확인
4294965196	프록시로 인증할 수 없습니다.	프록시에 대한 인증 자격 증명 확인
4294965187	프록시에 연결되었고 다운로	프록시 로그에서 다운로드 문제 확인

	드에 실패했습니다.	

추가 정보

- 위의 검사를 완료했음에도 불구하고 TETRA 정의를 다운로드하지 못하는 엔드포인트가 지속적으로 발견되면 정책에 정의된 업데이트 간격과 같은 시간 간격으로 디버그 모드에서 커넥터를 활성화하고 지원 번들을 생성하십시오. 커넥터가 디버그 모드인 경우, Wireshark 패킷 캡처도 수행해야 합니다. 패킷 캡처는 정책에 정의된 업데이트 간격과 동일한 시간 간격으로 실행되어야 합니다. 이 정보가 수집되면 추가 조사를 위해 이 정보와 함께 Cisco TAC 케이스를 여십시오.

AMP for Windows 커넥터에서 진단 데이터 수집

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.