TETRA 다운로드에 대한 사용자 지정 시간 구성

목차

소개

이 문서에서는 원하는 시간에 TETRA 업데이트를 다운로드하여 대역폭 사용량의 요구 사항을 충족하도록 로컬 엔드포인트를 구성하는 방법에 대해 설명합니다.

배경 정보

TETRA는 안티바이러스 서명을 사용하여 엔드포인트를 보호하는 보안 엔드포인트용 오프라인 엔진입니다. TETRA는 자사의 시그니처 데이터베이스에 대한 매일 업데이트를 받아 야생 환경의 모든 새로운 위협에 대처합니다. 이러한 업데이트는 대규모 환경에서 상당한 대역폭을 사용할 수 있으므로 각 엔드포인트는 업데이트 간격 내에 다운로드 시간을 임의로 지정하며, 기본적으로 이 시간은 1시간으로 설정됩니다. TETRA 정책에서 다른 업데이트 간격을 선택할 수 있지만 이 다운로드 프로세스를 트리거할 특정 시간을 선택할 수는 없습니다. 이 문서에서는 TETRA에서 Windows 일정 작업을 사용하여 AV 서명을 업데이트하도록 하는 해결 방법을 제공합니다.

사전 요구 사항

요구 사항

보안 엔드포인트 정책 구성 및 Windows 일정 작업에 대한 기본 지식

사용되는 구성 요소

- 보안 엔드포인트 클라우드 콘솔
- Windows 8.1.3용 보안 엔드포인트 커넥터
- Windows 10 Enterprise

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

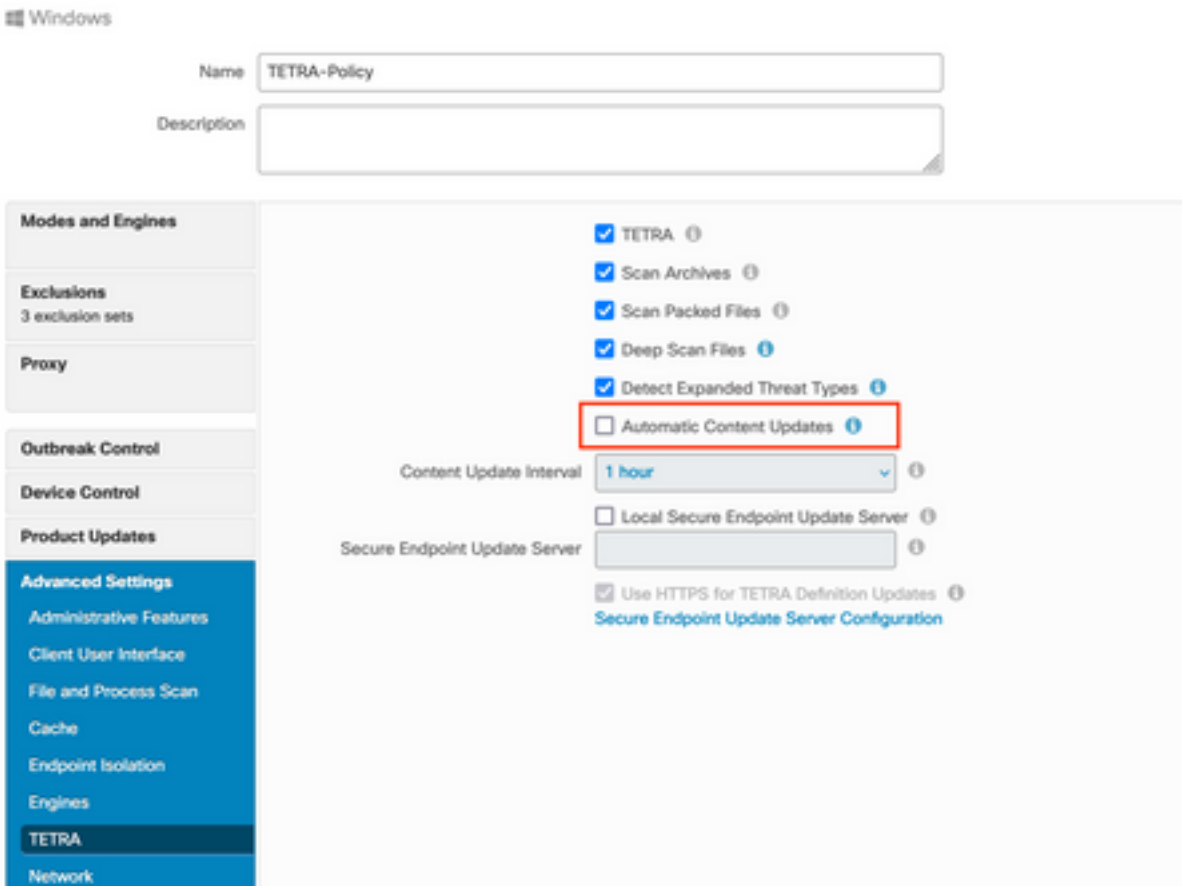
구성

경고: 백그라운드 섹션에서 설명한 것처럼 TETRA 업데이트는 상당한 대역폭을 소비할 수 있습니다. 기본적으로 보안 엔드포인트는 이러한 영향을 줄이고 업데이트 간격 내에 TETRA 업데이트를 임의 지정하려고 합니다. 이 값은 기본적으로 1시간으로 설정됩니다. 특히 대규모 환경에서 모든 커넥터가 동시에 정의를 업데이트하도록 강제하는 것은 권장되지 않습니다. 이 프로세스는 업데이트 시간을 제어하는 것이 중요한 특수한 상황에서만 사용해야 합니다. 다른 시나리오에서는 자동 업데이트를 사용하는 것이 좋습니다.

사용자 지정 TETRA 다운로드 시간에 대해 구성할 보안 엔드포인트 정책을 선택합니다.

참고: 이 컨피그레이션은 정책 기반으로 수행되며 이 정책의 모든 엔드포인트가 영향을 받는다는 점에 유의하십시오. 따라서 사용자 지정 TETRA 업데이트를 제어하려는 모든 디바이스를 동일한 보안 엔드포인트 정책에 두는 것이 좋습니다.

Secure Endpoint Management Console에 로그인하여 **Management** > **Policies**로 이동한 다음 사용하도록 선택한 정책을 검색하고 **edit**를 클릭합니다. 정책 컨피그레이션 페이지에서 TETRA 섹션으로 **이동합니다**. 이 섹션에서 Automatic Content Updates(**자동 콘텐츠 업데이트**) **확인란**의 선택을 취소하고 **정책**을 저장합니다. 이는 모두 Secure Endpoint Cloud 콘솔의 컨피그레이션과 관련이 있습니다.



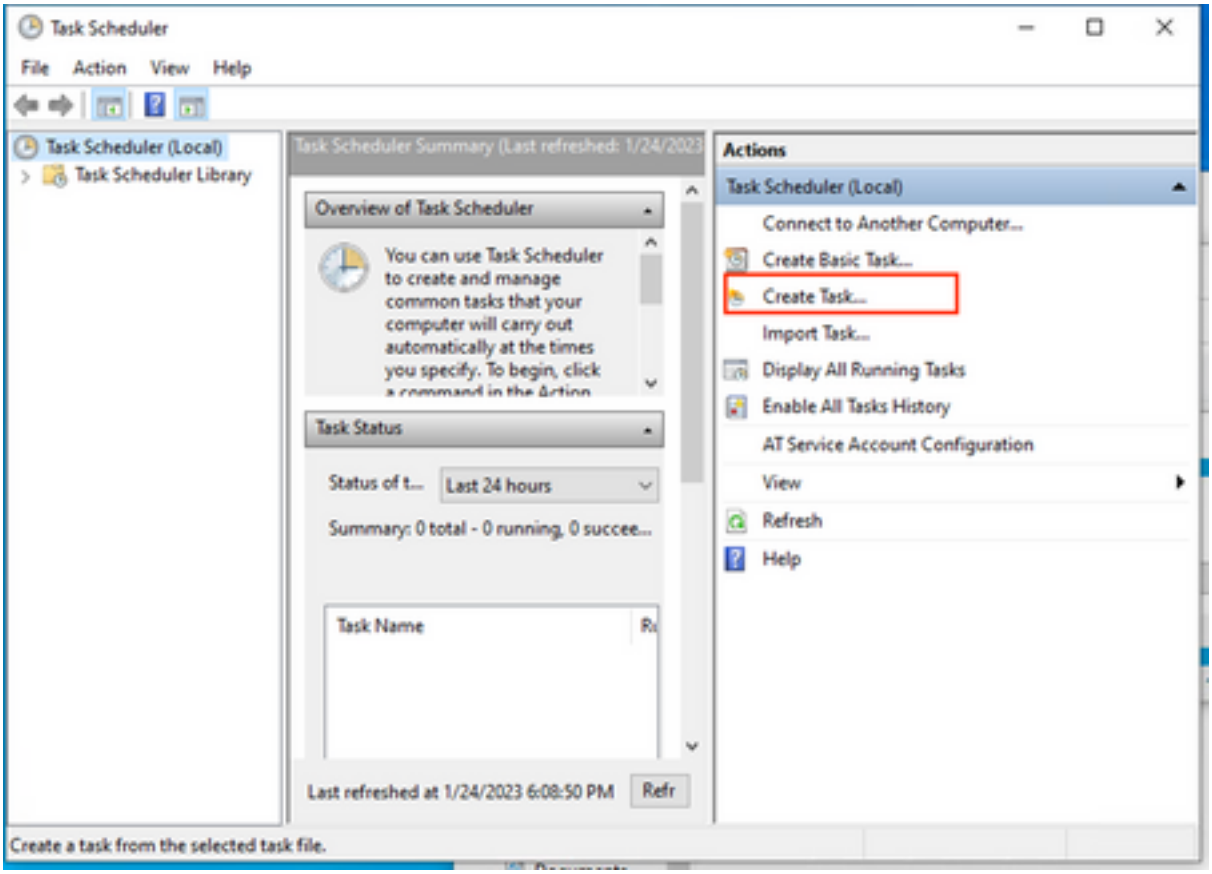
다음 구성 부분에서는 Windows 장치에 액세스하고 새 메모장 파일을 열어 다음 행을 추가합니다.

```
cd C:\Program Files\Cisco\AMP\8.1.3.21242
sfc.exe -forceupdate
```

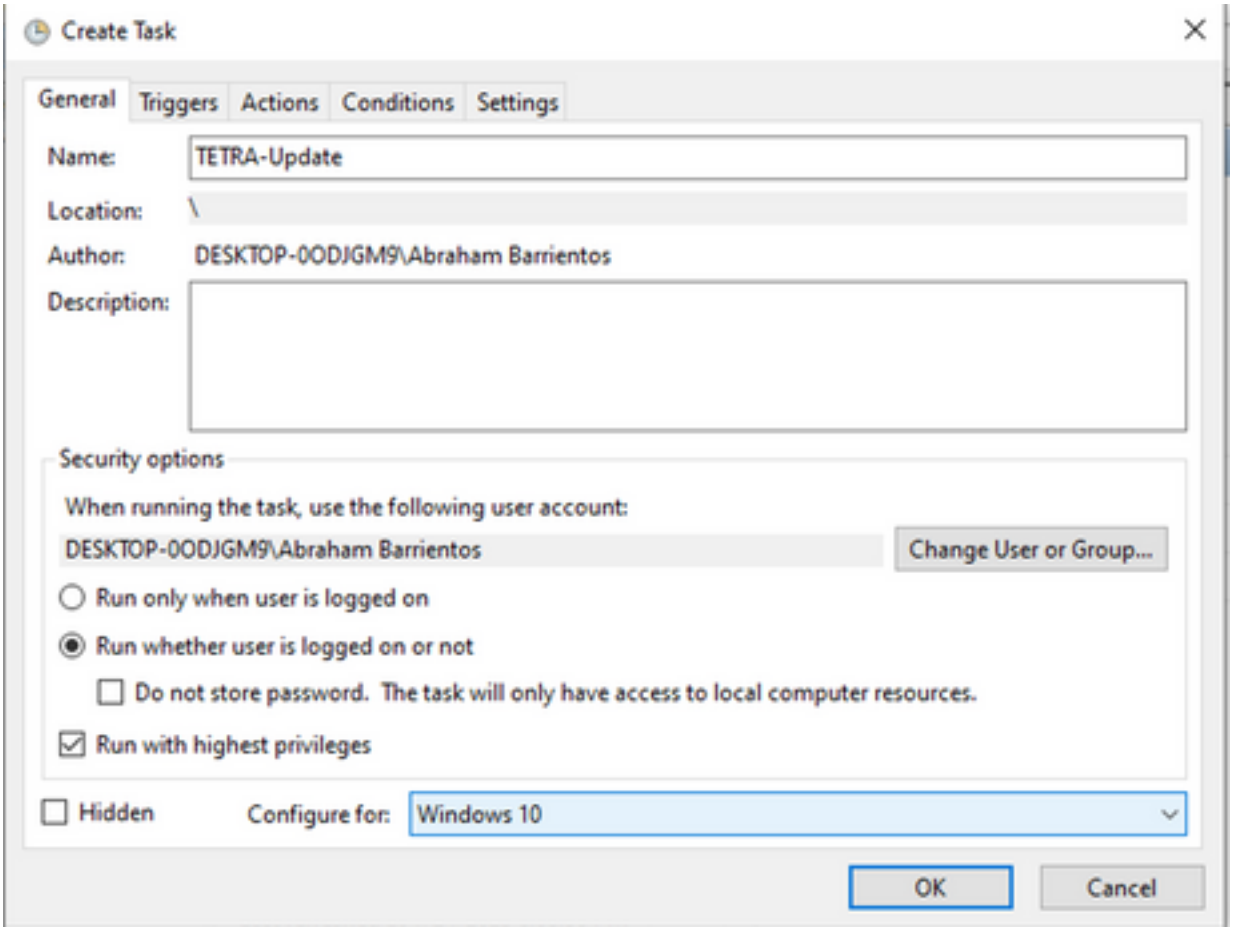
엔드포인트에 현재 설치된 버전과 일치하는 보안 엔드포인트 버전(이 예의 경우 8.1.3.21242v)을 사용해야 합니다. 버전을 모를 경우 **보안 엔드포인트** 사용자 인터페이스 기어 아이콘을 클릭한 다음 **통계 탭**을 클릭하여 현재 버전을 확인할 수 있습니다. 이러한 행을 메모장에 추가한 후 File(파일)을

클릭한 다음 Save As(다른 이름으로 **저장**)를 클릭합니다**.** 그런 다음 유형**으로 저장을** 클릭하고 **모든** 파일을 **선택합니다**. 마지막으로 파일 이름을 입력하고 .BAT 확장자로 저장합니다. C:\ 폴더 아래에 파일을 저장하려면 관리자 권한으로 메모장을 실행해야 합니다. 참고 사항으로 BAT 파일을 실행하여 테스트용 TETRA 업데이트를 강제로 실행할 수 있습니다.

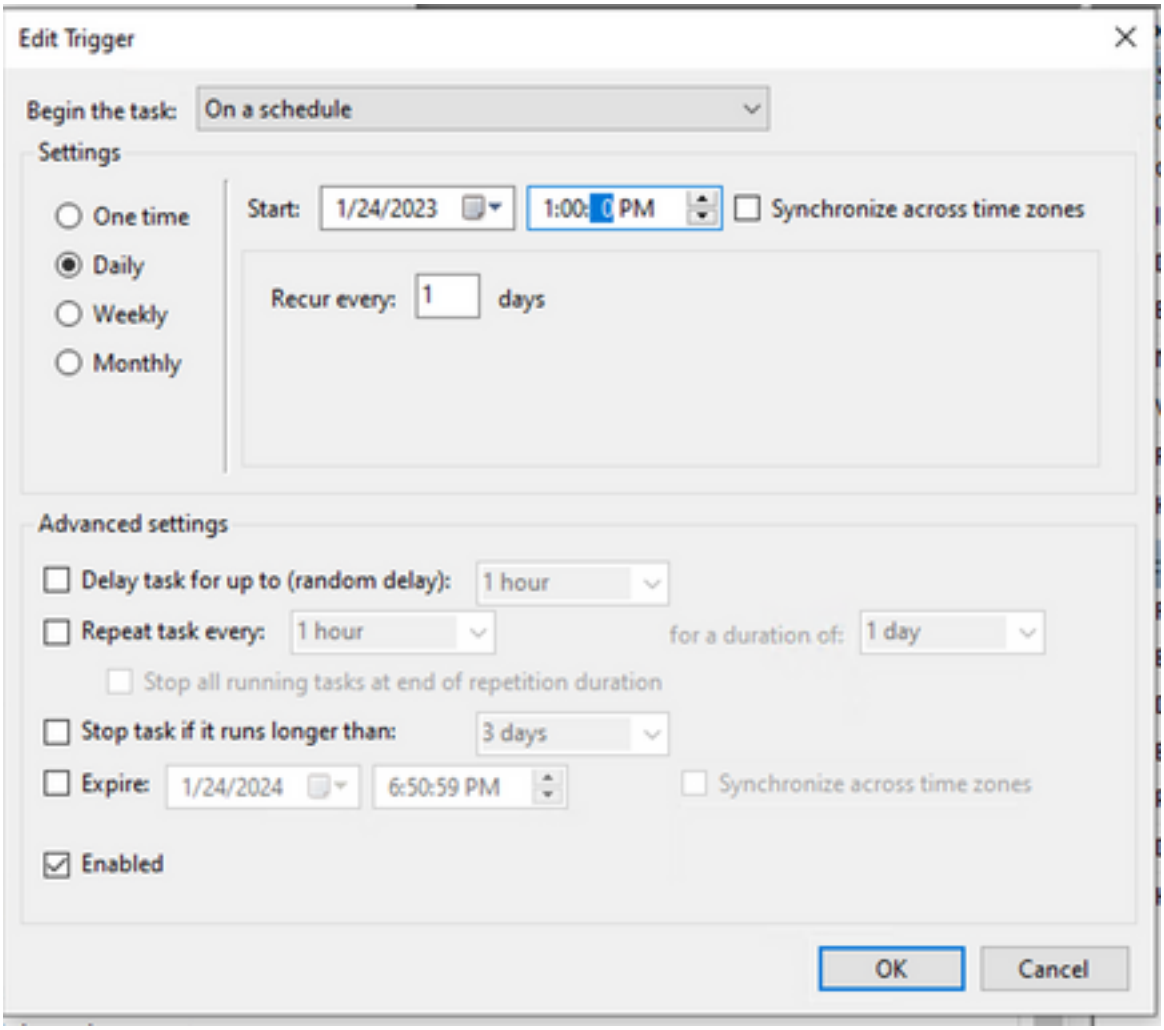
Windows 시스템에서 작업 일정 잡기 작업 일정 관리기 열기 를 열고 오른쪽 **열**에 있는 작업 만들기 단추를 클릭합니다.



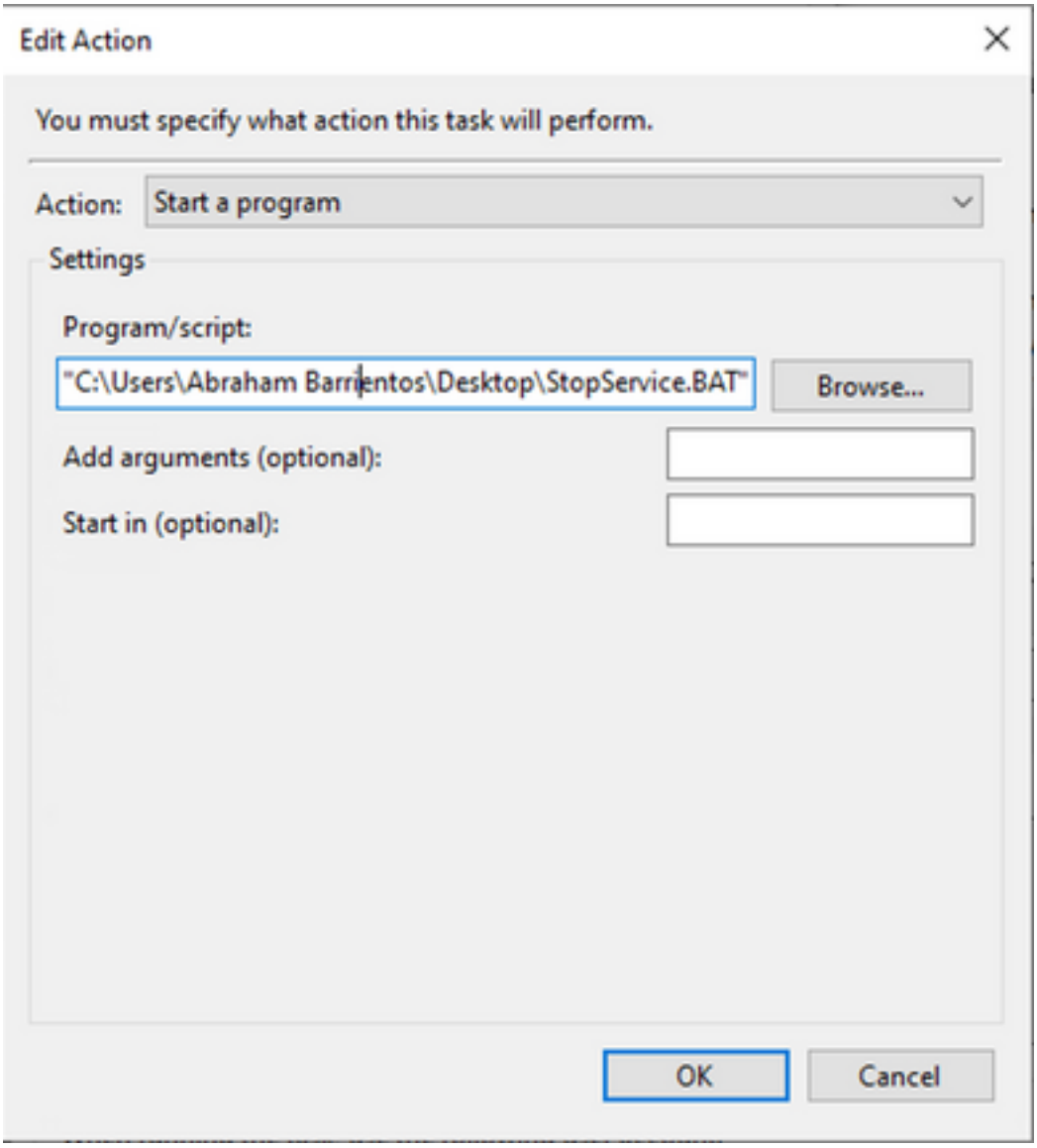
일반 탭에서 이 작업의 이름을 입력하고 사용자가 **로그인하거나 로그인하지 않을 때마다 실행을 선택합니다**. Run **with the highest privelages(가장 높은 권한으로** 실행) 확인란을 선택합니다. configure **for 옵션**에서 적용할 OS를 선택합니다. 이 데모에서는 Windows 10이 사용되었습니다.



Triggers(트리거) **탭**에서 New Trigger(**새 트리거)를 클릭합니다.** New trigger configuration(새 트리거 컨피그레이션) 페이지에서 TETRA에서 시그니처를 업데이트할 시간을 사용자 지정할 수 있습니다. 이 예에서는 현지 기계 시간 오후 1시에 실행되는 일별 일정이 사용되었습니다. 시작 날짜 옵션은 이 작업이 활성화되는 시기를 정의합니다. 일정 설정을 마쳤으면 확인을 **클릭합니다.**



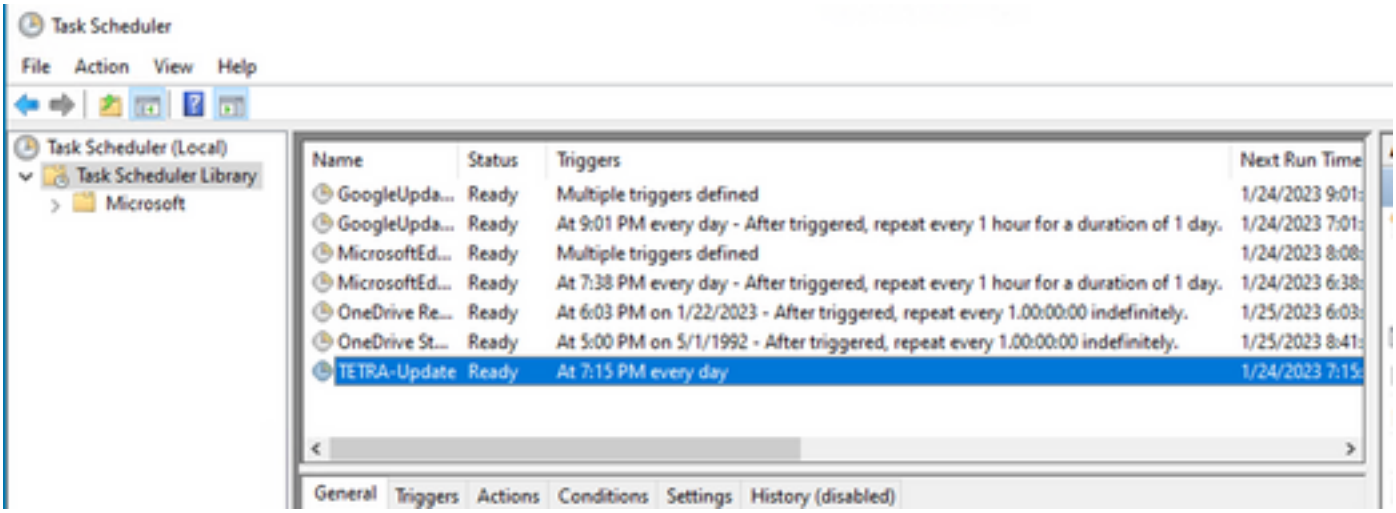
Actions(작업) **탭**에서 New Action(**새 작업)을** 클릭합니다. 새 **작업 탭**에서 작업 **설정에** 대한 **프로그램** 시작을 **선택합니다**. Program/Settings(프로그램/설정)에서 **Browse(찾아보기)**를 클릭하고 BAT 스크립트를 검색한 후 선택합니다. 확인을 **클릭하여** 작업을 생성합니다. 나머지 설정을 기본값으로 유지하고 **확인**을 클릭하여 작업을 만듭니다.



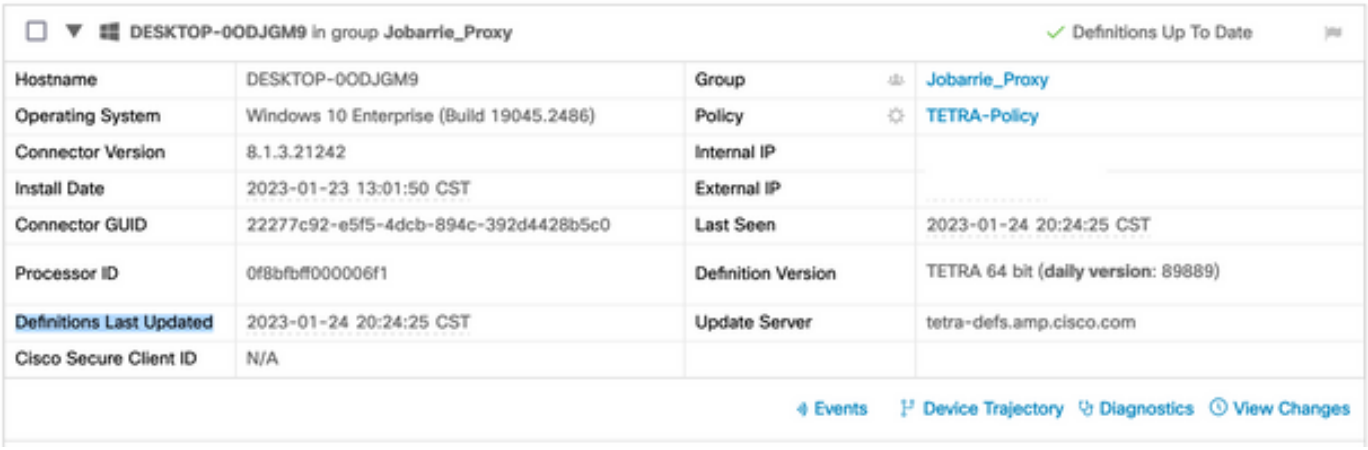
마지막으로, "가장 높은 권한으로 실행"을 선택했으므로 이 작업 스케줄러에서 작업을 만들려면 관리자 자격 증명이 필요합니다. 관리자 자격 증명으로 인증하면 구성된 일정에 따라 TETRA를 업데이트할 시기를 Secure Endpoint Service에 알리기 위해 작업을 실행하고 실행할 준비가 된 것입니다.

다음을 확인합니다.

왼쪽 **열**에서 작업 스케줄러 라이브러리 폴더를 클릭합니다. 일정이 생성되어 예상대로 나열되었는지 확인합니다.



Secure Endpoint User interface > statistics 탭 아래에서 커넥터가 다운로드한 최신 TETRA 정의 **번호**를 확인할 수 있습니다. 이 번호를 사용하여 콘솔에서 **Management(관리) > Av Definitions(Av 정의) 요약 아래**에서 사용 가능한 최신 정의를 비교하여 디바이스가 최신 정의와 함께 최신 상태인지 확인할 수 있습니다. 또 다른 대안은 Secure Endpoint Console에서 특정 엔드포인트에 대한 "Definitions Last Updated(마지막으로 업데이트된 정의)" 값을 모니터링하는 것입니다.



문제 해결

정의가 예상대로 업데이트되지 않으면 로그를 확인하여 TETRA 업데이트 오류를 검색할 수 있습니다. 이렇게 하려면 Schedule 작업 트리거 시간 전에 Advanced(고급) 탭 아래의 Secure Endpoint(보안 엔드포인트) 사용자 인터페이스에서 debug(디버그) 모드를 활성화합니다. 일정 작업 트리거 이후 최소 20분 동안 커넥터가 이 모드에서 실행되게 한 다음 C:\Program Files\Cisco\AMP\X.X.X에 있는 최신 sfcx**.exe.log** 파일(여기서 X.X.X는 시스템의 보안 엔드포인트의 현재 버전)을 확인합니다.

ForceWakeUpdateThreadAbout은 TETRA가 Schedule Job에 의해 트리거되어 예상대로 업데이트됨을 보여 줍니다. 이 로그가 표시되지 않으면 Windows 예약 작업 구성과 관련된 문제가 될 수 있습니다.

```
(99070187, +0 ms) Jan 24 20:30:01 [3544]: ForceWakeUpdateThreadAbout to force update thread
awake. Forcing tetra def update.
(99070187, +0 ms) Jan 24 20:30:01 [1936]: UpdateThread: Tetra ver string retrieved from config:
(99070781, +0 ms) Jan 24 20:30:02 [1936]: UpdateTetra entered...
(99070781, +0 ms) Jan 24 20:30:02 [1936]: UpdateTetra: elapsed: cur: 1674621002, last: 0,
interval:180
```

스케줄 작업이 TETRA를 트리거하여 정의를 갱신하는 경우 로그에서 관련 TETRA 오류를 검색해

야 합니다. 이는 업데이트 프로세스 중에 서비스가 중단되었음을 의미하는 TETRA 오류 코드 2200의 예입니다. 일반적인 TETRA 오류를 해결하는 방법은 이 문서의 범위를 벗어납니다. 그러나 이 문서의 끝부분에 있는 링크는 TETRA 오류 코드 트러블슈팅에 대한 유용한 Cisco 문서입니다.

```
ERROR: TetraUpdateInterface::update Update failed with error -2200
```

관련 정보

- TETRA
- Cisco Secure Endpoint - Tetra (3000)
- TETRA - Windows

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.