

수동으로 TETRA 정의 업데이트 적용 - Cisco Secure Endpoints

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco AMP(Secure Endpoints)에서 새 TETRA 정의를 수동으로 강제 적용하는 절차에 대해 설명합니다.

기고자: Jesus Javier Martinez와 Uriel Tores, Yeraldin Sanchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Windows OS
- 엔드포인트용 AMP

사용되는 구성 요소

이 문서의 정보는 Windows용 Cisco AMP(Secure Endpoint)를 기반으로 합니다.

이 문서의 정보는 특정 환경의 디바이스에서 생성되었습니다.

- Windows 10 장치
- AMP 커넥터 7.0.5 버전

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

배경 정보

사용 설명서, Tetra는 Cisco Secure Endpoint Solution을 위한 완전한 안티바이러스 솔루션입니다. 최상의 보호를 받으려면 Cisco Secure Endpoint와 함께 사용해야 합니다. 타사 AV가 설치된 경우 TETRA를 올바르게 설치하고 운영하기 위해 다른 AV를 제거해야 합니다. 정의를 다운로드할 때 TETRA는 상당한 대역폭을 사용할 수도 있습니다.

주의: 대규모 구축 전에 테스트 환경에서 Tetra를 실행해야 합니다.

TETRA 엔진이 활성화되고 정의가 최신 상태이면 AMP 버전 6.3.1에서 Windows Defender를 비활성화해야 하므로 Cisco Secure Endpoint가 활성 안티바이러스 및 위협 보호 공급자로 지정됩니다.

정의는 자동으로 다운로드되지만 수동으로 TETRA 정의를 강제로 업데이트할 수 있습니다.

문제 해결

참고: Cisco Secure Endpoint 버전 7.2.7 이상에서 '-forceupdate' 인수를 사용하여 커넥터를 강제로 업데이트를 가져올 수 있습니다.

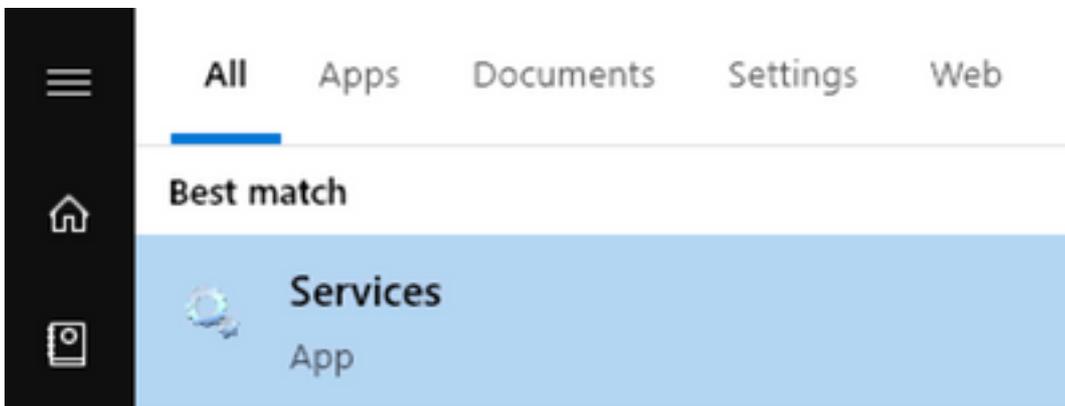
C:\Program Files\Cisco\AMP\7.2.7\sfc.exe -forceupdate

버전 7.2.7 아래에 정의를 업데이트하도록 하려면 이 가이드를 참조하십시오.

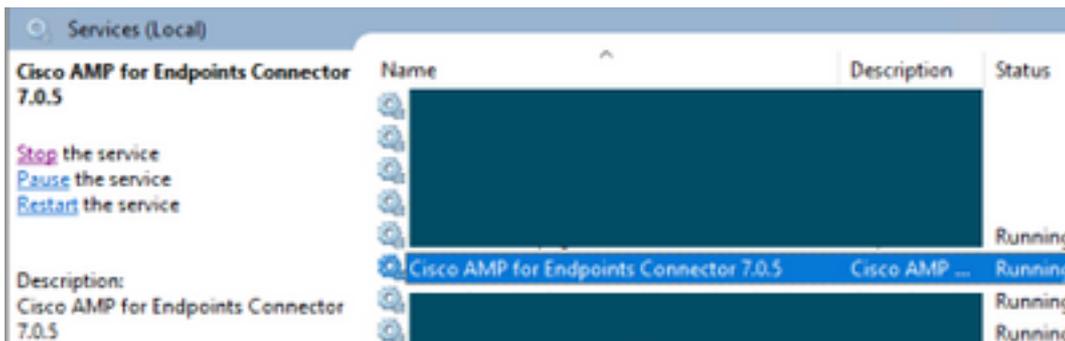
1단계. AMP 서비스를 중지합니다.

- 암호 보호가 없는 경우

1.1단계. 이미지에 표시된 대로 Services.msc를 엽니다.



1.2단계. 이미지에 표시된 대로 Services(서비스) > Cisco AMP for Endpoints Connector 7.0.5로 이동합니다.



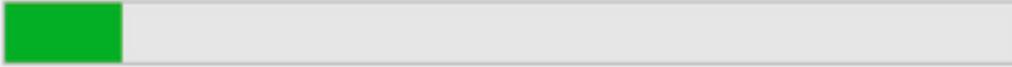
1.3단계. 이미지에 표시된 대로 AMP 서비스를 중지합니다.

Service Control



Windows is attempting to stop the following service on Local Computer...

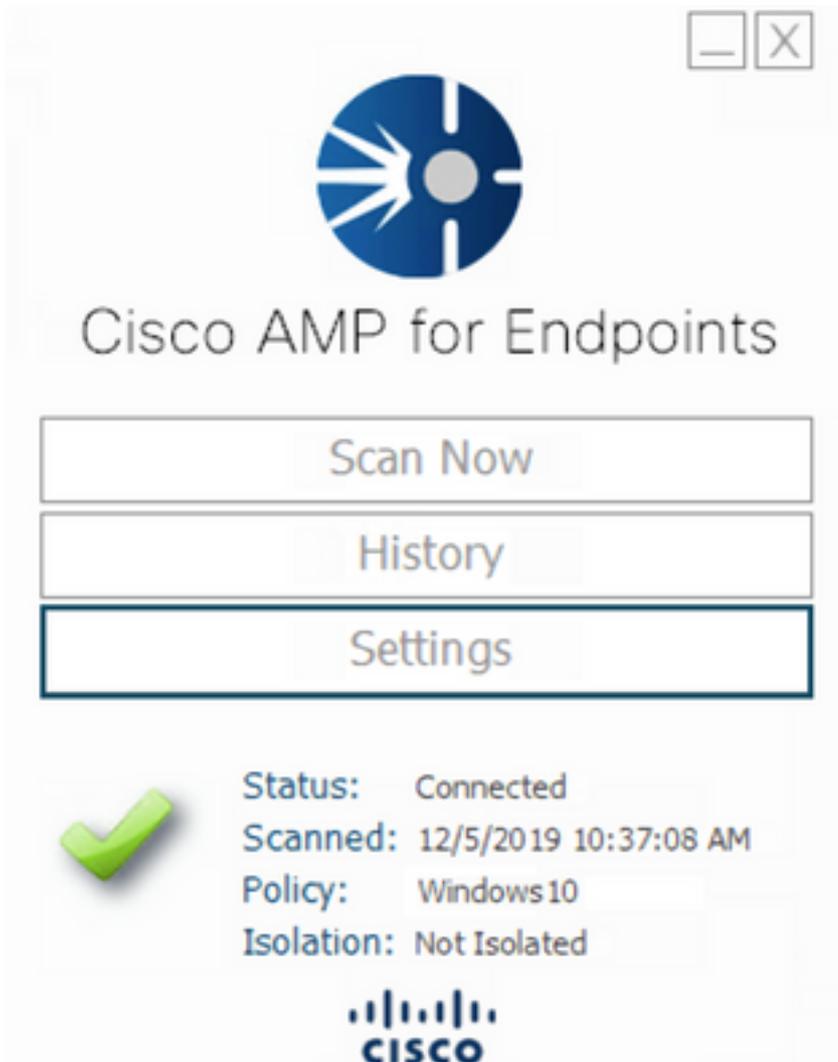
Cisco AMP for Endpoints Connector 7.0.5



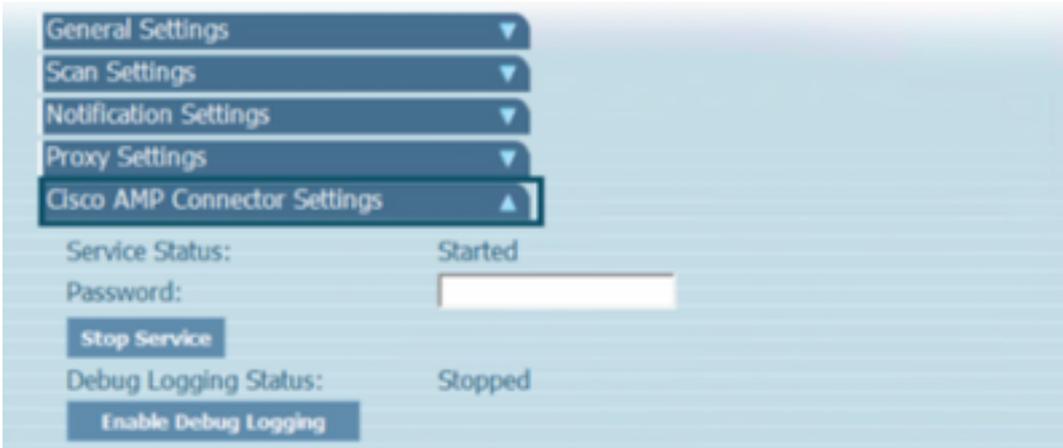
Close

- 암호 보호가 있는 경우

1.4단계. AMP User Interface(AMP 사용자 인터페이스)를 열고 이미지에 표시된 대로 **Settings(설정)**를 선택합니다.



1.5단계. 이미지에 표시된 대로 **Cisco AMP for Endpoints 설정**으로 이동합니다.

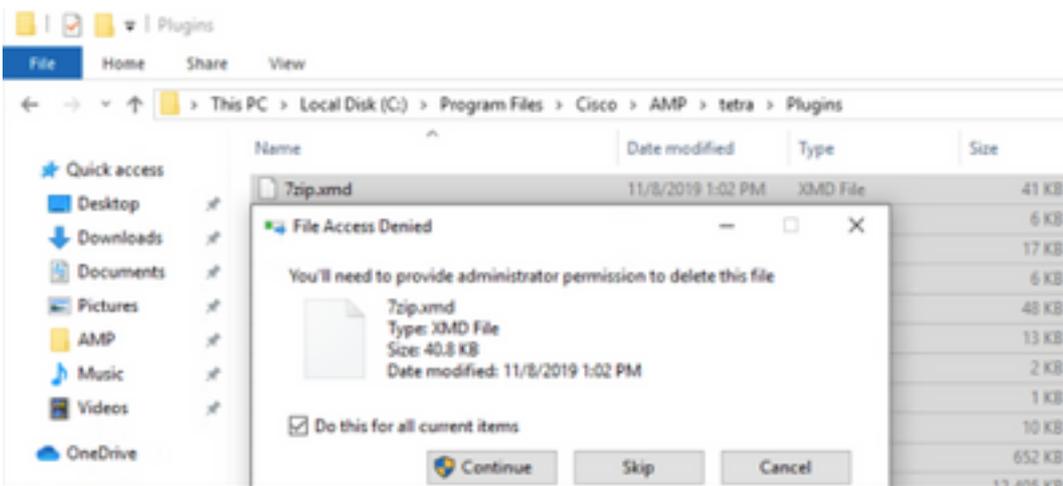


1.6단계. 비밀번호를 입력하고 이미지에 표시된 대로 서비스 중지를 클릭합니다.

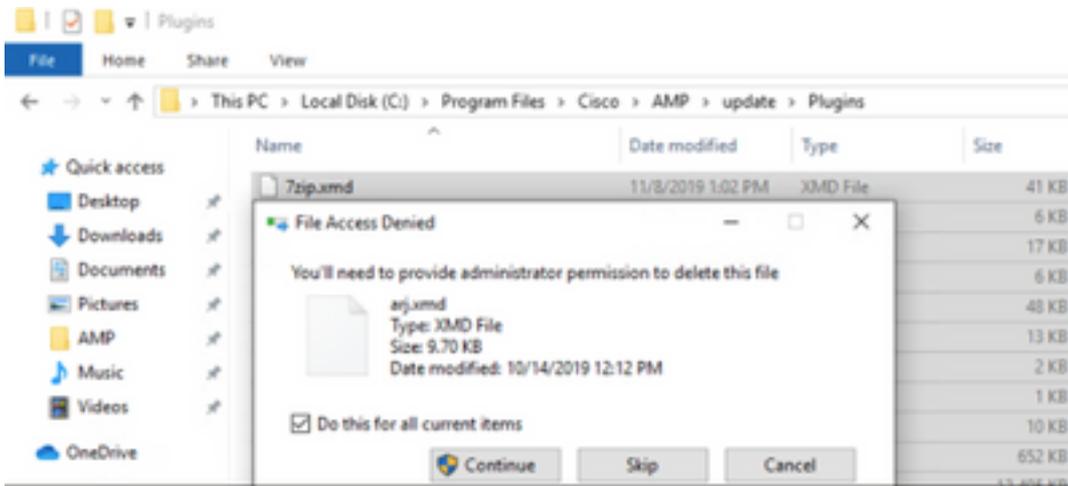


2단계. 일반적으로 C:\Program Files\Cisco\AMP에 있는 AMP 폴더로 이동합니다.

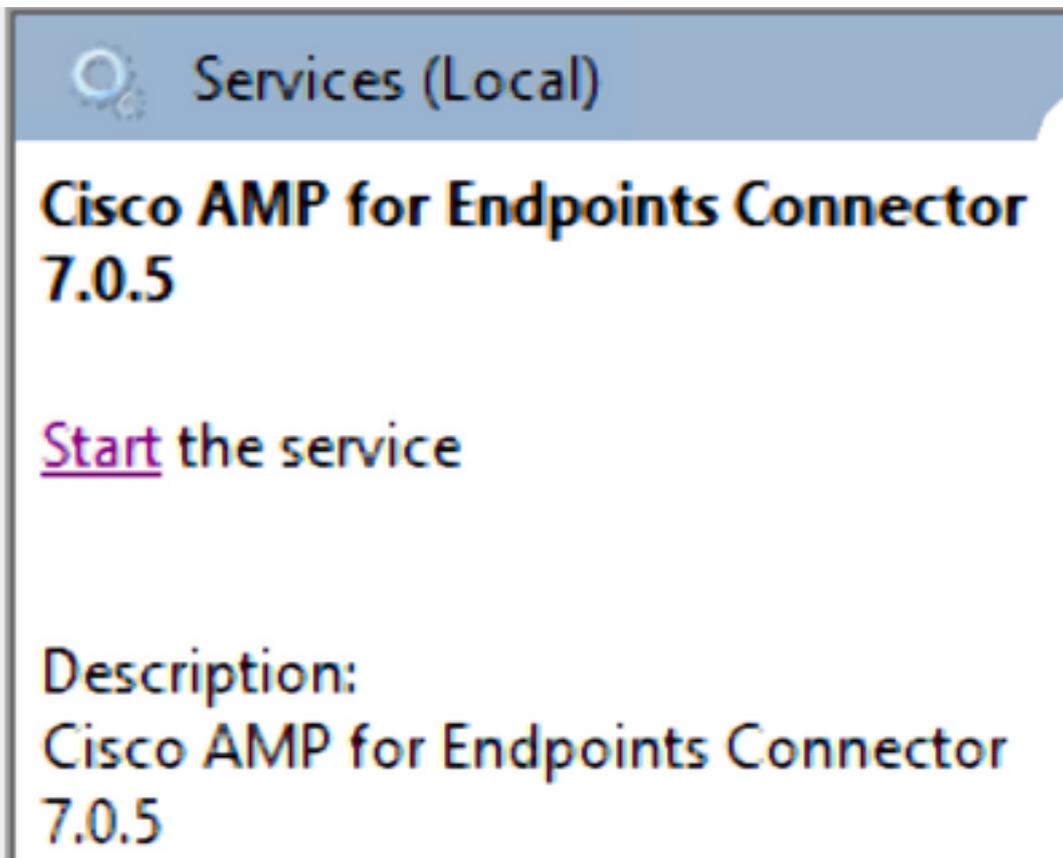
2.1단계. 이미지에 표시된 대로 C:\Program Files\Cisco\AMP\tetra\Plugins\ 폴더 내의 모든 내용을 삭제합니다.



2.2단계. 이미지에 표시된 대로 C:\Program Files\Cisco\AMP\update\Plugins\ 폴더 내의 모든 내용을 삭제합니다.

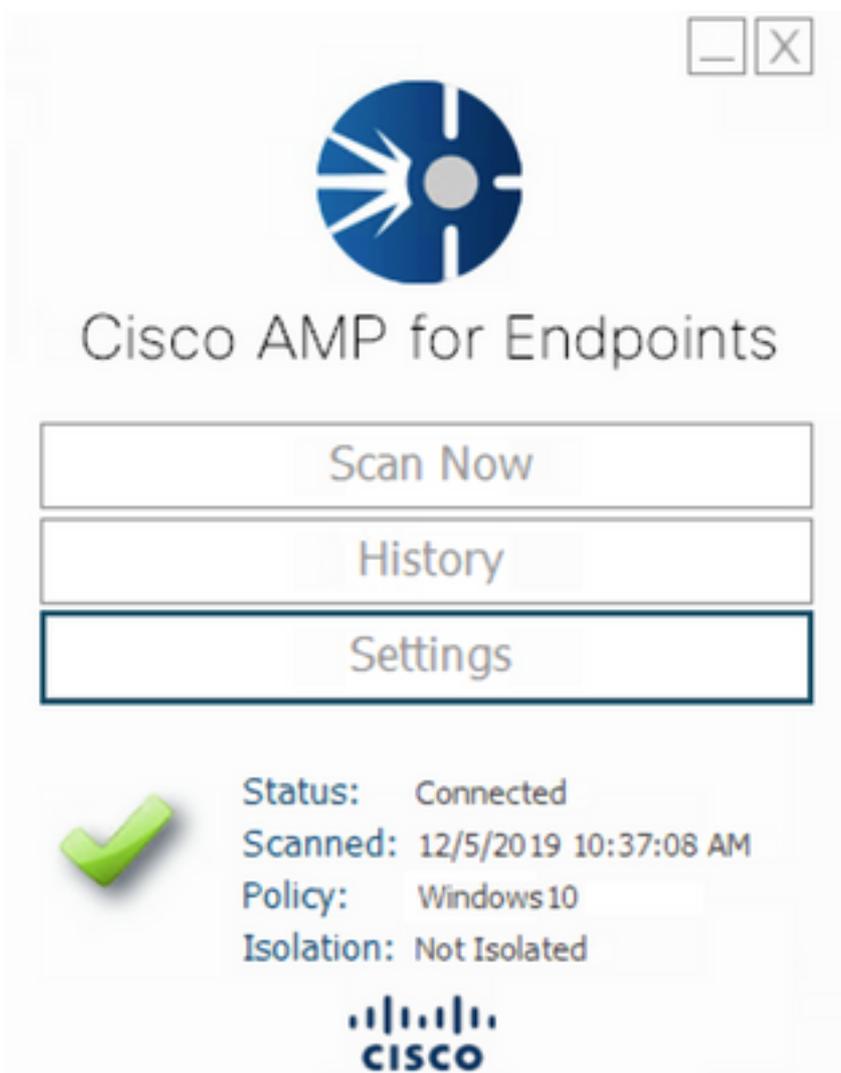


3단계. 이미지에 표시된 대로 Cisco AMP for Endpoints Connector 7.0.5 서비스를 시작합니다.

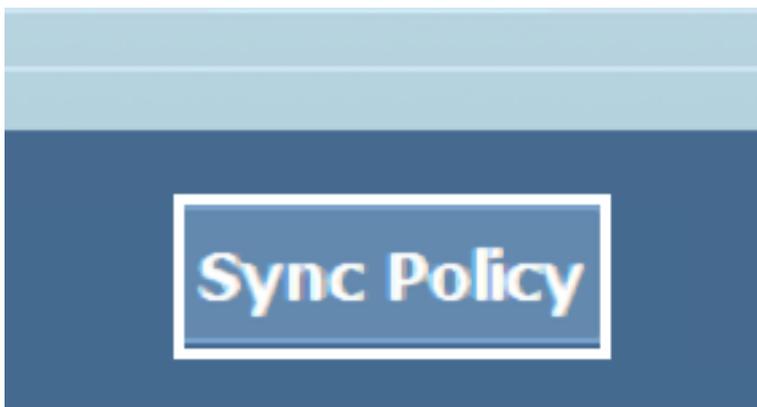


4단계. 이미지에 표시된 대로 AMP 사용자 인터페이스를 엽니다.

4.1단계. 이미지에 표시된 설정을 클릭합니다.



4.2단계. 이미지에 표시된 대로 동기화 정책을 선택합니다.



5단계. 라이선스가 동기화되면 Tetra 정의가 다운로드됩니다.

참고:정의를 다운로드하면 AMP 커넥터가 기본 AV가 됩니다(이미지에 표시됨).

Virus & threat protection

Protection for your device against threats.

Cisco AMP for Endpoints

Cisco AMP for Endpoints is turned on.

Current threats

 No actions needed.

Protection settings

 No actions needed.

Protection updates

 No actions needed.

[Open app](#)

TETRA 정의가 자동으로 다운로드되더라도 수동으로 정의 업데이트를 강제 적용할 수 있습니다. 고객의 요구 사항에 따라 달라집니다.

관련 정보

- [AMP4E - TETRA 정의 업데이트 비디오](#)
- [기술 지원 및 문서 - Cisco Systems](#)