복구 방법을 사용하여 격리된 보안 엔드포인트 문제 해결

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[격리 중지](#)
[콘솔에서 격리 세션 중지](#)
[명령줄에서 격리 세션 중지](#)
[복구 문제 해결](#)
[Mac 복구:](#)
[Windows 복구:](#)
[명령줄에서 복구 격리 방법](#)
[명령줄을 사용하지 않는 복구 격리 방법](#)
[다음을 확인합니다.](#)
[관련 정보](#)

소개

이 문서에서는 격리 모드에서 설치된 보안 엔드포인트 커넥터를 사용하여 엔드포인트를 복구하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 엔드포인트 커넥터
- 보안 엔드포인트 콘솔
- 엔드포인트 격리 기능

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Secure Endpoint 콘솔 버전 v5.4.2021092321
- Secure Endpoint Windows 커넥터 버전 v7.4.5.20701
- Secure Endpoint Mac 연결 버전 v1.21.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에 설명된 절차는 엔드포인트 디바이스가 이 상태에서 중단되고 격리 모드를 비활성화할 수 없는 경우에 유용합니다.

엔드포인트 격리는 데이터 유출 및 악성코드 전파와 같은 위협을 방지하기 위해 컴퓨터에서 네트워크 활동(수신 및 발신)을 차단할 수 있는 기능입니다. 사용 가능한 위치:

- Windows 커넥터 버전 7.0.5 이상을 지원하는 Windows 64비트 버전
- Mac 커넥터 버전 1.21.0 이상을 지원하는 Mac 버전.

엔드포인트 격리 세션은 커넥터와 Cisco 클라우드 간의 통신에 영향을 미치지 않습니다. 엔드포인트에는 세션 전과 동일한 수준의 보호 및 가시성이 있습니다. 활성 엔드포인트 격리 세션이 활성 상태일 때 커넥터가 문제의 IP 주소를 차단하지 않도록 하려면 IP 격리 허용 주소 목록을 구성할 수 있습니다. 여기서 엔드포인트 격리 기능에 대한 자세한 정보를 검토할 수 있습니다.

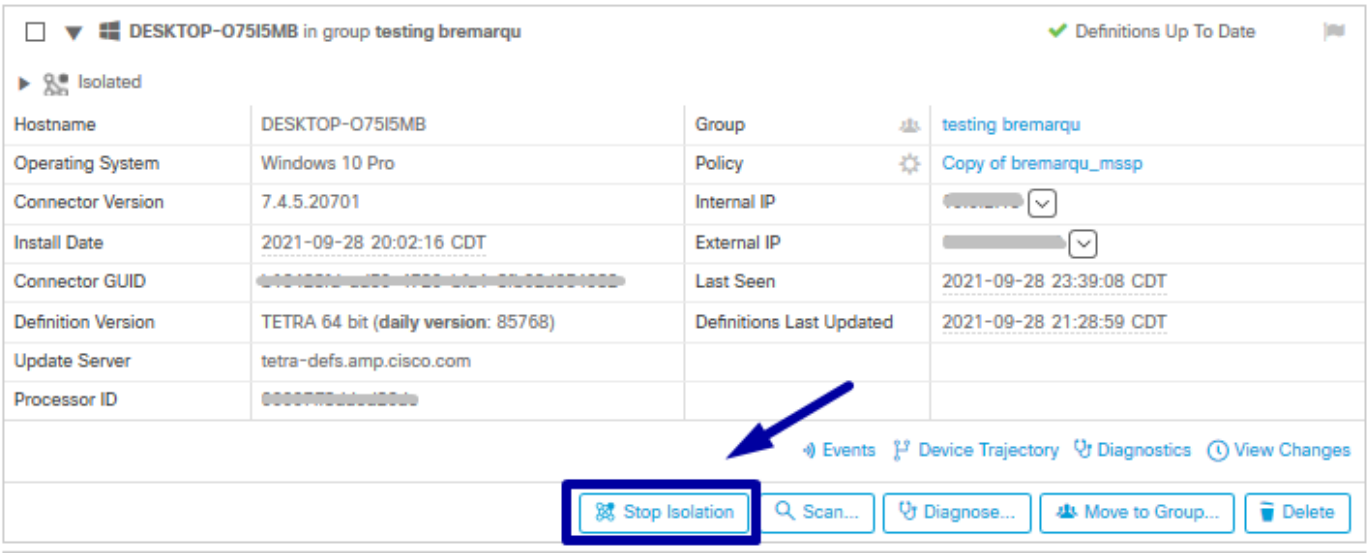
격리 중지

컴퓨터에서 엔드포인트 격리를 중지하려면 보안 엔드포인트 콘솔 또는 명령줄을 통해 이러한 빠른 단계를 수행하십시오.

콘솔에서 격리 세션 중지

격리 세션을 중지하고 모든 네트워크 트래픽을 엔드포인트로 복원하려면

1단계. 콘솔에서 **Management > Computers**로 **이동합니다**.
2단계. 격리를 중지할 컴퓨터를 찾고 을 클릭하여 세부 정보를 표시합니다.
3단계. 그림과 같이 **Stop Isolation**(격리 중지) 버튼을 클릭합니다.



4단계. 엔드포인트에서 격리 기능을 중지한 이유에 대한 설명을 입력합니다.

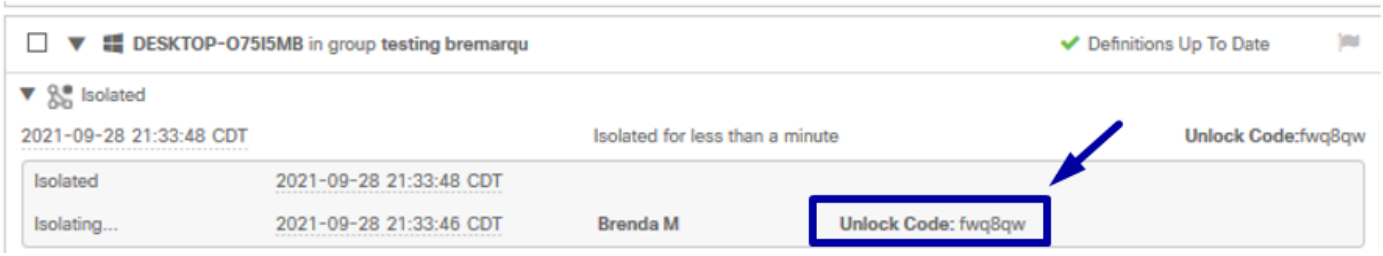
명령줄에서 격리 세션 중지

격리된 엔드포인트가 Cisco 클라우드와의 연결이 끊어진 경우 콘솔에서 격리 세션을 중지할 수 없습니다. 이러한 경우 잠금 해제 코드를 사용하여 명령줄에서 로컬로 세션을 중지할 수 있습니다.

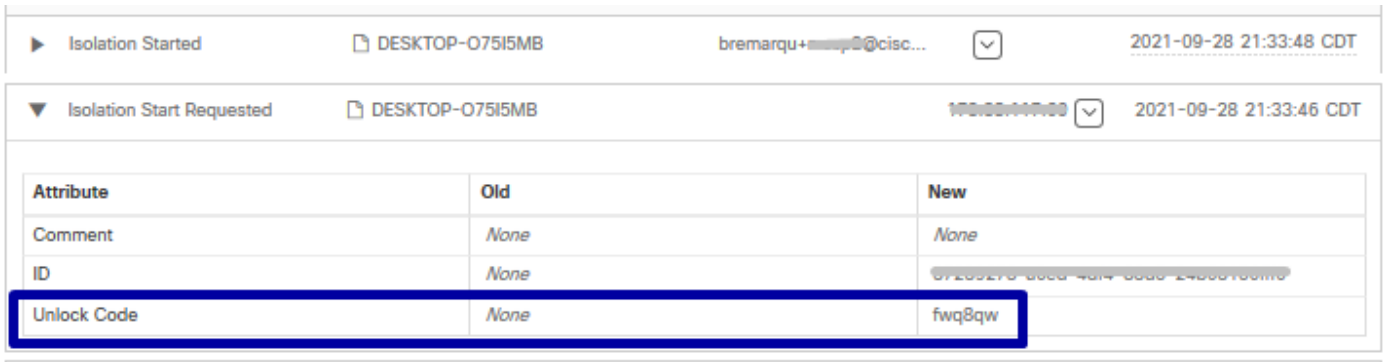
1단계. 콘솔에서 **Management > Computers**로 **이동합니다**.

2단계. 격리를 중지할 컴퓨터를 찾고 을 클릭하여 세부 정보를 표시합니다.

3단계. 그림과 같이 **잠금** 해제 코드를 확인합니다.



4단계. 그림과 같이 **Account(계정) > Audit Log(감사 로그)**로 이동하면 **Unlock Code(코드 잠금 해제)**를 찾을 수도 있습니다.



5단계. 격리된 컴퓨터에서 관리자 권한이 있는 명령 프롬프트를 엽니다.

6단계. 커넥터가 설치된 디렉토리로 이동합니다

Windows: C:\Program Files\Cisco\AMP\[버전 번호]

Mac: /opt/cisco/amp

7단계. stop 명령을 실행합니다.

```
Windows: sfc.exe -n [unlock code]
```

```
C:\Program Files\Cisco\AMP\7.4.5.20701>sfc.exe -n fwq8qw

C:\Program Files\Cisco\AMP\7.4.5.20701>
```

```
Mac: ampcli isolate stop [unlock code]
```

주의: 잠금 해제 코드를 5번 잘못 입력한 경우 다시 잠금 해제를 시도하기 전에 30분 정도 기

다려야 합니다.

복구 문제 해결

모든 경로를 다 소모한 경우에도 Secure Endpoint 콘솔에서 또는 잠금 해제 코드를 사용하여 로컬에서 격리된 엔드포인트를 복구할 수 없는 경우, 긴급 복구 방법을 사용하여 격리된 엔드포인트를 복구할 수 있습니다.

Mac 복구:

격리 컨피그레이션을 제거하고 보안 엔드포인트 서비스를 다시 시작합니다

```
sudo rm /Library/Application\ Support/Cisco/Secure\ Endpoint/endpoint_isolation.xml
sudo launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist
sudo launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist
```

Windows 복구:

명령줄에서 복구 격리 방법

엔드포인트 디바이스가 격리되어 있고 Secure Endpoint 콘솔 또는 잠금 해제 코드를 통해 격리를 비활성화할 수 없는 경우 다음 단계를 수행합니다.

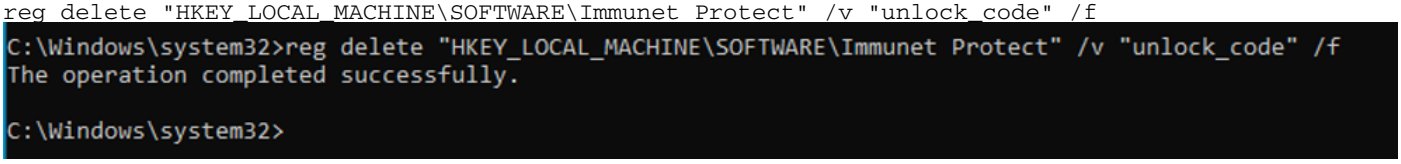
1단계. 커넥터 사용자 인터페이스 또는 **Windows** 서비스를 통해 커넥터 서비스를 **중지합니다**.

2단계. 보안 엔드포인트 커넥터 서비스를 찾아 서비스를 중지합니다.

3단계. 격리된 컴퓨터에서 관리자 권한이 있는 명령 프롬프트를 엽니다.

4단계. 이미지에 표시된 대로 **reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f** 명령을 실행합니다.

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
```



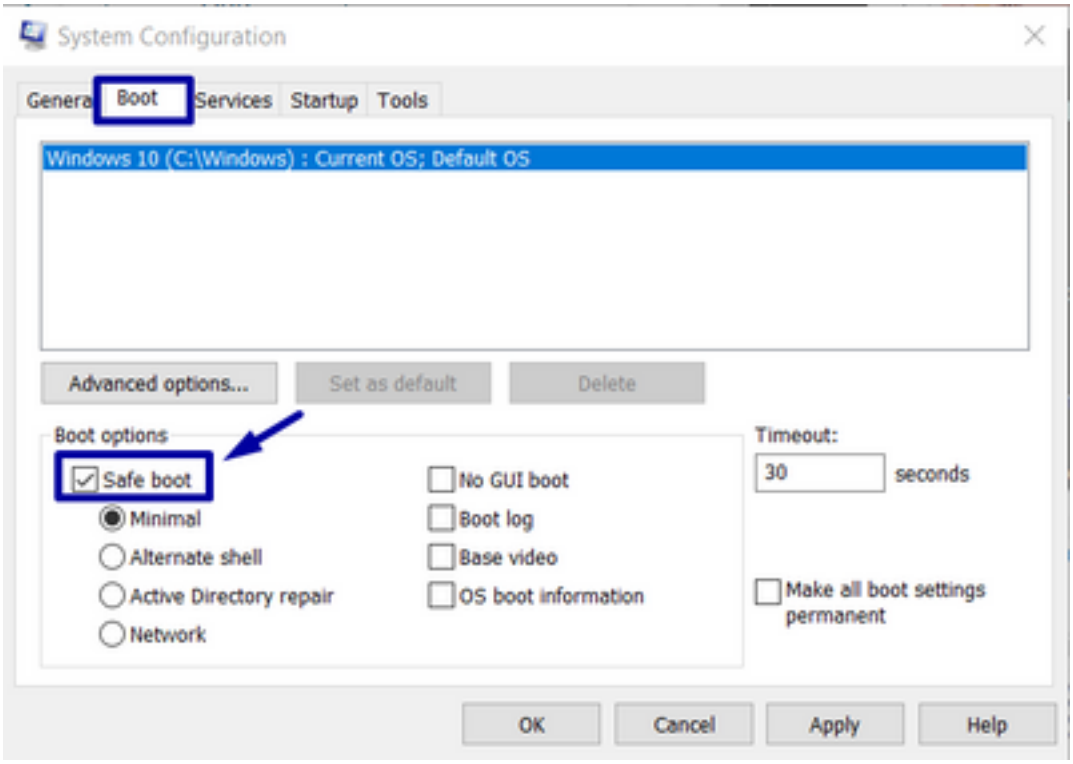
5단계. The operation **completed successfully(작업이 성공적**으로 완료됨) 메시지는 작업이 완료되었음을 나타냅니다. (다른 메시지가 "오류: 액세스가 거부되었습니다."와 같이 표시되면 명령을 실행하기 전에 보안 엔드포인트 커넥터 서비스를 중지해야 합니다.)

6단계. 보안 엔드포인트 커넥터 서비스를 시작합니다.

> **팁**: 커넥터 사용자 인터페이스 또는 Windows 서비스에서 보안 엔드포인트 커넥터 서비스를 중지할 수 없는 경우 안전 부팅을 수행할 수 있습니다.

격리된 엔드포인트에서 이미지에 표시된 대로 **System Configuration(시스템 컨피그레이션) >**

Boot(부팅) > Boot options(부팅 옵션)로 이동하고 **Safe boot(안전 부팅)**를 선택합니다.

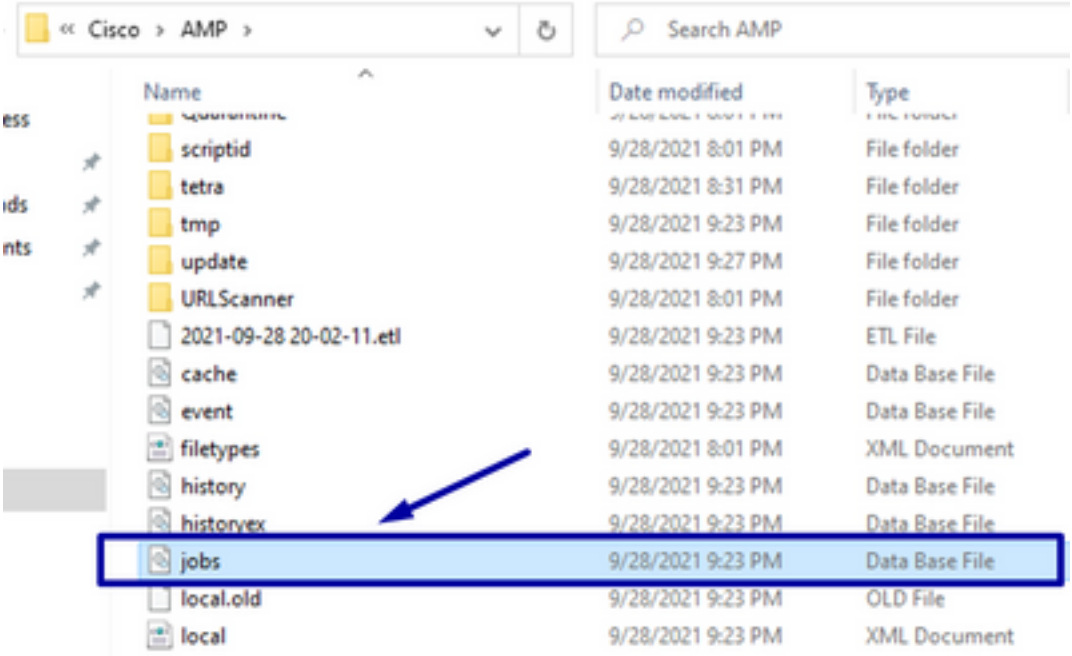


명령줄을 사용하지 않는 복구 격리 방법

엔드포인트 디바이스가 격리 상태에서 고정되며 Secure Endpoint 콘솔 또는 잠금 해제 코드를 통해 격리를 비활성화할 수 없거나 명령줄을 사용할 수 없는 경우에도 다음 단계를 수행하십시오.

1단계. 커넥터 사용자 인터페이스 또는 **Windows** 서비스를 통해 커넥터 서비스를 **중지합니다**.

2단계. 이미지에 표시된 대로 커넥터가 설치된 디렉토리(C:\Program Files\Cisco\AMP\)로 이동하고 **jobs.db** 파일을 삭제합니다.



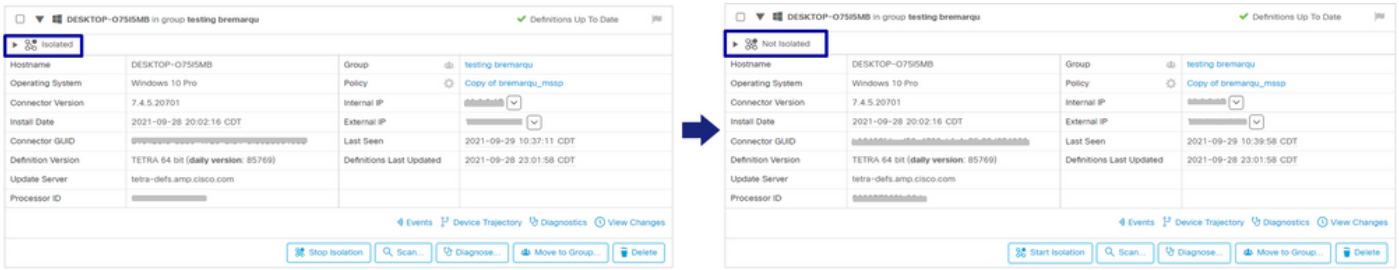
3. 컴퓨터를 재부팅합니다.

또한 콘솔에 Isolation(격리) 이벤트가 표시되는 경우 이미지에 표시된 대로 **오류 코드**와 해당 설명을 검토하기 위해 Error Details(오류 세부사항)로 이동할 수 있습니다.

다음을 확인합니다.

엔드포인트가 격리에서 돌아왔거나 더 이상 격리되지 않았는지 확인하기 위해 이미지에 표시된 것처럼 보안 엔드포인트 커넥터 사용자 인터페이스에 격리 상태가 **Not Isolated**(격리되지 않음)로 표시되는 것을 볼 수 있습니다.

Secure Endpoint(보안 엔드포인트) 콘솔에서 **Management(관리) > Computers(컴퓨터)**로 이동하고 문제의 컴퓨터를 찾은 경우 를 클릭하여 세부 정보를 표시할 수 있습니다. 그림과 같이 Isolation(격리) **상태**는 Not Isolated(격리되지 않음)로 표시됩니다.



관련 정보

- 보안 엔드포인트 사용 설명서
- 기술 지원 및 문서 – Cisco Systems

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.