

Cisco Secure Endpoint 명령줄 스위치

목차

[소개](#)

[배경 정보](#)

[Cisco Secure Endpoint 명령줄 스위치](#)

[보안 엔드포인트 설치 프로그램 스위치](#)

[amp_installer.exe](#)

[Secure Endpoint Support 진단 툴 스위치](#)

[ipsupporttool.exe](#)

[보안 엔드포인트 UI 스위치](#)

[iptraytool.exe](#)

[보안 엔드포인트 SFC 스위치](#)

[sfc.exe](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Secure Endpoint와 함께 사용할 수 있는 CLI(Command Line) 스위치에 대해 설명합니다.

배경 정보

Cisco Secure Endpoint에는 명령줄 스위치를 사용하여 엔드포인트에서 로컬로 수행할 수 있는 많은 사용자 지정 가능한 기능과 작업이 포함되어 있습니다. 이 문서에는 이러한 내용이 표시됩니다.

Cisco Secure Endpoint 명령줄 스위치

보안 엔드포인트 설치 프로그램 스위치

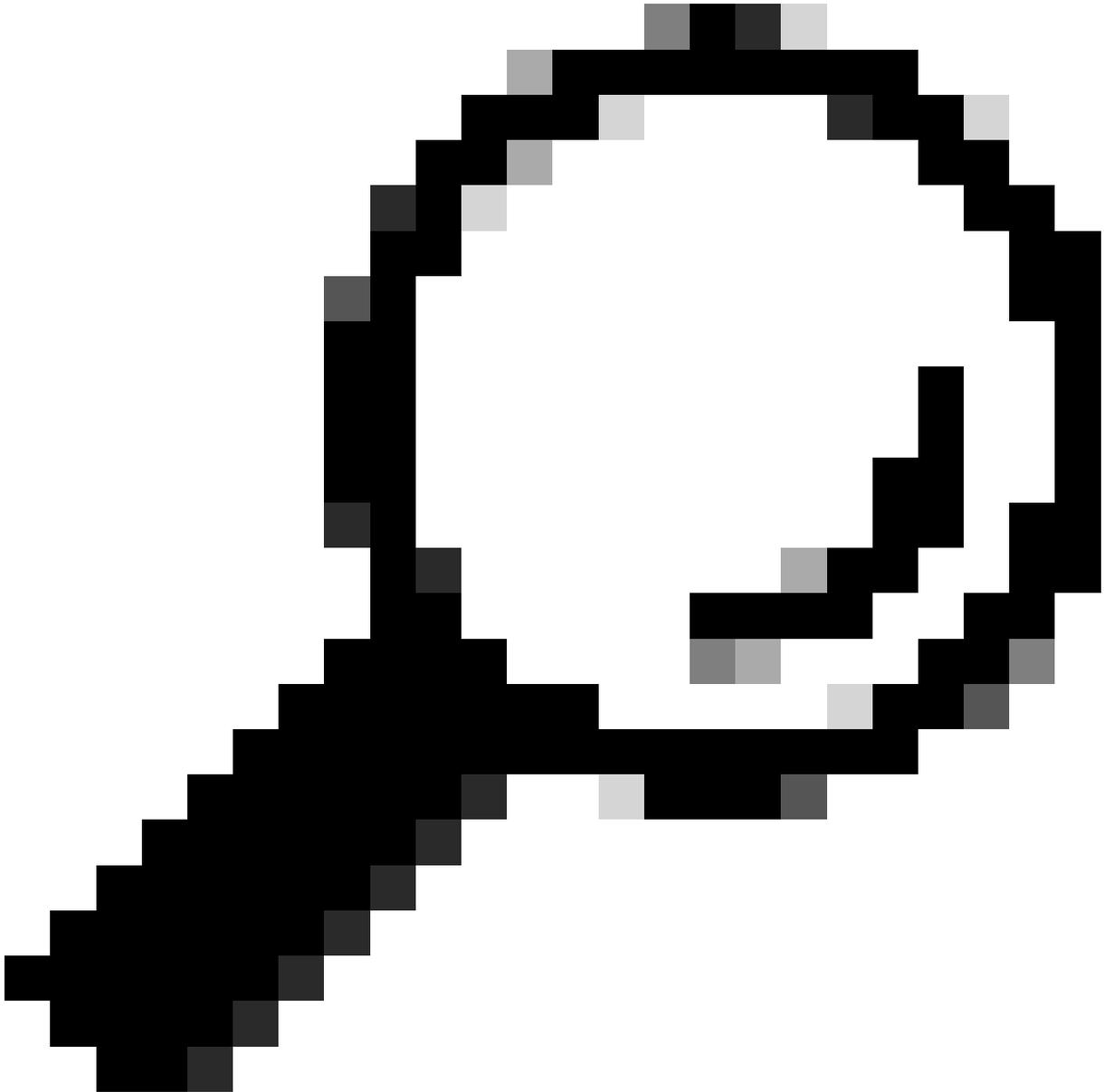
amp_installer.exe

1. Windows에서 명령 프롬프트를 엽니다.
2. 설치 관리자가 위치한 폴더(아래 예제로 사용되는 다운로드 폴더)를 명령 프롬프트에서 찾습니다.

```
cd C:\Users\sysadmin\Downloads
```

- 제공된 사용 가능한 스위치를 실행합니다.
amp_protect.exe <switch>

 참고: 명령을 실행한 후에는 출력이 반환되지 않습니다.



팁: 한 번에 둘 이상의 스위치를 사용할 수 있습니다.

명령줄 스위치	명령 설명	특별 참고 사항
/S	설치 프로그	

	램을 자동 모드로 설정하는 데 사용됩니다.	
/temppath	추출 및 실행할 설치 파일의 사용자 지정 임시 위치를 지정하는 데 사용됩니다.	/temppath C:\
/desktopicon 0	바탕 화면 아이콘이 생성되지 않도록 지정하는 데 사용됩니다.	이는 기본 컨피그레이션이므로 제공할 필요가 없습니다.
/desktopicon 1	바탕 화면 아이콘을 만들도록 지정하는 데 사용됩니다.	
/startmenu 0	시작 메뉴 바로 가기가 생성되지 않습니다.	
/startmenu 1	시작 메뉴 바로 가기가 생성됩니다.	이는 기본 컨피그레이션이므로 제공할 필요가 없습니다.
/contextmenu 0	마우스 오른쪽 버튼 클릭 컨텍스트 메뉴에서 Scan Now(지금 스캔)를 비활성화합니다.	

/contextmenu 1	오른쪽 클릭 컨텍스트 메뉴에서 Scan Now(지금 스캔)를 활성화합니다.	이는 기본 컨피그레이션이므로 제공할 필요가 없습니다.
/제거 0	커넥터를 제거하고 나중에 다시 설치할 수 있도록 파일을 남겨둡니다.	UUID가 있는 XML 파일은 남아 있으며 커넥터를 다시 설치할 때 기존 컴퓨터 개체를 다시 사용할 수 있습니다. 로그 파일도 보존됩니다. 커넥터 보호 암호를 사용 중인 경우 /uninstallpassword 플래그를 사용하여 지정해야 합니다.
/제거 1	커넥터를 제거하고 관련된 모든 파일을 제거합니다.	커넥터 보호 암호를 사용 중인 경우 /uninstallpassword 플래그를 사용하여 지정해야 합니다.
/uninstallpassword	/remove 플래그를 사용할 때 제거 암호를 지정합니다. 커넥터 보호 기능이 활성화된 경우 지정해야 합니다.	플래그 뒤에 제거 비밀번호를 지정합니다.
/skipdfc 1	DFC 드라이버 설치를 건너뛸니다.	이 플래그로 설치된 모든 커넥터는 네트워크 엔진이 비활성화된 정책이 있는 그룹에 있어야 합니다.
/스킵테트라 1	TETRA 드라이버 설치를 건너뛸니다.	이 플래그로 설치된 모든 커넥터는 Tetra 플래그가 선택되지 않은 정책이 있는 그룹에 있어야 합니다.
/D=[경로]	설치를 수행할 디렉토리를 지정하는데 사용됩니다.	이는 마지막 매개 변수로 지정해야 합니다. /D= 명령줄 스위치의 경우 기본 설치 디렉토리는 운영 체제마다 다릅니다. 다음은 Microsoft Windows XP 서비스 팩 3 이상의 기본

	다. 예: /D=C:\	설치 디렉토리입니다. x86 플랫폼의 경우: C:\Program Files (x86)\Cisco\AMP x64 플랫폼의 경우: C:\Program Files\Cisco\AMP
/goldenimage 1	골든 이미지 준비를 위한 커넥터 설치	이 플래그는 가상 환경에서 골든 이미지를 준비하는 데 도움이 되도록 설계되었습니다. 이 플래그를 사용하면 골든 이미지 생성 중에 커넥터가 시작되어 등록되지 않습니다. 자세한 내용은 다음을 참조하십시오. 안전한 엔드포인트로 최상의 이미지를 준비하는 방법 https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html
/스키포체크 1	설치하는 동안 OS 검사를 건너뛵니다.	이 플래그는 호환되지 않는 운영 체제에 Secure Endpoint를 설치하는 데 사용할 수 있습니다.

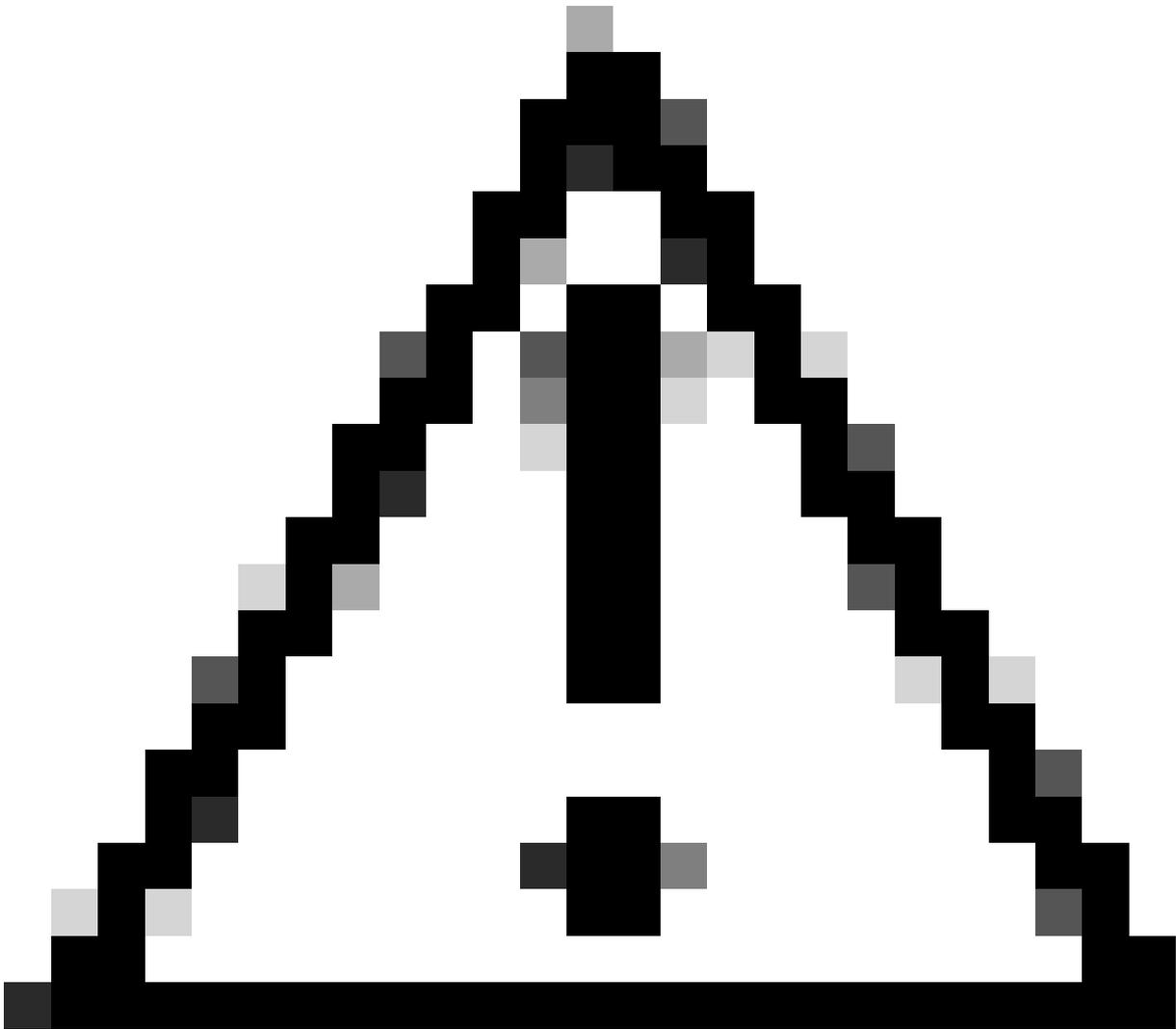
Secure Endpoint Support 진단 툴 스위치

ipsupporttool.exe

- Windows에서 명령 프롬프트를 엽니다.
- 명령 프롬프트에서 폴더로 이동합니다. 기본 경로: **C:\Program Files\Cisco\AMP\X.X.X**, theX.X.X는 버전 번호를 나타냅니다.
cd C:\Program Files\Cisco\AMP\8.2.1.21612\
- 제공된 사용 가능한 스위치를 실행합니다.
ipsupporttool.exe <switch>



참고: 스위치를 실행하면 출력이 반환되지 않습니다.



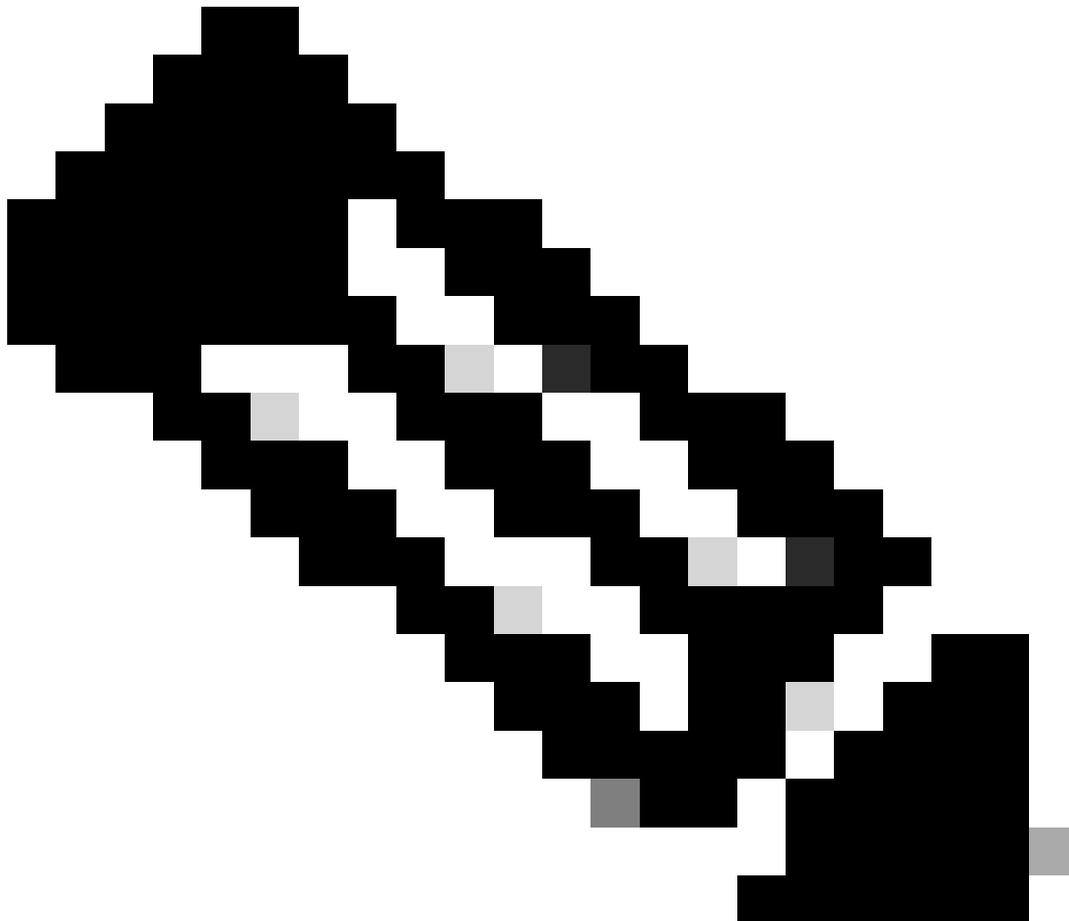
주의: 폴더 선택을 참조하는 모든 스위치에는 폴더가 이미 있어야 합니다

명령줄 스위치	명령 설명	특별 참고 사항
-o <경로>	지원 도구의 출력 폴더를 지정합니다.	이 옵션을 지정하지 않으면 기본적으로 바탕 화면이 표시됩니다.
-d <install_path>	Windows 지원 도구에서	지정하지 않은 경우 보안 엔드포인트의 기본 설치

	파일을 검색할 수 있는 폴더를 지정합니다.	디렉토리가 기본값으로 사용됩니다.
-t <분>	지정된 시간 동안 Windows 지원 도구에서 시간 제한 디버그 수준 진단을 실행합니다. 기간은 분 단위로 지정됩니다.	

보안 엔드포인트 UI 스위치

iptraytool.exe



참고: iptraytool.exe는 보안 엔드포인트의 레거시 버전에서만 사용할 수 있습니다.

- Windows에서 명령 프롬프트를 엽니다.
- 명령 프롬프트에서 폴더로 이동합니다. 기본 경로: C:\Program Files\Cisco\AMP\X.X.X\, theX.X.X는 버전 번호를 나타냅니다.
cd C:\Program Files\Cisco\AMP\7.5.3.20938\
- 제공된 사용 가능한 스위치를 실행합니다.
iptray.exe <switch>

명령줄 스위치	명령 설명	특별 참고 사항
-f	명령줄에서 클라이언트 사용자 인터페이스를 활성화할 수 있습니다.	이는 엔드포인트에서 Start Client User Interface(클라이언트 사용자 인터페이스 시작)가 선택되지 않은 정책을 통해 GUI가 꺼진 경우에만 필요합니다.

보안 엔드포인트 SFC 스위치

sfc.exe

- Windows에서 명령 프롬프트를 엽니다.
- 명령 프롬프트에서 폴더로 이동합니다. 기본 경로: C:\Program Files\Cisco\AMP\X.X.X\, theX.X.X는 버전 번호를 나타냅니다.
cd C:\Program Files\Cisco\AMP\8.2.1.21612\
- 제공된 사용 가능한 스위치를 실행합니다.
sfc.exe <switch>

명령줄 스위치	명령 설명	특별 참고 사항
-s	Immunet Protect(Windows Connector) 서비스를 시작합니다. 서비스를 시작하려면	

	SCM에 서비스가 이미 등록되어 있어야 합니다.	
-k	Immunet Protect(Windows 커넥터) 서비스를 중지합니다.	Connector Protection(커넥터 보호)이 활성화된 경우 서비스를 성공적으로 중지하려면 -k 뒤에 비밀번호를 입력합니다.
-u	Immunet Protect(Windows Connector) 서비스를 제거합니다. Windows SCM(서비스 제어 관리자)에서 서비스 등록 취소 이 옵션은 제거 프로그램에서 Windows 커넥터 서비스를 제거하는 데 사용됩니다.	
-r	Immunet Protect(Windows 커넥터) 서비스를 재설정합니다. 이 옵션은 -i 옵션과 매우 유사하지만 서비스를 설치하지 않습니다. 이것은 local.xml 손상을 해결하는 데 유용합니다.	
-i 시작	디버그 및 커널 로깅을 동적으로 토글합니다(트리거는 소문자 L).	이 상태는 전환되거나, 서비스가 다시 시작되거나, 로깅 수준을 변경하도록 새 정책이 구성될 때까지 유지됩니다.
-i 중지	디버그 및 커널 로깅을 동적으로 끕니다(트리거는 소문자 L).	
-unblock SHA_of_file	이 옵션은 프로세스의 실행을 차단합니다. 이 명령 스위치를 실행하면 애플리케이션 차단 목록의 로컬 커널 캐시에서 애플리케이션을 제거할 수 있습니다.	이 명령은 오탐 또는 실수로 인해 응용 프로그램이 차단되었을 때 사용할 수 있으며, 30분을 기다리거나 시스템을 재부팅하지 않고 응용 프로그램을 빠르게 차단해야 합니다.
-재등록	이 옵션은 서비스가 실행되는 동안 local.xml 및 레지스트리에서 uuid 및 certs를 지우고 재등록을 트리거할 수 있습니다. Local.xml 및 레지스트리가 새 값으로 업데이트됩니다. 그러나 ID 동기화가 활성화되어 있고 커넥터가 기존 UUID를 다시 가져오는 경우에는 차단됩니다. 초기 설치에 사용된 설치 패키지가 수정된 경	Connector Protection(Connector 보호)이 활성화된 경우 다음을 입력해야 합니다. sfc.exe -reregister _password_

	우 재등록 후 커넥터를 기본 그룹/정책에 배치할 수 있습니다.	
-forceupdate	이 옵션은 커넥터에서 TETRA 정의를 강제로 업데이트합니다.	

관련 정보

- [기술 지원 및 문서 - Cisco Systems](#)
- [Cisco 보안 엔드포인트 - TechNotes](#)
- [Cisco Secure Endpoint - 사용 설명서](#)
- [보안 엔드포인트 Mac/Linux CLI 사용](#)

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.