보안 엔드포인트 - Microsoft 공격 표면 감소로 인해 커넥터 업데이트가 차단됨

목차

소개

이 문서에서는 Microsoft Intune에서 관리되는 시스템에서 복사 또는 가장된 시스템 도구 기능을 사용하여 Microsoft Intune 공격 표면 감소 차단으로 인해 보안 끝점 업데이트가 실패하는 문제에 대해 설명합니다.

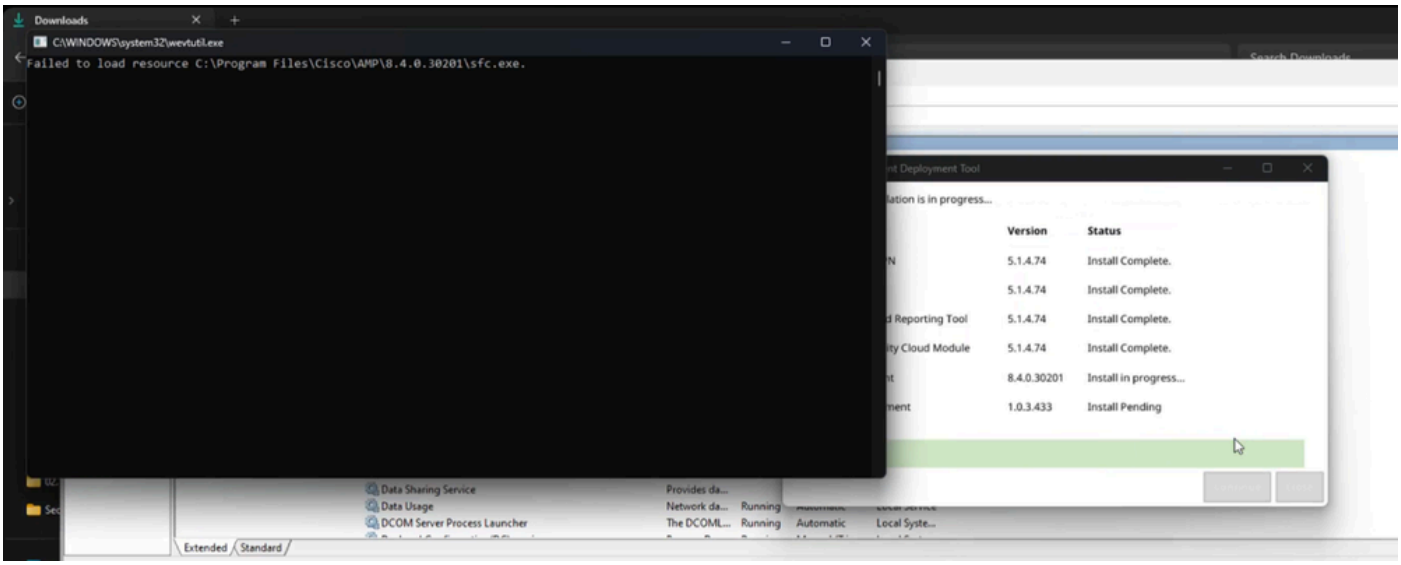
기능 설명서를 참조하십시오. https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

문제

이러한 오류 및 지표로 표시되는 보안 엔드포인트 업그레이드 또는 설치 문제가 발생할 수 있습니다.

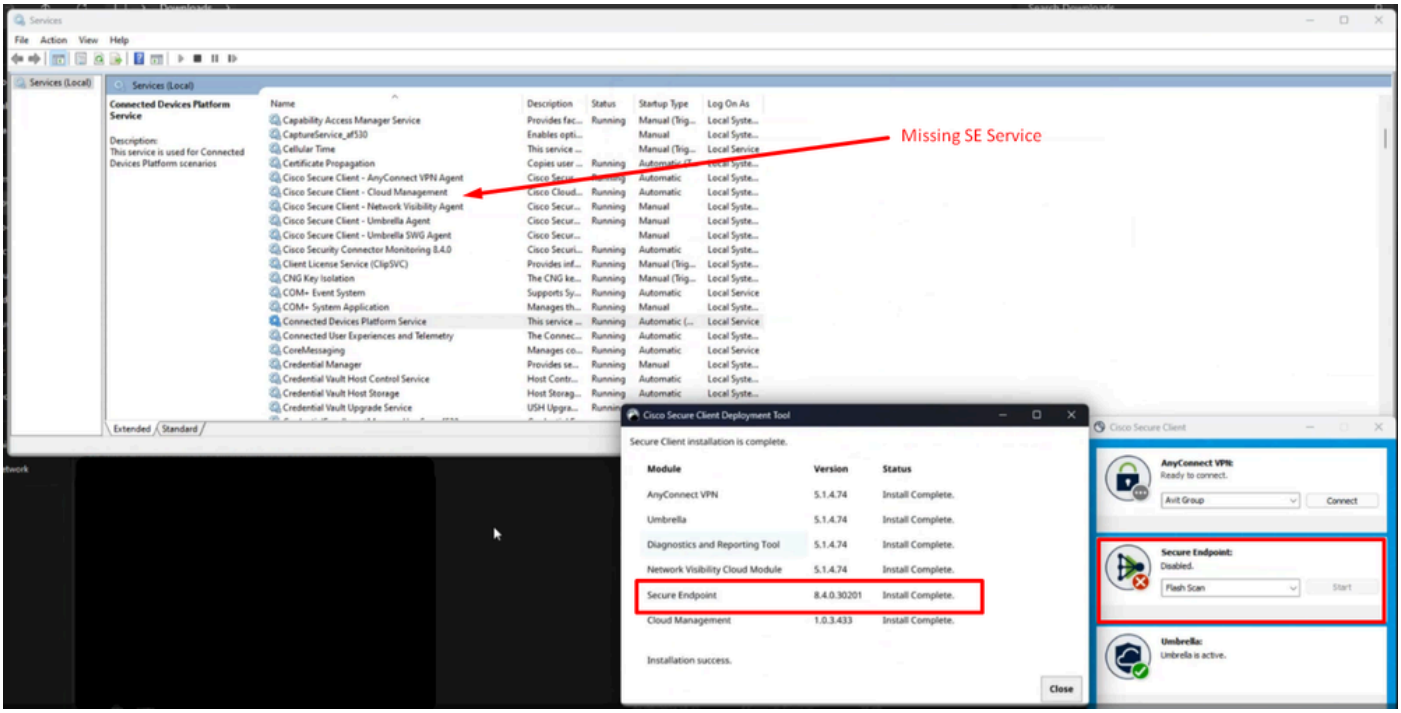
이 기능이 보안 엔드포인트 업데이트에 방해가 됨을 식별하는 데 사용할 수 있는 다양한 지표가 있습니다.

표시기 #1: 구축 중에 설치가 끝날 때 이 팝업 창이 나타납니다. 팝업은 매우 빠르며 설치가 완료된 후에는 다른 오류 회상이 없습니다.

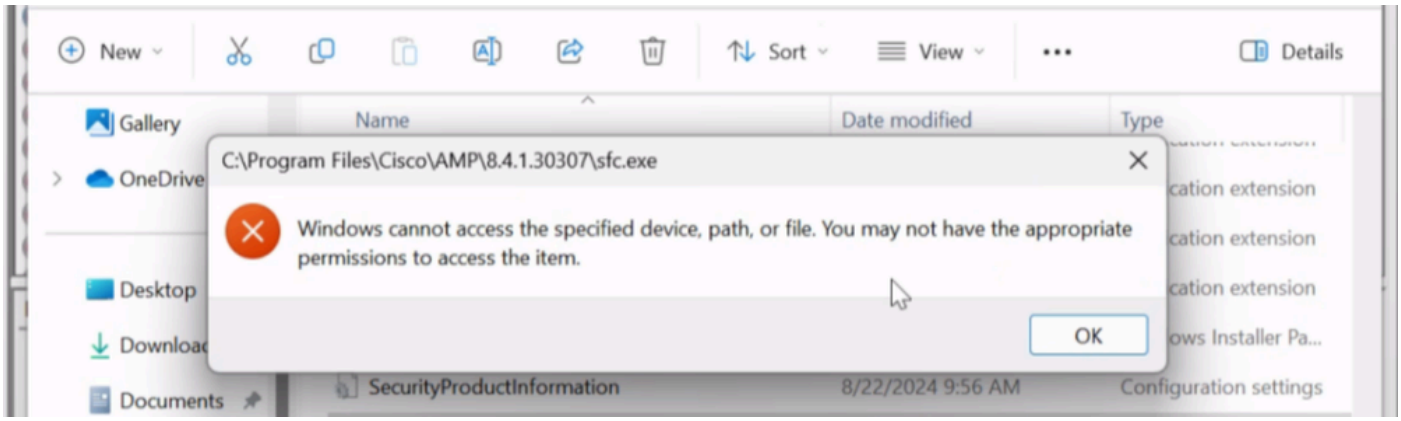


표시기 #2: 설치 후 보안 엔드포인트가 UI에서 비활성화 상태임을 확인합니다.

또한 작업 관리자 — > 서비스에서 sfc.exe(Secure Endpoint Service)가 완전히 누락되었습니다.



지표 #3: Cisco Secure Endpoint의 C:\Program Files\Cisco\AMP\ 버전 위치로 이동한 후 서비스를 수동으로 시작하려고 하면 로컬 관리자 계정에 대해서도 권한 액세스가 거부됩니다.



표시기 #4: 진단 번들의 일부인 immpro_install.log를 조사하면 이 출력과 유사하게 보이는 유사한 액세스 거부를 관찰할 수 있습니다.

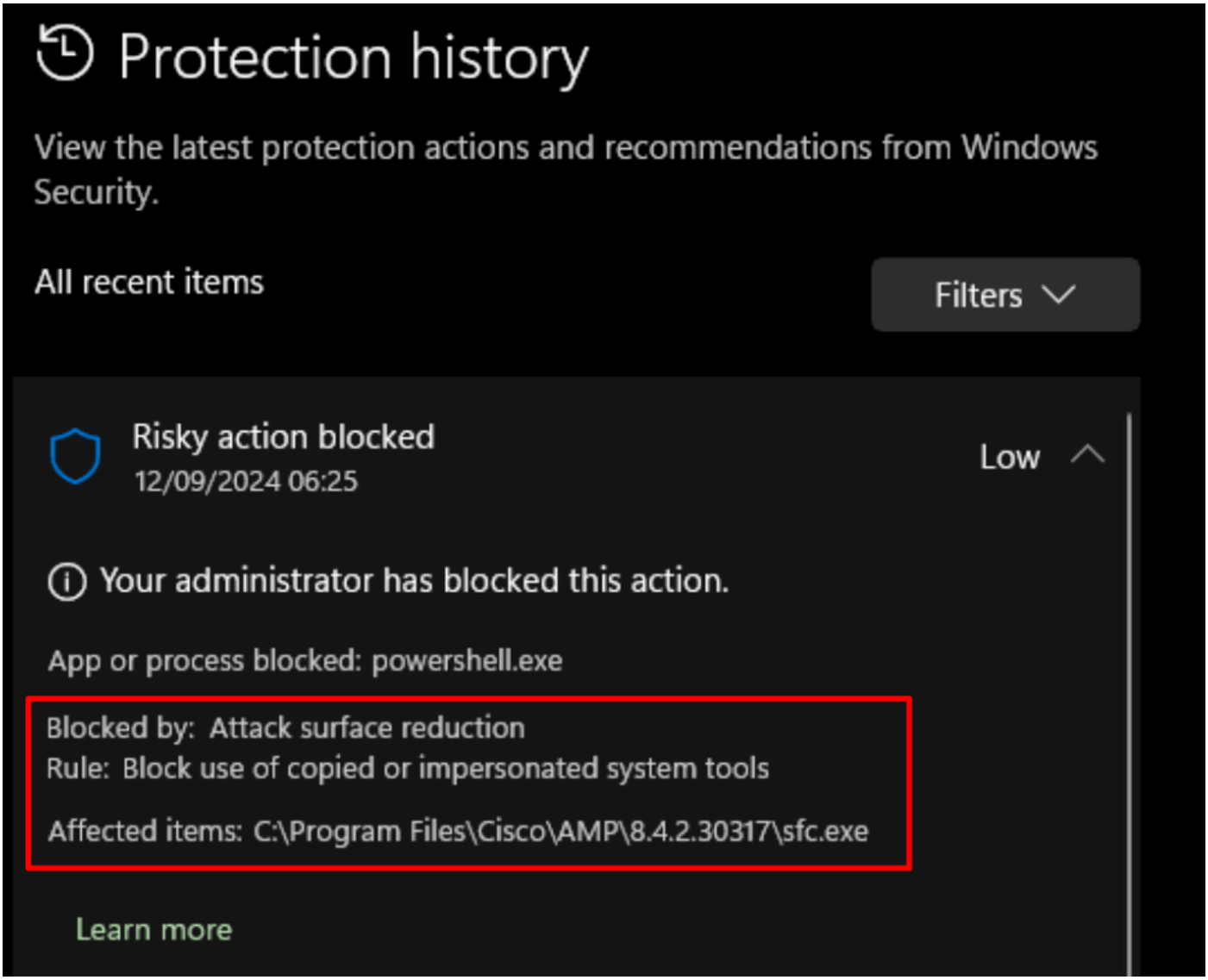
```
Example #1:
```

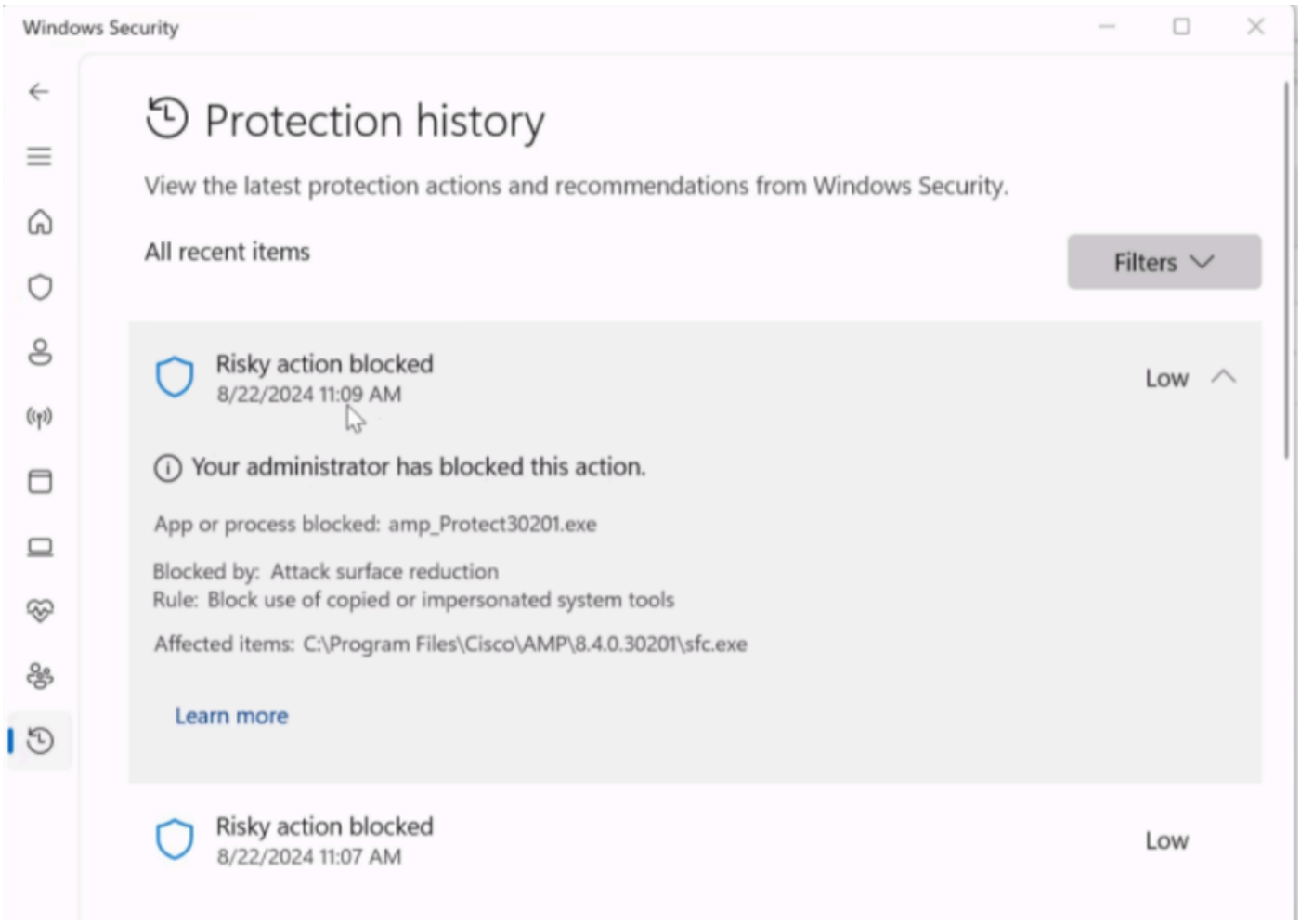
```
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\Pr
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\Ci
(5090625, +0 ms) Aug 22 09:56:33 [17732]: ERROR: VerifyAllInstalledFiles: Failed to verify $AMP_INSTALL
```

Example #2:

```
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: imn_error: fp_gen_internal: failed to open file C:\Pr
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: Util::GetFileSHA256: unable to generate file fp: C:\P
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyFile: Failed to grab hash of C:\Program Files\C
(1737859, +0 ms) Sept 11 14:04:05 [20180]: ERROR: VerifyAllInstalledFiles: Failed to verify $AMP_INSTAL
```

표시기 #5: Windows 보안 아래에서 탐색하고 보호 기록 로그를 보면 이러한 유형의 로그 메시지를 찾습니다.





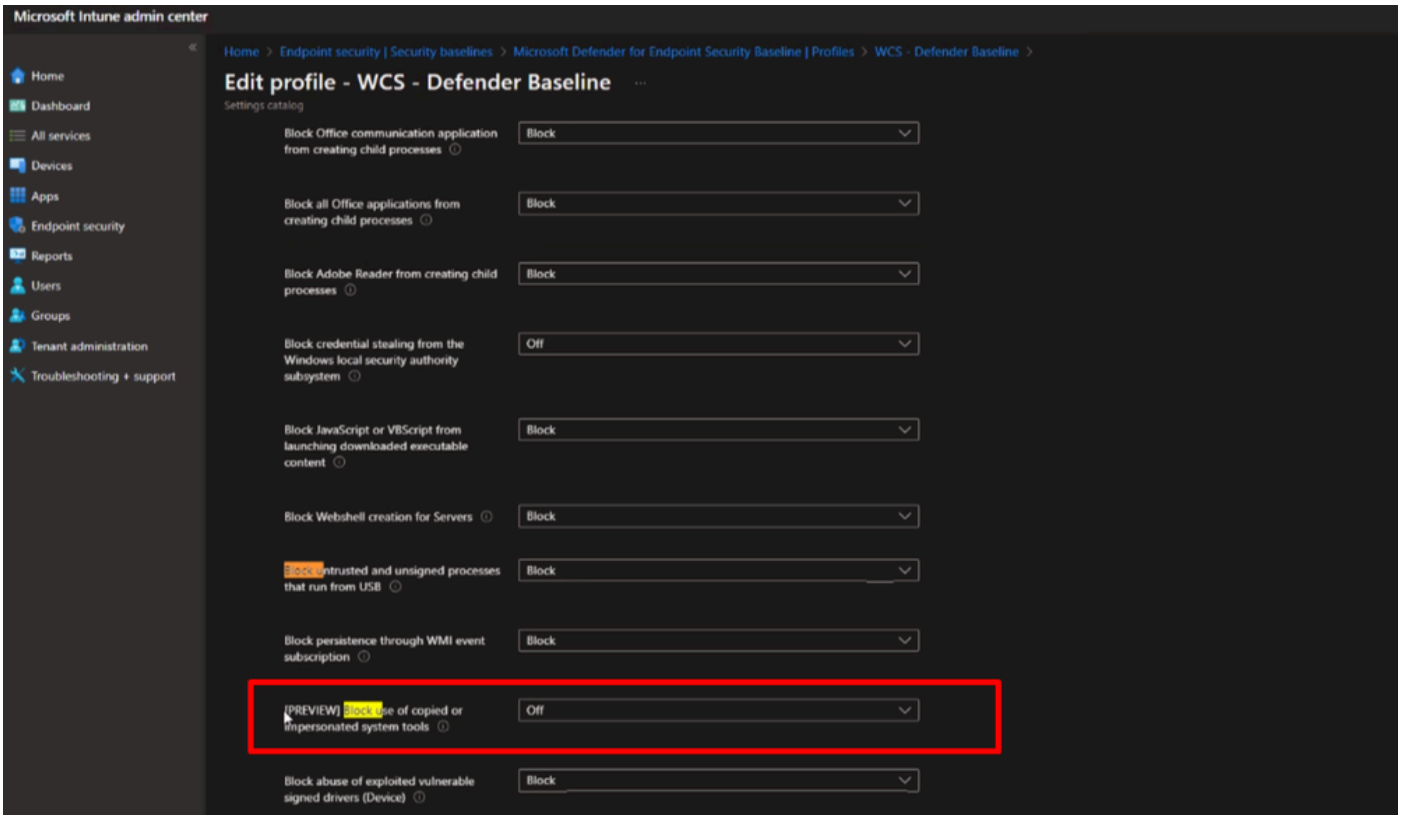
이러한 모든 사항은 보안 엔드포인트가 서드파티 애플리케이션에 의해 차단되고 있음을 나타냅니다. 이 시나리오에서는 Intune 관리 엔드포인트에서 잘못 구성되었거나 구성되지 않은 문제가 발생했습니다. 공격 표면 감소 - 복사되거나 가장된 시스템 기능의 사용을 차단합니다.

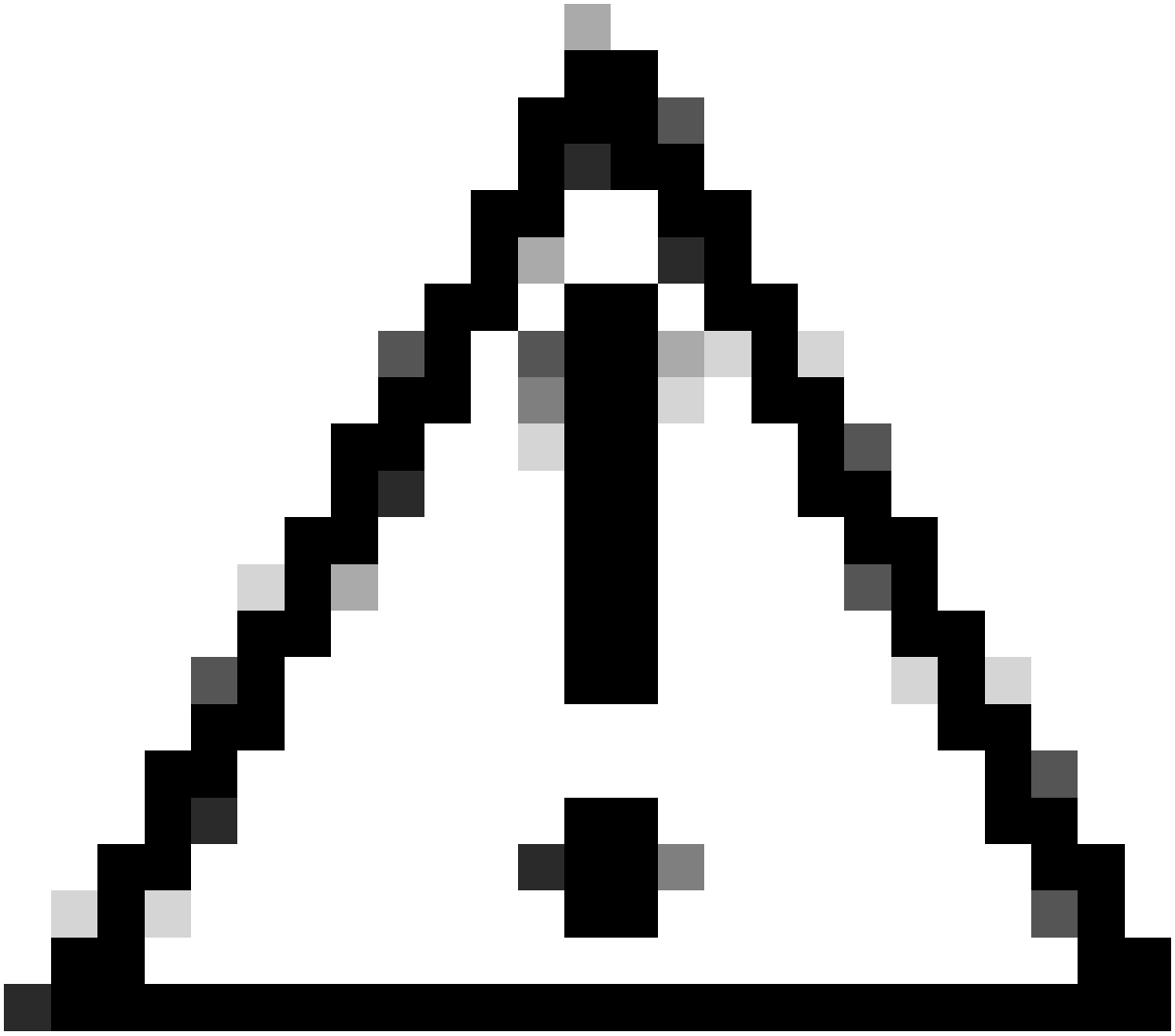
해결 방법

이 기능에 대한 컨피그레이션은 애플리케이션 개발자에게 문의하거나 이 지식 베이스를 통해 이 기능에 대해 자세히 참조하십시오.

즉각적인 교정을 위해 intune에서 관리되는 엔드포인트를 덜 제한적인 정책으로 이동하거나 적절한 단계가 만들어질 때까지 이 기능을 명시적으로 일시적으로 끌 수 있습니다.

보안 끝점 연결을 복원하기 위한 임시 측정값으로 사용된 Intune 관리 포털의 설정입니다.


Microsoft Intune admin center
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Endpoint security | Security baselines > Microsoft Defender for Endpoint Security Baseline | Profiles > WCS - Defender Baseline >
Edit profile - WCS - Defender Baseline
Settings catalog
Block Office communication application from creating child processes
Block
Block all Office applications from creating child processes
Block
Block Adobe Reader from creating child processes
Block
Block credential stealing from the Windows local security authority subsystem
Off
Block JavaScript or VBScript from launching downloaded executable content
Block
Block Webshell creation for Servers
Block
Block untrusted and unsigned processes that run from USB
Block
Block persistence through WMI event subscription
Block
(PREVIEW) Block use of copied or impersonated system tools
Off
Block abuse of exploited vulnerable signed drivers (Device)
Block



주의: 이 문제가 발생하면 sfc.exe가 없으므로 전체 설치를 시작해야 합니다.

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.