Secure Endpoint - Connectorupdates worden geblokkeerd vanwege Microsoft Attack-oppervlaktebeperking

Inhoud

Inleiding

In dit document worden problemen beschreven die worden veroorzaakt door oppervlakteverminderingsblokken van Microsoft Intune Attack met behulp van gekopieerde of nagemaakte systeemtools die voorkomen op systemen die worden beheerd door Microsoft Intune, die op zijn beurt ervoor zorgt dat Secure Endpoint updates mislukken.

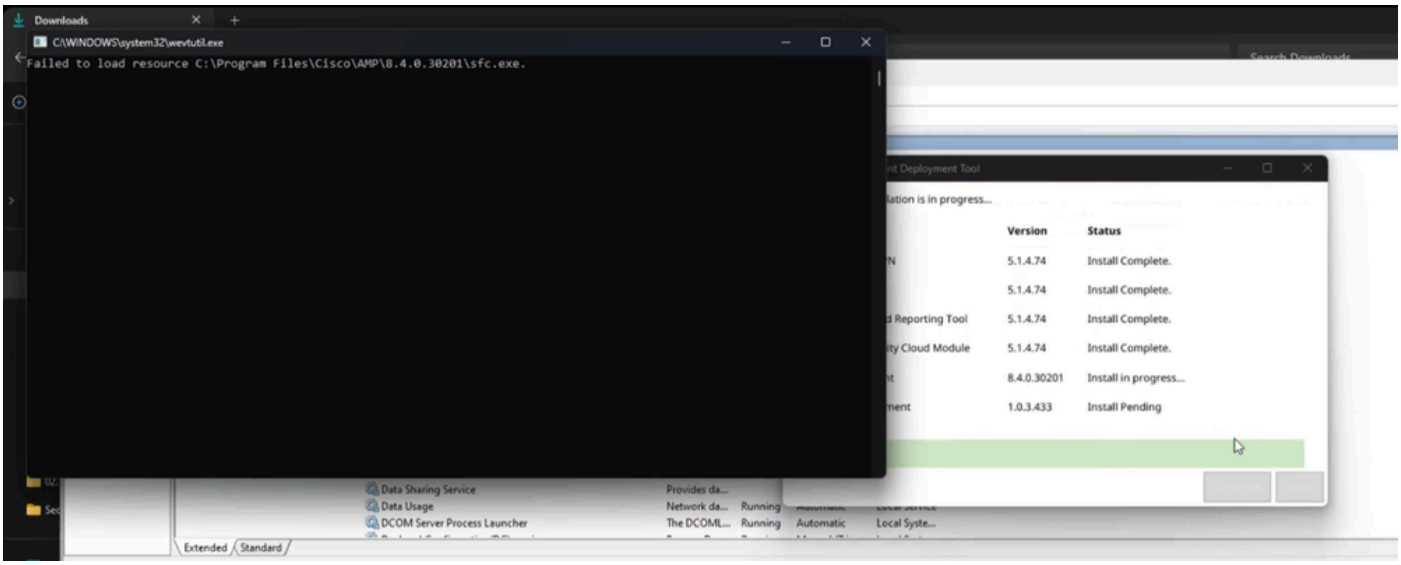
Raadpleeg de documentatie bij de functie: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

Probleem

We kunnen problemen ervaren met Secure Endpoint upgrades of installatie die wordt weergegeven door deze fouten en indicatoren.

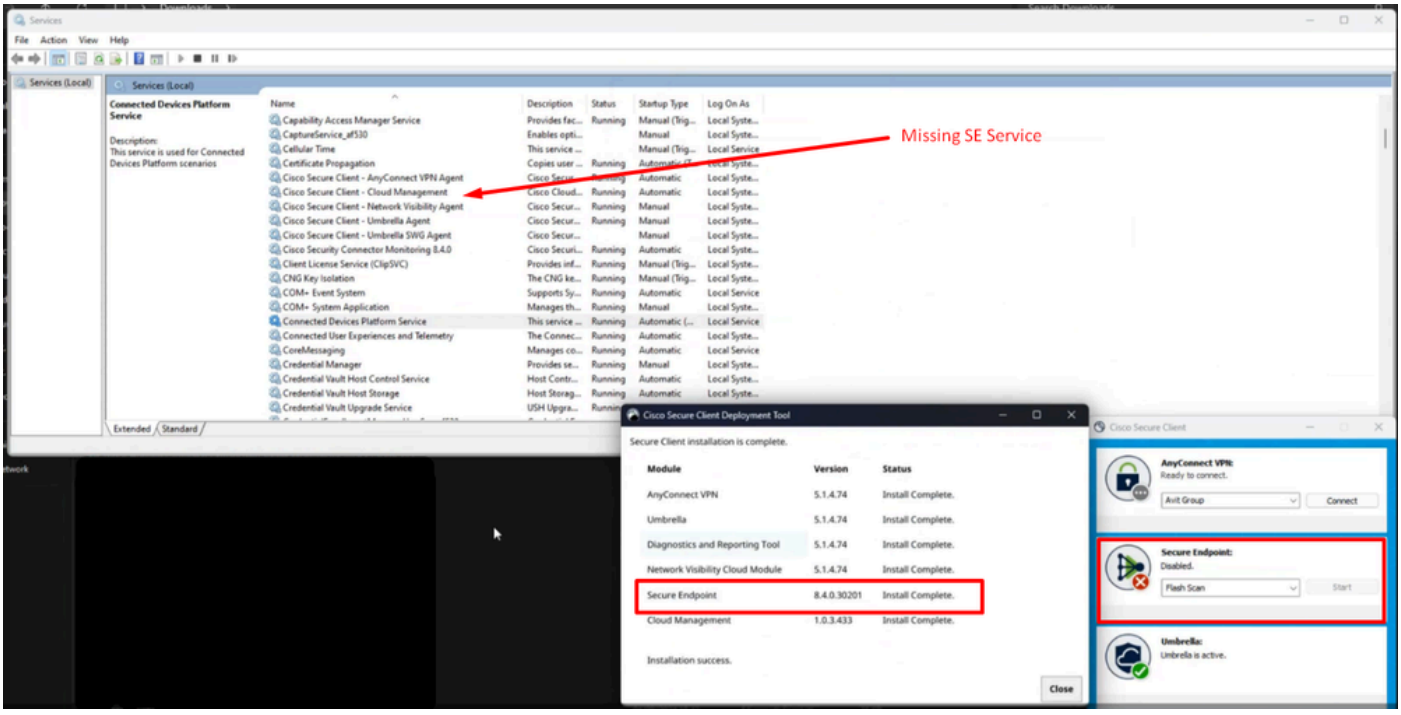
Er zijn verschillende indicatoren die kunnen worden gebruikt om aan te geven dat deze functie interfereert met Secure Endpoint updates.

Indicatielampje #1: tijdens de implementatie, zullen we dit pop-up venster aan het eind van de installatie opmerken. Houd er rekening mee dat het pop-upvenster tamelijk snel is en dat er na het voltooien van de installatie geen fouten meer worden herinnerd.

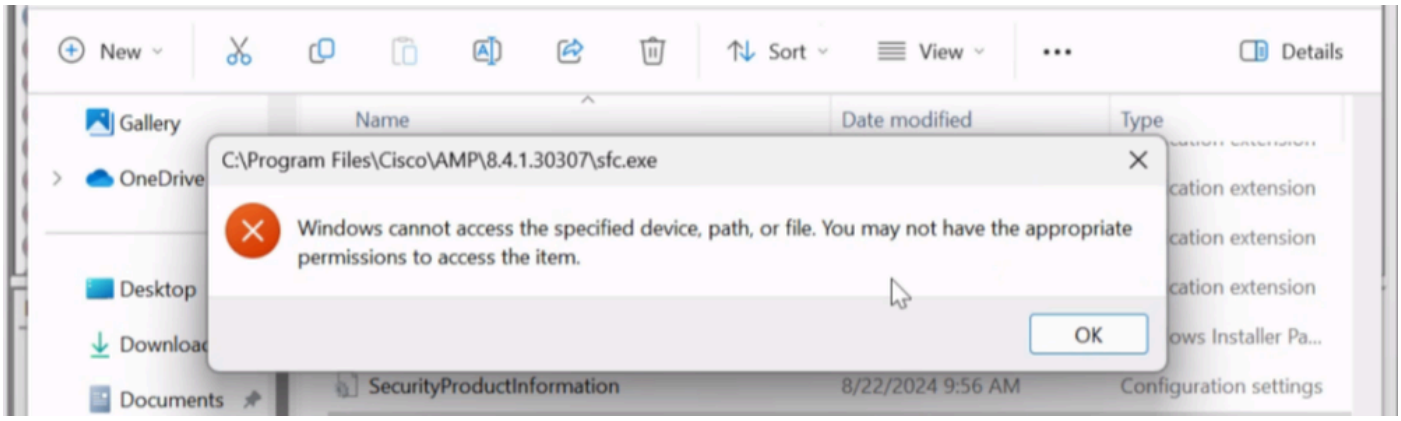


Indicatielampje #2: na de installatie, merk op dat Secure Endpoint in uitgeschakeld staat in de UI is.

Ook volledig ontbrekende Secure Endpoint Service (sfc.exe) in Taakbeheer — > Services



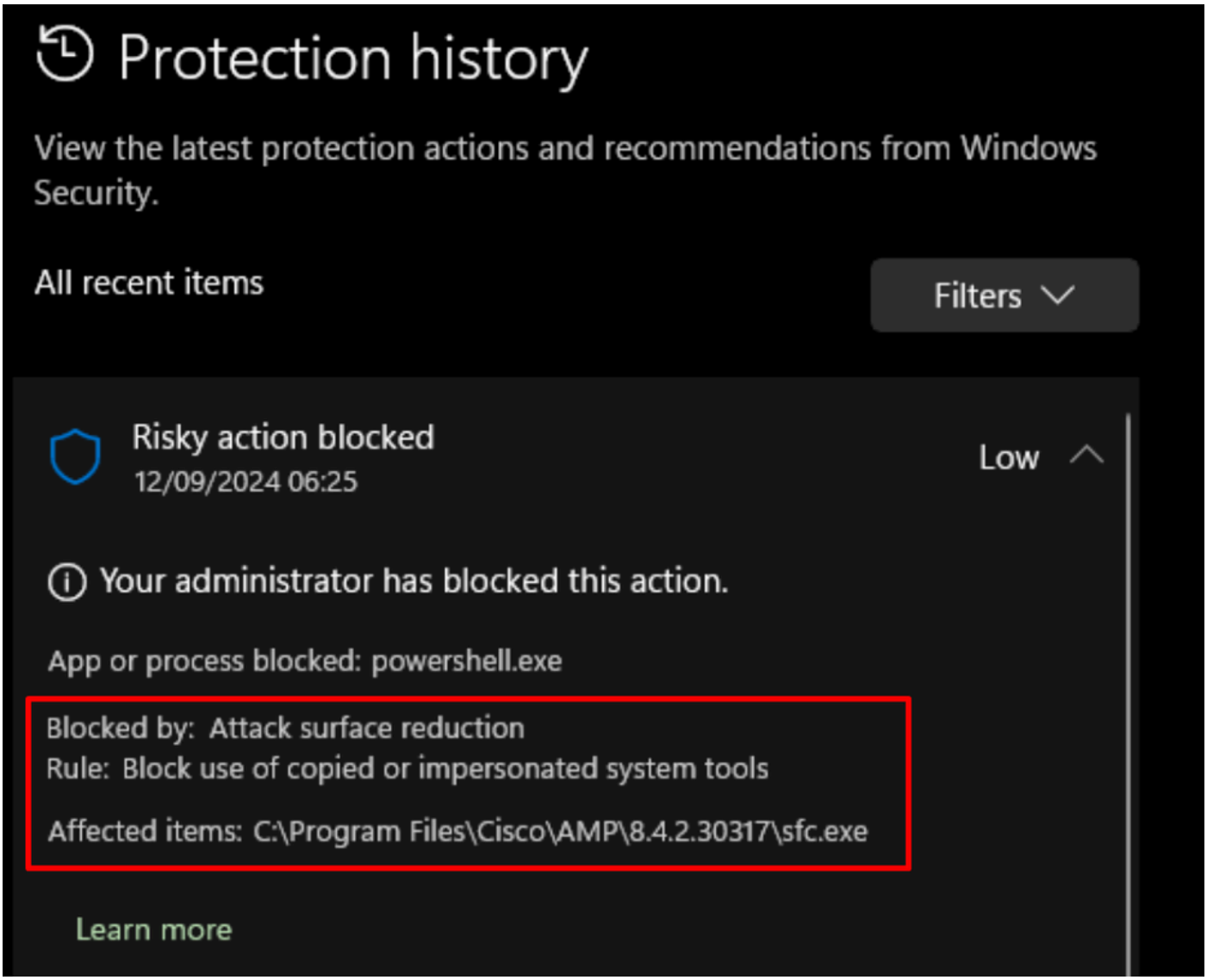
Indicatielampje #3: als we naar de locatie van Cisco Secure Endpoint onder C:\Program Files\Cisco\AMP\versie navigeren en we proberen de service handmatig te starten, dan wordt de toegang tot de toestemming geweigerd, zelfs voor de lokale admin-account

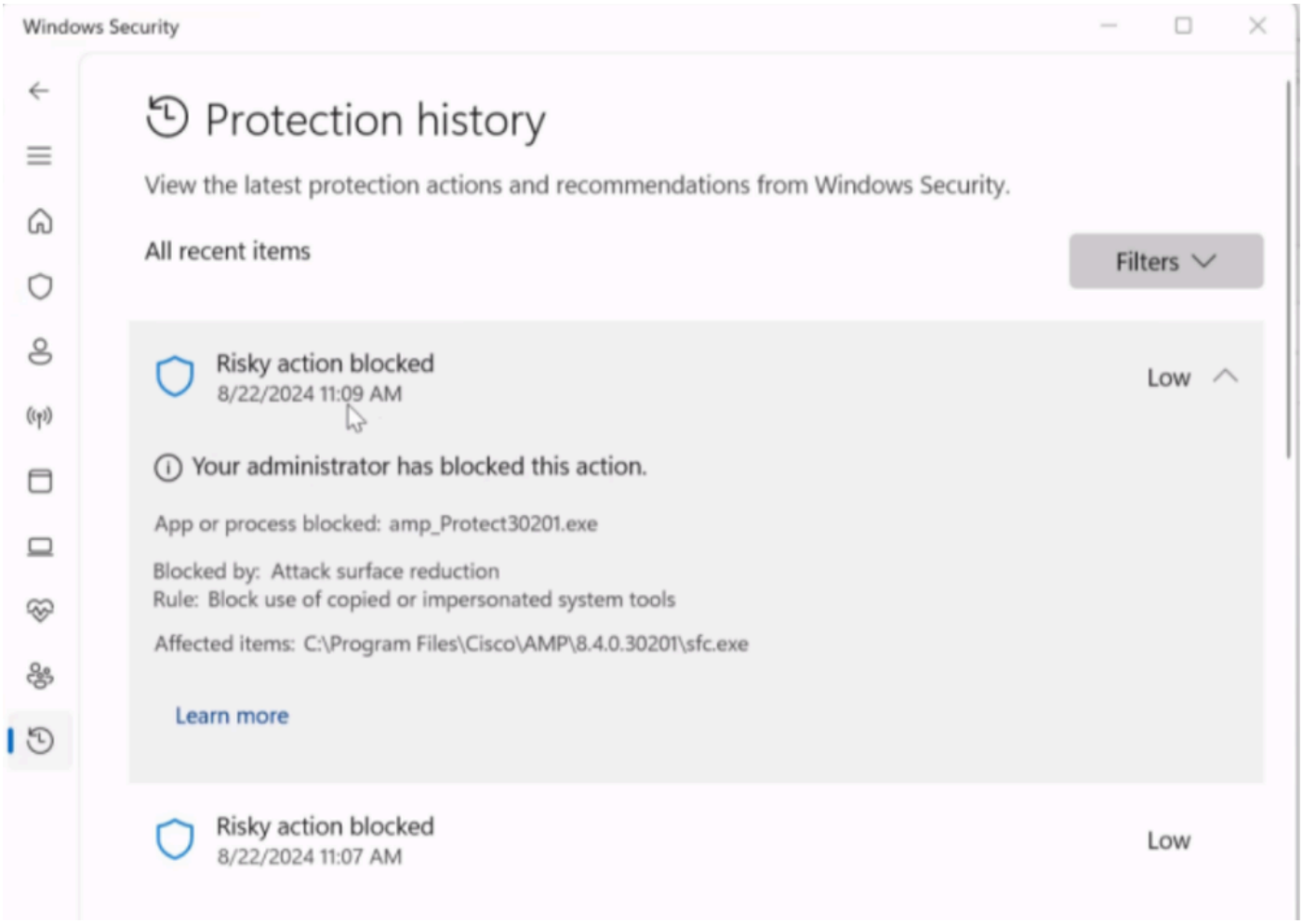


Indicator #4: Als we impro_install.log dat deel uitmaakt van de diagnostische bundel onderzoeken kunnen we een soortgelijke ontkenning van toegang waarnemen die lijkt op deze output.

```
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
```

Indicatielampje #5: Als we onder Windows-beveiliging navigeren en inkijken op de logboeken voor beschermingsgeschiedenis, zoeken we dit soort logberichten.


Protection history
View the latest protection actions and recommendations from Windows Security.
All recent items
Filters
Risky action blocked
12/09/2024 06:25
Low
Your administrator has blocked this action.
App or process blocked: powershell.exe
Blocked by: Attack surface reduction
Rule: Block use of copied or impersonated system tools
Affected items: C:\Program Files\Cisco\AMP\8.4.2.30317\sfc.exe
Learn more



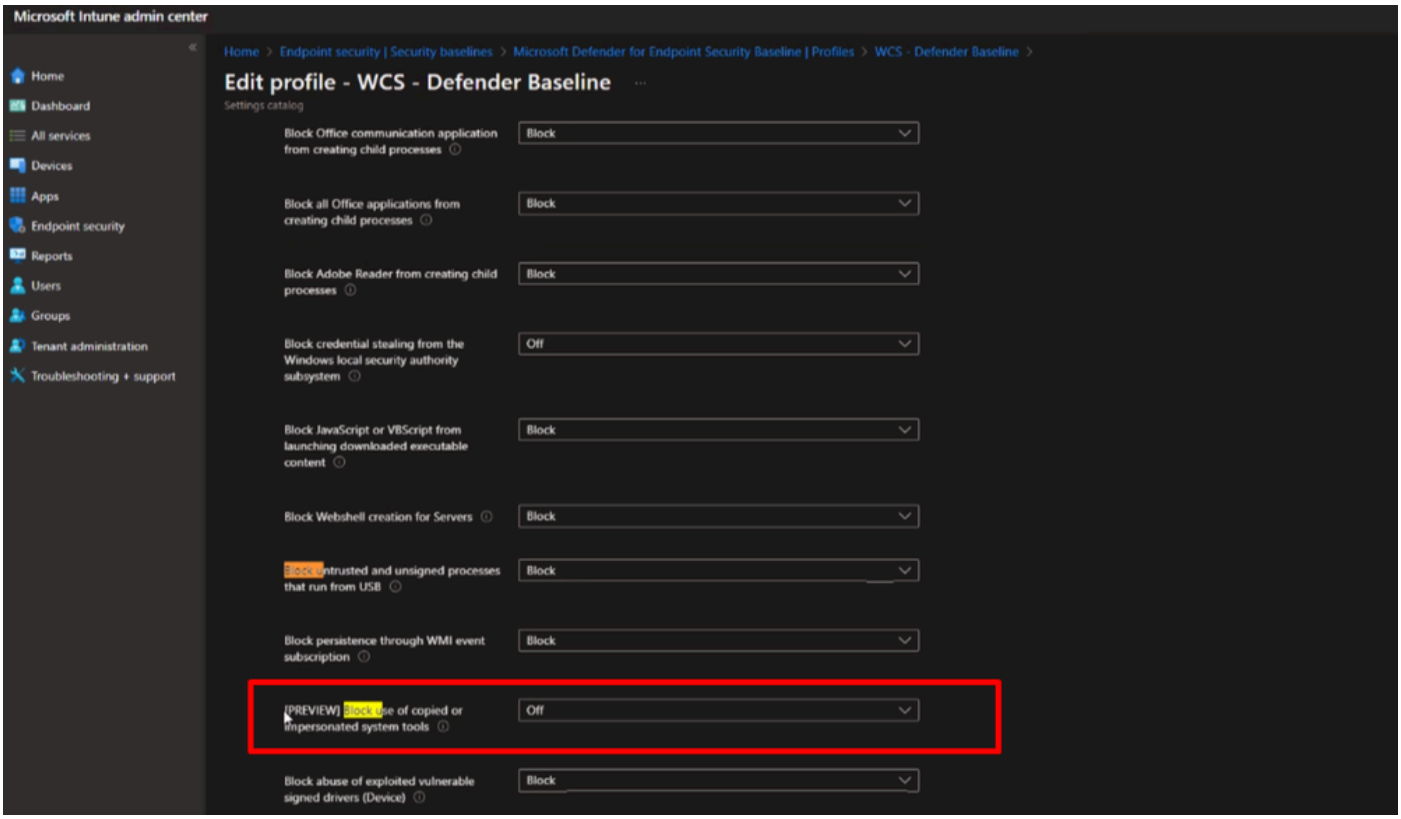
Dit zijn allemaal aanwijzingen dat het Secure Endpoint wordt geblokkeerd door applicatie van derden. In dit scenario werd het probleem gezien op Intune beheerde endpoints met of verkeerd geconfigureerd of niet geconfigureerd Attack oppervlakte reductie - BLOK gebruik van gekopieerde of nagemaakte systeem functie.

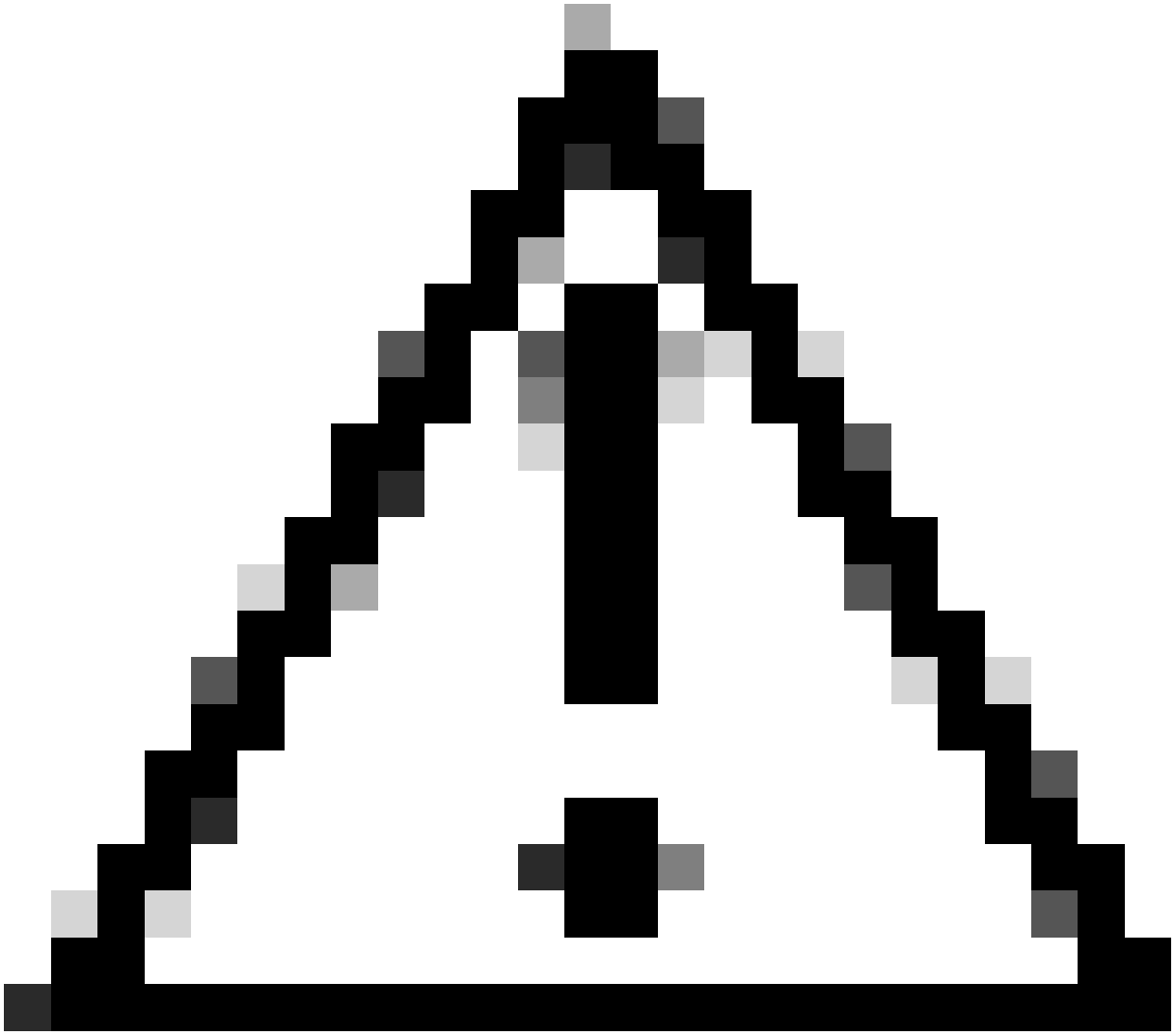
Tijdelijke oplossing

Aanbevolen wordt om de configuratie voor deze functie te raadplegen bij de applicatieontwikkelaar of deze optie verder te raadplegen via deze kennisbank.

Voor onmiddellijke remediëring kunnen we ons beheerde eindpunt in tegenspraak met een minder restrictief beleid verplaatsen of deze optie tijdelijk expliciet uitschakelen totdat de juiste stappen zijn gezet.

Dit is de instelling onder Intune Admin portal dat werd gebruikt als tijdelijke maatregel om beveiligde endpointconnectiviteit te herstellen.


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



Waarschuwing: Als u dit probleem ondervindt, moet u volledige installatie starten vanwege het ontbreken van sfc.exe

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.