# نقطة النهاية الآمنة - تم حظر تحديثات Microsoft الموصل بسبب تقليل سطح هجوم

## المحتويات



## المقدمة

يصف هذا المستند المشاكل التي تتسبب فيها كتل خفض سطح هجوم Microsoft Intune باستخدام ميزة أداوات النظام المنسوخة أو المنتحلة على الأنظمة التي يديرها Microsoft Intune والتي تتسبب بدورها في فشل تحديثات نقطة النهاية الآمنة.

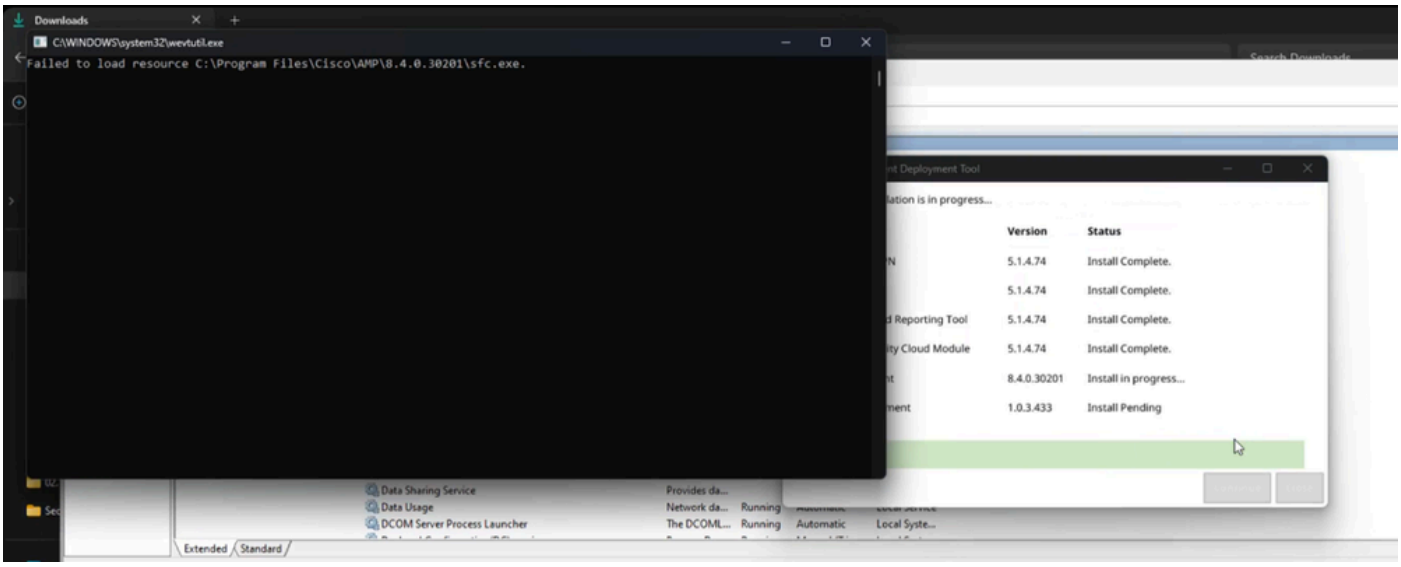
يرجى الرجوع إلى وثائق الميزة: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

## المشكلة

يمكن أن نواجه مشاكل في ترقيات نقطة النهاية الآمنة أو التثبيت الذي يتم تمثيله بهذه الأخطاء والمؤشرات.

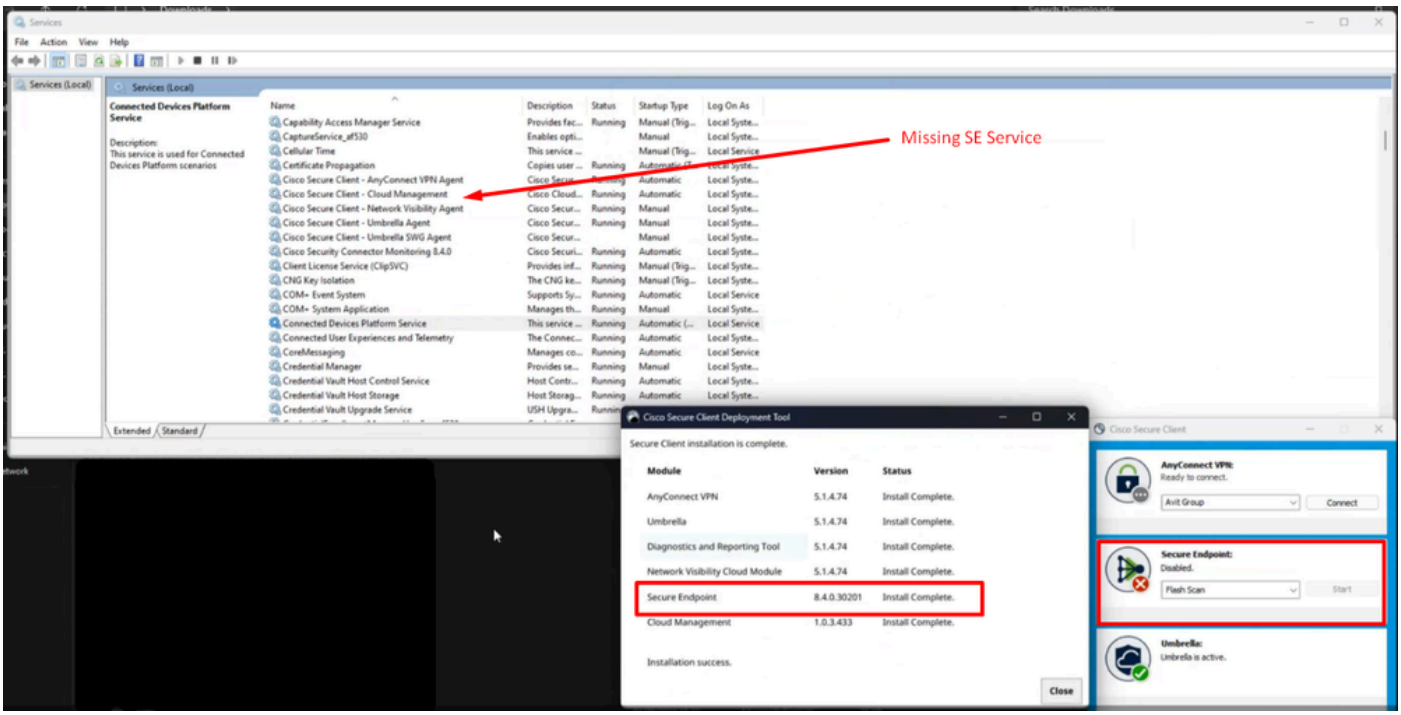
هناك مؤشرات مختلفة يمكن إستخدامها لتحديد أن هذه الميزة تتعارض مع تحديثات نقطة النهاية الآمنة.

المؤشر رقم 1: أثناء النشر، سنلاحظ هذه النافذة المنبثقة في نهاية التثبيت. يرجى ملاحظة أن القائمة المنبثقة سريعة إلى حد ما ولا يوجد أي تكرار آخر لأي خطأ بمجرد اكتمال التثبيت.

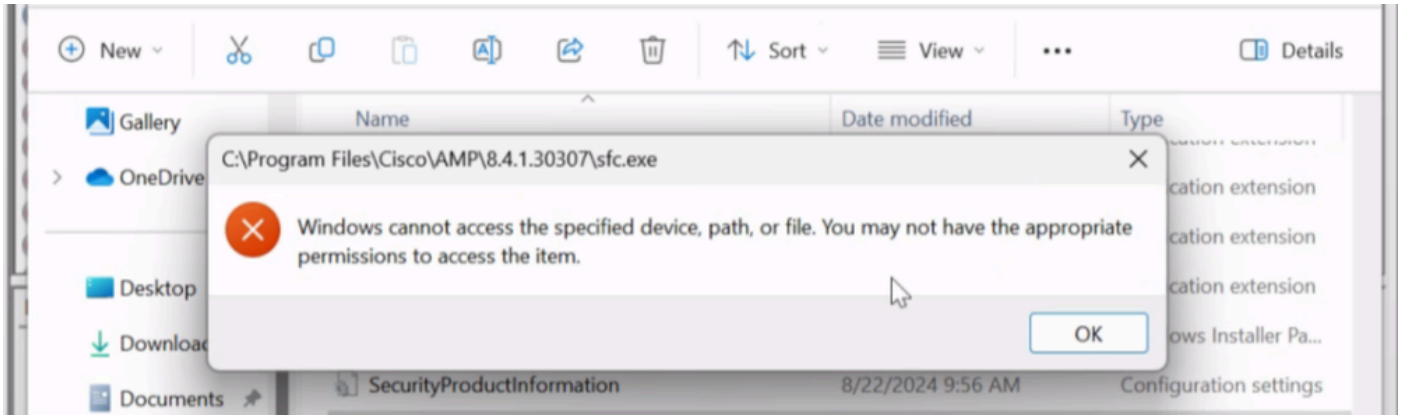


المؤشر #2: بعد التثبيت، لاحظ أن نقطة النهاية الآمنة في حالة معطلة في واجهة المستخدم.

كما أن خدمة نقطة النهاية الآمنة (sfc.exe) مفقودة تمامًا في مدير المهام — > الخدمات




المؤشر #3: إذا انتقلنا إلى موقع نقطة النهاية الآمنة من Cisco ضمن C:\Program Files\Cisco\AMP\version وحاولنا بدء الخدمة يدويًا، فيمكنك الحصول على الوصول إلى الإذن مرفوض حتى بالنسبة لحساب المسؤول المحلي

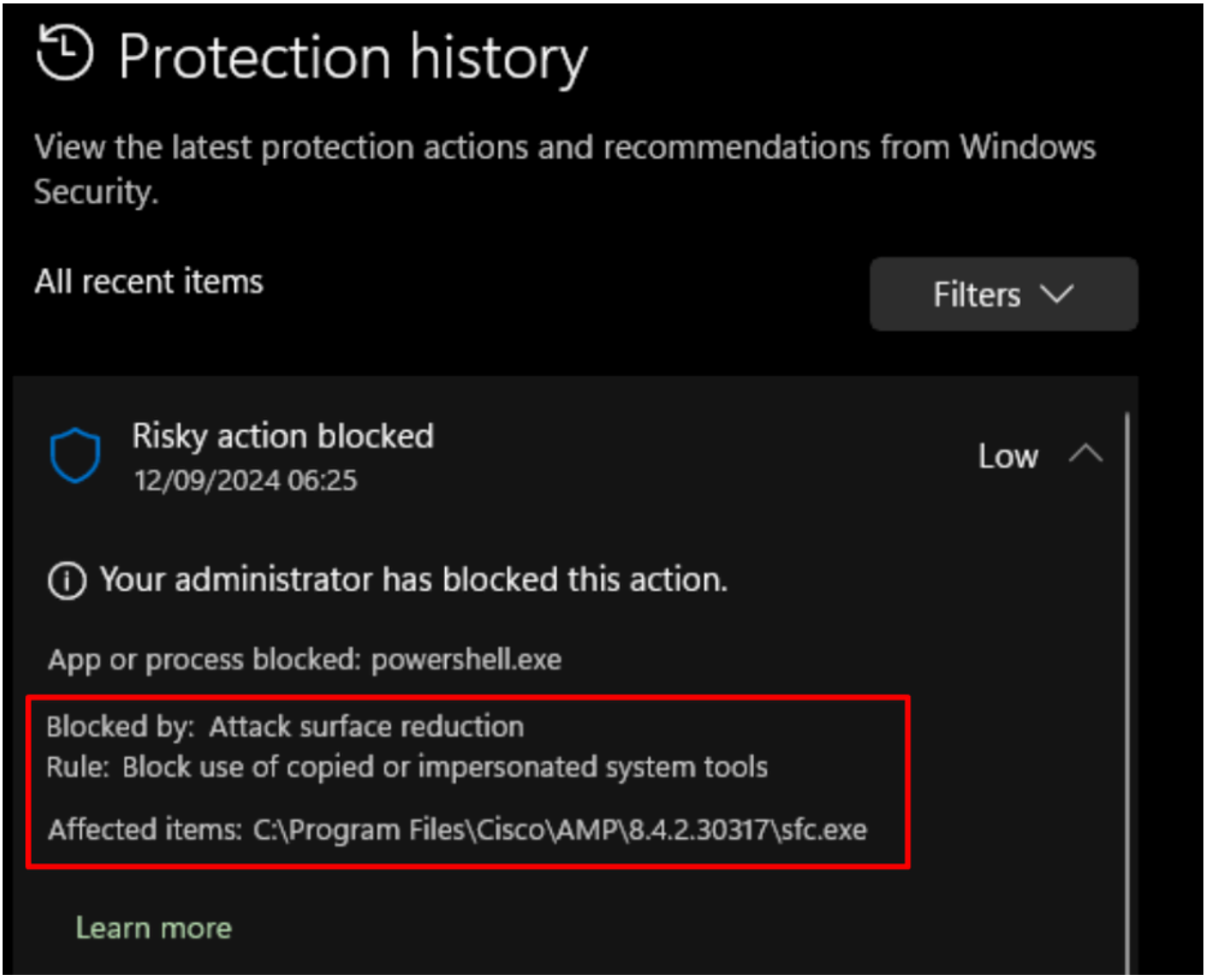


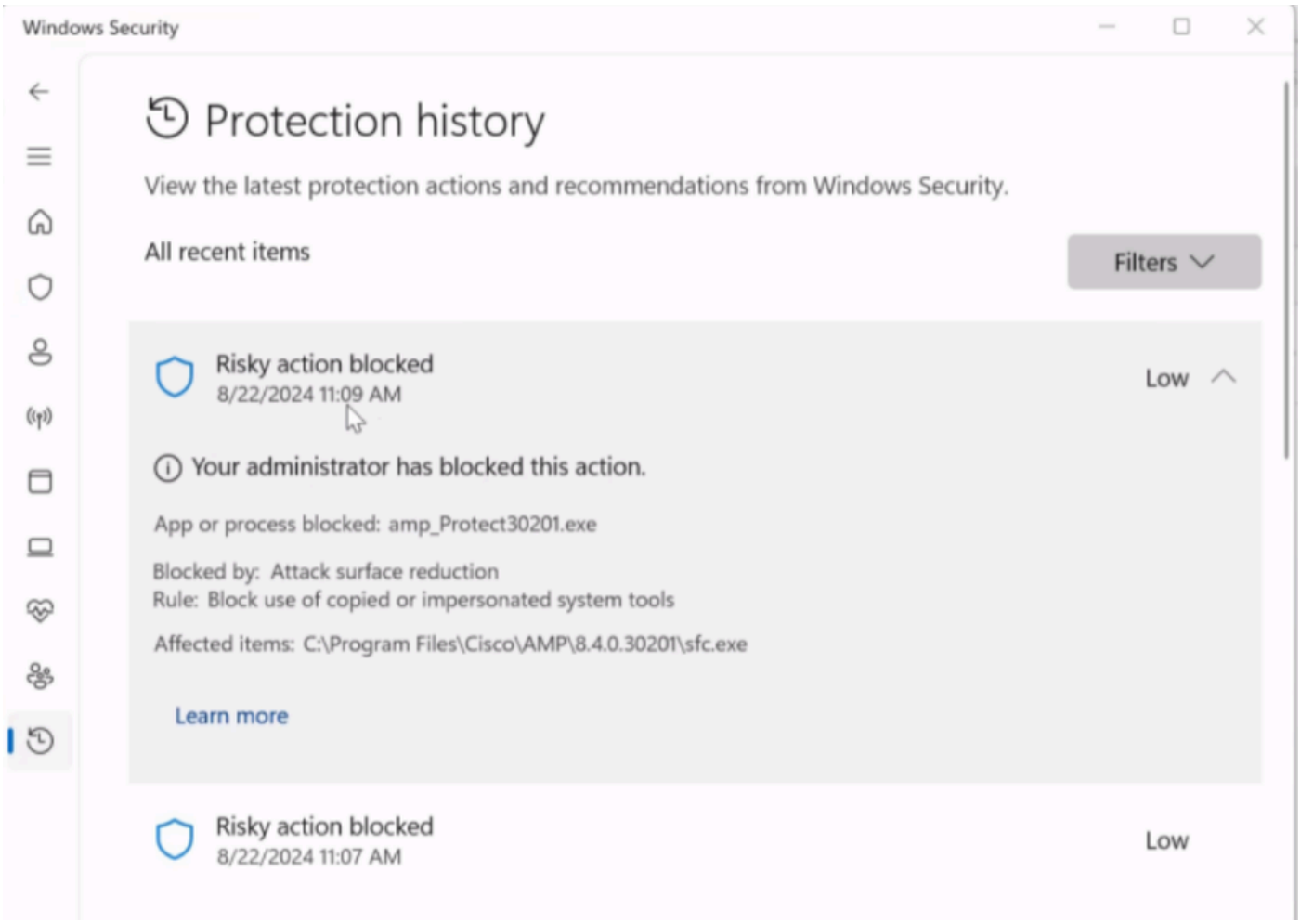

المؤشر #4: إذا قمنا بالتحقيق في impro_install.log الذي يعد جزءا من الحزمة التشخيصية،

فيمكننا ملاحظة رفض مماثل للوصول إلى ملف مشابه لهذا المخرج.

```
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
```

المؤشر رقم 5: إذا انتقلنا تحت أمان Windows ونظرنا إلى سجلات محفوظات الحماية ابحث عن هذا النوع من رسائل السجل.






كل هذه دلائل على حظر نقطة النهاية الآمنة بواسطة تطبيق من جهة خارجية. في هذا السيناريو، تمت رؤية المشكلة على نقاط النهاية المدارة من Intune التي تم تكوينها بشكل غير صحيح أو تم تكوينها لتقليل سطح الهجوم بشكل غير صحيح - إستخدام حظر ميزة النظام المنسوخ أو المنتحلة.

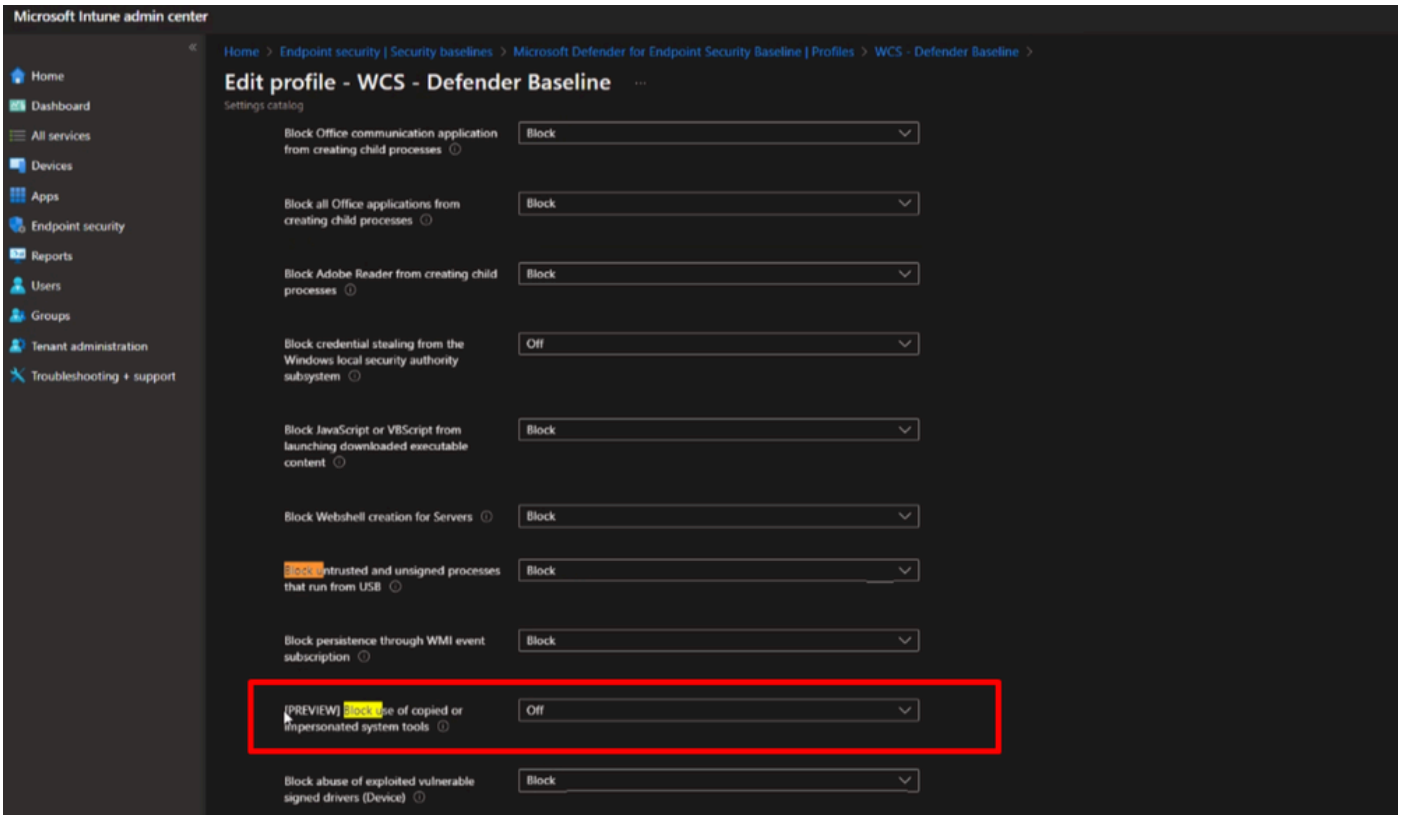
---

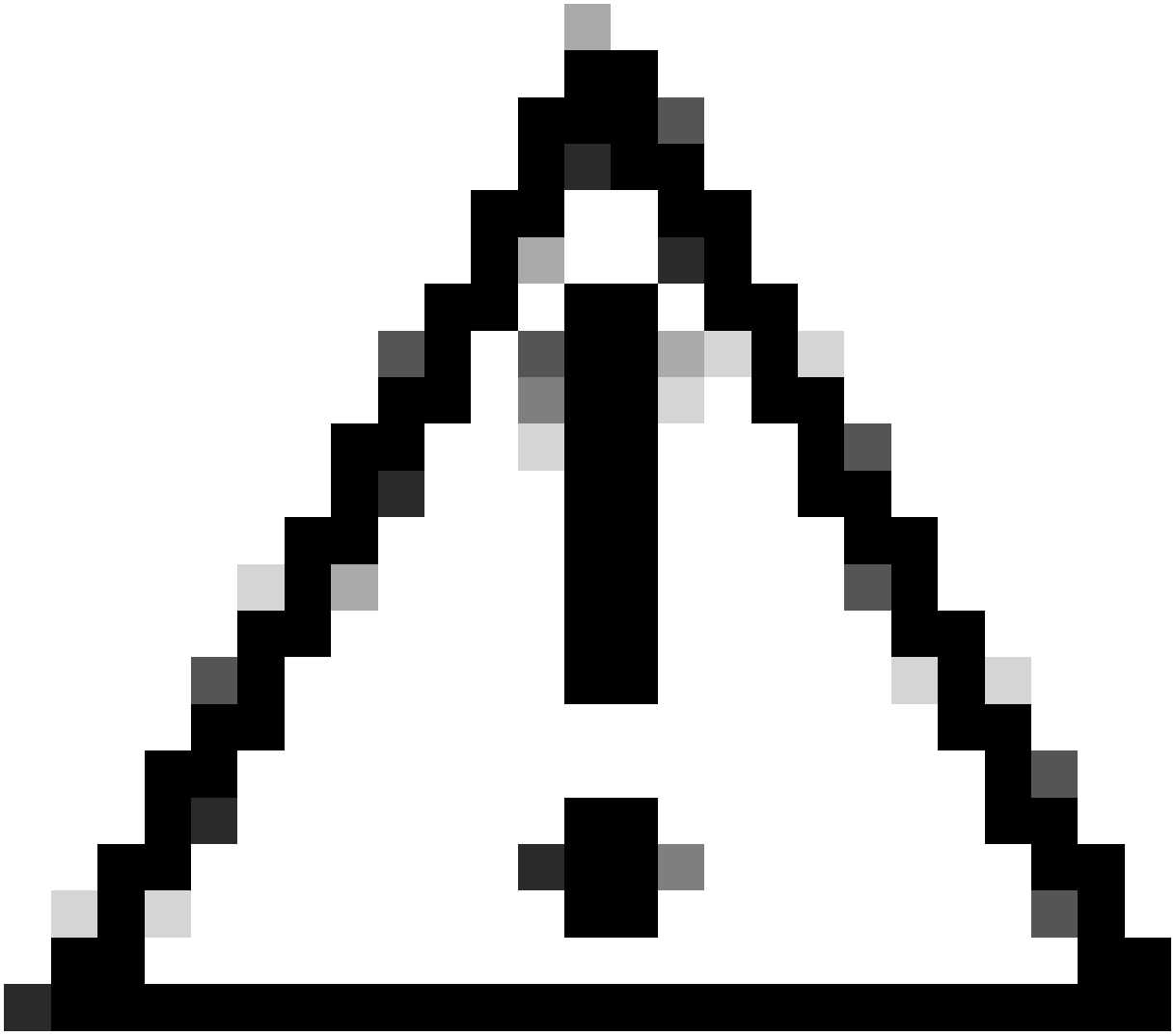
## الحل

ينصح بمراجعة تكوين هذه الميزة مع مطور التطبيق أو مراجعة هذه الميزة بشكل أكبر من خلال قاعدة المعارف هذه.

لحل المشكلات بشكل فوري، يمكننا إما نقل نقطة النهاية المدارة الخاصة بنا في الوقت المناسب إلى نهج أقل تقييدا أو إيقاف تشغيل هذه الميزة بشكل مؤقت بشكل صريح حتى يتم إتخاذ الخطوات المناسبة.

هذا هو الإعداد تحت مدخل إدارة Intune الذي تم إستخدامه كمقياس مؤقت لاستعادة اتصال نقطة النهاية الآمنة.


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



تحذير: إذا واجهت هذه المشكلة، فيجب عليك بدء التثبيت الكامل بسبب فقدان sfc.exe

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).