# Terminaux sécurisés : les mises à jour des connecteurs sont bloquées en raison de la réduction des attaques Microsoft

## Table des matières



## Introduction

Ce document décrit les problèmes causés par les blocs de réduction de surface de Microsoft Intune Attack utilisant la fonction d'outils système copiés ou empruntés sur les systèmes gérés par Microsoft Intune, qui à son tour entraîne l'échec des mises à jour de Secure Endpoint.

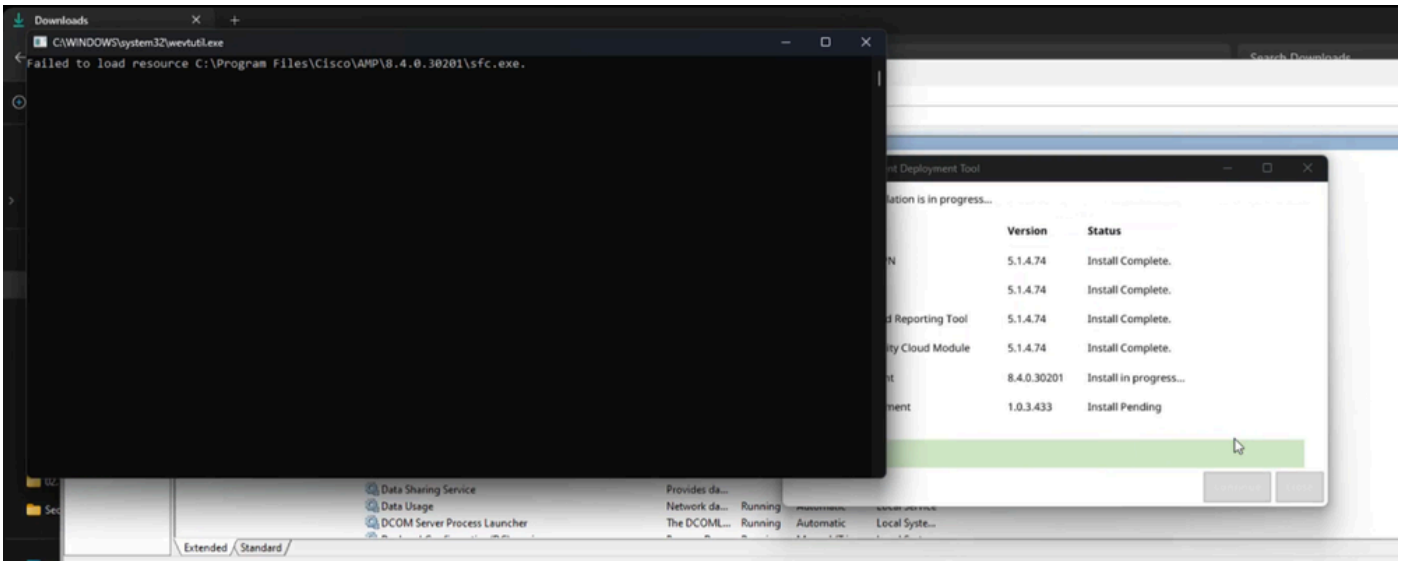
Reportez-vous à la documentation de la fonction : https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

## Problème

Nous pouvons rencontrer des problèmes avec les mises à niveau ou l'installation de Secure Endpoint qui sont représentés par ces erreurs et indicateurs.

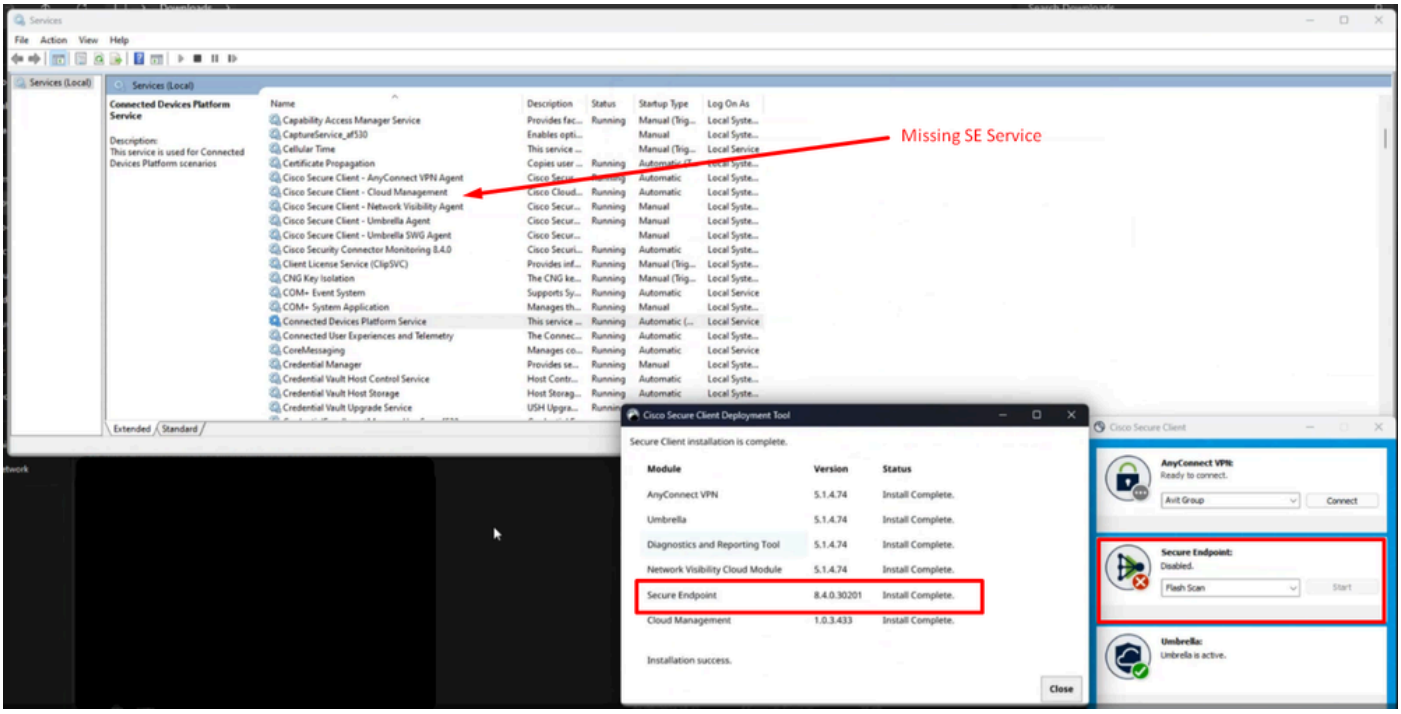
Divers indicateurs peuvent être utilisés pour identifier que cette fonctionnalité interfère avec les mises à jour de Secure Endpoint.

Indicateur #1 : pendant le déploiement, cette fenêtre contextuelle s’affichera à la fin de l’installation. Veuillez noter que la fenêtre contextuelle est assez rapide et qu'il n'y a aucun autre souvenir d'erreur une fois l'installation terminée.

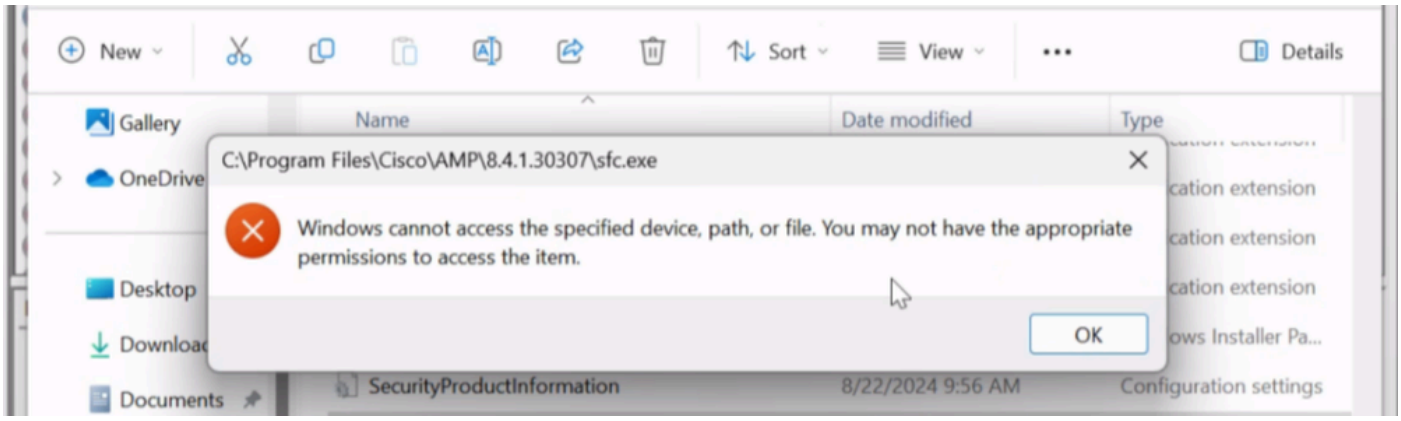



Indicateur #2 : après l'installation, notez que Secure Endpoint est désactivé dans l'interface utilisateur.

En outre, il manque complètement Secure Endpoint Service (sfc.exe) dans le Gestionnaire des tâches — > Services



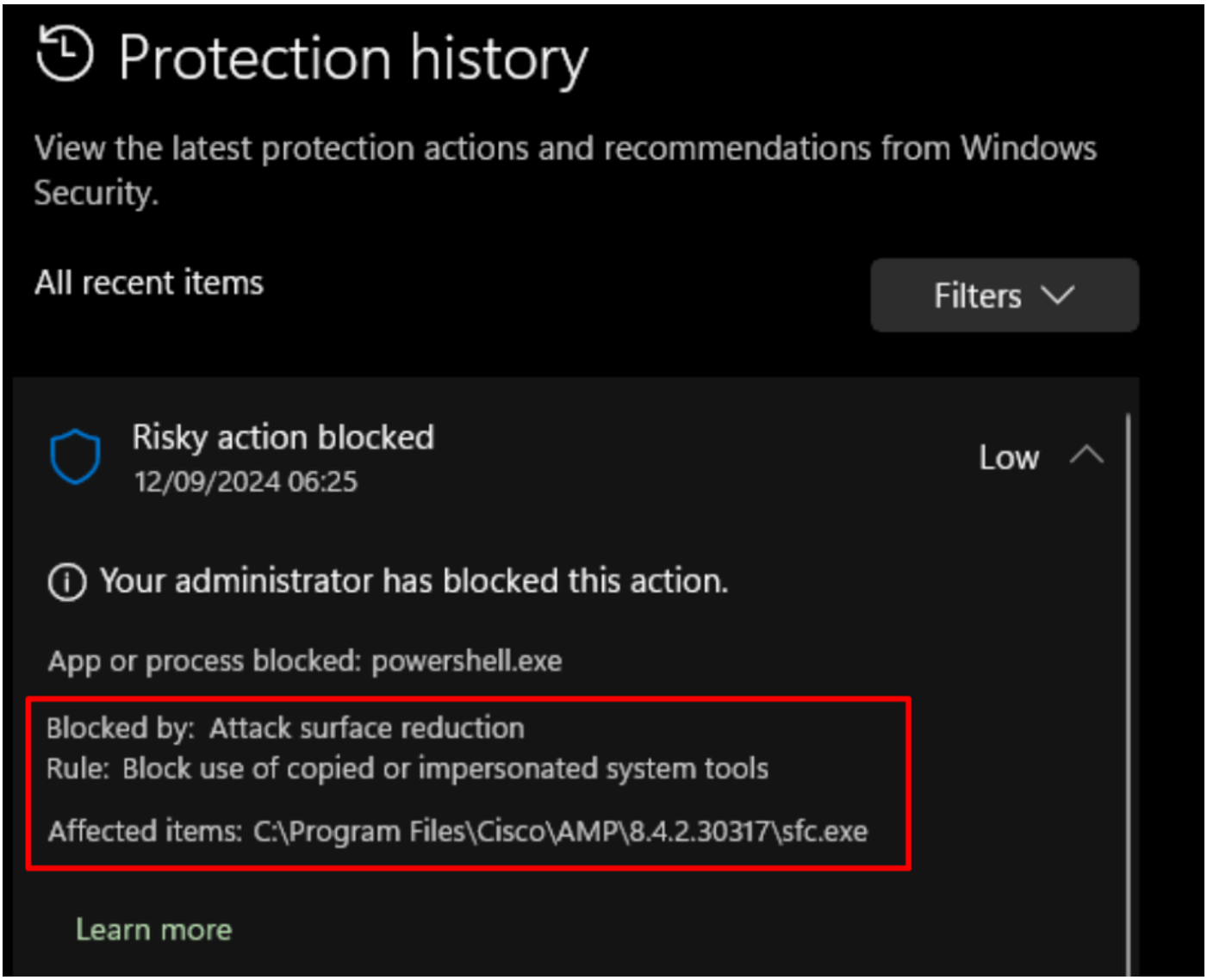

Indicateur #3 : si nous accédons à l'emplacement de Cisco Secure Endpoint sous C:\Program Files\Cisco\AMP\version et que nous essayons de démarrer le service manuellement, vous obtenez une autorisation d'accès refusée même pour le compte administrateur local

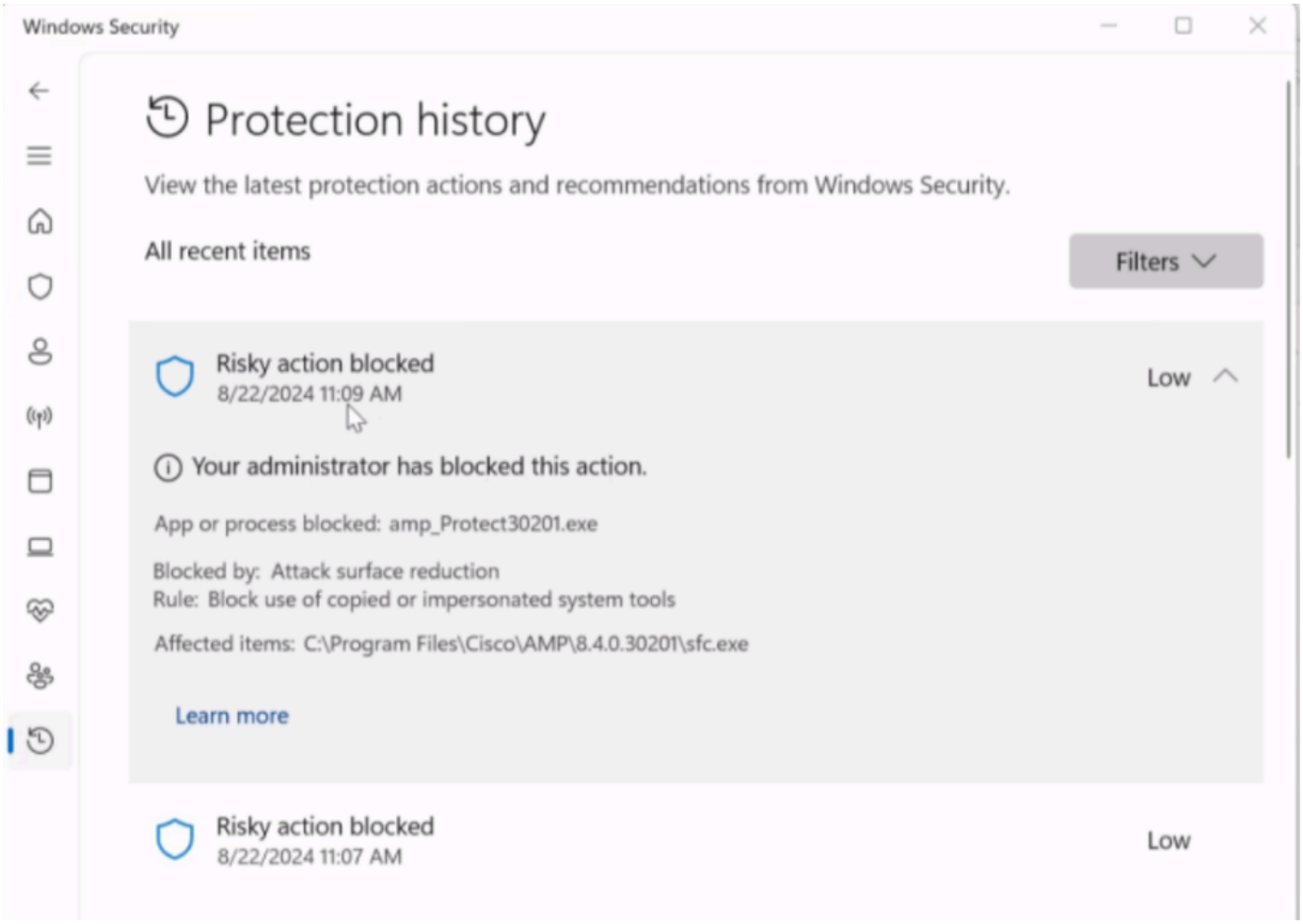



Indicateur #4 : Si nous examinons immpro_install.log qui fait partie du bundle de diagnostic, nous pouvons observer un déni d'accès similaire à celui-ci.

```
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
```

Indicateur #5 : si nous naviguons sous Sécurité Windows et que nous regardons dans les journaux Historique de protection, recherchez ces types de messages de journal.


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




Toutes ces informations indiquent que le terminal sécurisé est bloqué par une application tierce. Dans ce scénario, le problème a été constaté sur les terminaux gérés Intune avec une configuration incorrecte ou non configurée Réduction de la surface d'attaque - BLOQUER l'utilisation de la fonctionnalité système copiée ou usurpée d'identité.

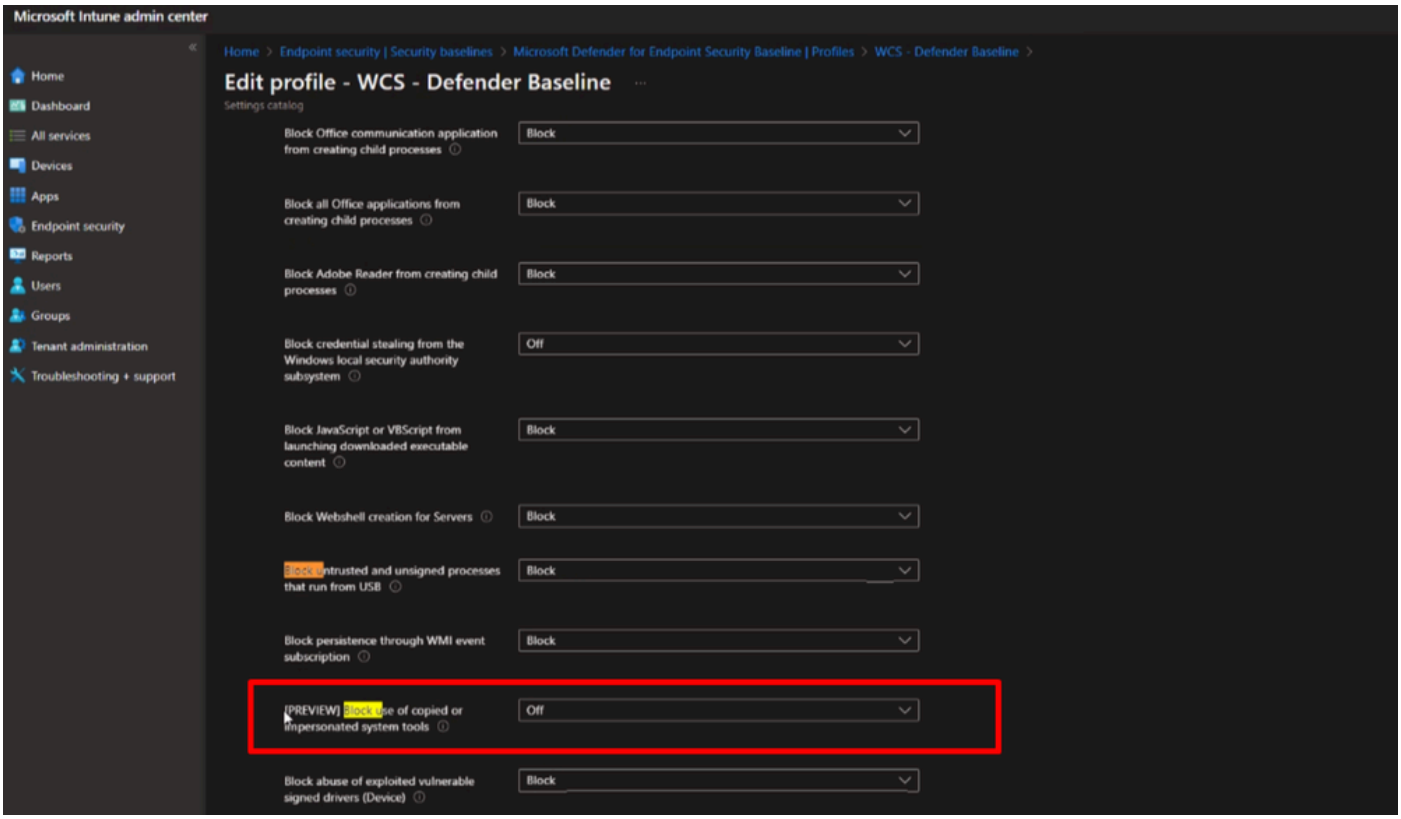
---

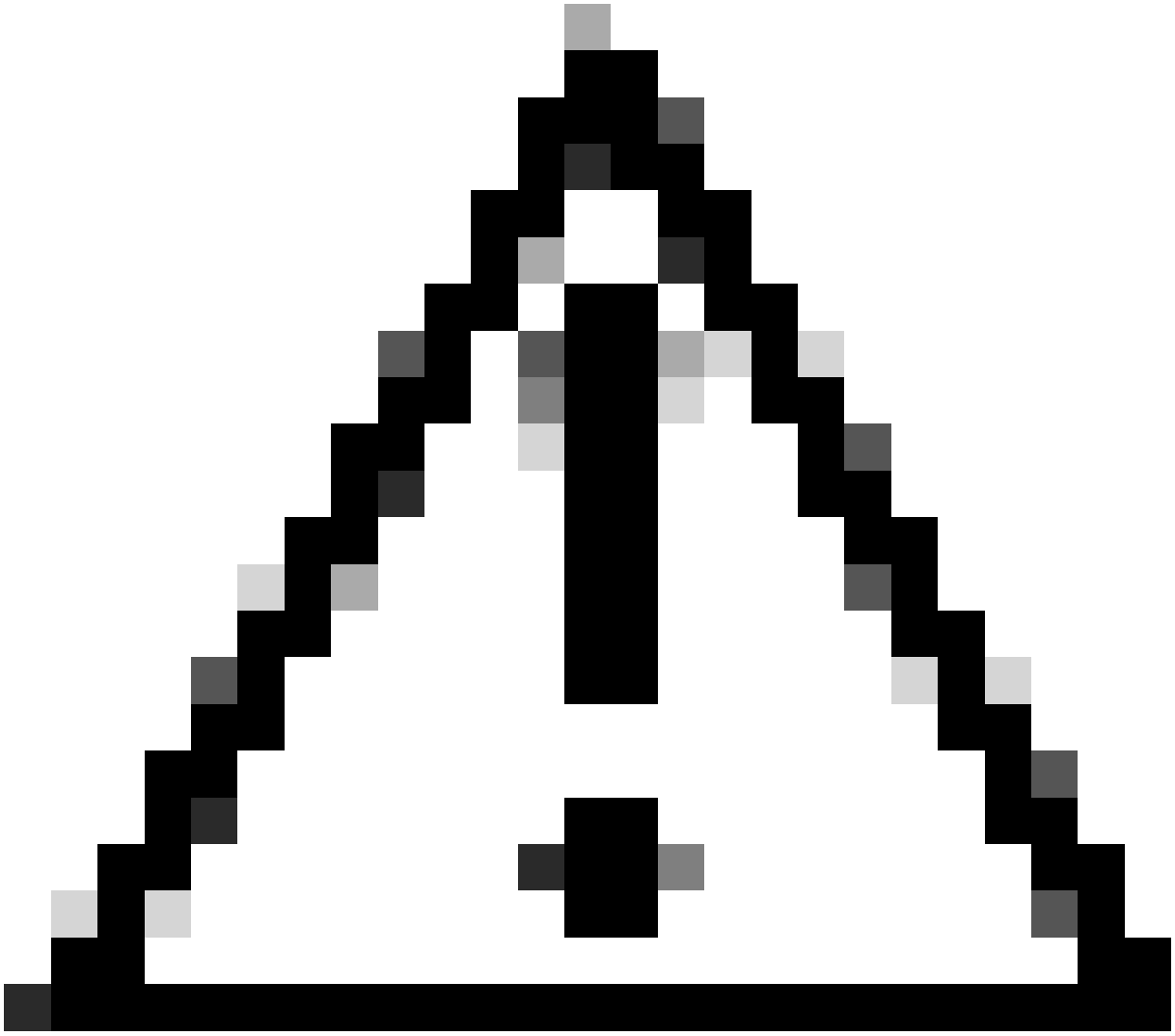
## Solution de contournement

Il est conseillé de consulter la configuration de cette fonctionnalité avec le développeur d'applications ou de consulter cette fonctionnalité plus en détail dans cette base de connaissances.

Pour une correction immédiate, nous pouvons soit déplacer notre point de terminaison géré de manière intune vers une stratégie moins restrictive, soit désactiver cette fonctionnalité de manière explicite jusqu'à ce que les étapes appropriées soient effectuées.

Il s'agit du paramètre sous Intune admin portal qui a été utilisé comme mesure temporaire pour restaurer la connectivité Secure Endpoint.


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



Attention : si vous rencontrez ce problème, vous devez lancer l'installation complète en raison de l'absence de sfc.exe

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.