安全終結點-聯結器更新因Microsoft攻擊面縮小而被阻止

目錄

[簡介](#)

[問題](#)

[因應措施](#)

簡介

本文檔介紹由Microsoft Intune管理的系統上使用複製或模擬系統工具功能的Microsoft Intune攻擊面縮減塊導致Secure Endpoint更新失敗所導致的問題。

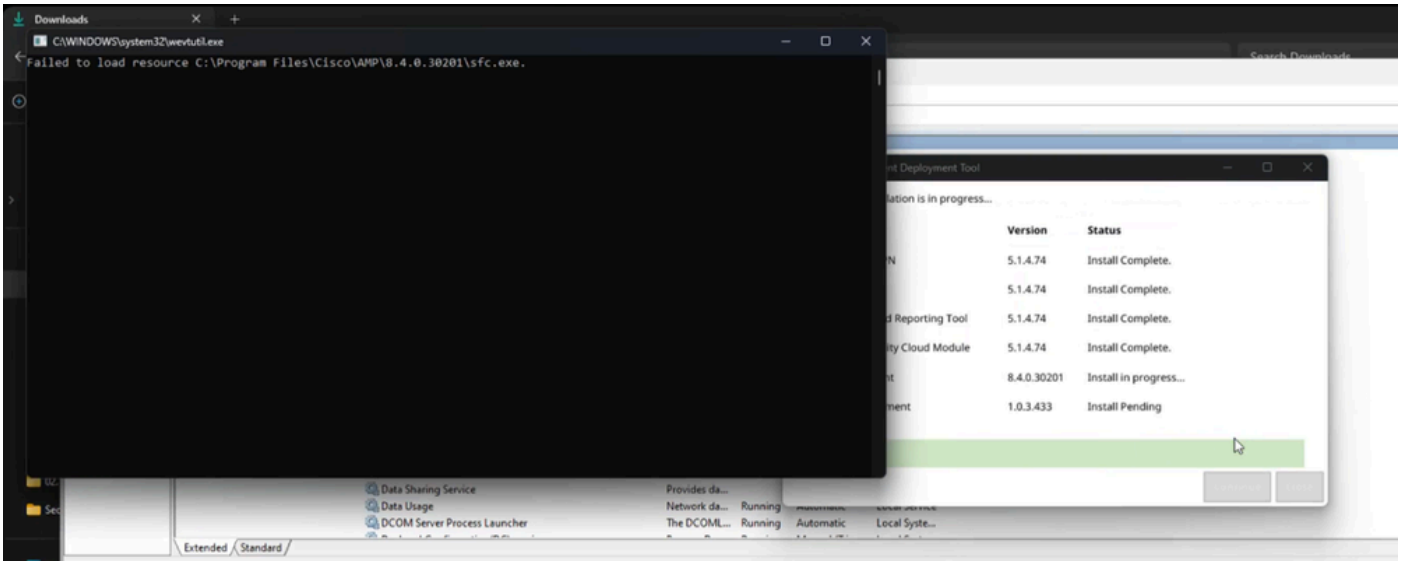
請參閱功能文檔：https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

問題

我們可能會遇到由這些錯誤和指示符表示的安全終端升級或安裝問題。

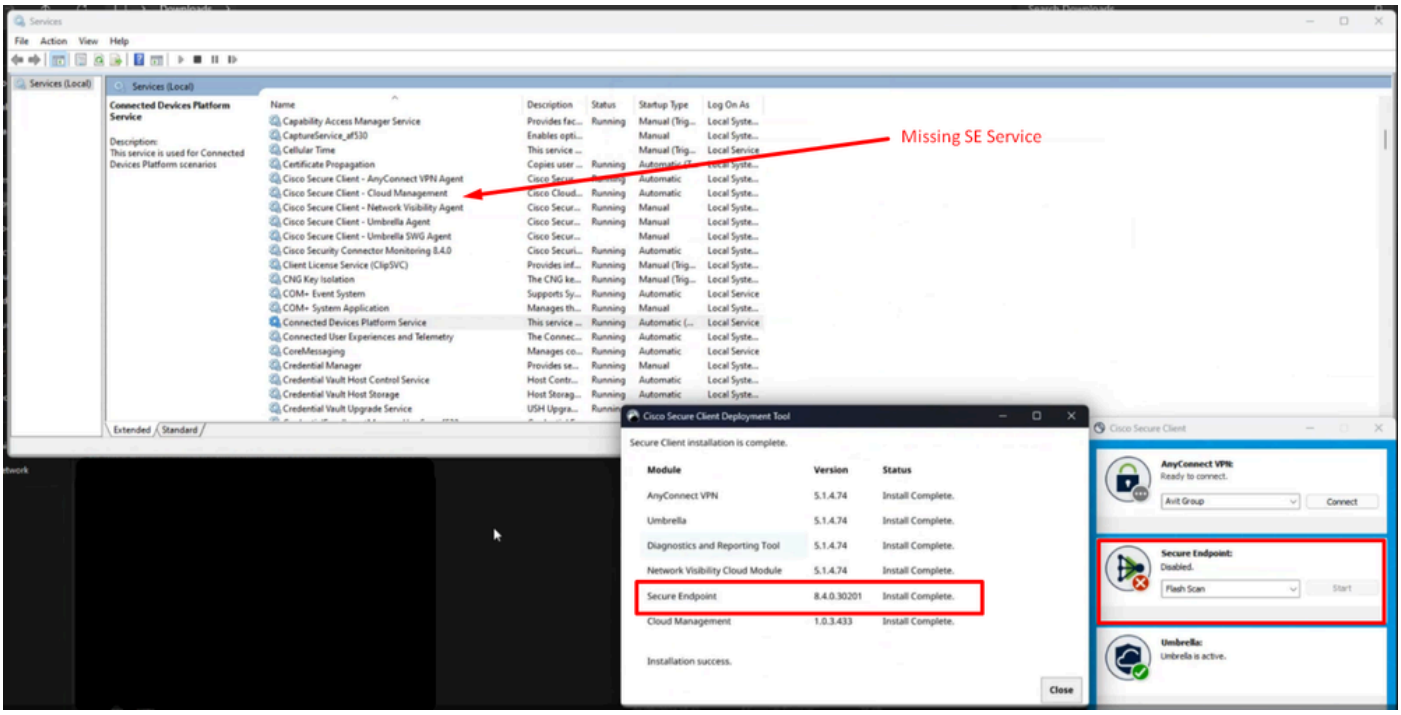
有多種指標可用於辨識此功能干擾安全終端更新。

指標#1：在部署期間，我們會在安裝結束時看到此彈出窗口。請注意，此快顯視窗相當快速，安裝完成後，便不會再有任何錯誤回憶。

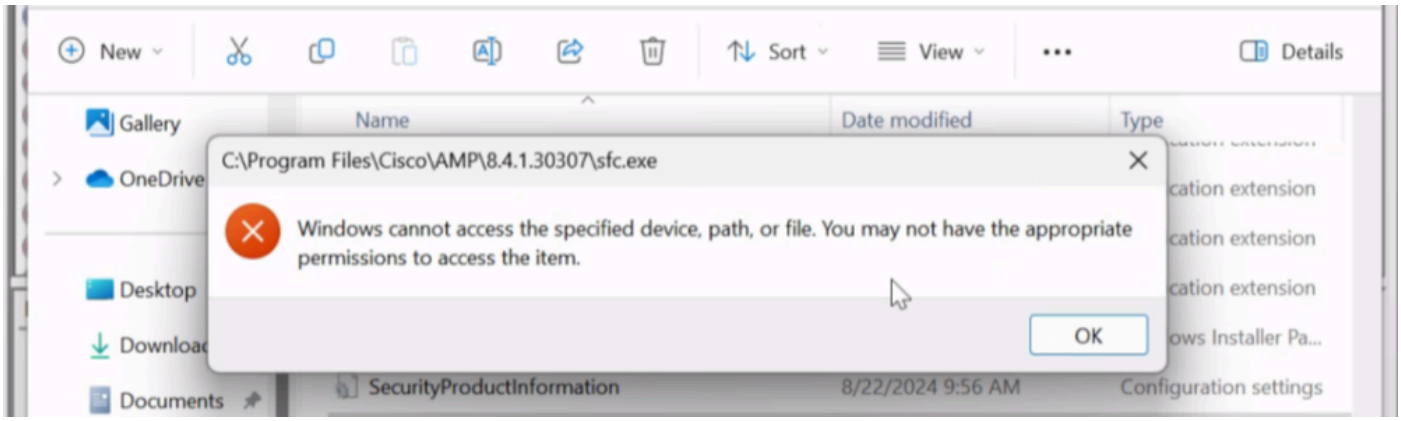


指示器#2：安裝完成後，請注意UI中的安全終端處於停用狀態。

此外，工作管理員— > Services中完全缺少Secure Endpoint Service (sfc.exe)。



指標#3：如果我們導航到C:\Program Files\Cisco\AMP\version下的Cisco Secure Endpoint位置，然後嘗試手動啟動服務，則即使對本地管理員帳戶，許可權訪問也會被拒絕

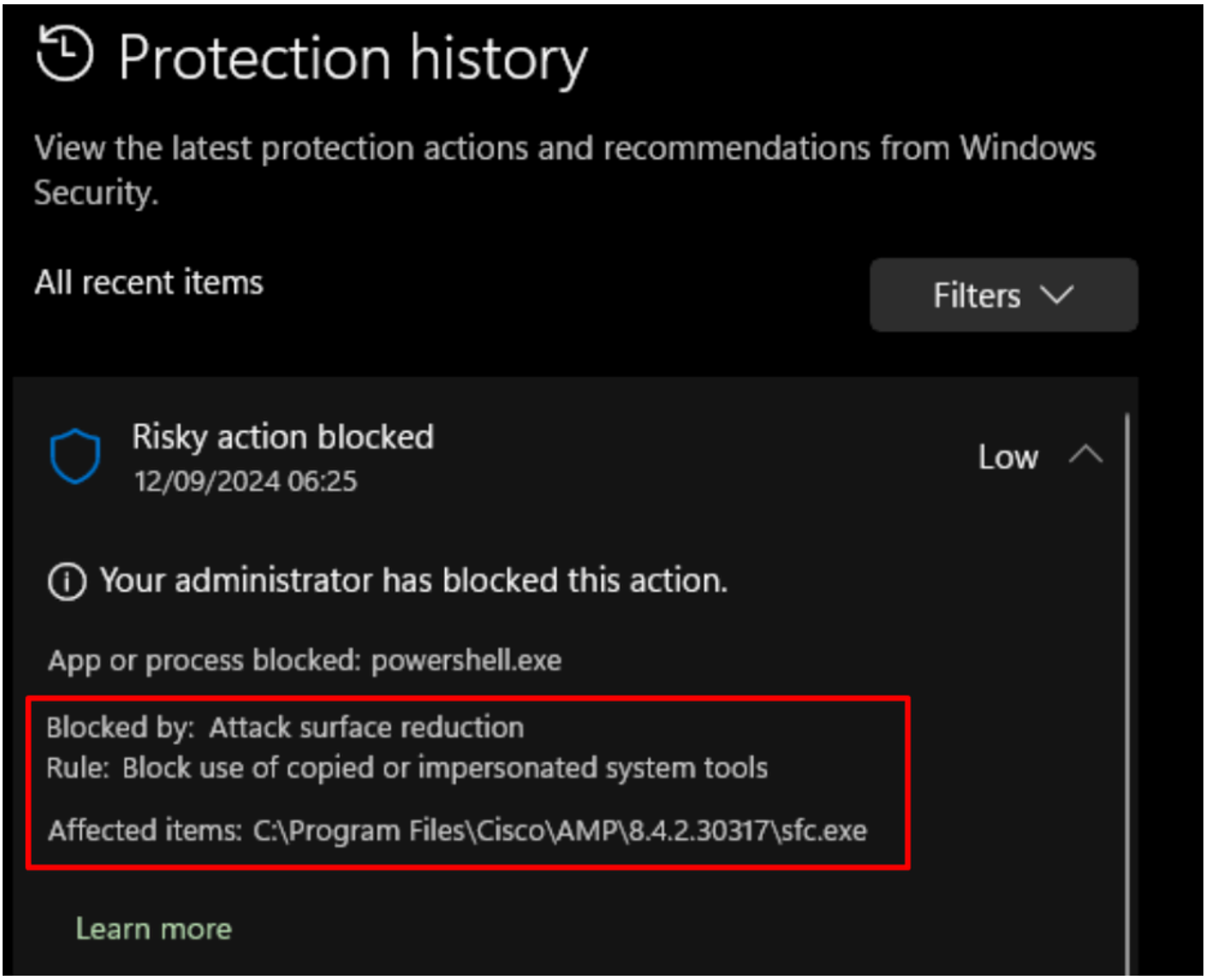


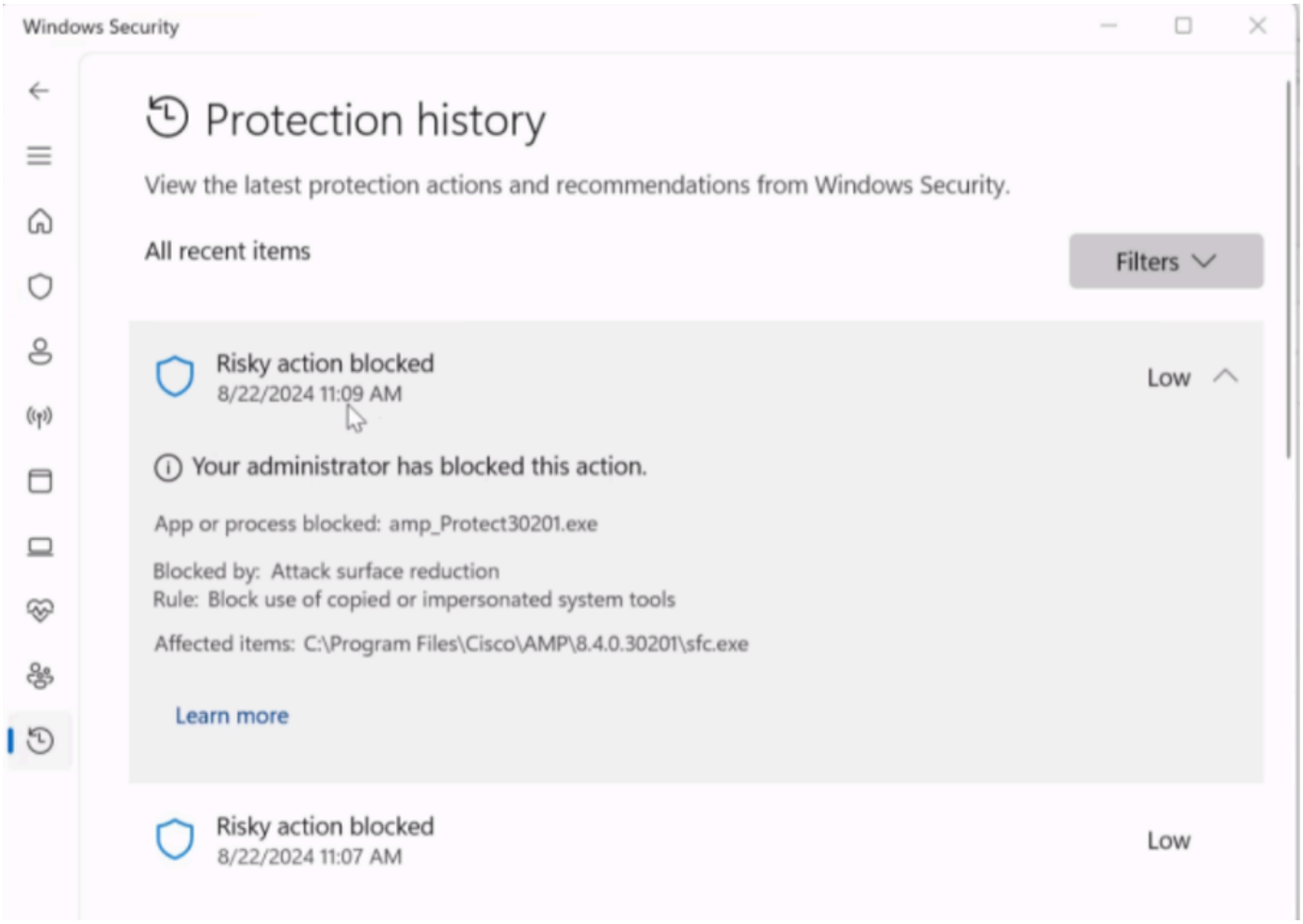
指示器#4：如果檢查診斷包中的immpro_install.log，我們可以看到類似以下輸出的類似拒絕訪問。

```
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
```

指標#5：如果導航到Windows安全下並檢視保護歷史記錄日誌，請查詢這些型別的日誌消息。





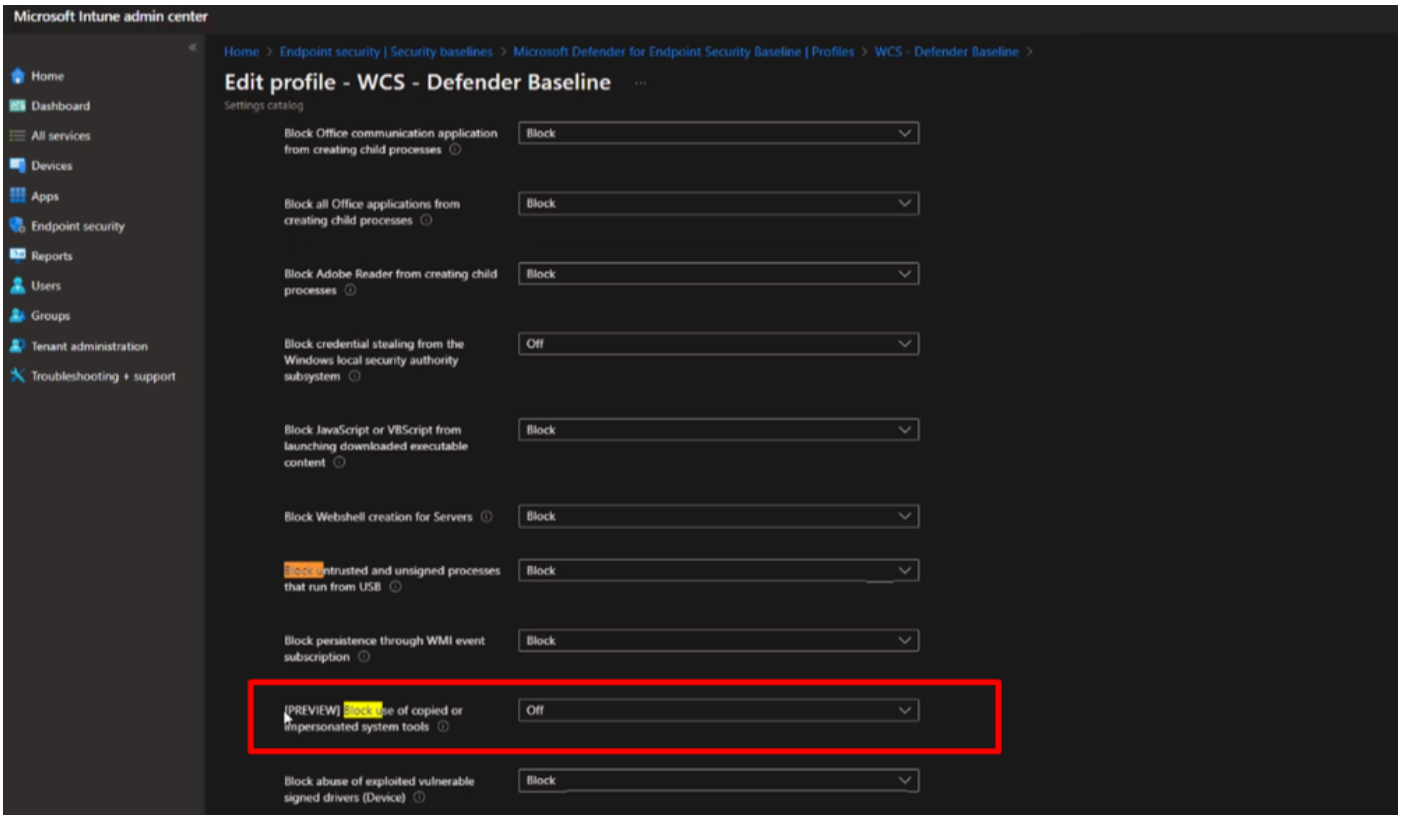
所有這些都表示安全終端正被第三方應用程式阻止。在此場景中，在Intune託管端點上發現該問題，這些端點配置錯誤或未配置攻擊面減少-阻止使用複製或模擬系統功能。

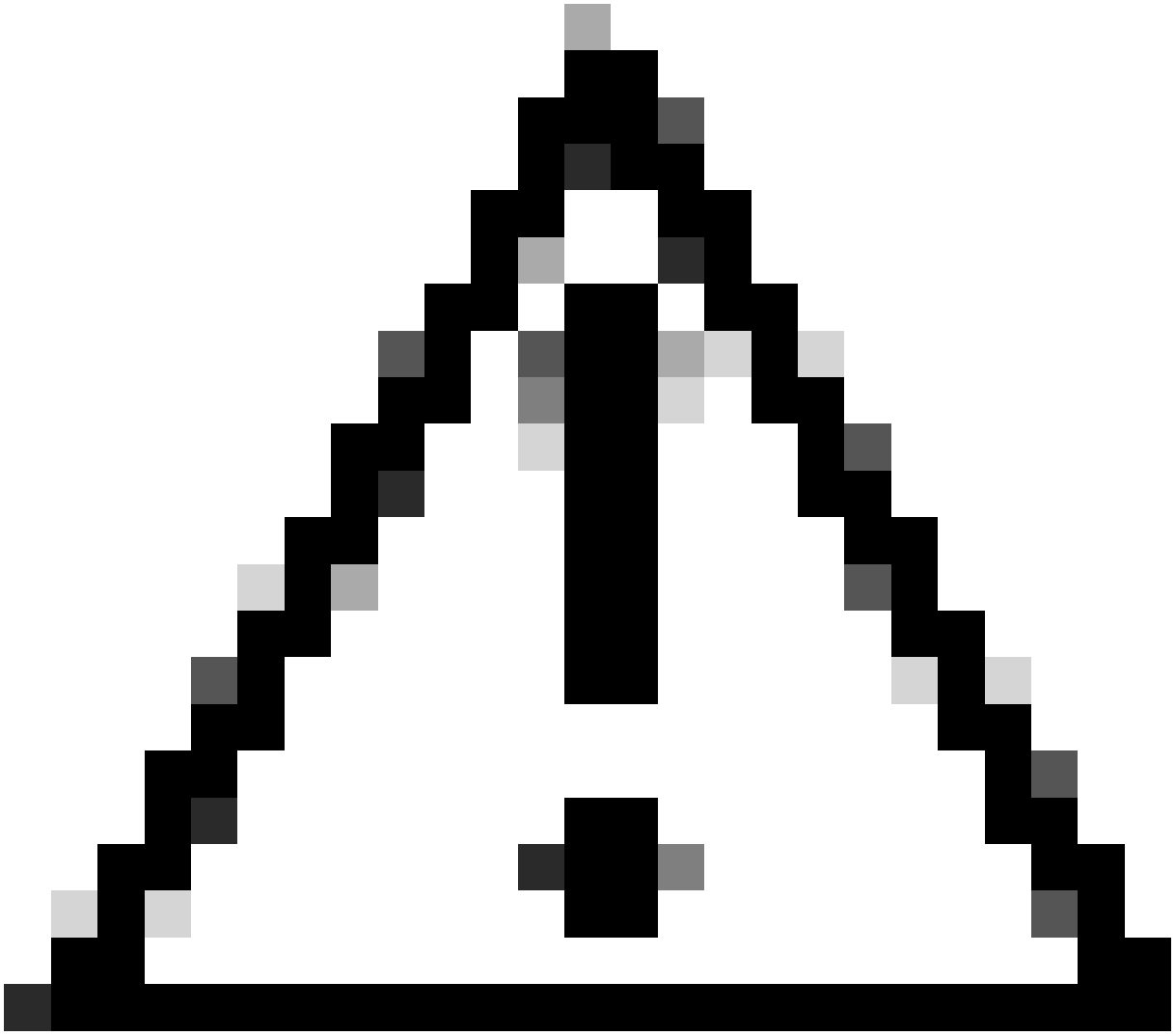
因應措施

建議向應用程式開發人員諮詢此功能的配置，或進一步透過此知識庫諮詢此功能。

為了立即進行補救，我們可以將受管終端改為限制較少的策略，或者臨時顯式關閉此功能，直到執行適當的步驟。

這是Intune管理門戶下的設定，用作恢復安全終結點連線的臨時措施。


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



注意：如果遇到此問題，由於缺少sfc.exe，必須啟動完全安裝

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。