Terminal seguro: se bloquean las actualizaciones de conectores debido a la reducción de la superficie de ataque de Microsoft

Contenido

Introducción

Este documento describe los problemas causados por los bloques de reducción de superficie de Microsoft Intune Attack mediante la función de herramientas del sistema copiadas o suplantadas en sistemas administrados por Microsoft Intune que, a su vez, hace que las actualizaciones de Secure Endpoint fallen.

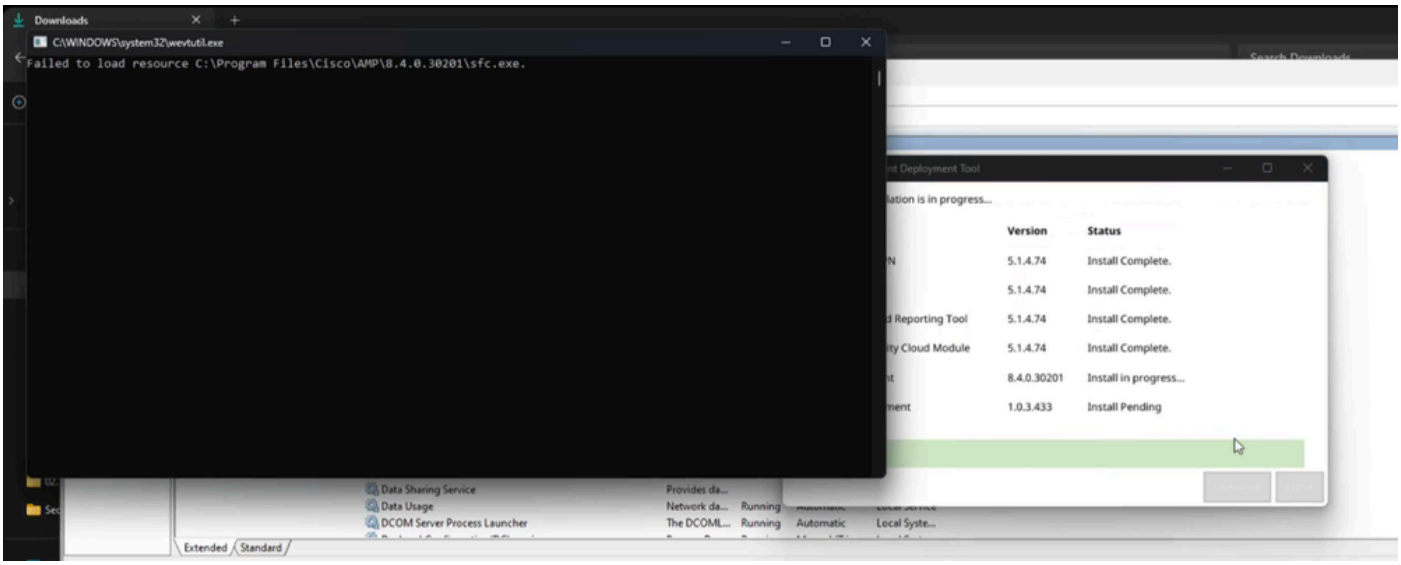
Consulte la documentación de la función: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

Problema

Podemos experimentar problemas con las actualizaciones o la instalación de terminales seguros, que se representan con estos errores e indicadores.

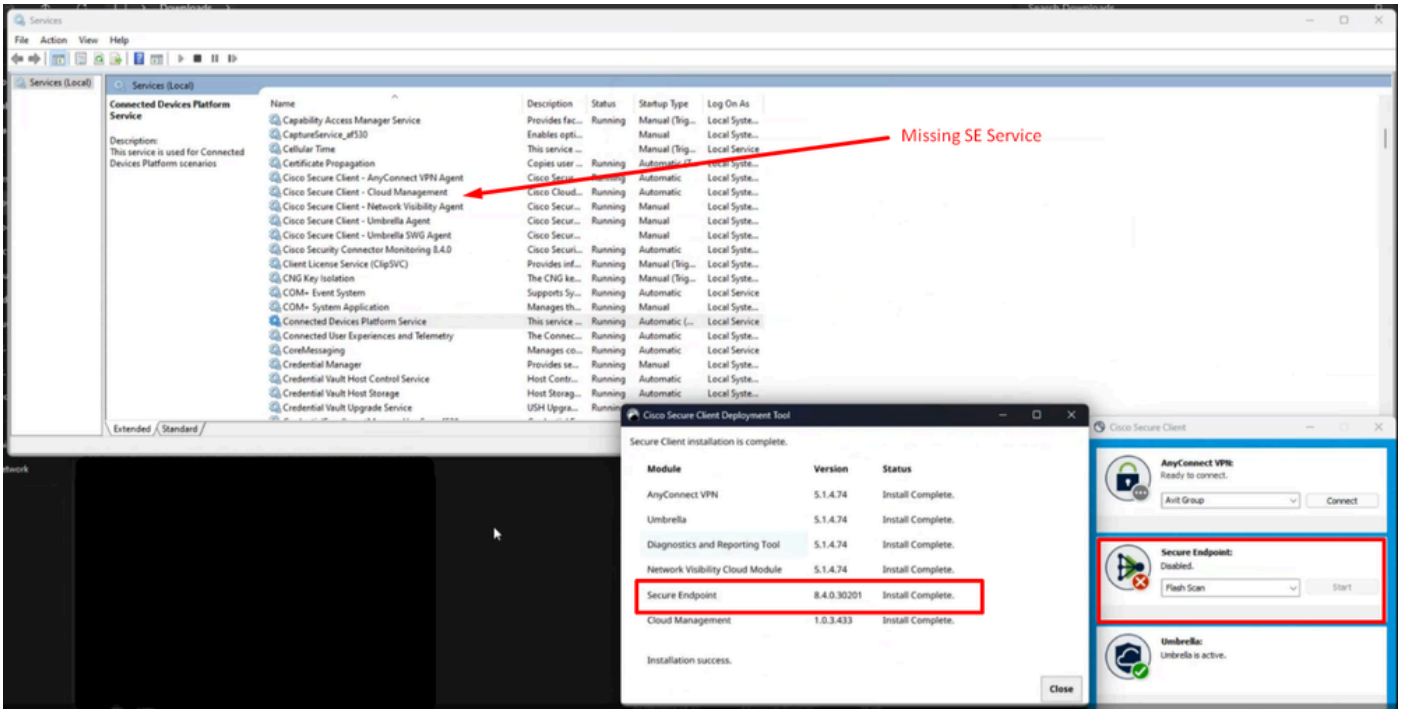
Existen varios indicadores que se pueden utilizar para identificar que esta función interfiere con las actualizaciones de terminales seguros.

Indicador #1: Durante la implementación, veremos esta ventana emergente al final de la instalación. Tenga en cuenta que la ventana emergente es bastante rápida y que no se puede recordar ningún otro error una vez finalizada la instalación.

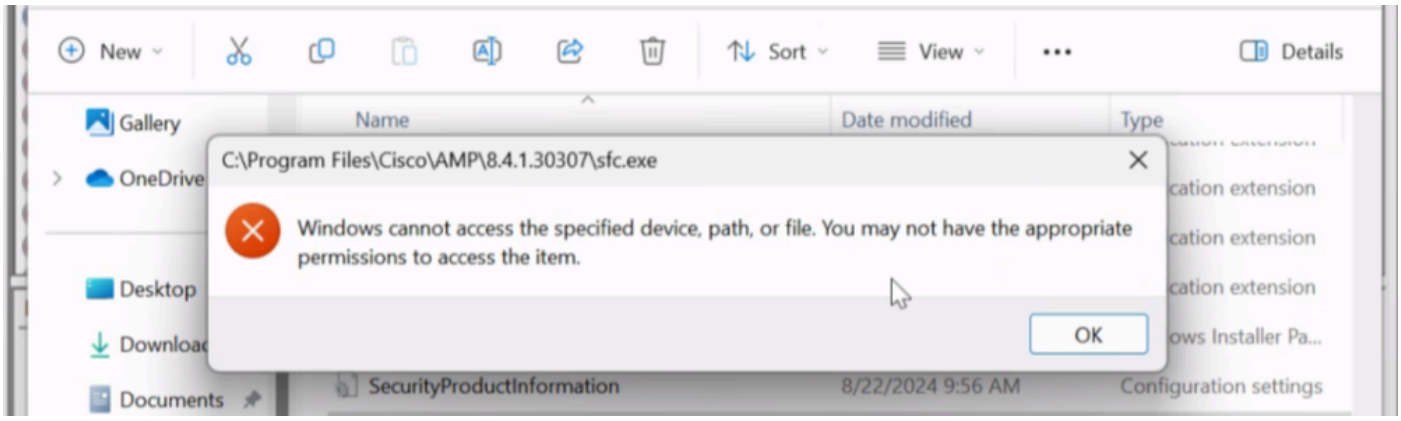


Indicador #2: Después de la instalación, observe que Secure Endpoint está en estado deshabilitado en la interfaz de usuario.

Además, falta completamente Secure Endpoint Service (sfc.exe) en el Administrador de tareas —> Servicios



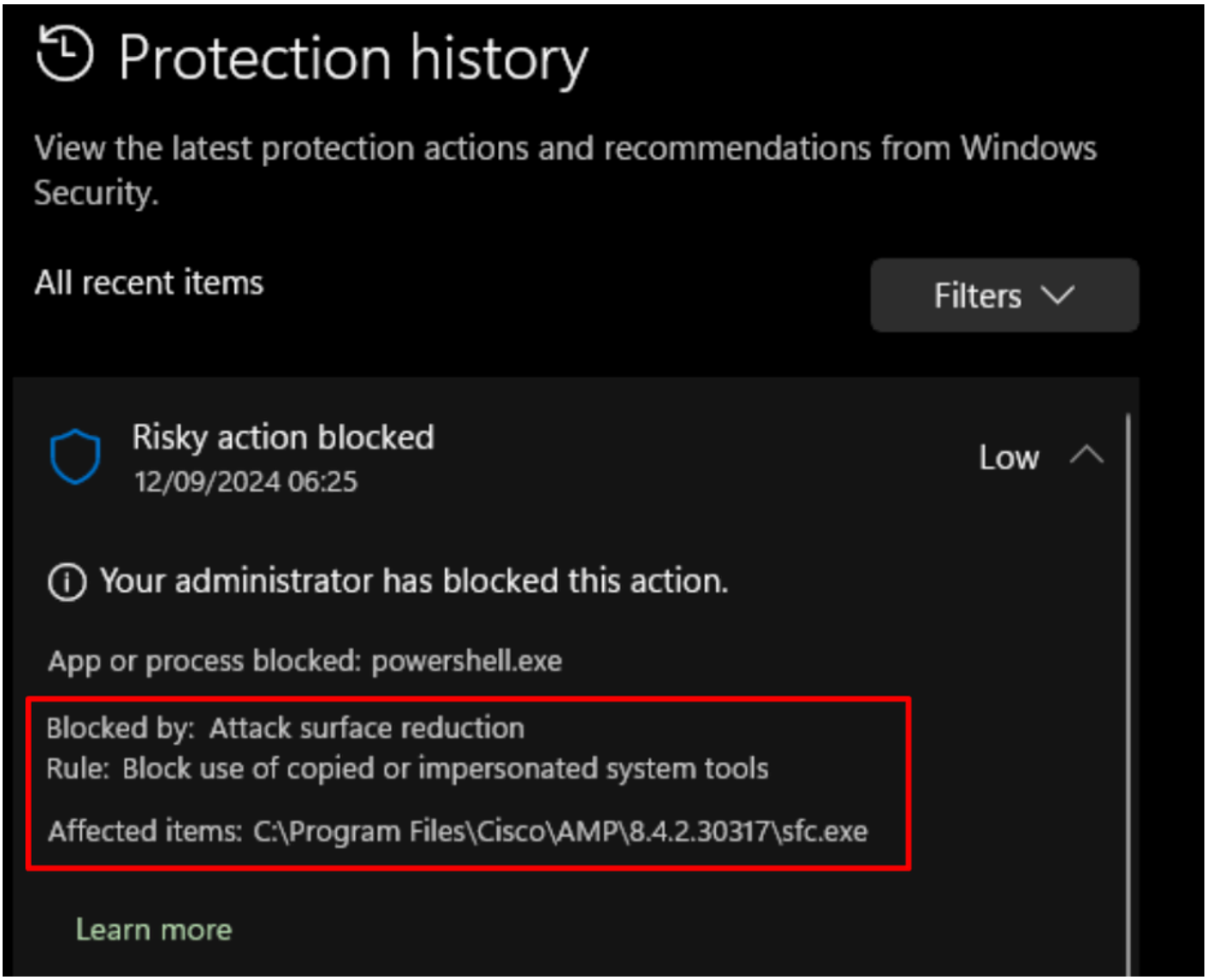
Indicador #3: Si navegamos hasta la ubicación de Cisco Secure Endpoint en C:\Program Files\Cisco\AMP\version e intentamos iniciar el servicio manualmente, se le deniega el acceso al permiso incluso para la cuenta de administrador local

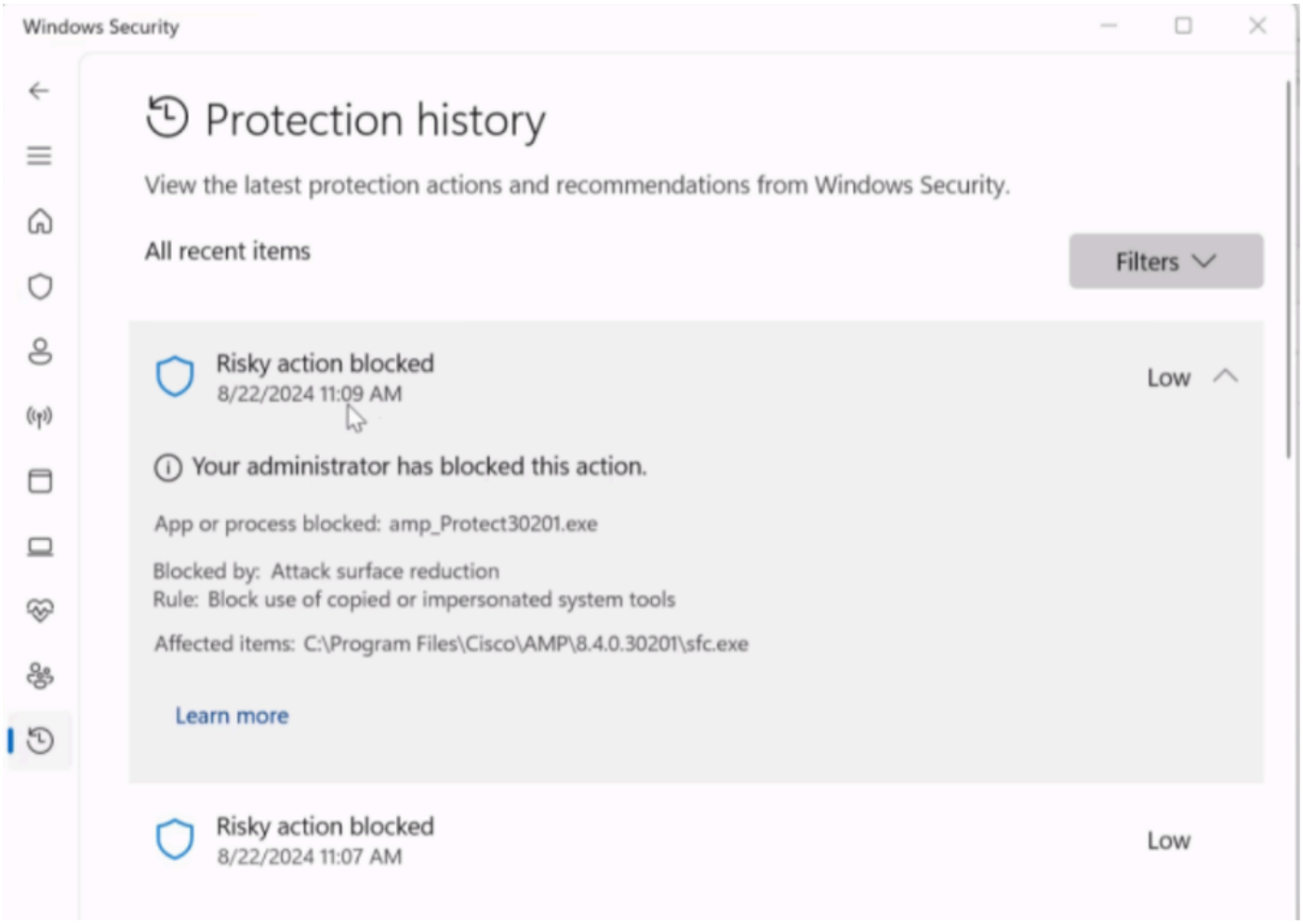


Indicador #4: Si investigamos immpro_install.log que es parte del paquete de diagnóstico, podemos observar una denegación de acceso similar que se parece a este resultado.

```
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
```

Indicador #5: Si navegamos bajo Seguridad de Windows y miramos en los registros del Historial de protección buscamos este tipo de mensajes de registro.


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



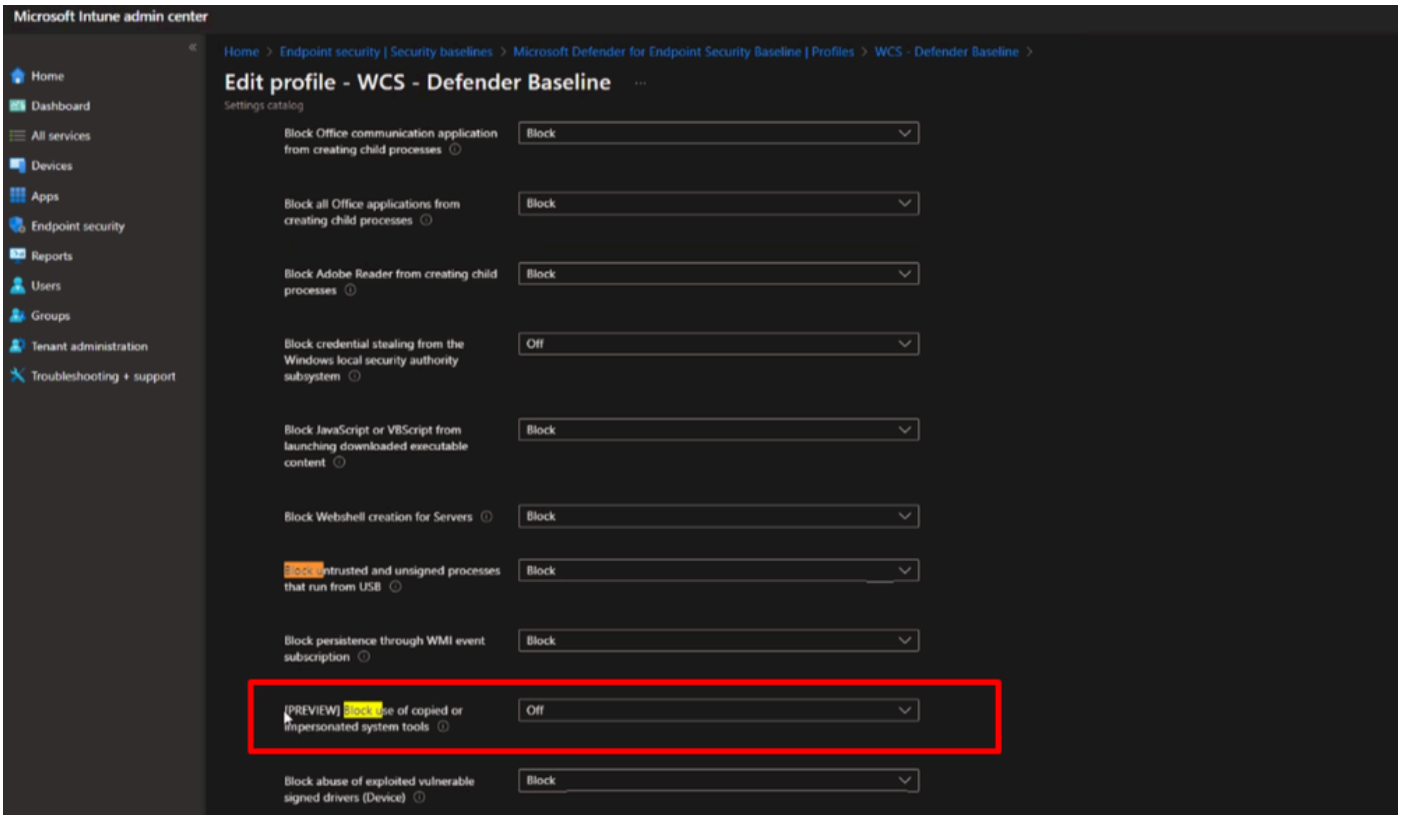
Todos estos son indicios de que el terminal seguro está siendo bloqueado por una aplicación de terceros. En este escenario, el problema se observó en los terminales administrados de Intune con reducción de superficie de ataque - BLOQUEO de uso de la función de sistema copiada o suplantada configurada incorrectamente o no configurada.

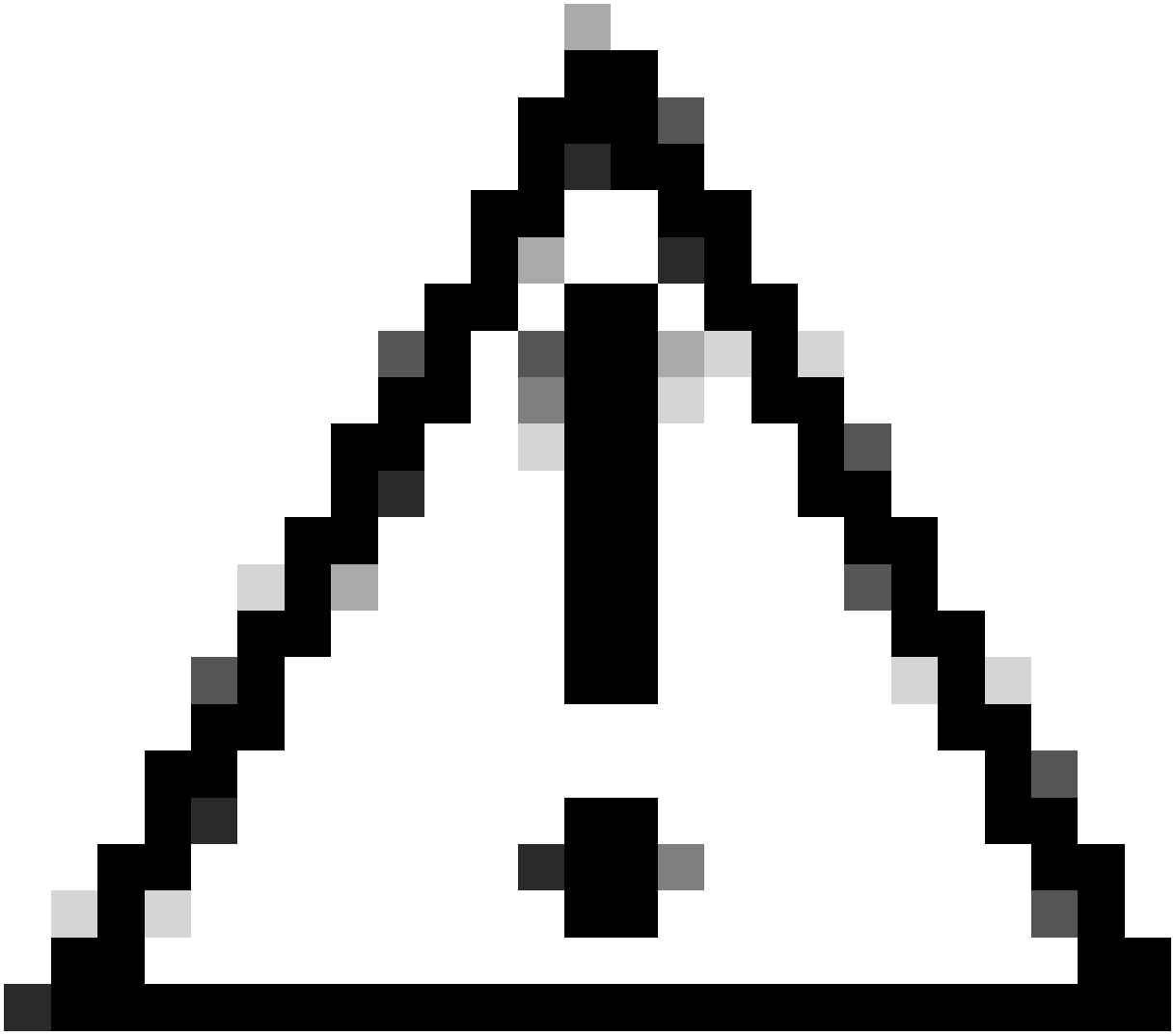
Solución Aternativa

Se recomienda consultar la configuración de esta función con el desarrollador de aplicaciones o consultar esta función más a fondo a través de esta base de conocimientos.

Para obtener una solución inmediata, podemos cambiar el terminal administrado de intune a una política menos restrictiva o desactivar esta función de forma explícita hasta que se realicen los pasos adecuados.

Esta es la configuración del portal de administración de Intune que se utilizó como medida temporal para restaurar la conectividad de terminal seguro.


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



Precaución: si experimenta este problema, debe iniciar la instalación completa debido a la falta de sfc.exe

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).