Endpoint seguro - Atualizações de conector sendo bloqueadas devido à redução da superfície de ataque da Microsoft

Contents

Introdução

Este documento descreve os problemas causados pelos blocos de redução de superfície do Microsoft Intune Attack usando o recurso de ferramentas do sistema copiadas ou personificadas em sistemas gerenciados pelo Microsoft Intune, o que, por sua vez, causa a falha das atualizações do Secure Endpoint.

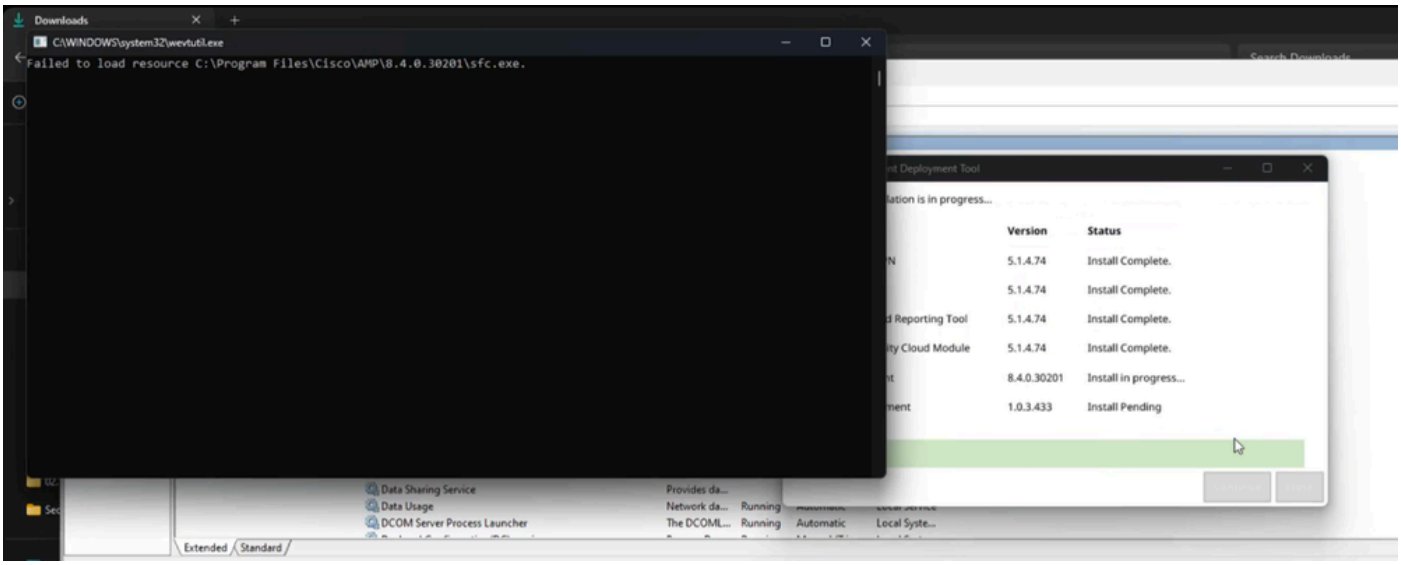
Consulte a documentação do recurso: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

Problema

Podemos ter problemas com as atualizações ou a instalação do Secure Endpoint, que é representada por esses erros e indicadores.

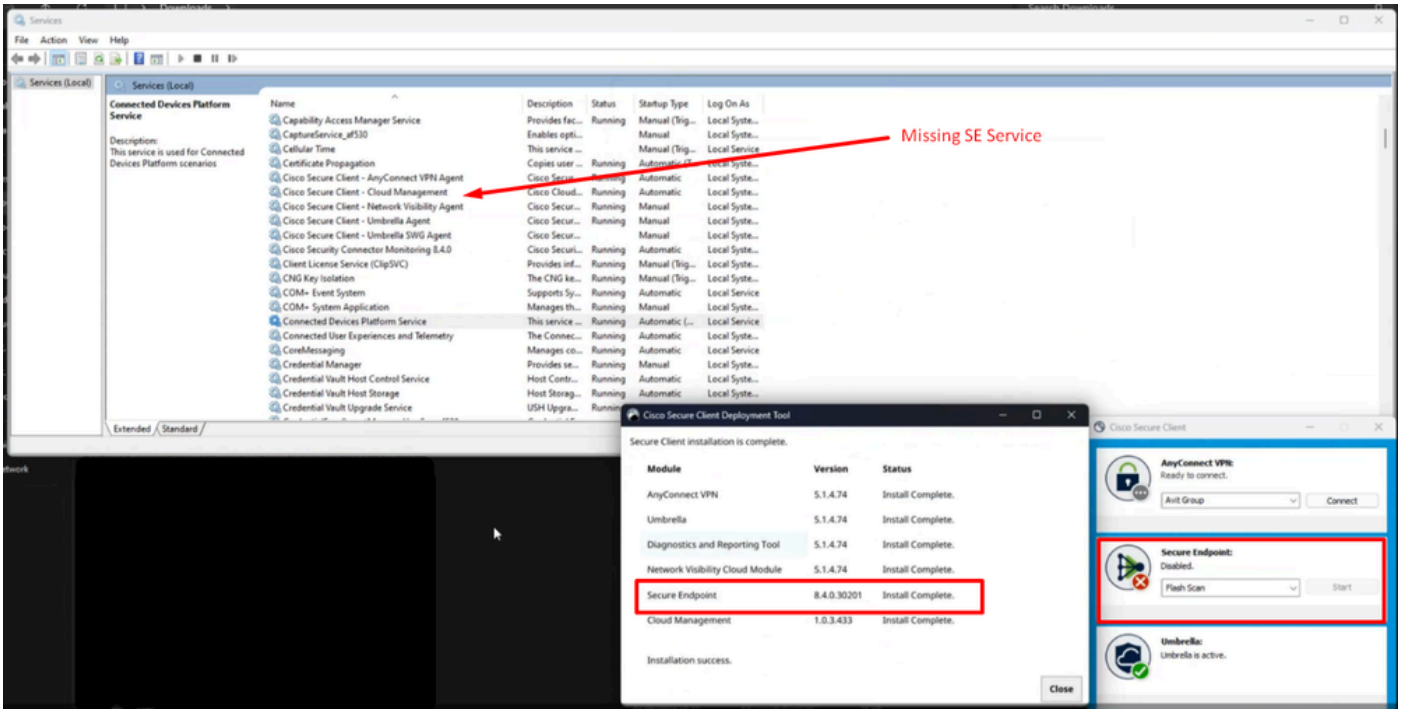
Há vários indicadores que podem ser usados para identificar se esse recurso está interferindo nas atualizações do Secure Endpoint.

#1 do indicador: Durante a implantação, observaremos essa janela pop-up no final da instalação. Observe que o pop-up é bem rápido e não há outra lembrança de nenhum erro após a conclusão da instalação.

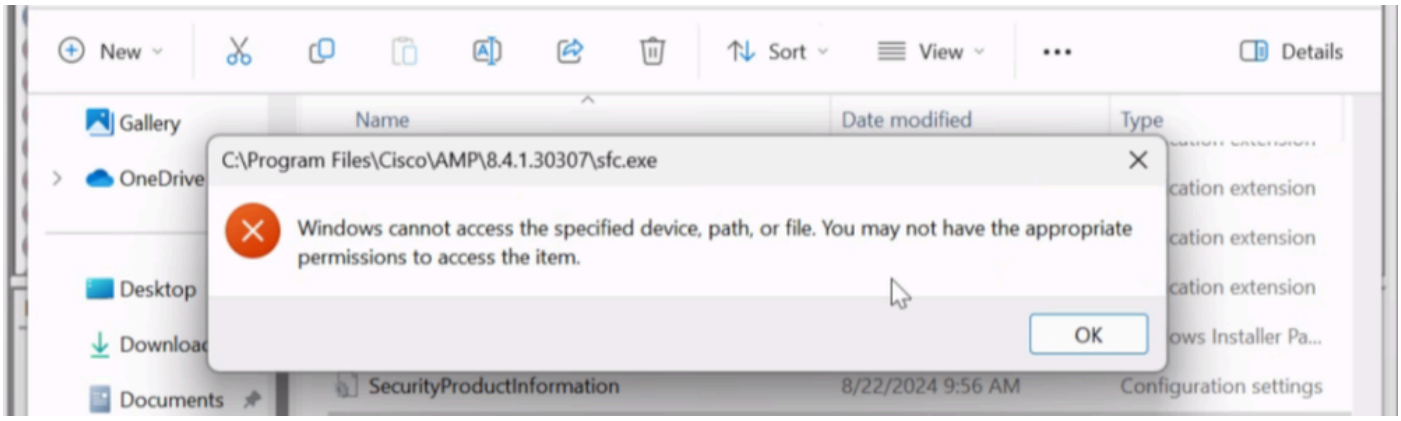


#2 do indicador: após a instalação, observe que o Secure Endpoint está no estado desabilitado na interface do usuário.

Além disso, o Secure Endpoint Service (sfc.exe) está completamente ausente no Gerenciador de tarefas — > Serviços



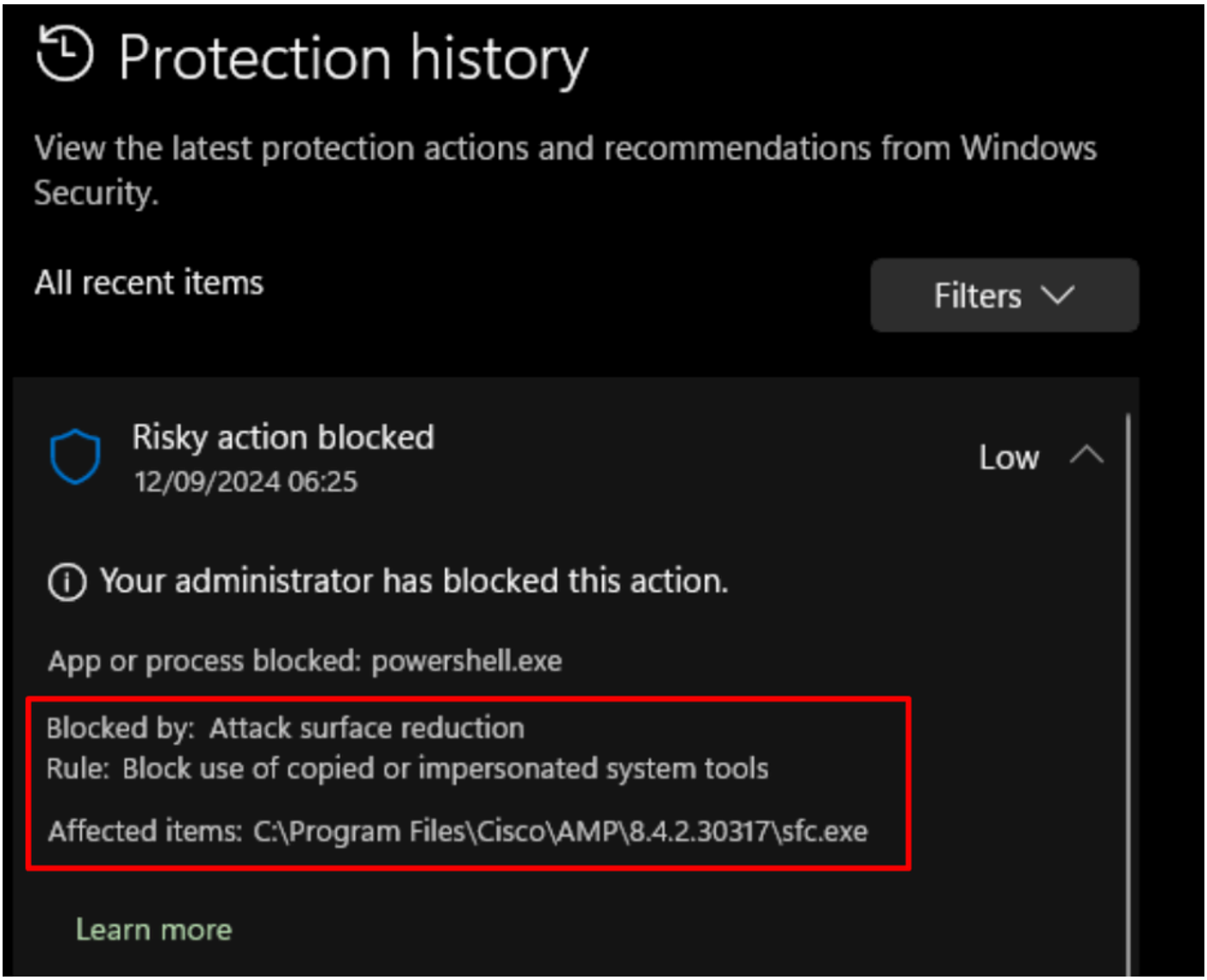
Indicador #3: Se navegarmos até o local do Cisco Secure Endpoint em C:\Program Files\Cisco\AMP\version e tentarmos iniciar o serviço manualmente, você terá acesso de permissão negado mesmo para a conta de administrador local

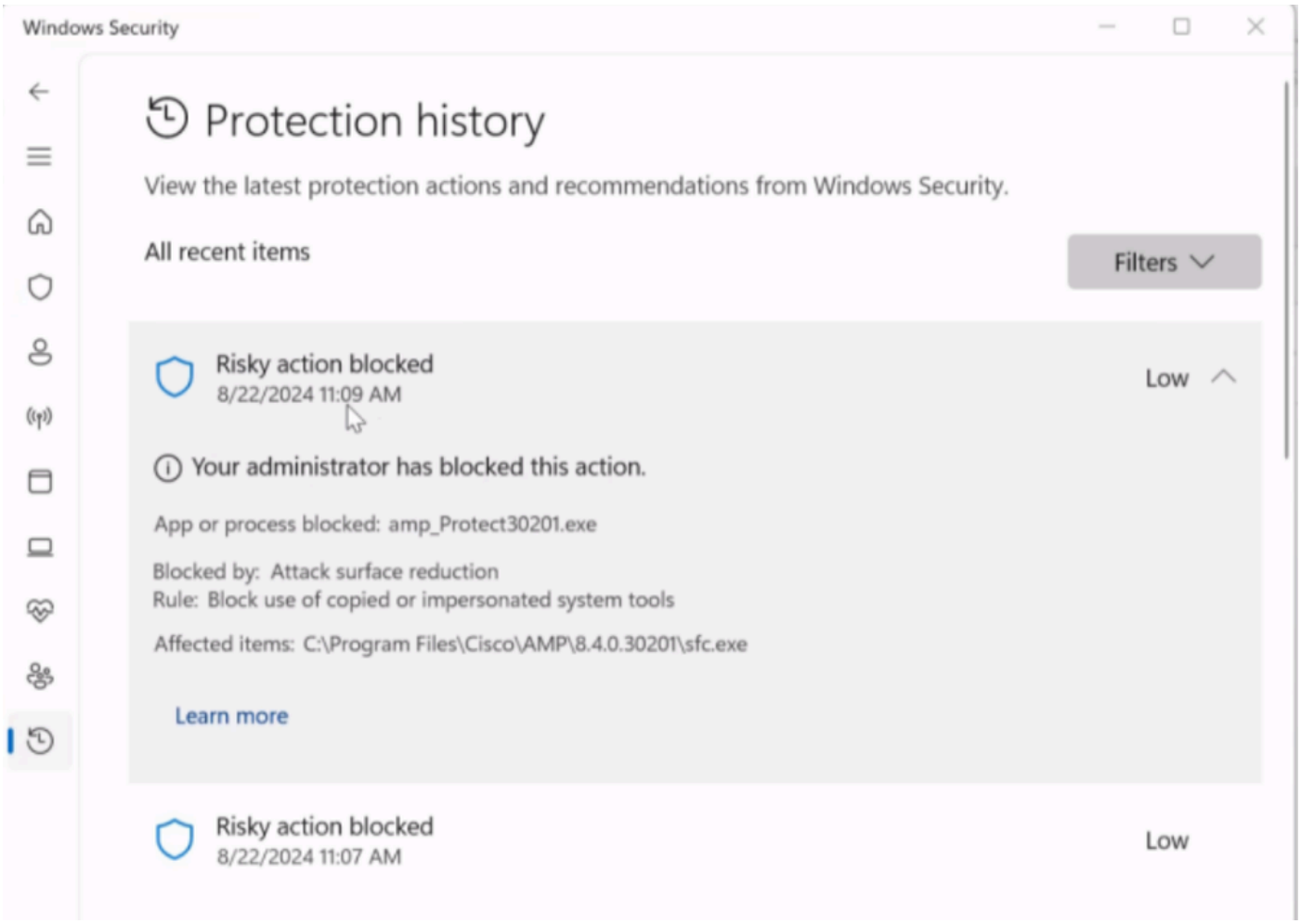


Indicador #4: Se investigarmos o immpro_install.log, que faz parte do pacote de diagnóstico, podemos observar uma negação de acesso semelhante a essa saída.

```
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: se navegarmos em Segurança do Windows e procurarmos os logs do Histórico de Proteção, procuraremos esses tipos de mensagens de log.


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



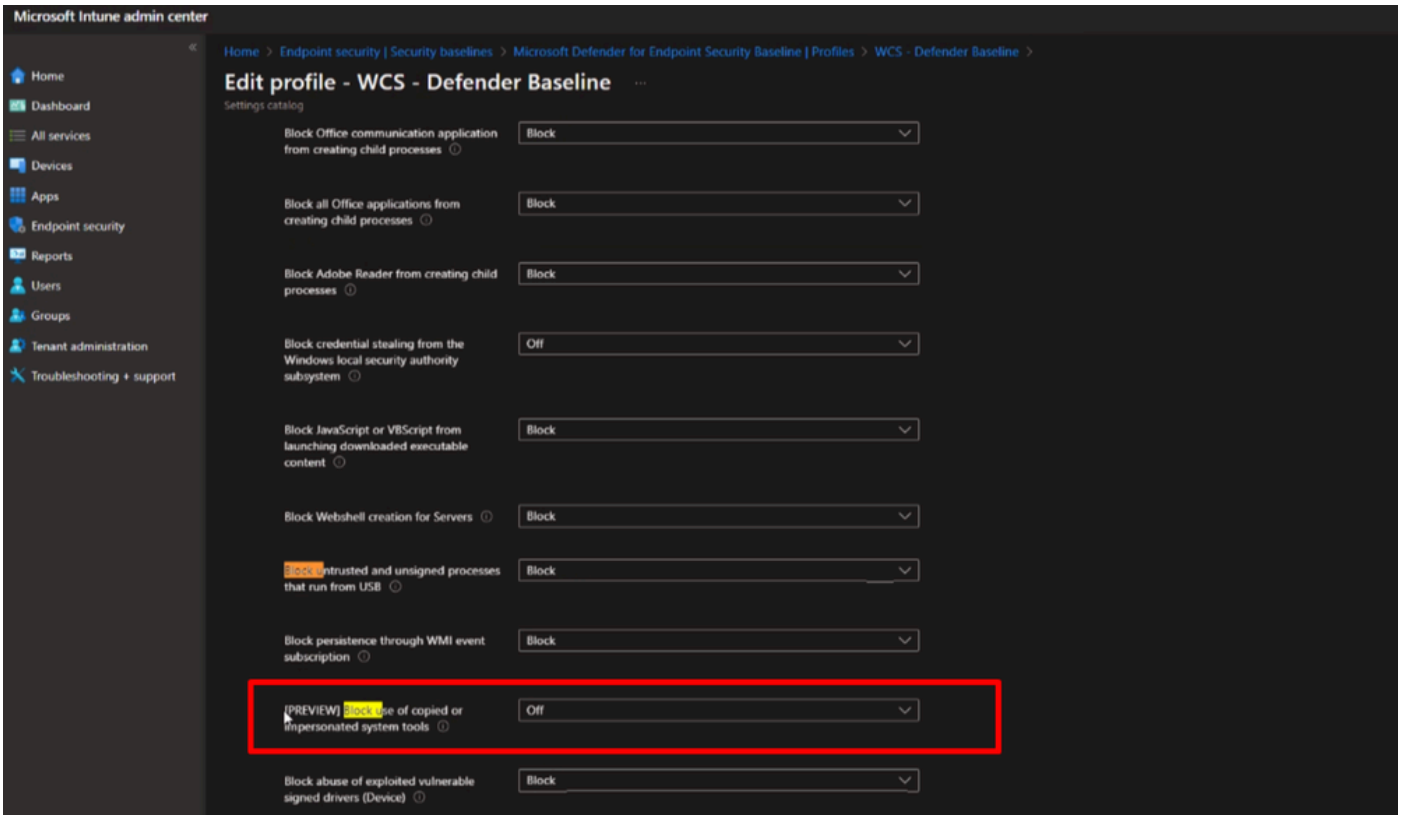
Tudo isso são indicações de que o Secure Endpoint está sendo bloqueado por aplicativos de terceiros. Neste cenário, o problema foi visto em endpoints gerenciados do Intune com redução da superfície de ataque configurada incorretamente ou não configurada - BLOQUEIE o uso do recurso do sistema copiado ou representado.

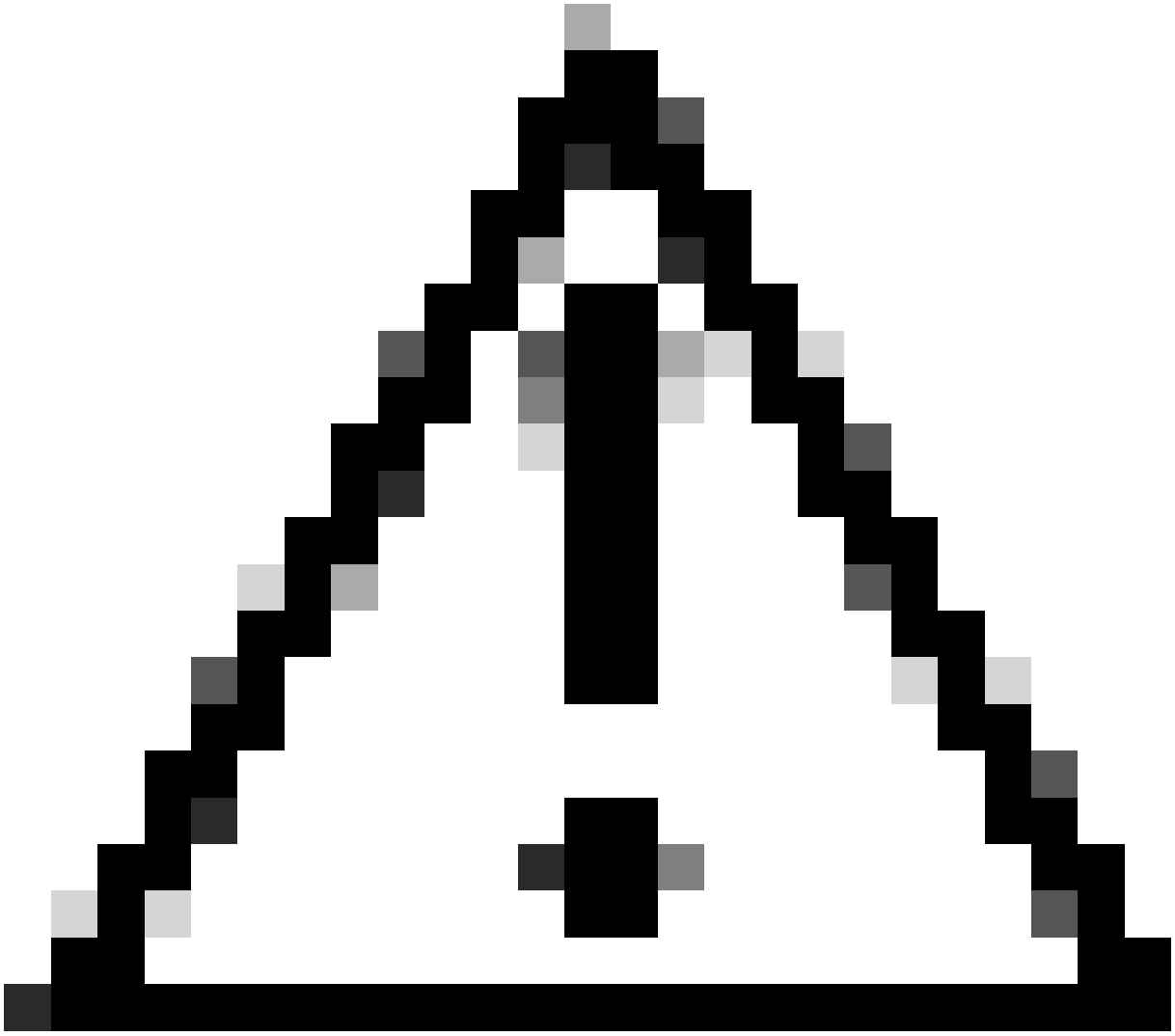
Solução

Recomenda-se consultar a configuração desse recurso com o desenvolvedor do aplicativo ou consultar esse recurso ainda mais por meio dessa base de dados de conhecimento.

Para remediação imediata, podemos mover nosso endpoint gerenciado no Intune para uma política menos restritiva ou desativar temporariamente esse recurso até que as etapas apropriadas sejam executadas.

Esta é a configuração no portal do administrador do Intune que foi usada como medida temporária para restaurar a conectividade do Ponto de Extremidade 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



Cuidado: se você tiver esse problema, inicie a instalação completa devido à ausência de sfc.exe

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.