

# Endpoint sicuro - Aggiornamenti dei connettori bloccati a causa della riduzione della superficie di attacco Microsoft

## Sommario

---

[Introduzione](#)

[Problema](#)

[Soluzione alternativa](#)

---

## Introduzione

In questo documento vengono descritti i problemi causati dai blocchi di riduzione della superficie di attacco di Microsoft Intune che utilizzano la funzionalità degli strumenti di sistema copiati o rappresentati nei sistemi gestiti da Microsoft Intune, che a sua volta causa il mancato completamento degli aggiornamenti di Secure Endpoint.

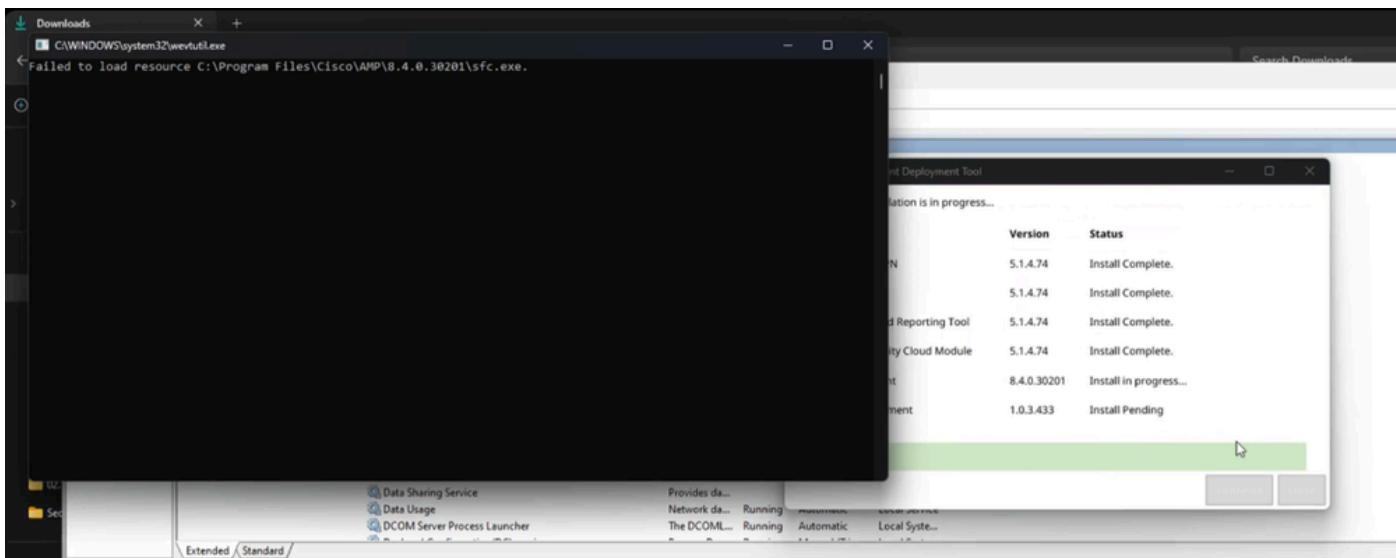
Fare riferimento alla documentazione relativa alle funzionalità: <https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction>

## Problema

Possiamo riscontrare problemi con gli aggiornamenti o l'installazione di Secure Endpoint, che sono rappresentati da questi errori e indicatori.

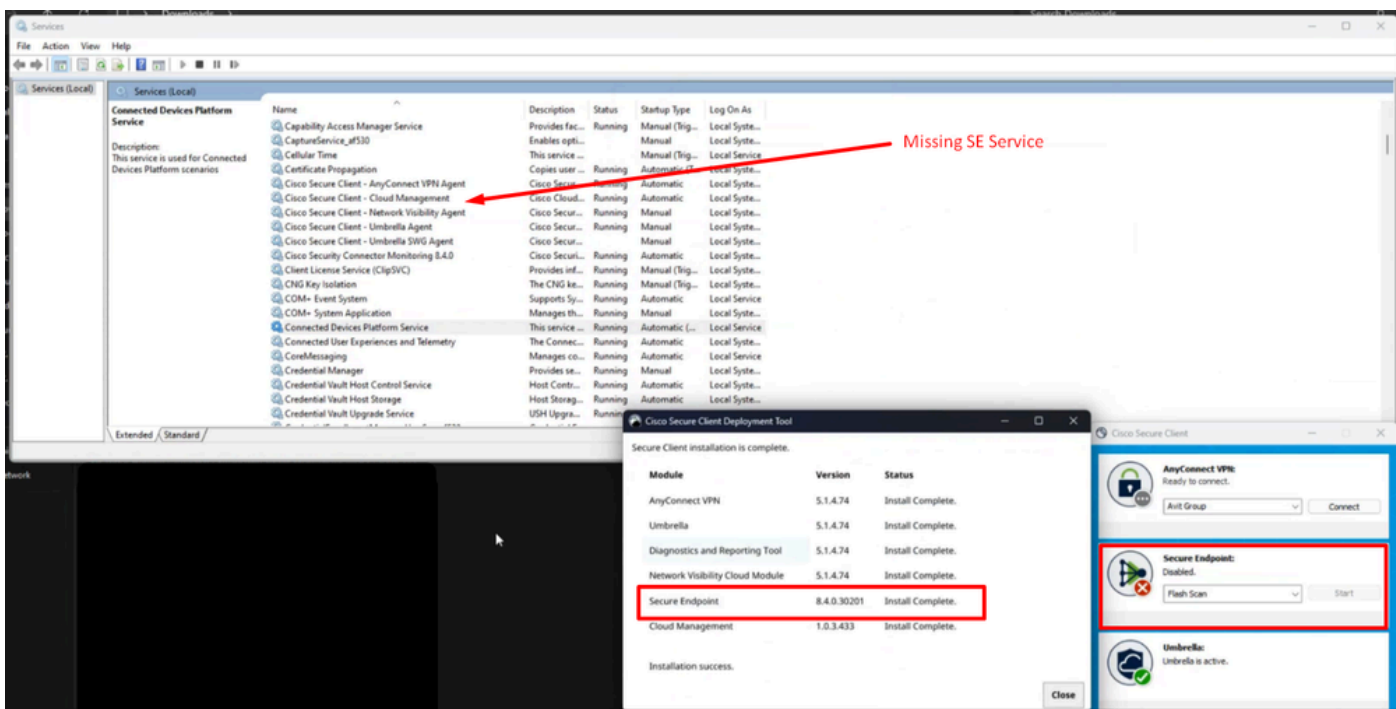
Per stabilire se questa funzionalità interferisce con gli aggiornamenti degli endpoint sicuri, è possibile utilizzare diversi indicatori.

Indicatore 1: durante la distribuzione, verrà visualizzata questa finestra popup al termine dell'installazione. Notare che il popup è abbastanza rapido e non c'è nessun altro richiamo di errori una volta completata l'installazione.

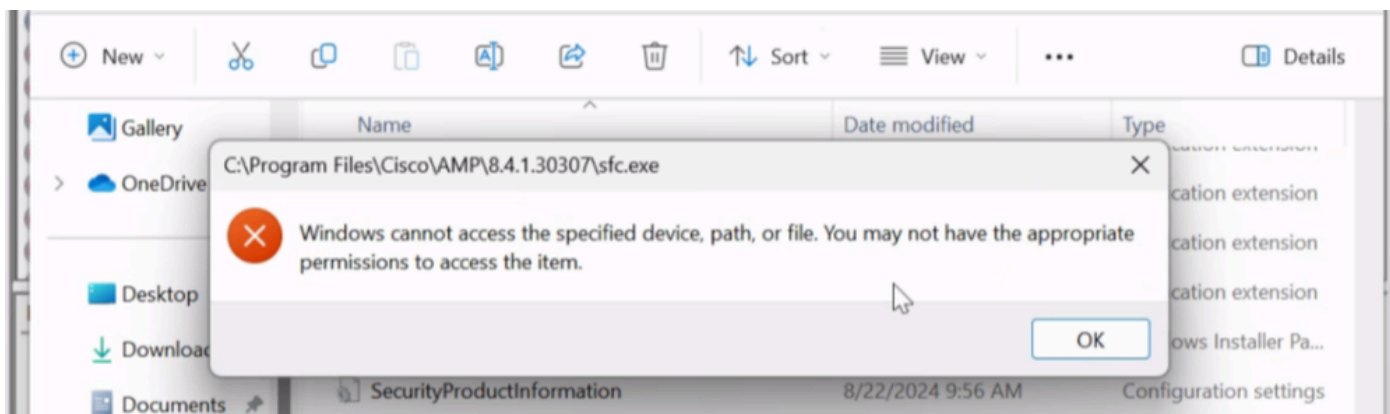


Indicatore n. 2: dopo l'installazione, notare che lo stato dell'endpoint protetto è disabilitato nell'interfaccia utente.

Inoltre, il servizio Secure Endpoint Service (sfc.exe) è completamente mancante in Task Manager —> Servizi



Indicatore 3: se si passa alla posizione di Cisco Secure Endpoint in C:\Program Files\Cisco\AMP\version e si tenta di avviare il servizio manualmente, si ottiene l'autorizzazione di accesso negata anche per l'account admin locale



Indicatore n.4: Se esaminiamo immpro\_install.log che fa parte del pacchetto diagnostico possiamo osservare un simile rifiuto di accesso che è simile a questo output.

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_INSTALL
```

Indicatore 5: se in Protezione di Windows si passa a Cronologia protezione cercare questi tipi di messaggi di 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.

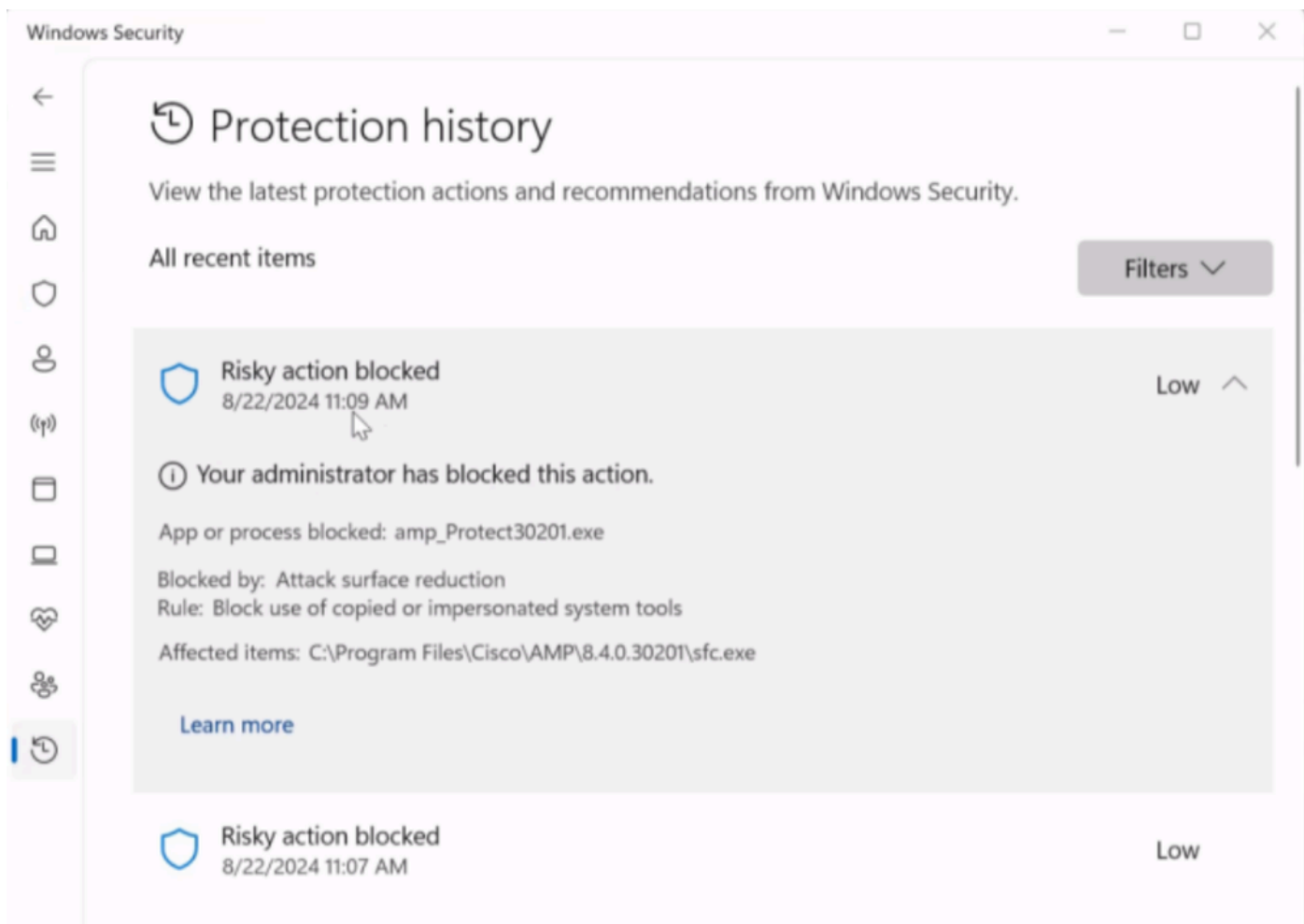
App or process blocked: powershell.exe

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](#)



Tutto ciò indica che l'endpoint sicuro è bloccato da un'applicazione di terze parti. In questo scenario, il problema è stato rilevato sugli endpoint gestiti di Intune con la riduzione della superficie di attacco configurata in modo errato o non configurata. Blocca l'uso della funzionalità di sistema copiata o rappresentata.

## Soluzione alternativa

Si consiglia di consultare la configurazione di questa funzionalità con lo sviluppatore dell'applicazione o di consultare ulteriormente questa funzionalità tramite la [knowledge base](#).

Per una correzione immediata, è possibile spostare l'endpoint gestito in una configurazione meno restrittiva oppure disattivare temporaneamente questa funzionalità in modo esplicito fino a quando non vengono eseguiti i passaggi appropriati.

Questa è l'impostazione del portale di amministrazione di Intune utilizzata come misura temporanea per ripristinare la connettività dell'endpoint sicuro.

## Edit profile - WCS - Defender Baseline

Settings catalog

Block Office communication application from creating child processes

Block all Office applications from creating child processes

Block Adobe Reader from creating child processes

Block credential stealing from the Windows local security authority subsystem

Block JavaScript or VBScript from launching downloaded executable content

Block Webshell creation for Servers

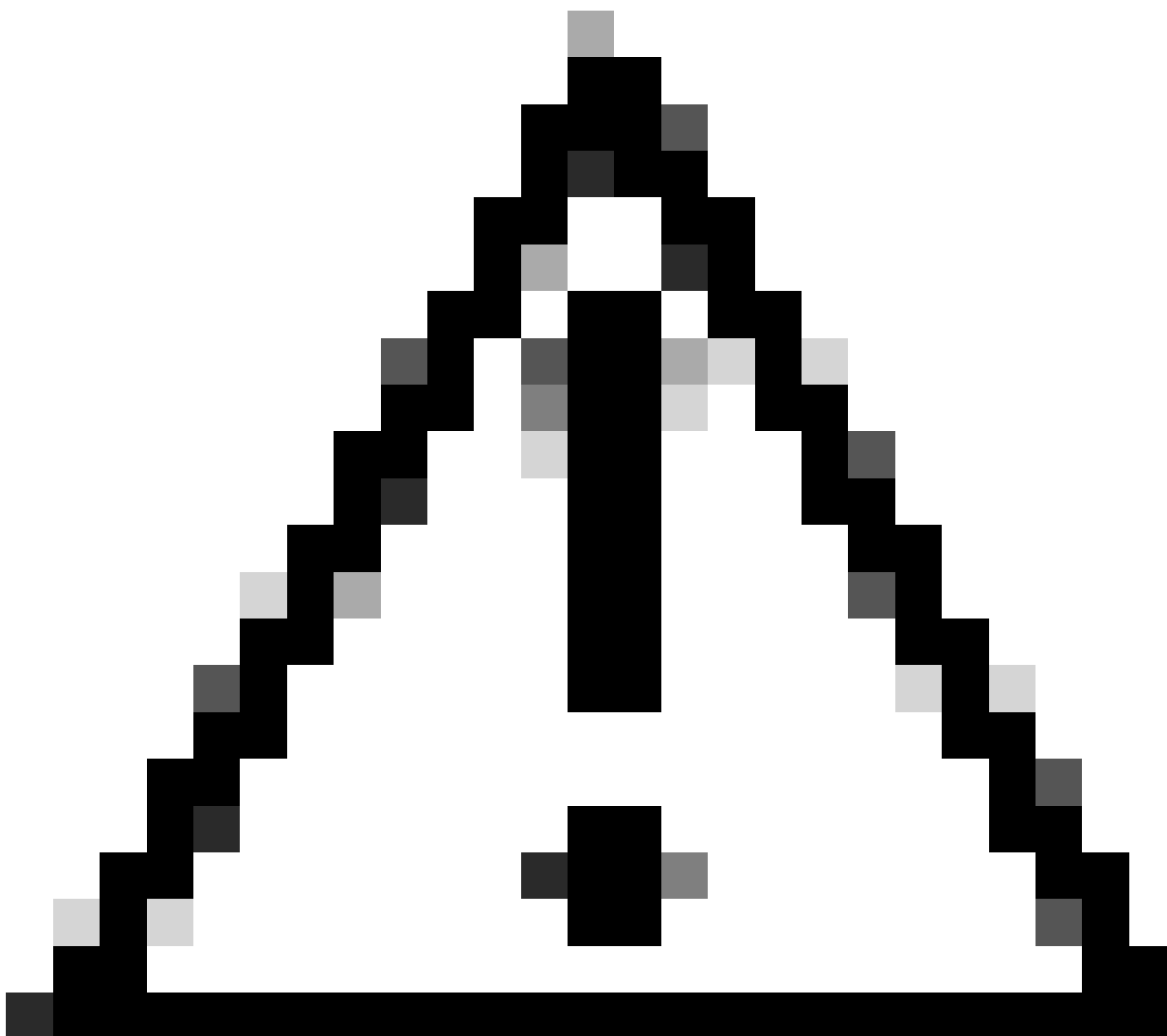
Block trusted and unsigned processes that run from USB

Block persistence through WMI event subscription

**[PREVIEW]** Block use of copied or impersonated system tools

Block abuse of exploited vulnerable signed drivers (Device)

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support



Attenzione: se si verifica questo problema, è necessario avviare l'installazione completa perché sfc.exe mancante

---

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).