Secure Endpoint - Connector Updates Being Blocked Due to Microsoft Attack Surface Reduction

Contents

Introduction

This document describes issues caused by **Microsoft Intune Attack surface reduction blocks using copied or impersonated system tools** feature on systems managed by Microsoft Intune which in turn causes Secure Endpoint updates to fail.

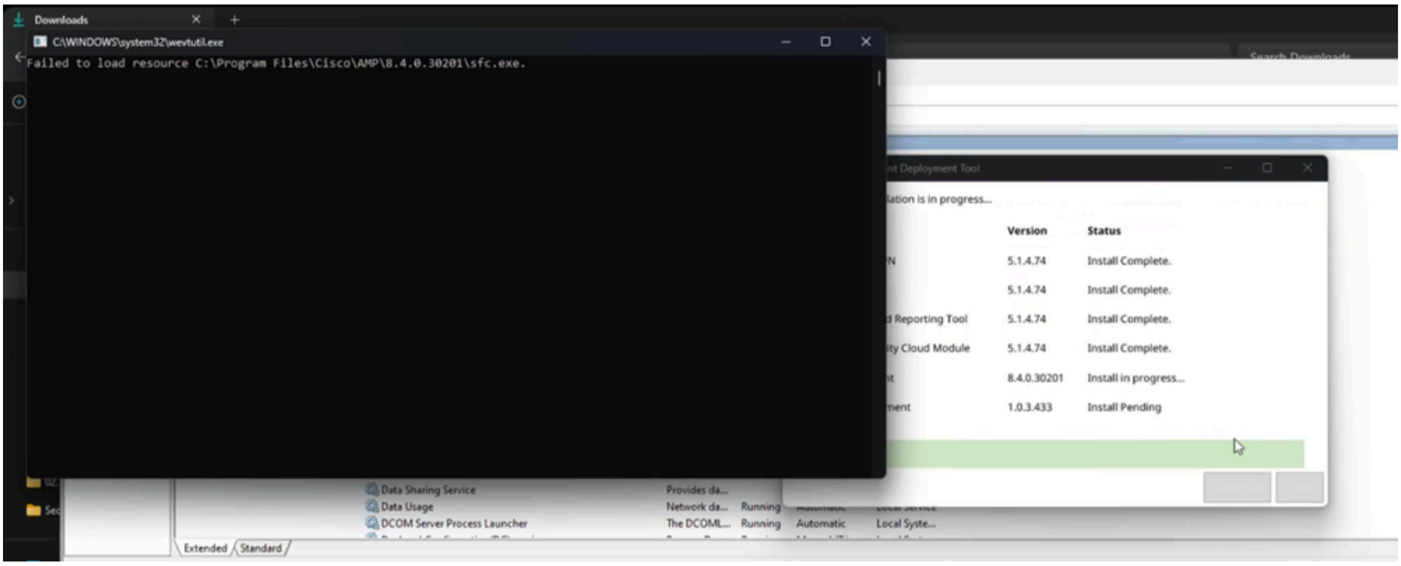
Please refer to the feature documentation: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction

Problem

We can experience issues with Secure Endpoint upgrades or installation which is represented by these errors and indicators.

There are various indicators that can be used to identify that this feature interfering with Secure Endpoint updates.

Indicator #1: During deployment, we going to notice this pop-up window at the end of the installation. Please note that the pop-up is fairly quick and there is no other recollection of any error once the installation is completed.



```
Failed to load resource C:\Program Files\Cisco\AMP\8.4.0.30201\sfc.exe.
```

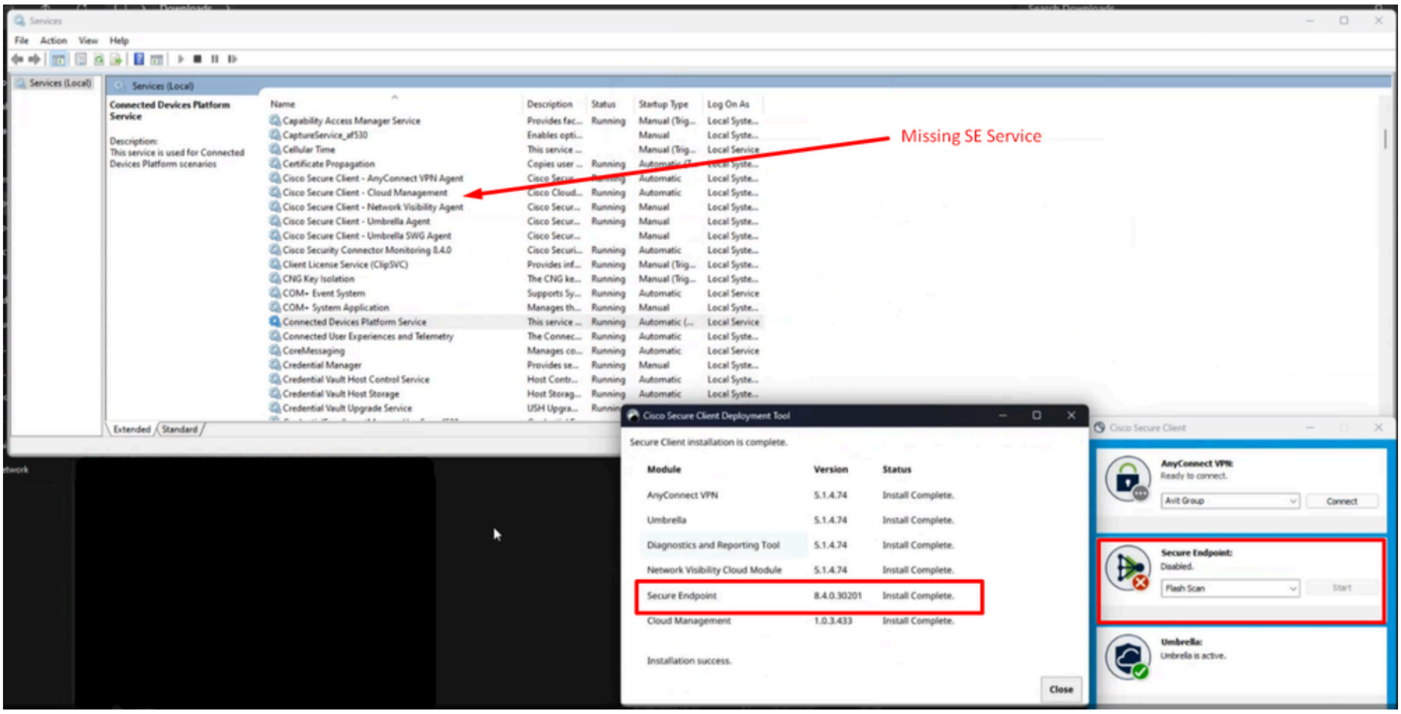
lation is in progress...

	Version	Status
N	5.1.4.74	Install Complete.
	5.1.4.74	Install Complete.
d Reporting Tool	5.1.4.74	Install Complete.
ity Cloud Module	5.1.4.74	Install Complete.
t	8.4.0.30201	Install in progress...
ment	1.0.3.433	Install Pending

Data Sharing Service	Provides da...			
Data Usage	Network da...	Running		
DCOM Server Process Launcher	The DCOML...	Running	Automatic	Local Syste...

Indicator #2: After the installation, notice that Secure Endpoint is in disabled state in the UI.

Also, completely missing Secure Endpoint Service *(sfc.exe)* in the **Task Manager -- > Services**



Connected Devices Platform Service

Description:
This service is used for Connected Devices Platform scenarios

Name	Description	Status	Startup Type	Log On As
Capability Access Manager Service	Provides fac...	Running	Manual (Trig...	Local Syste...
CaptureService_af530	Enables opti...		Manual	Local Syste...
Cellular Time	This service ...		Manual (Trig...	Local Service
Certificate Propagation	Copies user ...	Running	Automatic (T...	Local Syste...
Cisco Secure Client - AnyConnect VPN Agent	Cisco Secur...	Running	Automatic	Local Syste...
Cisco Secure Client - Cloud Management	Cisco Cloud...	Running	Automatic	Local Syste...
Cisco Secure Client - Network Visibility Agent	Cisco Secur...	Running	Manual	Local Syste...
Cisco Secure Client - Umbrella Agent	Cisco Secur...	Running	Manual	Local Syste...
Cisco Secure Client - Umbrella SWG Agent	Cisco Secur...		Manual	Local Syste...
Cisco Security Connector Monitoring 8.4.0	Cisco Securi...	Running	Automatic	Local Syste...
Client License Service (ClipSVC)	Provides inf...	Running	Manual (Trig...	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local Syste...
Connected Devices Platform Service	This service ...	Running	Automatic (...	Local Service
Connected User Experiences and Telemetry	The Connec...	Running	Automatic	Local Syste...
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...	Running	Manual	Local Syste...
Credential Vault Host Control Service	Host Contr...	Running	Automatic	Local Syste...
Credential Vault Host Storage	Host Storag...	Running	Automatic	Local Syste...
Credential Vault Upgrade Service	USH Upgra...	Runnin		

Cisco Secure Client Deployment Tool

Secure Client installation is complete.

Module	Version	Status
AnyConnect VPN	5.1.4.74	Install Complete.
Umbrella	5.1.4.74	Install Complete.
Diagnostics and Reporting Tool	5.1.4.74	Install Complete.
Network Visibility Cloud Module	5.1.4.74	Install Complete.
Secure Endpoint	8.4.0.30201	Install Complete.
Cloud Management	1.0.3.433	Install Complete.

Installation success.

Close

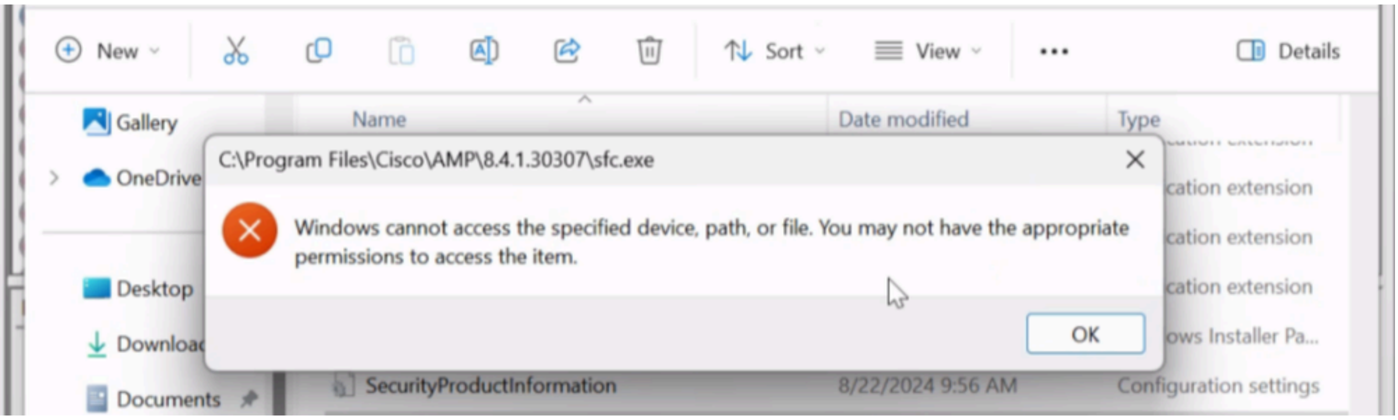
Cisco Secure Client

AnyConnect VPN:
Ready to connect.
Avit Group
Connect

Secure Endpoint:
Disabled.
Flash Scan
Start

Umbrella:
Umbrella is active.

Indicator #3: If we navigate to the location of Cisco Secure Endpoint under **C:\Program Files\Cisco\AMP\*version*** and try to start the service manually, you get permission access denied even for the **local admin** account



C:\Program Files\Cisco\AMP\8.4.1.30307\sfc.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

OK

Indicator #4: If we investigate **immpro_install.log** which is part of the diagnostic bundle we can observe a similar denial of access that look similar to this output.

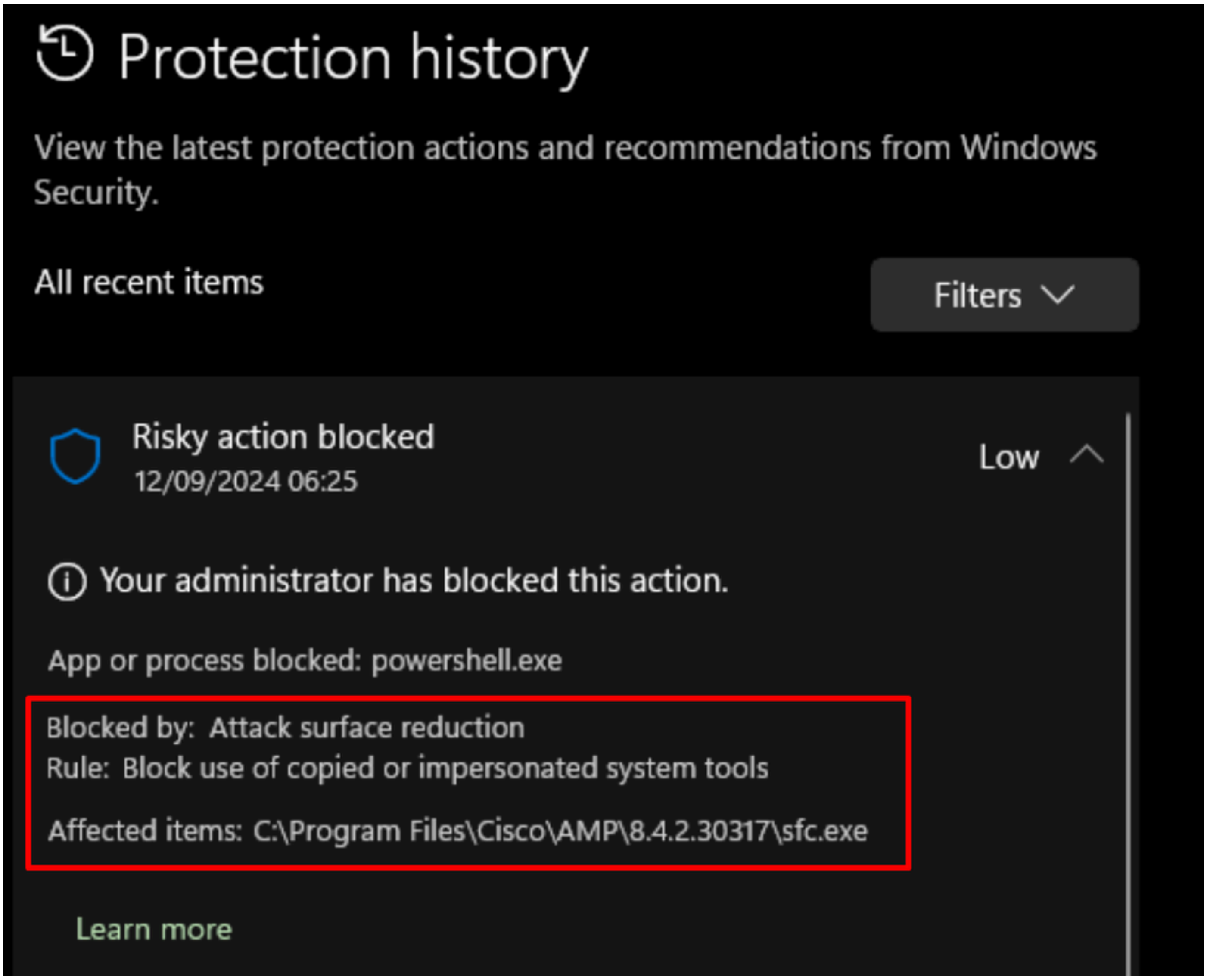
```
Example #1:
```

```
(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_INSTAL
```

Indicator #5: If we navigate under **Windows Security** and look in to the **Protection History logs** look for these type of log messages.



Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

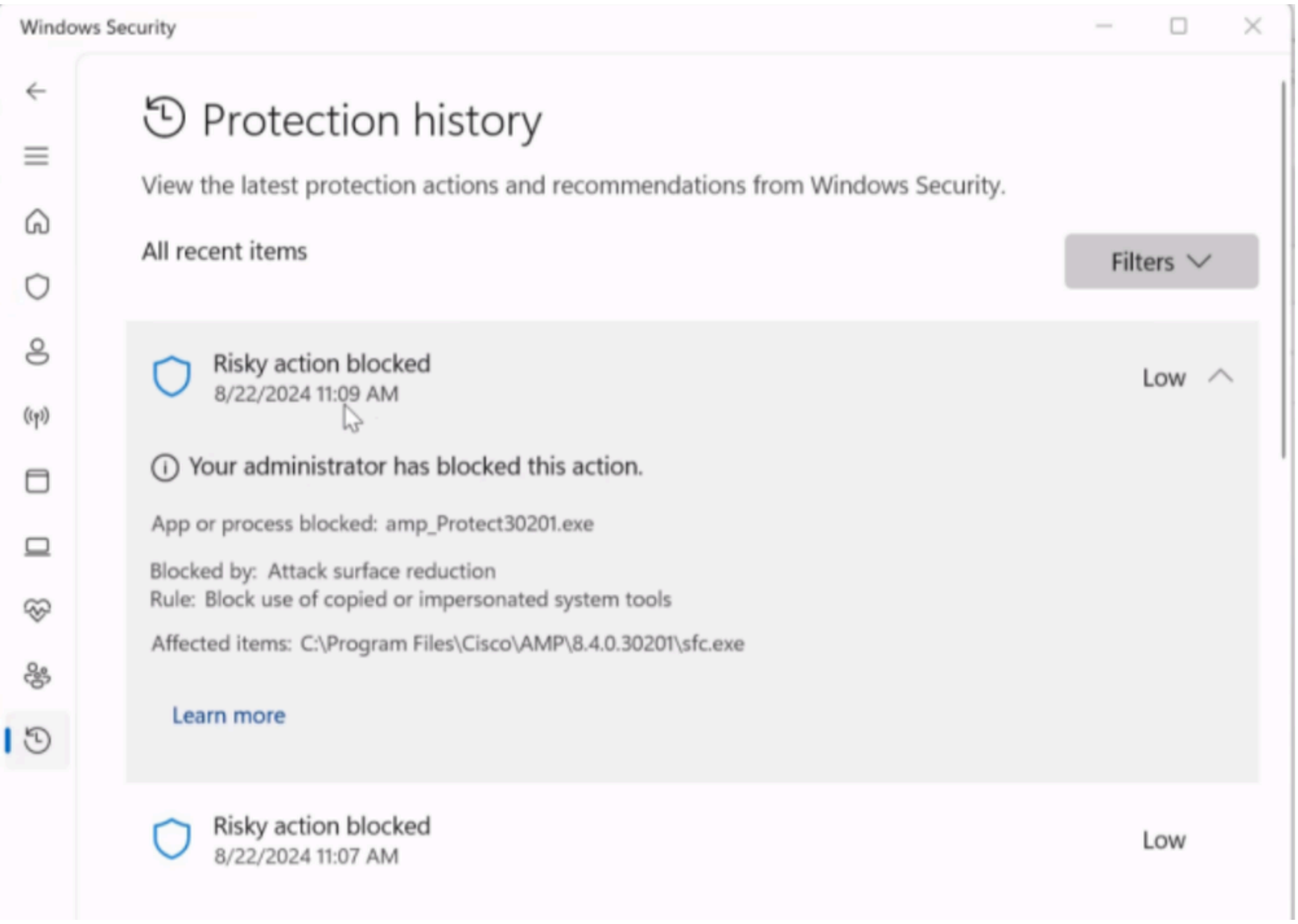
Risky action blocked
12/09/2024 06:25

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



Windows Security

Protection history

View the latest protection actions and recommendations from Windows Security.

All recent items

Risky action blocked
8/22/2024 11:09 AM
Low

Your administrator has blocked this action.

App or process blocked: amp_Protect30201.exe

Blocked by: Attack surface reduction
Rule: Block use of copied or impersonated system tools

Affected items: C:\Program Files\Cisco\AMP\8.4.0.30201\sfc.exe

Risky action blocked
8/22/2024 11:07 AM
Low

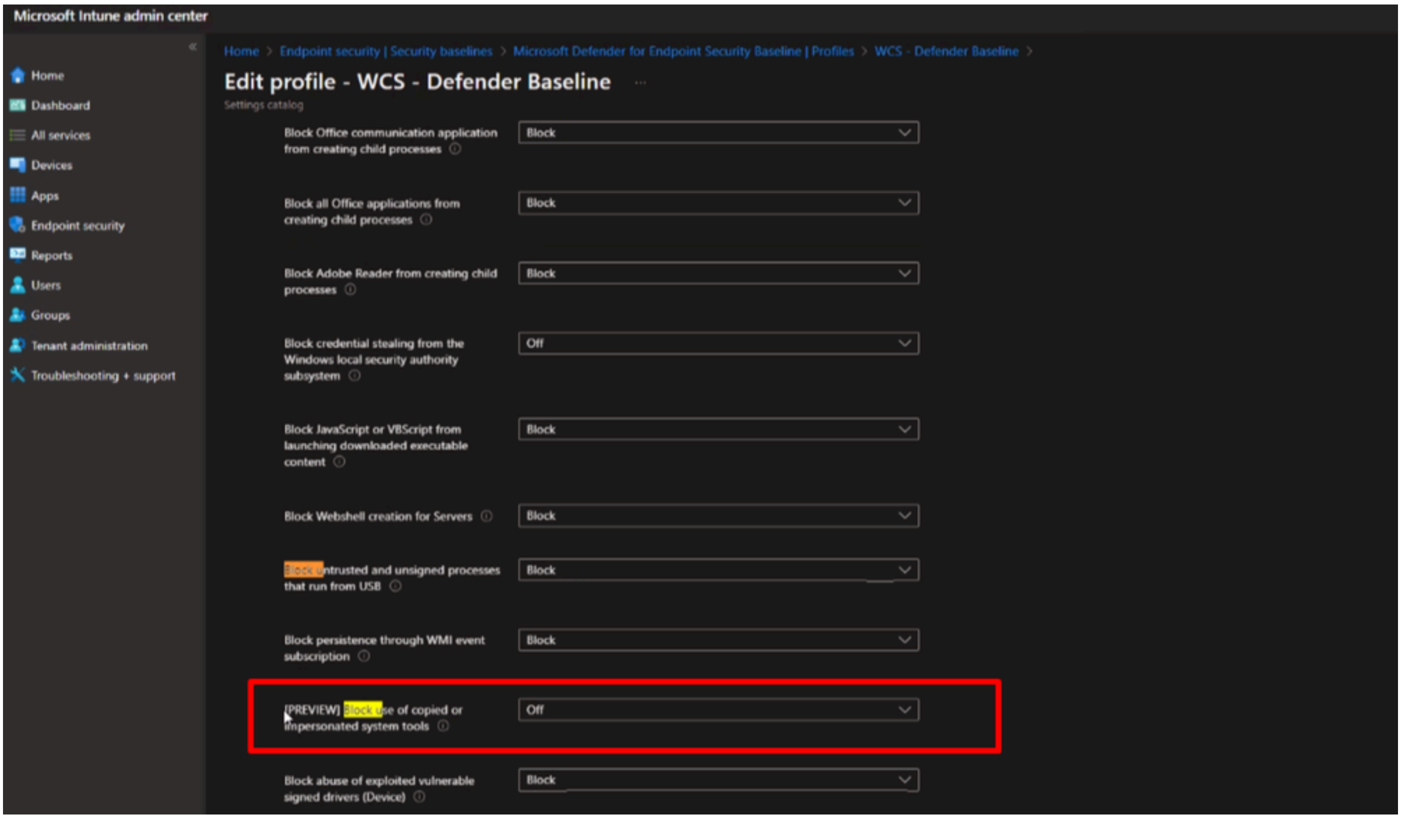
All these are indications that the Secure Endpoint is being blocked by 3rd party application. In this scenario, the issue was seen on Intune managed endpoints with either incorrectly configured or not configured **Attack surface reduction - BLOCK use of copied or impersonated system** feature.

Workaround

It is advised to consult configuration for this feature with the application developer or consult this feature further through this knowledge base.

For immediate remediation, we can either move our managed endpoint in intune to a less restrictive policy or temporary turn this feature explicitly off until proper steps are made.

This is the setting under Intune admin portal that was used as temporary measure to restore Secure Endpoint connectivity.


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

Caution: If you experience this issue, you must initiate full install due to missing **sfc.exe**