Mitigating Performance Impacts of Cisco Secure Endpoint

Optimizing Endpoint Efficiency While Maintaining Security

Andrew Koelbel
Security Technical Consulting Engineer

cisco Live !

Session ID: TACSEC-2022

01 Introduction
02 High Resource Examples
03 Policy Guidance
04 Advanced Policy Settings
05 Exclusions Overview
06 Collecting Debug Bundles
07 Leveraging Debug Bundles
08 Creating Exclusions
08 Q&A

About Me

- Started in Cisco Advanced Services (AS)
  - Recreates
  - Device configuration
- Advanced Threat Solutions TAC team 2 years
- Secure Endpoint, XDR, and Secure Malware Analytics SME
- Deliver training and develop documentation resources
- CCNA and DevNet Associate
- NBA & NFL Fan
- Traveler

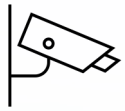
You can’t have a lot of great things without also having a lot of pain

Ray Dalio

Founder of Bridgewater Associates Hedge Fund

The Nature of Endpoint Detection and Response (EDR)

File Scans

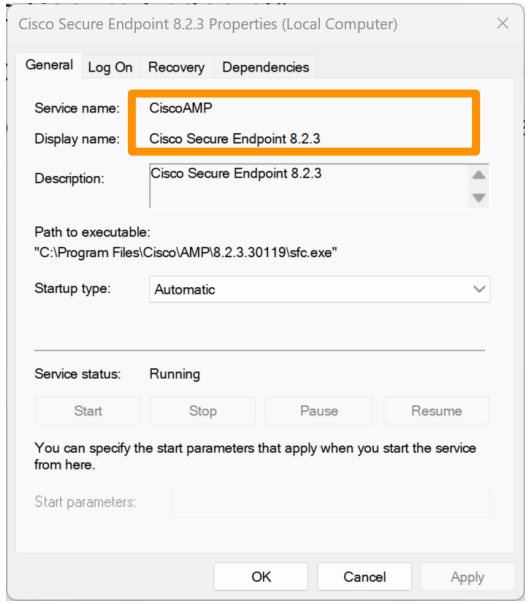


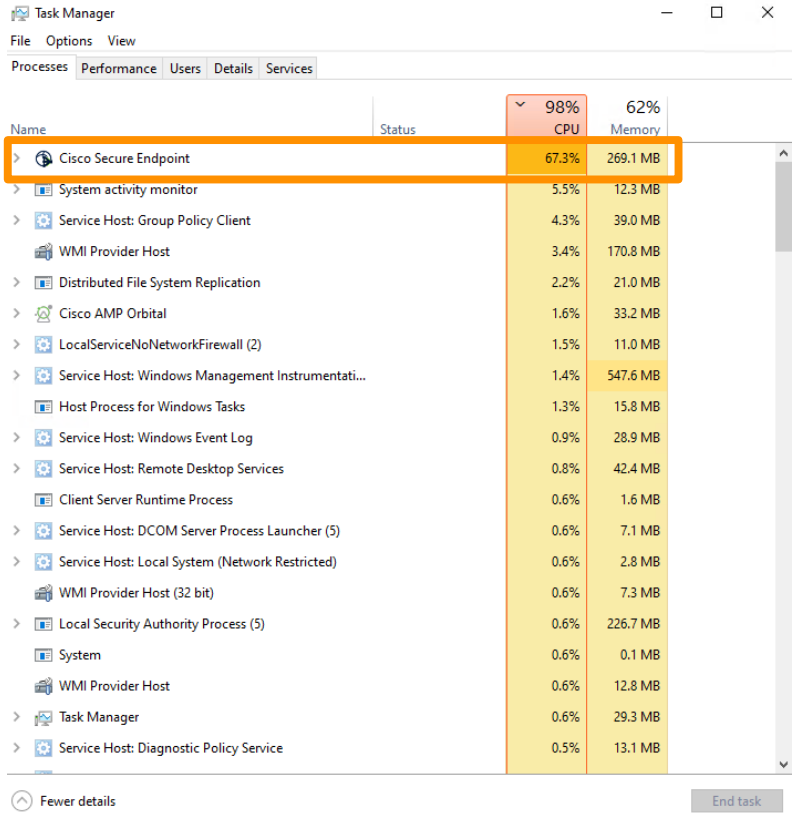
Process injections

System activity

What Does High Resource Usage Look Like On Windows?

- Process entitled “Cisco Secure Endpoint”
  - Links to sfc.exe





What Does High Resource Usage Look Like on MacOS & Linux?

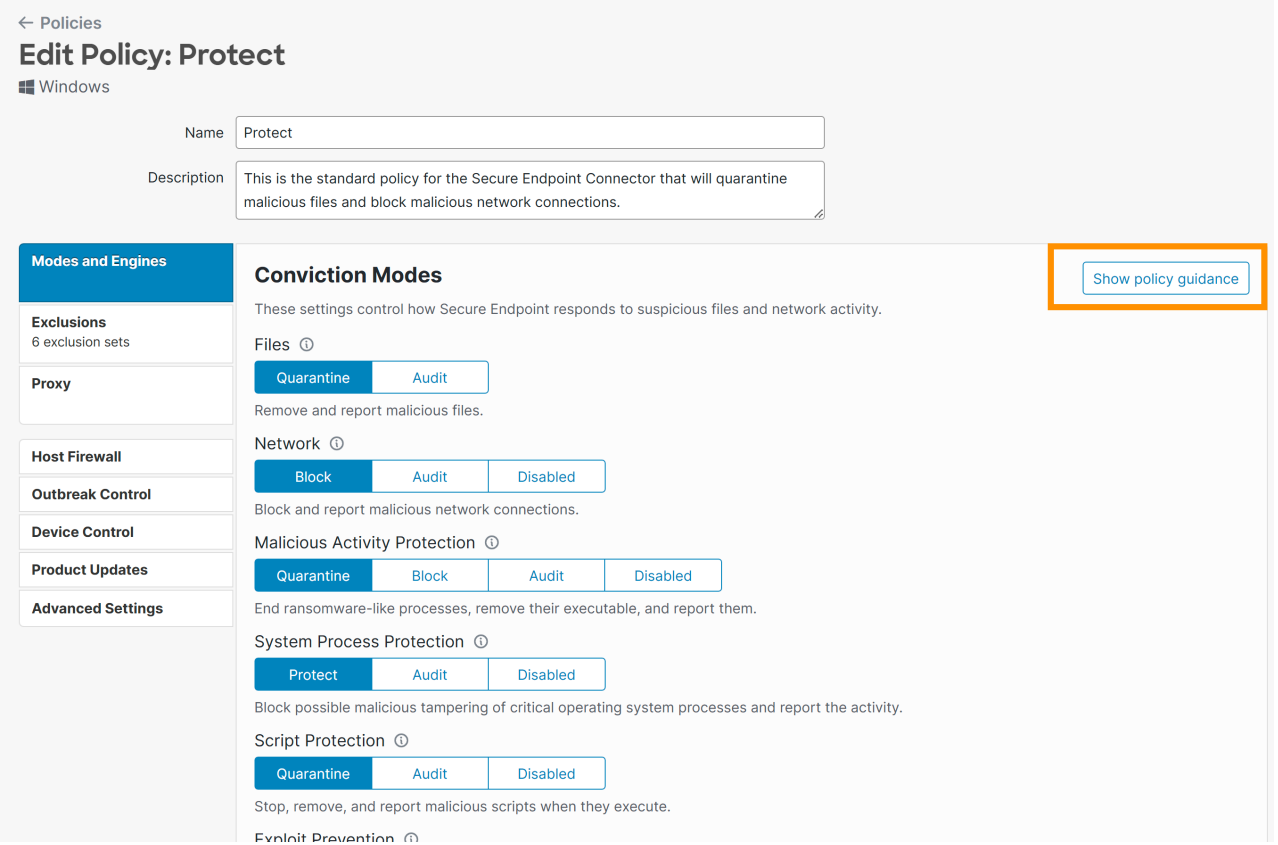
- Two main services – “amscansvc” & “ampdaemon”
- Runs with its own user
- Use top command to observe

```
top - 15:37:58 up 27 min,  2 users,  load average: 2.41, 0.67, 0.41
Tasks: 250 total,   2 running, 248 sleeping,   0 stopped,   0 zombie
%Cpu(s): 49.7 us,  8.0 sy, 37.6 ni,  0.0 id,  0.0 wa,  4.3 hi,  0.4 si,  0.0 st
MiB Mem :   3626.0 total,    410.6 free,   3007.6 used,    438.6 buff/cache
MiB Swap:   4012.0 total,   3436.0 free,    576.0 used.    618.4 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   9669 cisco-a+  20   0 1902172   1.5g   6272 S  89.8  41.6   1:30.98 ampscansvc
   2915 sysadmin  20   0 3929020  70592  36192 S   8.1   1.9   0:25.73 ampdaemon
```

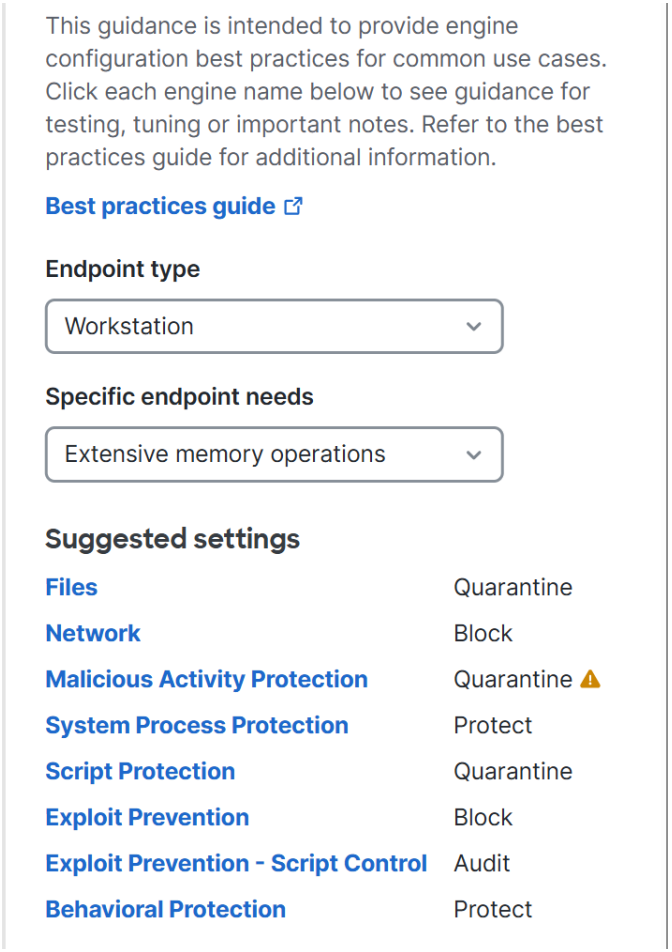
Policy Guidance

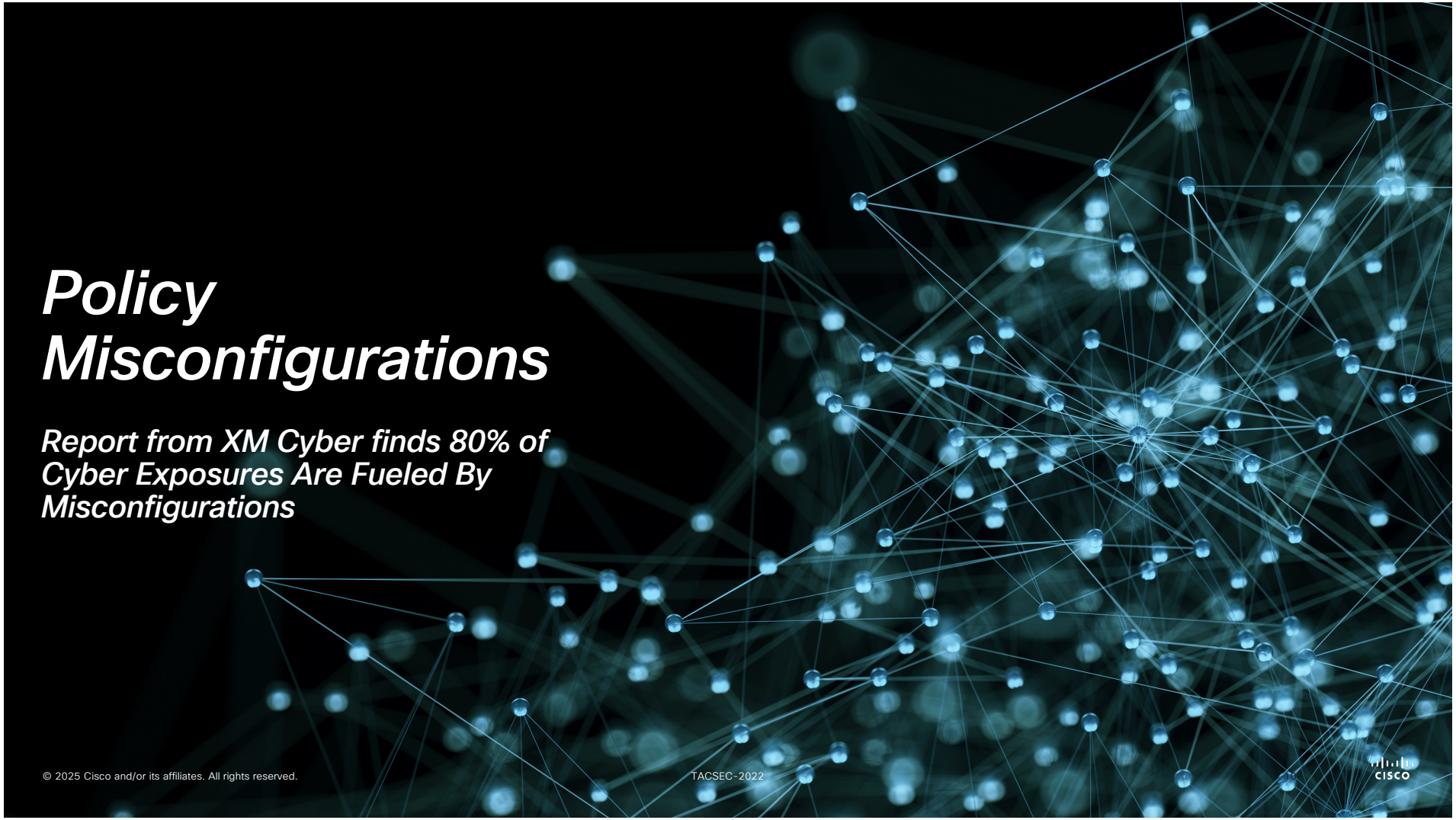
- Identify endpoint needs
- Server vs Workstation
- Tune engines according to needs
- Will differ based on OS



Policy Guidance Example

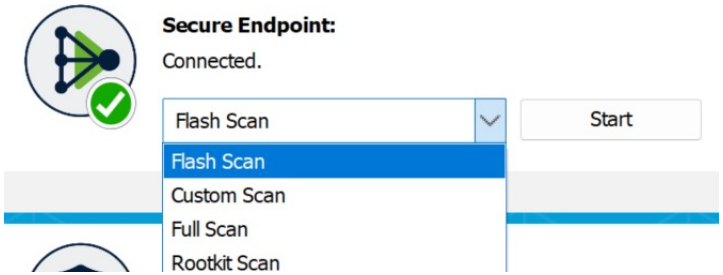
- Server or Workstation
- Specific endpoint needs:
  - General
  - Many network connections
  - Custom scripting
  - Extensive memory operations
  - Latency is critical

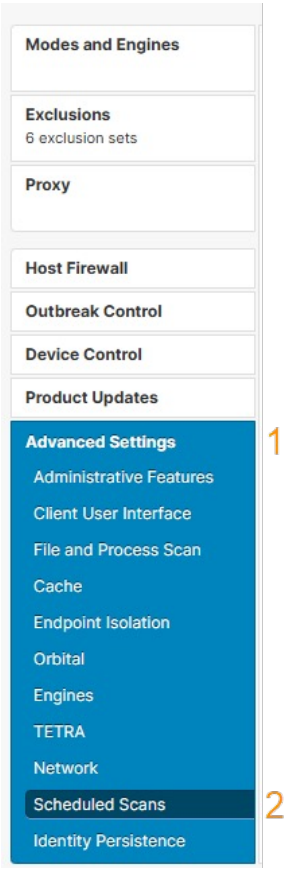




Advanced Policy Settings - Scheduled Scans

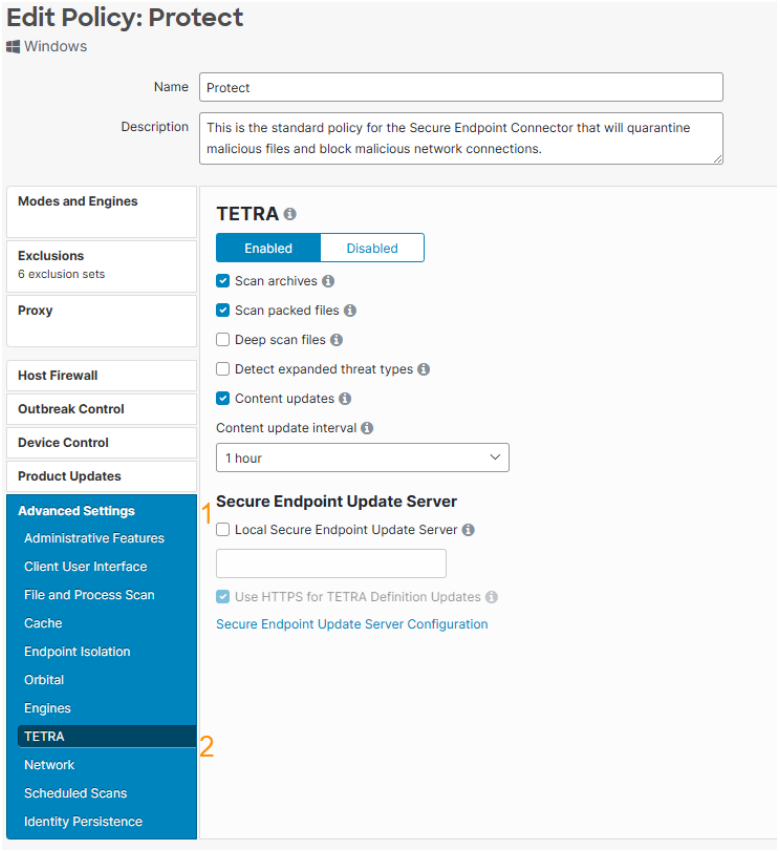
- May cause temporary high resource usage
- Full scans will scan ALL files on an endpoints
- Flash scans will check running processes & registry
- Can be scheduled or manual





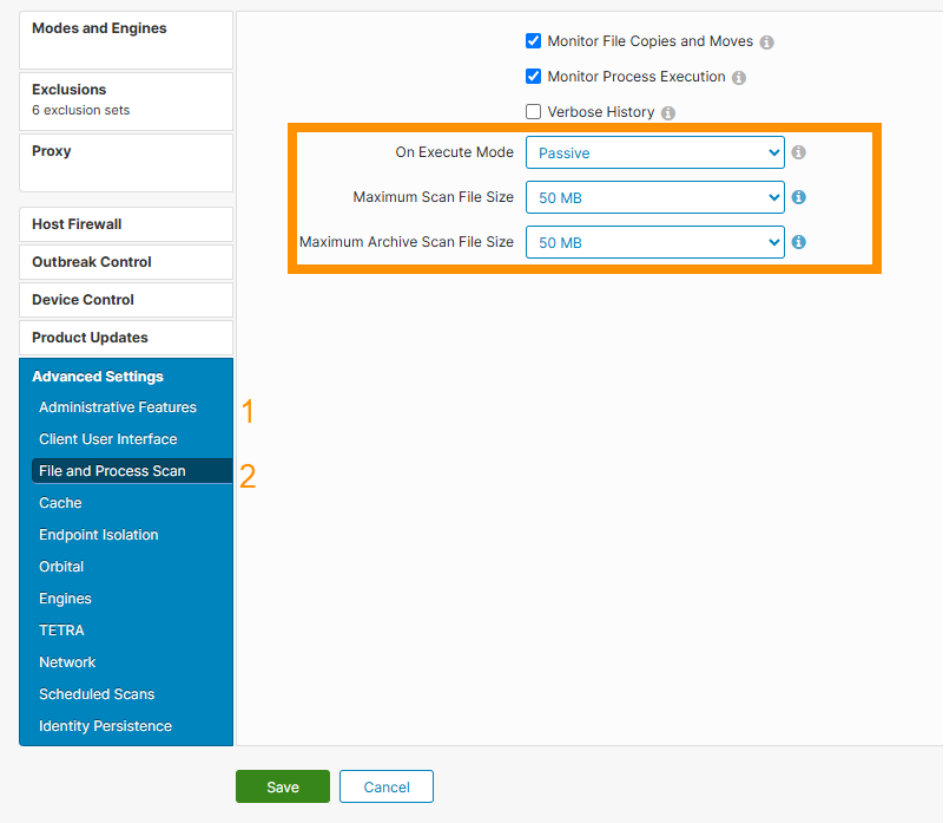
Advanced Policy Settings – Tetra Engine Considerations

- Tetra with 3rd Party Antivirus
- Scan Archives
- Scan Packed Files
- Deep Scan Files
- Detect Expanded Threat Types



Other Policy Considerations – Advanced Settings

- Debug settings
  - Administrative Features
- Maximum Scan File Size
- Maximum Archive Scan File Size
- On Execute Mode
  - Active
  - Passive

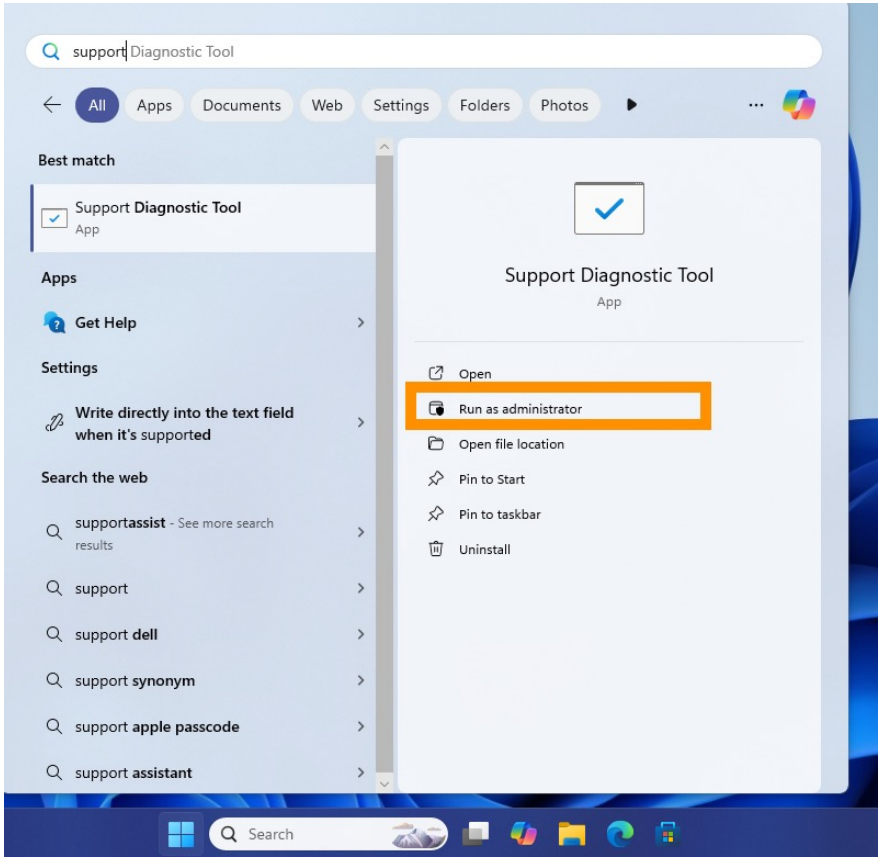


Exclusions

- Sometimes exclusions are needed
  - Applications with high activity
  - Applications you trust
- Secure Endpoint allows exclusion by engine type
- Cisco Maintained Exclusions
- Avoid using exclusions if possible
- Always refer to Best Practices

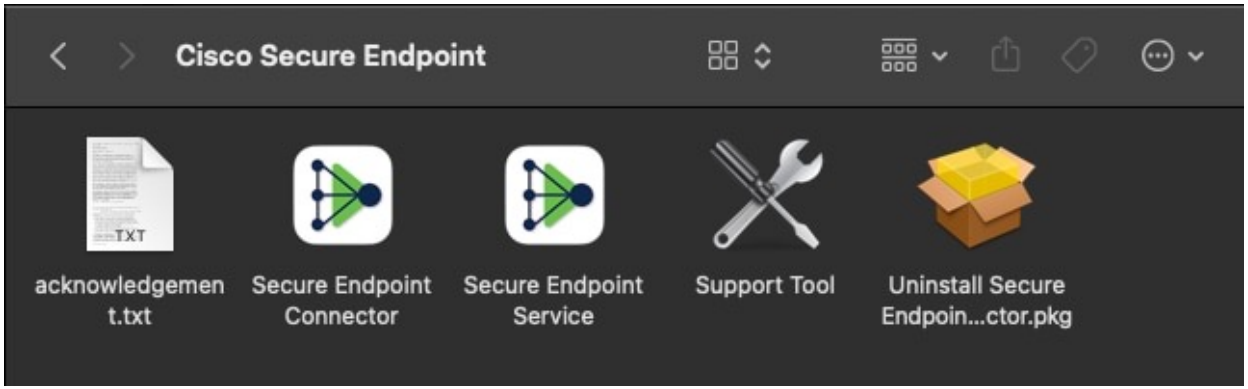
Collecting Debug Bundles for Windows

- Utilize Support Diagnostic Tool
  - Run from Windows search
  - Located in C:\Program Files\Cisco\AMP\<version>\ipsupporttool.exe
  - Can also be collected via dashboard or CLI
  - ZIP file will generate on desktop



Collecting Debug Bundles for MacOS

- Cisco Secure Endpoint folder in Applications
- Provide password
- Bundle will generate on desktop
- Can also be retrieved via dashboard or terminal

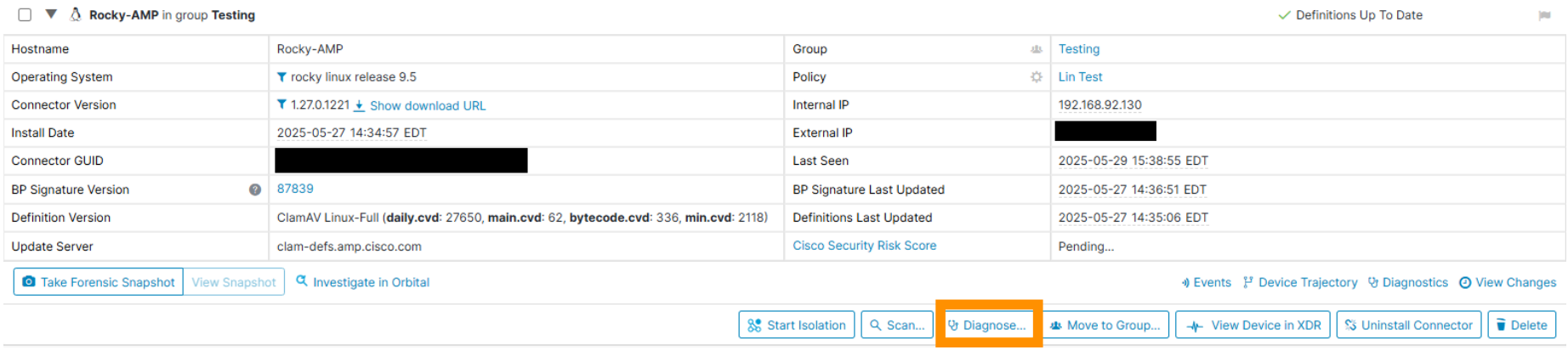


Collecting Debug Bundles for Linux

- Does not have a GUI
- Must be performed via CLI
- Use command:

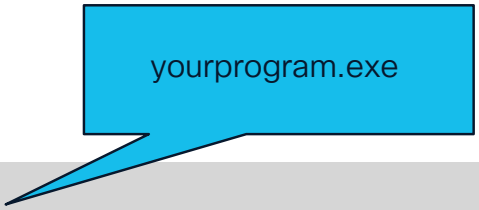
```
sudo /opt/cisco/amp/bin/ampsupport
```

- Can also be retrieved via Dashboard
- Support bundle is placed in current user's home directory



Leveraging Windows Debug Bundles

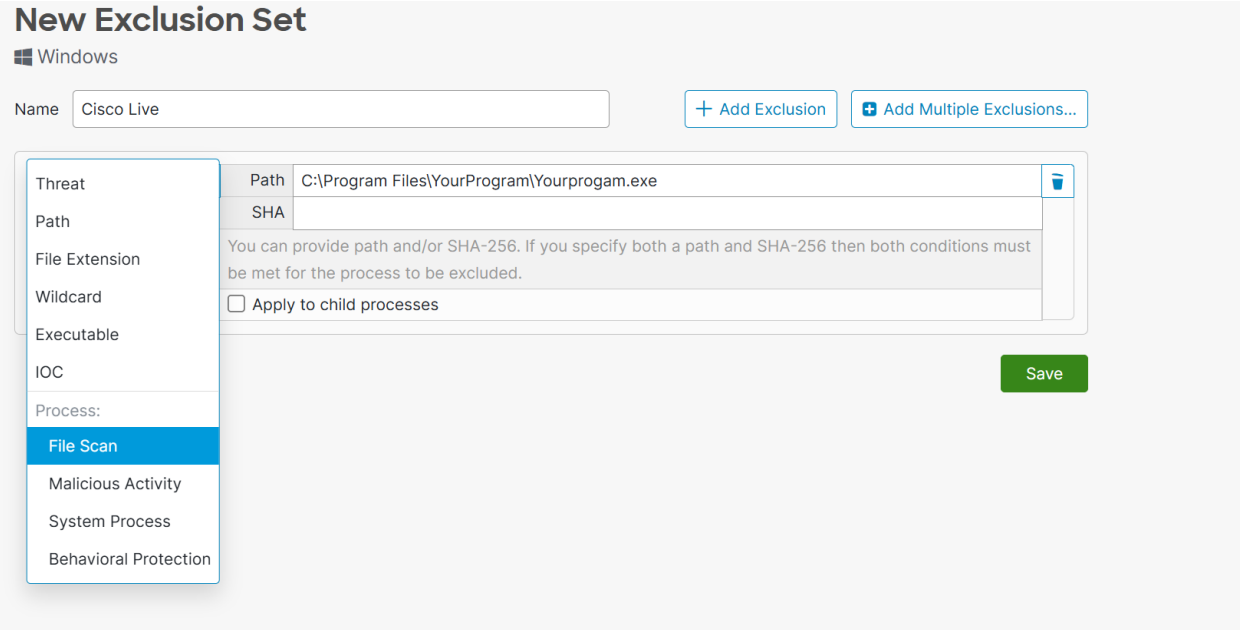
- Leverage debug bundles to assist with creating exclusions
- Cisco Security GitHub script - amp-05-windows-tune
- Top processes, files, extensions, paths




```
Top 10 Processes:
     423 C:\Program Files\YourProgram\yourprogram.exe
     170 C:\Windows\explorer.exe
     168 C:\Users\testuser\AppData\Local\Programs\Python\Python37-32\python.exe
      83 C:\Windows\System32\wbem\WmiPrvSE.exe
      64 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
      29 C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
      25 C:\Windows\System32\svchost.exe
```

Creating Windows Exclusions

- Exclude by engine, as few as possible
- Start with Process: File scan
- Ensure exclusion is attached to policy



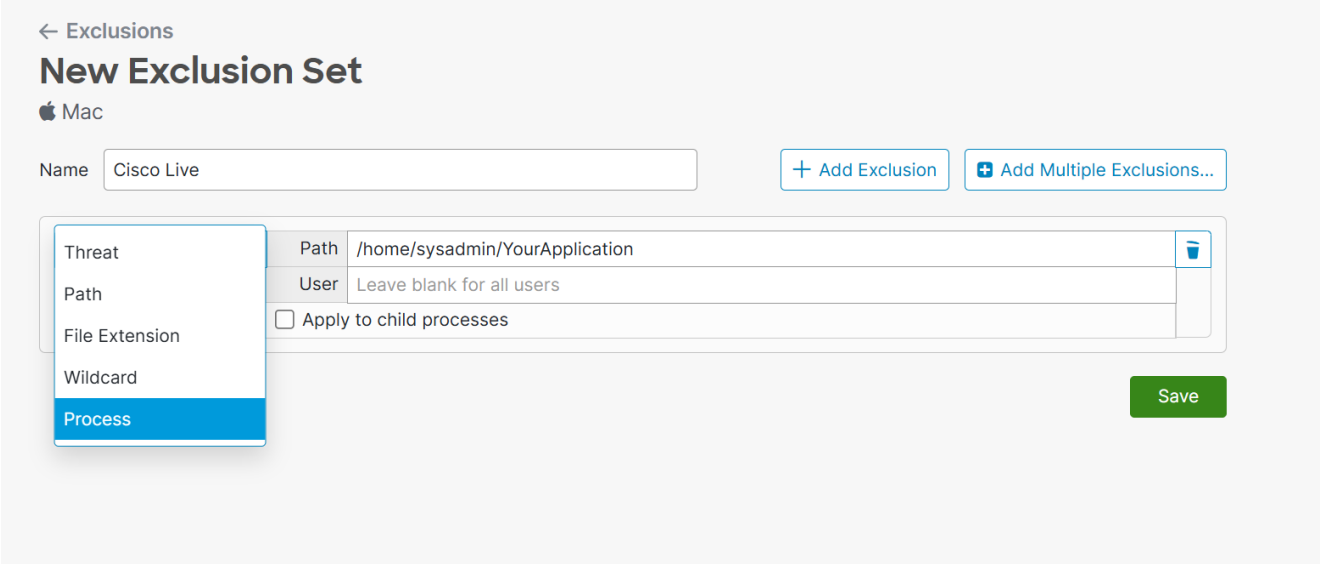
MacOS & Linux Debug Bundles

- No need to use a script, outputs many helpful files
- Fileops.txt
  - Includes files and processes
- Ampcli_status.txt
  - Connector health

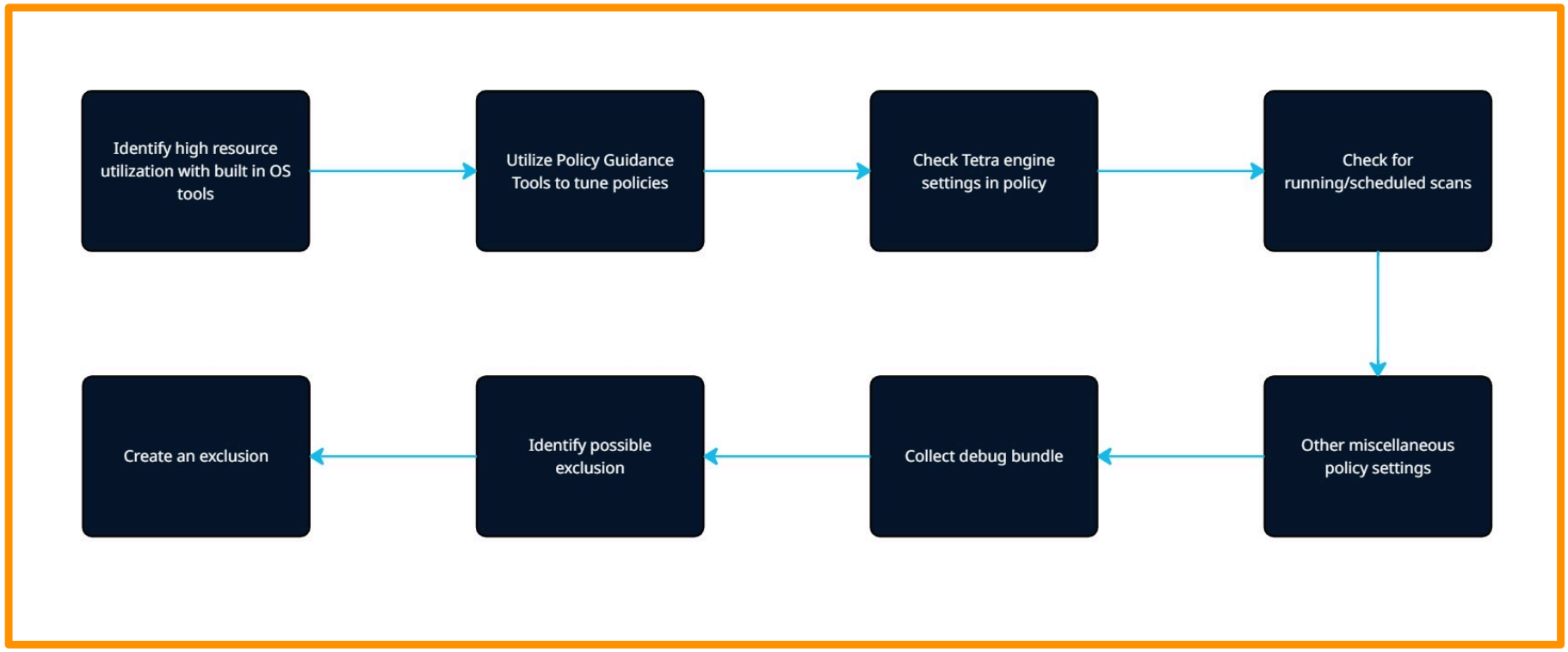
```
128 /home/sysadmin/YourApplication
58 /var/lib/rsyslog/imjournal.state
37 /var/log/cisco/ampupdater.log
33 /var/lib/rpm/rpmdb.sqlite-shm
20 /run/NetworkManager/devices/2
18 /run/user/1000/dconf/user
17 /root/.gnupg/trustdb.gpg
15 /var/log/cisco/orbitalupdater.log
```

Creating Mac & Linux Exclusions

- Exclude by engine, as few as possible
- Applications must use Process exclusion
  - Excludes from all engines



Recap – How to Identify and Address Performance Impacts



Questions

cisco Live !

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: akoelbel@cisco.com


cisco