Cisco Secure Endpoint Connector for Linux Diagnostic Data Collection

Contents

Introduction
Background Information
Generate Diagnostic Data
Generate Diagnostic Data Locally Using the Support Tool
Generate Diagnostic Data Using the Secure Endpoint Console
Troubleshooting
Enable Debug Mode
Enable Debug Mode Using the Secure Endpoint Console
Enable Debug Mode Using the Connector Command Line Interface
Disable Debug Mode
Disable Debug Mode Using the Secure Endpoint Console
Disable Debug Mode Using Connector Command Line Interface
See Also

Introduction

This document describes how to generate diagnostic data for the Cisco Secure Endpoint Linux connector.

Background Information

The Cisco Secure Endpoint Linux connector comes packaged with the Support Tool application, which is used in order to generate diagnostic data about the endpoint and the connector that is installed on it. The diagnostic data includes information such as:

- Resource utilization (disk, CPU, and memory).
- Connector-specific logs.
- Connector configuration information.

Generate Diagnostic Data

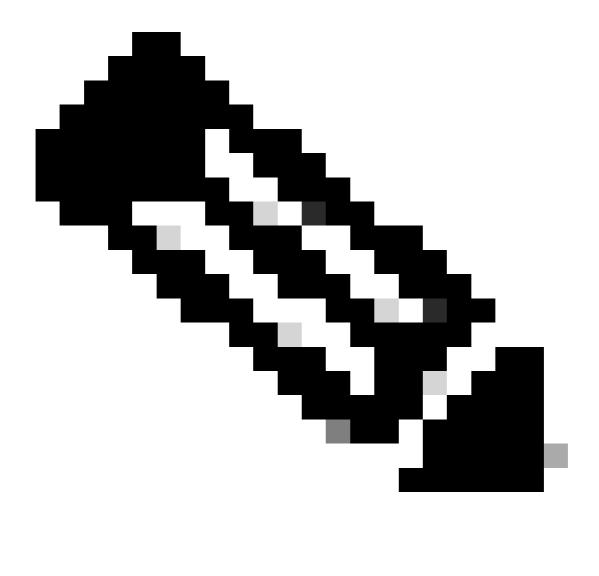
Diagnostic data can be generated via two different methods:

- Locally using the Support Tool.
- Remotely using the Secure Endpoint Console.

The generated diagnostic data can be provided to the Cisco Technical Assistance Center (TAC) for further analysis.

Generate Diagnostic Data Locally Using the Support Tool

Run the following command to generate diagnostic data for the Linux connector using the Support Tool:



Note: You must have sufficient privileges to run the Support Tool, so ensure that you preface the command with sudo.

The Support Tool creates a .zip archive file called AMP_Support_<timestamp>.zip at the current logged in user's Desktop directory if it exists, otherwise the archive file will be created at the current logged in user's home directory.

Generate Diagnostic Data Using the Secure Endpoint Console

Complete these steps to generate diagnostic data for the Linux connector through the Secure Endpoint Console:

1. Navigate to the Computers page by selecting Management -> Computers and identify your computer in the list. Click Diagnose....

] Dashboard	Computers						O Vie	w All Chan
) Inbox	4	•	•		~		•	
- Overview	1	0	0	1	0)	0	
Events	Computers	Not Seen in Over 7 Days	Need AV Update	Need Connector Update 🚳	Computers V	/ith Faults	Cisco Security Risk Score Critical 🚱	
Events								
	► Filters Hostname Operating S	ystems					Select a Filter	
Analysis	~							
t Outbreak Control	All Windows Mac Linux	Android IOS Network						
	4- Move to Group 🗑 Delete							0
Management	•							
Computers	v A centos-8-5-template in group v	Installation Demo					Definitions Up To Date	
Groups	Hostname	centos-8-5-template		Group	de Installa			
Policies	Operating System	centos linux release 8.5		Policy	O Demo I			
	Connector Version	T 124.0.1005 + Download		Internal IP		19.143, 192.168.122.1		
Exclusions	Install Date	2024-01-10 16:40:04 UTC		External IP	10.85.2			
Device Control	Connector GUID	47086935-c4d9-4a85-8cfc-77bb6046f01		Last Seen		1-15 16:10:08 UTC		
Host Firewall	Definition Version Update Server	ClamAV Linux-Full (daily.cvd: 27154, main. clam-defs.ga1.immunet.com	cvd: 62, bytecode.cvd: 334)	Definitions Last Updated	2024-0	1-14 15:44:02 UTC		
Download Connector								
	Take Forensic Snapshot View Snapsi	Q. Investigate in Orbital					♦ Events ¹² Device Trajectory ¹ ⊗ Diagnostics ¹ ⊙ ¹	/iew Char
Deploy Clarity for iOS						Q. Scan 19 Diagnose	Move to Group S Uninstall Connector	E Dele
Deployment Summary								
AV Definition Summary	1.00	cord 25 ^	/ page	< 1 of1 5			± Exp	port to CS

2. In the New Connector Diagnostic popup, select the length of the Debug session from the dropdown and ensure the checkboxes for Historical Data and Kernel Log are both selected. Click Create.

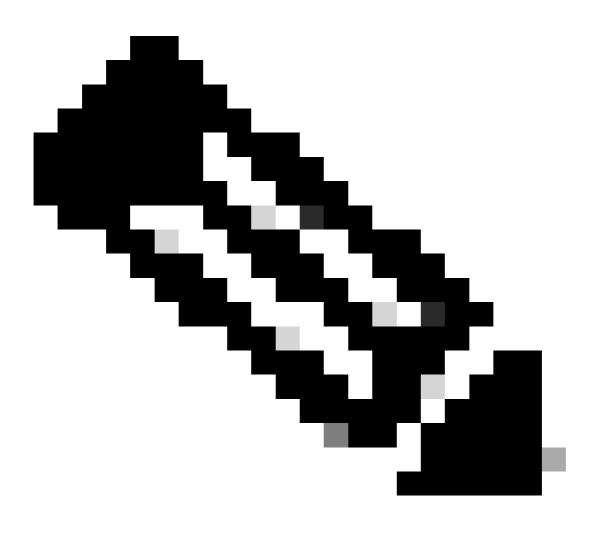
New Connector Diagnostic for centos-8-5-template ×						
Debug session 5 minutes 🗸						
Diagnostic files are limited to 50MB in size and can take up to 24 hours to generate.						
Cancel	e					

3. Still on the Computers page, click Diagnostics for your connector. You will be brought to the File Repository page in the Analysis section.

Dashboard	Computers					O View All Chang
1 Inbox	4	0	0	1	0	0
Overview	- I	0	0	1	0	0
Events	Computers	Not Seen in Over 7 Days	Need AV Update	Need Connector Update 🚱	Computers With Faults	Cisco Security Risk Score Critical 🚳
	Filters Hostname Operating System	ns				Select a Filter 🗸 🗸
d Analysis 🗸						
3t Outbreak Control	All Windows Mac Linux An	droid IOS Network				
CE Management	🔹 Move to Group 🗑 Delete					8
Computers	🔲 🔻 🔬 centos-8-5-template in group Insta	ellation Demo				Definitions Up To Date
Groups	Hostname	centos-8-5-template		Group	4 Installation Demo	
	Operating System	T centos linux release 8.5		Policy	O Demo Policy	
Policies	Connector Version	T 124.0.1005 + Download		Internal IP	10.85.219.143, 192.168.12	2.1
Exclusions	Install Date	2024-01-10 16:40:04 UTC		External IP	10.85.219.143	
Device Control	Connector GUID	47086935-c4d9-4a85-8cfc-77bb6046f01	4	Last Seen	2024-01-15 16:10:08 UT	0
	Definition Version	ClamAV Linux-Full (daily.ovd: 27154, main.	cvd: 62, bytecode.cvd: 334)	Definitions Last Updated	2024-01-14 16:44:02 UT	c
Host Firewall	Update Server	clam-defs.qa1.immunet.com				
Download Connector	Take Forensic Snapshot View Snapshot	Q. Investigate in Orbital				4 Events 12 Device Trajectory 19 Diagnostics O View Change
Deploy Clarity for iOS					Q, Scan	Diagnose) 🔿 Move to Group 15 Uninstall Connector 🗑 Delete
Deployment Summary						
AV Definition Summary	1 record	25 ^	/ page	-< 1 of 1 >-		🛓 Export to CSV

4. On the File Repository page, you can view the statuses of requested diagnostics. Locate the diagnostics for your computer using the filters. When your diagnostic has the "Available" status, click Download.

Dashboard	File Repository		Connector Diagnostics Feature Overview				() View All Chang	
 ⑦ Inbox ⇒ Overview ④ Events 	Search Search by SHA-256	or file name			1	ype Connector Diagnos	atics	
	Al Available Requi	isted Being Processed Failed	Rejected					88
세 Analysis	File				Status	Requested By	Date	Actions
Reports	▼ Connector diagnostics for	or centos-8-5-template			Available 🔘		2024-01-15 16:27:12 UTC	
File Analysis	Connector Diagnostics Reques	ted 2024-01-15 16:19:20 UTC						
File Repository	Original File Name	ampsupport_47086935_20240115_	092702.zip					
Vulnerable Software	File Size	10.1 MB						
Indicators	O View Changes	centos-8-5-tempiate					[]	wnload 🗑 Delete
iOS Clarity	() View Changes						± Dov	whiload Delete
Prevalence		1-1 of 1 item	25 ^ / page	< 1 of1 >				
Threat Root Cause								
Talos Threat Hunting								
Orbital								
3 Outbreak Control	~							
C Management	~							
.Q₂ Admin	~							



Note: You will also receive an email from Cisco Secure Endpoint when the requested diagnostic data is available for download.

Troubleshooting

Debug mode logging can be enabled for the Secure Endpoint Linux connector to provide more detailed troubleshooting information in the diagnostic data. Debug mode can be enabled/disabled remotely using the Secure Endpoint Console or locally using the Linux connector's command line tool.



Warning: Debug mode should be enabled only if a Cisco Technical Support Engineer makes a request for this data. If you keep Debug mode enabled for an extended period of time, it can fill up the disk space very quickly and might prevent the connector Log and Tray Log data from being gathered in the Support Diagnostic file due to excessive file size.

Enable Debug Mode

Enable Debug Mode Using the Secure Endpoint Console

Complete these steps in order to enable Debug mode and collect diagnostic data using the Secure Endpoint Console:

1. In the Secure Endpoint Console, navigate to the Policies page by selecting Management -> Policies.

Dashboard	Policies	⊙ View All Changes + New Policy ∨
Inbox	Search by policy name, description, or GUID Q	
	Al all Windows & Mac & Linux + Android () IOS To Network	Show Descriptions
4 Linents	Namo	 Modified Groups Computers
🖆 Analysis 🗸	No description	2018-05-01 19-57-47 UTC 0 0
3€ Outbreak Control ~	a policy for linux testing	2020-05-27 20:51:28 UTC 0 0
Computers	 Mail is somewhat of a test. 	2018-05-01 19:57:19 UTC 1 0
Groups Policies	No description	2023-12-15 20-36-52 UTC 1 0
Exclusions	 A secondaria 	2022-11-25 00 19/11 UTC 1 0
Device Control Host Firewall	No description	2020-09-21 23:20:49 UTC 1 0
Download Connector	> # No description	2023-05-19 21:52:33 UTC 0 0
Deploy Clarity for IOS Deployment Summary	No description	2018-05-01 18:57:22 UTC 1 0
AV Definition Summary	No description	2022-02-24 23:24:31 UTC 1 0

2. Locate and select the policy that is applied to the endpoint, this will expand the Policy window. Click Duplicate.

	×٩				Show Descriptions
I III Windows & Mac & Linux & Android	🛛 iOS 😤 Net	work		^ Modified	Groups Compute
Demo Policy No description				2024-01-10 22:03:19 UTC	1
Detection and Response		Exclusion Sets	Custom Detections	Groups	Ģ
Files Quarantine Network Audit Behavioral Protection Protect	Audit Protect	Not configured	Simple Not configured Advanced Not configured	Installation Demo	1
ClamAV Orbital	Protect Enabled		Application Control		
			Allow Not configured Block Not configured		
Device Control			Network Control	Proxy	
Not available for this type of policy			Not configured	Not configured	
View Changes Serial Number 9610				🛓 Download XML 🖉 Ed	it Duplicate 🗑 Dele
1-1 of 1 item		25 ~ / page < 1	of 1 >		

3. The Secure Endpoint Console will create a copy of the requested policy.

	Policy Copy of Demo Policy was created.	×			
Policies			() View All Changes + New Policy		
Demo Policy" X Q					
II 🛤 Windows 📽 Mac 🛆 Linux ♦ Android 🛛 iOS 😒 N	letwork		Show Descriptions		
Name			Modified Groups Compute		
Copy of Demo Policy No description			2024-01-10 22:06:47 UTC 0		
<u>A Demo Policy</u> No description			2024-01-10 22:03:19 UTC 1		
Detection and Response	Exclusion Sets	Custom Detections	Groups 🖵		
Files Quarantine Network Audit Behavioral Protection Protect	Not configured	Simple Not configured Advanced Not configured	Installation Demo 1		
ClamAV Protect Orbital Enabled		Application Control			
		Allow Not configured Block Not configured			
Device Control		Network Control	Proxy		
Not available for this type of policy		Not configured	Not configured		
View Changes Serial Number 9610			🛓 Download XML 🗡 Edit 🖉 Duplicate 🗑 Deleti		
1-2 of 2 items	25 ~ / page < 1	of 1 >			

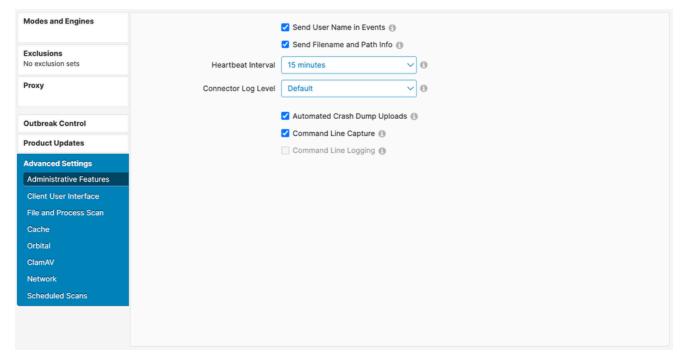
4. Select and expand the duplicate policy and click Edit. You will be brought to the Edit Policy page for that policy.

Policies			() View	v All Changes +	New Policy ~
"Demo Policy" X Q					
All 🛤 Windows 📽 Mac 🛆 Linux 🗣 Android 🛛 iOS 🕾 Ne	twork			Show Description	ons 😑 🕀
Name			^ Modified	Groups	Computers
Copy of Demo Policy No description			2024-01-10 22:06:47 UTC	0	0
Detection and Response	Exclusion Sets	Custom Detections	Groups		Ģ
Files Quarantine Network Audit Behavioral Protection Protect	Not configured	Simple Not configured Advanced Not configured	No groups		
ClamAV Protect Orbital Enabled		Application Control			
		Allow Not configured Block Not configured			
Device Control		Network Control	Proxy		
Not available for this type of policy		Not configured	Not configured		
() View Changes Serial Number 9611			Download XML Z	dit 🖣 Duplicate	Delete

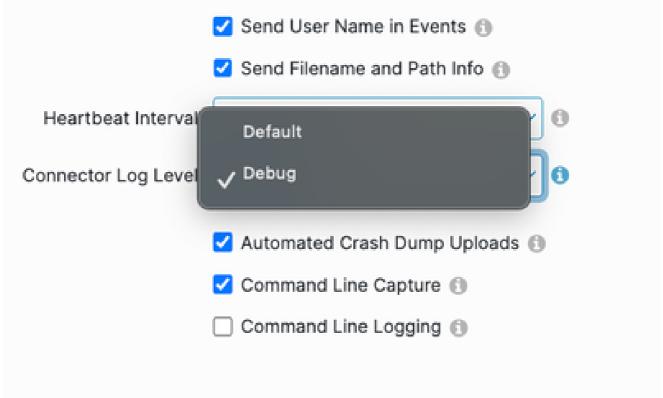
5. Change the name of the policy. For example, you could use *Debug TechZone Linux Policy*. \leftarrow Policies

Edit Policy	
Name	Debug TechZone Linux Policy
Description	
Modes and Engines	Conviction Modes
Exclusions No exclusion sets	These settings control how Secure Endpoint responds to suspicious files and network activity.
Proxy	Quarantine Audit Remove and report malicious files. Audit
Outbreak Control	Network
Product Updates	Audit Disabled
Advanced Settings	Report malicious network connections, but take no other action.
	Behavioral Protection Protect Audit Disabled
	Detect malicious activity, take remedial actions as needed, and report it.
	Detection Engines
	ClamAV ()
	Cancel Save

6. Select Advanced Settings, and select Administrative Features from the sidebar.



7. Expand the Connector Log Level dropdown and click "Debug".



- 8. Click Save in order to save the changes.
- 9. Navigate to the Groups page by selecting Management -> Groups and click Create Group. You will be brought to the New Group page.

	Dashboard		Groups		
\Box	Inbox		Search Q	Create Group	
≣₽	Overview				
-0	Events		test O View Changes	🖊 Edit 🗑 Delete	Groups allow the computers in your organization to be managed according to their function, location, or other criteria determined by the administrator. When you first log into Secure Endpoint, a
ъ	Analysis	~	No description		Default Group will already have been created for you. Clicking on a group in the list will expand details on that group,
æ	Outbreak Control	~	O View Changes	🖊 Edit 🔋 Delete	including the policies assigned to it and the members of the group. You can also create new groups, edit existing ones, and delete
cB	Management	~	No description		groups from this screen.
1	Computers		© View Changes	🖌 Edit 🔋 Delete	
	Groups				
			No description O View Changes	🖊 Edit 🗑 Delete	
	Policies				
	Exclusions		No description O View Changes	🖌 Edit 🔋 Delete	
	Device Control			(Con) (Conn)	
	Host Firewall		Audit Group for Your Company		
	Download Connector		© View Changes	🖊 Edit 🔋 Delete	
	Deploy Clarity for iOS		Default group with Linux Only cvd for the Linux Policy		
	Deployment Summary		O View Changes	🖊 Edit 🗑 Delete	
	AV Definition Summary		No description		
Q.	Admin	~	View Changes	🖌 Edit 🗑 Delete	
			No description		
			© View Changes	🖊 Edit 🗑 Delete	
			No description		
			View Changes	🖌 Edit 🗑 Delete	
			< < 1 2 3 4 5 - > >		

- 10. Enter a name for the group. For example, you could use *Debug TechZone Linux Group*.
- 11. Change the Linux Policy to the new policy that you just created, which is *Debug TechZone Linux Policy* in this example. Click Save.

← Groups New Group		
Name	Debug TechZone Linux Group	Computers
Description	This group will be used to debug Cisco Secure Endpoint connectors running on Linux.	Assign computers from the Computers page after you have saved the new group
Parent Group		
Windows Policy	Default Policy (Default FireAMP Windows \checkmark	
Android Policy	Default Policy (Default FireAMP Android) \checkmark	
Mac Policy	Default Policy (Default Policy for Mac - A \checkmark	
Linux Policy	Debug TechZone Linux Policy 🗸 🗸	
Network Policy	Default Policy (Default Network)	
iOS Policy	Default Policy (Default iOS eh)	
	Cancel Save	

12. Navigate to the Computers page by selecting Management -> Computers and identify your computer in the list. Select it and click Move to Group....

3 Dashboard	Computers					O View Al	ul Char			
) Inbox	4	•	•		•	0				
5 Overview	1	0	0	1	0	0				
Events	Computers	Not Seen in Over 7 Days	Need AV Update	Need Connector Update 🚳	Computers With Faults	Cisco Security Risk Score Critical 🔕				
	Filters Hostname Operating Sy	etame				Select a Filter				
		p101110				00000000000				
Analysis		Android IOS Network								
Outbreak Control		Anarow 105 Metalotic								
Management	C 4 Move to Oroque. P Deate									
Computers	🖉 🔻 👌 centos-8-5-template in group		Definitions Up To Date							
Groups	Hostname	centos-8-5-template		Group	de Installation Demo					
Policies	Operating System	T centos linux release 8.5		Policy	O Demo Policy					
Policies	Connector Version	T 1.24.0.1005 🛓 Download		Internal IP	10.85.219.143, 192.168.122.1					
Exclusions	Install Date	2024-01-10 16:40:04 UTC		External IP	10.85.219.143					
Device Control	Connector GUID	47086935-c4d9-4a85-8cfc-77bb6046f01	4	Last Seen	2024-01-12 22:11:23 UTC					
	Definition Version	ClamAV Linux-Full (daily.cvd: 27152, main.	cvd: 62, bytecode.cvd: 334)	Definitions Last Updated	2024-01-12 16:42:41 UTC					
Host Firewall	Update Server	clam-defs.ga1.immunet.com								
Download Connector	tas Forence Support Vere Suppor									
Deploy Clarity for iOS					Q. Scen	Xagnose 🔿 Move to Group 🕓 Uninstall Connector	Del			
Deployment Summary										
AV Definition Summary	1 rec	ord 25 ^	25 ^ / page < 1 of 1 >				to CS			

13. In the Move Connector to Group pop-up that appears, select your newly created group from the Select Group dropdown menu. Click Move to move the selected computer into your new group.

Move Co	Move Computer to Group								
A centos-8-5-template in group Installation Demo									
	Move To	Existing Group New Group							
	Select Group	Debug TechZone Linux Group	~						
			Cancel	Move					

Enable Debug Mode Using the Connector Command Line Interface

To enable Debug mode via the Linux connector Command Line Interface (CLI), run the following command:

/opt/cisco/amp/bin/ampcli debuglevel 1

The following output should be displayed:

Daemon now logging at 'info' level until next policy update

Disable Debug Mode

After the diagnostic data in Debug mode is obtained, you must revert the Secure Endpoint connector back to the normal mode. Debug mode can be disabled using either the Secure Endpoint Console or using the Linux connectors command line tool.

Disable Debug Mode Using the Secure Endpoint Console

To disable Debug mode, follow the same steps to <u>enable the Debug mode using the Secure Endpoint</u> <u>Console</u>, but change the Connector Log Level to "Default" in step 7.

Disable Debug Mode Using Connector Command Line Interface

To disable Debug mode via the Linux connector CLI, run the following command:

/opt/cisco/amp/bin/ampcli debuglevel 0

The following output should be displayed:

Daemon now logging at policy-specified log level

See Also

- <u>Cisco Secure Endpoint Connector for Mac Diagnostic Data Collection</u>
- <u>Technical Support & Documentation Cisco Systems</u>