Cisco Secure Endpoint Connector for Linux Diagnostic Data Collection

Contents

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:

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

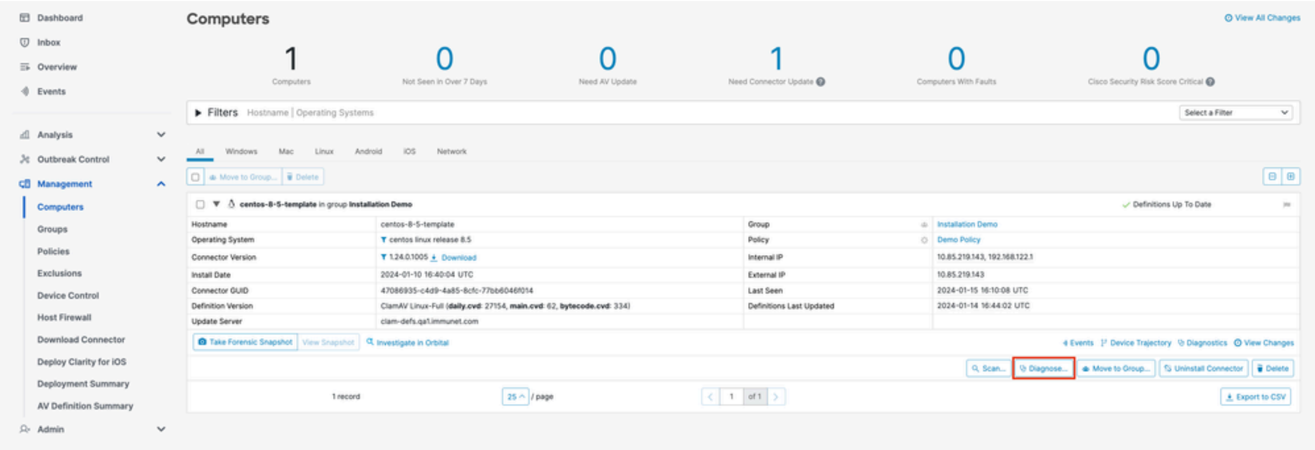
Note: You must have sufficient privileges to run the Support Tool, so ensure that you preface the command with sudo.

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...`.



Computers

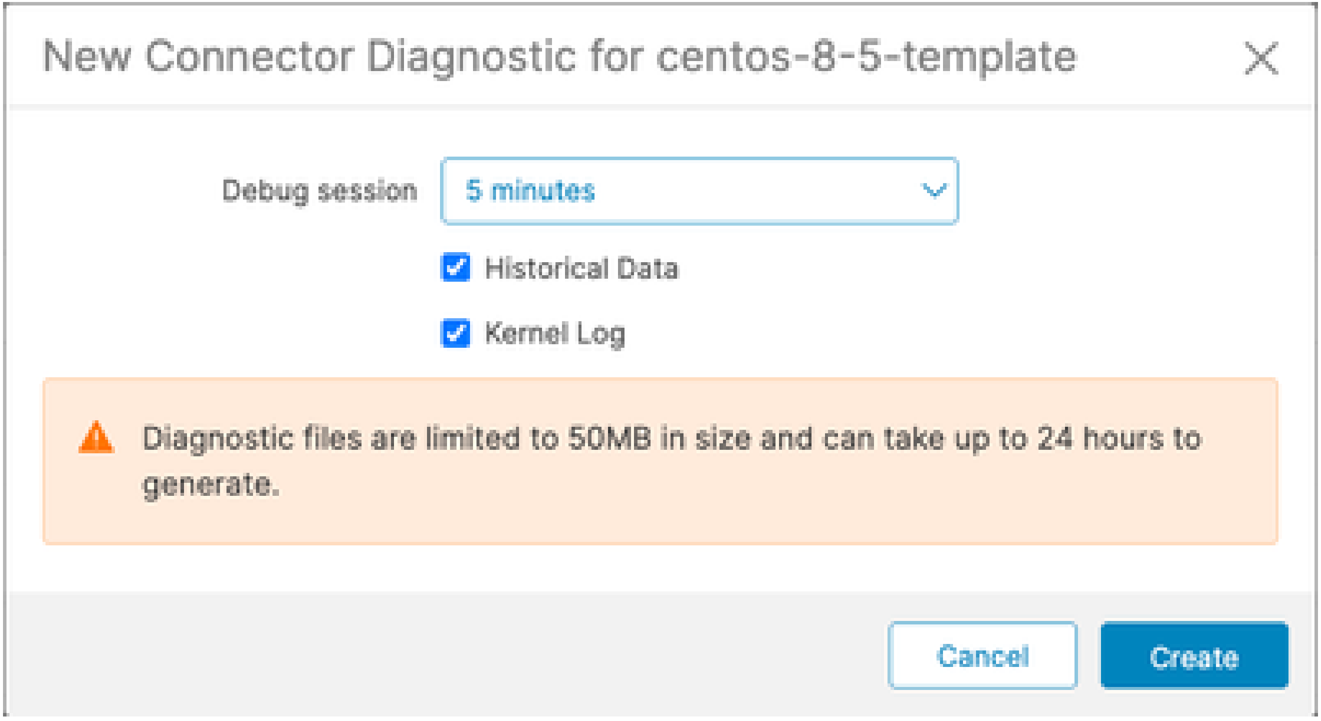
1	0	0	1	0	0
Computers	Not Seen in Over 7 Days	Need AV Update	Need Connector Update	Computers With Faults	Cisco Security Risk Score Critical

centos-8-5-template in group **Installation Demo** — Definitions Up To Date

Hostname	centos-8-5-template	Group	Installation Demo
Operating System	centos linux release 8.5	Policy	Demo Policy
Connector Version	1.24.0.1005 Download	Internal IP	10.85.219.143, 192.168.122.1
Install Date	2024-01-10 16:40:04 UTC	External IP	10.85.219.143
Connector GUID	47086935-c4d9-4a85-8cfc-77bb6046f014	Last Seen	2024-01-15 16:10:08 UTC
Definition Version	ClamAV Linux-Full (**daily.cvd**: 27154, **main.cvd**: 62, **bytecode.cvd**: 334)	Definitions Last Updated	2024-01-14 16:44:02 UTC
Update Server	clam-defs.qa1.immunet.com		

1 record · 25 / page · 1 of 1

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

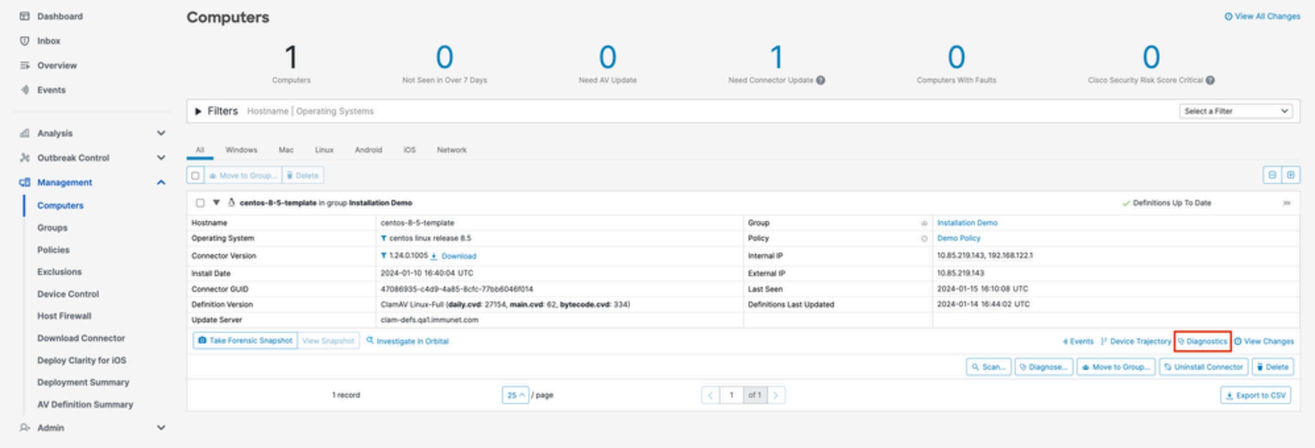
Debug session: 5 minutes

☑ Historical Data

☑ Kernel Log

Diagnostic files are limited to 50MB in size and can take up to 24 hours to generate.

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



Computers

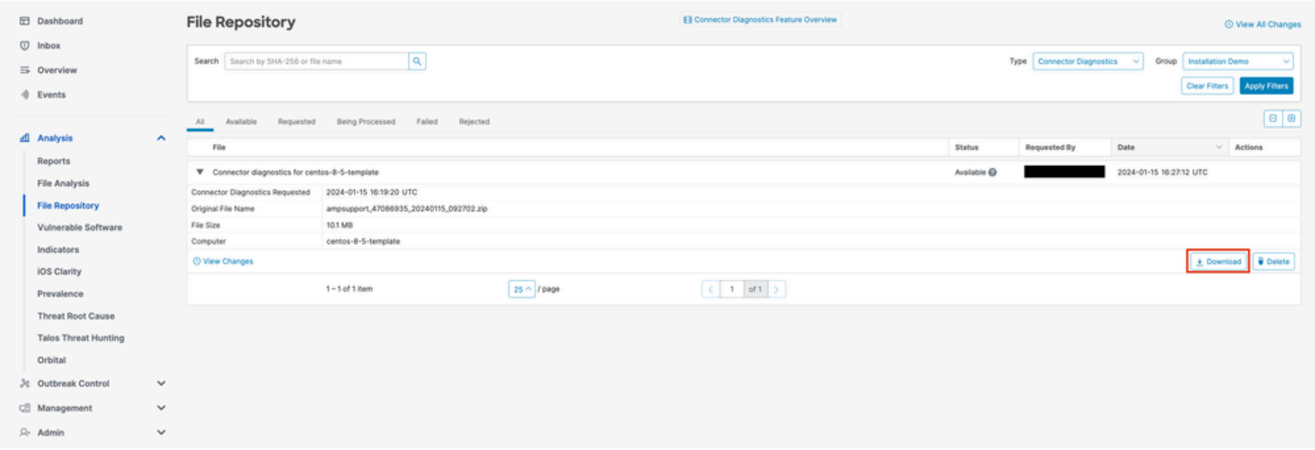
1	0	0	1	0	0
Computers	Not Seen in Over 7 Days	Need AV Update	Need Connector Update	Computers With Faults	Cisco Security Risk Score Critical

centos-8-5-template in group **Installation Demo** — Definitions Up To Date

Hostname	centos-8-5-template	Group	Installation Demo
Operating System	centos linux release 8.5	Policy	Demo Policy
Connector Version	1.24.0.1005 Download	Internal IP	10.85.219.143, 192.168.122.1
Install Date	2024-01-10 16:40:04 UTC	External IP	10.85.219.143
Connector GUID	47086935-c4d9-4a85-8cfc-77bb6046f014	Last Seen	2024-01-15 16:10:08 UTC
Definition Version	ClamAV Linux-Full (**daily.cvd**: 27154, **main.cvd**: 62, **bytecode.cvd**: 334)	Definitions Last Updated	2024-01-14 16:44:02 UTC
Update Server	clam-defs.qa1.immunet.com		

1 record · 25 / page · 1 of 1

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`.



File Repository

Search: Search by SHA-256 or file name

Type: Connector Diagnostics

Group: Installation Demo

File	Status	Requested By	Date	Actions
▼ Connector diagnostics for centos-8-5-template	Available	[redacted]	2024-01-15 16:27:12 UTC	

Connector Diagnostics Requested	2024-01-15 16:19:20 UTC
Original File Name	ampsupport_47086935_20240115_092702.zip
File Size	10.1 MB
Computer	centos-8-5-template

1 – 1 of 1 item   25 / page   1 of 1

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.

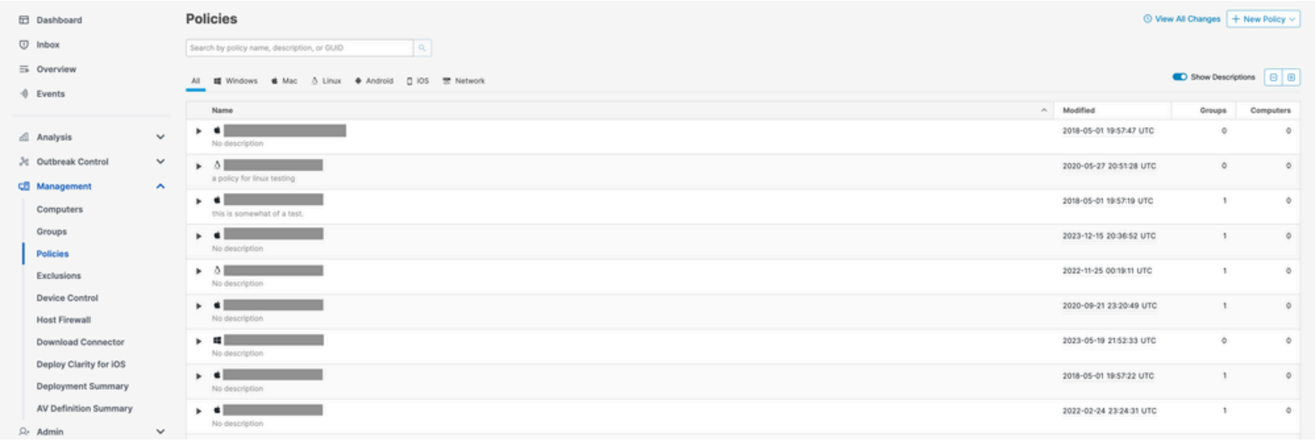
Warning: Debug mode should be enabled only if a Cisco Technical Support Engineer makes a request for this data. If you keep Debug mode enabled for an extended period of time, it can fill up the disk space very quickly and might prevent the connector Log and Tray Log data from being gathered in the Support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

Enable Debug Mode

Enable Debug Mode Using the Secure Endpoint Console

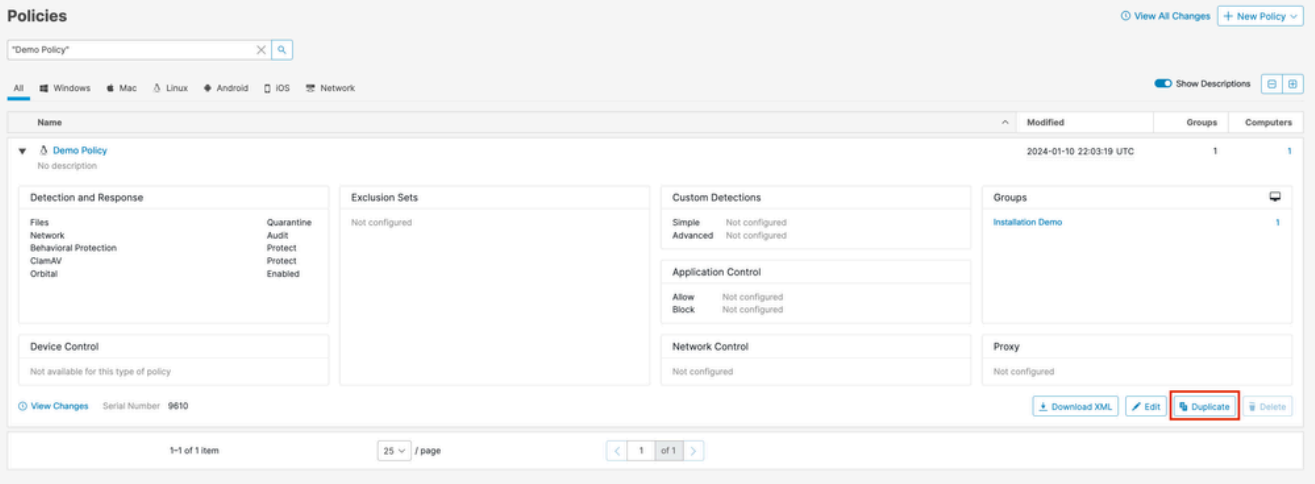
Complete these steps in order to enable Debug mode and collect diagnostic data using the Secure Endpoint Console:

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



Name	Modified	Groups	Computers
[redacted] No description	2018-05-01 19:57:47 UTC	0	0
[redacted] a policy for linux testing	2020-05-27 20:51:28 UTC	0	0
[redacted] this is somewhat of a test.	2018-05-01 19:57:19 UTC	1	0
[redacted] No description	2023-12-15 20:36:52 UTC	1	0
[redacted] No description	2022-11-25 00:19:11 UTC	1	0
[redacted] No description	2020-09-21 23:20:49 UTC	1	0
[redacted] No description	2023-05-19 21:52:33 UTC	0	0
[redacted] No description	2018-05-01 19:57:22 UTC	1	0
[redacted] 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`.



"Demo Policy"

Name	Modified	Groups	Computers
Demo Policy No description	2024-01-10 22:03:19 UTC	1	1

Detection and Response

Files	Quarantine
Network	Audit
Behavioral Protection	Protect
ClamAV	Protect
Orbital	Enabled

Exclusion Sets: Not configured

Custom Detections: Simple Not configured; Advanced Not configured

Application Control: Allow Not configured; Block Not configured

Groups: Installation Demo 1

Device Control: Not available for this type of policy

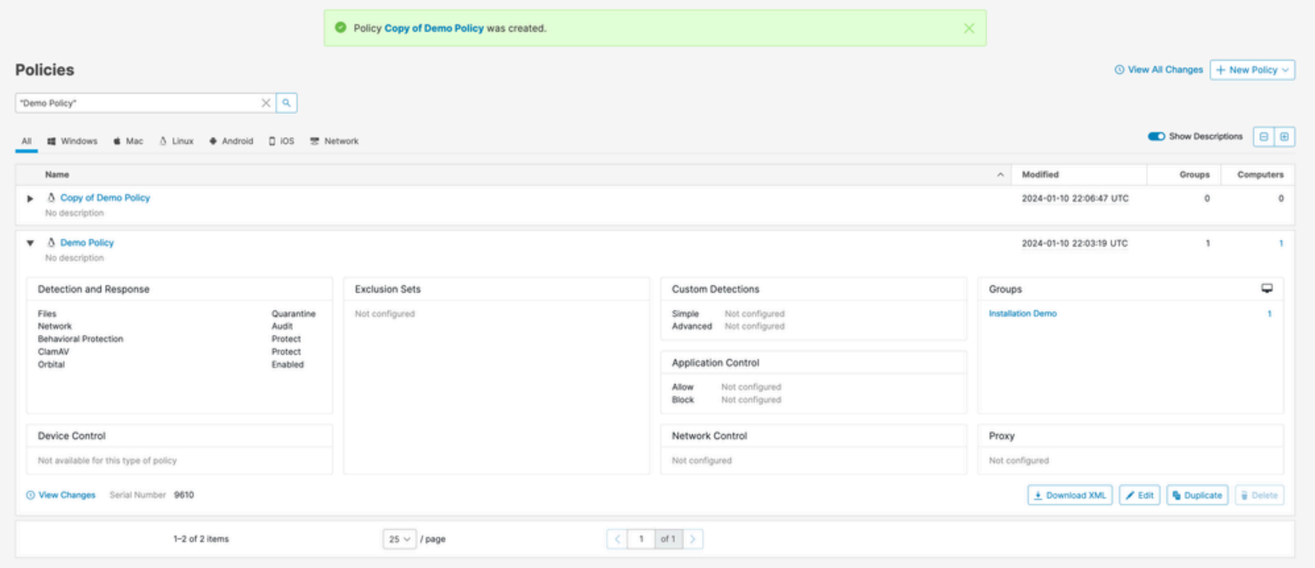
Network Control: Not configured

Proxy: Not configured

Serial Number 9610

1-1 of 1 item

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



Policy Copy of Demo Policy was created.

"Demo Policy"

Name	Modified	Groups	Computers
Copy of Demo Policy No description	2024-01-10 22:06:47 UTC	0	0
Demo Policy No description	2024-01-10 22:03:19 UTC	1	1

Detection and Response

Files	Quarantine
Network	Audit
Behavioral Protection	Protect
ClamAV	Protect
Orbital	Enabled

Exclusion Sets: Not configured

Custom Detections: Simple Not configured; Advanced Not configured

Application Control: Allow Not configured; Block Not configured

Groups: Installation Demo 1

Device Control: Not available for this type of policy

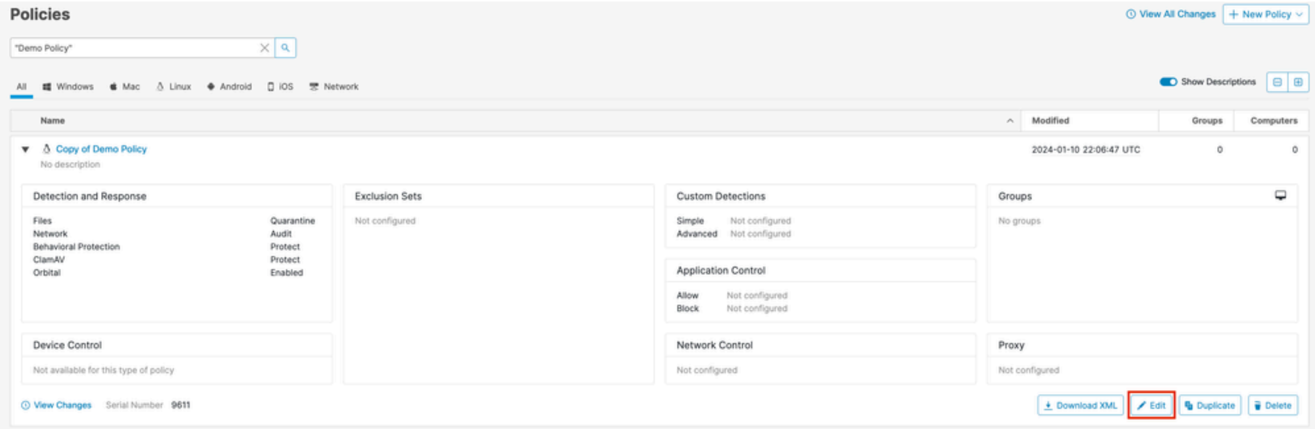
Network Control: Not configured

Proxy: Not configured

Serial Number 9610

1-2 of 2 items

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



"Demo Policy"

Name	Modified	Groups	Computers
Copy of Demo Policy No description	2024-01-10 22:06:47 UTC	0	0

Detection and Response

Files	Quarantine
Network	Audit
Behavioral Protection	Protect
ClamAV	Protect
Orbital	Enabled

Exclusion Sets: Not configured

Custom Detections

Simple: Not configured
Advanced: Not configured

Application Control

Allow: Not configured
Block: Not configured

Groups: No groups

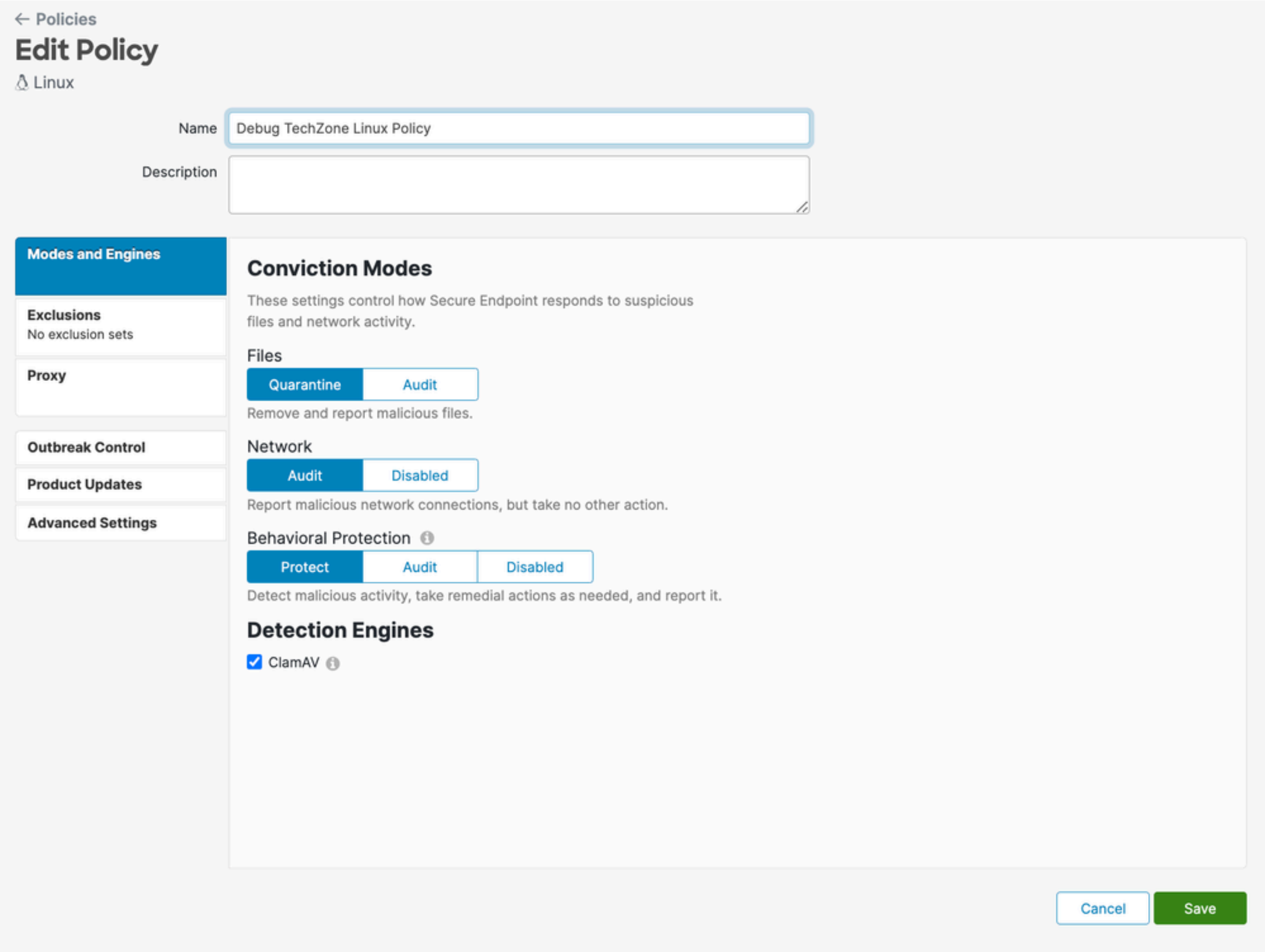
Device Control: Not available for this type of policy

Network Control: Not configured

Proxy: Not configured

Serial Number 9611

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



Name: Debug TechZone Linux Policy

Description:

Conviction Modes

These settings control how Secure Endpoint responds to suspicious files and network activity.

Files: [✓ Quarantine] Audit

Remove and report malicious files.

Network: [✓ Audit] Disabled

Report malicious network connections, but take no other action.

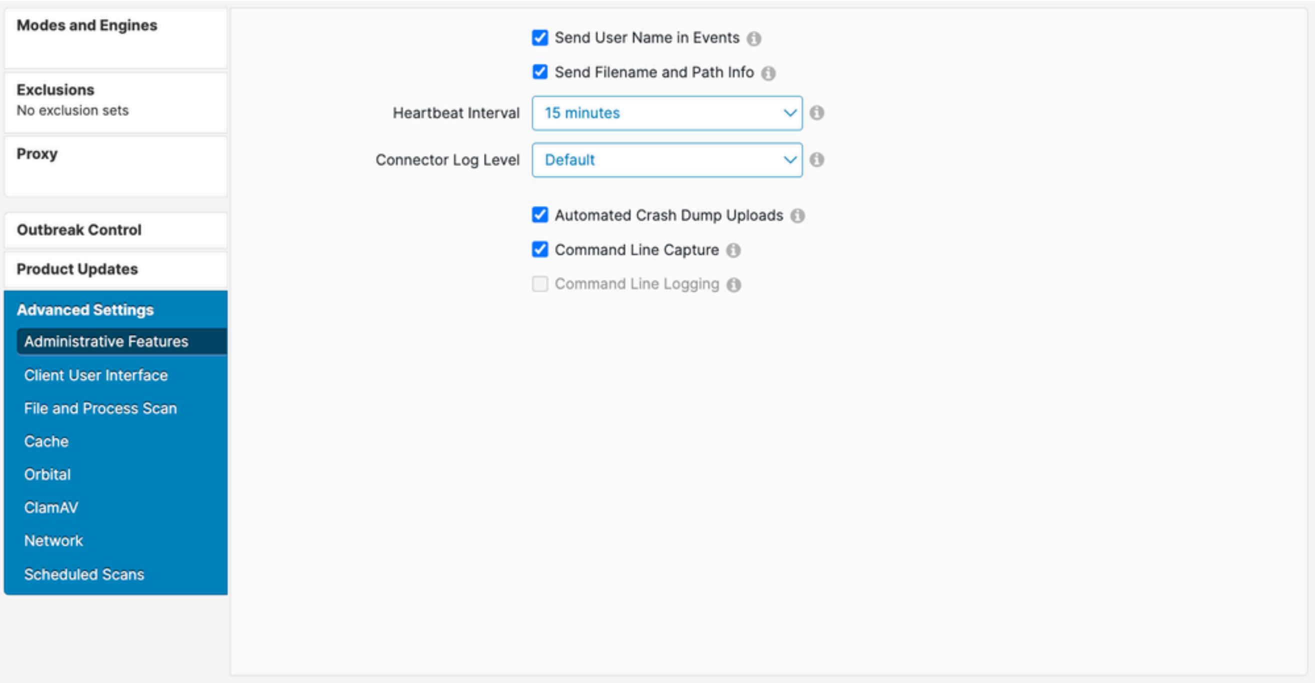
Behavioral Protection: [✓ Protect] Audit Disabled

Detect malicious activity, take remedial actions as needed, and report it.

Detection Engines

☑ ClamAV

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



☑ Send User Name in Events

☑ Send Filename and Path Info

Heartbeat Interval: 15 minutes

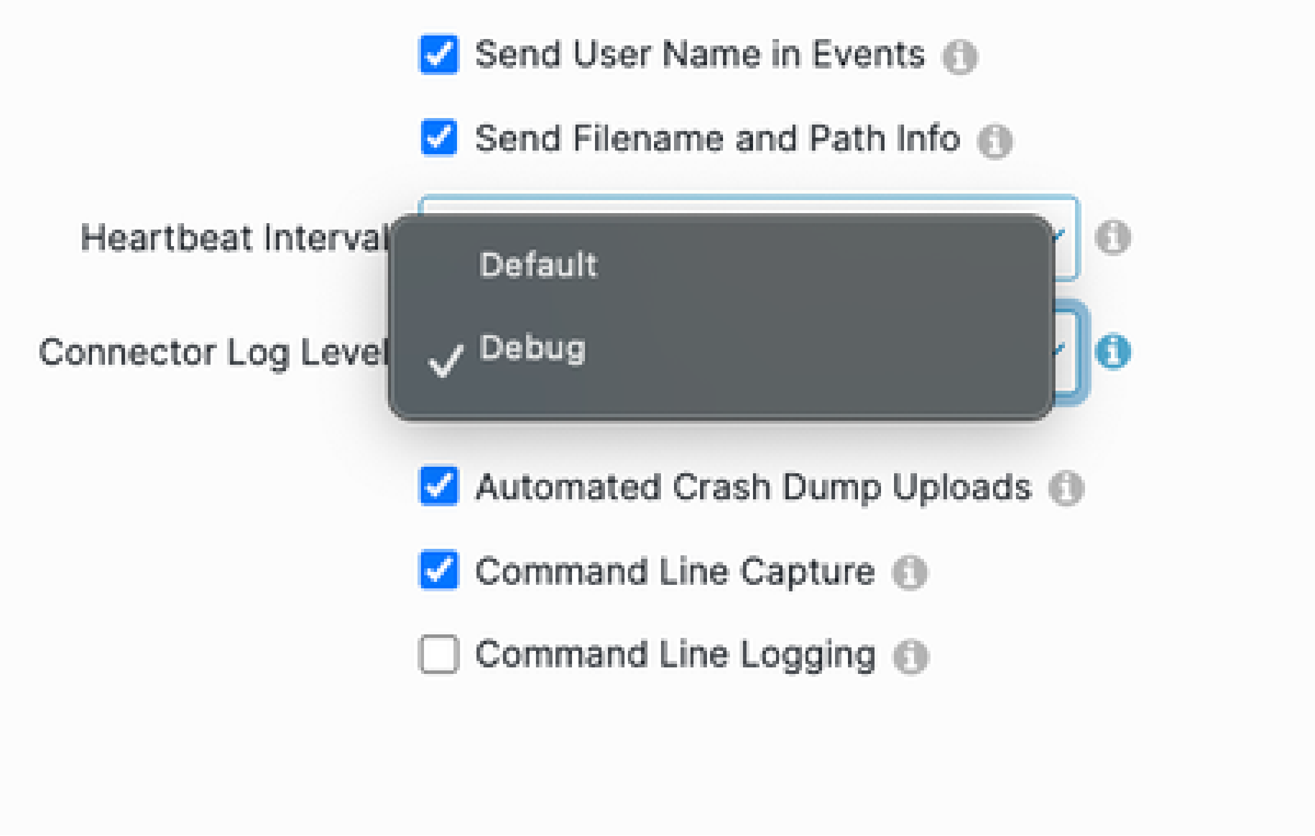
Connector Log Level: Default

☑ Automated Crash Dump Uploads

☑ Command Line Capture

□ Command Line Logging

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



☑ Send User Name in Events

☑ Send Filename and Path Info

Heartbeat Interval

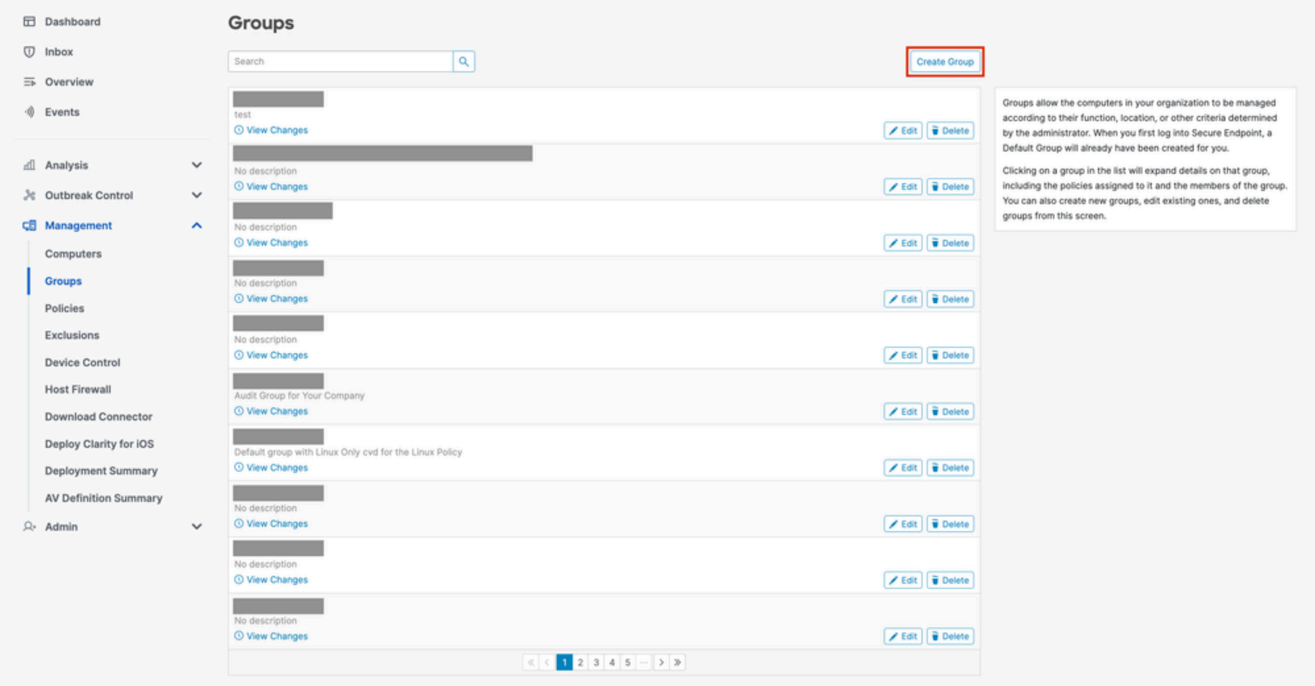
Connector Log Level

☑ Automated Crash Dump Uploads

☑ Command Line Capture

□ Command Line Logging

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.



[redacted]
test

[redacted]
No description

[redacted]
No description

[redacted]
No description

[redacted]
No description

[redacted]
Audit Group for Your Company

[redacted]
Default group with Linux Only cvd for the Linux Policy

[redacted]
No description

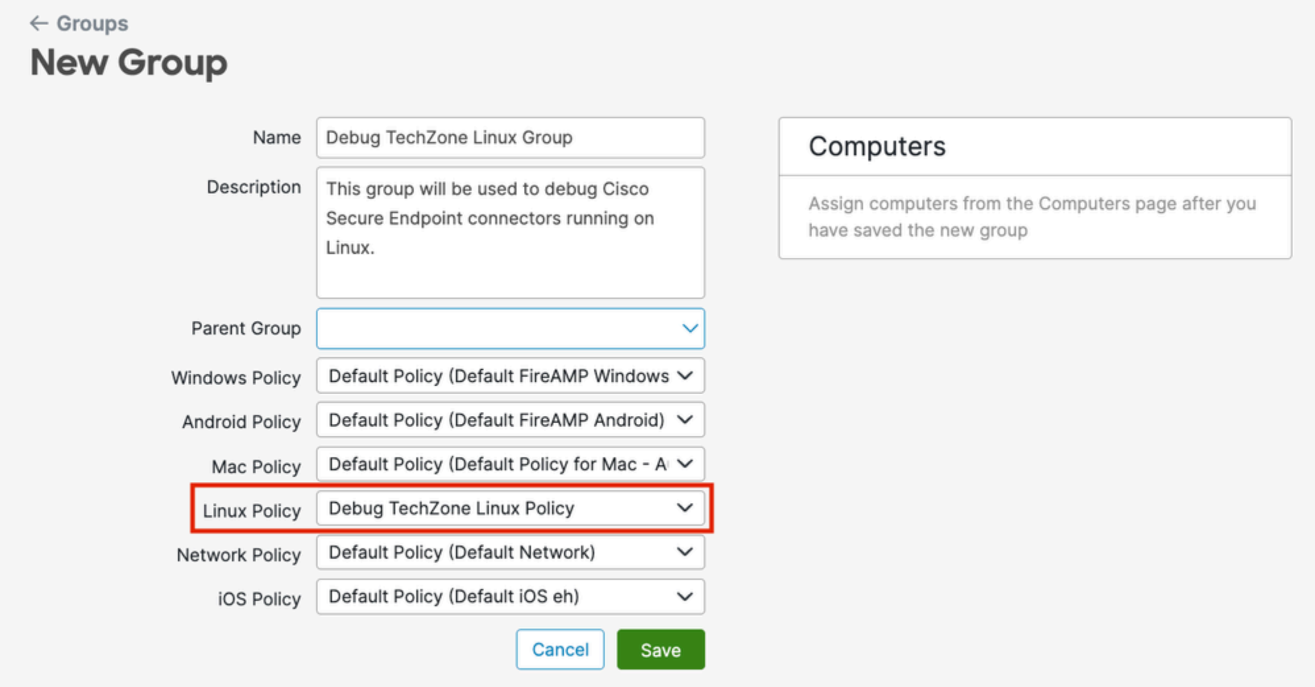
[redacted]
No description

[redacted]
No description

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 Default Group will already have been created for you.

Clicking on a group in the list will expand details on that group, including the policies assigned to it and the members of the group. You can also create new groups, edit existing ones, and delete groups from this screen.

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`.



Name: Debug TechZone Linux Group

Description: This group will be used to debug Cisco Secure Endpoint connectors running on Linux.

Parent Group:

Windows Policy: Default Policy (Default FireAMP Windows

Android Policy: Default Policy (Default FireAMP Android)

Mac Policy: Default Policy (Default Policy for Mac - A

Linux Policy: Debug TechZone Linux Policy

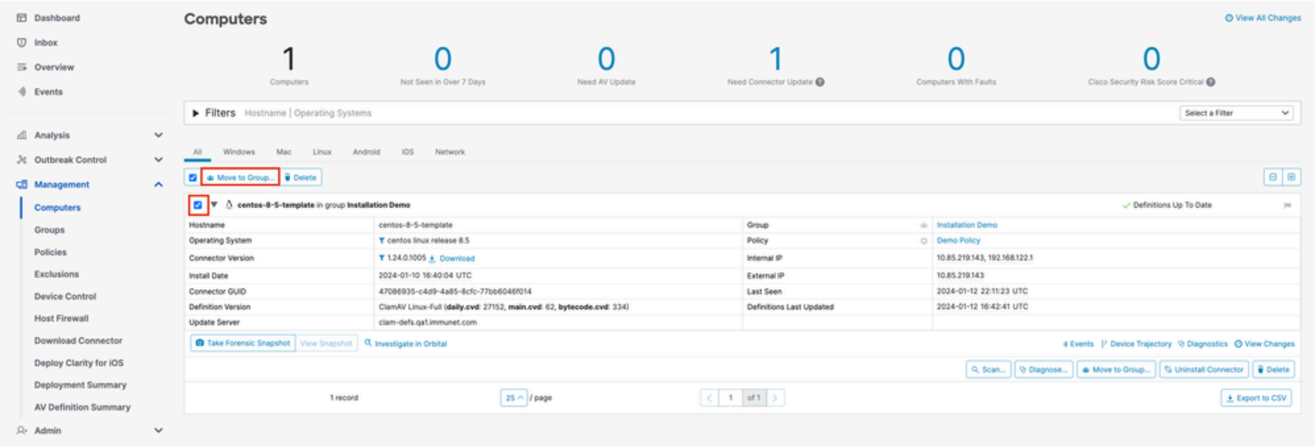
Network Policy: Default Policy (Default Network)

iOS Policy: Default Policy (Default iOS eh)

Computers

Assign computers from the Computers page after you have saved the new group

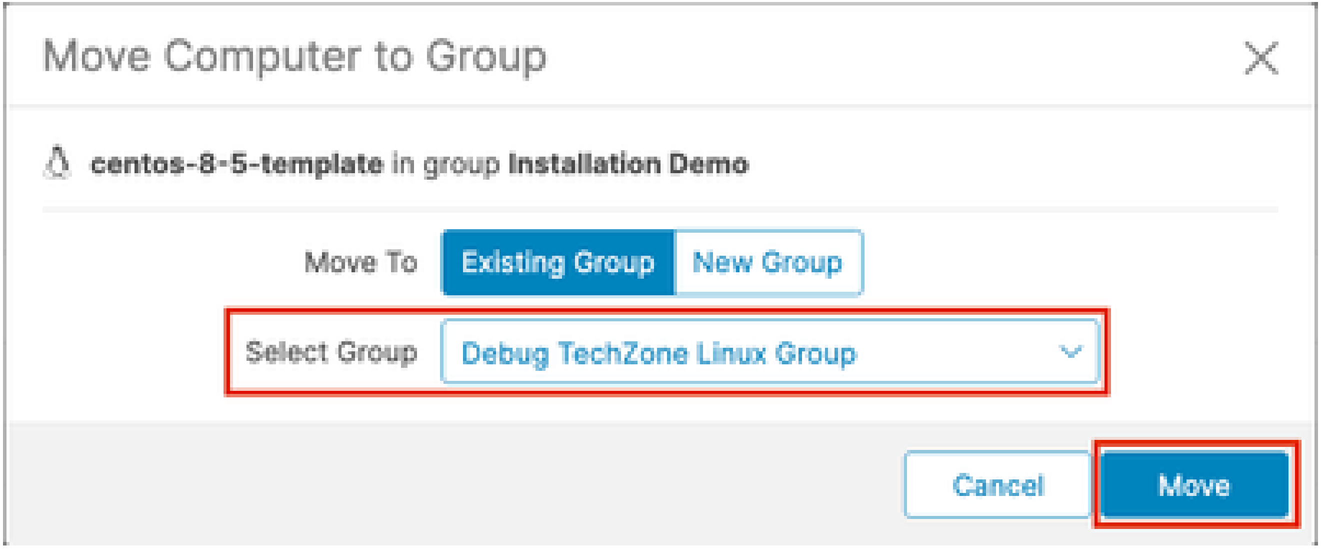
12. Navigate to the Computers page by selecting `Management` -> `Computers` and identify your computer in the list. Select it and click `Move to Group...`.



☑ centos-8-5-template in group **Installation Demo** ✓ Definitions Up To Date

Hostname	centos-8-5-template	Group	Installation Demo
Operating System	centos linux release 8.5	Policy	Demo Policy
Connector Version	1.24.0.1005 Download	Internal IP	10.85.219.143, 192.168.122.1
Install Date	2024-01-10 16:40:04 UTC	External IP	10.85.219.143
Connector GUID	47086935-c4d9-4a85-8cfc-77bb6046f014	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
Update Server	clam-defs.qa1.immunet.com		

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.



centos-8-5-template in group **Installation Demo**

Select Group: Debug TechZone Linux Group

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 enable the Debug mode using the Secure Endpoint Console, 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

- Cisco Secure Endpoint Connector for Mac Diagnostic Data Collection
- Technical Support & Documentation - Cisco Systems