Enable Debug on Endpoint from AMP for Endpoint Console

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Problem
<u>Configure</u>
Step 1: Identify the Endpoint to be Moved to Debug
Step 2: Duplicate the Existing Policy
Step 3: Configure the Log Level to Debug this Policy
Step 4: Create New Group and Link that New Policy
Step 5: Move the Identified Endpoint to this New Group
Step 6: Verify the Endpoint in Computer's Page and in Connector UI

Introduction

This document describes how to Enable Debug on the Endpoint from Cisco Secure Endpoint Console.

Prerequisites

Requirements

Before you begin, ensure you have:

- Administrative access to the Cisco Secure Endpoint for Endpoints console.
- The endpoint you wish to take debug is already registered in Cisco Secure Endpoint

Components Used

The information used in the document is based on these software versions:

- Cisco Secure Endpoint Console version 5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7 and later
- Microsoft Windows Operative System

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

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

The diagnostic data includes information such as:

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

Problem

Enable Debug on Endpoint from Cisco Secure Endpoint Console is required during one of the these scenarios.

Scenario 1: If you reboot the device, enable Debug mode from the IP Tray interface or it does not survive reboot. In case bootup debug logs are required, you can enable Debug mode from the policy configuration in the Secure Endpoint console.

Scenario 2: If you experience performance issues with the Cisco Secure Endpoint Connector on a device, enabling Debug mode can help gather detailed logs for analysis.

Scenario 3: When troubleshooting specific issues with the Secure Endpoint Connector, detailed logs can provide insights into the root cause of the problem.

Configure

Complete these steps to successfully enabled debug mode on the specified endpoint through the Secure Endpoint Console.

Step 1: Identify the Endpoint to be Moved to Debug

- 1. Log in to Cisco Secure Endpoint console. From the main dashboard, navigate to the **Management** section.
- 2. Navigate to **Management > Computers.**
- 3. **Identify** and **note** the endpoint that requires debug mode.

Step 2: Duplicate the Existing Policy

1. Navigate to **Management > Policies.**



- 2. Locate the policy currently applied to the identified endpoint.
- 3. Click the **policy** to expand the policy window.
- 4. Click **Duplicate** to create a copy of the existing policy.

etection and Response	Exclusion Sets	Custom Detections	Groups
les Querantine Interorik Block Block Querantine	Cisco-Maintained Microsoft Windows Default	Simple Not configured Advanced Not configured	TEST
ystem Process Protec. Protect cript Protection Quarantine		Application Control	
splot Prevention Block splot Prevention Scrip., Audit		Alow Not configured	
ehavioral Protection Protect ETRA Offine File Scan Disabled		Block Not configured	
esital Enabled		Network Control	
evice Control		Not configured	
58 Mass Stora Not configured			Proxy

Step 3: Configure the Log Level to Debug this Policy

- 1. Select and expand the **duplicated policy** window.
- 2. Click **Edit** and rename the policy (For example, Debug TechZone Policy).
- 3. Click Advanced Settings.
- 4. Select Administrative Features from the sidebar.
- 5. Set both the **Connector Log Level** and **Tray Log Level** to Debug.
- 6. Click **Save** to save the changes.

Policies Edit Policy Windows		
Name	Debug TechZone Policy	
Description	Taking debug on endpoint	
Modes and Engines	Stend User Name in Events ()	
Exclusiona 1 exclusion set	Heartbeat Interval 15 minutes · 0	
Prosy	Connector Log Level Debug - 0	
Host Firewall	Tray Log Level Debug 90	
Outlaneak Central Device Central	Connector Protection Password 0	
Product Updates	Automated Crash Dump Uploads ()	
Administrative Features	Command Line Capture ()	
Client User Interface File and Process Scan		
Cache Endpoint Isolation		
Orbital Engines		
TETRA Notwork		
Scheduled Scare		
		Cancel Save

Step 4: Create New Group and Link that New Policy

1. Navigate to **Management > Groups.**



- 2. Click **Create Group** near the top-right side of your screen.
- 3. Enter a name for the **group** (For example, Debug TechZone Group.)
- 4. Change the **Policy** from the default to the newly created debug policy.
- 5. Click Save.

Name	Debug TechZone Group		Computers
Description	This Group is used to Debug Cisco S Endpoint Connector	ecure	Assign computers from the Computers page after you have saved the new group
Parent Group		-	
Windows Policy	Debug TechZone Policy	~	
Android Policy	Default Policy (Protect)	~	
Mac Policy	Default Policy (Audit)	~	
Linux Policy	Default Policy (Audit)	v	
Network Policy	Default Policy (Default Network)	×	
iOS Policy	Default Policy (Audit)	~	

Step 5: Move the Identified Endpoint to this New Group

1. Navigate back to **Management > Computers.**

Clarke Secure Endpoint

≡			Management	×
	Dashboard		Computers	~
1 ©	Inbox		Groups	
	Overview		Policies	
۲	Events		Exclusions Device Control	
dd	Analysis	>	Deployment	
×	Outbreak Control	>	Download Connector	
	Management		Deploy Clarity for iOS	
20	Administration	>	Deployment Summary AV Definition Summary	

2. Select the **identified endpoint** from the list.

3. Click Move to Group.

• • • • • • • • • • • • • • • • • • •	prive TRMT			
Rodrate	045470P-MeGew0P	(integration of the second sec		Tist
Operating System	Bindows 10 Pro (Bulle 18045.4528)	Pulky	0	PLST
Connector terratori	T 8-K030001 1 Drew download URL	Internal IP		0
Install Onlin	2024 47-25 15-03/13 67	External IP		0
Convector 94/8	210tec76-010a-4784-ace8-ct/05e8096c98	Last Seen		2024-01-25 19:42:50 /67
Processor D	0%6/6/%000008/17	DP algorithms remained		100%
Class Secure Client ID	N/A	Cisco Security Hist Score	0	Pandrig.
Children Taransis Encounted	Report Recording to Child			a Dente - If Dente Transfory - 10 Deposition - © Hex Charges
		9, 5cm.][2 Daprose

4. Select the **newly created group** from the **Select Group** drop-down menu.

5. Click **Move** to move the selected endpoint into the new group.

Move Computers to	Group	\times	
III DESKTOP- in gr	roup TEST		
Move To	Existing Group New Group		
Select Group	Debug TechZone Group	~	
		Cancel Move	

Step 6: Verify the Endpoint in Computer's Page and in Connector UI

- Ensure the endpoint is listed under the new group in the Computers page.
 On the endpoint, open the Secure Endpoint connector UI.
- 3. Verify that the new debug policy is applied by checking the **Secure Endpoint** icon in the **menu** bar.



Secure Client

Secure Endpoint

stistics	Update	Advanced		
Agen	t			
Status:			Connected	
Version	i:		8.4.0.30201	
GUID:			202dac7b-093a-4784-ace8-cb95e8696c96	
Last Sc	an:		Today 03:03:18 PM	
Isolatio	n:		Not Isolated	
Polic	у ———			
Name:			Debug TechZone Policy	
Serial N	lumber:		229	
Last Up	date:		Today 03:52:38 PM	
© 0	isco Secu	ure Client	×	
(Secure End Connected.	lpoint:	
	~	Flash Scan	 ✓ Start 	



Note: Debug mode can only be enabled if a Cisco Technical Support Engineer requests this data. Keeping debug mode enabled for an extended period can fill up disk space quickly and can prevent the connector Log and Tray Log data from being gathered in the Support Diagnostic file due to excessive file size.

Contact Cisco support for further assistance.

Cisco Worldwide Support Contacts