Troubleshoot Secure Endpoint Stuck in Isolation with Recovery Methods

Contents

Introduction Prerequisites Requirements Components Used Background Information Stop Isolation Stop Isolation Session from the Console Stop Isolation Session from the Command Line Recovery Troubleshoot Mac Recovery: Windows Recovery: Recovery Isolation Method from the Command Line Recovery Isolation Method Without the Command Line Verify Related Information

Introduction

This document describes the process to recover an endpoint with the Secure Endpoint connector installed from isolation mode.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Endpoint Connector
- Secure Endpoint Console
- Endpoint Isolation feature

Components Used

The information in this document is based on these software and hardware versions:

- Secure Endpoint console version v5.4.2021092321
- Secure Endpoint Windows connector version v7.4.5.20701
- Secure Endpoint Mac connection version v1.21.0

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 procedure described in this document is helpful in situations where the endpoint device is stuck in this state and it is not possible to disable isolation mode.

Endpoint isolation is a feature that lets you block network activity (IN and OUT) on a computer to prevent threats such as data exfiltration and malware propagation. It is available on:

- 64-bit versions of Windows that support version 7.0.5 and later of the Windows connector
- Mac versions that support version 1.21.0 and later of the Mac connector.

Endpoint isolation sessions do not affect communication between the connector and the Cisco cloud. There is the same level of protection and visibility on your endpoints as before the session. You can configure IP Isolation Allow Lists of addresses in order to avoid that the connector blocks the IP addresses in question while an active endpoint isolation session is active. You can review more detailed information about the Endpoint Isolation feature <u>here</u>.

Stop Isolation

Once you want to stop the Endpoint Isolation on a computer, do these quick steps via the Secure Endpoint console or command line.

Stop Isolation Session from the Console

In order to stop an isolation session and restore all network traffic to an endpoint.

- Step 1. In the console, navigate to **Management > Computers**.
- Step 2. Locate the computer you want to stop isolation and click to display details.
- Step 3. Click the Stop Isolation button, as shown in the image.

🗌 🔻 👯 DESKTOP-075I5MB in group testing bremarqu 🗸 Definitions Up To Date						
Se Isolated						
Hostname	DESKTOP-075I5MB	Group 👜	testing bremarqu			
Operating System	Windows 10 Pro	Policy 🔅	Copy of bremarqu_mssp			
Connector Version	7.4.5.20701	Internal IP				
Install Date	2021-09-28 20:02:16 CDT	External IP	\sim			
Connector GUID	41010012-0100-1700-0101-010002-000-	Last Seen	2021-09-28 23:39:08 CDT			
Definition Version	TETRA 64 bit (daily version: 85768)	Definitions Last Updated	2021-09-28 21:28:59 CDT			
Update Server	tetra-defs.amp.cisco.com					
Processor ID	0000777044440044					
Sevents P Device Trajectory U Diagnostics ① View Changes						
🐹 Stop Isolation 🔍 Scan 😲 Diagnose 🏕 Move to Group 📦 Delete						

Step 4. Enter any comments about why you stopped the isolation feature on the endpoint.

Stop Isolation Session from the Command Line

If an isolated endpoint loses its connection to the Cisco cloud, and you are unable to stop the isolation session from the console. In these situations, you can stop the session locally from the command line with the unlock code.

Step 1. In the console, navigate to **Management > Computers**.

Step 2. Locate the computer you want to stop isolation and click to display details.

Step 3. Note the Unlock Code, as shown in the image.

- 🗸 🕊	DESKTOP-075I5MB in group testing bremarqu	✓ Definitions Up To Date			
V 😵 Isolat	d				
2021-09-28	21:33:48 CDT	Isolated for less than a r	minute	Unlock Code:fv	wq8qw
Isolated	2021-09-28 21:33:48 CDT				
Isolating	2021-09-28 21:33:46 CDT	Brenda M	Unlock Code: fwq8qw		

Step 4. You can also find the **Unlock Code** if you navigate to **Account > Audit Log**, as shown in the image.

Isolation Started DESKTOP	-O75I5MB bremarqu+	2021-09-28 21:33:48 CDT		
▼ Isolation Start Requested □ DESKTOP-	075I5MB	10010010100 V 2021-09-28 21:33:46 CDT		
Attribute	Old	New		
Comment	None	None		
ID	None	07200270-0000-4014-0000-24000100110		
Unlock Code	None	fwq8qw		

Step 5. On the isolated computer, open a command prompt with administrator privileges.

Step 6. Navigate to the directory where the connector is installed

Windows: C:\Program Files\Cisco\AMP\[version number]

Mac: /opt/cisco/amp

Step 7. Run the stop command

Windows: sfc.exe -n [unlock code]

C:\Program Files\Cisco\AMP\7.4.5.20701>sfc.exe -n fwq8qw

C:\Program Files\Cisco\AMP\7.4.5.20701>

Caution: If the unlock code is entered incorrectly 5 times, it is necessary to wait 30 minutes before you make another unlock attempt.

Recovery Troubleshoot

In case you exhausted all avenues and you are still unable to recover an isolated endpoint from the Secure Endpoint console or locally with the unlock code; you can recover the isolated endpoint with the emergency recovery methods.

Mac Recovery:

Remove the isolation configuration and restart the Secure Endpoint Service

sudo rm /Library/Application\ Support/Cisco/Secure\ Endpoint/endpoint_isolation.xml sudo launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist sudo launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist

Windows Recovery:

Recovery Isolation Method from the Command Line

In situations where your endpoint device is stuck in isolation and it is not possible to disable isolation via the Secure Endpoint console or with the unlock code, do these steps.

Step 1. Stop the connector service via the connector user interface or **Windows Services**.

Step 2. Locate the Secure Endpoint connector service and stop the service.

Step 3. On the isolated computer, open a command prompt with administrator privileges.

Step 4. Run the command **reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f** as shown in the image.

reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
C:\Windows\system32>reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
The operation completed successfully.
C:\Windows\system32>

Step 5. The message **The operation completed successfully** indicates the operation was completed. (If another message is displayed, as "Error: Access is denied" you need to stop the Secure Endpoint connector service prior that you run the command).

Step 6. Start the Secure Endpoint connector service.

Tip: If you are unable to stop the Secure Endpoint connector service from the connector user interface or Windows Services, you can do a Safe boot.

On the isolated endpoint, navigate to **System Configuration > Boot > Boot options** and select **Safe boot**, as shown in the image.

system comigatation			
nera Boot Services Startup	Tools		
Vindows 10 (C:\Windows) : Currer	nt OS; Default OS		
Advanced options Set a	as default Delete		
Root options		Timeout	
CZ Safe hoot	No Cill boot	30	seconds
Sale boot	Boot log		
1 J MIDION 1			
Alternate shell	Base video		
Alternate shell Active Directory repair	Base video	Make all	boot settings
Alternate shell Active Directory repair Network	Base video OS boot information	Make all permane	boot settings ent
Alternate shell Active Directory repair Network	Base video OS boot information	Make all permane	boot settings ent

Recovery Isolation Method Without the Command Line

In case your endpoint device is stuck in isolation and it is not possible to disable isolation via the Secure Endpoint console or with the unlock code or even if you are unable to use the command line, do these steps:

Step 1. Stop the connector service via the connector user interface or **Windows Services**.

Step 2. Navigate to the directory where the connector is installed (C:\Program Files\Cisco\AMP\) and delete the file **jobs.db**, as shown in the image.

🔤 « Ci	sco > AMP > V	õ	, Search AMP	
	Name		Date modified	Туре
۰ د	scriptid		9/28/2021 8:01 PM	File folder
	tetra		9/28/2021 8:31 PM	File folder
Я	tmp		9/28/2021 9:23 PM	File folder
*	update		9/28/2021 9:27 PM	File folder
*	URLScanner		9/28/2021 8:01 PM	File folder
	2021-09-28 20-02-11.etl		9/28/2021 9:23 PM	ETL File
	cache		9/28/2021 9:23 PM	Data Base File
	event		9/28/2021 9:23 PM	Data Base File
	filetypes	-	9/28/2021 8:01 PM	XML Document
	istory		9/28/2021 9:23 PM	Data Base File
	🗟 historyex 🦯		9/28/2021 9:23 PM	Data Base File
[💿 jobs		9/28/2021 9:23 PM	Data Base File
	local.old		9/28/2021 9:23 PM	OLD File
	🕋 local		9/28/2021 9:23 PM	XML Document

3. Reboot the computer.

Additionally, if you see the Isolation event in the console, you can navigate to **Error Details** in order to review the error code and its description, as shown in the image.

failed to stop isolation			🖵 🖓 🗞 Isolation Stop	Failed 2021-12-15 21:27:51 UTC
Connector Details	Error Code	3240624137		
Comments	Description	Invalid unlock code		
Error Details	Q Run Scan			

Verify

In order to verify the endpoint is back from isolation or is no longer isolated, you can see the Secure Endpoint connector user interface displays the Isolation status as **Not Isolated**, as shown in the image.



From the Secure Endpoint console, if you navigate the **Management > Computers**, and locate the computer in question, you can click to display details. The Isolation status displays **Not Isolated**, as shown in the image.

🕞 🔻 💐 DESKTOP-075ISMB in group testing bremarqu 🗸 Detroitons Up To Date 🛛					75I5M8 in group testing bremarqu		✓ Definitions Up To Date IIII
▶ Stolated			R Not Isolated				
Hostname	DESKTOP-075I5MB	Group da	testing bremarqu	Hostname	DESKTOP-075I5MB	Group da	testing bremarqu
Operating System	Windows 10 Pro	Policy 🔅	Copy of bremarqu_mssp	Operating System	Windows 10 Pro	Policy 🔅	Copy of bremargu_mssp
Connector Version	7.4.5.20701	Internal IP		Connector Version	7.4.5.20701	Internal IP	
Install Date	2021-09-28 20:02:16 CDT	External IP		Install Date	2021-09-28 20:02:16 CDT	External IP	
Connector GUID		Last Seen	2021-09-29 10:37:11 CDT	Connector GUID		Last Seen	2021-09-29 10:39:58 CDT
Definition Version	TETRA 64 bit (daily version: 85769)	Definitions Last Updated	2021-09-28 23:01:58 CDT	Definition Version	TETRA 64 bit (daily version: 85769)	Definitions Last Updated	2021-09-28 23:01:58 CDT
Update Server	tetra-defs.amp.cisco.com			Update Server	tetra-defs.amp.cisco.com		
Processor ID				Processor ID			
4 Events 12 Device Trajectory 13 Diagnostics (3) View Changes			4 Events 1 ⁴ Device Trajectory 19 Diagnostics (3) View Char			Device Trajectory 🕲 Diagnostics 💿 View Changes	
🐹 Stop Isolation 🔍 Scan 🔮 Diagnose) 🕸 Move to Group) 🗃 Delete			💱 Start Isolation 🔍 Scan 🕅 Diagnose) 🕼 Move to Group) 📦			Diagnose 🏼 🏙 Move to Group 🗑 Delete	

Related Information

- Secure Endpoint User Guide
- <u>Technical Support & Documentation Cisco Systems</u>