Troubleshoot Secure Endpoint Stuck in Isolation with Recovery Methods

Contents

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 here.

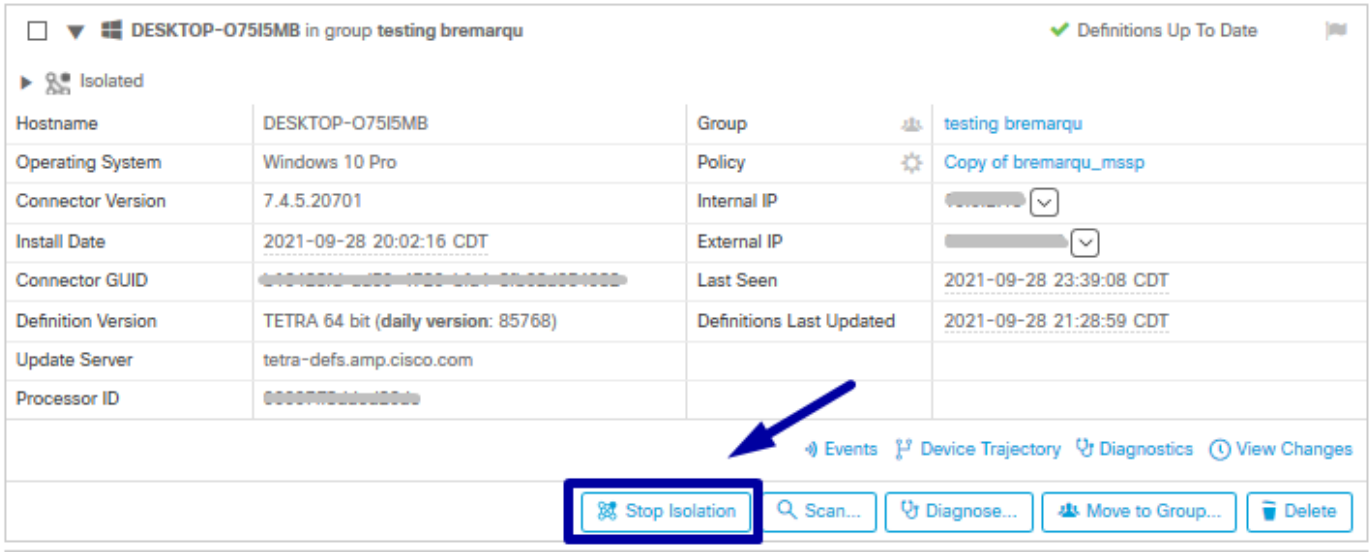
Stop Isolation

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.



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

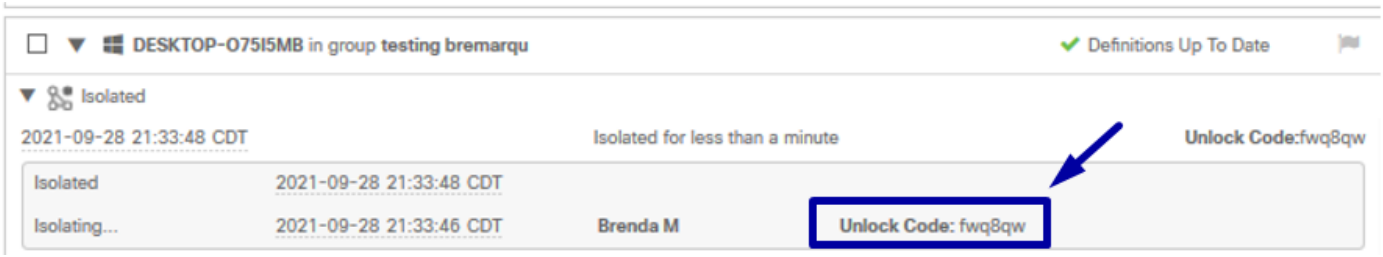
Stop Isolation Session from the Command Line

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.

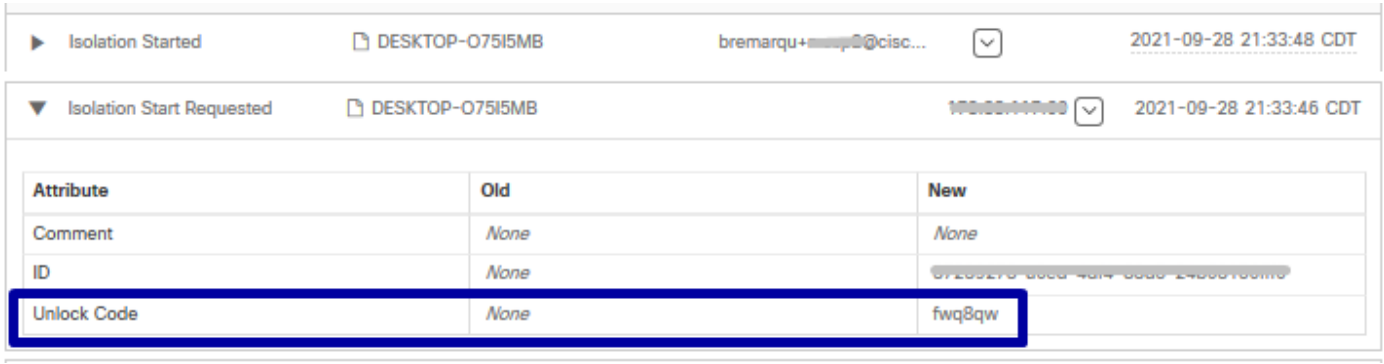
Step 1. In the console, navigate to **Management > Computers**.

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.



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



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

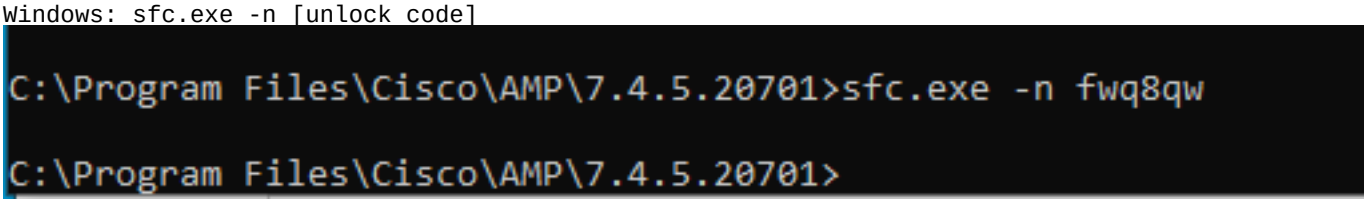
Step 6. Navigate to the directory where the connector is installed

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

Mac: /opt/cisco/amp

Step 7. Run the stop command

```
Windows: sfc.exe -n [unlock code]
```




```
Mac: ampcli isolate stop [unlock code]
```

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.

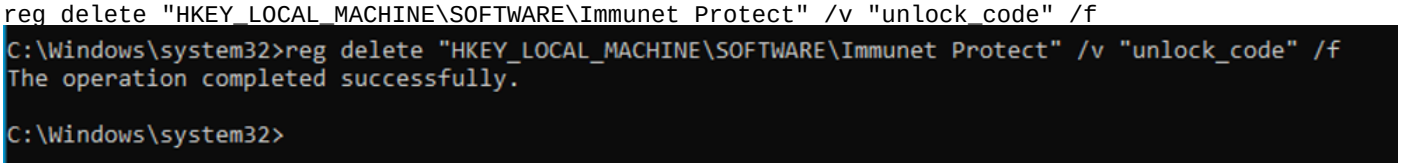
Step 1. Stop the connector service via the connector user interface or **Windows Services**.

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
```

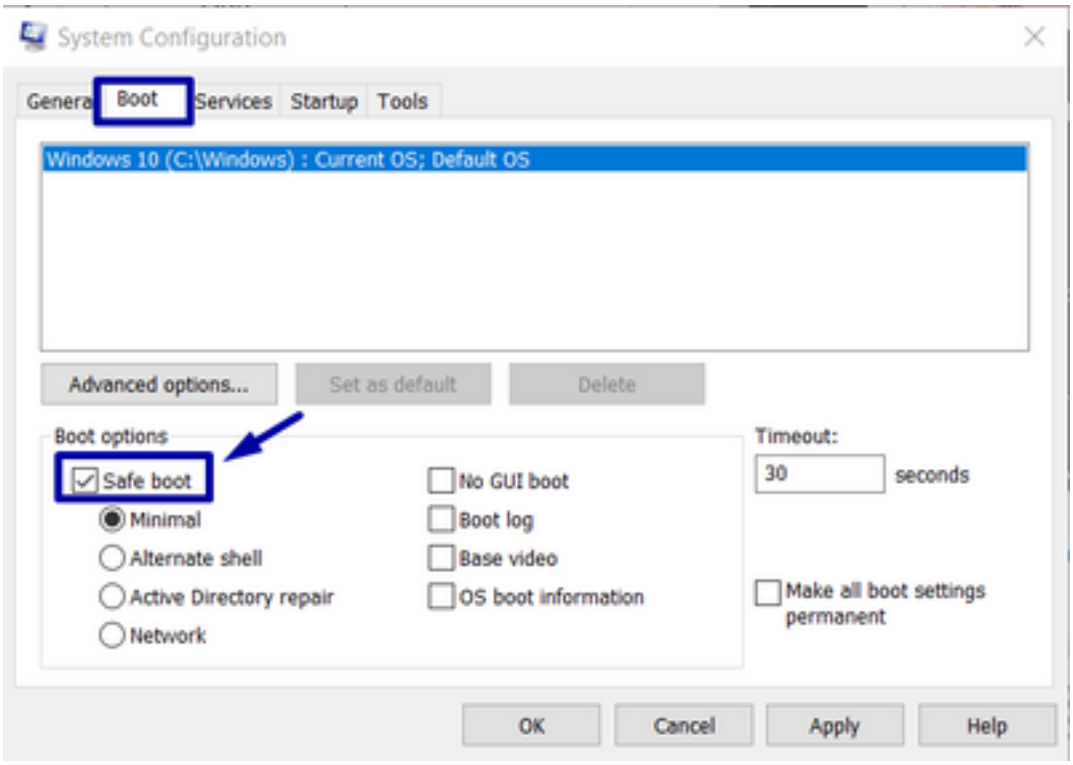


Step 5. The message **The operation completed successfully** indicates the operation was completed. (If another message is displayed, as "Error: Access is denied" you need to stop the Secure Endpoint connector service prior that you run the command).

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.

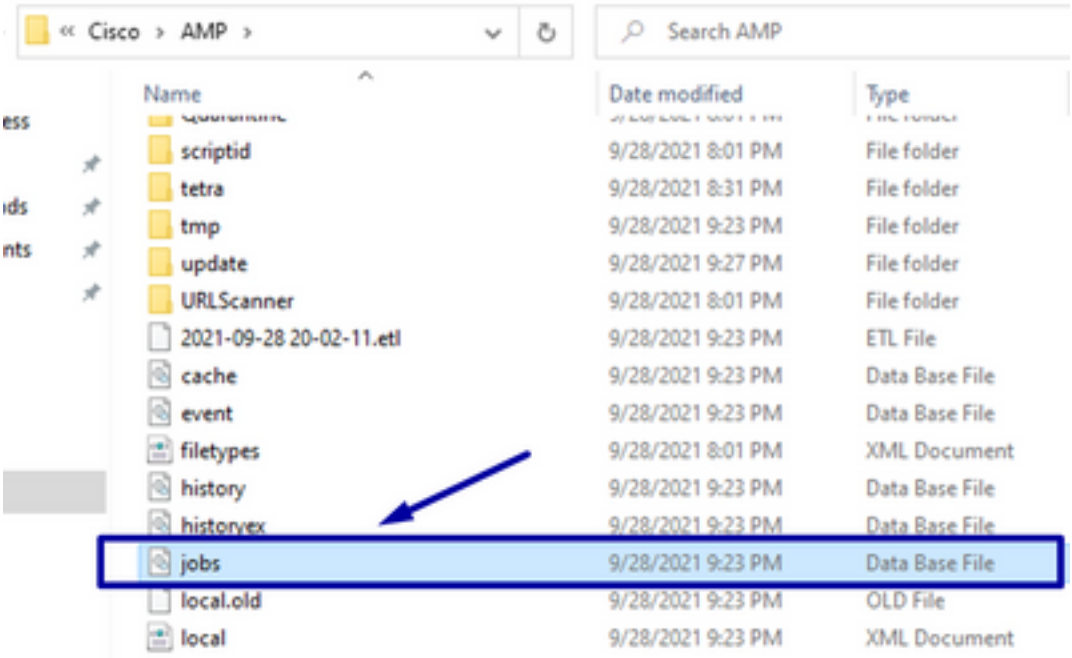


Recovery Isolation Method Without the Command Line

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.



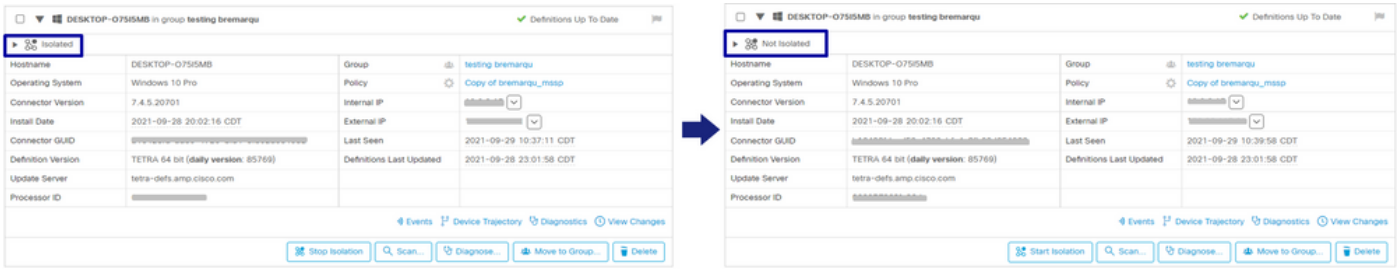
3. Reboot the computer.

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.

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.



Related Information

- [Secure Endpoint User Guide]
- [Technical Support & Documentation - Cisco Systems]