

# 回復方法を使用して隔離されたセキュアエンドポイントの問題をトラブルシューティングする

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[分離の停止](#)

[コンソールからの分離セッションの停止](#)

[コマンドラインからの分離セッションの停止](#)

[回復のトラブルシューティング](#)

[Macリカバリ:](#)

[Windowsの回復:](#)

[コマンドラインからのリカバリ分離方法](#)

[コマンドラインを使用しないリカバリ分離方法](#)

[確認](#)

[関連情報](#)

## 概要

このドキュメントでは、分離モードからインストールされたセキュアエンドポイントコネクタを使用してエンドポイントを回復するプロセスについて説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- セキュアエンドポイントコネクタ
- セキュアエンドポイントコンソール
- エンドポイント分離機能

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Endpointコンソールバージョンv5.4.2021092321
- Secure Endpoint Windowsコネクタバージョンv7.4.5.20701
- セキュアエンドポイントMac接続バージョンv1.21.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

このドキュメントで説明する手順は、エンドポイントデバイスがこの状態のままになり、分離モードを無効にできない場合に役立ちます。

エンドポイントの分離は、コンピュータ上のネットワークアクティビティ（INおよびOUT）をブロックして、データの流出やマルウェアの伝播などの脅威を防止する機能です。次のサイトで入手できます。

- バージョン7.0.5以降のWindowsコネクタをサポートする64ビットバージョンのWindows
- Macコネクタのバージョン1.21.0以降をサポートするMacバージョン。

エンドポイント分離セッションは、コネクタとシスコクラウド間の通信に影響を与えません。エンドポイントには、セッション前と同じレベルの保護と可視性があります。アクティブなエンドポイント分離セッションがアクティブな間にコネクタが問題のIPアドレスをブロックすることを回避するために、アドレスのIP分離許可リストを設定できます。エンドポイント分離機能の詳細については、[ここ](#)を参照してください。

## 分離の停止

コンピュータでエンドポイントの分離を停止する場合は、セキュアエンドポイントのコンソールまたはコマンドラインから次の手順を実行します。

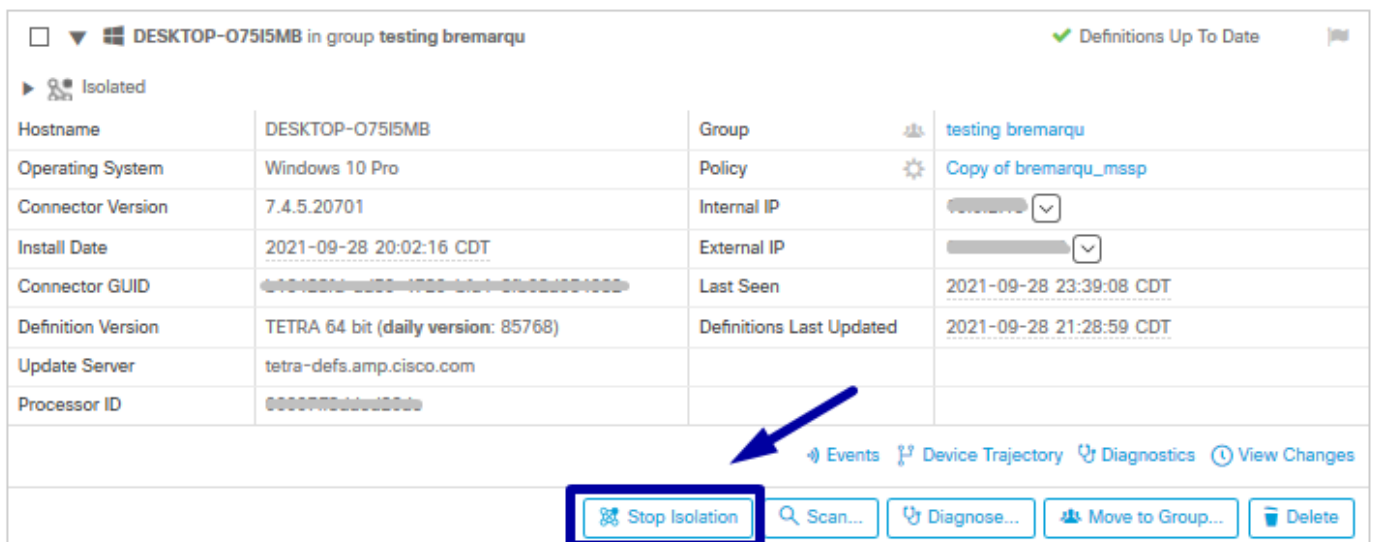
### コンソールからの分離セッションの停止

分離セッションを停止し、すべてのネットワークトラフィックをエンドポイントに復元する。

ステップ 1：コンソールで、[Management] > [Computers] に移動します。

ステップ 2：分離を停止するコンピューターを見つけて、クリックして詳細を表示します。

ステップ 3：図に示すように、[Stop Isolation] ボタンをクリックします。



DESKTOP-075I5MB in group testing bremarqu

Definitions Up To Date

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	
Connector GUID	44b422f2-4d50-4720-b1af-07b02d004020	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	0000070000000000		

Events Device Trajectory Diagnostics View Changes

Stop Isolation Scan... Diagnose... Move to Group... Delete

ステップ 4 : エンドポイントで隔離機能を停止した理由についてコメントを入力します。

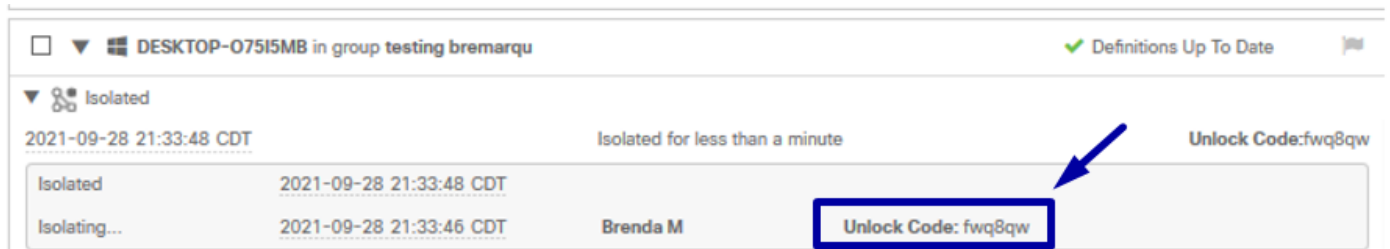
## コマンドラインからの分離セッションの停止

隔離されたエンドポイントがシスコクラウドへの接続を失い、コンソールから隔離セッションを停止できない場合。このような状況では、ロック解除コードを使用して、コマンドラインからローカルにセッションを停止できます。

ステップ 1 : コンソールで、[Management] > [Computers] に移動します。

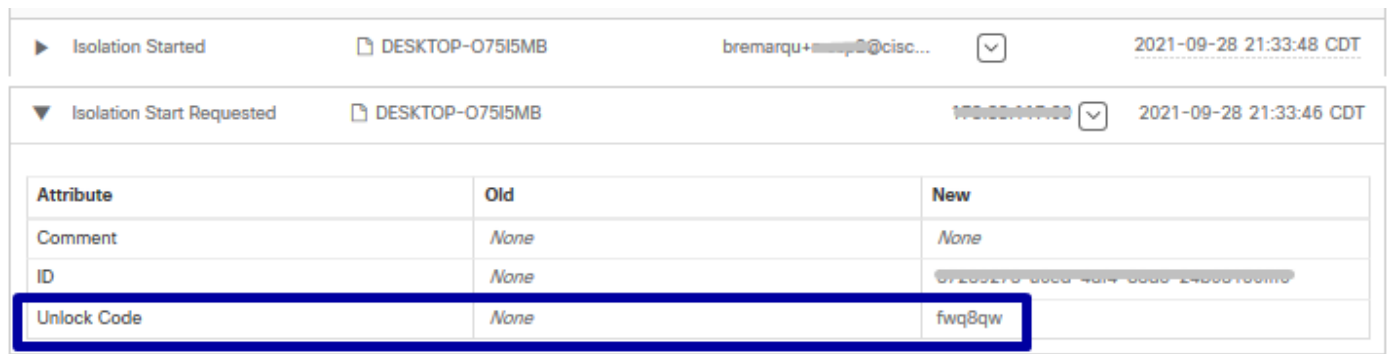
ステップ 2 : 分離を停止するコンピューターを見つけて、クリックして詳細を表示します。

ステップ 3 : 次の図に示すように、[Unlock Code] をメモします。



Isolated	2021-09-28 21:33:48 CDT	Isolated for less than a minute	Unlock Code:fwq8qw
Isolated	2021-09-28 21:33:48 CDT		
Isolating...	2021-09-28 21:33:46 CDT	Brenda M	Unlock Code: fwq8qw

ステップ 4 : 図に示すように、[Account] > [Audit Log] に移動して[Unlock Code] を見つけることもできます。



Attribute	Old	New
Comment	None	None
ID	None	07200270-0000-4014-0000-240001000000
Unlock Code	None	fwq8qw

ステップ 5 : 隔離されたコンピューターで、管理者特権を使用してコマンドプロンプトを開きます。

手順 6 : コネクタがインストールされているディレクトリに移動します

Windows:C:\Program Files\Cisco\AMP\[バージョン番号]

Mac:/opt/cisco/amp

手順 7 : stopコマンドを実行します。

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>
```

Mac: `ampcli isolate stop [unlock code]`

**注意：**ロック解除コードが5回誤って入力された場合は、再度ロック解除を試みる前に30分待つ必要があります。

## 回復のトラブルシューティング

すべての手段を使い果たしても、Secure Endpointコンソールから、またはロック解除コードを使用してローカルに、隔離されたエンドポイントを回復できない場合は、緊急回復方法を使用して隔離されたエンドポイントを回復できます。

## Macリカバリ：

分離設定を削除し、セキュアエンドポイントサービスを再起動します

```
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の回復：

### コマンドラインからのリカバリ分離方法

エンドポイントデバイスが隔離されたままになり、セキュアエンドポイントコンソールまたはアンロックコードを使用して隔離を無効にできない場合は、次の手順を実行します。

ステップ 1：コネクタユーザインターフェイスまたはWindows Servicesを使用して、コネクタサービスを停止します。

ステップ 2：Secure Endpoint Connectorサービスを見つけて、サービスを停止します。

ステップ 3：隔離されたコンピュータで、管理者特権を使用してコマンドプロンプトを開きます。

ステップ 4：次の図に示すように、コマンド`reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f`を実行します。

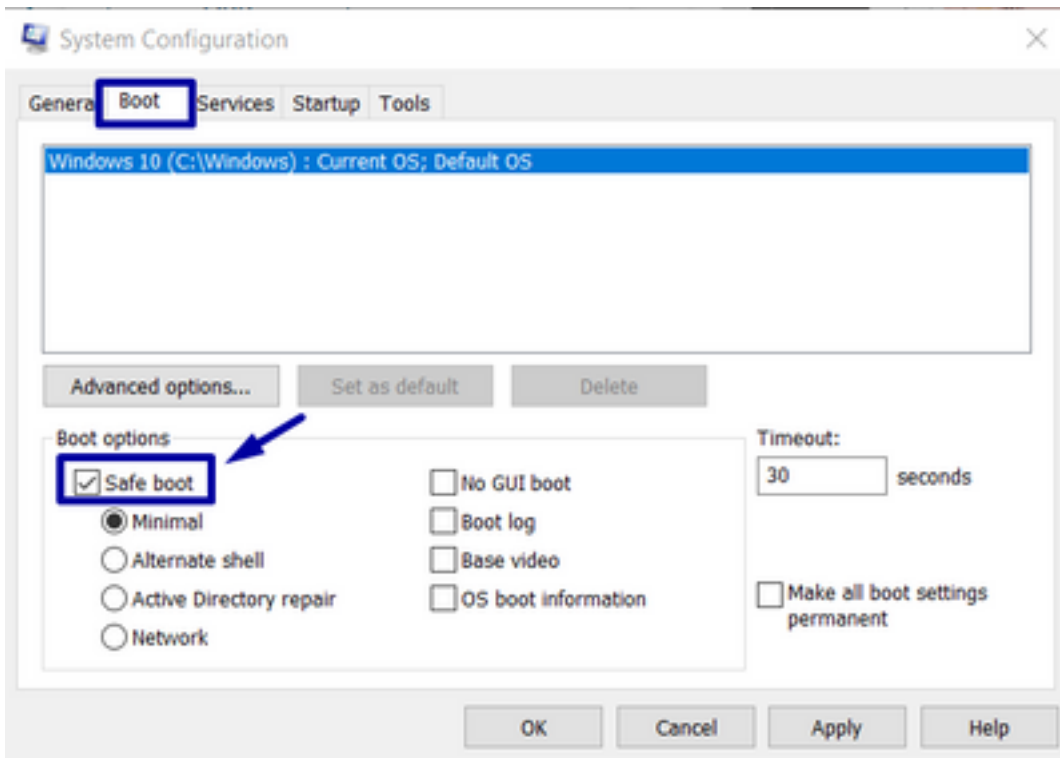
```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
C:\Windows\system32>reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
The operation completed successfully.
C:\Windows\system32>
```

ステップ 5：「The operation completed successfully」というメッセージは、操作が完了したことを示します。（「Error: Access is denied」という別のメッセージが表示された場合は、コマンドを実行する前にSecure Endpointコネクタサービスを停止する必要があります）。

手順 6：Secure Endpointコネクタサービスを開始します。

ヒント：コネクタのユーザーインターフェイスまたはWindowsサービスからセキュアエンドポイントコネクタサービスを停止できない場合は、セーフブートを実行できます。

隔離されたエンドポイントで、[System Configuration] > [Boot] > [Boot options] に移動し、図に示すように[Safe boot] を選択します。



## コマンドラインを使用しないリカバリ分離方法

エンドポイントデバイスが分離でスタックし、セキュアエンドポイントコンソールまたはロック解除コードを使用して分離を無効にできない場合、またはコマンドラインを使用できない場合は、次の手順を実行します。

ステップ 1：コネクタユーザーインターフェイスまたはWindows Servicesを使用して、コネクタサービスを停止します。

ステップ 2：図に示すように、コネクタがインストールされているディレクトリ (C:\Program Files\Cisco\AMP\) に移動し、ファイル jobs.db を削除します。

« Cisco > AMP > Search AMP

Name	Date modified	Type
scriptid	9/28/2021 8:01 PM	File folder
tetra	9/28/2021 8:31 PM	File folder
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
history	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.コンピュータを再起動します。

また、コンソールにIsolationイベントが表示されている場合は、[Error Details] に移動して、図に示すようにエラーコードとその説明を確認できます。

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**

## 確認

エンドポイントが分離から戻っているか、または分離されていないことを確認するには、図に示すように、セキュアエンドポイントコネクタのユーザーインターフェイスに[Isolation]ステータスが[Not Isolated]と表示されていることを確認します。

Secure Endpoint

Scan Now

History

Settings

Status: Connected  
Scanned: Never  
Policy: Copy of bremarqu\_mssp  
**Isolation: Isolated**

CISCO  
**SECURE**

About

➔

Secure Endpoint

Scan Now

History

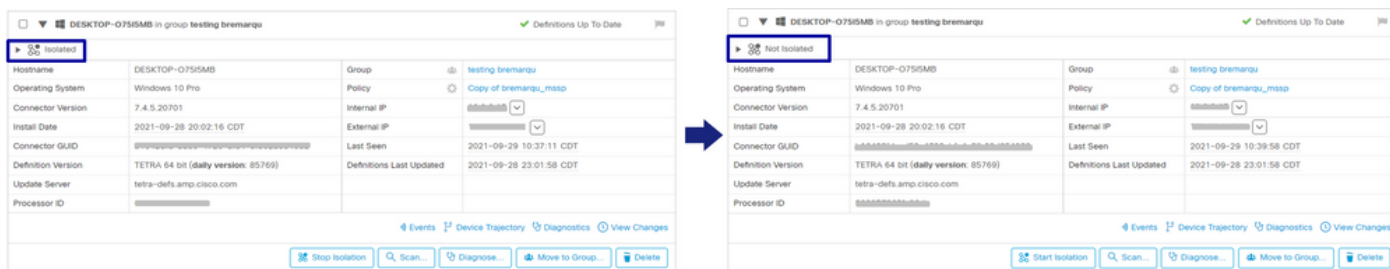
Settings

Status: Connected  
Scanned: Never  
Policy: Copy of bremarqu\_mssp  
**Isolation: Not Isolated**

CISCO  
**SECURE**

About

Secure Endpointコンソールから、[Management] > [Computers] に移動し、問題のコンピュータを見つけたら、クリックして詳細を表示できます。図に示すように、[Isolation]ステータスに[Not Isolated]が表示されます。



## 関連情報

- [セキュアエンドポイントユーザガイド](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。