

Fehlerbehebung bei isolierten, sicheren Endgeräten mit Wiederherstellungsmethoden

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Isolation beenden](#)

[Isolationssitzung von der Konsole aus anhalten](#)

[Beenden der Isolationssitzung über die Befehlszeile](#)

[Fehlerbehebung für Wiederherstellung](#)

[Mac-Wiederherstellung:](#)

[Windows-Wiederherstellung:](#)

[Wiederherstellungsisolationsmethode über die Befehlszeile](#)

[Recovery-Isolationsmethode ohne Befehlszeile](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird der Prozess zum Wiederherstellen eines Endpunkts beschrieben, bei dem der Secure Endpoint-Connector im Isolationsmodus installiert ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Endgeräteanschluss
- Konsole für sichere Endgeräte
- Funktion zur Endpunktisolierung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Version 5.4.2021092321 der Secure Endpoint-Konsole
- Secure Endpoint Windows Connector Version 7.4.5.20701
- Version 1.21.0 der Secure Endpoint Mac-Verbindung

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Das in diesem Dokument beschriebene Verfahren ist in Situationen hilfreich, in denen das Endgerät in diesem Zustand feststeckt und es nicht möglich ist, den Isolationsmodus zu deaktivieren.

Die Endpunktisolierung ist eine Funktion, mit der Sie Netzwerkaktivitäten (IN und OUT) auf einem Computer blockieren können, um Bedrohungen wie Datendiebstahl und Malwareverbreitung zu verhindern. Sie ist abrufbar unter:

- 64-Bit-Versionen von Windows, die Version 7.0.5 und höher des Windows-Connectors unterstützen
- Mac-Versionen, die Version 1.21.0 und höher des Mac-Connectors unterstützen.

Sitzungen zur Endpunktisolierung wirken sich nicht auf die Kommunikation zwischen dem Connector und der Cisco Cloud aus. Ihre Endgeräte sind genauso geschützt und transparent wie vor der Sitzung. Sie können IP-Isolation-Zulassungslisten (Allow Lists) von Adressen konfigurieren, um zu vermeiden, dass der Connector die betreffenden IP-Adressen blockiert, während eine aktive Endpunkt-Isolationssitzung aktiv ist. Detailliertere Informationen zur Endpunktisolierung finden Sie [hier](#).

Isolation beenden

Wenn Sie die Endpunktisolierung auf einem Computer beenden möchten, führen Sie die folgenden Schritte über die Konsole oder Befehlszeile von Secure Endpoint aus.

Isolationssitzung von der Konsole aus anhalten

Um eine Isolationssitzung zu stoppen und den gesamten Netzwerkverkehr an einen Endpunkt wiederherzustellen.

Schritt 1: Navigieren Sie in der Konsole zu **Verwaltung > Computer**.

Schritt 2: Suchen Sie den Computer, dessen Isolation Sie beenden möchten, und klicken Sie auf, um Details anzuzeigen.

Schritt 3: Klicken Sie auf die Schaltfläche **Isolation beenden**, wie im Bild dargestellt.

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	██████████-██████████-██████████-██████████-██████████	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	0000000000000000		

Events Device Trajectory Diagnostics View Changes

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

Schritt 4: Geben Sie Kommentare darüber ein, warum Sie die Isolationsfunktion auf dem Endpunkt gestoppt haben.

Beenden der Isolations Sitzung über die Befehlszeile

Wenn ein isolierter Endpunkt seine Verbindung zur Cisco Cloud verliert und Sie die Isolationsitzung von der Konsole aus nicht stoppen können. In diesen Situationen können Sie die Sitzung lokal über die Befehlszeile mit dem Entsperrcode beenden.

Schritt 1: Navigieren Sie in der Konsole zu **Verwaltung > Computer**.

Schritt 2: Suchen Sie den Computer, dessen Isolation Sie beenden möchten, und klicken Sie auf, um Details anzuzeigen.

Schritt 3: Beachten Sie den **Entsperrcode**, wie im Bild dargestellt.

DESKTOP-075I5MB in group testing bremarqu ✔ Definitions Up To Date

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

Schritt 4: Sie können den **Entsperrcode** auch finden, wenn Sie zu **Konto > Audit Log** navigieren, wie im Bild gezeigt.

Isolation Started DESKTOP-075I5MB bremarqu+...@cisc... 2021-09-28 21:33:48 CDT

Isolation Start Requested DESKTOP-075I5MB 2021-09-28 21:33:46 CDT

Attribute	Old	New
Comment	None	None
ID	None	██████████-██████████-██████████-██████████-██████████
Unlock Code	None	fwq8qw

Schritt 5: Öffnen Sie auf dem isolierten Computer eine Eingabeaufforderung mit

Administratorrechten.

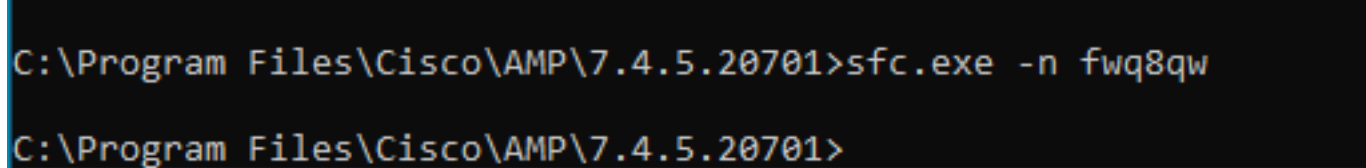
Schritt 6: Navigieren Sie zu dem Verzeichnis, in dem der Connector installiert ist.

Windows: C:\Program Files\Cisco\AMP\[Versionsnummer]

Mac: /opt/cisco/amp

Schritt 7. Den Befehl stop ausführen

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]

Vorsicht: Wenn der Entsperrcode 5 Mal falsch eingegeben wurde, müssen Sie 30 Minuten warten, bevor Sie einen weiteren Entsperrungsversuch unternehmen.

Fehlerbehebung für Wiederherstellung

Falls Sie alle Möglichkeiten ausgeschöpft haben und immer noch nicht in der Lage sind, einen isolierten Endpunkt über die Secure Endpoint-Konsole oder lokal mithilfe des Entsperrcodes wiederherzustellen, können Sie den isolierten Endpunkt mithilfe der Wiederherstellungsmethoden für Notfälle wiederherstellen.

Mac-Wiederherstellung:

Entfernen Sie die Isolationskonfiguration, und starten Sie den Secure Endpoint Service neu.

```
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-Wiederherstellung:

Wiederherstellungsisolationsmethode über die Befehlszeile

Wenn Ihr Endgerät isoliert ist und es nicht möglich ist, die Isolierung über die Secure Endpoint-Konsole oder mit dem Entsperrcode zu deaktivieren, führen Sie die folgenden Schritte aus.

Schritt 1: Beenden Sie den Connector-Dienst über die Connector-Benutzeroberfläche oder **Windows Services**.

Schritt 2: Suchen Sie nach dem Connector-Dienst für sichere Endpunkte, und beenden Sie den Dienst.

Schritt 3: Öffnen Sie auf dem isolierten Computer eine Eingabeaufforderung mit Administratorrechten.

Schritt 4: Führen Sie den Befehl **reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immune Protect" /v "unlock_code" /f** aus, wie im Bild gezeigt.

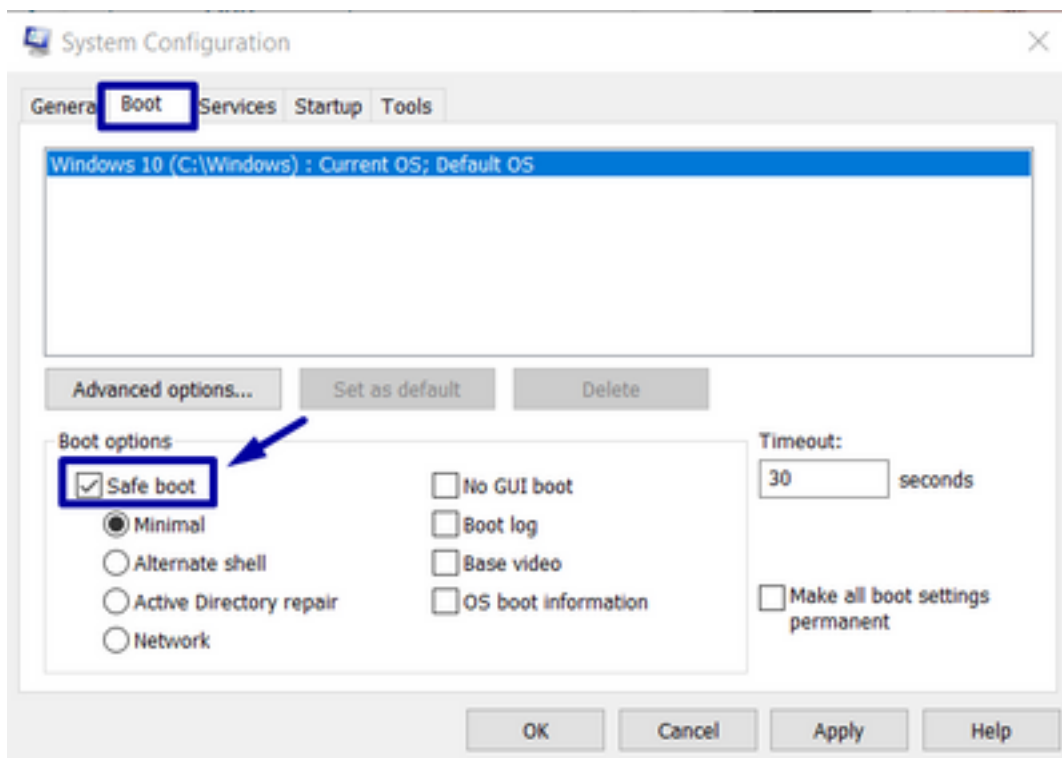
```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immune Protect" /v "unlock_code" /f
C:\Windows\system32>reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immune Protect" /v "unlock_code" /f
The operation completed successfully.
C:\Windows\system32>
```

Schritt 5: Die Meldung **Der Vorgang wurde erfolgreich abgeschlossen** zeigt an, dass der Vorgang abgeschlossen wurde. (Wenn eine weitere Meldung angezeigt wird, die wie folgt lautet: "Fehler: Zugriff verweigert", müssen Sie den Connector-Dienst für sichere Endpunkte beenden, bevor Sie den Befehl ausführen.)

Schritt 6: Starten Sie den Connector-Dienst für sichere Endpunkte.

Tip: Wenn Sie den Connector-Dienst Secure Endpoint nicht über die Connector-Benutzeroberfläche oder Windows Services stoppen können, können Sie einen sicheren Start durchführen.

Navigieren Sie auf dem isolierten Endpunkt zu **Systemkonfiguration > Start > Startoptionen**, und wählen Sie **Abgesichertes Booten** aus, wie im Abbild dargestellt.

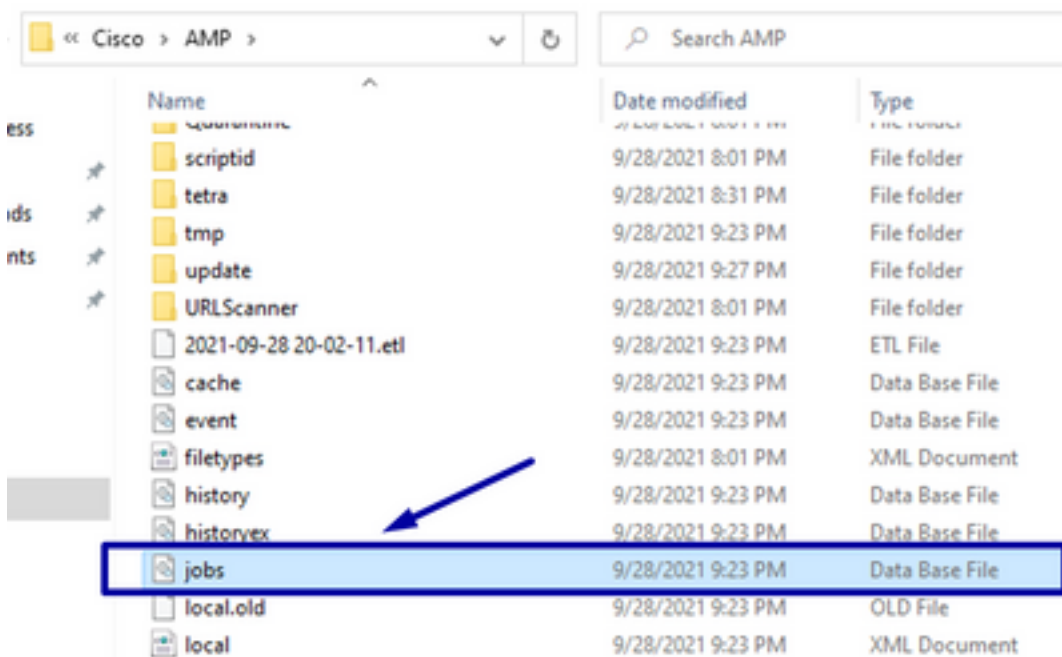


Recovery-Isolationsmethode ohne Befehlszeile

Falls Ihr Endgerät isoliert bleibt und es nicht möglich ist, die Isolierung über die Secure Endpoint-Konsole oder mit dem Entsperrcode zu deaktivieren oder selbst wenn Sie die Befehlszeile nicht verwenden können, gehen Sie wie folgt vor:

Schritt 1: Beenden Sie den Connector-Dienst über die Connector-Benutzeroberfläche oder **Windows Services**.

Schritt 2: Navigieren Sie zu dem Verzeichnis, in dem der Connector installiert ist (C:\Program Files\Cisco\AMP\), und löschen Sie die Datei **jobs.db**, wie im Bild dargestellt.



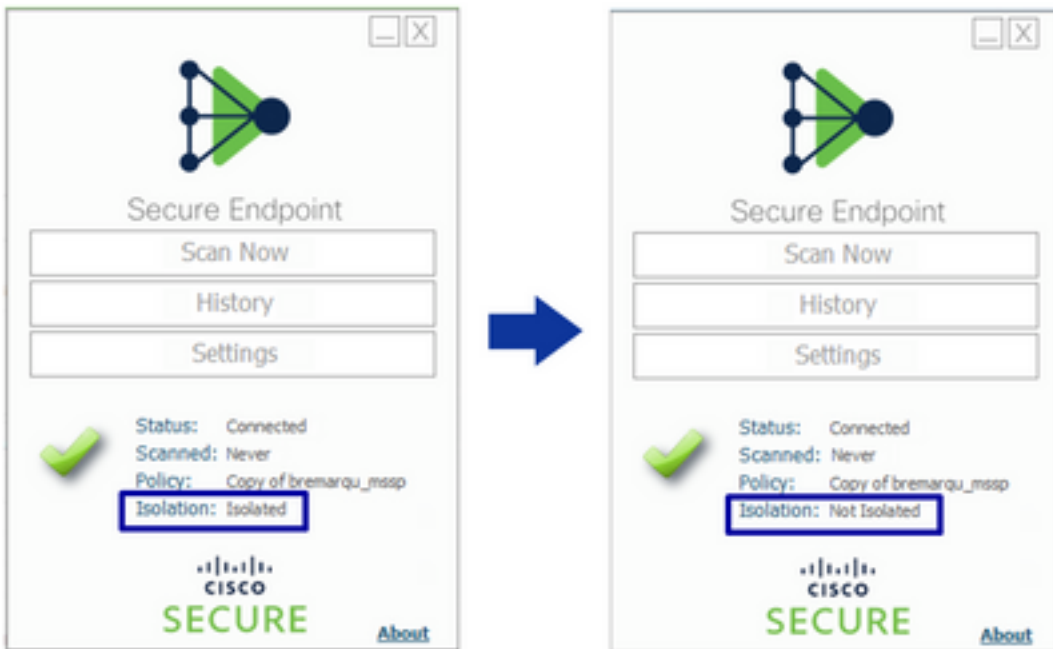
3. Starten Sie den Computer neu.

Wenn das Isolation-Ereignis in der Konsole angezeigt wird, können Sie außerdem zu **Error Details (Fehlerdetails)** navigieren, um den Fehlercode und seine Beschreibung zu überprüfen, wie in der Abbildung dargestellt.

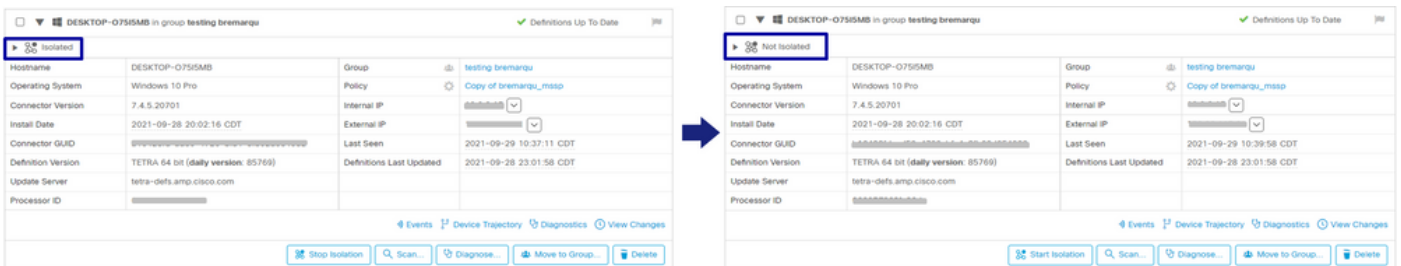


Überprüfung

Um zu überprüfen, ob der Endpunkt wieder isoliert ist oder nicht mehr isoliert ist, wird in der Benutzeroberfläche des Secure Endpoint Connectors der Isolationsstatus **"Nicht isoliert"** angezeigt, wie im Bild gezeigt.



Wenn Sie in der Konsole für sichere Endgeräte unter **Verwaltung > Computer** nach dem betreffenden Computer suchen, können Sie auf klicken, um Details anzuzeigen. Der Isolationsstatus zeigt **Nicht isoliert an**, wie im Bild dargestellt.



Zugehörige Informationen

- [Secure Endpoint - Benutzerhandbuch](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.