

Probleemoplossing voor beveiligde endpoints die geïsoleerd zijn geraakt met herstelmethoden

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Stoppen met isoleren](#)

[Isolatiesessie stoppen vanaf de console](#)

[Isolatiesessie stoppen vanaf de opdrachtregel](#)

[Probleemoplossing voor herstel](#)

[Mac-herstel:](#)

[Windows Herstel:](#)

[Herstel Isolatiemethode vanaf de opdrachtregel](#)

[Herstel isolatiemethode zonder de opdrachtregel](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het proces om een endpoint te herstellen met de Secure Endpoint-connector die is geïnstalleerd vanuit de isolatiemodus.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure Endpoint-connector
- Secure Endpoint-console
- Endpoint Isolation-functie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Endpoint console versie v5.4.2021092321
- Secure Endpoint voor Windows-connector versie v7.4.5.20701
- Secure Endpoint Mac-verbindingsversie v1.21.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De procedure die in dit document wordt beschreven, is handig in situaties waarin het eindpuntapparaat in deze toestand is vastgezet en het niet mogelijk is de isolatiemodus uit te schakelen.

Endpoint isolation is een functie waarmee u netwerkactiviteit (IN en OUT) op een computer kunt blokkeren om bedreigingen zoals gegevensexfiltratie en malware-propagatie te voorkomen. Het is beschikbaar op:

- 64-bits versies van Windows die versie 7.0.5 en hoger van de Windows-connector ondersteunen
- Mac-versies die versie 1.21.0 en hoger van de Mac-connector ondersteunen.

Endpoint isolatiesessies hebben geen invloed op de communicatie tussen de connector en de Cisco-cloud. Er is hetzelfde niveau van bescherming en zichtbaarheid op uw eindpunten als voor de sessie. U kunt IP Isolation Allow Lists van adressen configureren om te voorkomen dat de connector de IP-adressen blokkeert terwijl een actieve endpointisolatiesessie actief is. U kunt [hier](#) meer gedetailleerde informatie over de functie Endpoint Isolation bekijken.

Stoppen met isoleren

Als u de Isolatie van het Endpoint op een computer wilt stoppen, voert u deze snelle stappen uit via de Secure Endpoint console of opdrachtregel.

Isolatiesessie stoppen vanaf de console

Om een isolatiesessie te stoppen en al het netwerkverkeer te herstellen naar een eindpunt.

Stap 1. Navigeer in de console naar **Management > Computers**.

Stap 2. Zoek de computer die u wilt stoppen met de isolatie en klik om de details weer te geven.

Stap 3. Klik op de knop **Isolatie stoppen**, zoals in de afbeelding.

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	[REDACTED]
Install Date	2021-09-28 20:02:16 CDT	External IP	[REDACTED]
Connector GUID	[REDACTED]	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	[REDACTED]		

Events Device Trajectory Diagnostics View Changes

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

Stap 4. Voer opmerkingen in over de reden waarom u de isolatieoptie op het eindpunt hebt gestopt.

Isolatiesessie stoppen vanaf de opdrachtregel

Als een geïsoleerd eindpunt zijn verbinding met de Cisco-cloud verliest en u de isolatiesessie vanaf de console niet kunt stoppen. In deze situaties kunt u de sessie lokaal stoppen vanaf de opdrachtregel met de ontgrendelingscode.

Stap 1. Navigeer in de console naar **Management > Computers**.

Stap 2. Zoek de computer die u wilt stoppen met de isolatie en klik om de details weer te geven.

Stap 3. Let op de **Unlock Code**, zoals in de afbeelding.

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

Stap 4. U kunt de **Unlock Code** ook vinden als u naar **Account > Auditlogboek** navigeert, zoals in de afbeelding wordt getoond.

Isolation Started	DESKTOP-075I5MB	bremarqu+...@cisc...	2021-09-28 21:33:48 CDT
Isolation Start Requested	DESKTOP-075I5MB	[REDACTED]	2021-09-28 21:33:46 CDT

Attribute	Old	New
Comment	None	None
ID	None	[REDACTED]
Unlock Code	None	fwq8qw

Stap 5. Open op de geïsoleerde computer een opdrachtprompt met administratorrechten.

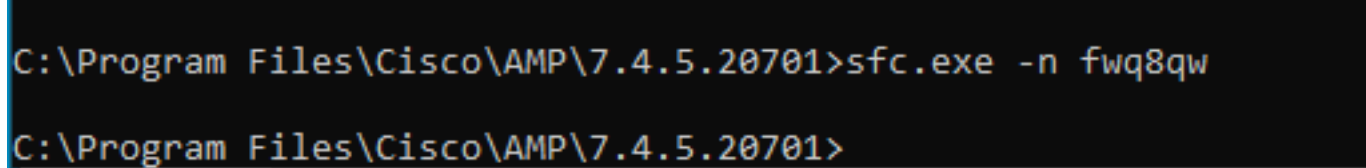
Stap 6. Navigeer naar de map waarin de connector is geïnstalleerd

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

Mac: /opt/cisco/amp

Stap 7. De stopopdracht uitvoeren

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]

Waarschuwing: als de unlock code 5 keer onjuist is ingevoerd, moet u 30 minuten wachten voordat u nog een unlock poging doet.

Probleemoplossing voor herstel

Indien u alle wegen uitput en u nog steeds niet in staat bent om een geïsoleerd eindpunt te herstellen van de Secure Endpoint console of lokaal met de unlock code; u kunt het geïsoleerde eindpunt herstellen met de noodherstel methoden.

Mac-herstel:

Verwijder de isolatieconfiguratie en start de Secure Endpoint Service opnieuw

```
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 Herstel:

Herstel Isolatiemethode vanaf de opdrachtregel

In situaties waar uw eindpuntapparaat in isolatie wordt vastgeplakt en het niet mogelijk is om isolatie via de Secure Endpoint console of met de unlock code uit te schakelen, doe deze stappen.

Stap 1. Stop de aansluitservice via de gebruikersinterface van de connector of **Windows Services**.

Stap 2. Zoek de Secure Endpoint connector-service en stop de service.

Stap 3. Open op de geïsoleerde computer een opdrachtprompt met administratorrechten.

Stap 4. Voer de opdracht **reg verwijderen "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f** zoals in de afbeelding.

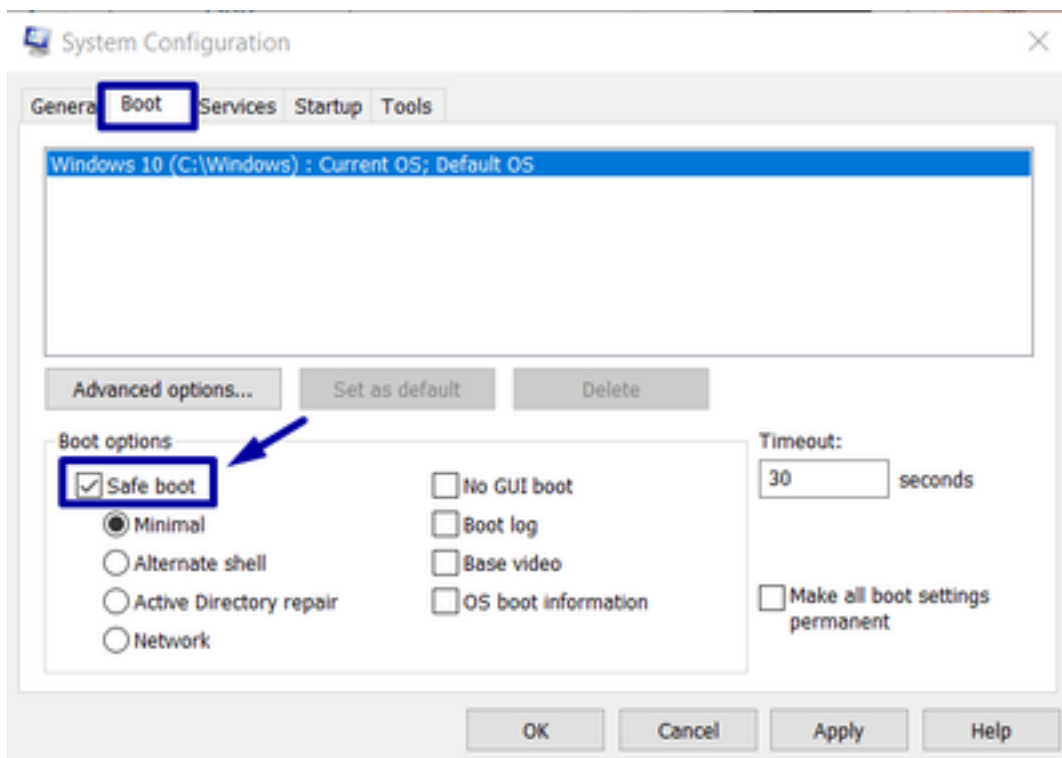
```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immune Protect" /v "unlock_code" /f
C:\Windows\system32>reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immune Protect" /v "unlock_code" /f
The operation completed successfully.
C:\Windows\system32>
```

Stap 5. Het bericht **De met succes voltooide bewerking** geeft aan dat de bewerking is voltooid. (Als een ander bericht wordt weergegeven, zoals "Fout: Toegang wordt geweigerd", moet u de Secure Endpoint connector service stoppen voordat u de opdracht uitvoert.)

Stap 6. Start de Secure Endpoint connector-service.

Tip: Als u de Secure Endpoint connector service niet kunt stoppen via de connector-gebruikersinterface of Windows Services, kunt u een Safe-boot doen.

Ga op het geïsoleerde eindpunt naar **Systeemconfiguratie > Opstarten > Opstartopties** en selecteer **Veilig opstarten**, zoals in de afbeelding.



Herstel isolatiemethode zonder de opdrachtregel

Als uw endpointapparaat in isolatie vastzit en het niet mogelijk is om isolatie via de Secure Endpoint console of met de unlock code uit te schakelen of zelfs als u de opdrachtregel niet kunt gebruiken, doe dan de volgende stappen:

Stap 1. Stop de aansluitservice via de gebruikersinterface van de connector of **Windows Services**.

Stap 2. Navigeer naar de map waarin de connector is geïnstalleerd (C:\Program Files\Cisco\AMP\), en verwijder het bestand **jobs.db**, zoals in de afbeelding.

« 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. Start de computer opnieuw op.

Daarnaast, als u de Isolatie-gebeurtenis in de console ziet, kunt u naar **Error Details** navigeren om de foutcode en de beschrijving ervan te bekijken, zoals in de afbeelding.

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

Verifiëren

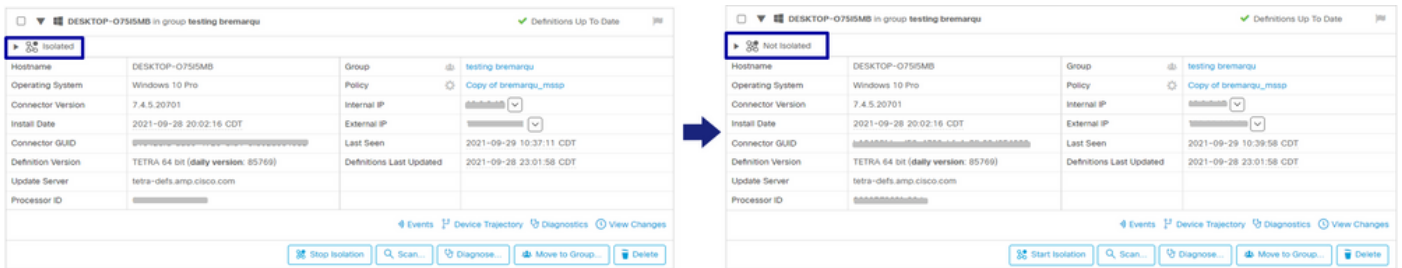
Om te verifiëren dat het eindpunt zich weer in de isolatie bevindt of niet langer geïsoleerd is, kunt u de gebruikersinterface van de Secure Endpoint-connector zien om de isolatiestatus weer te geven als **niet geïsoleerd**, zoals in het beeld wordt weergegeven.

The image shows two side-by-side screenshots of the Cisco Secure Endpoint user interface, separated by a blue arrow pointing from left to right. Both screenshots show a 'Secure Endpoint' window with a green checkmark icon and the following information:

- Status: Connected
- Scanned: Never
- Policy: Copy of bremarqu_mssp
- Isolation: **Isolated** (in the left screenshot) / **Not Isolated** (in the right screenshot)

The interface also includes buttons for 'Scan Now', 'History', and 'Settings', and the Cisco logo with the word 'SECURE' and an 'About' link.

Vanuit de Secure Endpoint console, als u navigeert in **Management > Computers**, en de computer in kwestie vindt, kunt u klikken om details weer te geven. De isolatiestatus wordt **niet weergegeven als geïsoleerd**, zoals in het beeld wordt weergegeven.



Gerelateerde informatie

- [Gebruikershandleiding Secure Endpoint](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.