# Risoluzione dei problemi relativi all'endpoint sicuro bloccato in isolamento con i metodi di ripristino

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Interrompi isolamento Arresta sessione di isolamento dalla console Arresta sessione di isolamento dalla riga di comando Risoluzione dei problemi di ripristino Ripristino Mac: Ripristino di Windows: Metodo di isolamento del recupero dalla riga di comando Metodo di isolamento del recupero senza riga di comando Verifica Informazioni correlate

# Introduzione

In questo documento viene descritto il processo di ripristino di un endpoint con il connettore Secure Endpoint installato dalla modalità di isolamento.

# Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Endpoint Connector
- Secure Endpoint Console
- Funzione Isolamento endpoint

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Secure Endpoint console versione v5.4.2021092321

- Connettore Windows Secure Endpoint versione v7.4.5.20071
- Connessione Secure Endpoint Mac versione 1.21.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

La procedura descritta in questo documento è utile nelle situazioni in cui il dispositivo dell'endpoint è bloccato in questo stato e non è possibile disabilitare la modalità di isolamento.

L'isolamento degli endpoint è una funzionalità che consente di bloccare l'attività di rete (IN e OUT) in un computer per impedire minacce quali l'esfiltrazione di dati e la propagazione di malware. Il testo è disponibile all'indirizzo:

- Versioni a 64 bit di Windows che supportano la versione 7.0.5 e successive di Windows Connector
- versioni Mac che supportano la versione 1.21.0 e successive del connettore Mac.

Le sessioni di isolamento degli endpoint non influiscono sulla comunicazione tra il connettore e il cloud Cisco. Sugli endpoint è disponibile lo stesso livello di protezione e visibilità raggiunto prima della sessione. È possibile configurare gli elenchi di indirizzi consentiti per l'isolamento IP in modo da evitare che il connettore blocchi gli indirizzi IP in questione mentre è attiva una sessione attiva di isolamento degli endpoint. Qui è possibile esaminare informazioni più dettagliate sulla funzione Isolamento endpoint.

## Interrompi isolamento

Per interrompere l'isolamento degli endpoint in un computer, eseguire rapidamente le operazioni seguenti tramite la console o la riga di comando di Secure Endpoint.

### Arresta sessione di isolamento dalla console

Per interrompere una sessione di isolamento e ripristinare tutto il traffico di rete su un endpoint.

Passaggio 1. Nella console passare a **Gestione > Computer**.

Passaggio 2. Individuare il computer per il quale si desidera interrompere l'isolamento e fare clic su per visualizzare i dettagli.

Passaggio 3. Fare clic sul pulsante Interrompi isolamento, come illustrato nell'immagine.

🗌 🔻 🖬 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	01010012-0300-1700-04x1-010003001000-	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	00007/10////00//					
🗱 Stop Isolation 🔍 Scan 🕲 Diagnose 🕼 Move to Group 🗑 Delete						

Passaggio 4. Immettere eventuali commenti sul motivo per cui è stata arrestata la feature di isolamento sull'endpoint.

### Arresta sessione di isolamento dalla riga di comando

Se un endpoint isolato perde la connessione al cloud Cisco e non è possibile interrompere la sessione di isolamento dalla console. In questi casi, è possibile interrompere la sessione localmente dalla riga di comando con il codice di sblocco.

Passaggio 1. Nella console passare a **Gestione > Computer**.

Passaggio 2. Individuare il computer per il quale si desidera interrompere l'isolamento e fare clic su per visualizzare i dettagli.

Passaggio 3. Notare il codice di sblocco, come mostrato nell'immagine.

	DESKTOP-075I5MB in group testing bremarqu					<ul> <li>Definitions Up To Date</li> </ul>	
1	Se Isolated						
1	2021-09-28 21:33:48 CDT		Isolated for less than a min	nute		Unlock Code:fv	wp8pv
	Isolated	2021-09-28 21:33:48 CDT					
	Isolating	2021-09-28 21:33:46 CDT	Brenda M	Unlock Code: fwq8qw			

Passaggio 4. È inoltre possibile trovare il **codice di sblocco** selezionando **Account > Registro di controllo**, come illustrato nell'immagine.

► Isolation Started  □ DESKT	DESKTOP-07515MB		$\sim$	2021-09-28 21:33:48 CDT	
▼ Isolation Start Requested  □ DESKTO	P-075I5MB		100.00.000	0 🗸 2021-09-28 21:33:46 CDT	
Attribute	Old		New		
Comment	None	None			
ID	None			a 4414 0040 24000100110	
Unlock Code	None		fwq8qw		

Passaggio 5. Nel computer isolato aprire un prompt dei comandi con privilegi di amministratore.

Passaggio 6. Passare alla directory in cui è installato il connettore

Windows: C:\Program Files\Cisco\AMP\[numero versione]

Mac: /opt/cisco/amp

Passaggio 7. Eseguire il comando stop

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]

**Attenzione**: se il codice di sblocco viene immesso 5 volte in modo errato, è necessario attendere 30 minuti prima di tentare un altro sblocco.

## Risoluzione dei problemi di ripristino

Se sono stati esauriti tutti i percorsi e non è ancora possibile ripristinare un endpoint isolato dalla console dell'endpoint sicuro o localmente con il codice di sblocco, è possibile ripristinare l'endpoint isolato con i metodi di ripristino di emergenza.

## **Ripristino Mac:**

Rimuovere la configurazione di isolamento e riavviare il servizio Endpoint protetto

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

## **Ripristino di Windows:**

### Metodo di isolamento del recupero dalla riga di comando

Nei casi in cui il dispositivo dell'endpoint è bloccato in isolamento e non è possibile disattivare l'isolamento tramite la console dell'endpoint sicuro o con il codice di sblocco, eseguire la procedura seguente.

Passaggio 1. Arrestare il servizio connettore tramite l'interfaccia utente del connettore o **Servizi Windows**.

Passaggio 2. Individuare il servizio Connettore endpoint sicuro e arrestare il servizio.

Passaggio 3. Nel computer isolato aprire un prompt dei comandi con privilegi di amministratore.

Passaggio 4. Eseguire il comando **reg delete "HKEY\_LOCAL\_MACHINE\SOFTWARE\Immunet Protect" /v "unlock\_code" /f** come mostrato nell'immagine.

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>

Passaggio 5. Il messaggio **Operazione completata** indica che l'operazione è stata completata. (Se viene visualizzato un altro messaggio, ad esempio "Errore: Accesso negato", è necessario arrestare il servizio Connettore endpoint sicuro prima di eseguire il comando).

Passaggio 6. Avviare il servizio Connettore endpoint sicuro.

**Suggerimento**: se non è possibile arrestare il servizio Connettore endpoint sicuro dall'interfaccia utente del connettore o dai servizi Windows, è possibile eseguire un avvio sicuro.

Sull'endpoint isolato, selezionare **Configurazione di sistema > Avvio > Opzioni di avvio** e selezionare **Avvio sicuro**, come mostrato nell'immagine.

era Boot Services Startup	Tools		
indows 10 (C:\Windows) : Curr	ent OS; Default OS		
Advanced options Se	t as default Delete		
loot options		Timeout:	
Safe boot	No GUI boot	30	seconds
Minimal	Boot log		
O Alternate shell	Base video		
	OS boot information	Make all I	boot settings
Active Directory repair		permaner	nt
<ul> <li>Active Directory repair</li> <li>Network</li> </ul>			

### Metodo di isolamento del recupero senza riga di comando

Se il dispositivo dell'endpoint è bloccato in isolamento e non è possibile disattivare l'isolamento tramite la console Secure Endpoint o con il codice di sblocco o anche se non è possibile utilizzare la riga di comando, eseguire la procedura seguente:

Passaggio 1. Arrestare il servizio connettore tramite l'interfaccia utente del connettore o **Servizi Windows**.

Passaggio 2. Passare alla directory in cui è installato il connettore (C:\Program Files\Cisco\AMP\) ed eliminare il file **jobs.db**, come mostrato nell'immagine.

<u> </u>	Cisco > AMP > V Č	, Search AMP	
	Name	Date modified	Туре
s	scriptid	9/28/2021 8:01 PM	File folder
	tetra	9/28/2021 8:31 PM	File folder
5 7	tmp	9/28/2021 9:23 PM	File folder
s x	🕈 🔄 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
	A 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. Riavviare il computer.

Inoltre, se nella console viene visualizzato l'evento Isolamento, è possibile passare a **Dettagli** errore per esaminare il codice di errore e la relativa descrizione, come mostrato nell'immagine.

Failed to stop isolation			💶 צ 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			

# Verifica

Per verificare che l'endpoint sia tornato dall'isolamento o non sia più isolato, è possibile vedere che nell'interfaccia utente del connettore Secure Endpoint lo stato di isolamento è **Non isolato**, come mostrato nell'immagine.



Dalla console di Secure Endpoint, se si seleziona **Gestione > Computer** e si individua il computer in questione, è possibile fare clic su per visualizzare i dettagli. Lo stato Isolamento (Isolation) viene visualizzato come **Non isolato** (**Not Isolated**), come mostrato nell'immagine.

🗌 🔻 💐 DESKTOP-07555MB in group testing bremarqu 🗸 Definitions Up To Date 🕅				75I5MB in group testing bremarqu		✓ Definitions Up To Date III	
► Se isolated				<ul> <li>St Not Isolated</li> </ul>			
Hostname	DESKTOP-075I5MB	Group da	testing bremarqu	Hostname	DESKTOP-075I5M8	Group da	testing bremarqu
Operating System	Windows 10 Pro	Policy 🔅	Copy of bremarqu_mssp	Operating System	Windows 10 Pro	Policy 🔅	Copy of bremarqu_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)	Defnitions 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 2 Device Trajectory 10 Diagnostics 3 View Changes			4 Events (P Device Trajectory (9 Diagnostics (9 V			Device Trajectory 🕲 Diagnostics 🕲 View Changes	
	😹 Stop Isolation 🔍 Scan 🕅 Diagnose 🕅 da Move to Group ) 🗑 Delete				Start I	olation Q. Scan 양	Diagnose 🏼 🌢 Move to Group 📄 Delete

# Informazioni correlate

- Guida per l'utente di Secure Endpoint
- Documentazione e supporto tecnico Cisco Systems

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).