# Solução de problemas de endpoint seguro preso em isolamento com métodos de recuperação

# Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Parar Isolamento Interromper sessão de isolamento no console Parar sessão de isolamento no console Parar sessão de isolamento a partir da linha de comando Solução de problemas de recuperação Recuperação Mac: Recuperação do Windows: Método de Isolamento de Recuperação a partir da Linha de Comando Método de Isolamento de Recuperação sem a Linha de Comando Verificar Informações Relacionadas

# Introduction

Este documento descreve o processo para recuperar um endpoint com o conector Secure Endpoint instalado a partir do modo de isolamento.

# Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conector de endpoint seguro
- Console de endpoint seguro
- Recurso de isolamento de endpoint

### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Console Secure Endpoint versão v5.4.2021092321
- Conector Secure Endpoint Windows versão v7.4.5.20701
- Conexão Secure Endpoint Mac versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O procedimento descrito neste documento é útil em situações em que o dispositivo de ponto final está preso nesse estado e não é possível desativar o modo de isolamento.

O isolamento de endpoint é um recurso que permite bloquear a atividade de rede (IN e OUT) em um computador para impedir ameaças como extração de dados e propagação de malware. Ele está disponível em:

- Versões de 64 bits do Windows que oferecem suporte à versão 7.0.5 e posterior do conector Windows
- Versões para Mac que suportam a versão 1.21.0 e posterior do conector Mac.

As sessões de isolamento de endpoint não afetam a comunicação entre o conector e a nuvem da Cisco. Há o mesmo nível de proteção e visibilidade em seus endpoints que havia antes da sessão. Você pode configurar Isolamento de IP Permitir Listas de endereços para evitar que o conector bloqueie os endereços IP em questão enquanto uma sessão de isolamento de ponto final ativo estiver ativa. Você pode revisar informações mais detalhadas sobre o recurso de Isolamento de Ponto de Extremidade <u>aqui</u>.

## Parar Isolamento

Quando quiser parar o isolamento de endpoint em um computador, siga estas etapas rápidas através do console ou da linha de comando do Secure Endpoint.

### Interromper sessão de isolamento no console

Para interromper uma sessão de isolamento e restaurar todo o tráfego de rede para um endpoint.

Etapa 1. No console, navegue até Gerenciamento > Computadores.

Etapa 2. Localize o computador que deseja interromper o isolamento e clique nele para exibir os detalhes.

Etapa 3. Clique no botão Stop Isolation, conforme mostrado na imagem.

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				
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	0000777044440044					
🕅 Stop Isolation 🔍 Scan 🕲 Diagnose 🕸 Move to Group 🗑 Delete						

Etapa 4. Insira comentários sobre o motivo pelo qual você parou o recurso de isolamento no ponto de extremidade.

#### Parar sessão de isolamento a partir da linha de comando

Se um endpoint isolado perder sua conexão com a nuvem da Cisco e você não conseguir parar a sessão de isolamento do console. Nessas situações, você pode parar a sessão localmente a partir da linha de comando com o código de desbloqueio.

Etapa 1. No console, navegue até **Gerenciamento > Computadores**.

Etapa 2. Localize o computador que deseja interromper o isolamento e clique nele para exibir os detalhes.

Etapa 3. Observe o Código de desbloqueio, como mostrado na imagem.

🗆 🔻 🔣 DESKTO	✓ Definitions Up To Date	)es		
▼ Se Isolated				
2021-09-28 21:33:4	8 CDT	Isolated for less ti	an a minute Unlock Coo	de:fwq8qw
Isolated	2021-09-28 21:33:48 CDT			
Isolating	2021-09-28 21:33:46 CDT	Brenda M	Unlock Code: fwq8qw	

Etapa 4. Você também pode encontrar o **Código de desbloqueio** se navegar para **Conta > Log de auditoria**, como mostrado na imagem.

► Isolation Started DESKTOP	-075I5MB	bremarqu+C@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	one		- 0000 24000100110
Unlock Code	None		fwq8qw	

Etapa 5. No computador isolado, abra um prompt de comando com privilégios de administrador.

Etapa 6. Navegue até o diretório onde o conector está instalado

Windows: C:\Program Files\Cisco\AMP\[número da versão]

Mac: /opt/cisco/amp

Passo 7. Execute o 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]

**Cuidado**: se o código de desbloqueio for inserido incorretamente 5 vezes, será necessário aguardar 30 minutos antes de fazer outra tentativa de desbloqueio.

## Solução de problemas de recuperação

Caso você tenha esgotado todos os caminhos e ainda não consiga recuperar um endpoint isolado do console do Secure Endpoint ou localmente com o código de desbloqueio; é possível recuperar o endpoint isolado com os métodos de recuperação de emergência.

## Recuperação Mac:

Remova a configuração de isolamento e reinicie o 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

## Recuperação do Windows:

### Método de Isolamento de Recuperação a partir da Linha de Comando

Em situações em que o dispositivo de endpoint está preso no isolamento e não é possível desativar o isolamento por meio do console do Secure Endpoint ou com o código de desbloqueio, siga estas etapas.

Etapa 1. Interrompa o serviço do conector por meio da interface de usuário do conector ou dos **Serviços do Windows**.

Etapa 2. Localize o serviço do conector de Ponto Final Seguro e pare o serviço.

Etapa 3. No computador isolado, abra um prompt de comando com privilégios de administrador.

Etapa 4. Execute o comando **reg delete "HKEY\_LOCAL\_MACHINE\SOFTWARE\Immunet Protect" /v "unlock\_code" /f** como mostrado na imagem.

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>

Etapa 5. A mensagem **A operação foi concluída com êxito** indica que a operação foi concluída. (Se outra mensagem for exibida, como "Erro: Acesso negado", você precisará parar o serviço do conector de Ponto de Extremidade Seguro antes de executar o comando).

Etapa 6. Inicie o serviço do conector de Ponto Final Seguro.

**Dica**: se você não conseguir parar o serviço do conector de Ponto de Extremidade Seguro na interface de usuário do conector ou nos Serviços do Windows, poderá fazer uma inicialização segura.

No endpoint isolado, navegue para **System Configuration > Boot > Boot options** e selecione **Safe boot**, como mostrado na imagem.

Boot Services Startup	Tools		
Vindows 10 (C:\Windows) : Curren	t OS; Default OS		
Advanced options Set a	s default Delete		
Boot options		Timeout:	
Safe boot	No GUI boot	30	seconds
Minimal	Boot log		
Alternate shell	Base video		
V			
Active Directory repair	OS boot information	Make all	boot settings
Active Directory repair     Network	OS boot information	Make all permane	boot settings nt

### Método de Isolamento de Recuperação sem a Linha de Comando

Caso seu dispositivo de endpoint esteja preso no isolamento e não seja possível desativar o isolamento por meio do console do Secure Endpoint ou com o código de desbloqueio ou mesmo se você não puder usar a linha de comando, siga estas etapas:

Etapa 1. Interrompa o serviço do conector por meio da interface de usuário do conector ou dos **Serviços do Windows**.

Etapa 2. Navegue até o diretório onde o conector está instalado (C:\Program Files\Cisco\AMP\) e exclua o arquivo **jobs.db**, como mostrado na imagem.

_ « c	isco > AMP > V	õ	, Search AMP	
	Name		Date modified	Туре
د ہ	scriptid		9/28/2021 8:01 PM	File folder
	tetra		9/28/2021 8:31 PM	File folder
1	tmp		9/28/2021 9:23 PM	File folder
\$ 1	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
	istory		9/28/2021 9:23 PM	Data Base File
	istoryex		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. Reinicialize o computador.

Além disso, se você vir o evento Isolation no console, poderá navegar até **Error Details** para revisar o código de erro e sua descrição, como mostrado na imagem.

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	Q Run Scan			

# Verificar

Para verificar se o ponto de extremidade está de volta do isolamento ou não está mais isolado, você pode ver a interface do usuário do conector de Ponto de Extremidade Seguro exibir o status de Isolamento como **Não Isolado**, como mostrado na imagem.



No console do Secure Endpoint, se navegar em **Management > Computers** e localizar o computador em questão, você poderá clicar para exibir detalhes. O status Isolation exibe **Not Isolated**, como mostrado na imagem.

🖸 🔻 🛍 DESKTOP-075ISMB in group testing bremarque 🖌 Definitions Up To Date 🛛					75I5MB in group testing bremarqu		✓ Definitions Up To Date I®
► S <sup>®</sup> Isolated			► St Not isolated				
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 bremargu_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 1/2 Device Trajectory 1/3 Diagnostics (3) View Changes			4 Events 12 Device Trajectory 13 Diagnostics (3) V			Device Trajectory 🕲 Diagnostics 💿 View Changes	
	😹 Stop Isolation 🛛 Q. Scan 😯 Diagnose 📾 Move to Group ) 🗑 Delete			💱 Start Isolation 🔍 Scan ) 🔮 Diagnose ) 🏜 Move to Group			Diagnose

# Informações Relacionadas

- Guia do usuário do Secure Endpoint
- Suporte Técnico e Documentação Cisco Systems

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.