# Ative a depuração no endpoint a partir do console do AMP for Endpoint

## Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Problema
Configurar
Etapa 1: Identifique o endpoint a ser movido para a depuração
Etapa 2: Duplicar a política existente
Etapa 3: Configurar o Nível de Log para Depurar esta Política
Etapa 4: Criar novo grupo e vincular essa nova política
Etapa 5: Mover o ponto final identificado para este novo grupo
Etapa 6: Verifique o endpoint na página do computador e na interface do usuário do conector

## Introdução

Este documento descreve como habilitar a depuração no endpoint a partir do Cisco Secure Endpoint Console.

### Pré-requisitos

#### Requisitos

Antes de começar, verifique se você tem:

- Acesso administrativo ao console do Cisco Secure Endpoint for Endpoints.
- O ponto de extremidade que você deseja executar a depuração já está registrado no Cisco Secure Endpoint

#### **Componentes Utilizados**

As informações usadas no documento são baseadas nestas versões de software:

- Cisco Secure Endpoint Console versão 5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7 e posterior
- Sistema operacional Microsoft Windows

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

#### Informações de Apoio

Os dados de diagnóstico gerados podem ser fornecidos ao Cisco Technical Assistance Center (TAC) para análise adicional.

Os dados de diagnóstico incluem informações como:

- Utilização de recursos (disco, CPU e memória)
- · Registros específicos do conector
- · Informações de configuração do conector

#### Problema

É necessário habilitar a depuração no endpoint a partir do Cisco Secure Endpoint Console durante um destes cenários.

Cenário 1: se você reinicializar o dispositivo, habilite o modo de depuração na interface da bandeja IP ou ele não sobreviverá à reinicialização. Caso os logs de depuração de inicialização sejam necessários, você pode habilitar o modo de depuração na configuração de política no console do Secure Endpoint.

Cenário 2: se você tiver problemas de desempenho com o Cisco Secure Endpoint Connector em um dispositivo, a ativação do modo de depuração pode ajudar a reunir logs detalhados para análise.

Cenário 3: ao solucionar problemas específicos com o conector de endpoint seguro, logs detalhados podem fornecer informações sobre a causa raiz do problema.

### Configurar

Conclua estas etapas para habilitar com êxito o modo de depuração no ponto de extremidade especificado por meio do Console de Ponto de Extremidade Seguro.

Etapa 1: Identifique o endpoint a ser movido para a depuração

- 1. Faça login no console Cisco Secure Endpoint. No painel principal, navegue até a seção Gerenciamento.
- 2. Navegue até Gerenciamento > Computadores.
- 3. Identifique e anote o ponto final que requer o modo de depuração.

Etapa 2: Duplicar a política existente

1. Navegue até Gerenciamento > Políticas.

Ξ		Management ×
55	Dashboard	Computers
$ _{\Theta}^{ _{1} }$	Inbox	Groups
dil =	Overview	Policies 🗸
-	-	Exclusions
w.	Events	Device Control
dil	Analysis >	Host Firewall
*	Outbreak Control >	Deployment
5	Management	Download Connector
-		Deploy Clarity for iOS
20	Administration >	Deployment Summary
		AV Definition Summary

- 2. Localize a política atualmente aplicada ao ponto final identificado.
- 3. Clique na política para expandir a janela da política.
- 4. Clique em Duplicar para criar uma cópia da política existente.

Vetection and Response	Exclusion Sets	Custom Detections	Groups	- 5
lies Quarantine letwork Block Asticious Activity Prote. Quarantine	Oaco-Maintained Microsoft Windows Default	Simple Not configured Advanced Not configured	TEST	
lystem Process Protec Protect Icript Protection Quarantine		Application Control		
xploit Prevention Block xploit Prevention Scrip Audit		Alow Not configured		
ehavioral Protection Protect ETRA Offine File Scan Disabled		Block Not configured		
Orbital Enabled		Network Control		
Vevice Control		Not configured		
58 Mass Store. Not configured			Proxy	

Etapa 3: Configurar o Nível de Log para Depurar esta Política

- 1. Selecione e expanda a janela política duplicada.
- 2. Clique em Editar e renomeie a política (por exemplo, Depurar política do TechZone).
- 3. Clique em Advanced Settings (Configurações avançadas).
- 4. Selecione Administrative Features na barra lateral.
- 5. Defina Connector Log Level e Tray Log Level como Debug.
- 6. Clique em Save para salvar as alterações.

Folicies Edit Policy Windows		
Name	Debug TechZone Policy	
Description	Taking-debug on endpoint	
Modes and Engines		Send User Name in Events ()
Exclusions		Send Filename and Path Info ()
1 exclusion set	Heartbeat Interval	15 minutes ~ 0
Proxy	Connector Log Level	Debug ~ 0
The second second	Tray Log Level	Debug ~ 0
Paper Provide		Enable desearche Bestartion du
Outbreak Control		
Device Control	Connector Protection Password	0
Product Updates		Automated Crash Dump Uploads ()
Advanced Settings		Command Line Capture ()
Administrative Features		Command Line Logging ()
Client User Interface		
File and Process Scan		
Calle		
England Isolation		
Coulous Coulous		
TTTPA		
Notwork		
Scheduled Scene		
		Cancel

Etapa 4: Criar novo grupo e vincular essa nova política

1. Navegue até Gerenciamento > Grupos.

≡			Management ×	
	Dashboard		Computers	
1  ©	Inbox		Groups 🗸	
	Overview		Policies	
•	Events		Exclusions	
			Device Control	C
ш	Analysis	>	Host Firewall	
ж	Outbreak Control	>	Deployment	
Ţ,	Management		Download Connector	
			Deploy Clarity for iOS	
20	Administration	>	Deployment Summary	
			AV Definition Summary	

- 2. Clique em Criar Grupo próximo ao lado superior direito da tela.
- 3. Insira um nome para o grupo (Por exemplo, Depurar Grupo TechZone.)
- 4. Altere a Política do padrão para a política de depuração recém-criada.
- 5. Clique em Salvar.

Name	Debug TechZone Group		Computers
Description	This Group is used to Debug Cisco S Endpoint Connector	ecure	Assign computers from the Computers page after you have saved the new group
Parent Group		~	
Windows Policy	Debug TechZone Policy	~	
Android Policy	Default Policy (Protect)	~	
Mac Policy	Default Policy (Audit)	~	
Linux Policy	Default Policy (Audit)	v	
Network Policy	Default Policy (Default Network)	~	
iOS Policy	Default Policy (Audit)	~	

Etapa 5: Mover o ponto final identificado para este novo grupo

1. Volte para Gerenciamento > Computadores.

# Secure Endpoint

≡			Management	×
5	Dashboard		Computers	~
$  _{\mathfrak{S}}^{ 1 }$	Inbox		Groups	
	Overview		Policies	
•	Events		Exclusions Device Control	
dd	Analysis	>	Deployment	
×	Outbreak Control	>	Download Connector	
	Management		Deploy Clarity for iOS	
20	Administration	>	AV Definition Summary	

- 2. Selecione o ponto final identificado na lista.
- 3. Clique em Mover para Grupo.

O Y 8 00000 Hg	rise TENT		,e
Fostratie	DESCTOP MIG-MOP	free a	TEST
Operating System	T Mindows 10 Pre Bulle 18045-85280	Policy 0	151
Connector territori	T 8-K030001 * Drow download UK.	Intering IP	0
Install (Inte	2024 07-25 15:03/13 67	External IP	0
Connector 64/0	201tte://p-040a-4784-ace8-cb85e8096c98	Last Seen	2024-07-25 18-42-50 /07
Processor (D)	0786/fb/700000817	BP apprature section	1004
Cisco Secure Client (D	N/A	Classi Security Hist Score	Pendra_
Children Strends Drapshot Vice 1-	epinet R investigate in Orbital		a bents (2 Device Trajectory 10 Disposition (3) New Changes
		G. Som.	10 Degrees

- 4. Selecione o grupo recém-criado no menu drop-down Selecionar Grupo.
- 5. Clique em Mover para mover o ponto final selecionado para o novo grupo.

Move Computers to	Group			$\times$
ESKTOP- in g	roup TEST			
Move To	Existing Group	New Group		
Select Group	Debug TechZon	e Group	~	
			Cancel	Move

Etapa 6: Verifique o endpoint na página do computador e na interface do usuário do conector

- 1. Certifique-se de que o ponto final esteja listado no novo grupo na página Computers.
- 2. No endpoint, abra a interface do usuário do conector Secure Endpoint.
- 3. Verifique se a nova política de depuração é aplicada verificando o ícone Secure Endpoint na barra de menus.



# Secure Client

#### Secure Endpoint

tatistics	Update	Advanced	
Agen	t		
Status:			Connected
Version	c		8.4.0.30201
GUID:			202dac7b-093a-4784-ace8-cb95e8696c96
Last Sc	an:		Today 03:03:18 PM
Isolatio	n:		Not Isolated
Policy	y		
Name:			Debug TechZone Policy
Serial N	lumber:		229
Last Up	date:		Today 03:52:38 PM
() ()	isco Secu	ure Client	×
(	$\mathbf{b}$	Secure End Connected.	point:
		Flash Scan	✓ Start



Observação: o modo de depuração só poderá ser ativado se um engenheiro de suporte técnico da Cisco solicitar esses dados. Manter o modo de depuração habilitado por um período prolongado pode ocupar espaço em disco rapidamente e pode impedir que os dados de log e log de bandeja do conector sejam reunidos no arquivo de diagnóstico de suporte devido ao tamanho excessivo do arquivo.

Entre em contato com o suporte da Cisco para obter mais assistência.

Contatos mundiais de suporte da Cisco

#### 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.