Coleta de dados de diagnóstico do Cisco Secure Endpoint Connector para Mac

Contents

Introduction

Este documento descreve o processo usado para gerar um arquivo de diagnóstico através do aplicativo Support Tool que está disponível no conector Cisco Secure Endpoint Mac e como solucionar problemas de desempenho.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conector Mac de endpoint seguro
- MacOS

Componentes Utilizados

As informações neste documento são baseadas no conector Mac do Secure Endpoint.

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. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

O conector Secure Endpoint Mac empacota um aplicativo chamado Support Tool, que é usado

para gerar informações de diagnóstico sobre o conector que está instalado em seu Mac. Os dados de diagnóstico incluem informações sobre seu Mac, como:

- Utilização de recursos (disco, CPU e memória)
- logs específicos do conector
- informação de configuração de conector

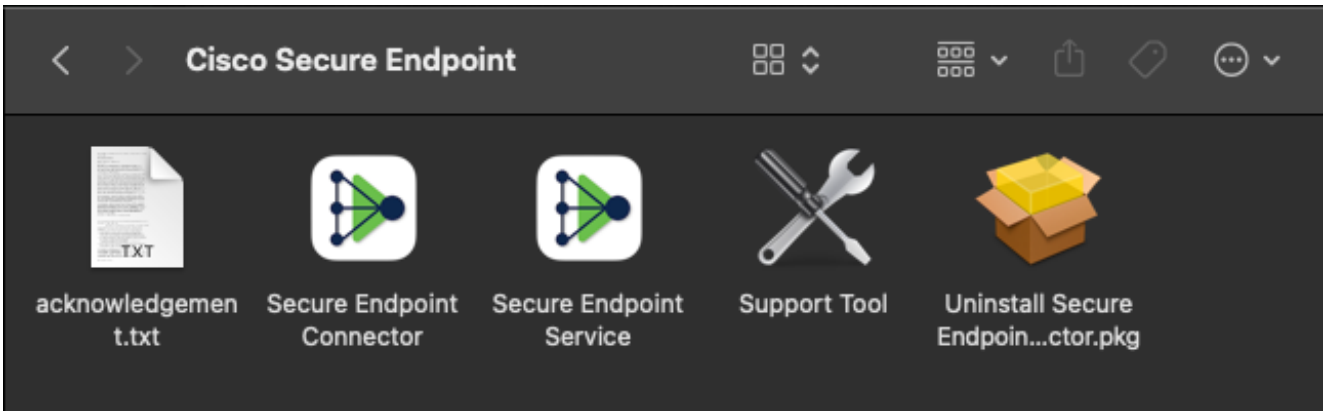
Gere um arquivo de diagnóstico com a ferramenta de suporte

Esta seção descreve como iniciar o aplicativo Support Tool pela GUI ou CLI para gerar um arquivo de diagnóstico.

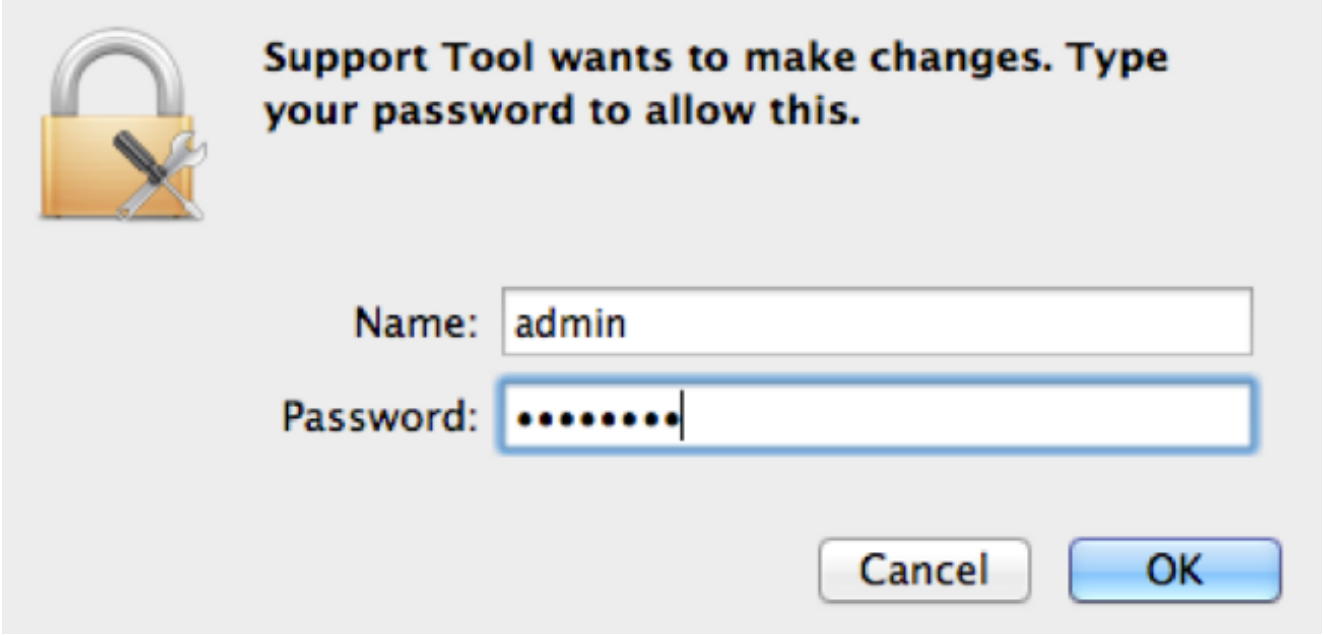
Inicie a ferramenta de suporte usando o macOS Finder

Conclua estes passos para iniciar a Secure Endpoint Mac connector Support Tool usando o macOS Finder:

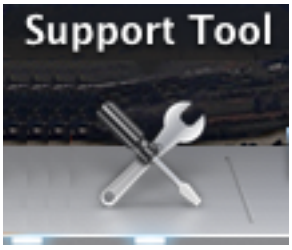
1. Navegue até o diretório Cisco Secure Endpoint na pasta Applications e localize o iniciador da Support Tool:



2. Clique duas vezes no iniciador da Ferramenta de suporte e você será solicitado a fornecer credenciais administrativas:

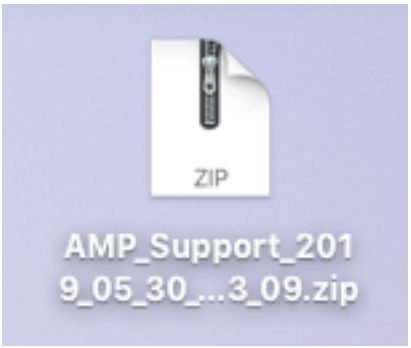


3. Depois de inserir suas credenciais, o ícone Support Tool será exibido na doca:

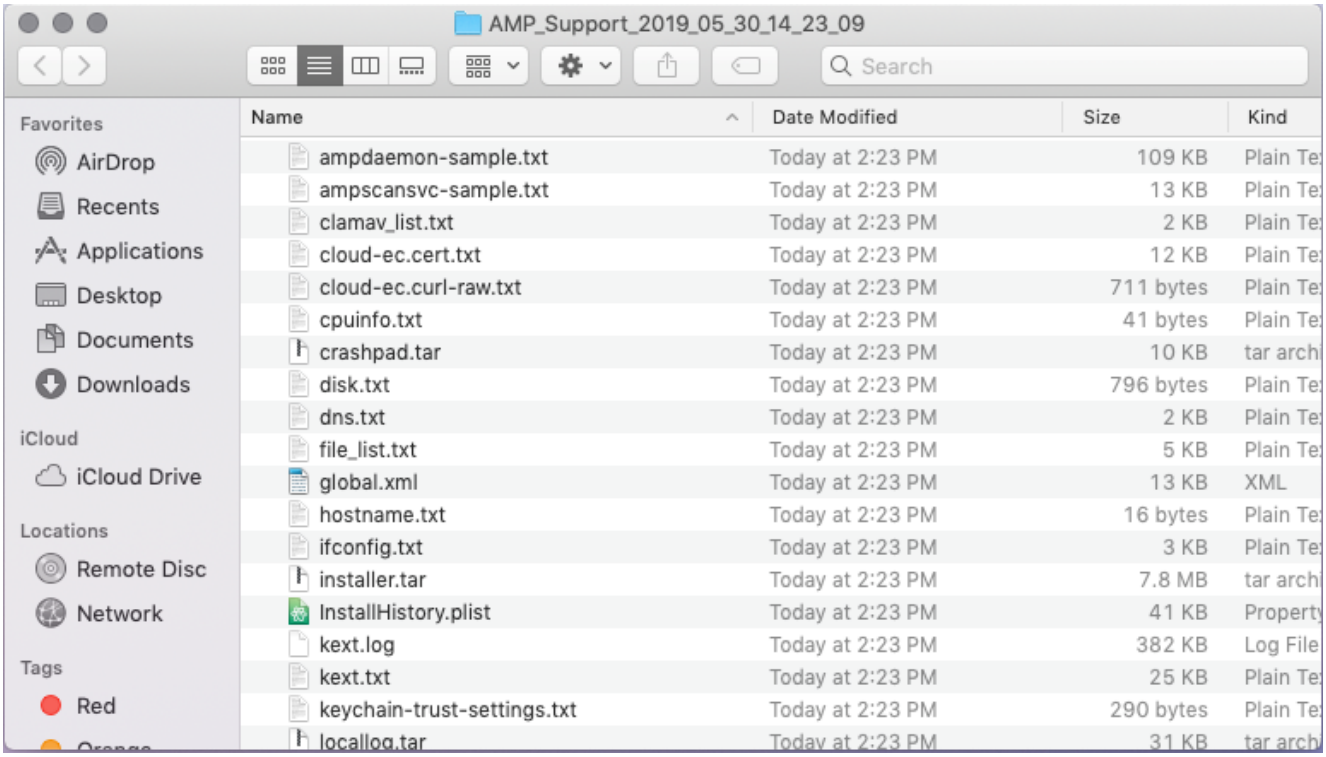


Note: O aplicativo Support Tool é executado em segundo plano e leva algum tempo para ser concluído (aproximadamente 20 a 30 minutos).

4. Quando o aplicativo Support Tool for concluído, um arquivo será gerado e colocado na área de trabalho:



Aqui está um exemplo da saída não compactada:



5. Para analisar os dados, forneça esse arquivo à equipe de suporte técnico da Cisco.

Inicie a ferramenta de suporte usando o terminal macOS

O iniciador da Ferramenta de Suporte está localizado neste diretório:

```
/Library/Application Support/Cisco/AMP for Endpoints Connector/
```

Para iniciar o aplicativo Support Tool, insira o seguinte comando:

> **Note**: Você deve executar esse comando como root, portanto certifique-se de alternar para root ou prefaciar o comando com **sudo**.

```
root@mac# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector root@mac#
./SupportTool
```

> **Note: Esse comando é executado de forma detalhada. Depois de concluído, um arquivo de diagnóstico é gerado e colocado em sua área de trabalho.**

Troubleshooting

Esta seção descreve como habilitar e desabilitar o modo de depuração no conector Secure Endpoint Mac para solucionar problemas de desempenho.

Habilitar Modo de Depuração

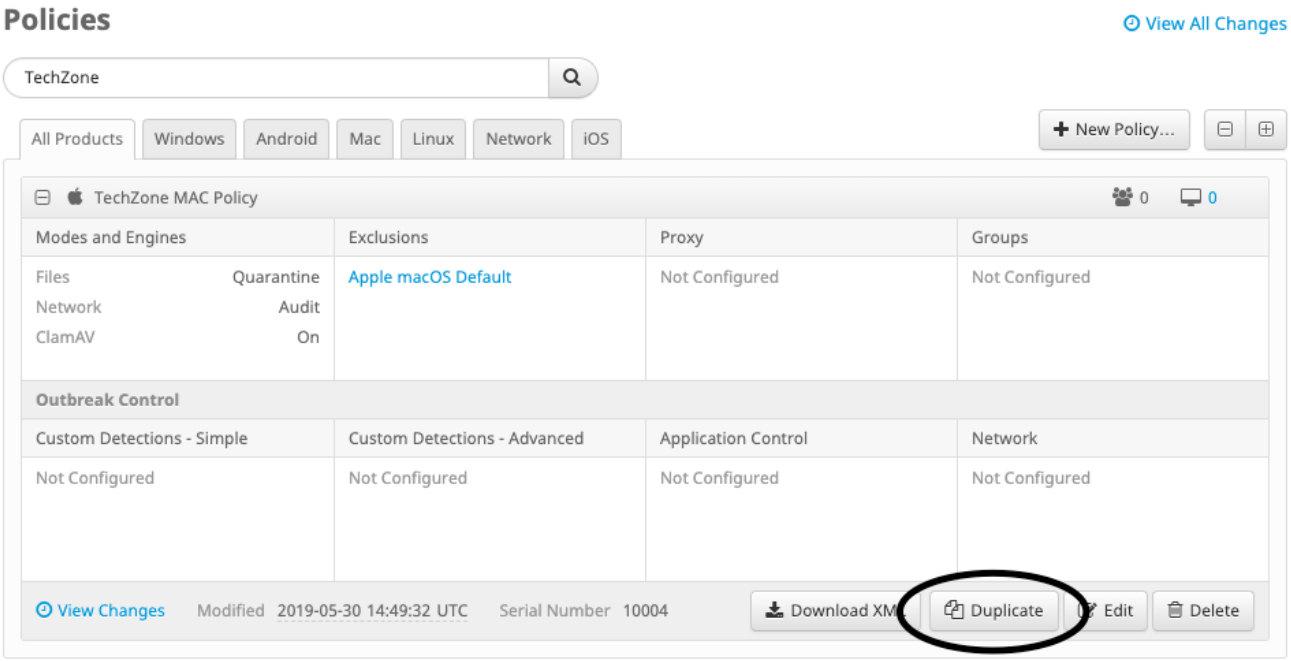
> **Aviso**: o modo de depuração deve ser ativado somente se um engenheiro de suporte técnico da Cisco fizer uma solicitação para esses dados. Se você mantiver o modo de

depuração ativado por um longo período, ele poderá ocupar o espaço em disco muito rapidamente e poderá impedir que os dados de log do conector e do log da bandeja sejam reunidos no arquivo de Diagnóstico de Suporte devido ao tamanho excessivo do arquivo.

O modo de depuração é útil nas tentativas de solucionar problemas de desempenho em um conector de Ponto de Extremidade Seguro. Conclua estes passos para habilitar o modo de depuração e coletar dados de diagnóstico;

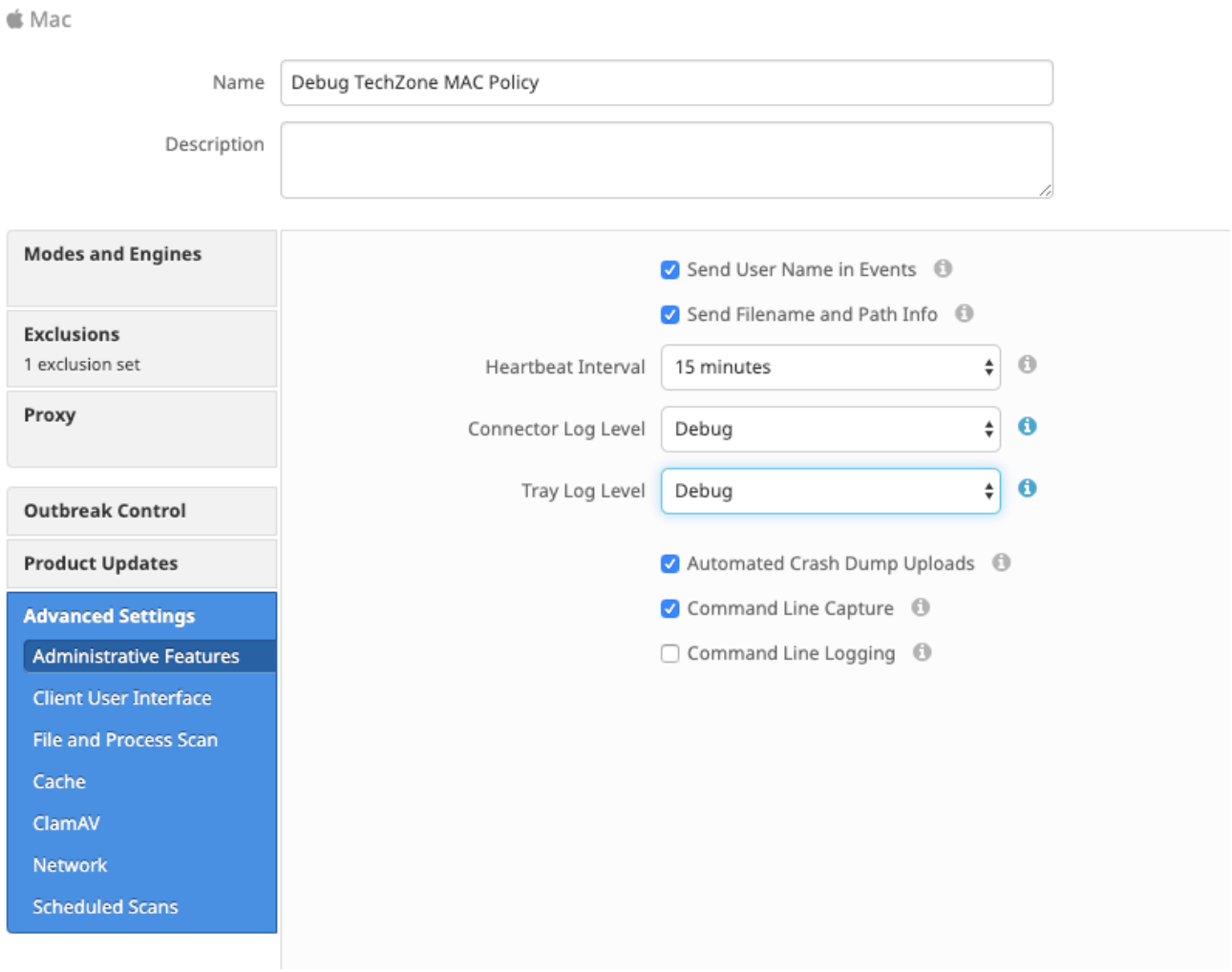
1. Faça login no console do Secure Endpoint.
2. Navegue até **Gerenciamento > Políticas**.

3. Localize uma diretiva que seja aplicada a um computador, clique na diretiva que expandirá a janela da diretiva e clique em **Duplicar**. O Console de endpoint seguro é atualizado com a política duplicada:

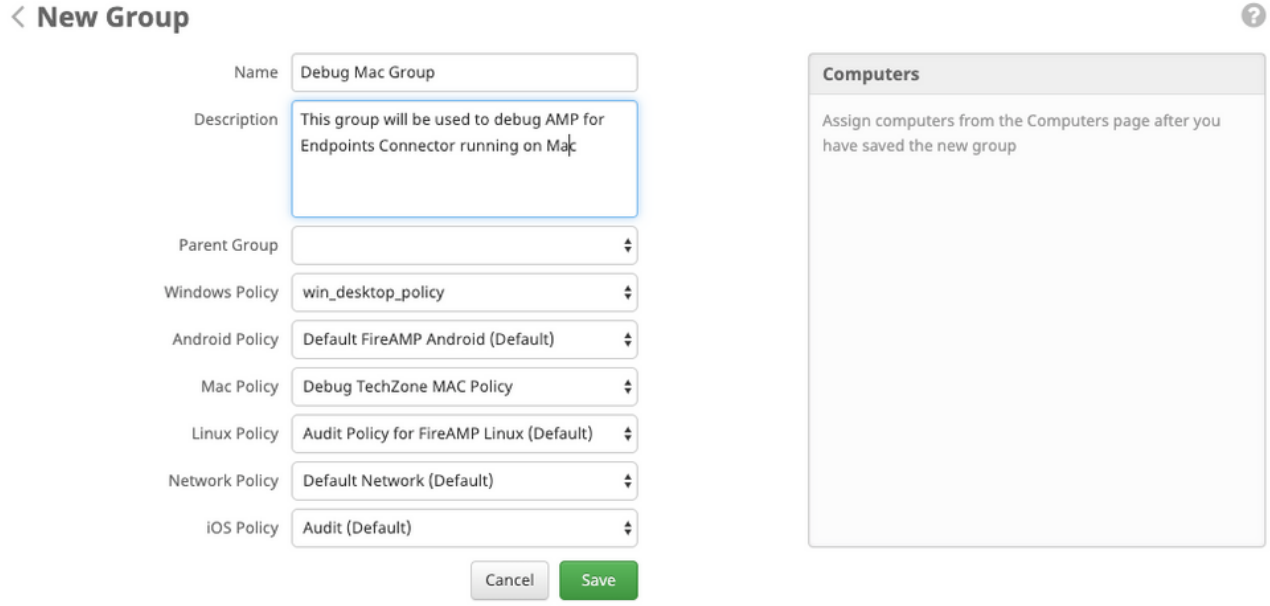


4. Selecione e expanda a janela Diretiva de duplicação, clique em **Editar** e alterar o nome da política. Por exemplo, você pode usar *Debug TechZone MAC Policy*.

5. Clique em **Configurações avançadas**, selecione **Recursos administrativos** na barra lateral e selecione **Debug** para os menus suspensos Nível de log do conector e Nível de log da bandeja:



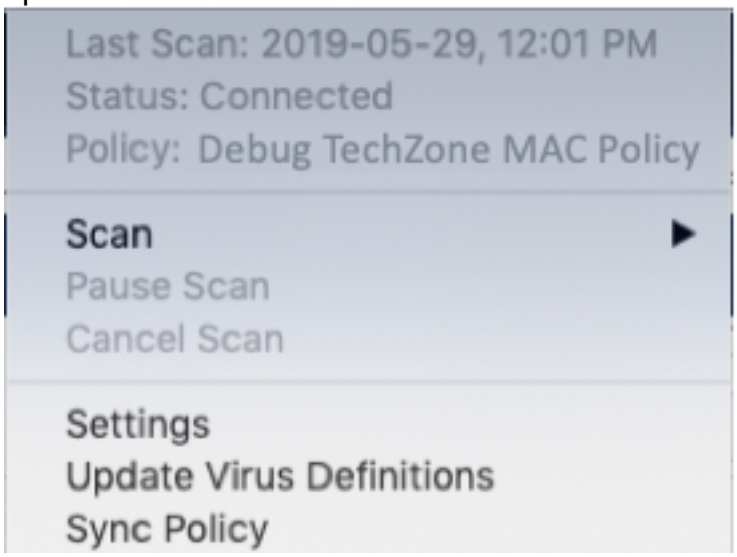
6. Clique no botão **Save** para salvar as alterações.
7. Navegue até **Gerenciamento > Grupos** e clique em **Criar grupo** perto da parte superior direita da tela.
8. Digite um nome para o grupo. Por exemplo, você poderia *usarDebug TechZone Mac Group*.



9. Alterar a Política de Mac de *Política Mac Padrão* à nova política duplicada que você acabou de criar, que é **Debug TechZone Mac Policy** neste exemplo. Clique em **Save**.
10. Navegue até **Gerenciamento > Computadores** e identificar o computador na lista.

Selecione-a e clique em **Mover para grupo...**.

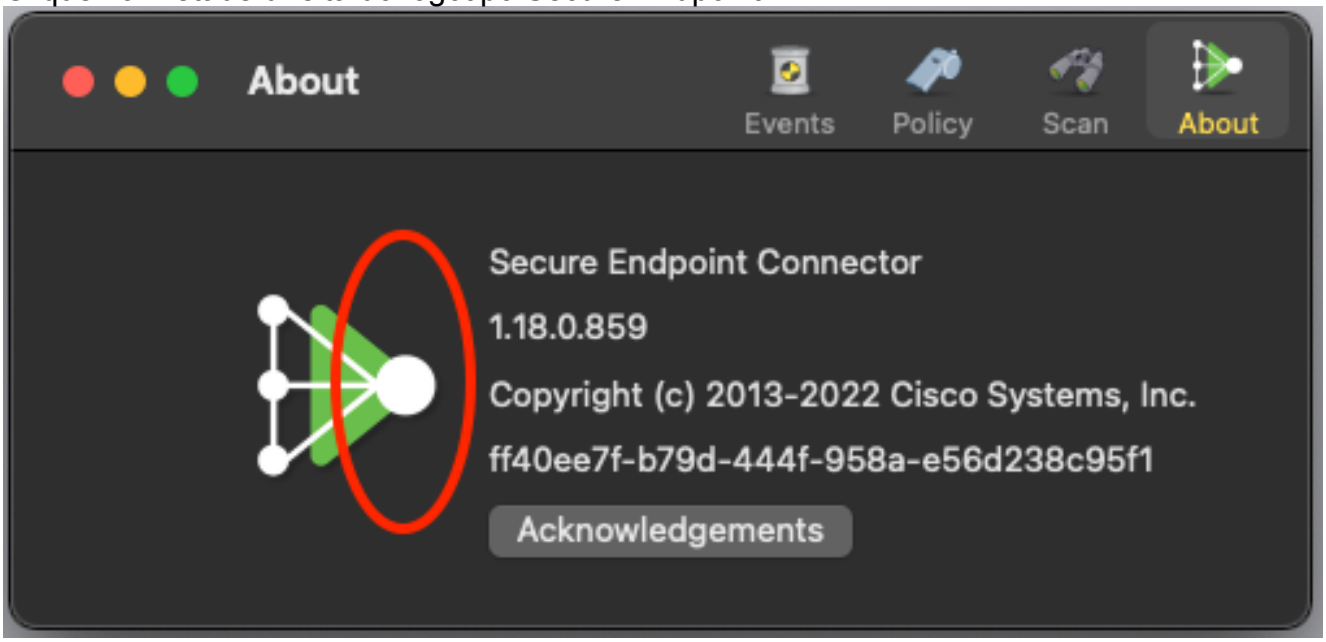
11. Selecione o grupo recém-criado na **Selecionar grupo** menu suspenso. Clique em **Mover** para mover o computador selecionado para o novo grupo. Seu Mac agora deve ter uma política de depuração funcional. Você pode selecionar o ícone Ponto de extremidade seguro que aparece na barra de menus e garantir que a nova política seja aplicada:



Habilitar Modo de Depuração de Pulsação Única

Este procedimento está disponível apenas para o conector 1.0.4 e acima. Isso permite que um único conector seja colocado no modo de depuração até o próximo heartbeat. Dependendo da situação, isso pode fornecer informações suficientes para nossos desenvolvedores, mas, dependendo da duração do heartbeat, há o risco de não capturar todos os processos necessários para fazer uma análise completa do diagnóstico. Estas são as etapas para ativar a depuração para uma única pulsação:

1. Acesse a barra de menus do conector e vá para **Configurações.**
2. Clique em **Sobre.**
3. Clique na metade direita do logotipo Secure Endpoint.



4. se tiver sido feito corretamente, o seguinte aviso será exibido no lado direito da tela:

A depuração será desabilitada automaticamente após a próxima pulsação.

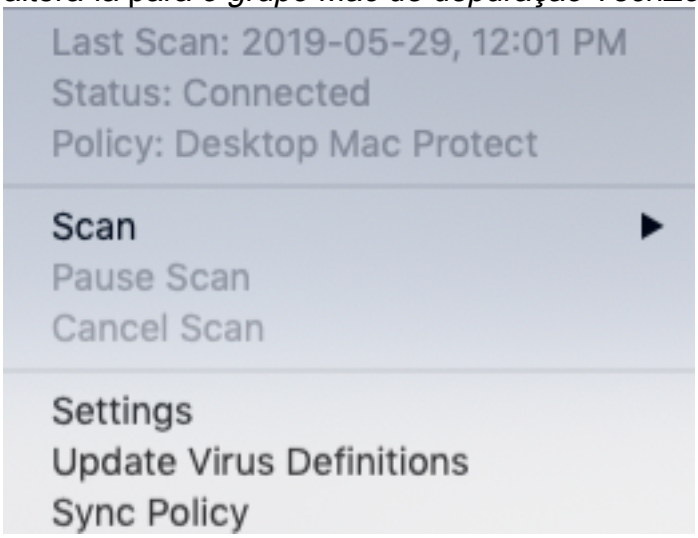
Desativar modo de depuração

Depois que os dados de diagnóstico no modo de depuração forem obtidos, você deverá reverter o conector de Ponto de Extremidade Seguro de volta ao modo normal. Conclua estes passos para desativar o modo de depuração:

1. Faça login no console Secure Endpoint.
2. Navegue até **Gerenciamento > Grupos**.

3. Localize o novo grupo,*Debug TechZone Mac Group*, criado no modo de depuração.
4. Clique em **Editar**.

5. Na janela Computadores localizada na parte superior direita da tela, localize seu computador na lista. Selecione-o, o que o levará para a páginaComputadores. Mais uma vez, selecione seu computador na lista e **clique em Mover para grupo...**.
6. Selecione seu grupo anterior **no menu** suspenso **Selecionar** grupo. Clique em Moverpara mover o computador selecionado para o grupo anterior.
7. Clique no ícone Secure Endpoint na barra de menus. **SelecionePolítica** de **Sincronização** no menu.
8. Verifique se a política agora voltou ao valor padrão anterior. Marque isto na barra de menus. A política agora deve ter sido revertida para a política original que foi usada antes de você alterá-la para *o grupo Mac de depuração TechZone*:



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.