Integre o AMP para endpoints e o Threat Grid com o WSA

Contents

Introduction

Este documento descreve as etapas para integrar a Proteção avançada contra malware (AMP) para endpoints e o Threat Grid (TG) com o Web Security Appliance (WSA).

Contribuído por Uriel Montero e editado por Yeraldin Sanchez, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- AMP para acesso de endpoints
- Acesso premium TG
- WSA com análise de arquivo e chaves de recurso de reputação de arquivo

Componentes Utilizados

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

- Console de nuvem pública AMP
- GUI do WSA
- Console TG

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.

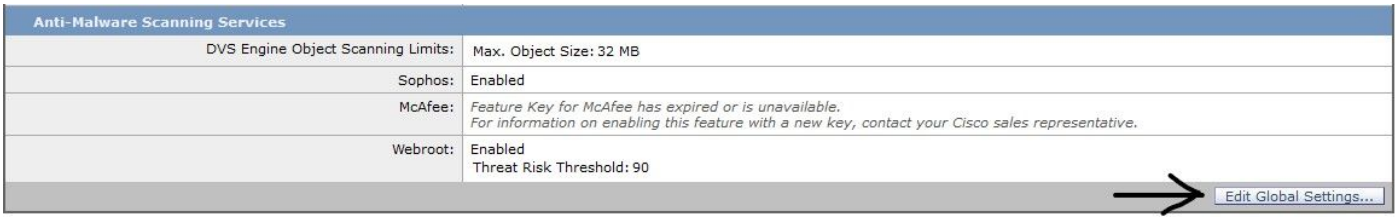
Configurar

Faça login no console WSA.

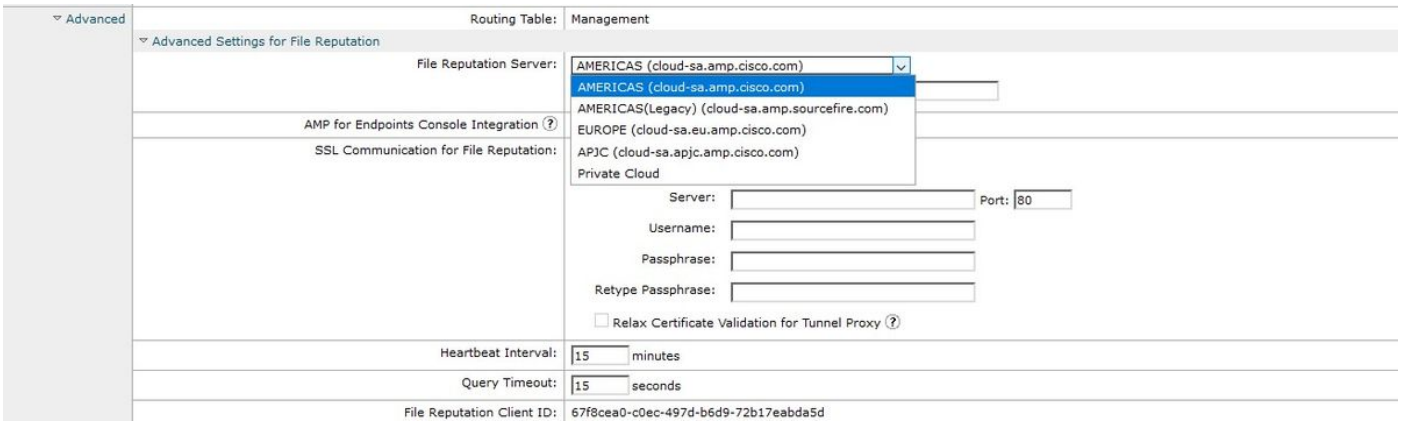
Depois de fazer login, navegue até **Security Services > Anti-Malware and Reputation,** nesta seção, você pode encontrar as opções para integrar AMP e TG.

Integração da AMP

Na seção Anti-Malware Scanning Services, clique em **Edit Global Settings**, conforme mostrado na imagem.

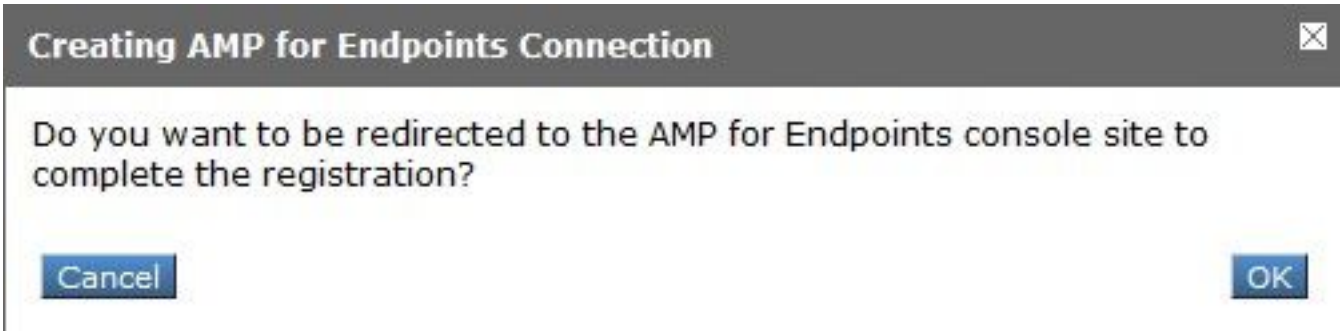


Procure a seção **Advanced > Advanced Settings for File Reputation** e expanda-a; em seguida, uma série de opções de servidores de nuvem são exibidas; escolha a mais próxima de sua localização.

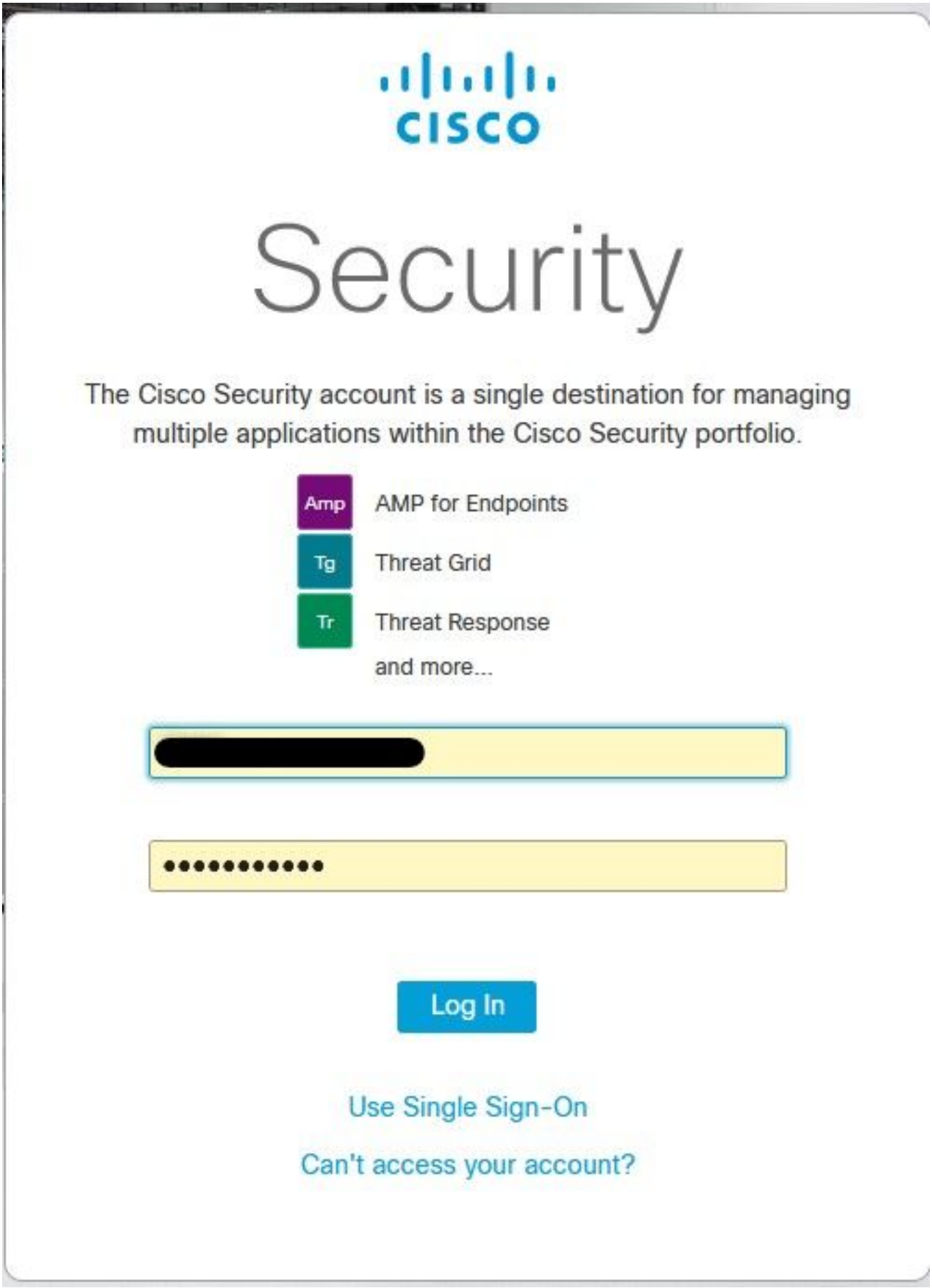


Depois que a nuvem for selecionada, clique no botão **Register Appliance with AMP for Endpoints**.

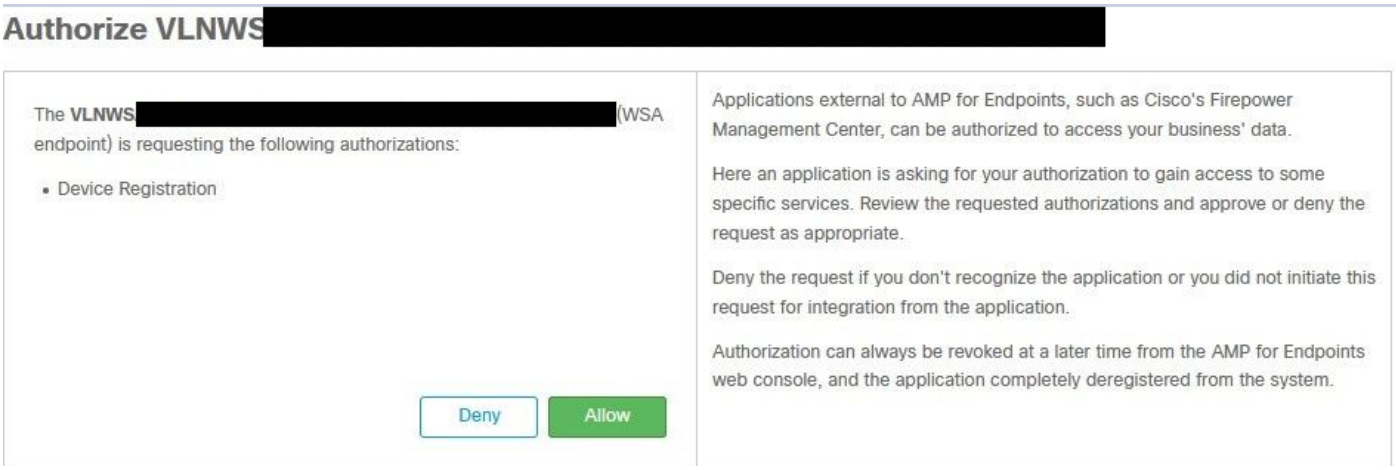
Uma janela pop-up exibida que é redirecionada para o console AMP, clique no **botão Ok,** como mostrado na imagem.



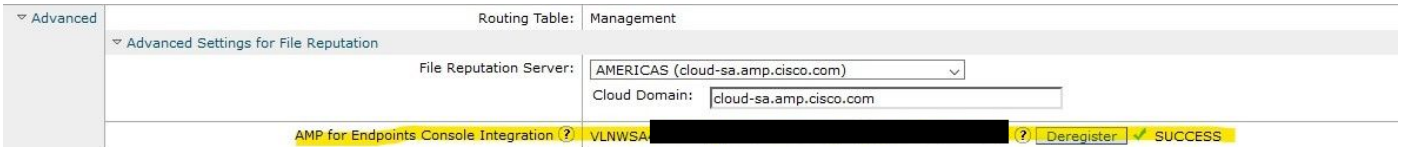
Você precisa ingressar em Credenciais AMP válidas e clicar em **Fazer login,** como mostrado na imagem.



Aceite o Device Registration, anote o ID do cliente, pois ele ajuda a encontrar o WSA posteriormente no console.



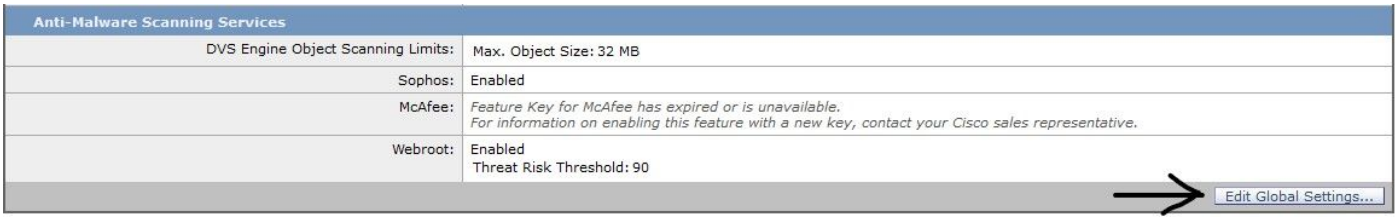
Volte para o console WSA, uma verificação é exibida na seção Amp for Endpoints Console Integration, como mostrado na imagem.



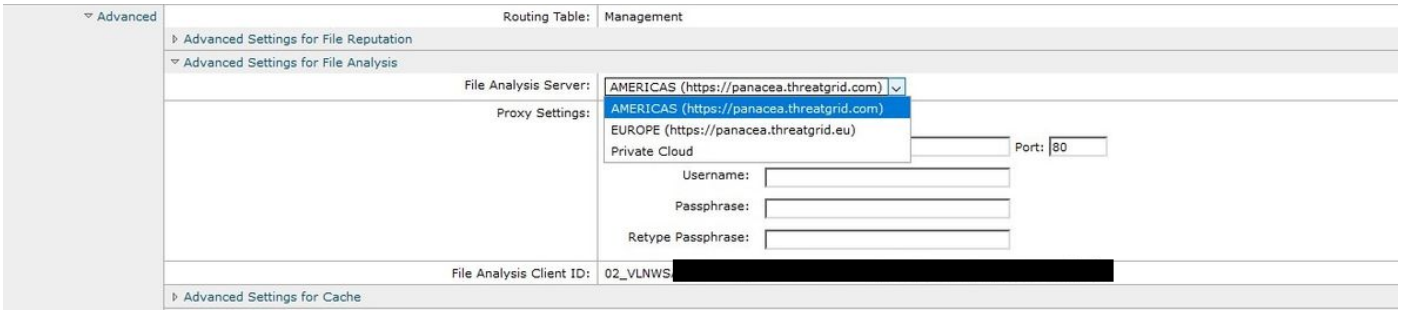
Observação: não se esqueça de clicar em **Enviar** e **Confirmar** as alterações (se solicitado); caso contrário, o processo precisa ser feito novamente.

Integração do Threat Grid

Navegue até **Security Services > Anti-Malware and Reputation** e, em seguida, nos Anti-Malware Protection Services, clique no botão **Edit Global Settings**, conforme mostrado na imagem.

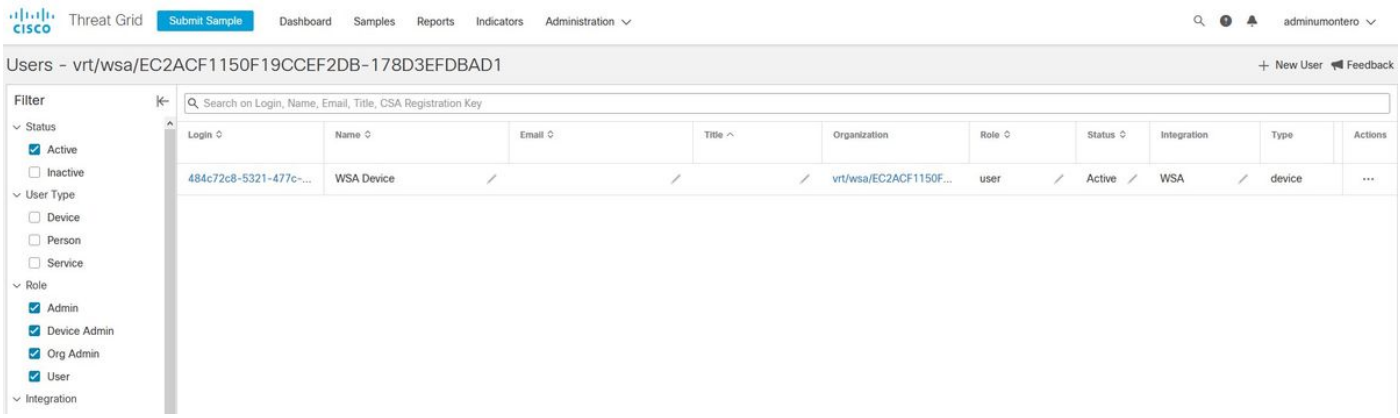


Procure a seção **Advanced > Advanced Settings for File Analysis** e expanda-a, escolha a opção mais próxima de seu local, como mostrado na imagem.



Clique em **Enviar** e **Confirmar** as alterações.

No lado do portal TG, procure o dispositivo WSA na guia Users (Usuários) se o dispositivo foi integrado com êxito ao AMP/TG.



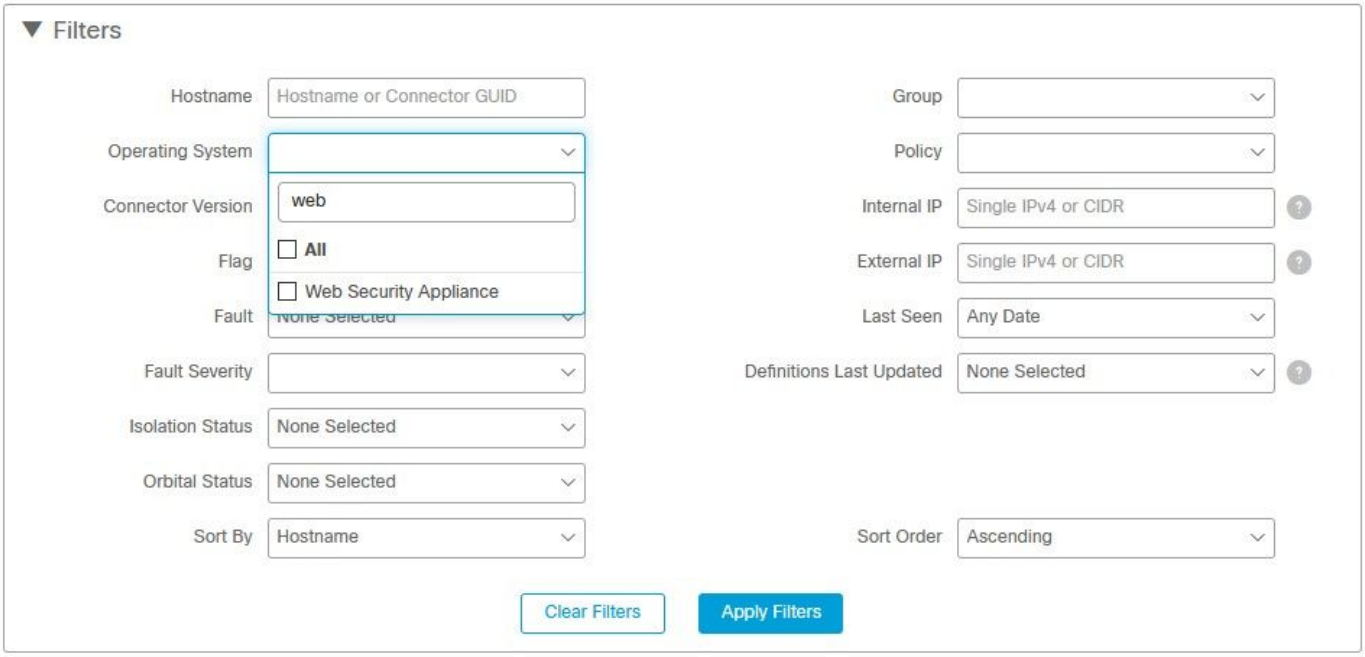
Se clicar em Login, você poderá acessar as informações desse aplicativo.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

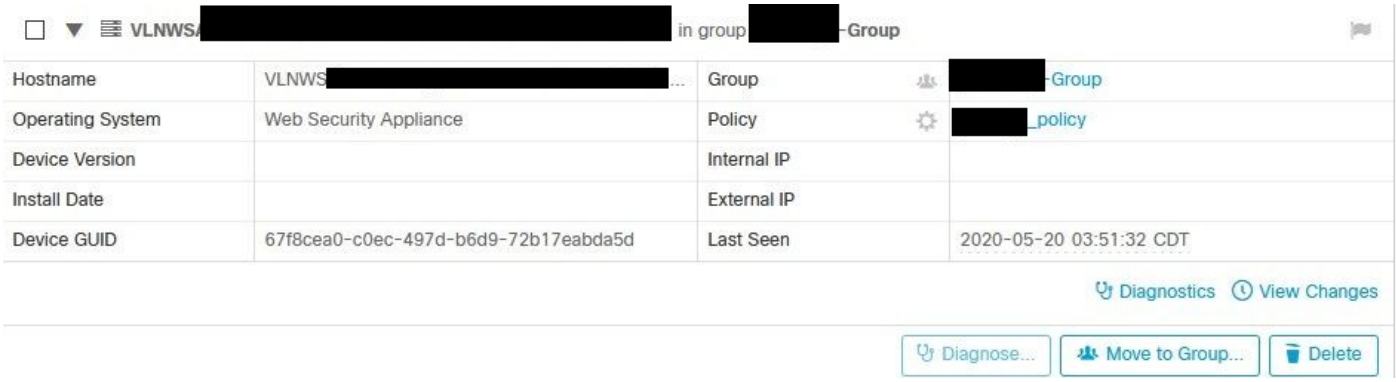
Para verificar se a integração entre o AMP e o WSA foi bem-sucedida, você pode fazer login no console do AMP e procurar seu dispositivo WSA.

Navegue até **Gerenciamento > Computadores**, na seção filtros, procure **Web Security Appliance** e aplique o filtro

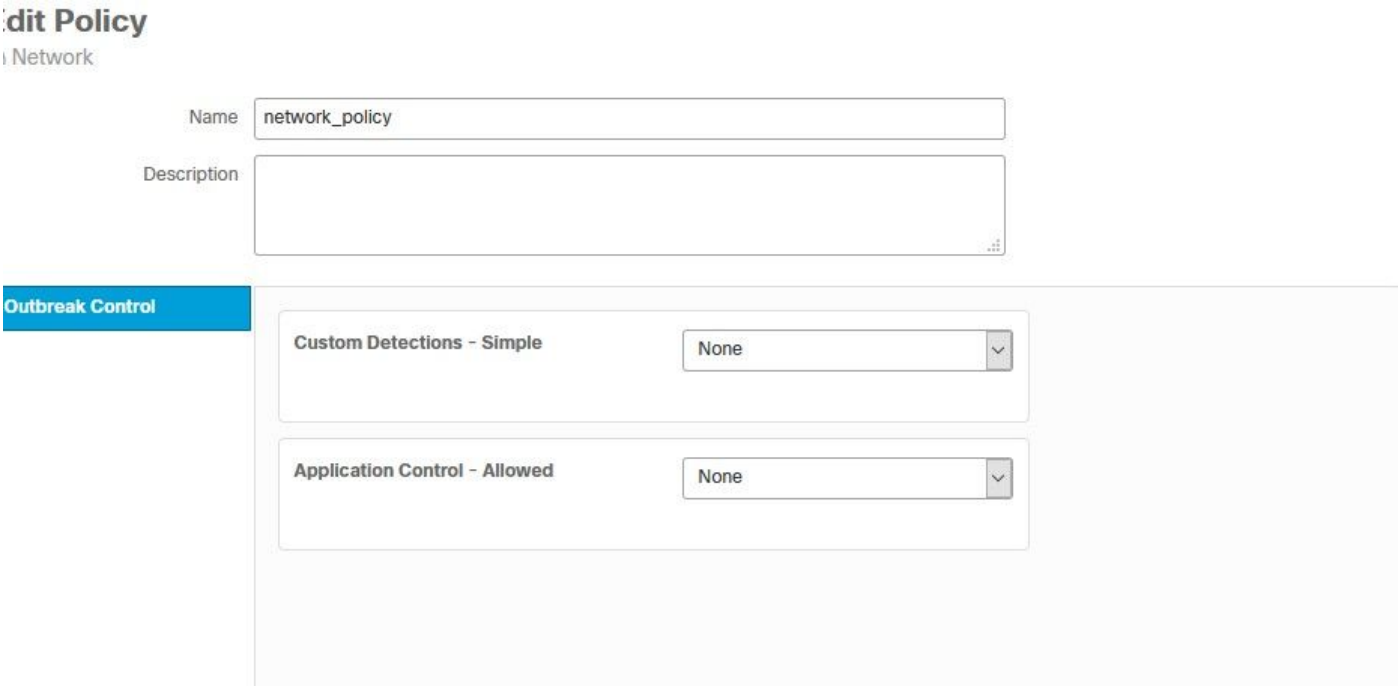


Se você tiver vários dispositivos WSA registrados, poderá identificá-los com a ID do cliente de análise de arquivo.

Se você expandir o dispositivo, poderá ver a qual grupo ele pertence, a Política aplicada e o GUID do dispositivo podem ser usados para exibir a trajetória do dispositivo.

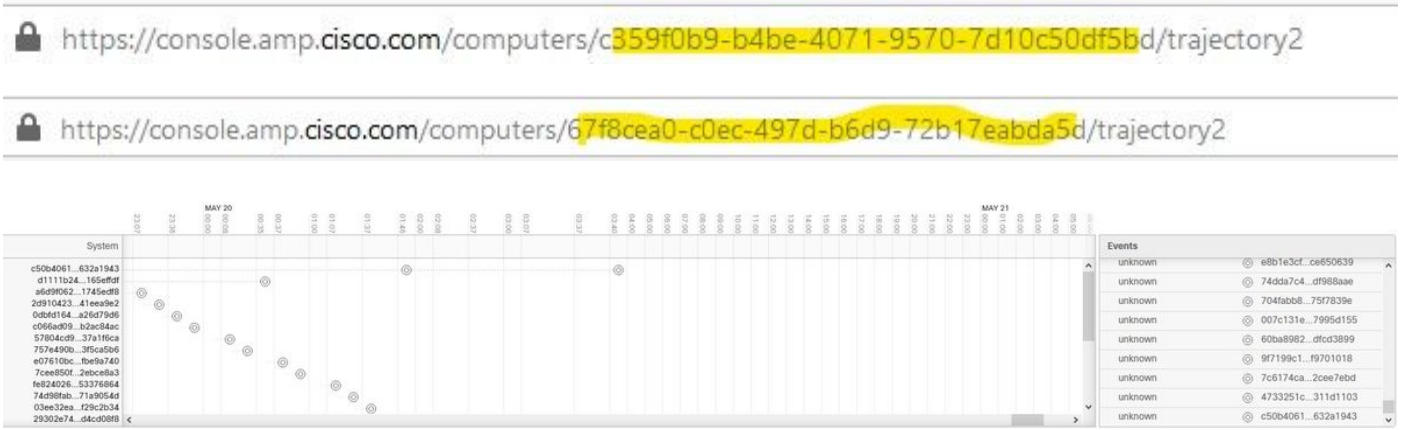


Na seção de política, você pode configurar Detecções Personalizadas Simples e Controle de Aplicativos - Permitido que é aplicado ao dispositivo.

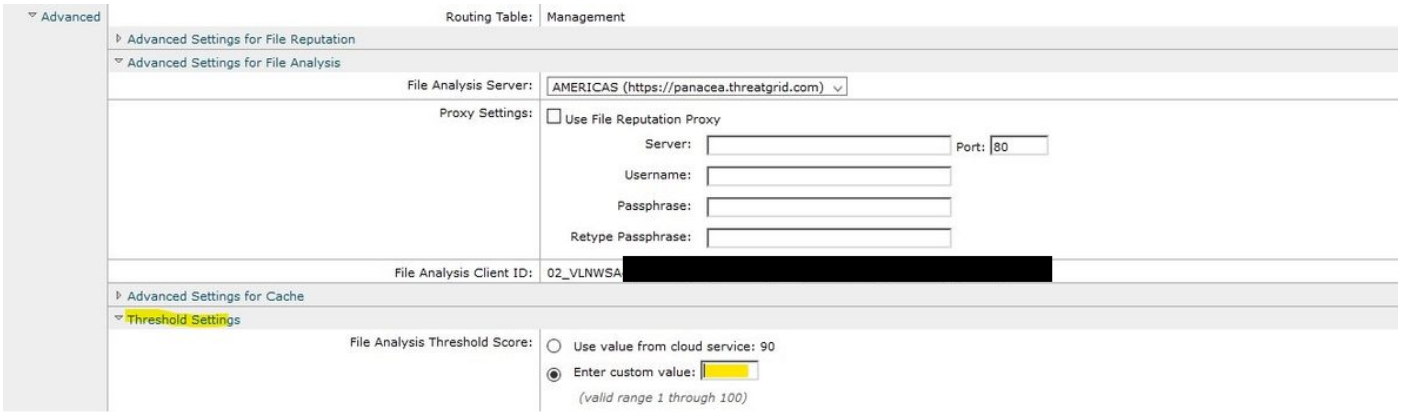


Há um truque para exibir a seção Trajetória do dispositivo do WSA. Você precisa abrir a Trajetória do dispositivo de outro computador e usar o GUID do dispositivo.

A alteração é aplicada ao URL, como mostrado nas imagens.



Para o Threat Grid, há um limite de 90. Se um arquivo obtiver uma pontuação abaixo desse número, o arquivo não será marcado como mal-intencionado, entretanto, você pode configurar um limite personalizado no WSA.



Troubleshoot

O WSA não redireciona para a página AMP

- Certifique-se de que o firewall permita os endereços necessários para o AMP, clique aqui.
- Verifique se você selecionou a nuvem da AMP adequada (evite escolher a nuvem antiga).

O WSA não bloqueia os SHAs especificados

- Verifique se o WSA está no grupo correto.
- Verifique se o WSA está usando a política correta.
- Certifique-se de que o SHA não esteja limpo na nuvem; caso contrário, o WSA não poderá bloqueá-lo.

O WSA não aparece na minha organização TG

- Verifique se você selecionou a nuvem TG apropriada (Américas ou Europa).
- Certifique-se de que o Firewall permita os endereços necessários para TG.
- Anote a ID do cliente de análise de arquivo.
- Procure-o na seção Usuários.
- Se você não o encontrar, entre em contato com o Suporte da Cisco para que ele possa ajudá-lo a movê-lo entre as empresas.