Integre o AMP para valores-limite e grade da ameaça com WSA

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Configurar](#)
[Integração AMP](#)
[Integração da grade da ameaça](#)
[Verificar](#)
[Troubleshooting](#)
[WSA não reorienta à página AMP](#)
[WSA não obstrui os SHA especificados](#)
[WSA não aparece em minha organização TG](#)

Introdução

Este original descreve as etapas para integrar a proteção avançada do malware (AMP) para valores-limite e grade da ameaça (TG) com ferramenta de segurança da Web (WSA).

Contribuído por Uriel Montero e editado por Yeraldin Sánchez, engenheiros de TAC da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- AMP para o acesso dos valores-limite
- Acesso do prêmio TG
- WSA com chaves de recurso da análise do arquivo e da reputação do arquivo

Componentes Utilizados

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

- Console público da nuvem AMP
- WSA GUI
- Console TG

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.

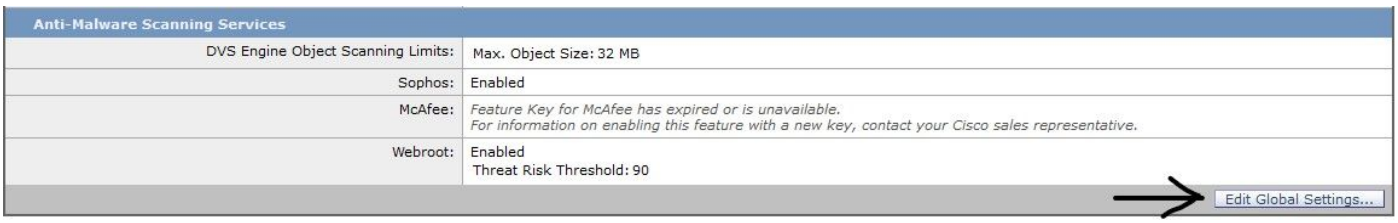
Configurar

Entre ao console WSA.

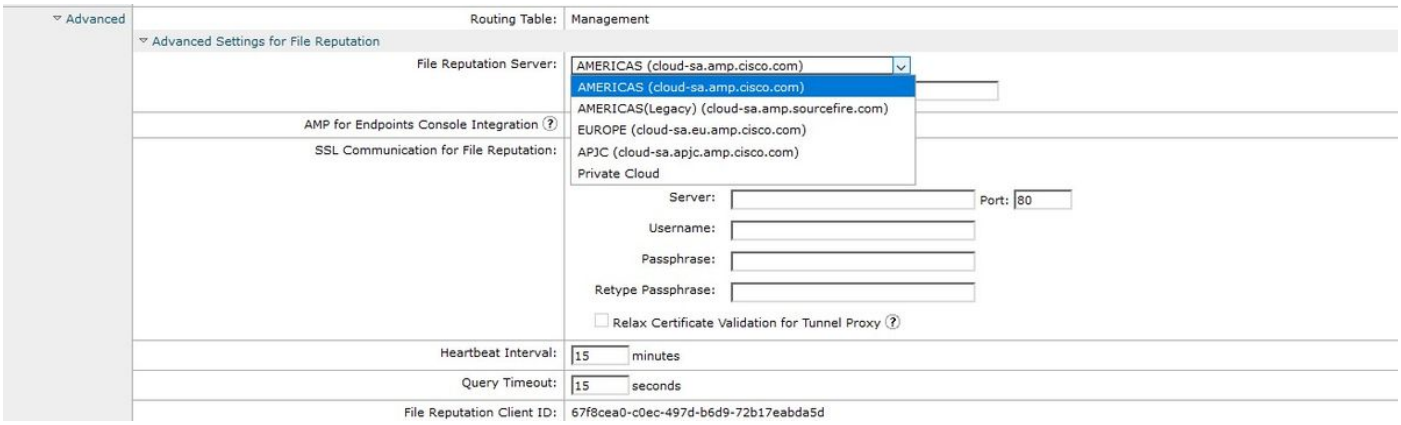
Uma vez que entrado, navegue aos **Serviços de segurança > ao Anti-malware e à reputação, n**esta seção você pode encontrar as opções para integrar o AMP e o TG.

Integração AMP

Na exploração do Anti-malware os serviços secionam, clicam sobre **configurações globais Edit**, segundo as indicações da imagem.

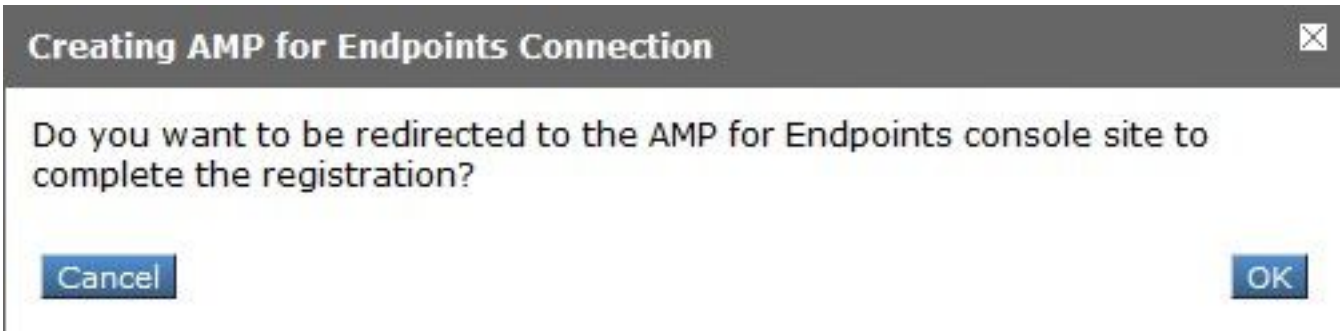


Procure pelo **avançado > avançou ajustes para a** seção da **reputação do arquivo** e expandem-nos, a seguir uma série de opções dos server da nuvem é indicada, escolhe o mais próximo a seu lugar.

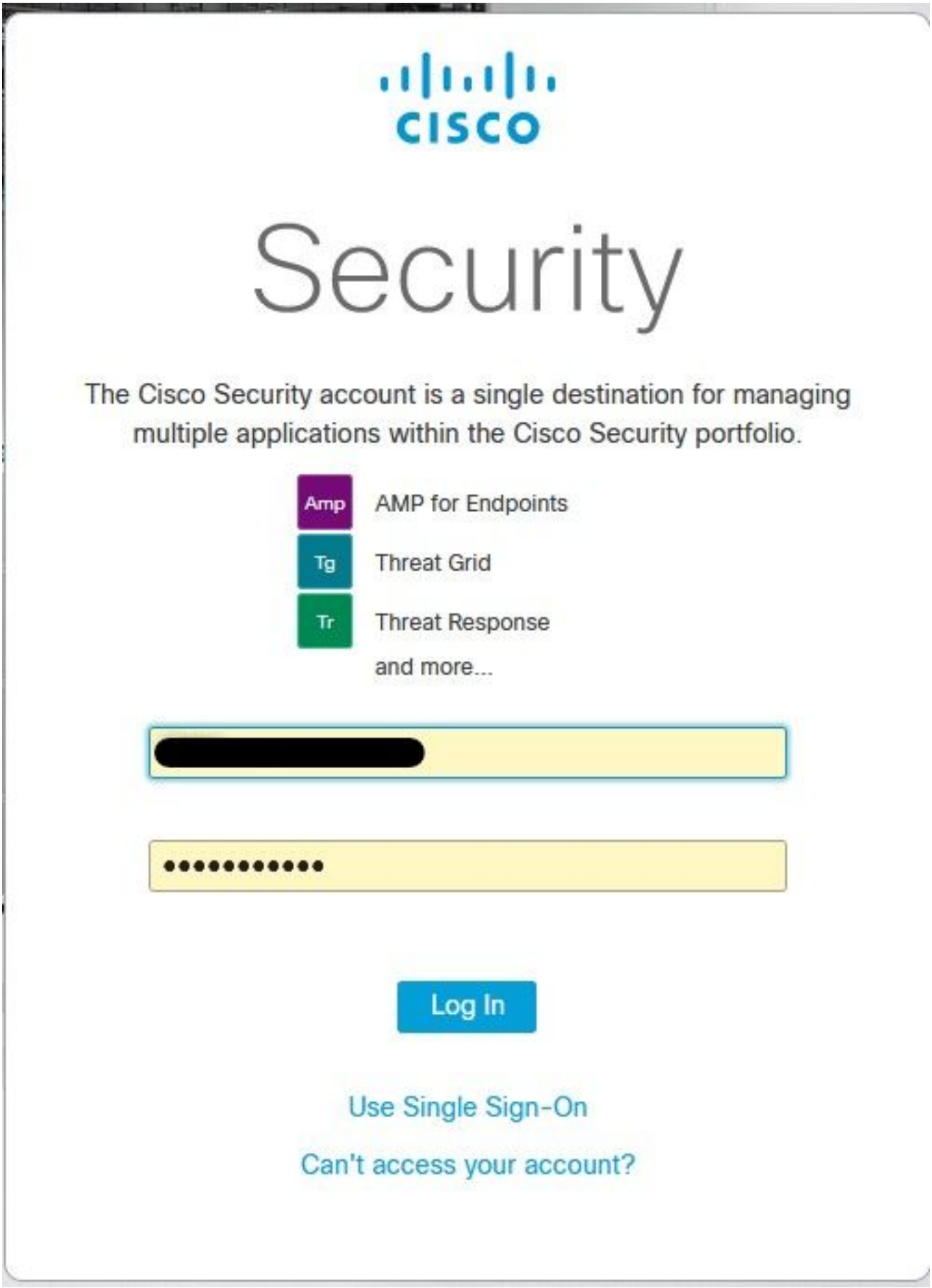


Uma vez que a nuvem foi selecionada, clique sobre o **dispositivo do registro com o AMP para o** botão dos **valores-limite**.

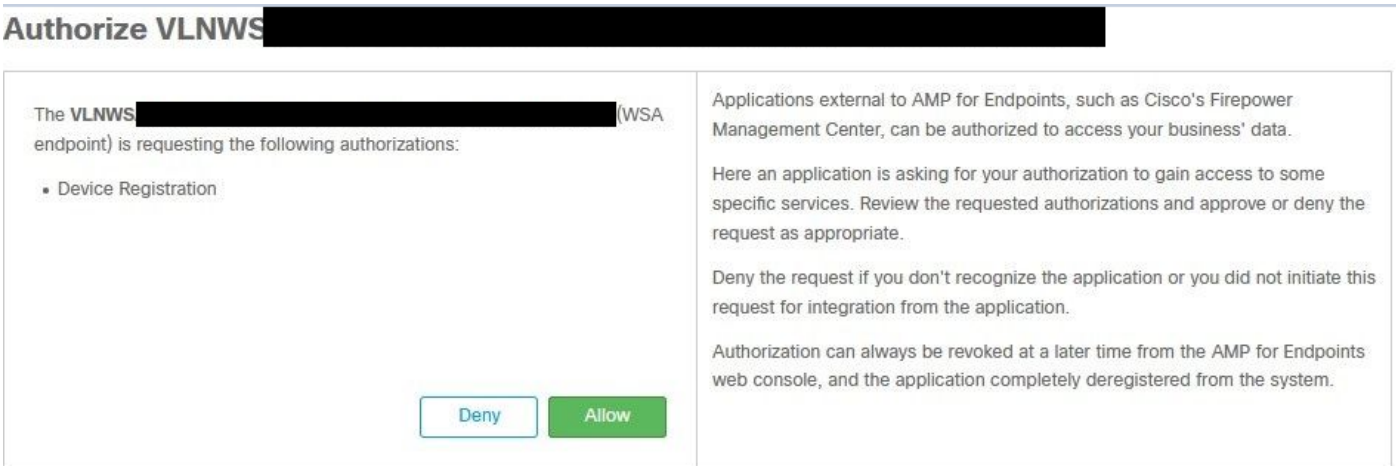
Um estalo aparece acima que reoriente ao console AMP, clica o **botão OK,** segundo as indicações da imagem.



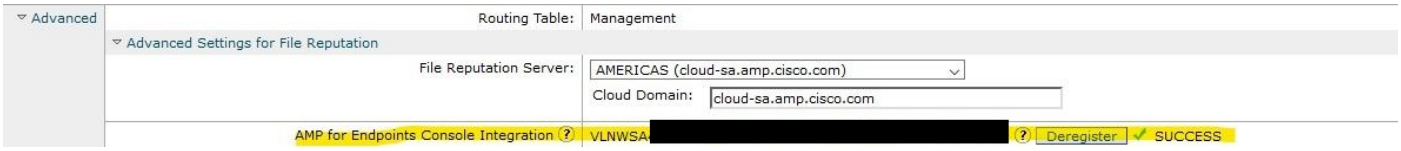
Você precisa credenciais válidas do ingresso AMP e clica sobre o **início de uma sessão,** segundo as indicações da imagem.



Aceite o registro do dispositivo, tome a nota da identificação de cliente, como ajuda a encontrar mais tarde o WSA o console.



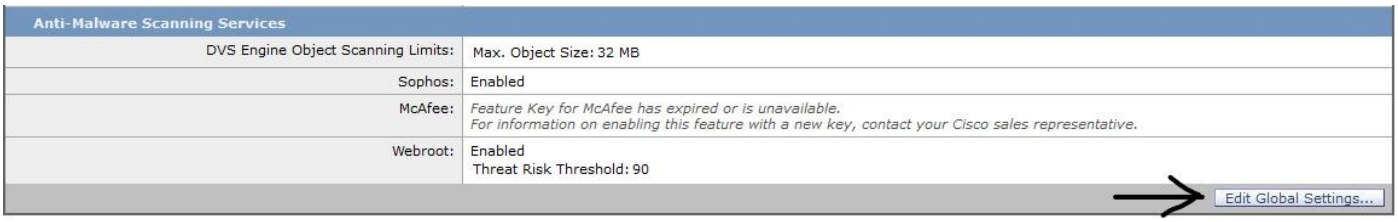
Vai para trás ao console WSA, uma verificação aparece no ampère para a seção de integração do console dos valores-limite, segundo as indicações da imagem.



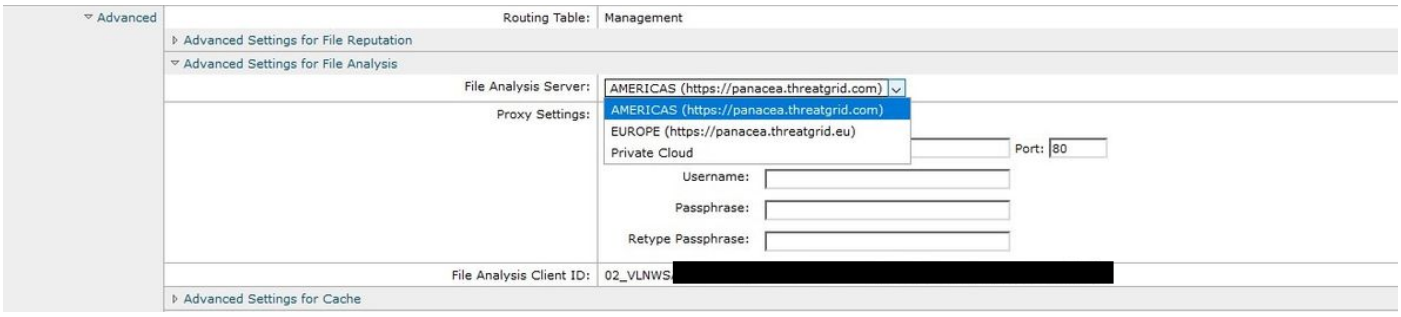
> Nota: Não esqueça clicar sobre **Submit** e **Commit as** mudanças (se alertado), se não, o processo precisa de ser feito outra vez.

Integração da grade da ameaça

Navegue aos **Serviços de segurança > ao Anti-malware e à reputação**, a seguir nos serviços de proteção do Anti-malware, clicam sobre as **configurações globais da edição** abotoam-se, segundo as indicações da imagem.

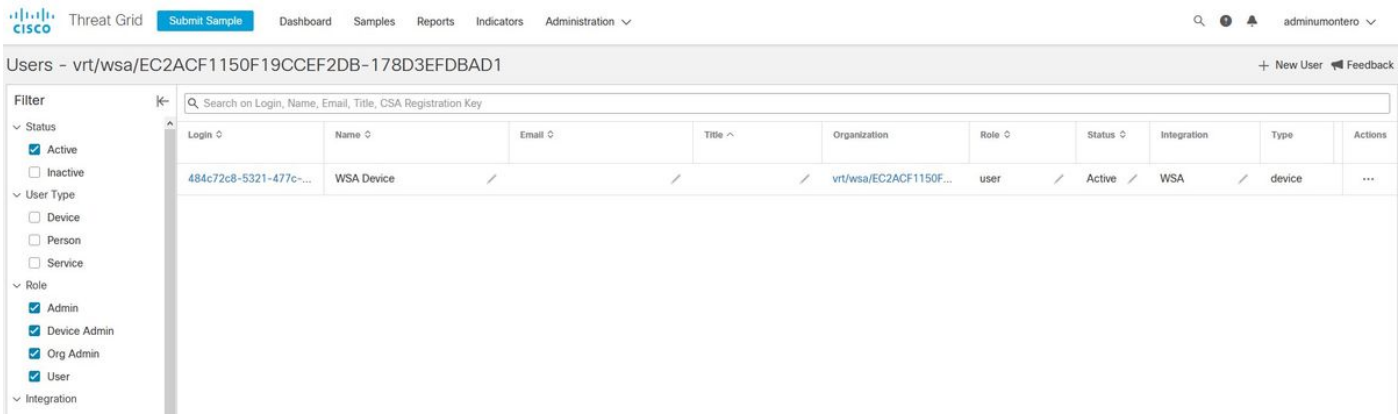


Procure pelo **avançado > avançou ajustes para a** seção da **análise do arquivo** e expandem-nos, escolhem-nos a opção a mais próxima a seu lugar, segundo as indicações da imagem.



Clique sobre **Submit** e **Commit as** mudanças.

No lado portal TG, busca para o dispositivo WSA sob a aba dos usuários se o dispositivo foi integrado com sucesso com AMP/TG.



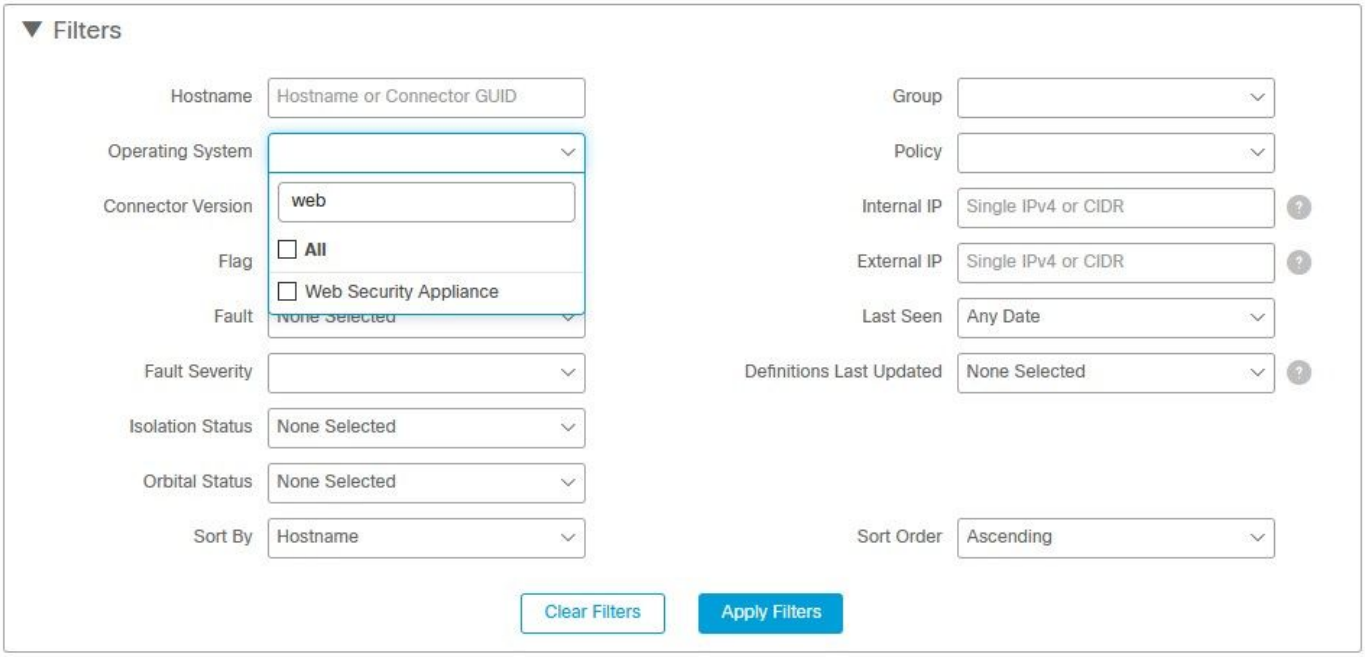
Se você clica sobre o início de uma sessão, você pode alcançar a informação de dispositivo dito.

Verificar

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

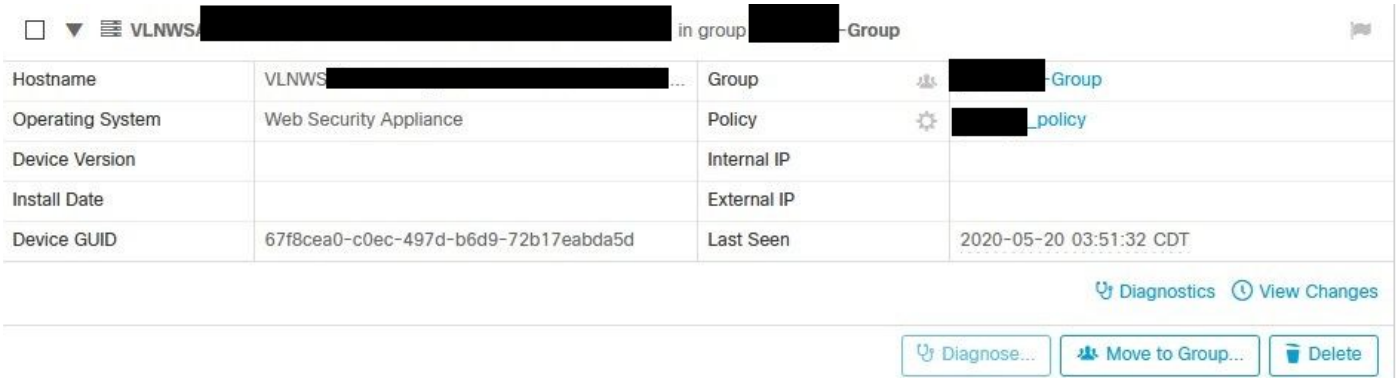
A fim verificar que a integração entre o AMP e o WSA é bem sucedida, você pode entrar ao console e à busca AMP para seu dispositivo WSA.

Navegue ao **Gerenciamento > aos computadores**, na seção dos filtros, procuram pela **ferramenta de segurança da Web** e aplicam o filtro

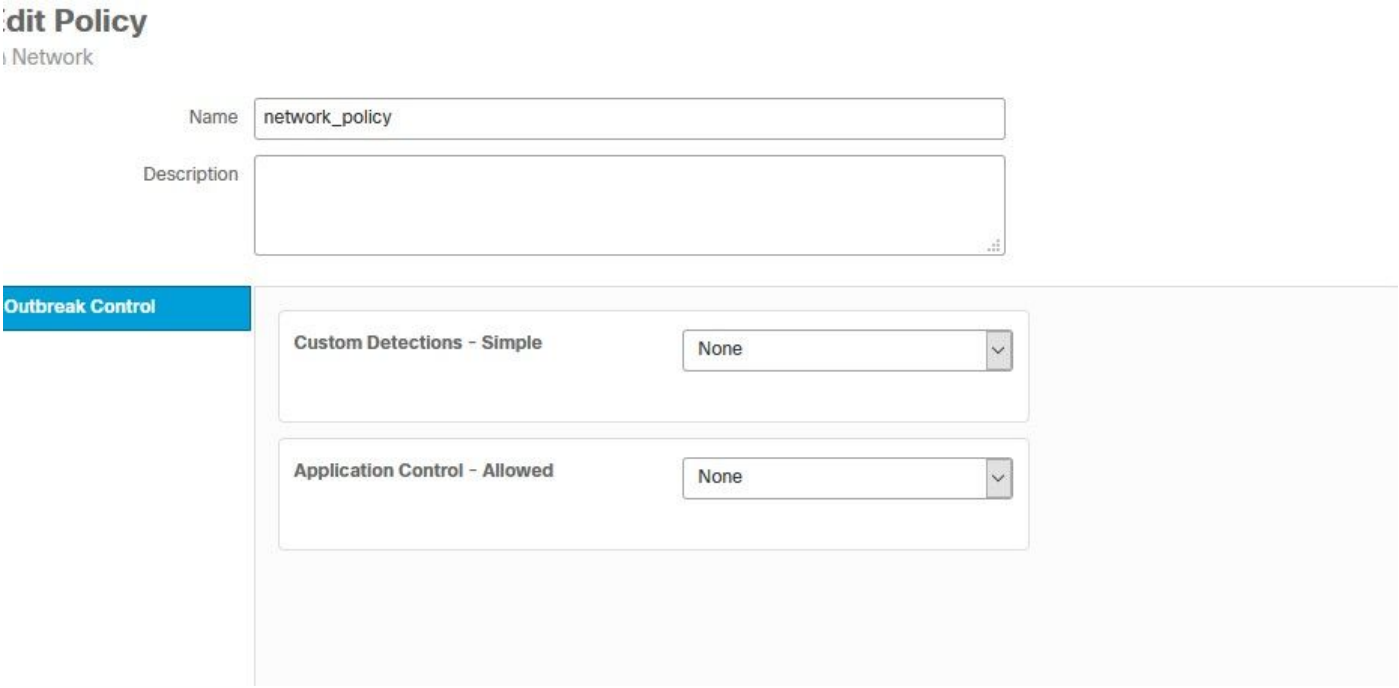


Se você tem dispositivos múltiplos WSA registrados, você pode identificá-los com a identificação de cliente da análise do arquivo.

Se você expande o dispositivo, você pode ver que grupo pertence, a política aplicada e o dispositivo GUID pode ser usado para ver a trajetória do dispositivo.

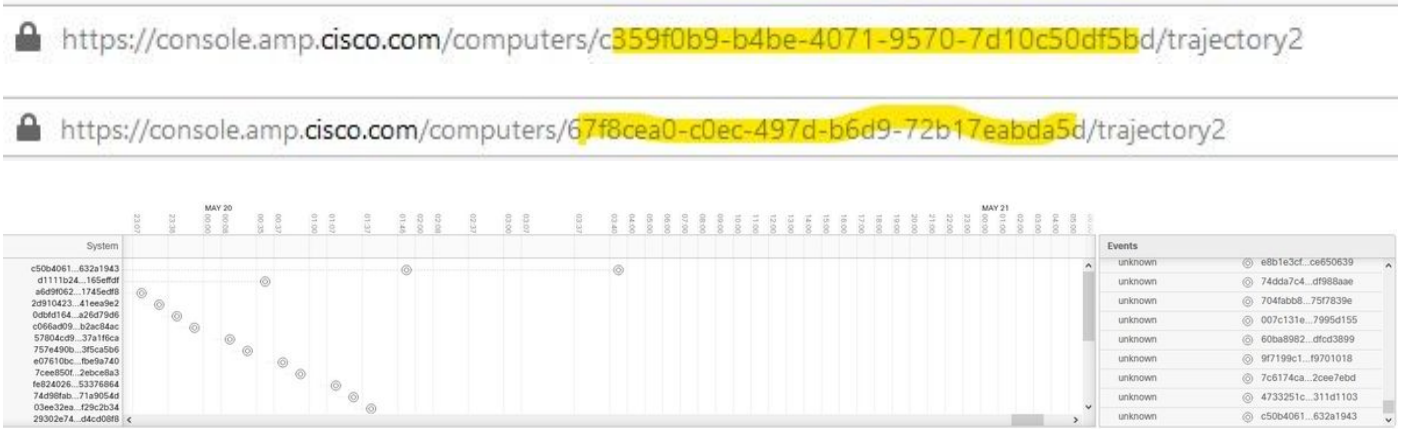


Na seção de política, você pode configurar detecções simples e o controle de aplicativo feitos sob encomenda - permitidos que é aplicado ao dispositivo.

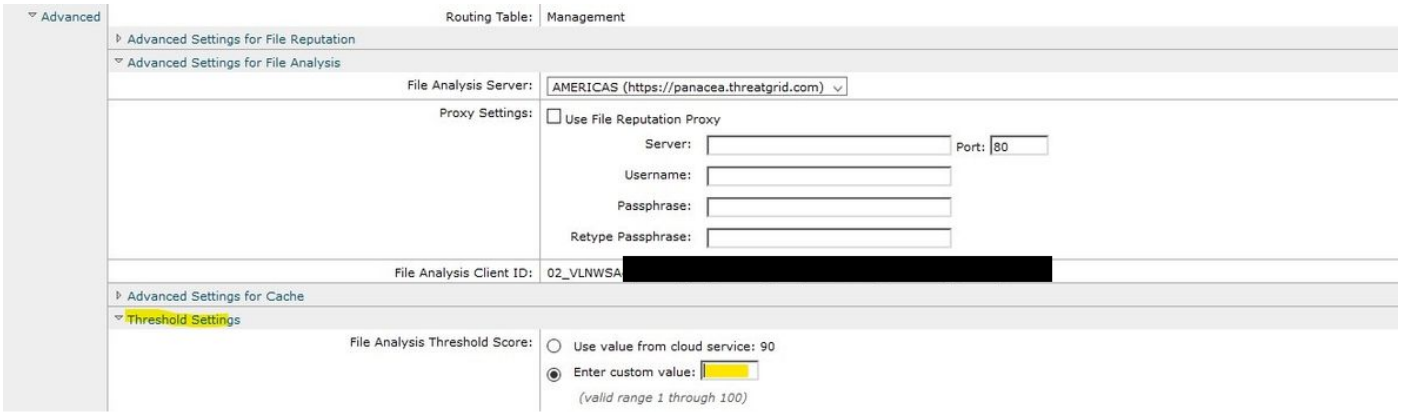


Há um truque para ver a seção da trajetória do dispositivo do WSA, você precisa de abrir a trajetória do dispositivo de um outro computador e de usar o dispositivo GUID.

A mudança é aplicada à URL, segundo as indicações das imagens.



Para a grade da ameaça, há um ponto inicial de 90, se um arquivo obtém uma contagem sob número dito, o arquivo não está malicioso picado, contudo, você pode configurar um ponto inicial feito sob encomenda no WSA.



Troubleshooting

WSA não reorienta à página AMP

- Assegure-se de que o Firewall permita os endereços exigidos para o AMP, os clique aqui.
- Assegure-se de que você selecione a nuvem apropriada AMP (evite escolher a nuvem do legado).

WSA não obstrui os SHA especificados

- Assegure-se de que seu WSA esteja no grupo correto.
- Assegure-se de que seu WSA esteja usando a política correta.
- Assegure-se de que o SHA não esteja limpo na nuvem, se não, WSA não poderia a obstruir.

WSA não aparece em minha organização TG

- Assegure-se de que você selecione a nuvem apropriada TG (Americas ou Europa).
- Assegure-se de que o Firewall permita os endereços exigidos para o TG.
- Tome a nota da identificação de cliente da análise do arquivo.
- Procure por ela sob a seção dos usuários.
- Se você não a encontra, contacte por favor o apoio de Cisco assim que podem ajudá-lo a movê-lo entre organizações.