

# 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**, nesta seção você pode encontrar as opções para integrar o AMP e o TG.

## Integração AMP

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

Anti-Malware Scanning Services	
DVS Engine Object Scanning Limits:	Max. Object Size: 32 MB
Sophos:	Enabled
McAfee:	Feature Key for McAfee has expired or is unavailable. For information on enabling this feature with a new key, contact your Cisco sales representative.
Webroot:	Enabled Threat Risk Threshold: 90

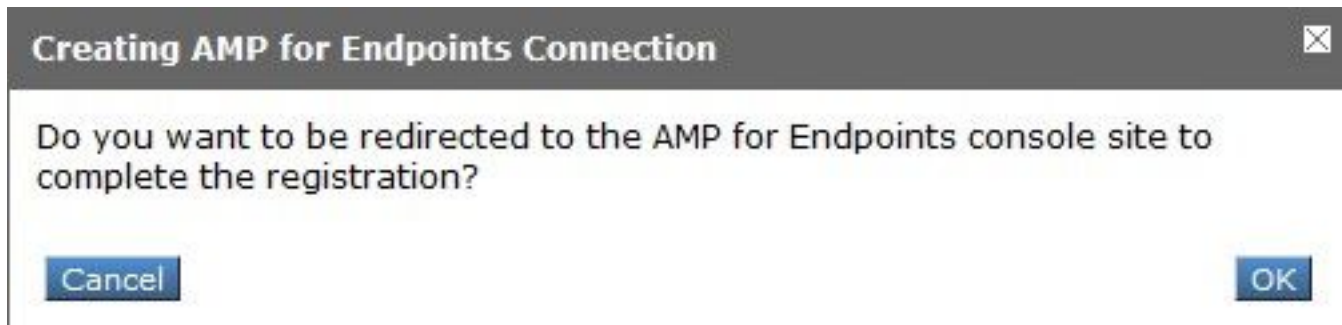
 [Edit Global Settings...](#)

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.

Advanced	Routing Table: Management
Advanced Settings for File Reputation	
File Reputation Server:	<input type="text" value="AMERICAS (cloud-sa.amp.cisco.com)"/> <ul style="list-style-type: none"> <li>AMERICAS (cloud-sa.amp.cisco.com)</li> <li>AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)</li> <li>EUROPE (cloud-sa.eu.amp.cisco.com)</li> <li>APJC (cloud-sa.apjc.amp.cisco.com)</li> <li>Private Cloud</li> </ul>
AMP for Endpoints Console Integration ?	
SSL Communication for File Reputation:	Server: <input type="text"/> Port: <input type="text" value="80"/> Username: <input type="text"/> Passphrase: <input type="text"/> Retype Passphrase: <input type="text"/> <input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy ?
Heartbeat Interval:	<input type="text" value="15"/> minutes
Query Timeout:	<input type="text" value="15"/> seconds
File Reputation Client ID:	67f8cea0-c0ec-497d-b6d9-72b17eabda5d

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.



# Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

-  AMP for Endpoints
-  Threat Grid
-  Threat Response  
and more...

[Log In](#)

[Use Single Sign-On](#)

[Can't access your account?](#)

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

## Authorize VLNWS

The VLNWS [redacted] (WSA endpoint) is requesting the following authorizations:

- Device Registration

Applications external to AMP for Endpoints, such as Cisco's Firepower Management Center, can be authorized to access your business' data.

Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.

Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.

Authorization can always be revoked at a later time from the AMP for Endpoints web console, and the application completely deregistered from the system.

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.

Advanced	Routing Table: Management
Advanced Settings for File Reputation	
File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com)
Cloud Domain:	cloud-sa.amp.cisco.com
AMP for Endpoints Console Integration ?	VLNWS [redacted] ? Deregister ✓ SUCCESS

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.

Anti-Malware Scanning Services	
DVS Engine Object Scanning Limits:	Max. Object Size: 32 MB
Sophos:	Enabled
McAfee:	Feature Key for McAfee has expired or is unavailable. For information on enabling this feature with a new key, contact your Cisco sales representative.
Webroot:	Enabled Threat Risk Threshold: 90



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.

Advanced	Routing Table: Management
Advanced Settings for File Reputation	
Advanced Settings for File Analysis	
File Analysis Server:	AMERICAS (https://panacea.threatgrid.com)
Proxy Settings:	AMERICAS (https://panacea.threatgrid.com) EUROPE (https://panacea.threatgrid.eu) Port: 80 Private Cloud
	Username: <input type="text"/> Passphrase: <input type="text"/> Retype Passphrase: <input type="text"/>
File Analysis Client ID:	02_VLNWS [redacted]
Advanced Settings for Cache	

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.

Threat Grid [Submit Sample](#) Dashboard Samples Reports Indicators Administration

Users - vrt/wsa/EC2ACF1150F19CCEF2DB-178D3EFDBAD1 [+ New User](#) [Feedback](#)

Filter

Login	Name	Email	Title	Organization	Role	Status	Integration	Type	Actions
484c72c8-5321-477c-...	WSA Device	/	/	vrt/wsa/EC2ACF1150F...	user	Active	WSA	device	...

Filter sidebar options:

- Status
  - Active
  - Inactive
- User Type
  - Device
  - Person
  - Service
- Role
  - Admin
  - Device Admin
  - Org Admin
  - User
- Integration

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

▼ Filters

Hostname

Operating System

Connector Version

Flag  All  Web Security Appliance

Fault

Fault Severity

Isolation Status

Orbital Status

Sort By

Group

Policy

Internal IP

External IP

Last Seen

Definitions Last Updated

Sort Order

[Clear Filters](#) [Apply Filters](#)

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.

VLNWSA [redacted] in group [redacted]-Group	
Hostname	VLNWSA [redacted] ... Group [redacted]-Group
Operating System	Web Security Appliance Policy [redacted].policy
Device Version	Internal IP
Install Date	External IP
Device GUID	67f8cea0-c0ec-497d-b6d9-72b17eabda5d Last Seen 2020-05-20 03:51:32 CDT

[Diagnostics](#) [View Changes](#)

[Diagnose...](#) [Move to Group...](#) [Delete](#)

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

## dit Policy

Network

Name:

Description:

---

**Outbreak Control**

Custom Detections - Simple:

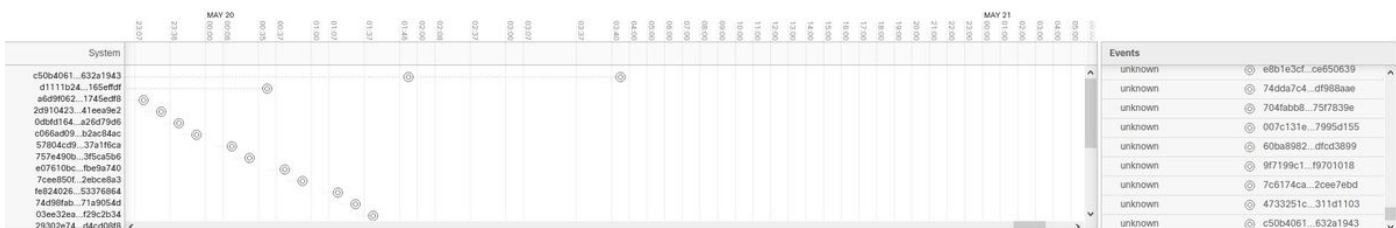
Application Control - Allowed:

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.

<https://console.amp.cisco.com/computers/c359f0b9-b4be-4071-9570-7d10c50df5bd/trajectory2>

<https://console.amp.cisco.com/computers/67f8cea0-c0ec-497d-b6d9-72b17eabda5d/trajectory2>



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.

Advanced Routing Table: Management

Advanced Settings for File Reputation

Advanced Settings for File Analysis

File Analysis Server: AMERICAS (https://panacea.threatgrid.com) ▾

Proxy Settings:

Use File Reputation Proxy

Server:  Port:

Username:

Passphrase:

Retype Passphrase:

File Analysis Client ID: 02\_VLNWSA [REDACTED]

Advanced Settings for Cache

Threshold Settings

File Analysis Threshold Score:

Use value from cloud service: 90

Enter custom value:

(valid range 1 through 100)

## 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.