

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

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Integração da AMP](#)

[Integração do Threat Grid](#)

[Verificar](#)

[Troubleshoot](#)

[O WSA não redireciona para a página AMP](#)

[O WSA não bloqueia os SHAs especificados](#)

[O WSA não aparece na minha organização TG](#)

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.

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

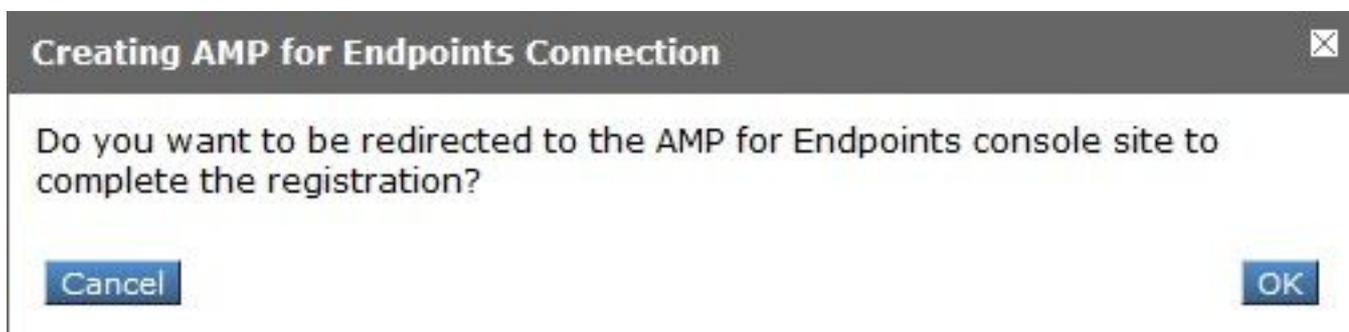
 [Edit Global Settings...](#)

Procure 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.

Advanced	Routing Table: Management
Advanced Settings for File Reputation	File Reputation Server: AMERICAS (cloud-sa.amp.cisco.com)
AMP for Endpoints Console Integration ?	AMERICAS (cloud-sa.amp.cisco.com)
SSL Communication for File Reputation:	AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
	EUROPE (cloud-sa.eu.amp.cisco.com)
	APJC (cloud-sa.apjc.amp.cisco.com)
	Private Cloud
	Server: <input type="text"/> Port: 80
	Username: <input type="text"/>
	Password: <input type="text"/>
	Retype Password: <input type="text"/>
	<input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy ?
Heartbeat Interval:	15 minutes
Query Timeout:	15 seconds
File Reputation Client ID:	67f8cea0-c0ec-497d-b6d9-72b17eabda5d

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.



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

Authorize VLNWS [REDACTED]

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

- Device Registration

Deny Allow

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.

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

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.

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

Private Cloud

Port: 80

Username: []

Passphrase: []

Retype Passphrase: []

File Analysis Client ID: 02_VLNWS [REDACTED]

Advanced Settings for Cache

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.

Threat Grid Administration

Users - vrt/wsa/EC2ACF1150F19CCEF2DB-178D3EFDBAD1

Filter

Search on Login, Name, Email, Title, CSA Registration Key

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

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

Filters

Hostname: Hostname or Connector GUID

Operating System: [Dropdown]

Connector Version: web

Flag: All Web Security Appliance

Fault: None Selected

Fault Severity: [Dropdown]

Isolation Status: None Selected

Orbital Status: None Selected

Sort By: Hostname

Group: [Dropdown]

Policy: [Dropdown]

Internal IP: Single IPv4 or CIDR

External IP: Single IPv4 or CIDR

Last Seen: Any Date

Definitions Last Updated: None Selected

Sort Order: Ascending

Clear Filters Apply Filters

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.

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 Personalizadas Simples e Controle de Aplicativos - Permitido que é aplicado ao dispositivo.

dit Policy

Network

Name:

Description:

Outbreak Control

Custom Detections - Simple:

Application Control - Allowed:

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.

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

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

The screenshot shows a trajectory graph with a list of system GUIDs on the left and a list of events on the right. The GUIDs include: c50b4061_632a1943, d1111b24_165effdf, a6d9f062_1745edf8, 2b910423_41eaa9e2, c0b8d164_2d267799, c096ad09_b2ac84ac, 57804cd9_37a18ca, 757e490b_2fca5096, e07810cc_8ed874d0, 7cee850f_2ebce8a3, f8824026_53376884, 74d508ab_719f05d3, 03ee32ea_f29c2b34, and 29302e74_d4cd08f8. The events list includes several 'unknown' entries with GUIDs like e8b1e3cf_c6850639, 74dda7c4_d988a8ae, 704fabbb_75f7839e, 007c131e_7995d155, 60ba8982_dfcc3899, 9f7199c1_f9701018, 7c6174ca_2cee7ebd, 4733251c_311d1103, and c50b4061_632a1943.

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.

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)

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.