

Integre AMP para terminales y Threat Grid con WSA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[integración de AMP](#)

[Integración de Threat Grid](#)

[Verificación](#)

[Troubleshoot](#)

[WSA no redirige a la página de AMP](#)

[WSA no bloquea los SHA especificados](#)

[WSA no aparece en mi organización TG](#)

Introducción

Este documento describe los pasos para integrar la protección frente a malware avanzado (AMP) para terminales y Threat Grid (TG) con Web Security Appliance (WSA).

Colaborado por Uriel Montero y editado por Yeraldin Sanchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- AMP para acceso de terminales
- acceso TG premium
- WSA con claves de característica de análisis de archivos y reputación de archivos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Consola de nube pública AMP
- GUI de WSA
- Consola 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Inicie sesión en la consola WSA.



Una vez que haya iniciado sesión, navegue hasta **Servicios de seguridad > Anti-Malware y reputación**, en esta sección encontrará las opciones para integrar AMP y TG.

integración de AMP

En la sección Anti-Malware Scanning Services, haga clic en **Edit Global Settings**, como se muestra en la imagen.

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

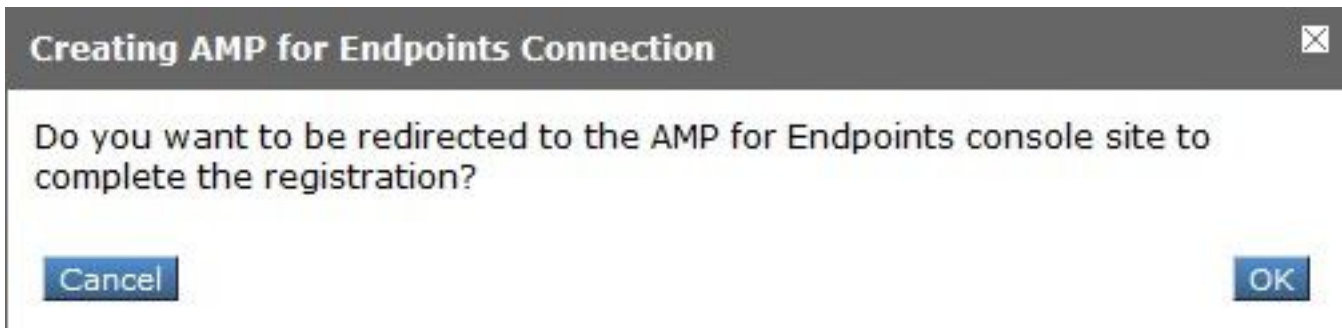
 [Edit Global Settings...](#)

Busque la sección **Advanced > Advanced Settings for File Reputation** y amplíela. A continuación, se muestra una serie de opciones de servidores en la nube y elija la más cercana a su ubicación.

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

Una vez seleccionada la nube, haga clic en el botón **Registrar dispositivo con AMP para terminales**.

Aparece una ventana emergente que se redirige a la consola de AMP y hace clic en el botón **Aceptar**, como se muestra en la imagen.



Debe ingresar credenciales de AMP válidas y hacer clic en **Iniciar sesión**, como se muestra en la imagen.



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?](#)

Acepte el Registro de dispositivos, tenga en cuenta la ID de cliente, ya que ayuda a encontrar el WSA más adelante en la consola.

Authorize VLNWS

The VLNWS (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.

Vuelva a la consola WSA, aparece una comprobación en la sección Integración de la consola de Amp para terminales, como se muestra en la imagen.


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 ?	VLNWSA [redacted] ? Deregister SUCCESS

Nota: No olvide hacer clic en **Enviar** y **Registrar** los cambios (si se le solicita); de lo contrario, el proceso debe realizarse de nuevo.

Integración de Threat Grid

Navigate hasta **Servicios de seguridad > Anti-Malware y Reputación**, luego en los Servicios de protección anti-malware, haga clic en el **botón Edit Global Settings**, como se muestra en la imagen.

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



Busque la sección **Avanzada > Configuración avanzada para el análisis de archivos** y expanda, elija la opción más cercana a su ubicación, como se muestra en la imagen.

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	

Haga clic en **Enviar** y **Registrar** los cambios.

En el lado del portal TG, busque el dispositivo WSA en la ficha Users (Usuarios) si el dispositivo se integró correctamente con AMP/TG.

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	...

Si hace clic en Inicio de sesión, puede acceder a la información de dicho dispositivo.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Para verificar que la integración entre AMP y WSA es correcta, puede iniciar sesión en la consola de AMP y buscar su dispositivo WSA.

Vaya a **Administración > Equipos**, en la sección Filtros, busque **Web Security Appliance** y aplique el 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

Si tiene varios dispositivos WSA registrados, puede identificarlos con la ID de cliente de análisis de archivos.

Si expande el dispositivo, puede ver a qué grupo pertenece, la política aplicada y el GUID del dispositivo se pueden utilizar para ver la trayectoria del 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	Last Seen 2020-05-20 03:51:32 CDT

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

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

En la sección de políticas, puede configurar Detecciones simples personalizadas y Control de aplicaciones: permitido que se aplica al dispositivo.

dit Policy

Network

Name:

Description:

Outbreak Control

Custom Detections - Simple:

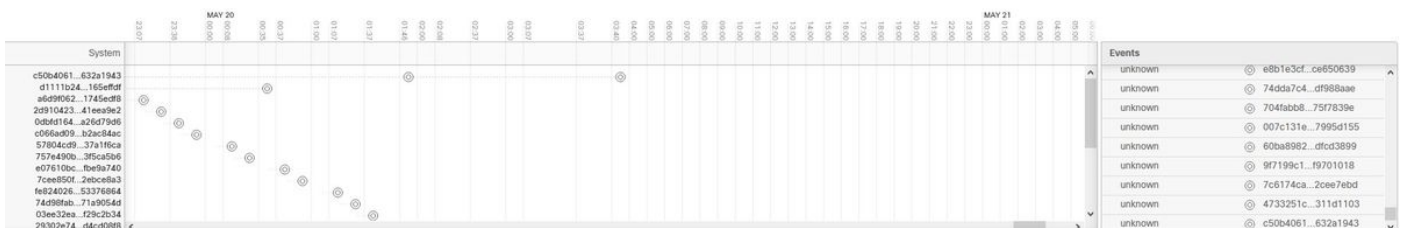
Application Control - Allowed:

Hay un truco para ver la sección Trayectoria del dispositivo de WSA, debe abrir la trayectoria del dispositivo de otro equipo y utilizar el GUID del dispositivo.

El cambio se aplica a la URL, como se muestra en las imágenes.

<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 Threat Grid, hay un umbral de 90; si un archivo obtiene una puntuación en dicho número, el archivo no se muestra malicioso; sin embargo, puede configurar un umbral personalizado en el 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

WSA no dirige a la página de AMP

- Asegúrese de que el firewall permita las direcciones necesarias para AMP, haga clic [aquí](#).
- Asegúrese de que ha seleccionado la nube de AMP adecuada (evite elegir la nube antigua).

WSA no bloquea los SHA especificados

- Asegúrese de que el WSA se encuentra en el grupo correcto.
- Asegúrese de que WSA utiliza la política correcta.
- Asegúrese de que el SHA no esté limpio en la nube; de lo contrario, WSA no podría bloquearlo.

WSA no aparece en mi organización TG

- Asegúrese de que ha seleccionado la nube TG adecuada (América o Europa).
- Asegúrese de que el firewall permite las direcciones necesarias para TG.
- Tome nota de la ID del cliente de análisis de archivos.
- Busque en la sección Usuarios.
- Si no lo encuentra, póngase en contacto con el servicio de asistencia de Cisco para que le ayuden a trasladarlo de una organización a otra.