

# Integrate AMP for Endpoints and Threat Grid with WSA

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[AMP integration](#)

[Threat Grid integration](#)

[Verify](#)

[Troubleshoot](#)

[WSA does not redirect to AMP page](#)

[WSA does not block the specified SHAs](#)

[WSA does not appear on my TG Organization](#)

## Introduction

This document describes the steps to integrate Advanced Malware Protection (AMP) for endpoints and Threat Grid (TG) with Web Security Appliance (WSA).

Contributed by Uriel Montero and Edited by Yeraldin Sanchez, Cisco TAC Engineers.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- AMP for endpoints access
- TG premium access
- WSA with File Analysis and File Reputation Feature Keys

### Components Used

The information in this document is based on these software and hardware versions:

- AMP Public cloud console
- WSA GUI
- TG Console

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. If your network is

live, ensure that you understand the potential impact of any command.

## Configure

Log in to the WSA console.



Once logged in, navigate to **Security Services > Anti-Malware and Reputation**, in this section you can find the options to integrate AMP and TG.

### AMP integration

On the Anti-Malware Scanning Services section, click on **Edit Global Settings**, as shown in the image.

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

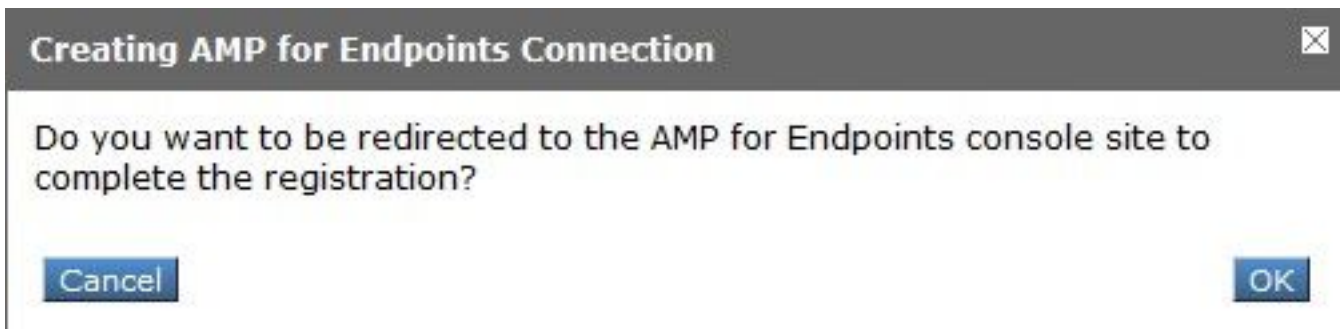
 [Edit Global Settings...](#)

Search for the **Advanced > Advanced Settings for File Reputation** section and expand it, then a series of Cloud servers options are displayed, choose the closest to your location.

Advanced	Routing Table:	Management
Advanced Settings for File Reputation		
File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com) [v] AMERICAS (cloud-sa.amp.cisco.com) AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com) EUROPE (cloud-sa.eu.amp.cisco.com) APJC (cloud-sa.apjc.amp.cisco.com) Private Cloud	
AMP for Endpoints Console Integration ?		
SSL Communication for File Reputation:	Server: [ ] Port: [80] Username: [ ] Passphrase: [ ] Retype Passphrase: [ ] <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	

Once the Cloud was selected, click on **Register Appliance with AMP for Endpoints** button.

A pop up appears that redirects to the AMP console, click the **Ok button**, as shown in the image.



You need to ingress valid AMP Credentials and click on **Log in**, as shown in the image.



# 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?](#)

Accept the Device Registration, take note of the Client ID, as it helps to find the WSA later on the console.

## 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.

Go back to the WSA console, a check appears on the Amp for Endpoints Console Integration section, as shown in the image.


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 ? Deregister ✓ SUCCESS

**Note:** Don't forget to click on **Submit** and **Commit** the changes (if prompted), otherwise, the process needs to be done again.

## Threat Grid integration

Navigate to **Security Services > Anti-Malware and Reputation**, then on the Anti-Malware Protection Services, click on the **Edit Global Settings** button, as shown in the image.

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



Search for the **Advanced > Advanced Settings for File Analysis** section and expand it, choose the closest option to your location, as shown in the image.

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: <input type="text"/>
	Passphrase: <input type="text"/>
	Retype Passphrase: <input type="text"/>
File Analysis Client ID:	02_VLNWS
Advanced Settings for Cache	

Click on **Submit** and **Commit** the changes.

On the TG portal side, search for the WSA device under the Users tab if the appliance was successfully integrated with AMP/TG.

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

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:

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

If you click on Login, you can access the information of said Appliance.

## Verify

Use this section to confirm that your configuration works properly.

In order to verify that the integration between AMP and WSA is successful, you can log in to the AMP console and search for your WSA device.

Navigate to **Management > Computers**, on the filters section, search for **Web Security Appliance** and apply the filter

▼ 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](#)

If you have multiple WSA devices registered, you can identify them with the File analysis client ID.

If you expand the device, you can see which group it belongs to, the Policy applied and the Device GUID can be used to view the Device Trajectory.

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](#)

In the policy section, you can configure Simple Custom Detections and Application Control - Allowed that is applied to the device.

## Edit Policy

Network

Name

Description

**Outbreak Control**

Custom Detections - Simple

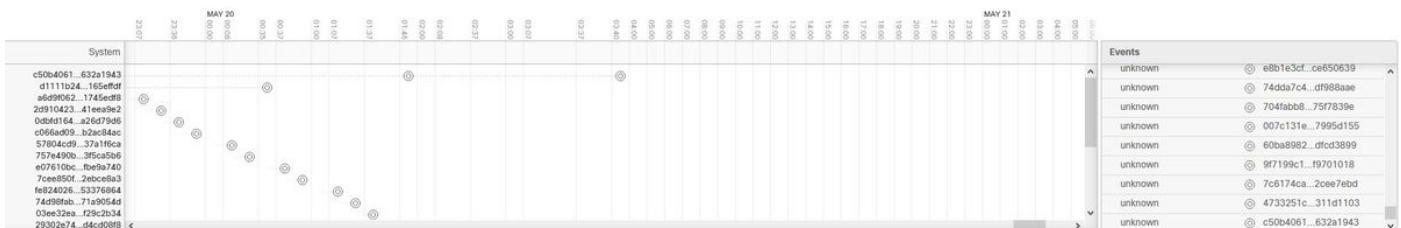
Application Control - Allowed

There is a trick to view the Device Trajectory section of the WSA, you need to open the Device Trajectory of another computer and use the Device GUID.

The change is applied to the URL, as shown in the images.

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

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



For Threat Grid, there is a threshold of 90, if a file gets a score under said number, the file is not poked malicious, however, you can configure a custom Threshold on the 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 does not redirect to AMP page

- Ensure the Firewall allows the required addresses for AMP, click [here](#).
- Ensure you have selected the proper AMP cloud (avoid choosing Legacy cloud).

### WSA does not block the specified SHAs

- Ensure your WSA is in the correct Group.
- Ensure your WSA is using the correct Policy.
- Ensure the SHA is not clean on the cloud, otherwise, WSA would not be able to block it.

### WSA does not appear on my TG Organization

- Ensure you selected the proper TG cloud (Americas or Europe).
- Ensure the Firewall allows the required addresses for TG.
- Take note of the File Analysis Client ID.
- Search for it under Users section.
- If you don't find it, please contact Cisco Support so they can help you move it between organizations.