

Advanced Malware Protection voor endpoints en Threat Grid met WSA

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[AMP-integratie](#)

[Threat Grid-integratie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[WSA wijst niet terug naar AMP-pagina](#)

[WSA blokkeert niet de gespecificeerde SHAs](#)

[WSA verschijnt niet op mijn TG Organisatie](#)

Inleiding

In dit document worden de stappen beschreven om Advanced Malware Protection (AMP) voor endpoints en Threat Grid (TG) te integreren met Web Security Appliance (WSA).

Bijgedragen door Uriel Montero en bewerkt door Yeraldin Sanchez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Advanced Malware Protection voor endpoints
- TG-premietoegang
- WSA met functiekaarten voor bestandsanalyse en bestanduploaden

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- AMP openbare cloudconsole
- WSA GUI
- TG-console

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren


Meld u aan bij de WSA-console.



Nadat u hebt aangemeld, navigeer u naar **Security Services > Anti-Malware en Reputation**. In deze sectie vindt u de opties om AMP en TG te integreren.

AMP-integratie

Klik in het gedeelte Anti-Malware scans op **Global Settings**, zoals in de afbeelding, om de **Global Settings** te bewerken.

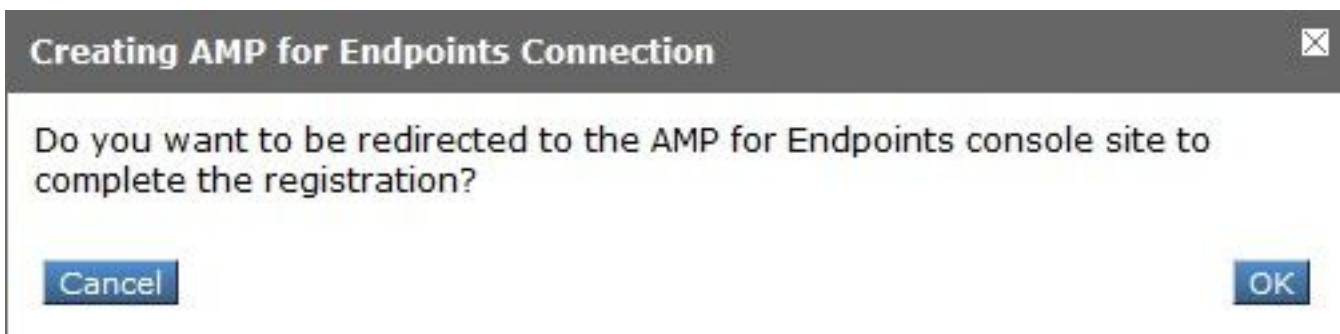
Anti-Malware Scanning Services	
DVS Engine Object Scanning Limits:	Max. Object Size: 32 MB
Sophos:	Enabled
McAfee:	<i>Feature Key for McAfee has expired or is unavailable. For information on enabling this feature with a new key, contact your Cisco sales representative.</i>
Webroot:	Enabled Threat Risk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

Zoeken naar het gedeelte **Geavanceerde instellingen voor bestandupdatie** en uitvouwen, dan wordt een serie Cloud-serveropties weergegeven en kies de dichtstbijzijnde optie van uw locatie.

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: Port: 80
	Username:
	Password:
	Retype Password:
	<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

Klik op de knop **Registreren** van **applicatie met AMP voor endpoints**.

Er verschijnt een pop-up-pop die wordt omgeleid naar de AMP-console, op de **OK-knop** zoals in de afbeelding wordt weergegeven.



U moet geldige AMP Credentials invoeren en op **Log in**, zoals in de afbeelding weergegeven.



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?](#)

Accepteer de apparaatregistratie, neem nota van de client-ID omdat deze de WSA later op de console helpt vinden.

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.

Terug naar de WSA console, verschijnt een controle op de Amp voor de sectie van de Integratie van Endpoints, zoals in de afbeelding getoond.


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 ? Deregister ✓ SUCCESS	

Opmerking: vergeet niet op **Verzenden** te klikken en de wijzigingen **aan te binden** (indien dit wordt gevraagd). Anders moet het proces opnieuw uitgevoerd worden.

Threat Grid-integratie

Navigeer naar **Security Services > Anti-Malware en Reputation**, dan klik op de anti-Malware Protection Services op de knop **Global Settings**, zoals in de afbeelding wordt getoond.

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...](#)

Zoeken naar het gedeelte **Geavanceerde instellingen voor bestandsanalyse** en uitvouwen, kies de dichtstbijzijnde optie voor uw locatie, zoals in de afbeelding.

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	

Klik op **Inzenden** en de wijzigingen **Commit**.

Aan de kant van het TG-portaal kunt u het WSA-apparaat zoeken onder het tabblad Gebruikers als het apparaat met succes is geïntegreerd met 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

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

Als u op Aanmelden klikt, kunt u de informatie over dit apparaat benaderen.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Om te verifiëren dat de integratie tussen AMP en WSA succesvol is, kunt u aan de console van AMP en aan onderzoek naar uw apparaat van WSA inloggen.

Navigeren in op **Beheer > Computers**, in het gedeelte Filters, op **Web security applicatie** en pas het filter toe

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

Als u meerdere WSA-apparaten hebt geregistreerd, kunt u deze identificeren met de client-ID voor bestandsanalyse.

Als u het apparaat uitvouwt, kunt u zien tot welke groep het behoort, het toegepaste Beleid en het Dienstmiddel kan worden gebruikt om het traject van het apparaat te bekijken.

▼ **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 het beleidsgedeelte kunt u Eenvoudige Aangepaste Detecties en Toepassingscontrole configureren - toegestaan dat op het apparaat wordt toegepast.

edit Policy

Network

Name:

Description:

Outbreak Control

Custom Detections - Simple:

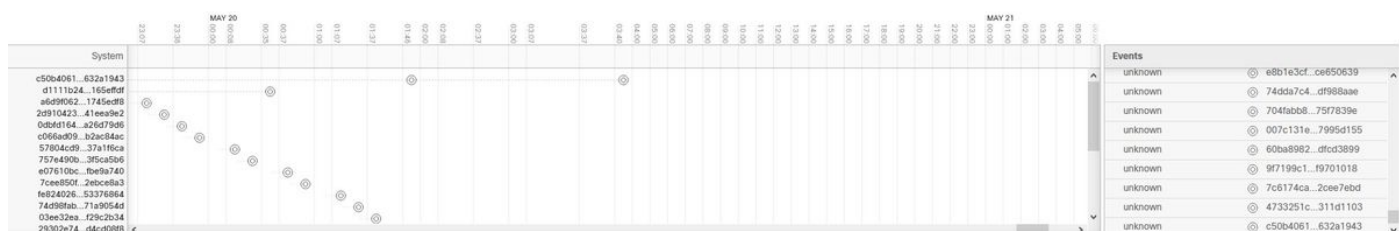
Application Control - Allowed:

Er is een truc om het gedeelte van het WSA van de Transmissie van het Apparaat te bekijken, moet u het Transformer van een andere computer openen en het apparaat GUI gebruiken.

De verandering wordt toegepast op de URL, zoals in de afbeeldingen wordt getoond.

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

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



Voor Threat Grid is er een drempelwaarde van 90, als een bestand een score krijgt onder dat nummer, wordt het bestand niet kwaadwillig gepikt, maar u kunt een aangepaste drempel op de WSA configureren.

Advanced Routing Table: Management

Advanced Settings for File Reputation

Advanced Settings for File Analysis

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

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)

Problemen oplossen

WSA wijst niet terug naar AMP-pagina

- Zorg ervoor dat de firewall de vereiste adressen voor AMP toestaat, klik [hier](#).
- Zorg ervoor dat u de juiste AMP-cloud hebt geselecteerd (vermijd het kiezen van een verouderde cloud).

WSA blokkeert niet de gespecificeerde SHAs

- Zorg ervoor dat uw WSA in de juiste Groep is.
- Zorg ervoor dat uw WSA het juiste beleid gebruikt.
- Zorg ervoor dat de SHA niet op de cloud is schoon, anders zou WSA niet in staat zijn deze te blokkeren.

WSA verschijnt niet op mijn TG Organisatie

- Zorg ervoor dat u de juiste TG-wolk (Amerika of Europa) hebt geselecteerd.
- Zorg ervoor dat de firewall de vereiste adressen voor TG toestaat.
- Let op de client-ID voor bestandsanalyse.
- Zoeken onder het kopje Gebruikers.
- Als u deze niet vindt, neemt u contact op met Cisco-ondersteuning zodat u deze tussen organisaties kunt verplaatsen.