

# Integrazione di AMP for Endpoints and Threat Grid con WSA

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Integrazione AMP](#)

[Integrazione Threat Grid](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[WSA non reindirizza alla pagina AMP](#)

[WSA non blocca gli Agenti integrità sistema specificati](#)

[WSA non viene visualizzato nell'organizzazione TG](#)

## Introduzione

In questo documento viene descritta la procedura per integrare Advanced Malware Protection (AMP) per gli endpoint e Threat Grid (TG) con Web Security Appliance (WSA).

Contributo di Uriel Montero e modificato da Yeraldin Sanchez, Cisco TAC Engineers.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AMP for endpoints access
- TG premium access
- WSA con analisi dei file e chiavi delle funzionalità di reputazione dei file

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Console cloud pubblica AMP
- GUI WSA
- Console TG

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

Accedere alla console WSA.



Una volta eseguito l'accesso, selezionare **Security Services > Anti-Malware and Reputation** (Servizi di sicurezza > Antimalware e reputazione). In questa sezione sono disponibili le opzioni per l'integrazione di AMP e TG.

### Integrazione AMP

Nella sezione Servizi di scansione antimalware fare clic su **Modifica impostazioni globali**, come mostrato nell'immagine.

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...](#)

Cercare la sezione **Avanzate > Impostazioni avanzate per la reputazione del file** ed espanderla, quindi vengono visualizzate una serie di opzioni di server cloud, scegliere la posizione più vicina.

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

Una volta selezionato il cloud, fare clic sul pulsante **Register Appliance with AMP for Endpoints**.

Viene visualizzata una schermata di popup che reindirizza alla console AMP, fare clic sul pulsante **OK**, come mostrato nell'immagine.

### Creating AMP for Endpoints Connection

Do you want to be redirected to the AMP for Endpoints console site to complete the registration?

È necessario immettere le credenziali AMP valide e fare clic su **Log In**, come mostrato nell'immagine.



# 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?](#)

Accettare Device Registration (Registrazione dispositivo), prendere nota dell'ID client, in quanto aiuta a trovare il WSA più avanti sulla 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.

Tornando alla console WSA, viene visualizzato un segno di spunta nella sezione Integrazione console Amp for Endpoints, come mostrato nell'immagine.

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:** non dimenticare di fare clic su **Invia** e **Conferma** le modifiche (se richiesto), altrimenti il processo deve essere eseguito nuovamente.

## Integrazione Threat Grid

Selezionare **Security Services > Anti-Malware and Reputation** (Servizi di sicurezza > Antimalware e reputazione), quindi in Anti-Malware Protection Services (Servizi di protezione antimalware), fare clic sul pulsante **Edit Global Settings** (Modifica impostazioni globali), come mostrato nell'immagine.

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



Cercare la sezione **Advanced > Advanced Settings for File Analysis** ed espanderla, scegliere l'opzione più vicina alla propria posizione, come mostrato nell'immagine.

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	

Fare clic su **Submit** (Invia) e **Commit** delle modifiche.

Sul portale TG, cercare il dispositivo WSA nella scheda Utenti se l'accessorio è stato integrato con AMP/TG.

Se si fa clic su Login, è possibile accedere alle informazioni di tale accessorio.

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Per verificare che l'integrazione tra AMP e WSA abbia esito positivo, è possibile accedere alla console AMP e cercare il dispositivo WSA.

Passare a **Gestione > Computer**, nella sezione filtri cercare **Web Security Appliance** e applicare il filtro

Se sono stati registrati più dispositivi WSA, è possibile identificarli con l'ID del client di analisi dei file.

Se si espande la periferica, è possibile vedere a quale gruppo appartiene, il criterio applicato e il GUID della periferica possono essere utilizzati per visualizzare la traiettoria della periferica.

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](#)

Nella sezione dei criteri è possibile configurare Rilevamenti personalizzati semplici e Controllo applicazione - Consentito che viene applicato al dispositivo.

## edit Policy

Network

Name

Description

### Outbreak Control

Custom Detections - Simple

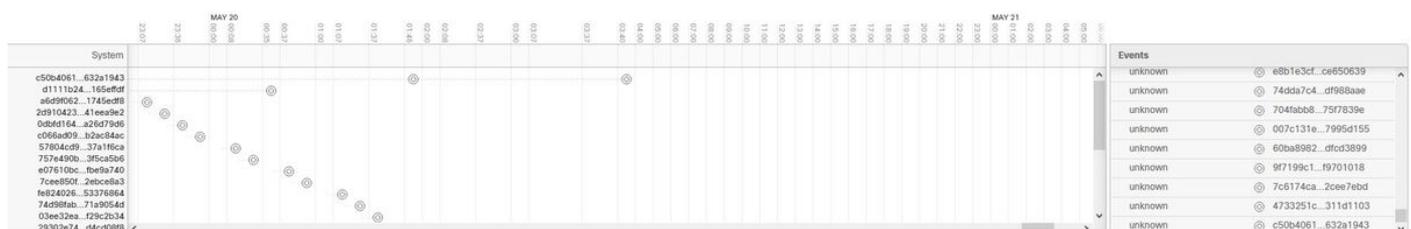
Application Control - Allowed

Per visualizzare la sezione Traiettorie periferica di WSA, è necessario aprire la sezione Traiettorie periferica di un altro computer e utilizzare il GUID della periferica.

La modifica viene applicata all'URL, come mostrato nelle immagini.

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

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



Per Threat Grid, è prevista una soglia di 90; se un file ottiene un punteggio inferiore a tale numero, il file non è dannoso, tuttavia, è possibile configurare una soglia personalizzata sul 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)

## Risoluzione dei problemi

### WSA non reindirizza alla pagina AMP

- Verificare che il firewall consenta gli indirizzi richiesti per AMP, fare clic [qui](#).
- Accertarsi di aver selezionato il cloud AMP appropriato (evitare di scegliere il cloud legacy).

### WSA non blocca gli Agenti integrità sistema specificati

- Verificare che il server WSA si trovi nel gruppo corretto.
- Assicurarsi che il WSA utilizzi i criteri corretti.
- Assicurarsi che l'Agente integrità sistema non sia pulito nel cloud, altrimenti WSA non sarà in grado di bloccarlo.

### WSA non viene visualizzato nell'organizzazione TG

- Accertarsi di aver selezionato il cloud TG appropriato (Americhe o Europa).
- Assicurarsi che il firewall consenta gli indirizzi richiesti per TG.
- Prendere nota dell'ID del client di analisi file.
- Cercarlo nella sezione Utenti.
- Se non lo trovi, contatta il supporto Cisco in modo che possa aiutarti a spostarlo tra le organizzazioni.