

將面向終端的AMP和Threat Grid與WSA整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[AMP整合](#)

[Threat Grid整合](#)

[驗證](#)

[疑難排解](#)

[WSA不會重定向到AMP頁面](#)

[WSA不會阻止指定的SHA](#)

[WSA不會出現在我的TG組織上](#)

簡介

本檔案介紹將適用於終端和威脅網格(TG)的高級惡意軟體防護(AMP)與網路安全裝置(WSA)相整合的步驟。

作者：Uriel Montero，編輯者：Yeraldin Sanchez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- AMP端點訪問
- TG高級訪問
- 具有檔案分析和檔案信譽功能金鑰的WSA

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AMP公共雲控制檯
- WSA GUI
- TG主控台

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

登入到WSA控制檯。




登入後，請導航至**安全服務>防惡意軟體和信譽**，在此部分中，您可以找到用於整合AMP和TG的選項。

AMP整合

在「Anti-Malware Scanning Services」部分，按一下**Edit Global Settings**，如下圖所示。

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

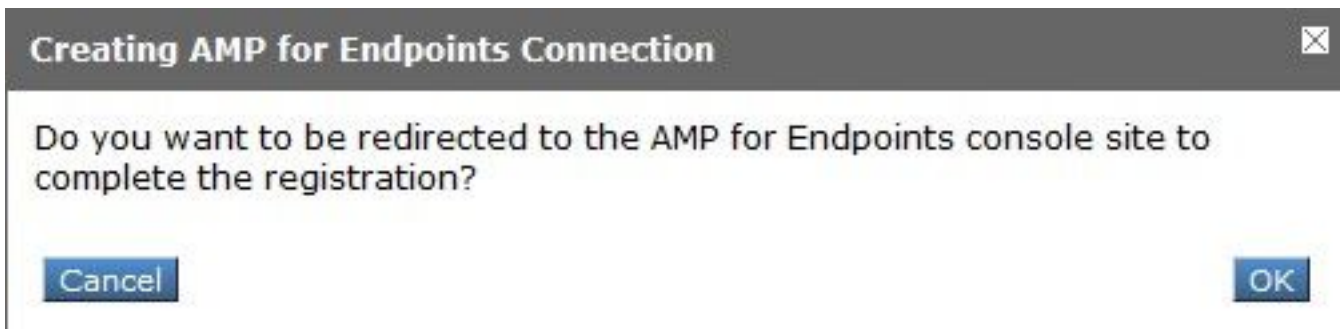
 [Edit Global Settings...](#)

搜尋**Advanced > Advanced Settings for File Reputation**部分並展開它，然後顯示一系列雲伺服器選項，選擇最接近您的位置。

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	

選擇雲後，按一下向面向終端的AMP註冊裝置按鈕。

系統將顯示一個彈出視窗，重定向到AMP控制檯，按一下OK按鈕，如下圖所示。



您需要輸入有效的AMP憑據並按一下Log in，如下圖所示。



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?](#)

接受裝置註冊，注意客戶端ID，因為它有助於以後在控制檯上查詢WSA。

Authorize VLNWS

The VLNWS [redacted] (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.


返回WSA控制檯，檢查內容將出現在Amp for Endpoints控制檯整合部分，如下圖所示。

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	

註：不要忘記點選Submit和Commit更改（如果出現提示），否則需要再次完成該過程。

Threat Grid整合

導覽至Security Services > Anti-Malware and Reputation，然後在Anti-Malware Protection Services上按一下Edit Global Settings 按鈕，如下圖所示。

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
 <input type="button" value="Edit Global Settings..."/>	

搜尋「Advanced> Advanced Settings for File Analysis」部分並展開它，選擇最靠近您所在位置的選項，如下圖所示。

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	

按一下「Submit」和「Commit」變更內容。

在TG門戶端，如果裝置成功與AMP/TG整合，請在Users（使用者）頁籤下搜尋WSA裝置。

The screenshot shows the Cisco Threat Grid interface. At the top, there's a navigation bar with 'Threat Grid', 'Submit Sample', and various menu items like 'Dashboard', 'Samples', 'Reports', 'Indicators', and 'Administration'. The main header displays 'Users - vrt/wsa/EC2ACF1150F19CCEF2DB-178D3EFDBAD1'. Below this is a search bar and a table of users. The table has columns for Login, Name, Email, Title, Organization, Role, Status, Integration, Type, and Actions. One user is listed with Login '484c72c8-5321-477c-...', Name 'WSA Device', and Type 'device'. On the left, a 'Filter' sidebar is open, showing options for Status (Active, Inactive), User Type (Device, Person, Service), Role (Admin, Device Admin, Org Admin, User), and Integration.

如果按一下Login (登入) ，則可以訪問所述裝置的資訊。

驗證

使用本節內容，確認您的組態是否正常運作。

為了驗證AMP和WSA之間的整合是否成功，您可以登入到AMP控制檯並搜尋WSA裝置。

導航到**管理>電腦**，在過濾器部分上搜尋**Web安全裝置**並應用過濾器

The screenshot shows the 'Filters' section of the Cisco Threat Grid interface. It contains various filter fields: Hostname (text input), Operating System (dropdown), Connector Version (text input with 'web' entered), Flag (checkboxes for 'All' and 'Web Security Appliance'), Fault (dropdown), Fault Severity (dropdown), Isolation Status (dropdown), Orbital Status (dropdown), Sort By (dropdown), Group (dropdown), Policy (dropdown), Internal IP (text input), External IP (text input), Last Seen (dropdown), Definitions Last Updated (dropdown), and Sort Order (dropdown). At the bottom, there are 'Clear Filters' and 'Apply Filters' buttons.

如果註冊了多個WSA裝置，則可以使用檔案分析客戶端ID來識別它們。

如果展開裝置，您可以看到它屬於哪個組、應用的策略和裝置GUID可用於檢視裝置軌跡。

Hostname	VLNWSA-██████████	Group	██████████-Group
Operating System	Web Security Appliance	Policy	██████████_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](#)

在策略部分，可以配置應用到裝置的簡單自定義檢測和應用控制 — 允許。

Edit Policy

Network

Name:

Description:

Outbreak Control

Custom Detections - Simple:

Application Control - Allowed:

檢視WSA的「裝置軌跡」部分很有用，您需要開啟另一台電腦的裝置軌跡並使用裝置GUID。

更改將應用於URL，如圖所示。

<https://console.amp.cisco.com/computers/c359f0b9-b4be-4071-9570-7d10c50df55d/trajectory2>

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

System	Events
c50b4061...632a1943	unknown @ e8b1e3cf...c6e50639
01111024...165e6af	unknown @ 74d5a7c4...df988aae
a6d9062...1745e98	unknown @ 704fab08...75f7839e
20910423...41ee9e2	unknown @ 007c131e...7995d155
0d9d164...a26d7996	unknown @ 60ba8982...dfcd3899
c956a89...32c284c	unknown @ 9f7199c1...f9701018
57804cd9...37a1f6ca	unknown @ 7c6174ca...2cee7ebd
757e490b...3f5ca506	unknown @ 4733251c...311d1103
407610dc...9e9b740	unknown @ c50b4061...632a1943
7cee850f...2ebce8a3	
fe824026...53376864	
74d98fab...71a9054d	
03ae32ea...f29c2b34	
29302e74...d4cd0988	

對於Threat Grid，有一個閾值90，如果檔案在該數值下獲得分數，則該檔案不會受到惡意攻擊，但是您可以在WSA上配置自定義閾值。

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)

疑難排解

WSA不會重定向到AMP頁面

- 確保防火牆允許AMP所需的地址，按一下 [此處](#)。
- 確保您已選擇正確的AMP雲（避免選擇傳統雲）。

WSA不會阻止指定的SHA

- 確保您的WSA位於正確的組中。
- 確保您的WSA使用正確的策略。
- 確保SHA在雲上不是乾淨的，否則WSA將無法阻止它。

WSA不會出現在我的TG組織上

- 確保您選擇了正確的TG雲（美洲或歐洲）。
- 確保防火牆允許TG所需的地址。
- 注意File Analysis Client ID。
- 在「使用者」部分下搜尋它。
- 如果您沒有找到它，請聯絡思科支援人員，以便他們能夠幫助您在組織之間移動它。