

将面向终端的AMP和Threat Grid与WSA集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[AMP集成](#)

[Threat Grid集成](#)

[验证](#)

[故障排除](#)

[WSA不重定向到AMP页面](#)

[WSA不阻止指定的SHA](#)

[WSA不出现在我的TG组织中](#)

简介

本文档介绍将面向终端的高级恶意软件防护(AMP)和Threat Grid(TG)与网络安全设备(WSA)集成的步骤。

作者：Uriel Montero，编辑者：Yeraldin Sanchez，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 面向终端的AMP访问
- TG高级访问
- 具有文件分析和文件信誉功能密钥的WSA

使用的组件

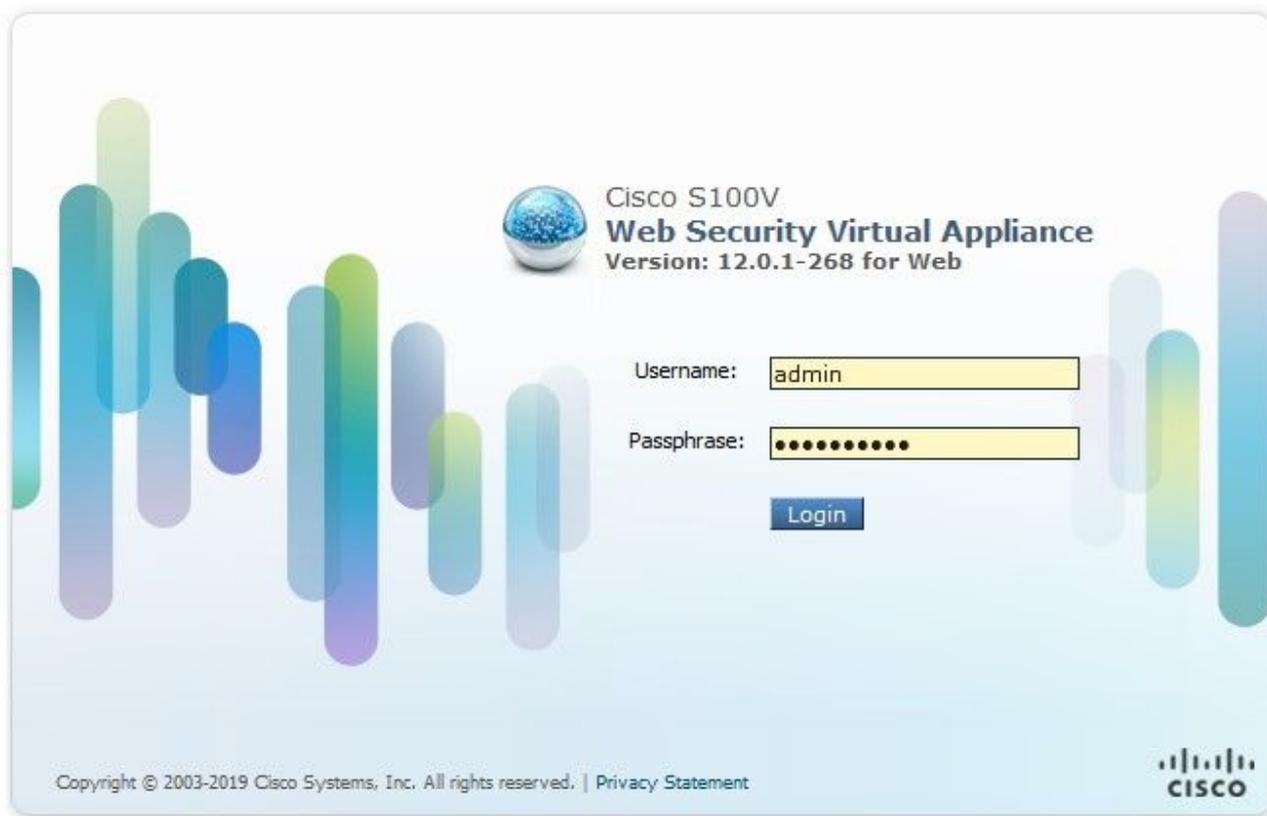
本文档中的信息基于以下软件和硬件版本：

- AMP公共云控制台
- WSA GUI
- TG控制台

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

登录到WSA控制台。



登录后，导航至**安全服务>防恶意软件和信誉**，在此部分中，您可以找到集成AMP和TG的选项。

AMP集成

在防恶意软件扫描服务(Anti-Malware Scanning Services)部分，单击**编辑全局设置(Edit Global Settings)**，如图所示。

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

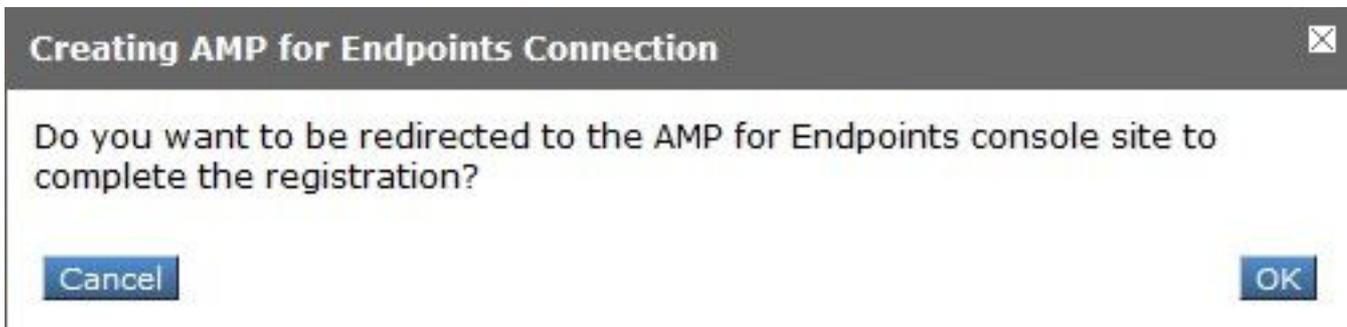
 [Edit Global Settings...](#)

搜索“文件信誉的高级”>“高级设置”部分并展开该部分，然后显示一系列云服务器选项，选择离您位置最近的位置。

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	

选择云后，点击向终端注册AMP的设备按钮。

系统将显示一个弹出窗口，可重定向到AMP控制台，单击“确定”按钮，如图所示。



您需要输入有效的AMP凭证，然后点击Log in(登录)，如图所示。



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?](#)

接受设备注册，记下客户端ID，因为它有助于稍后在控制台上查找WSA。

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.

返回WSA控制台，在面向终端的AMP的终端控制台集成部分会显示一个检查，如图所示。

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 ? Deregister ✓ SUCCESS	

注意：不要忘记单击“提交”并提交更改（如果出现提示），否则，需要再次完成该流程。

Threat Grid集成

导航到安全服务>防恶意软件和信誉，然后在防恶意软件防护服务上，单击编辑全局设置按钮，如图所示。

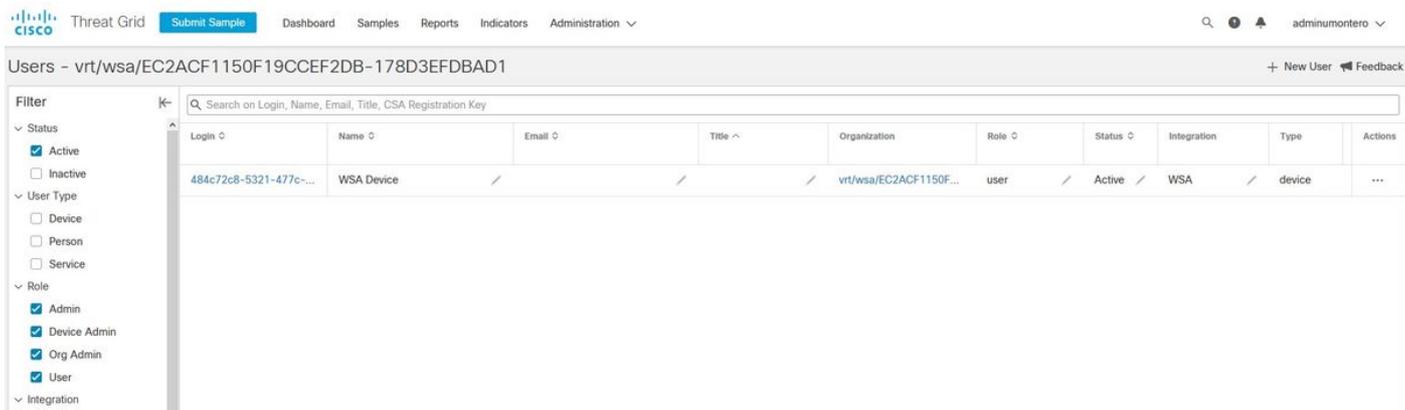
Anti-Malware Scanning Services	
DVS Engine Object Scanning Limits:	Max. Object Size: 32 MB
Sophos:	Enabled
McAfee:	Feature Key for McAfee has expired or is unavailable. For information on enabling this feature with a new key, contact your Cisco sales representative.
Webroot:	Enabled Threat Risk Threshold: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

搜索“高级”>“文件分析的高级设置”部分并展开该部分，选择离您所在位置最近的选项，如图所示。

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)
	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	

单击“提交并提交更改”。

在TG门户端，如果设备已成功与AMP/TG集成，请在“用户”选项卡下搜索WSA设备。



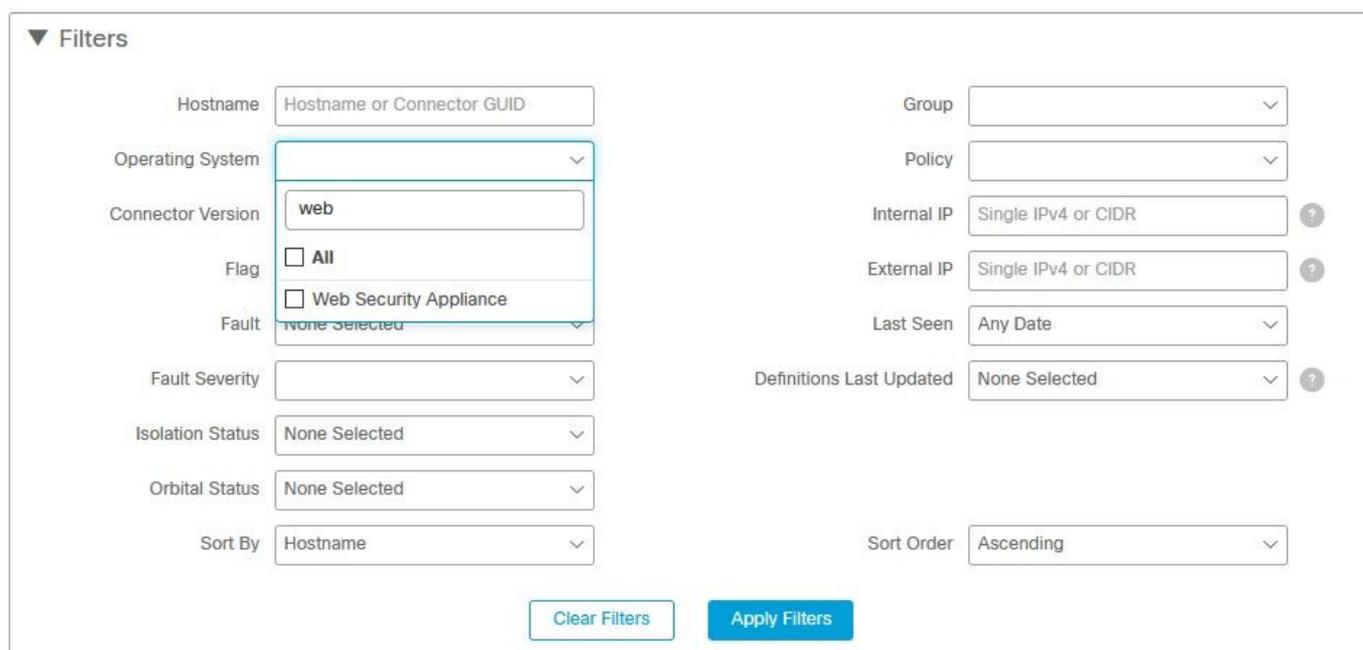
如果点击登录(Login)，则可以访问所述设备的信息。

验证

使用本部分可确认配置能否正常运行。

为了验证AMP与WSA之间的集成是否成功，您可以登录AMP控制台并搜索WSA设备。

导航至“管理”>“计算机”，在“过滤器”部分搜索网络安全设备并应用过滤器



如果注册了多台WSA设备，可以使用文件分析客户端ID来识别这些设备。

如果展开设备，您可以看到它所属的组、应用的策略和设备GUID可用于查看设备轨迹。

Hostname	VLNWSA-... Group	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，可以配置应用于设备的简单自定义检测和应用控制 — 允许。

Policy

Network

Name:

Description:

Outbreak Control

Custom Detections - Simple:

Application Control - Allowed:

查看WSA的Device Trajectory部分有一个技巧，您需要打开另一台计算机的Device Trajectory并使用Device GUID。

如图所示，更改将应用于URL。



对于Threat Grid，阈值为90，如果文件在该数字下获得分数，则文件不会被恶意攻击，但是，您可以在WSA上配置自定义阈值。

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)

故障排除

WSA不重定向到AMP页面

- 确保防火墙允许AMP所需的地址，请单击[此处](#)。
- 确保您已选择正确的AMP云（避免选择传统云）。

WSA不阻止指定的SHA

- 确保您的WSA位于正确的组中。
- 确保您的WSA使用正确的策略。
- 确保云上的SHA不干净，否则WSA将无法阻止它。

WSA不出现在我的TG组织中

- 确保您选择了正确的TG云（美洲或欧洲）。
- 确保防火墙允许TG所需的地址。
- 记录文件分析客户端ID。
- 在“用户”部分下搜索。
- 如果您找不到，请联系思科支持，以便他们帮助您在组织之间移动。