将面向终端的AMP和Threat Grid与WSA集成

目录

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。

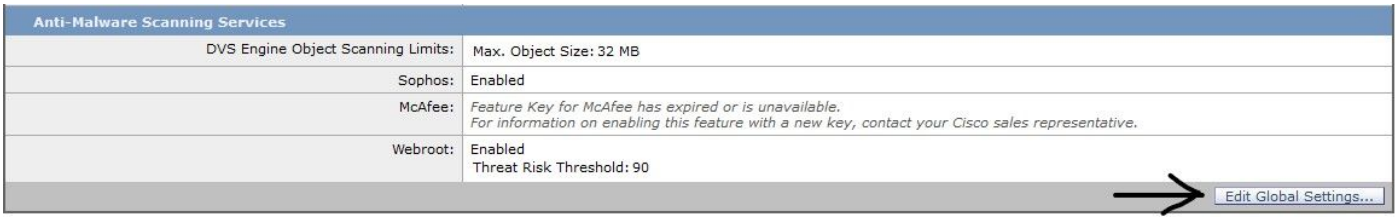
配置

登录到WSA控制台。

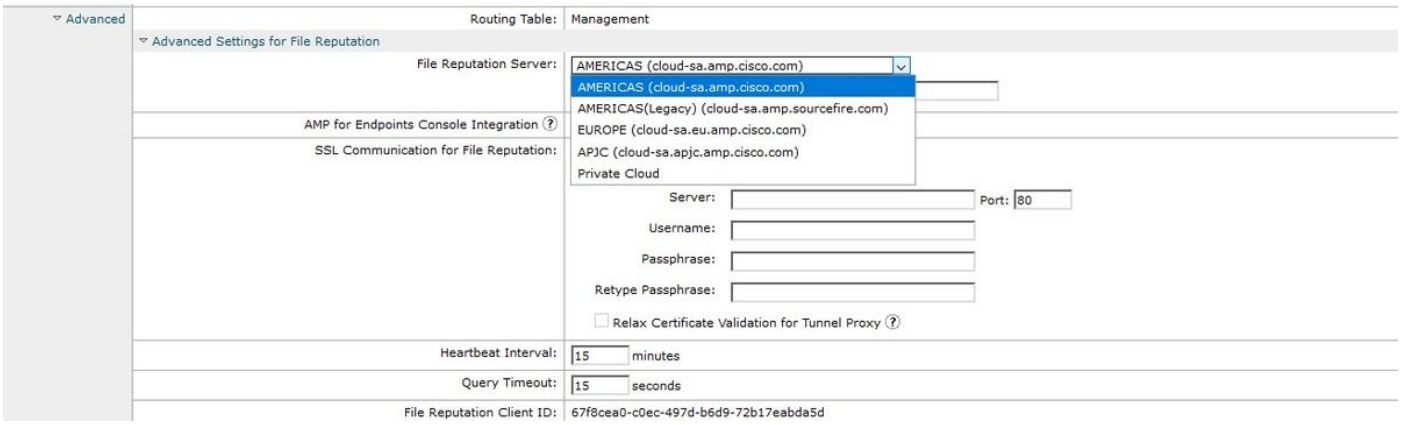
登录后，导航至**安全服务>防恶意软件和信誉，在**此部分中，您可以找到集成AMP和TG的选项。

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。

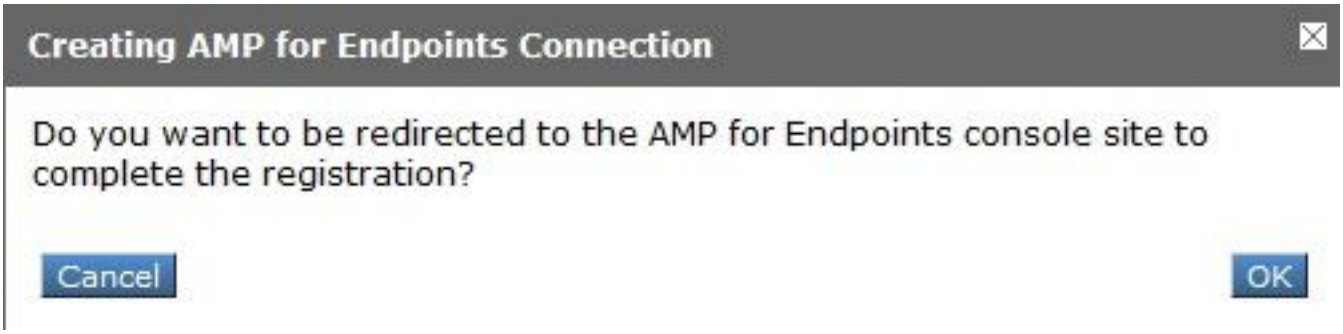


搜索“文件信**誉的高级”>“高级设置”**部分并展开该部分，然后显示一系列云服务器选项，选择离您位置最近的位置。

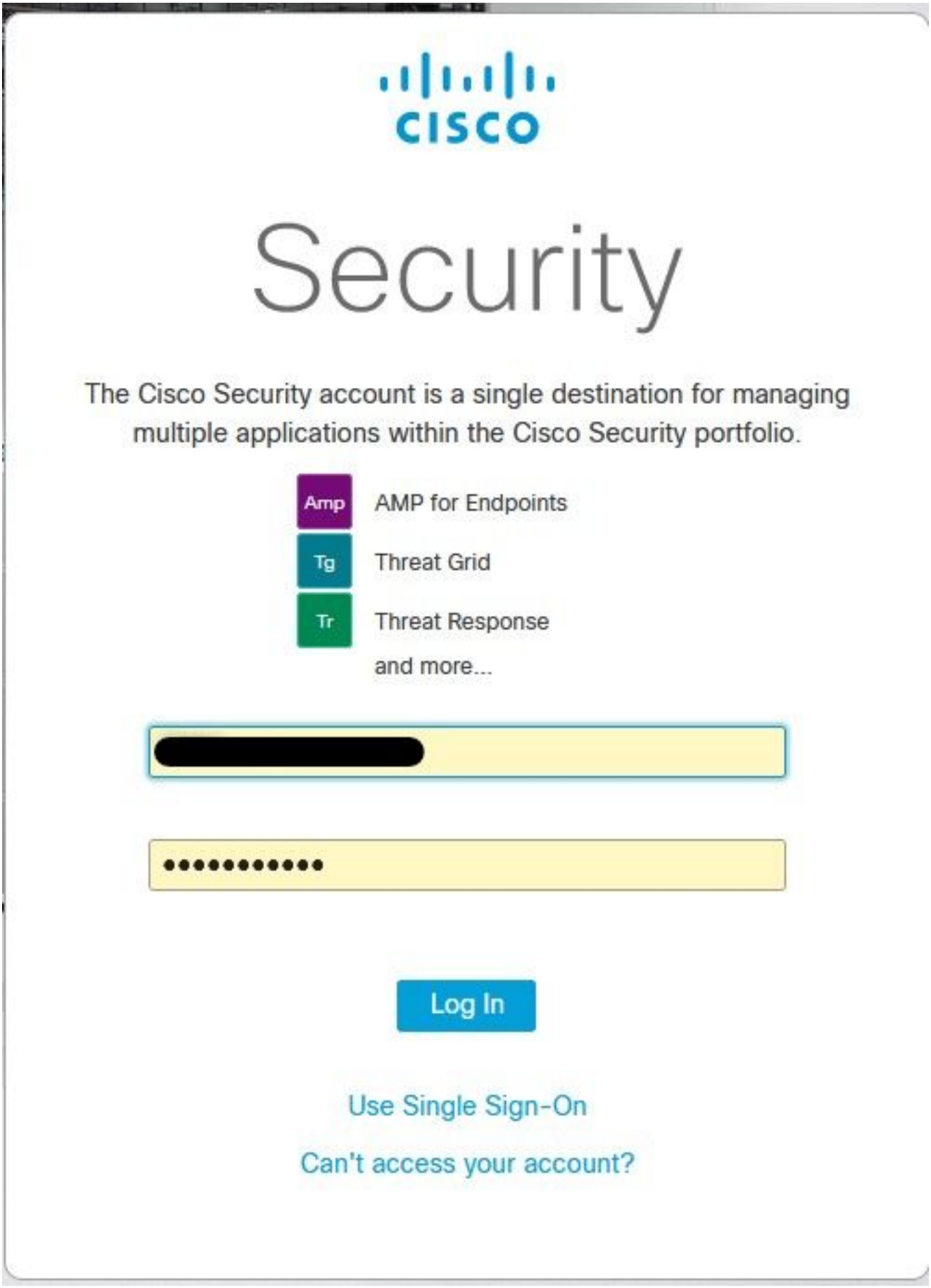


选择云后，点击向终端注**册AMP的设备按**钮。

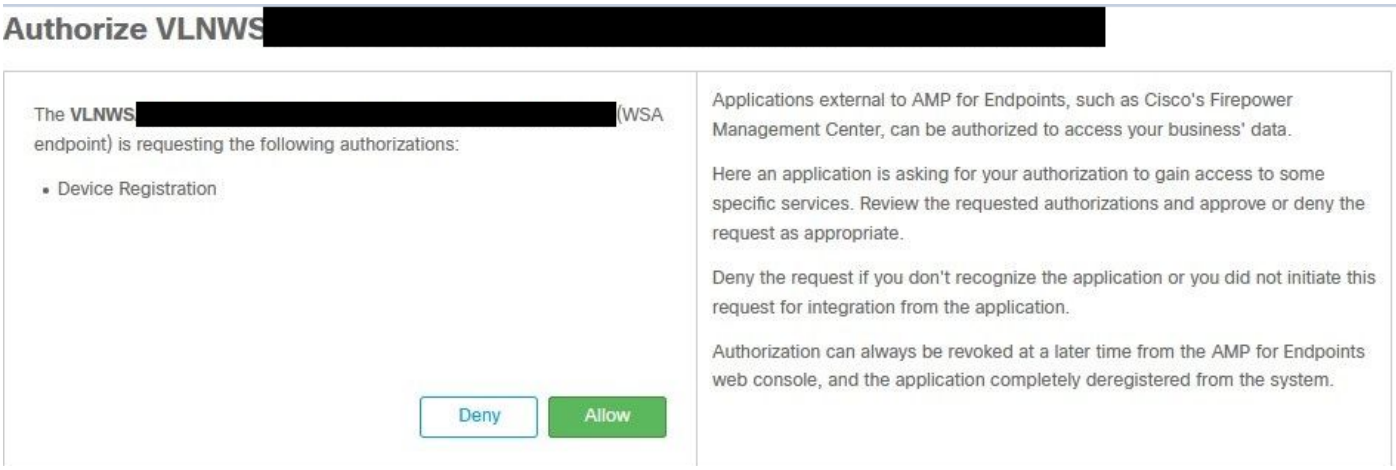
系统将显示一个弹出窗口，可重定向到AMP控制台，**单击"确**定"按钮，如图所示。



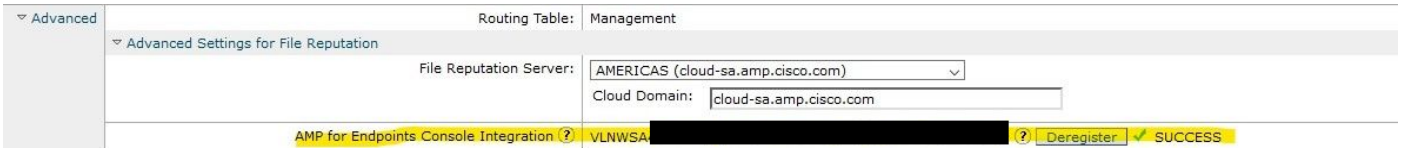
您需要输入有效的AMP凭证，然后点击Log in(登录)，如图所示。



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。



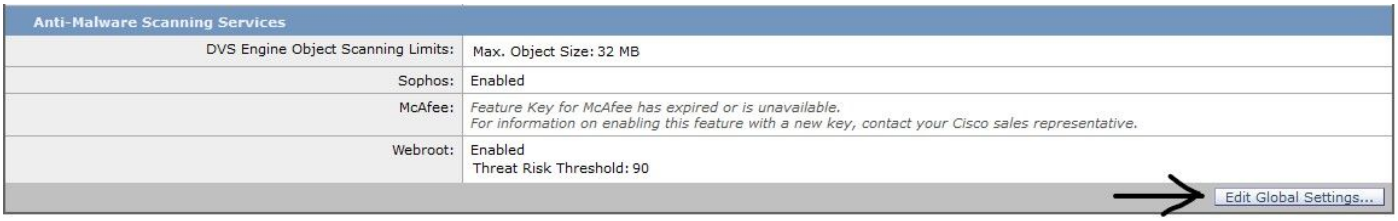
返回WSA控制台，在面向终端的AMP的终端控制台集成部分会显示一个检查，如图所示。



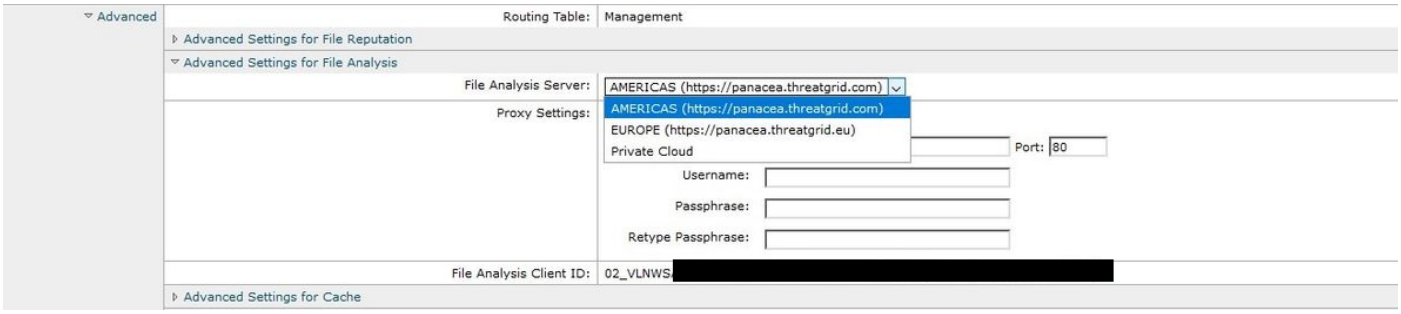
注意：不要忘记单击“提交”**并**提交**更**改（如果出现提示），否则，需要再次完成该流程。

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。

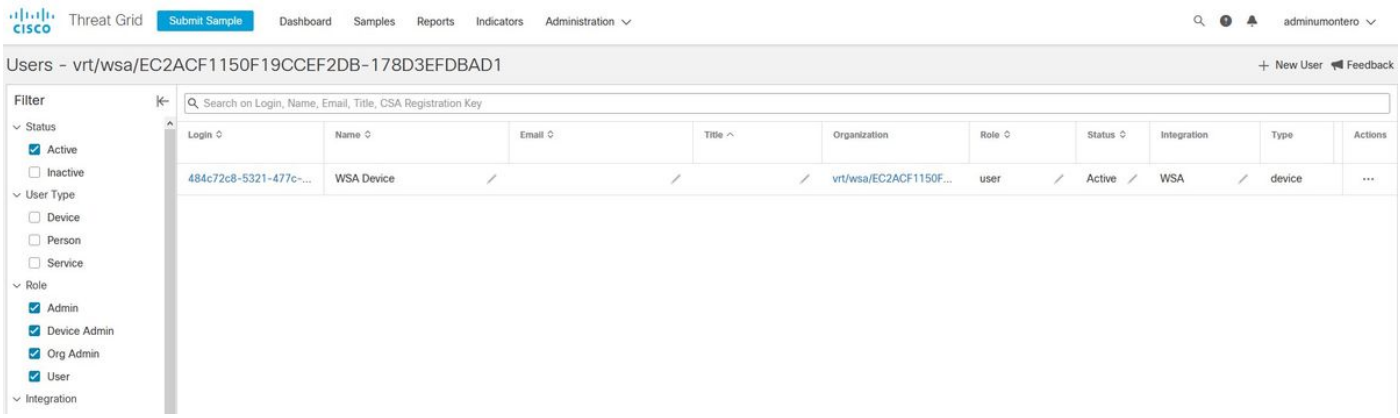


搜索“高级”**>“文件分析的高级设置”**部分并展开该部分，选择离您所在位置最近的选项，如图所示。



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。



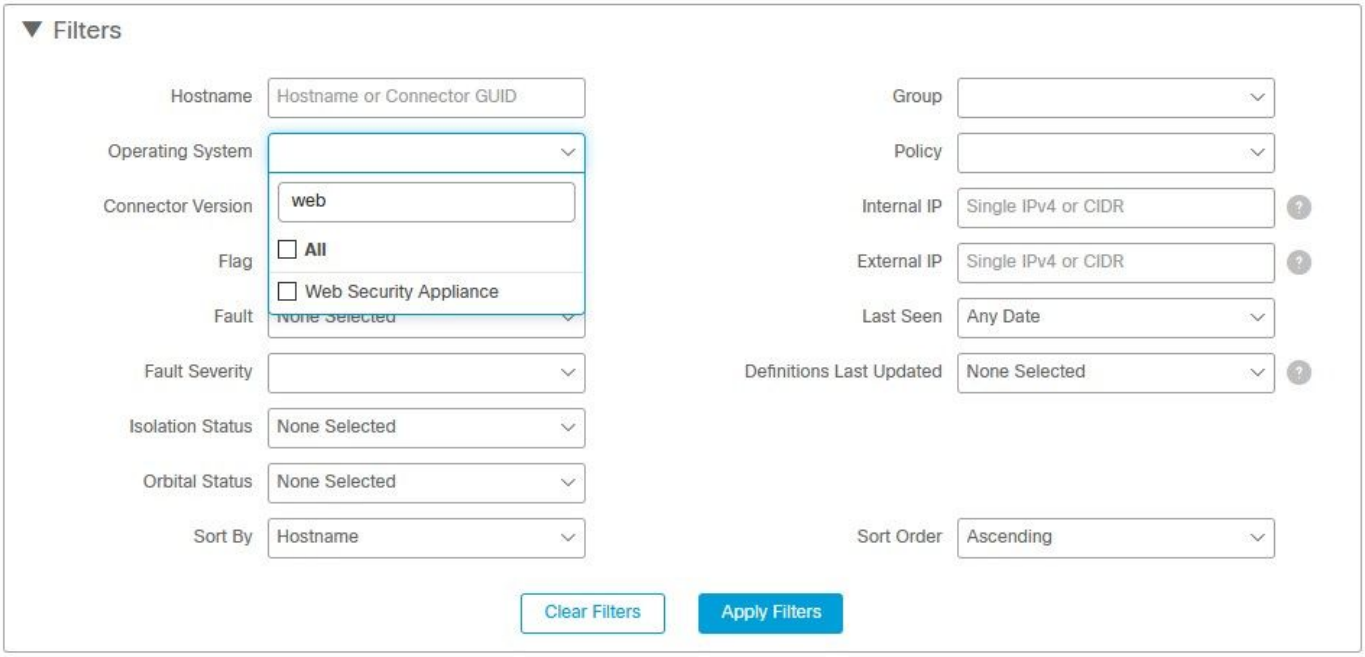
如果点击登录(Login)，则可以访问所述设备的信息。

验证

使用本部分可确认配置能否正常运行。

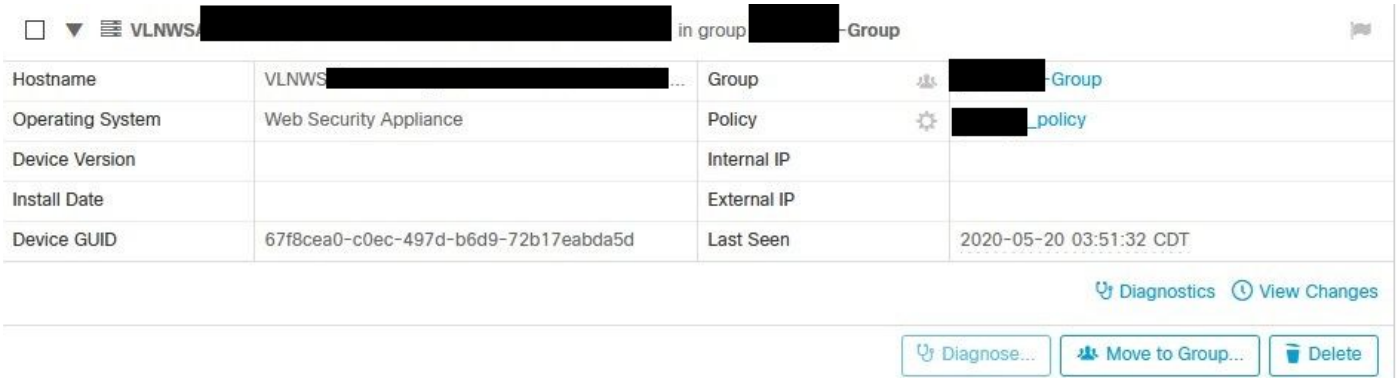
为了验证AMP与WSA之间的集成是否成功，您可以登录AMP控制台并搜索WSA设备。

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

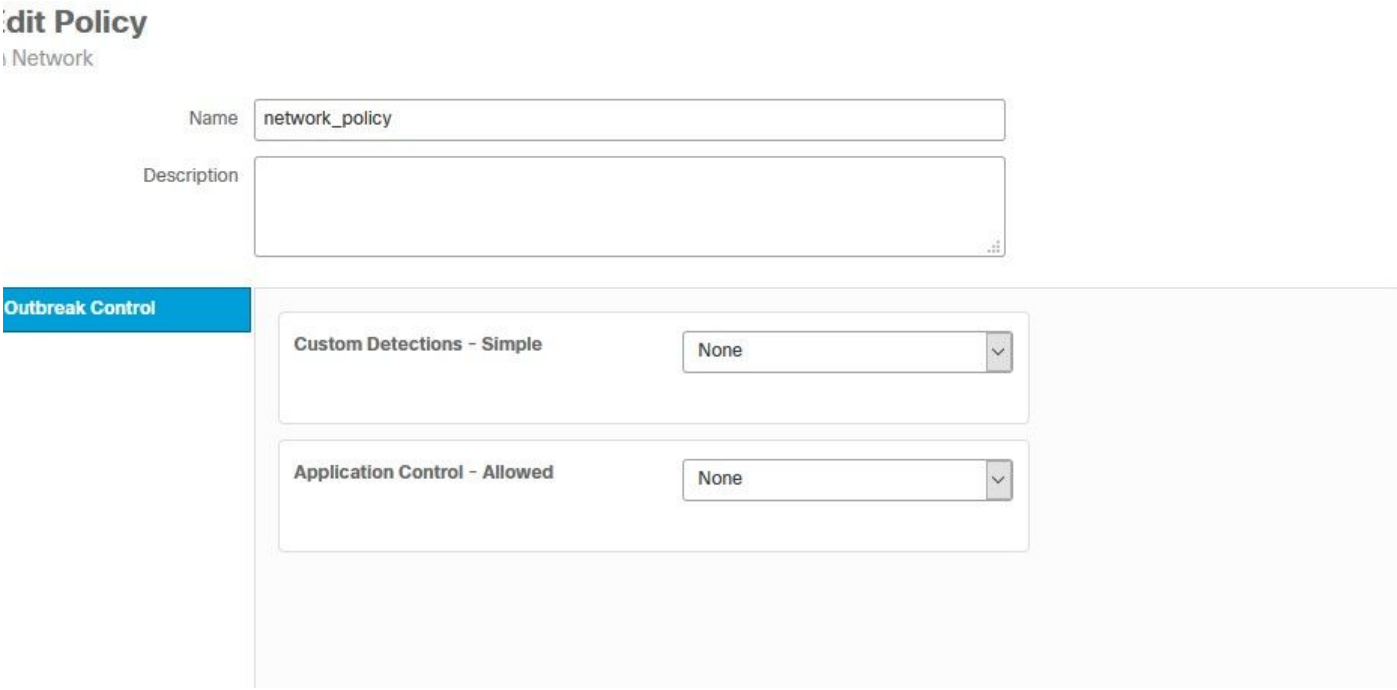


如果注册了多台WSA设备，可以使用文件分析客户端ID来识别这些设备。

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。

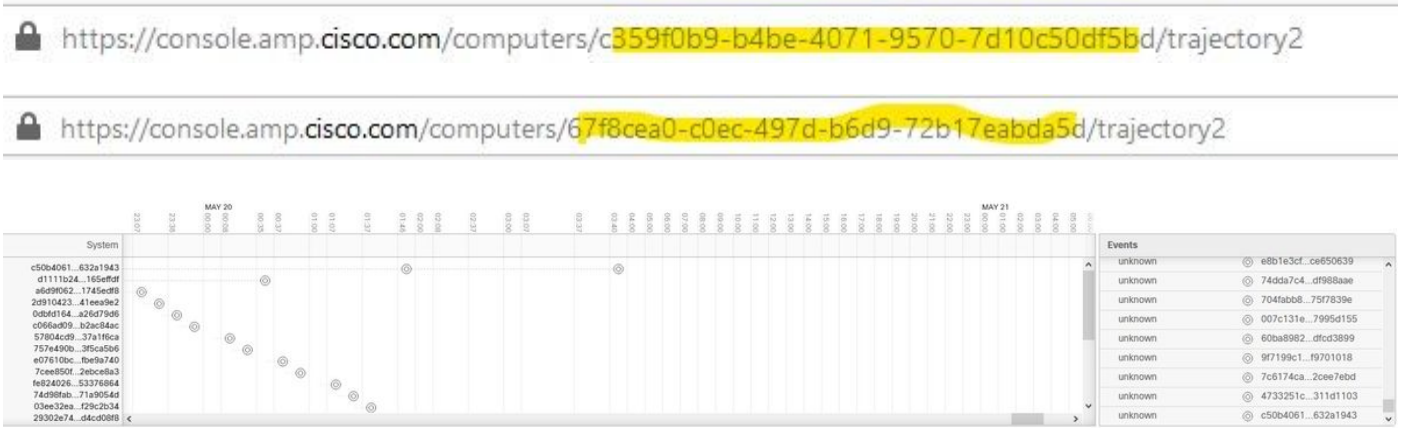


在策略部分，可以配置应用于设备的简单自定义检测和应用控制 — 允许。

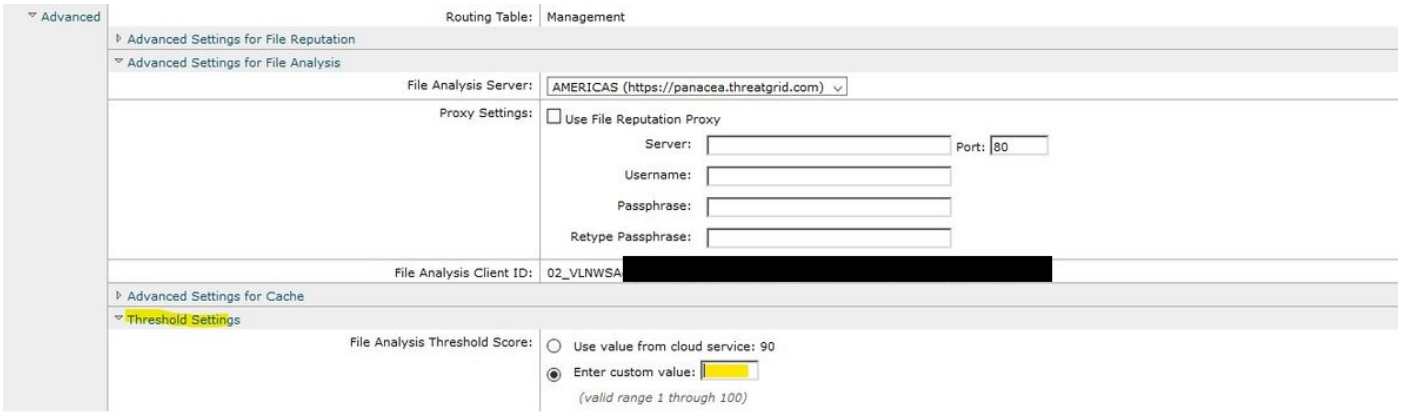


查看WSA的Device Trajectory部分有一个技巧，您需要打开另一台计算机的Device Trajectory并使用Device GUID。

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。



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。