配置安全恶意软件分析（以前称为Threat Grid）与Umbrella的集成

目录

简介

本文档介绍如何将Secure Malware Analytics（以前称为Threat Grid）与Umbrella集成。

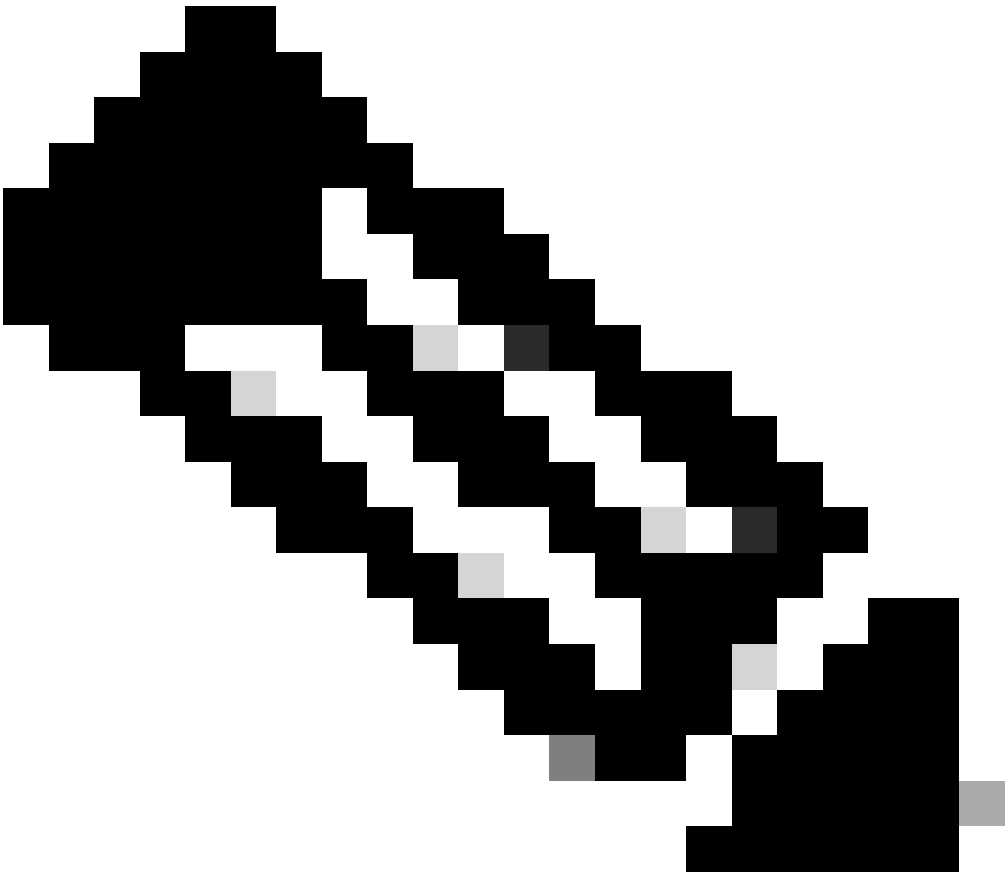
适用于Cisco Umbrella的思科安全恶意软件分析(Threat Grid)集成概述

通过集成Cisco Secure Malware Analytics（以前称为Threat Grid）和Cisco Umbrella，安全团队现在能够扩展其可视性，针对漫游笔记本电脑、平板电脑或电话的当今高级威胁实施保护，同时为分布式企业网络提供另一层实施层。

本指南概述如何配置思科安全恶意软件分析(Threat Grid)以与Cisco Umbrella进行通信，以便可以将思科安全恶意软件分析(Threat Grid)生成的威胁情报自动集成到可以保护思科Umbrella下客户端的策略中。

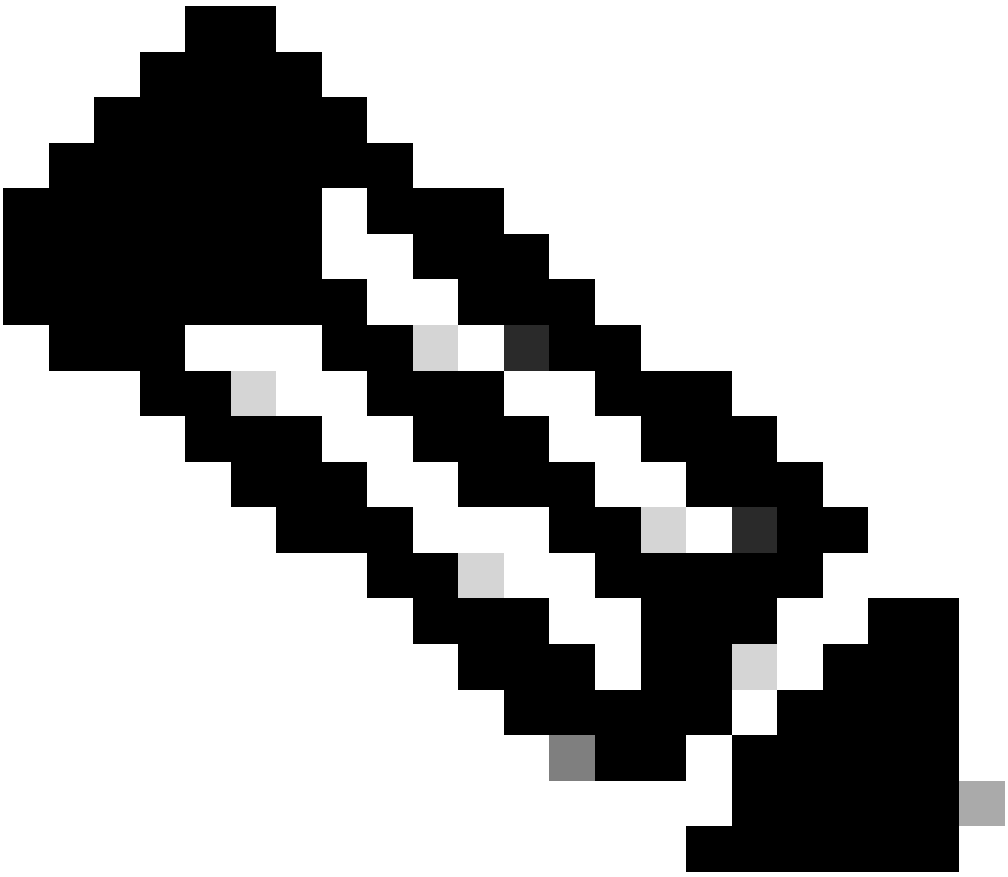
先决条件

- 功能强大的思科安全恶意软件分析(Threat Grid)控制面板，可访问您帐户的API密钥。



注意：目前不支持思科安全恶意软件分析(Threat Grid)设备和终端。

- Cisco Umbrella Dashboard管理权限。
- Cisco Umbrella控制面板必须启用思科安全恶意软件分析(Threat Grid)集成。



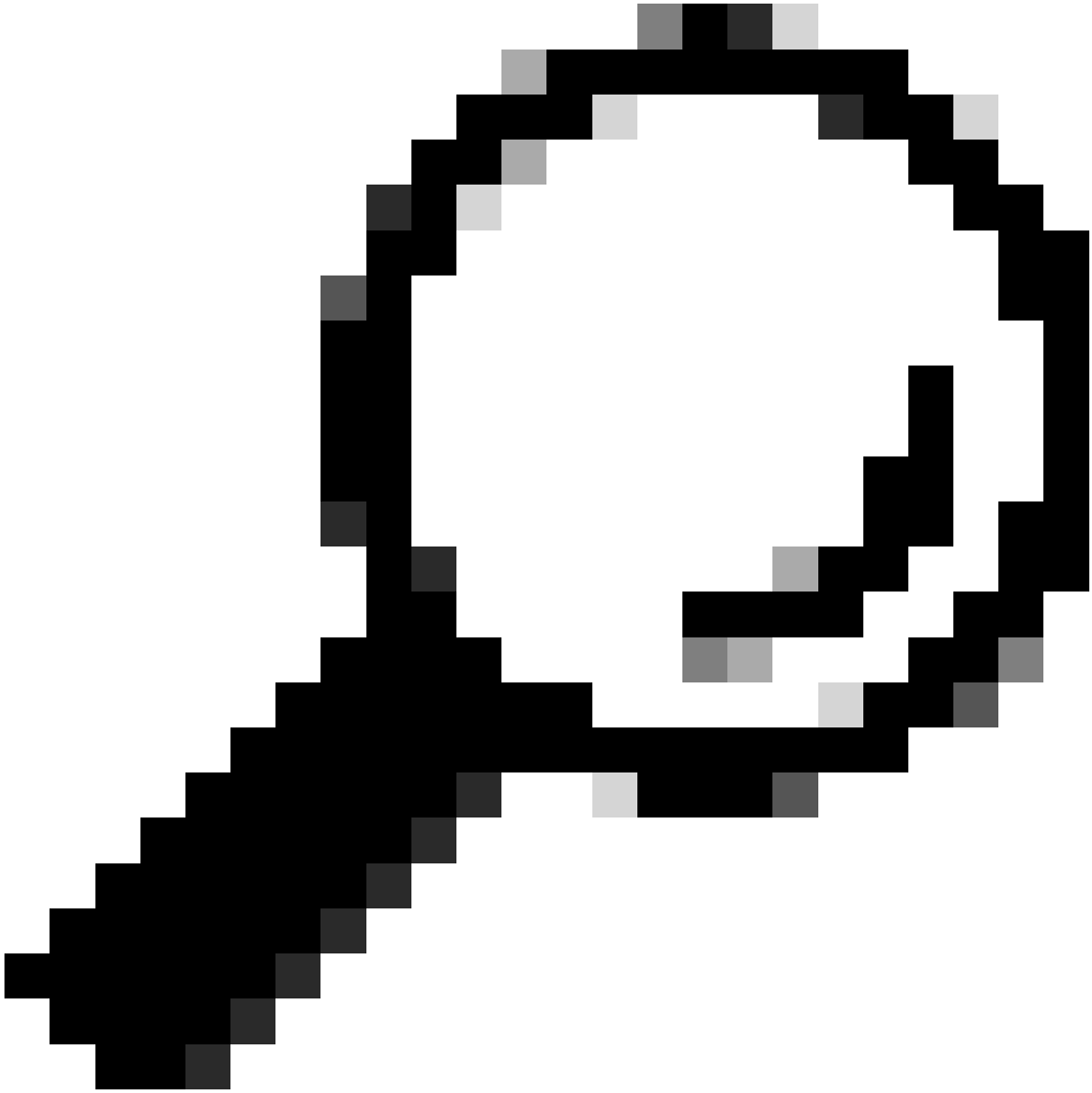
注意：思科安全恶意软件分析(Threat Grid)集成仅包含在Cisco Umbrella软件包中，例如DNS Essentials、DNS Advantage、SIG Essentials或SIG Advantage。如果您没有Cisco Umbrella软件包并希望进行此集成，请联系您的Cisco Umbrella客户经理。如果您有Cisco Umbrella软件包，但没有将思科安全恶意软件分析(Threat Grid)视为控制面板集成，请联系Cisco Umbrella支持。

此集成如何工作？

思科Umbrella接触思科安全恶意软件分析(Threat Grid)API，并检索通过分析恶意样本生成的域列表。然后，Cisco Umbrella通过Cisco Umbrella Enforcement API导入此列表。此方法不同于其他集成在Cisco Umbrella中的工作方式，Cisco Umbrella通过向Cisco Secure Malware Analytics(Threat Grid)API进行API查询，而不是接受来自将威胁情报推送到Cisco Umbrella服务的其他系统的事件，从而引入威胁情报。

然后，Cisco Umbrella验证威胁以确保将其添加到您的策略中。如果确认来自思科安全恶意软件分析(Threat Grid)的信息是威胁或不是已知正常域，则域地址会作为可应用于任何思科Umbrella策略的安全设置的一部分添加到思科安全恶意软件分析(Threat Grid)目标列表。该策略会立即应用到使用思科安全恶意软件分析(Threat Grid)集成的策略从设备发出的任何请求。

Cisco Umbrella从思科安全恶意软件分析(Threat Grid)获取两个独立的源：公共（全球）馈送和仅客户（专用，特定于单个客户）馈送。



提示：虽然Cisco Umbrella会尽力验证和允许已知安全域（例如Google和Salesforce），以避免任何不必要的中断，我们建议您根据您的策略将您从未希望阻止的任何域添加到全局允许列表或其他目标列表。

示例包括：

- 您组织的主页。
- 代表您提供的服务的域，可能同时具有内部和外部记录。例如，“mail.myservicedomain.com”和“portal.myotherservicedomain.com”。
- 您严重依赖于Cisco Umbrella的知名度较低的云应用，可能并不了解这些应用或在其自动域验证中包括这些应用。例如，“localcloudservice.com”。

这些域必须添加到Global Allow List，该列表位于Cisco Umbrella的Policies > Destination Lists下。

配置Cisco Umbrella控制面板以从Cisco Secure Malware Analytics(Threat Grid)获取信息

第一步是在思科安全恶意软件分析(Threat Grid)控制面板中查找或生成API密钥：

1. 登录思科安全恶意软件分析(Threat Grid)控制面板并选择您的帐户详细信息。
2. 在Account Details下，如果您已经创建了一个API密钥，则可能已看到该API密钥。如果没有，请选择“生成新API密钥”。

   然后，您的API密钥在User Details > API Key下可见。

接下来，将API密钥添加到Cisco Umbrella Dashboard，以便其从思科安全恶意软件分析(Threat Grid)提取数据：

1. 以管理员身份登录您的Cisco Umbrella控制面板。
2. 导航至策略>策略组件>集成，然后在表中选择“Cisco AMP Threat Grid”（思科安全恶意软件分析[Threat Grid]）以展开它。
3. 选择Enable，将API密钥粘贴到API Key框中，然后选择Save。

此时，如果您收到错误，很可能是因为您的API密钥或服务之间的通信有问题。检查您的API密钥并重试，如果仍然失败，请联系思科Umbrella支持。

如果收到成功消息，则表明Cisco Umbrella服务能够使用API密钥建立到思科安全恶意软件分析(Threat Grid)API的初始连接。Cisco Umbrella服务使用五分钟的轮询间隔从思科安全恶意软件分析(Threat Grid)检索数据。

即使在5分钟间隔之后，如果没有有效数据或有效的威胁事件可供思科Umbrella控制面板调用，信息也可能不会显示。当首次启用集成时，对于全局和仅组织源，它只需返回五分钟开始，并且它第一次获取数据是在接下来的五分钟间隔内，因此数据可能不会立即显示。

如果思科安全恶意软件分析(Threat Grid)端的API密钥已停用或删除，则集成将被禁用。要恢复集成，必须在Cisco Umbrella Dashboard中提供新的API密钥。如果Cisco Umbrella和Cisco Secure Malware Analytics(Threat Grid)之间存在超时或内部服务错误，则会引发不同类型的异常，并且不会禁用集成，而是像正常情况下一样，每五分钟尝试一次连接。

技术详细资料

下面列出了用于从思科安全恶意软件分析(Threat Grid)提取信息的精确API查询。请注意，仅收集严重性大于90、置信度大于90以及域类型的事件。此示例中的时间是一个五分钟范围，该范围针对下一个查询递增。使用Cisco Umbrella中提供的`api_key`代替`<key>`变量：

- 公共（全局源）：

hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence

- 仅限客户（专用馈送）：

hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence

或:

- 公共（全局源）：

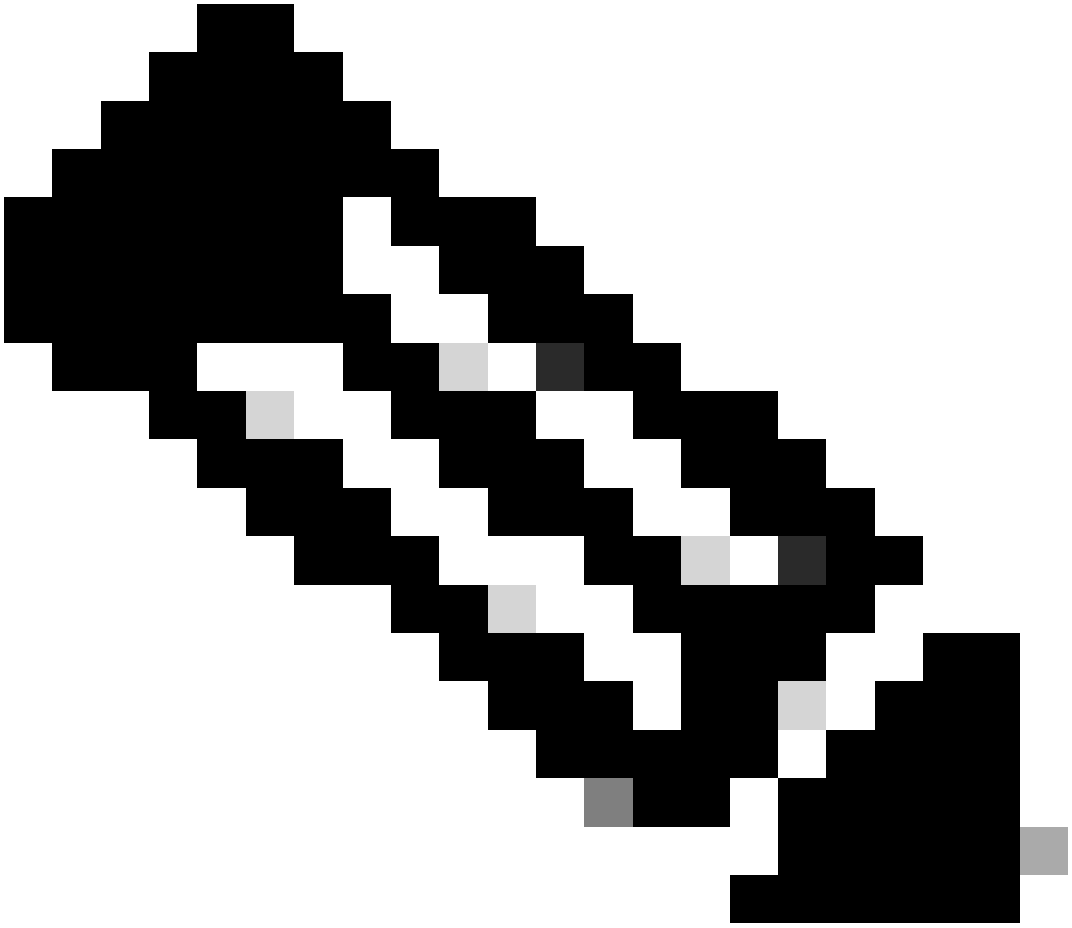
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence

- 仅限客户（专用馈送）：

hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence=

观察在“审核模式”下添加到思科安全恶意软件分析(Threat Grid)的事件

随着时间的推移，来自思科安全恶意软件分析(Threat Grid)的事件开始填充可以应用于策略的特定目标列表，作为思科安全恶意软件分析(Threat Grid)类别。默认情况下，目标列表和安全类别处于“审核模式”下，不应用于任何策略，因此不会导致任何请求被阻止。但是，您可以看到哪些请求与Cisco AMP Threat Grid安全类别关联（并且可能已被阻止）。



注意：“审核模式”可根据需要随时启用，甚至可以无限期启用，具体取决于您的部署配置文件和网络配置。

查看目标列表

您可以随时查看思科安全恶意软件分析(Threat Grid)目标列表。

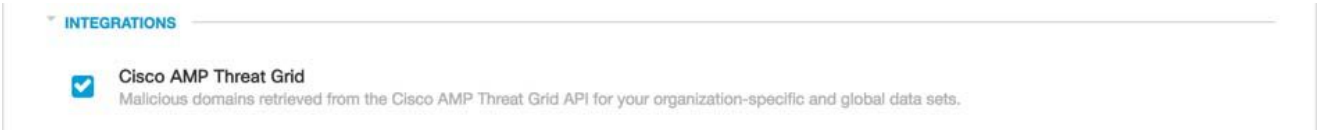
1. 导航到Policies > Policy Components > Integrations。
2. 展开表中的“思科AMP Threat Grid”（思科安全恶意软件分析[Threat Grid]），然后选择“查看域”。

查看策略的安全设置

您可以随时在Cisco Umbrella中查看可以为策略启用的安全设置：

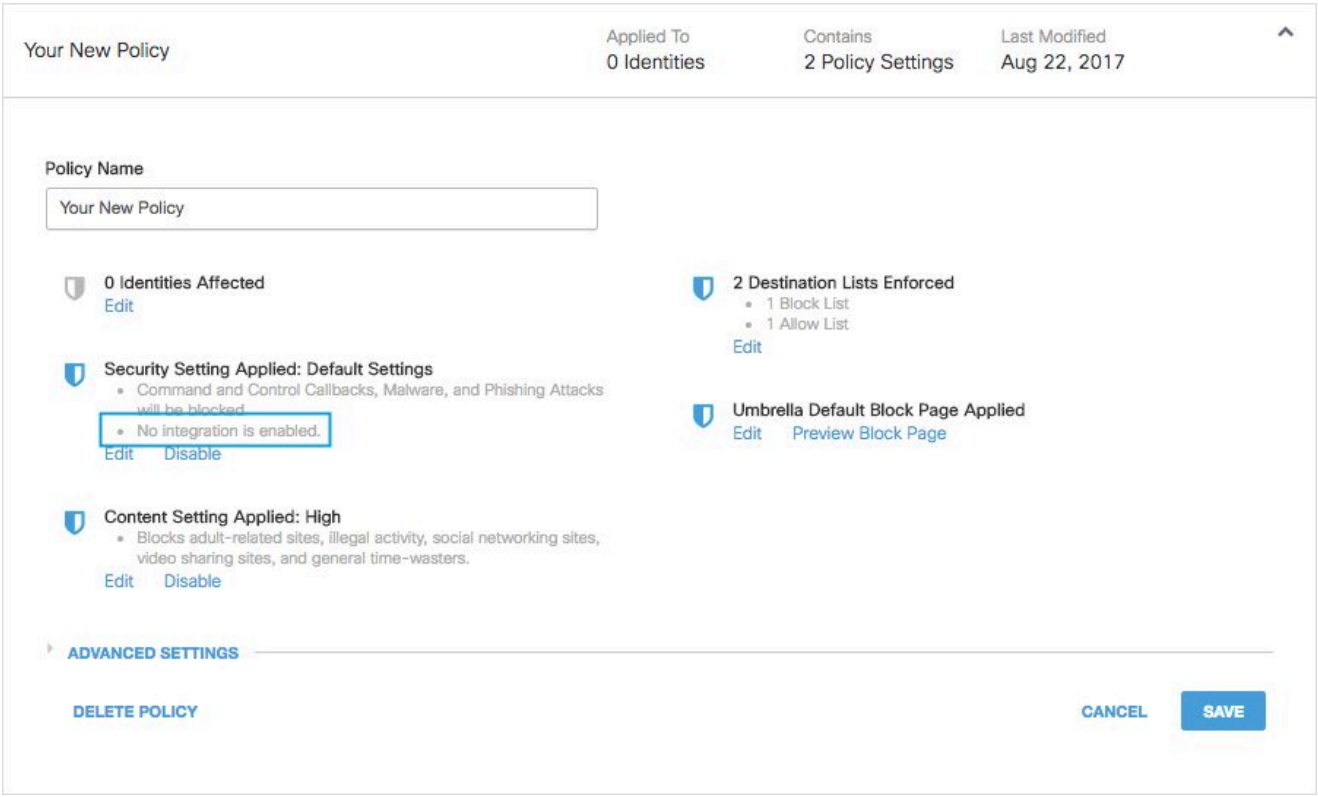
1. 导航到策略>策略组件>安全设置。
2. 单击表中的安全设置将其展开。

3. 滚动到集成部分并展开该部分以显示Cisco AMP Threat Grid（思科安全恶意软件分析[Threat Grid]）集成。
4. 选中Cisco AMP Threat Grid集成(思科安全恶意软件分析(Threat Grid))框，然后选择Save。

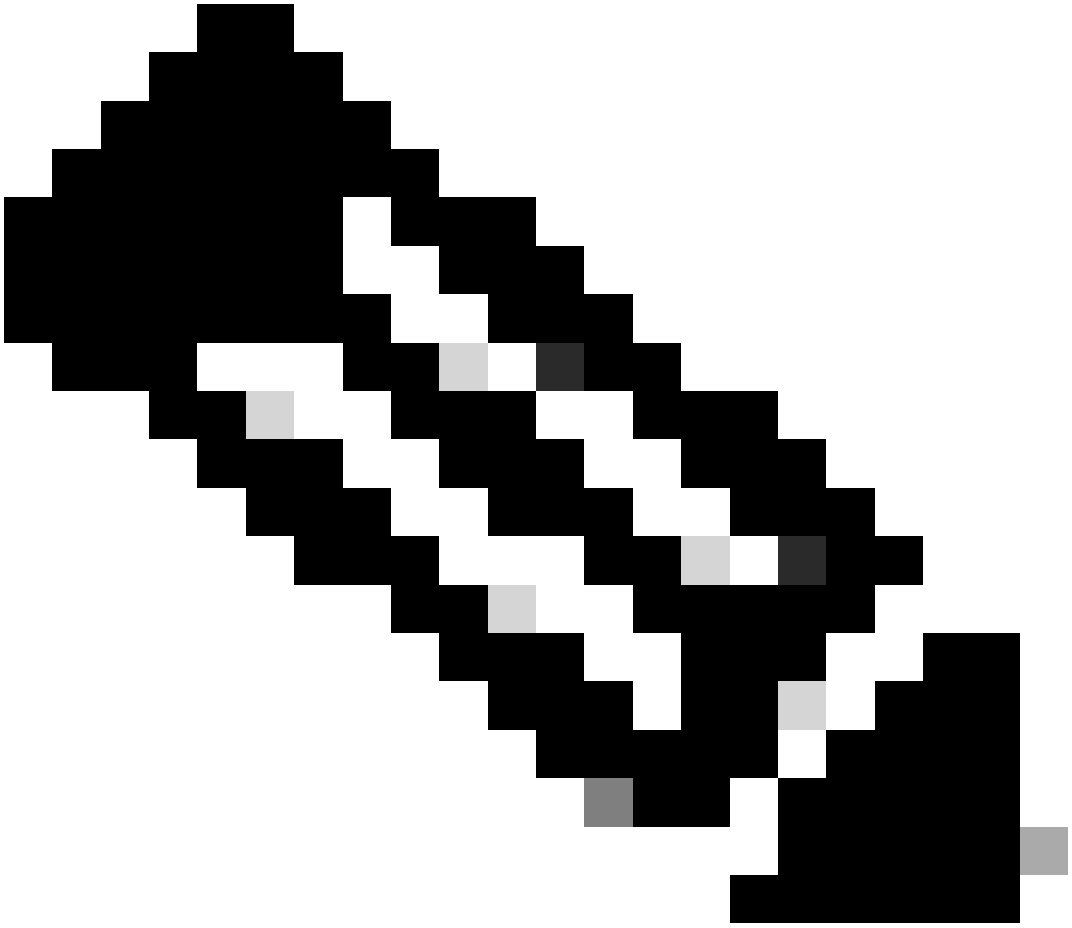


115014151543

您还可以通过“安全设置摘要”页面查看集成信息。



20993269073556

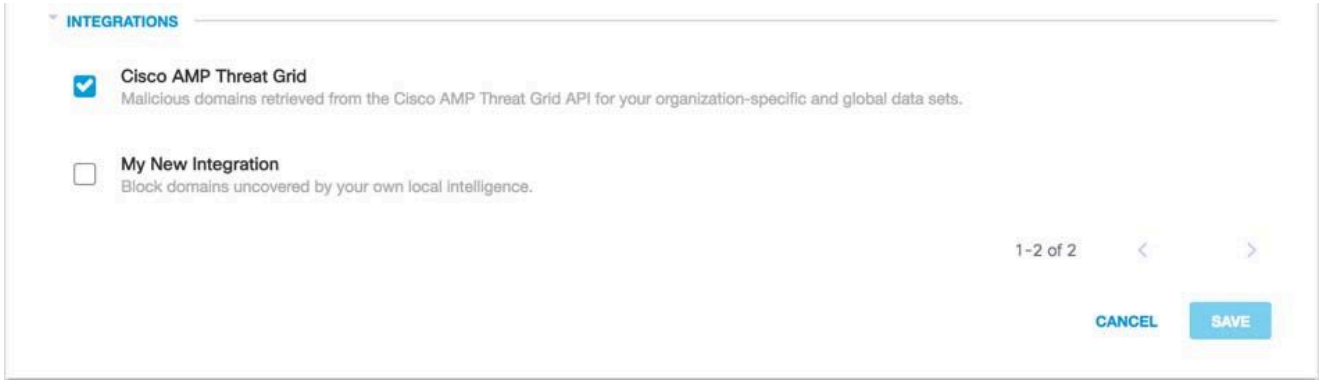


注意：应用设置可能需要最多五分钟的时间，如果未将新事件注入到思科安全恶意软件分析(Threat Grid)系统，则您可能看不到正在向集成中添加的新域。

在“阻止模式”下将思科安全恶意软件分析(Threat Grid)安全设置应用于托管客户端的策略

一旦您准备好阻止这些域用于由Cisco Umbrella管理的客户端，请更改现有策略的安全设置，或创建位于默认策略之上的新策略，以确保首先实施该策略。

1. 导航到策略>策略组件>安全设置。
2. 在Integrations下，验证“Cisco AMP Threat Grid”框已选中。否则，请选中该框并选择保存。



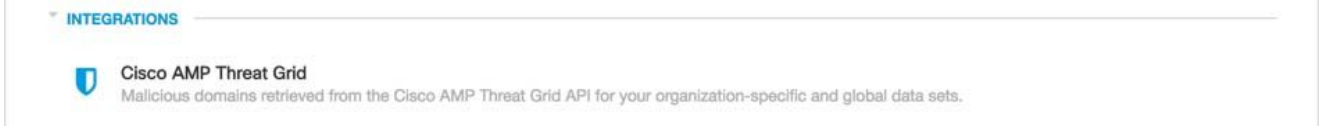
115013987086

接下来，在Cisco Umbrella Policy向导中，将安全设置添加到正在编辑的策略中：

1. 导航到Policies > Management > All Policies。
2. 展开策略并在Security Setting Applied下选择Edit。
3. 在Security Settings下拉列表中，选择包含“Cisco AMP Threat Grid”设置的安全设置。

20993282642708

“集成”(Integrations)下的屏蔽图标将更新为蓝色。



115013987446

4. 选择设置并返回。

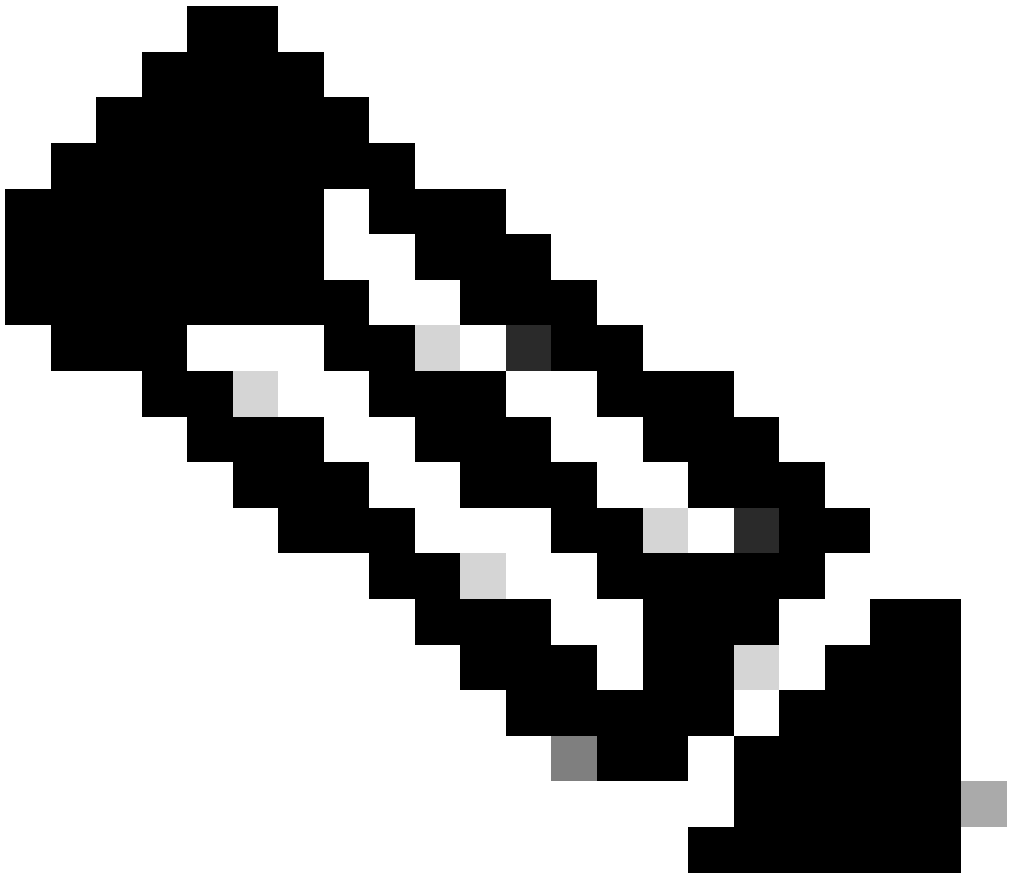
思科安全恶意软件分析(Threat Grid)安全设置中包含的思科安全恶意软件分析(Threat Grid)域会使用策略对这些身份进行阻止。

在Cisco Umbrella内报告思科安全恶意软件分析事件

思科安全恶意软件分析(Threat Grid)安全事件报告

思科安全恶意软件分析(Threat Grid)目标列表是您可以报告的安全类别列表之一。大多数或全部报告将安全类别用作过滤器。例如，您可以过滤安全类别，仅显示与思科安全恶意软件分析(Threat Grid)相关的活动。

1. 导航到报告>核心报告>活动搜索，在安全类别下选择“Cisco AMP Threat Grid”(思科安全恶意软件分析(Threat Grid))以过滤报告，仅显示思科安全恶意软件分析(Threat Grid)的安全类别。



注意：如果思科AMP Threat Grid集成被禁用，则它不会出现在安全类别过滤器中。

115014210123

2. 选择Apply。

报告域何时添加到思科安全恶意软件分析(Threat Grid)目标列表

Cisco Umbrella Admin Audit日志包含来自Cisco Secure Malware Analytics(Threat Grid)控制面板的事件，因为它将域添加到目标列表。名为“Cisco AMP Threat Grid域列表”（也带有思科徽标）的用户生成事件。这些事件包括添加的域和添加的时间。

选择Admin Audit Log（管理员审核日志）条目会将其展开以显示详细信息，包括添加的特定域。

通过为“Cisco AMP Threat Grid域列表”用户应用过滤器，您可以过滤以仅包含思科安全恶意软件分析(Threat Grid)更改。

处理不需要的检测或误报

两种类型的思科安全恶意软件分析(Threat Grid)检测和两种解决方案

目前，有两种类型的思科安全恶意软件分析(Threat Grid)块：一个具有一种可能的分辨率，而另一个具有一种当前的分辨率，用于不需要的检测。

1. Global Threat Grid条目（公共）：此时，允许该域的唯一方法是将其添加到您的允许列表。
2. 仅客户源（专用）：可使用允许列表条目或从AMP Threat Grid集成列表中删除进行寻址。

允许列表

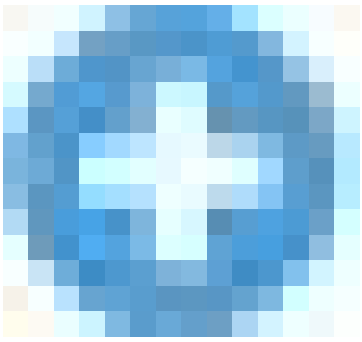
尽管可能性不大，但您的思科安全恶意软件分析(Threat Grid)集成自动添加的域可能会触发不必要的检测，阻止您的用户访问特定网站。在这种情况下，我们建议将域添加到允许列表(Policies > Destination Lists)，该列表优先于所有其他类型的阻止列表，包括安全设置。

首选此方法有两个原因。首先，如果思科安全恶意软件分析(Threat Grid)控制面板在删除域后再次重新添加域，则允许列表可防止出现进一步的问题。其次，允许列表显示了问题域的历史记录，可用于调查分析或审核报告。

默认情况下，全局允许列表应用于所有策略。将域添加到全局允许列表(Global Allow List)会导致在所有策略中允许该域。

如果阻止模式下的思科安全恶意软件分析(Threat Grid)安全设置仅适用于托管思科Umbrella身份的子集（例如，它仅适用于漫游计算机和移动设备），则可以为这些身份或策略创建特定的允许列表。

要创建允许列表，请执行以下操作：



1. 导航到Policies > Policy Components > Destination Lists，然后选择

   25463394696852

   （“添加”）。
2. 选择Allow并将您的域添加到列表中。
3. 选择Save。

保存该列表后，您可以将其添加到现有策略中，该策略涵盖了那些受不需要的阻止影响的客户端。

从思科安全恶意软件分析(Threat Grid)目标列表中删除域

思科安全恶意软件分析(Threat Grid)列表中的每个域名旁边都有一个（“删除”）图标。通过删除域，您可以在发生意外检测时清除思科安全恶意软件分析(Threat Grid)目标列表。

如果Cisco Secure Malware Analytics(Threat Grid)控制面板将域重新发送到Cisco Umbrella，则删除操作不是永久的。

1. 导航到策略>策略组件>集成，然后选择“Cisco AMP Threat Grid”（思科安全恶意软件分析[Threat Grid]）进行扩展。
2. 选择See Domains。
3. 搜索要删除的域名。
4. 选择（“删除”）图标。
5. 选择Close。
6. 选择Save。

对于不需要的检测或误报，我们建议立即在Cisco Umbrella中创建允许列表，然后在Cisco Secure Malware Analytics(Threat Grid)控制面板中修复误报。之后，您可以从思科安全恶意软件分析(Threat Grid)目标列表中删除该域。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。