将ThreatQ与Umbrella集成

目录

简介

本文档介绍如何将ThreatQ与Cisco Umbrella集成。

先决条件

要求

Cisco 建议您了解以下主题：

- ThreatQ控制面板，具有更新集成URL的访问权限
- Umbrella控制面板管理权限
- Umbrella控制面板必须启用ThreatQ集成。

使用的组件

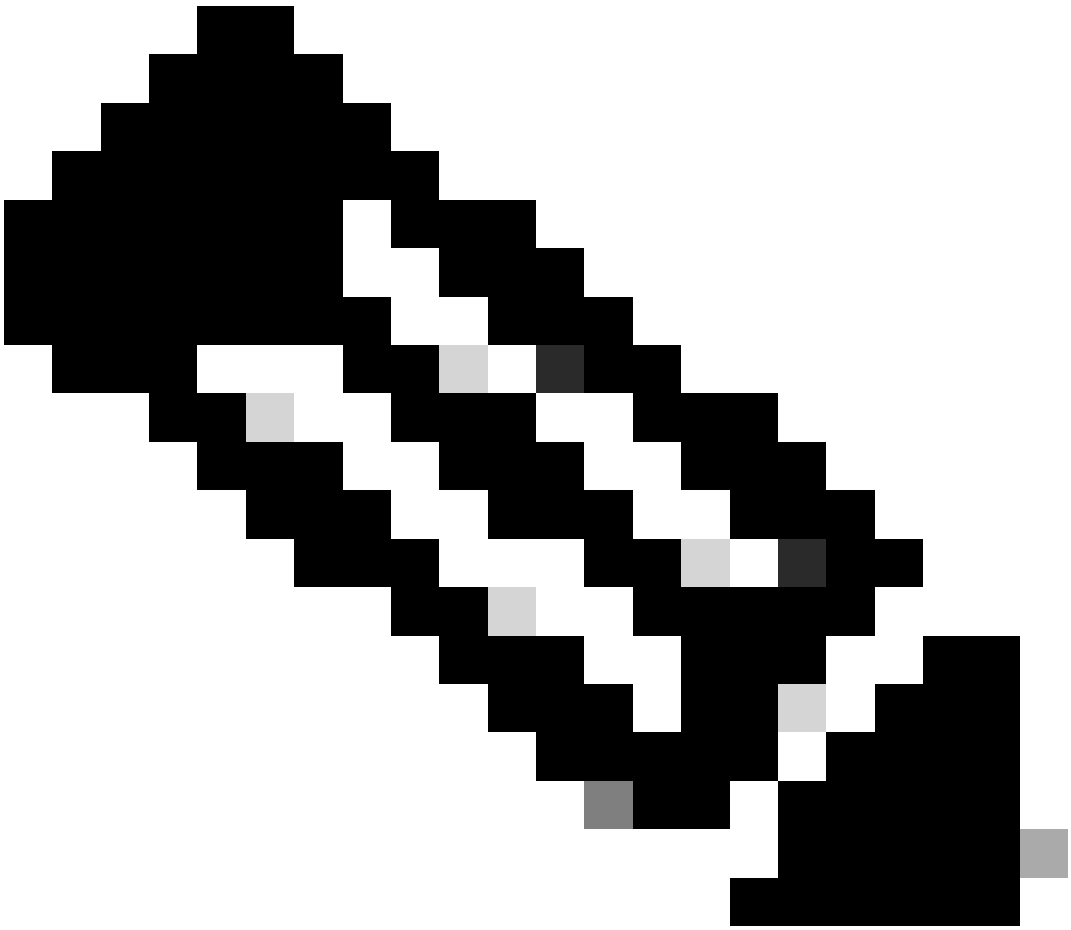
本文档中的信息基于Cisco Umbrella。

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。

ThreatQ和Cisco Umbrella集成概述

通过将ThreatQ与Cisco Umbrella相集成，安全人员和管理员现在能够针对漫游的笔记本电脑、平板电脑或电话的高级威胁提供保护，同时为分布式企业网络提供另一层实施。

本指南概述如何配置ThreatQ以与Umbrella通信，以便将ThreatQ TIP的安全事件集成到策略中，这些策略可以应用于受Cisco Umbrella保护的客户端。



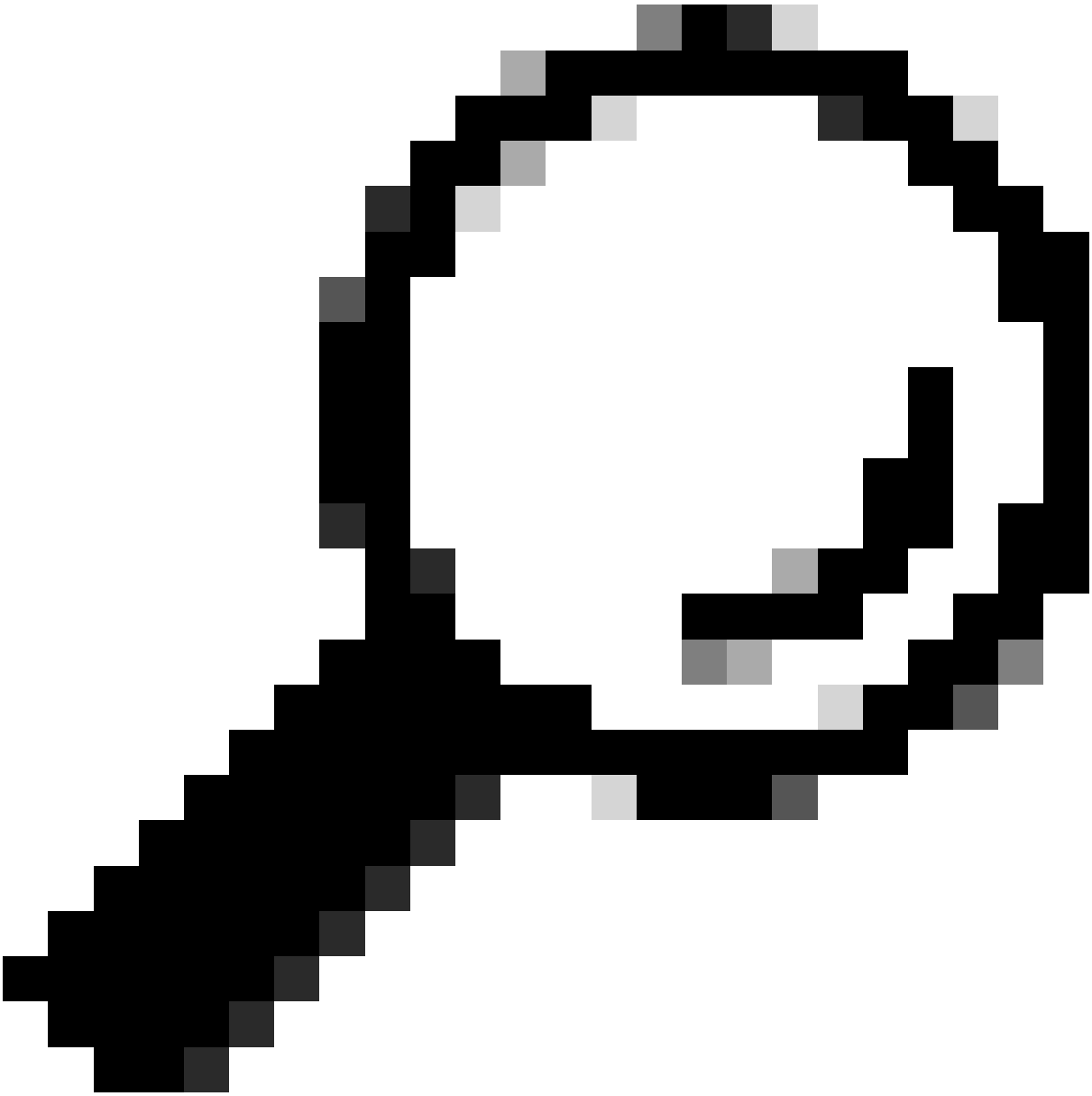
注意：ThreatQ集成仅包含在某些Cisco Umbrella软件包中。如果您没有所需的软件包并想要集成ThreatQ，请联系您的Cisco Umbrella代表。如果您有正确的Cisco Umbrella软件包，但是没有将ThreatQ视为控制面板集成，请与Cisco Umbrella支持联系。

集成功能

ThreatQ平台首先将其发现的网络威胁情报（例如托管恶意软件的域、僵尸网络或网络钓鱼站点的命令和控制）发送到Umbrella。

然后，Umbrella验证威胁以确保将其添加到策略中。如果确认来自ThreatQ的信息是威胁，则域地址会作为可应用到任何Umbrella策略的安全设置的一部分添加到ThreatQ目标列表。该策略会立即应用于使用带有ThreatQ目标列表的策略从设备发出的任何请求。

接下来，Umbrella会自动解析ThreatQ警报并将恶意站点添加到ThreatQ目标列表。这会将ThreatQ保护扩展到所有远程用户和设备，并为您的企业网络提供另一层实施功能。



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域添加到Global Allow List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，可以同时具有内部和外部记录。例如，“mail.myservicedomain.com”和“portal.myotherservicedomain.com”。
- 您依赖于Cisco Umbrella的基于云的应用不太为人所知，它不会包含在自动域验证中。例如，“localcloudservice.com”。

这些域可以添加到Global Allow List(全局允许列表)，该列表位于Cisco Umbrella中的Policies > Destination Lists（策略>目标列表）下。

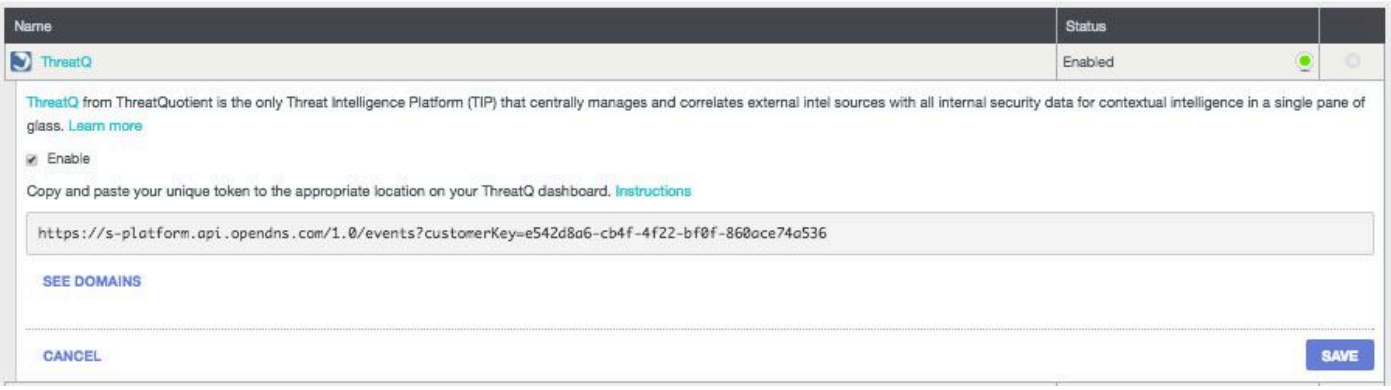
Umbrella脚本和API令牌生成

首先在Umbrella中查找您的唯一URL，以便ThreatQ设备与以下设备通信：

1.登录您的Umbrella控制面板。

2.定位至设置>集成，然后在表中选择ThreatQ以展开它。

3.选择启用，然后选择保存。这会在Umbrella中为组织生成唯一的特定URL。



稍后配置ThreatQ以向Umbrella发送数据时，您需要该URL，因此请复制URL并转至您的ThreatQ控制面板。

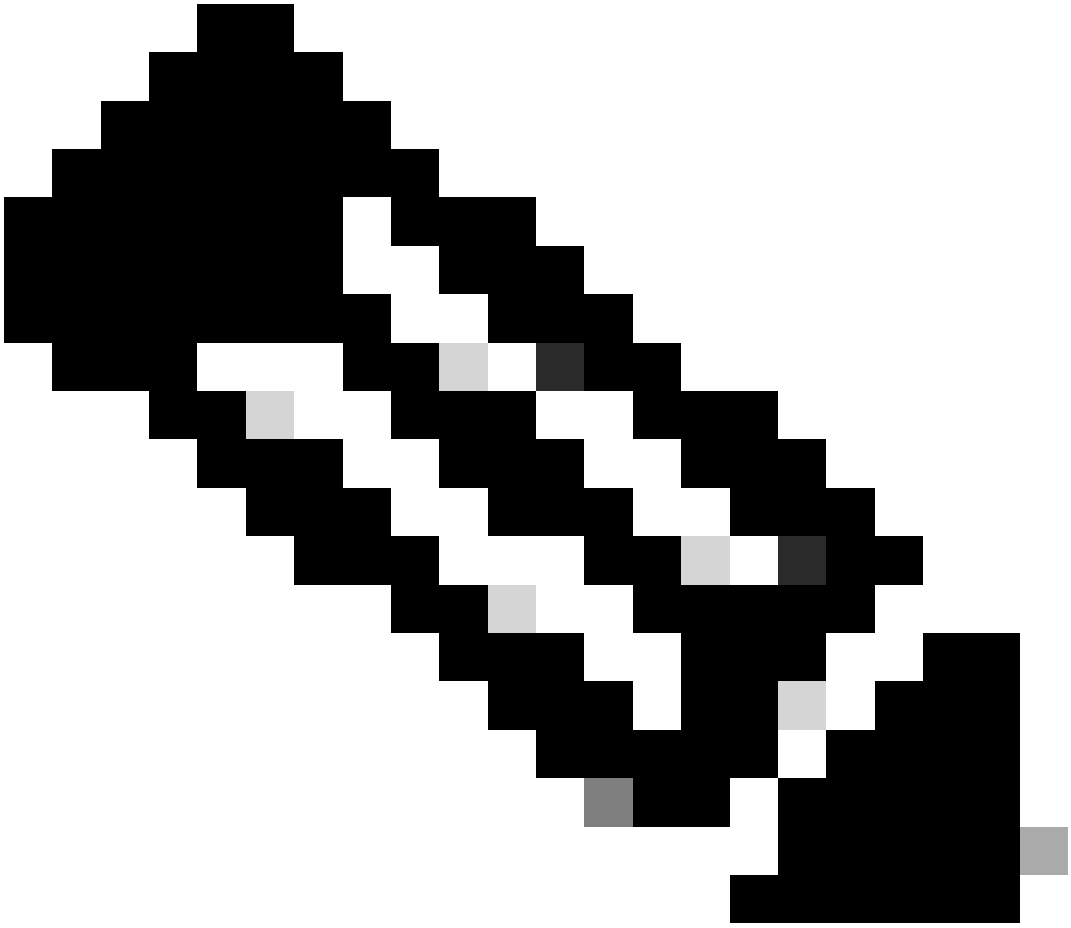
如何配置ThreatQ与Umbrella通信

登录您的ThreatQ控制面板并将URL添加到适当的区域以与Umbrella连接。

具体说明各不相同，如果您不确定如何或何处在ThreatQ中配置API集成，Umbrella建议联系ThreatQ支持。

在审核模式下观察添加到ThreatQ安全类别的事件

随着时间的推移，来自ThreatQ控制面板的事件开始填充可以作为ThreatQ安全类别应用到策略的特定目标列表。默认情况下，目标列表和安全类别处于审核模式，这意味着它们不应用于任何策略，且不会导致对现有Umbrella策略进行任何更改。



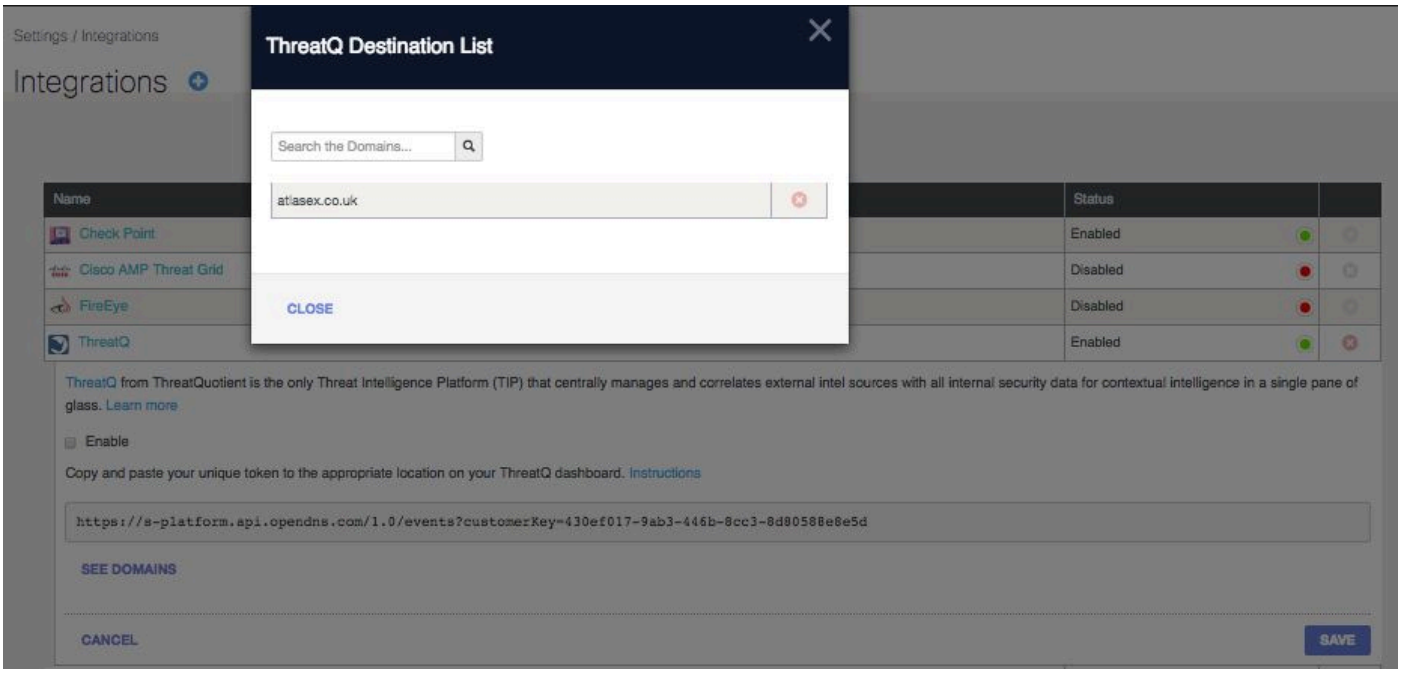
注意：可以启用审核模式，但根据您的部署配置文件和网络配置，审核模式需要多长时间。

查看目标列表

您可以随时查看Umbrella中的ThreatQ目标列表：

1.定位至设置>集成。

2.展开表中的ThreatQ，然后选择See Domains。



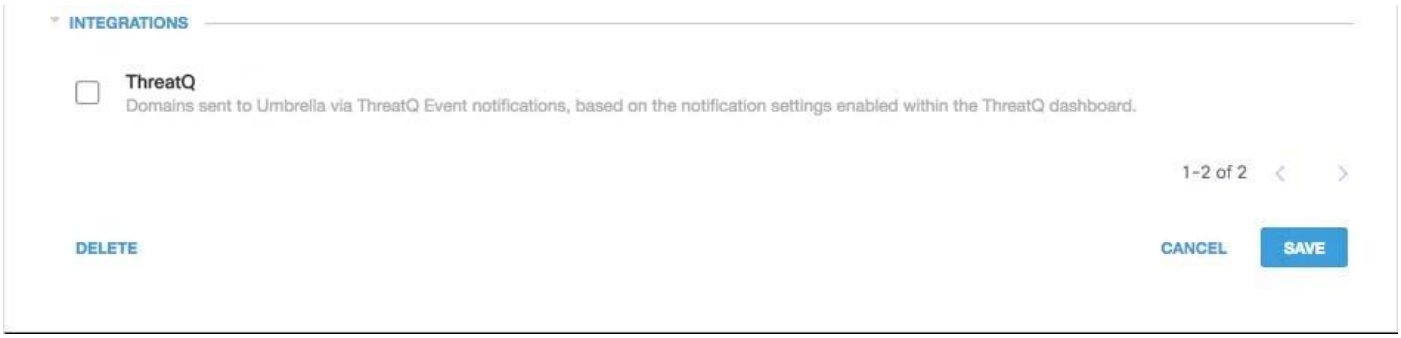
查看策略的安全设置

您可以随时查看可以为Umbrella中的策略启用的安全设置：

1.定位至策略>安全设置。

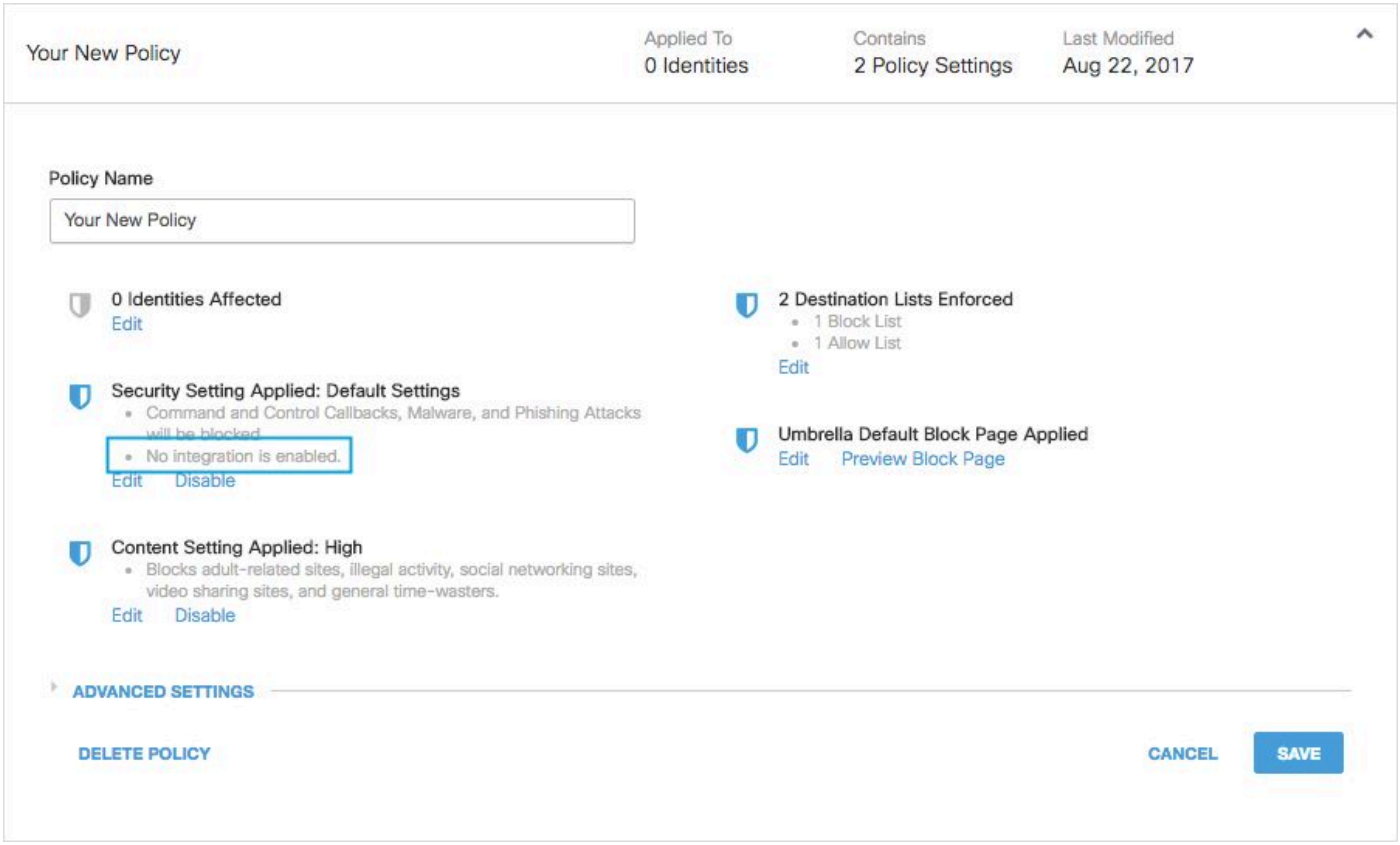
2.选择表中的安全设置将其展开。

3.滚动到集成以查找ThreatQ设置。



115014040286

您还可以通过Security Settings Summary页查看集成信息。



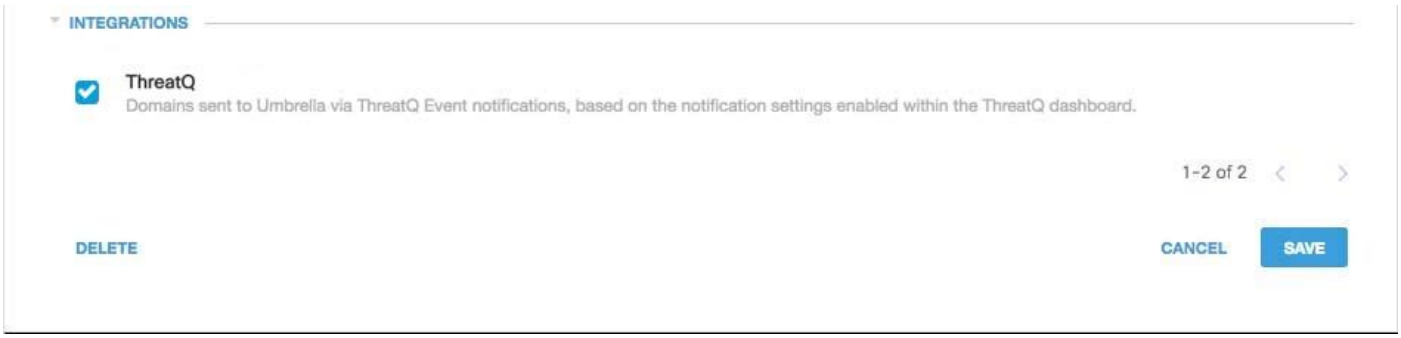
25464141748116

在阻止模式下将ThreatQ安全设置应用于托管客户端的策略

一旦您准备好让这些附加安全威胁由Umbrella管理的客户端实施，您可以更改现有策略的安全设置，或创建高于默认策略的新策略，以确保首先实施该策略：

1.导航到策略>安全设置。

2.在“集成”下，选择ThreatQ，然后选择保存。



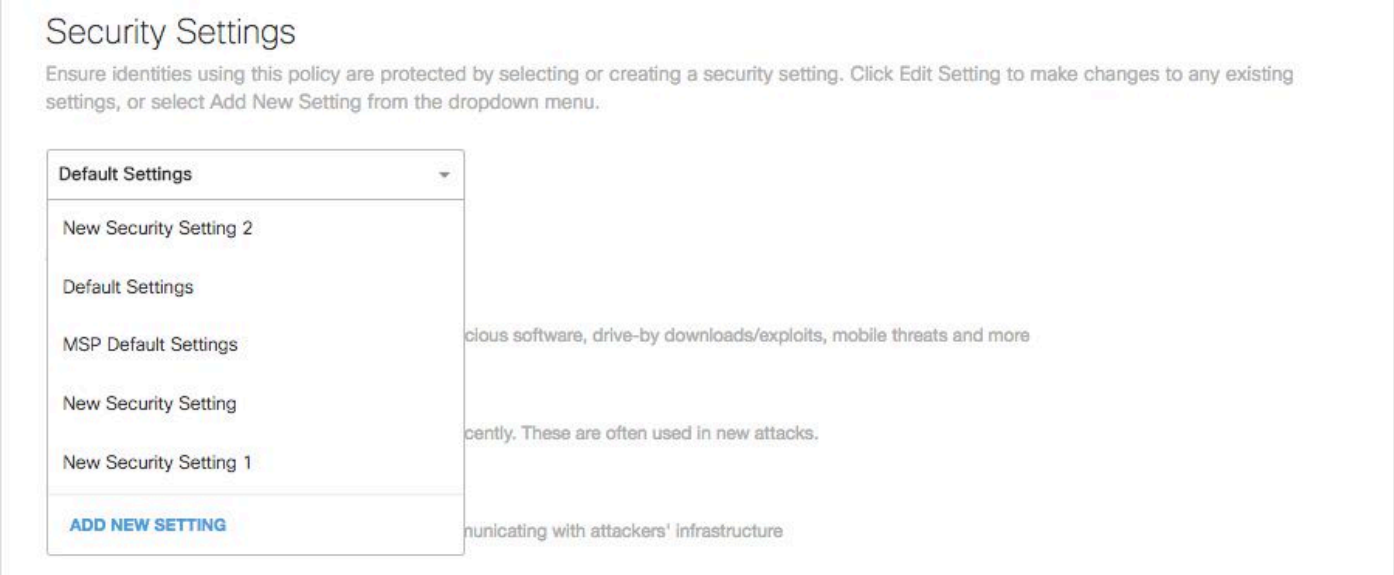
115014207403

接下来，在策略向导中，将安全设置添加到正在编辑的策略中：

1.定位至策略>策略列表。

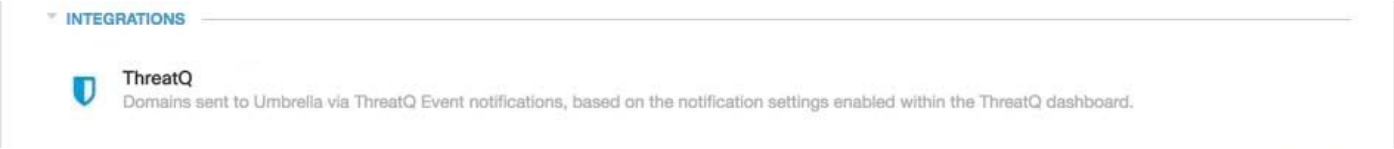
2.展开策略并在应用的安全设置下选择编辑。

3.在Security Settings下拉列表中，选择包含ThreatQ设置的安全设置。



25464141787668

“集成”(Integrations)下的屏蔽图标将更新为蓝色。



115014040506

4.选择Set & Return。

ThreatQ的安全设置中包含的ThreatQ域现在被阻止用于使用该策略的身份。

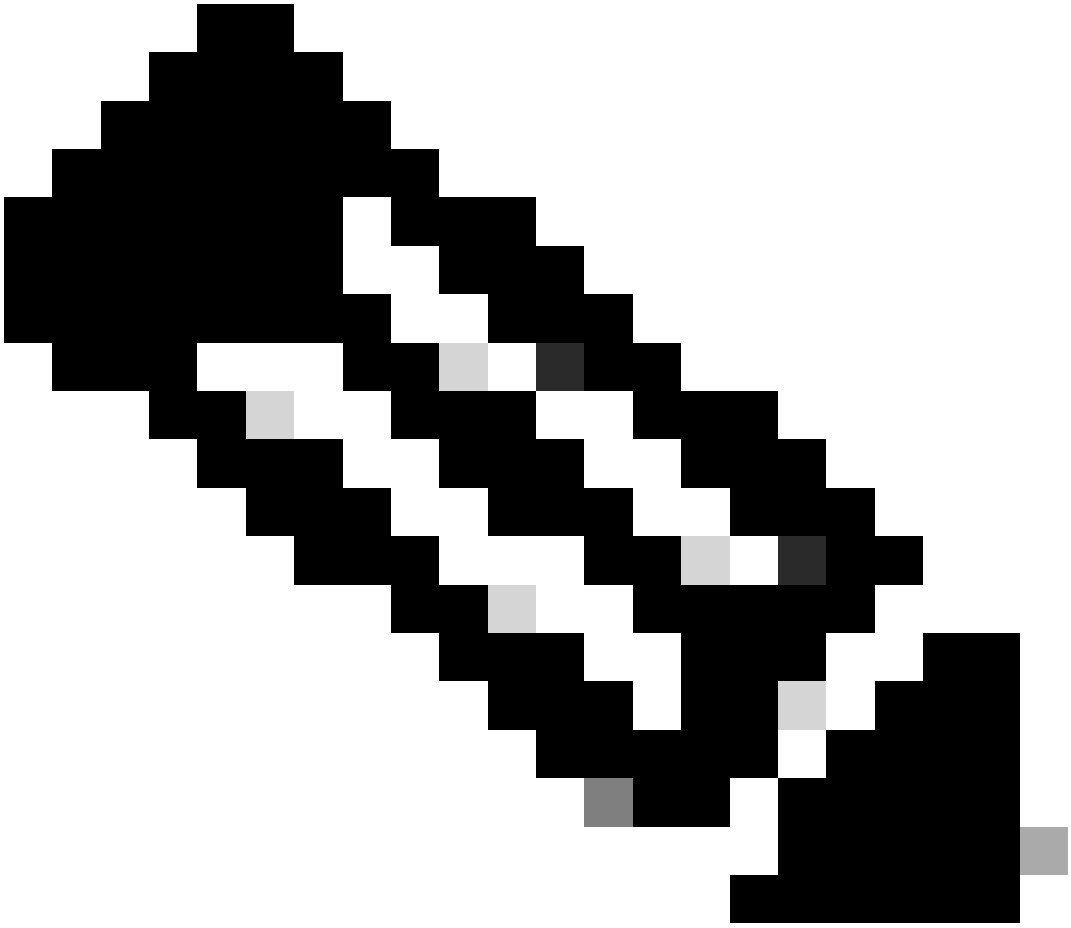
在Umbrella中报告ThreatQ事件

报告ThreatQ安全事件

ThreatQ Destination List是您可以报告的安全类别列表之一。大多数或所有报告将安全类别用作过滤器。例如，您可以过滤安全类别，以便仅显示与ThreatQ相关的活动。

1.定位至“报告”>“活动搜索”。

2.在Security Categories下，选择ThreatQ以过滤报告，以便仅显示ThreatQ的安全类别。



注意：如果禁用了ThreatQ集成，则它不会出现在安全类别过滤器中。

115014207603

3.选择Apply。

报告域添加到ThreatQ目标列表的时间

Umbrella Admin Audit日志包含ThreatQ控制面板中的事件，因为它将域添加到目标列表。名为“ThreatQ帐户”（也带有ThreatQ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。Umbrella Admin Audit日志位于Reporting > Admin Audit Log。

通过为ThreatQ帐户用户应用过滤器，您可以过滤以仅包含ThreatQ更改。

处理不需要的检测或误报

允许列表

虽然不太可能，但ThreatQ自动添加的域可能会触发不必要的阻止，阻止用户访问特定网站。在这种情况下，Umbrella建议向允许列表添加域，该列表优先于所有其他类型的阻止列表，包括安全设置。

此方法更可取有两个原因：

- 首先，如果ThreatQ控制面板在删除域后再次重新添加该域，则允许列表可防止引起进一步问题的情况发生。
- 其次，允许列表显示问题域的历史记录，可用于调查分析或审计报告。

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。

如果阻止模式中的ThreatQ安全设置仅应用于托管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允许列表。

要创建允许列表，请执行以下操作：

1.定位至策略>目标列表，然后选择添加图标。

2.选择允许，然后将您的域添加到列表中。

3.选择保存。

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

从ThreatQ目标列表中删除域

在ThreatQ Destination List中的每个域名旁边都有一个Delete图标。通过删除域，您可以在出现不需要的检测时清除ThreatQ目标列表。但是，如果ThreatQ控制面板将域重新发送到Cisco Umbrella，则删除操作不是永久的。

删除域的步骤：

1.定位至“设置”>“集成”，然后选择ThreatQ将其展开。

2.选择查看域。

3.搜索要删除的域名。

4.选择删除图标。

5.选择关闭。

6.选择保存。

在意外检测或误报的情况下，Umbrella建议立即在Umbrella中创建允许列表，然后在ThreatQ控制面板中修复误报。稍后，您可以从ThreatQ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）。