将ZeroFOX与Umbrella集成

目录

简介

本文档介绍如何将ZeroFOX Enterprise与Umbrella集成，以便可以将安全事件应用于受Umbrella保护的客户端。

ZeroFOX Enterprise和Cisco Umbrella集成概述

通过将ZeroFOX Enterprise与Cisco Umbrella集成，安全人员和管理员可以针对漫游的笔记本电脑、平板电脑或电话的当今基于社交媒体的威胁提供保护，同时为分布式企业网络提供另一层实施措施。

Cisco Umbrella和ZeroFox集成：此计划如何运作？

ZeroFOX Enterprise将其发现的任何威胁（例如基于社交媒体的网络威胁，包括针对性恶意软件、网络钓鱼、社交工程、模拟和其他欺诈或恶意活动）推送到Cisco Umbrella，以便在全球范围内实施。

然后，Umbrella验证威胁以确保将其添加到策略中。如果确认来自ZeroFOX的信息是威胁，则域地址会作为可应用于任何Umbrella策略的安全设置的一部分添加到ZeroFOX目标列表。该策略会立即应用于从分配给该策略的设备发出的任何请求。

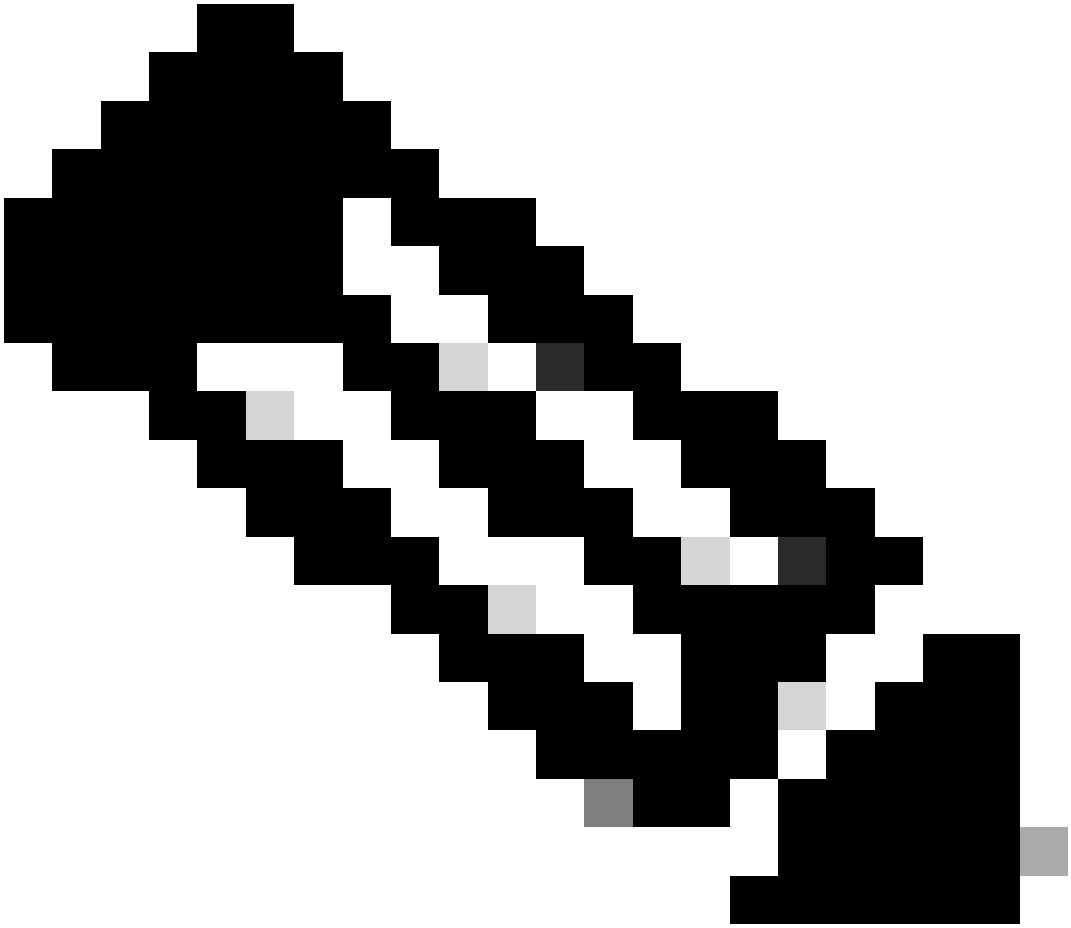
今后，Cisco Umbrella会自动解析ZeroFOX警报并将恶意站点添加到ZeroFOX目标列表，从而将ZeroFOX智能扩展到所有远程用户和设备，并为您的企业网络提供另一层实施。

这可通过以下简单的设置步骤实现：

1. 在Umbrella中启用集成以生成API令牌。
2. 将该API令牌粘贴到您的ZeroFOX帐户中。
3. 将ZeroFOX设置为在所需策略的安全设置下阻止

先决条件

- ZeroFOX Enterprise管理权限
- Umbrella控制面板管理权限
- Umbrella控制面板必须启用ZeroFOX集成



注意：ZeroFOX集成仅包含在Umbrella Platform软件包中。如果您没有平台软件包并且希望集成ZeroFOX，请联系您的Cisco Umbrella代表。如果您有平台软件包，但没有将ZeroFOX视为控制面板集成，请与Umbrella支持部门联系。

重要信息：虽然Umbrella会尽力验证和允许已知安全域（例如Google和Salesforce），以避免任何不需要的中断，我们建议根据您的策略将您不希望阻止的任何域添加到Global Allow List或其他目标列表。

示例包括：

- 您组织的主页。例如，mydomain.com。
- 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。
- 您严重依赖的鲜为人知的云应用，Umbrella无法感知或在其自动域验证中包括这些应用。例如，localcloudservice.com。

全局允许列表位于Umbrella中的Policies > Destination Lists。有关详细信息，请参阅我们的文档：管理目标列表

步骤 1：Umbrella脚本和API令牌生成

首先在Umbrella中查找您的唯一URL，以便ThreatQ设备与之通信。

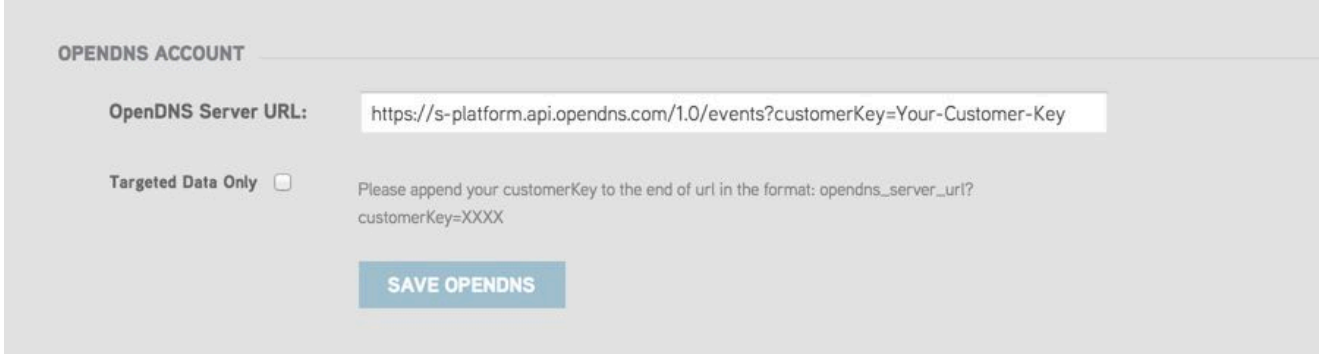
1. 以Admin身份登录到Umbrella控制面板，导航到Settings > Integrations，然后点击表中的“ZeroFOX”将其展开。
2. 选中Enable，然后单击Save。这会生成带有客户密钥的唯一URL。

以后配置ZeroFOX时需要URL，因此请复制URL并转到您的ThreatQ控制面板。

步骤 2：设置ZeroFOX企业控制面板以向Umbrella发送信息

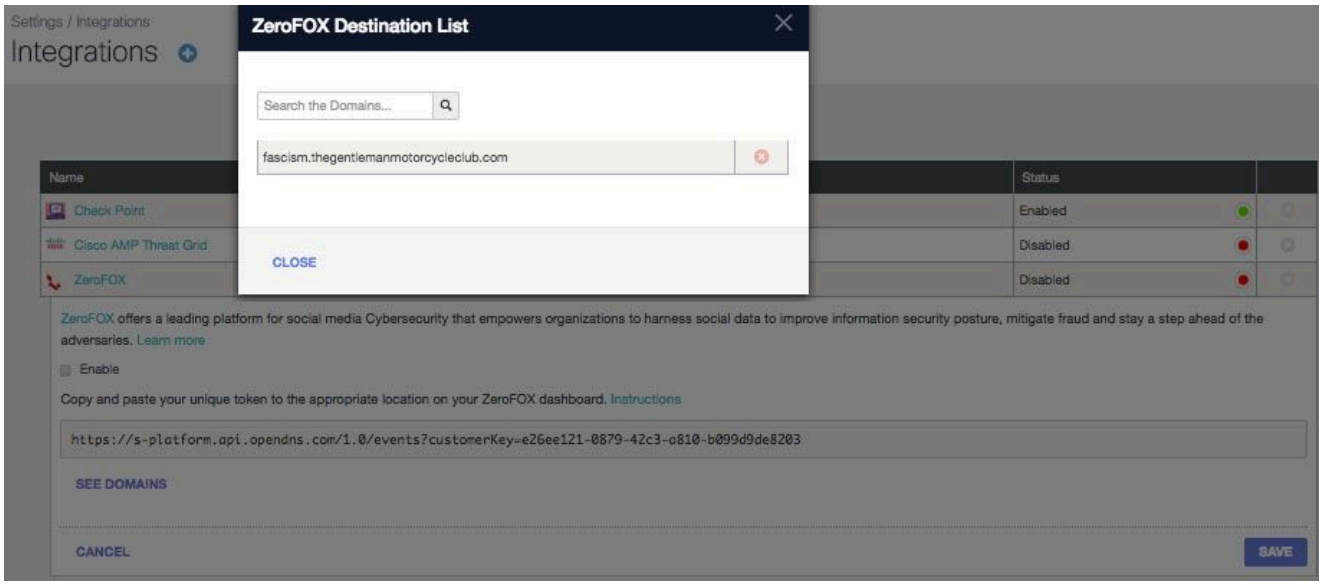
下一步是将您在步骤1中复制的URL添加到ZeroFOX控制面板。

1. 单击Zerofox控制面板中的齿轮图标，然后选择Account Settings。
2. 向下滚动集成列表，直到您看到OpenDNS Account信息，然后将Umbrella中的URL粘贴到OpenDNS Server URL字段。
3. 在首次启用集成后，我们建议您选中Targeted Data Only(仅限目标数据)。



步骤 3：在Umbrella内设置要阻止的ZeroFOX事件

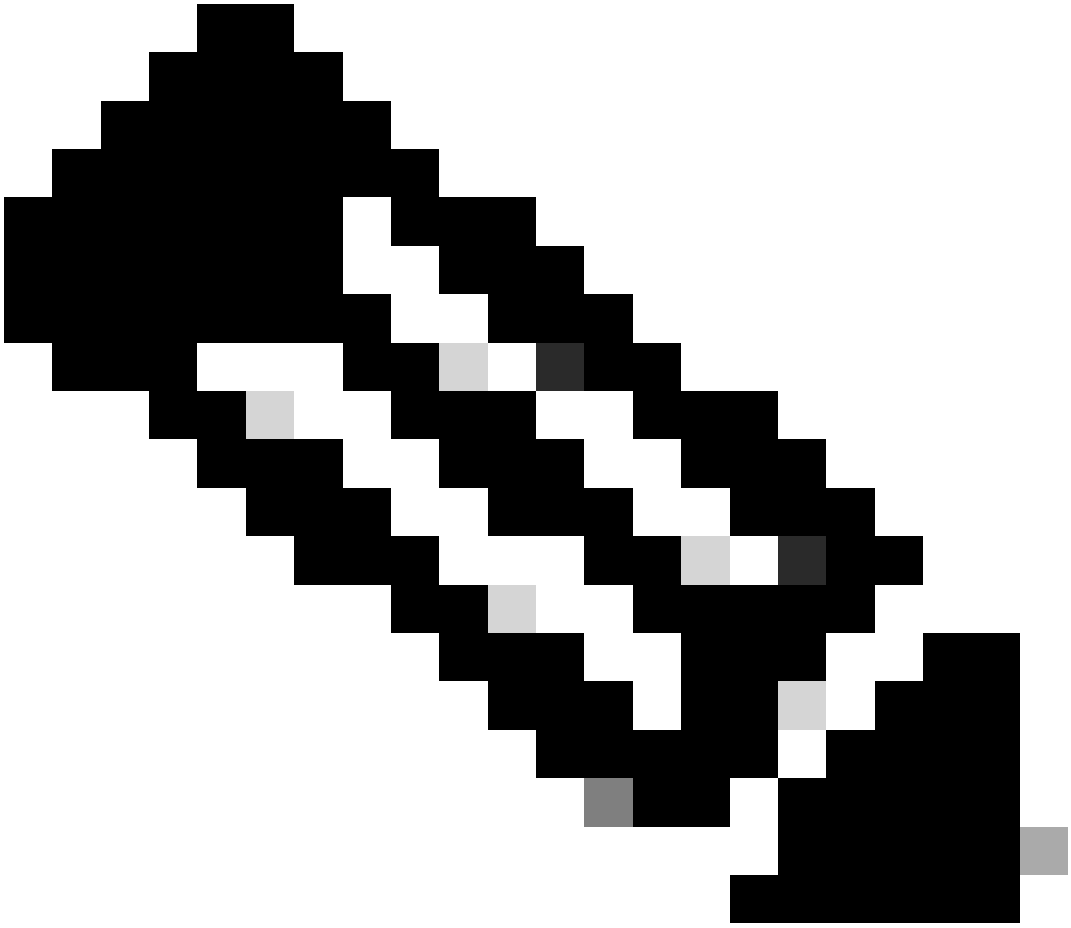
1. 以管理员身份重新登录到Umbrella控制面板。
2. 导航到设置>集成，然后单击表中的“ZeroFOX”将其展开。
3. 单击See Domains。
   这将展开一个域列表，其中包括来自您的ZeroFOX帐户的最后几个小时事件。从那时起，可搜索列表开始填充和增长。



下一步是观察和审核添加到新ZeroFOX安全类别的事件。

观察在审核模式下添加到ZeroFOX安全类别的事件

ZeroFOX Enterprise中的事件开始填充可以作为ZeroFOX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，不应用于任何策略，也不会导致对现有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

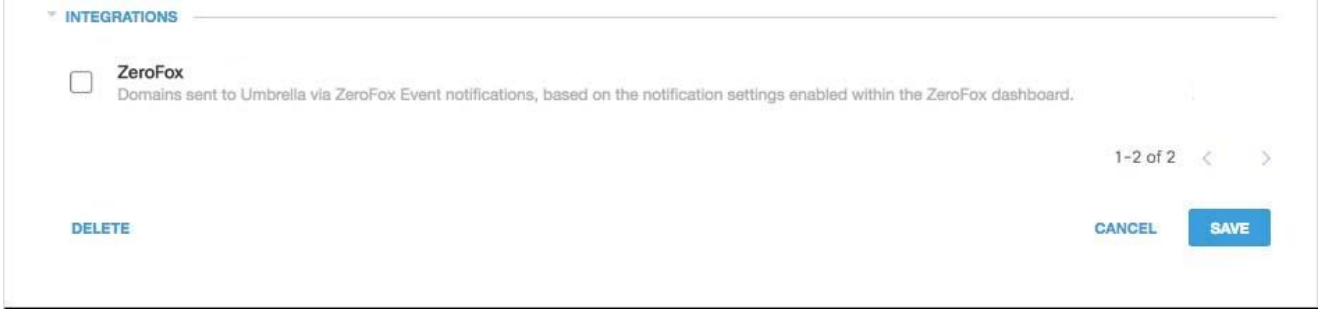
您可以随时查看ZeroFox目标列表。

1. 导航到设置>集成。
2. 展开表中的“ZeroFOX”，然后点击See Domains。

查看策略的安全设置

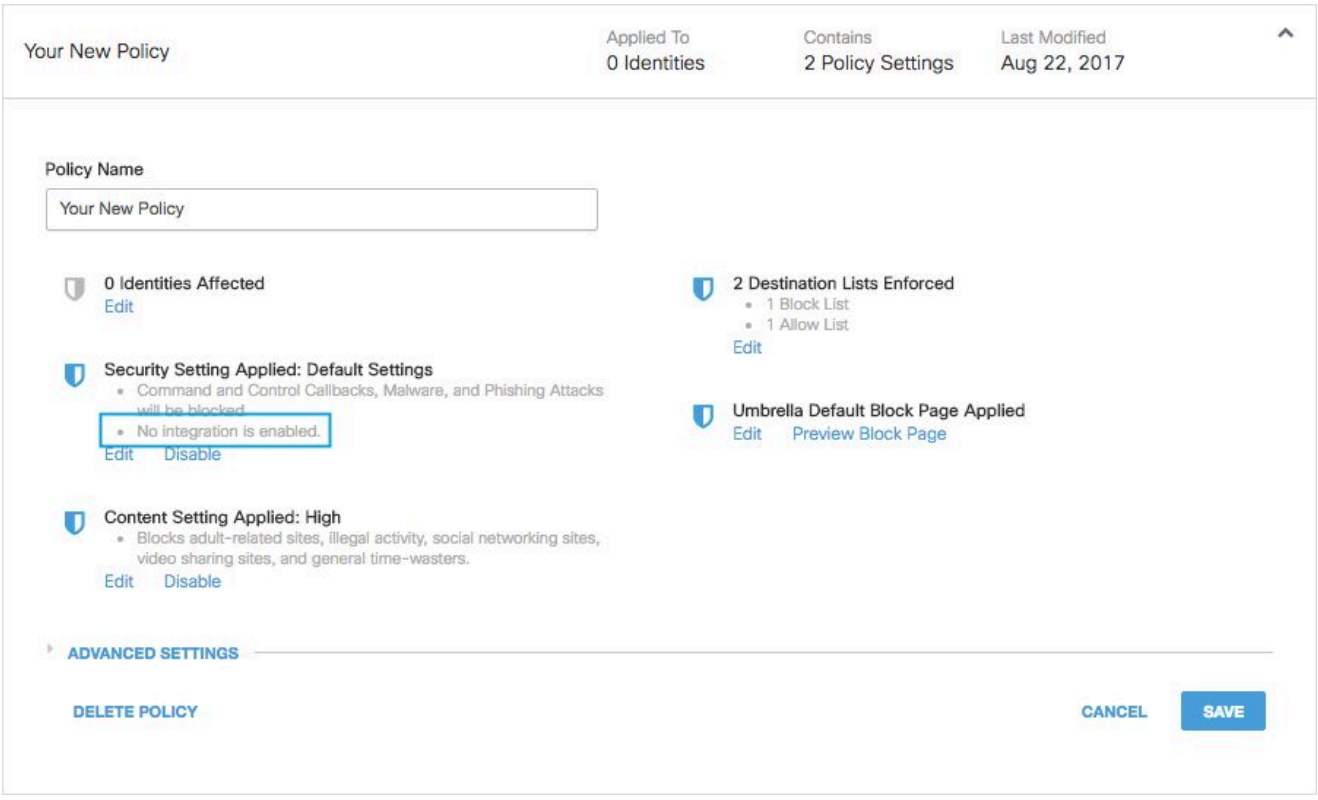
您可以随时查看可以为策略启用的安全设置。

1. 导航到策略>安全设置。
2. 单击表中的安全设置将其展开，然后滚动到Integrations以查找ZeroFOX设置。



115014041606

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

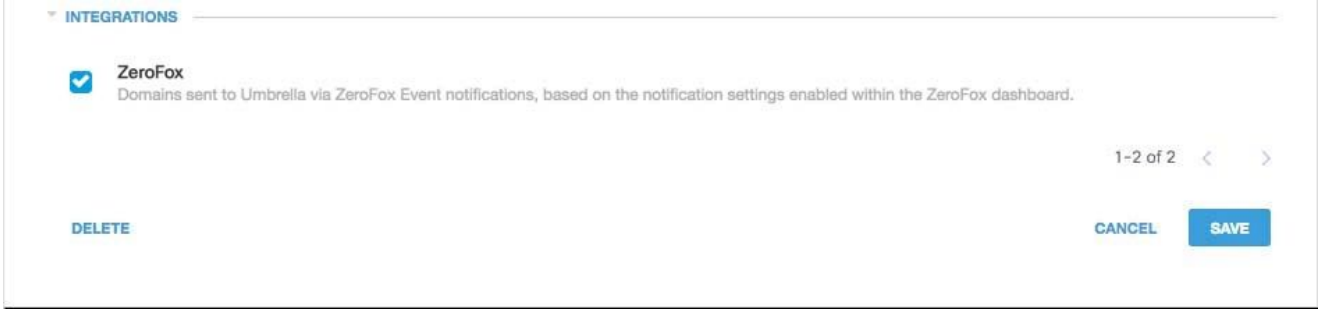


25464154913556

在阻止模式下将ZeroFOX安全设置应用于托管客户端的策略

当您准备好让这些附加安全威胁由Umbrella管理的客户端实施后，只需更改现有策略的安全设置，或创建一个高于默认策略的新策略，以确保首先实施该策略。

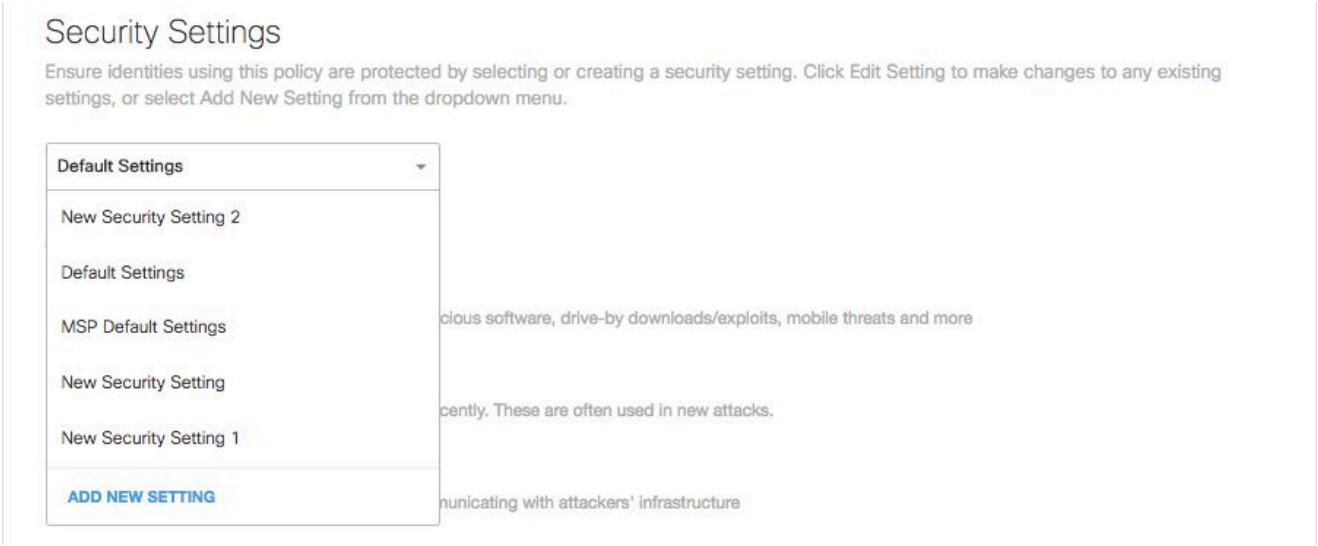
1. 导航到Policies > Security Settings，然后在Integrations下选中ZeroFOX，然后单击Save。



115014042806

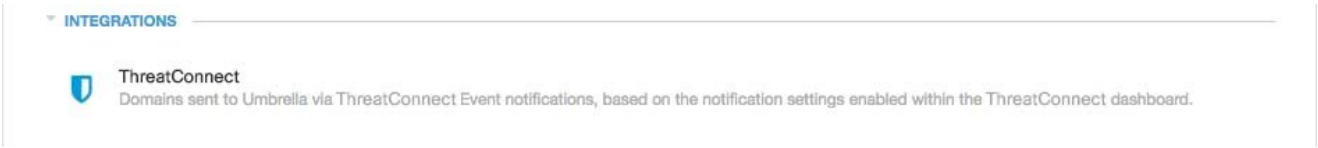
接下来，在策略向导中，将安全设置添加到正在编辑的策略中：

1. 导航到Policies > Policy List。
2. 展开策略并点击Security Setting Applied下的Edit。
3. 在Security Settings下拉列表中，选择包含ThreatConnect设置的安全设置。



25464147943700

Integrations下的屏蔽图标将更新为蓝色。



25464147957652

4. 单击Set & Return。

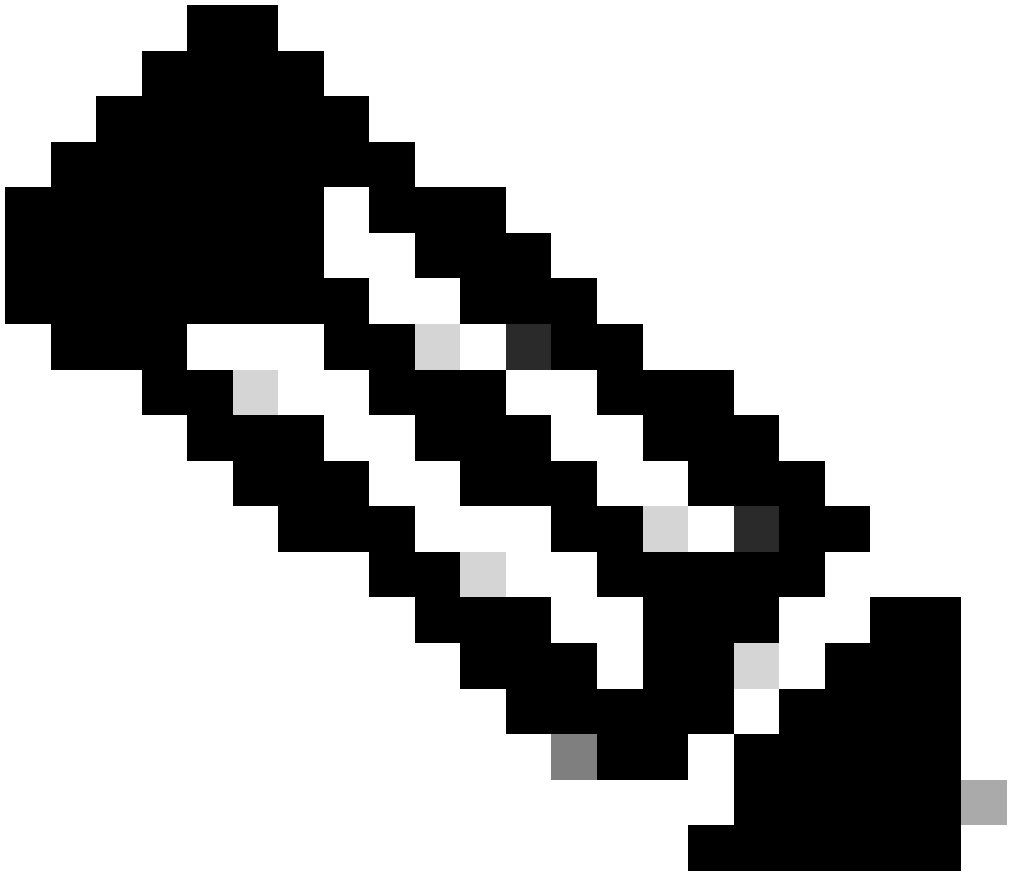
ZeroFOX的安全设置中包含的ZeroFOX域对于使用该策略的那些标识被阻止。

ZeroFOX事件的Umbrella中的报告

报告ZeroFOX安全事件

ZeroFOX Destination List是可以报告的其中一个安全类别列表。大多数或所有报表都使用安全类别作为筛选器。例如，您可以筛选安全类别，以便仅显示与ZeroFOX相关的活动。

1. 导航到Reporting > Activity Search，并在Security Categories下选择ZeroFOX以过滤报告，以便只显示ZeroFOX的安全类别。



注意：如果禁用了ZeroFOX集成，则它不会出现在安全类别过滤器中。

115014043046

2. 单击 Apply。

报告域添加到ZeroFOX目标列表的时间

Umbrella Admin Audit日志包含来自ZeroFOX帐户的事件，因为它将域添加到目标列表。

Umbrella Admin Audit日志位于Reporting > Admin Audit Log。要报告添加域的时间，请通过将过滤器应用于ZeroFox目标列表的标识和设置，进行过滤，以仅包含ZeroFOX更改。

运行报告后，您会看到从集成添加ZeroFOX目标列表时所进行的更改的列表。

处理不需要的检测或误报

管理不需要的检测的允许列表

虽然不太可能，但ZeroFOX自动添加的域可能会触发一个不需要的阻止，阻止用户访问特定网站。

在这种情况下，我们建议将域添加到允许列表，该列表优先于所有其他类型的阻止列表，包括安全设置。当两个域中都存在域时，允许列表优先于阻止列表。

此方法更可取有两个原因。首先，如果ZeroFOX设备在删除域后再次重新添加该域，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。

如果块模式中的ZeroFOX安全设置仅应用于受管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。

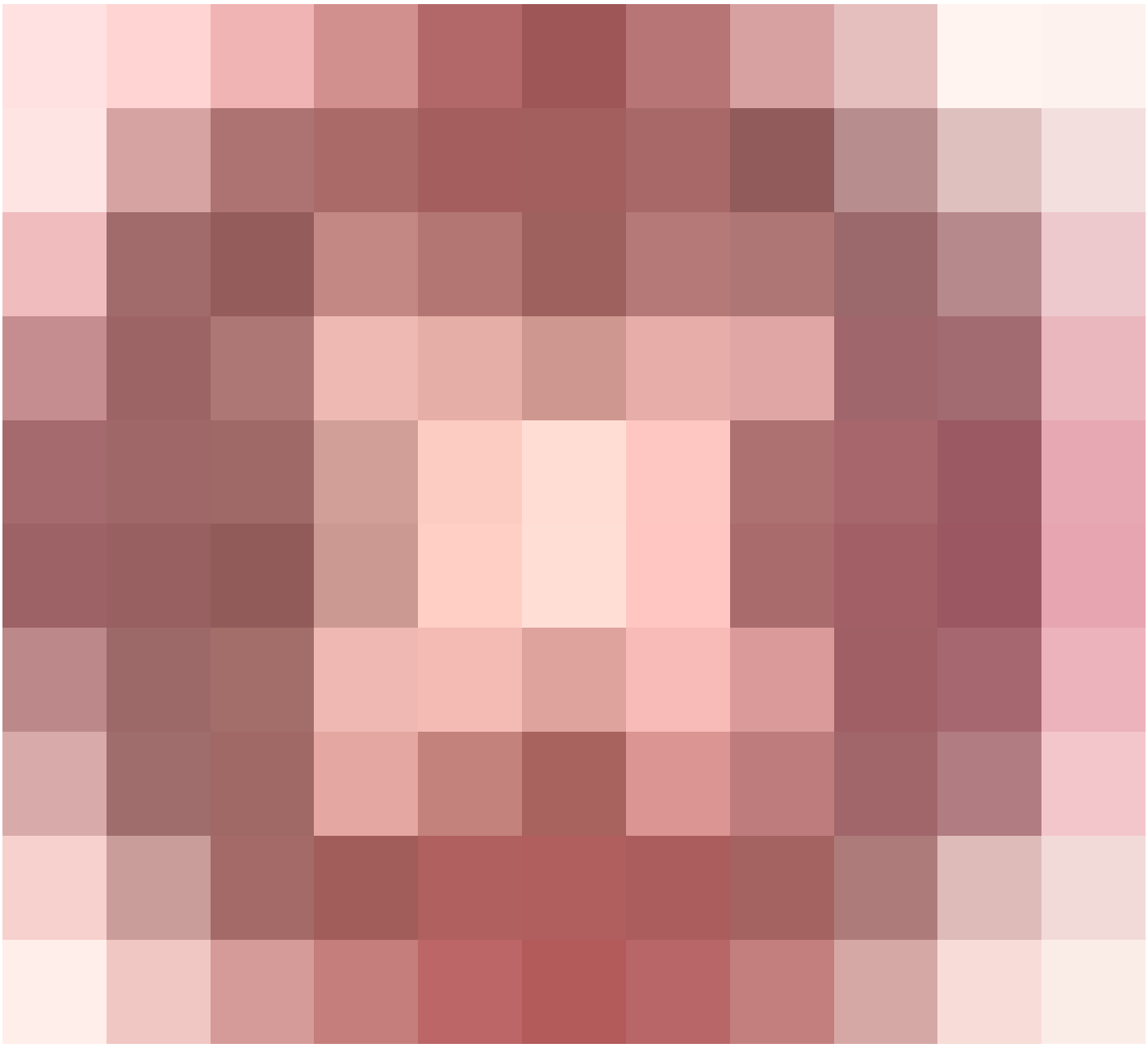
要创建允许列表，请执行以下操作：

1. 导航到Policies > Destination Lists，点击 
   25464155856404
   添加图标。
2. 选择允许，然后将您的域添加到列表中。
3. Click Save.

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ZeroFOX目标列表中删除域

有一个



ZeroFOX Destination列表中每个域名旁边的（删除）图标。通过删除域，可以在出现意外检测时清除ZeroFOX目标列表。

但是，如果ZeroFOX将域重新发送到Umbrella，则删除操作不是永久性的。

删除域的步骤：

1. 导航到设置>集成，然后单击“ZeroFOX”将其展开。
2. 单击See Domains。
3. 搜索要删除的域名。
4. 单击Delete图标。

5. 单击 Close。
6. Click Save.

对于不需要的检测或误报，我们建议立即在Umbrella中创建允许列表，然后在ZeroFOX中修复误报。稍后，您可以从ZeroFOX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）。