集成伞和FireEye

目录

简介

本文档介绍如何将Cisco Umbrella与FireEye集成。

先决条件

要求

Cisco 建议您了解以下主题：

- 可访问公共互联网的FireEye设备。
- Cisco Umbrella Dashboard管理权限。
- Cisco Umbrella Dashboard必须启用FireEye集成。

使用的组件

本文档中的信息基于Cisco Umbrella。

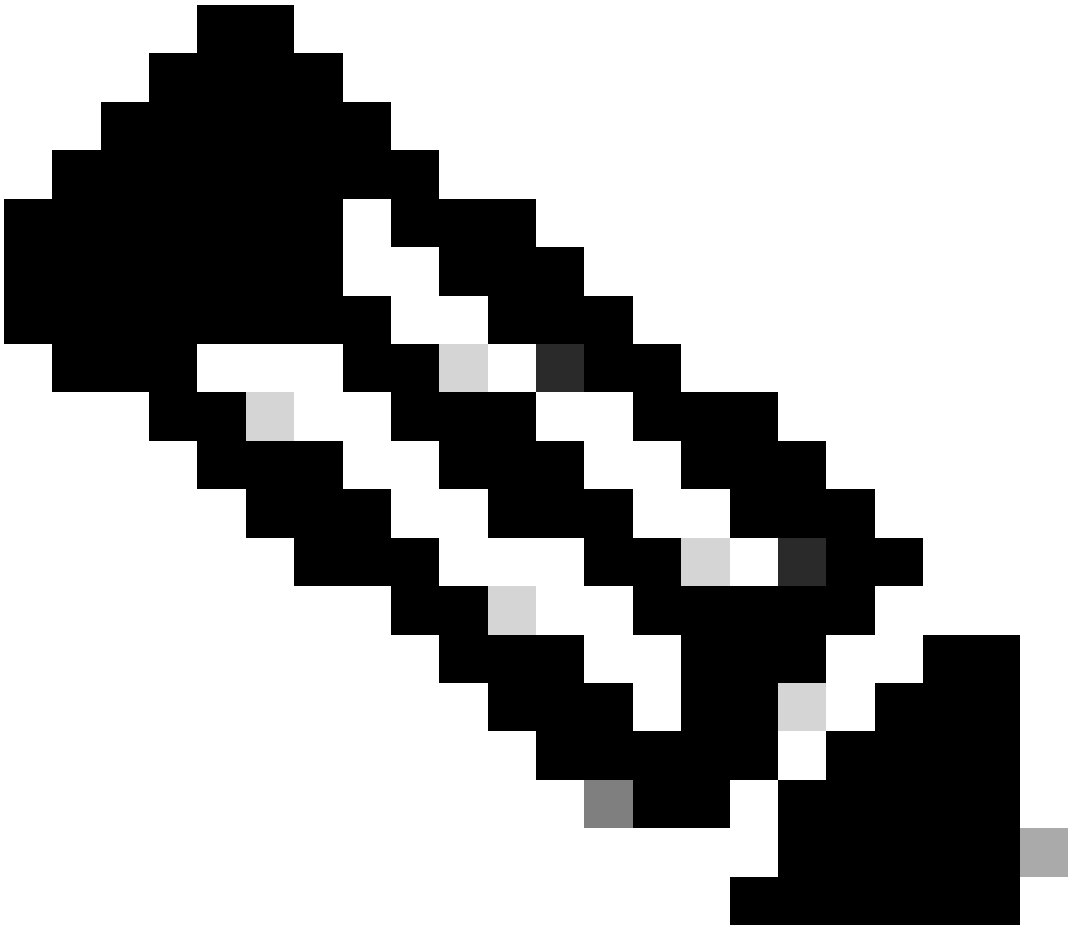
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

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。

概述

通过FireEye安全设备和Cisco Umbrella之间的集成，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FireEye以与Cisco Umbrella通信，以便将FireEye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。



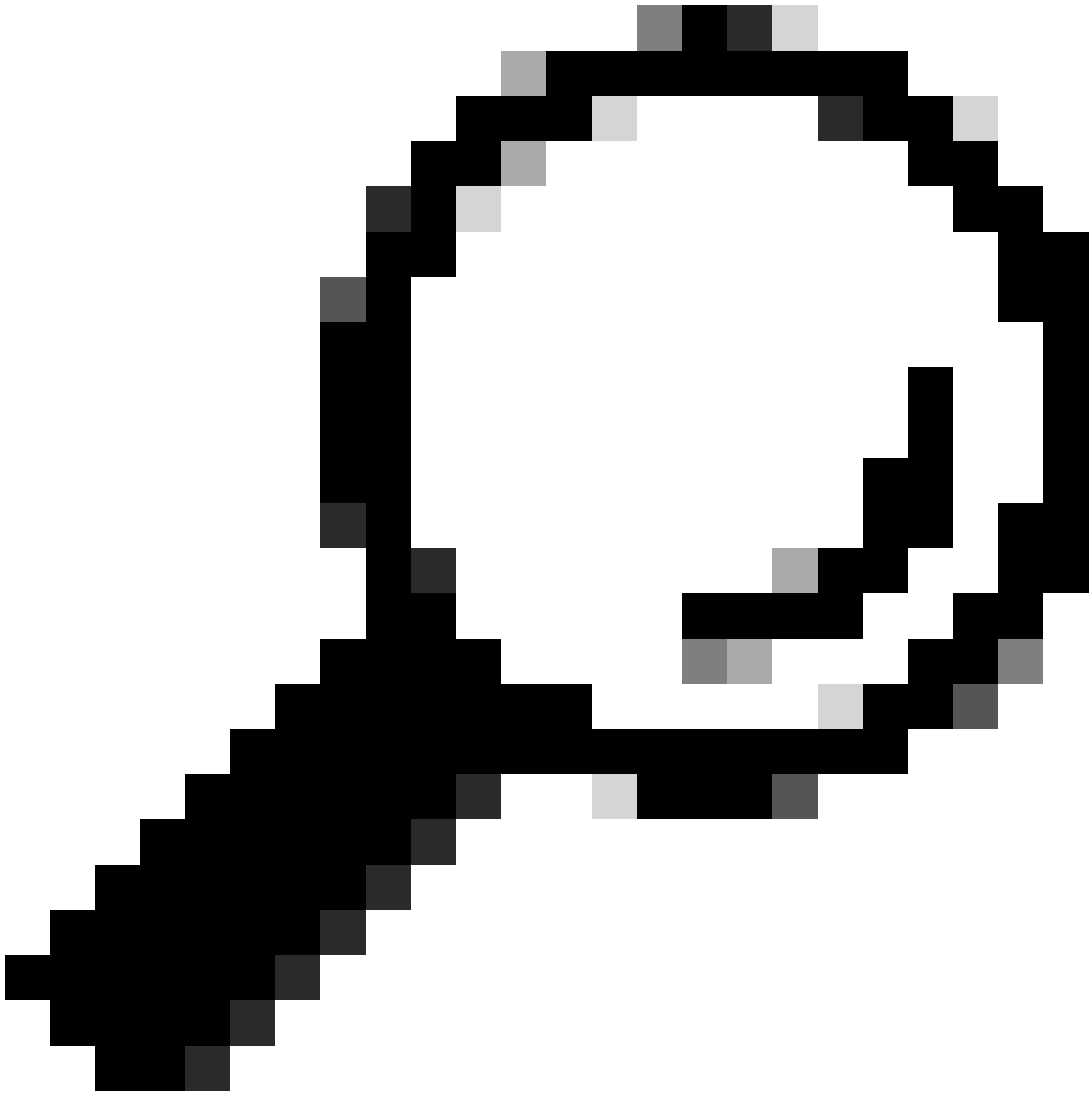
注意：FireEye集成仅包含在Cisco Umbrella包中，例如DNS Essentials、DNS Advantage、SIG Essentials或SIG Advantage。如果您没有这些软件包之一，并且希望集成FireEye，请联系您的思科Umbrella客户经理。如果您有正确的Cisco Umbrella软件包，但是没有将FireEye视为控制面板集成，请与Cisco Umbrella支持联系。

集成功能

FireEye设备首先将其发现的基于互联网的威胁（例如托管恶意软件的域、僵尸网络的命令和控制或网络钓鱼站点）发送到Cisco Umbrella。

然后，Cisco Umbrella验证传递到Cisco Umbrella的信息，以确保其有效并可添加到策略中。如果确认来自FireEye的信息格式正确（例如，它不是文件、复杂的URL或高度流行的域），则域地址会作为可应用于任何Cisco Umbrella策略的安全设置的一部分添加到FireEye目标列表。该策略会立即应用于使用具有FireEye目标列表的策略从设备发出的任何请求。

接下来，Cisco Umbrella会自动解析FireEye警报，并将恶意站点添加到FireEye目标列表。这会将FireEye保护扩展到所有远程用户和设备，并为您的公司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。

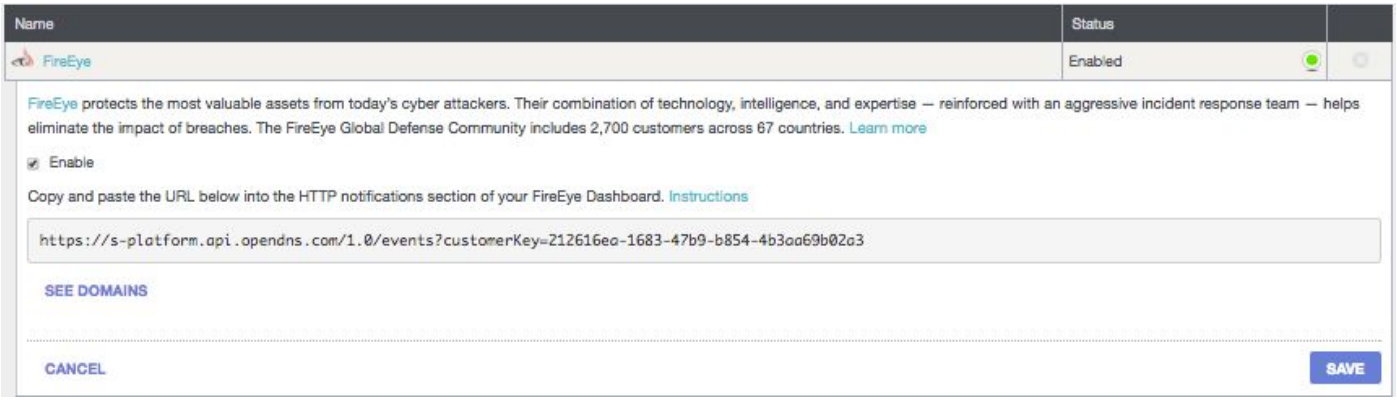
配置Cisco Umbrella控制面板以从FireEye接收信息

第一步是在Cisco Umbrella中查找您的唯一URL，以便FireEye设备与之通信。

1.以管理员身份登录Cisco Umbrella Dashboard。

2.定位至策略>策略组件>集成，然后在表中选择FireEye以展开它。

3.选择启用框，然后选择保存。这会为您在Cisco Umbrella中的组织生成一个唯一的特定URL。

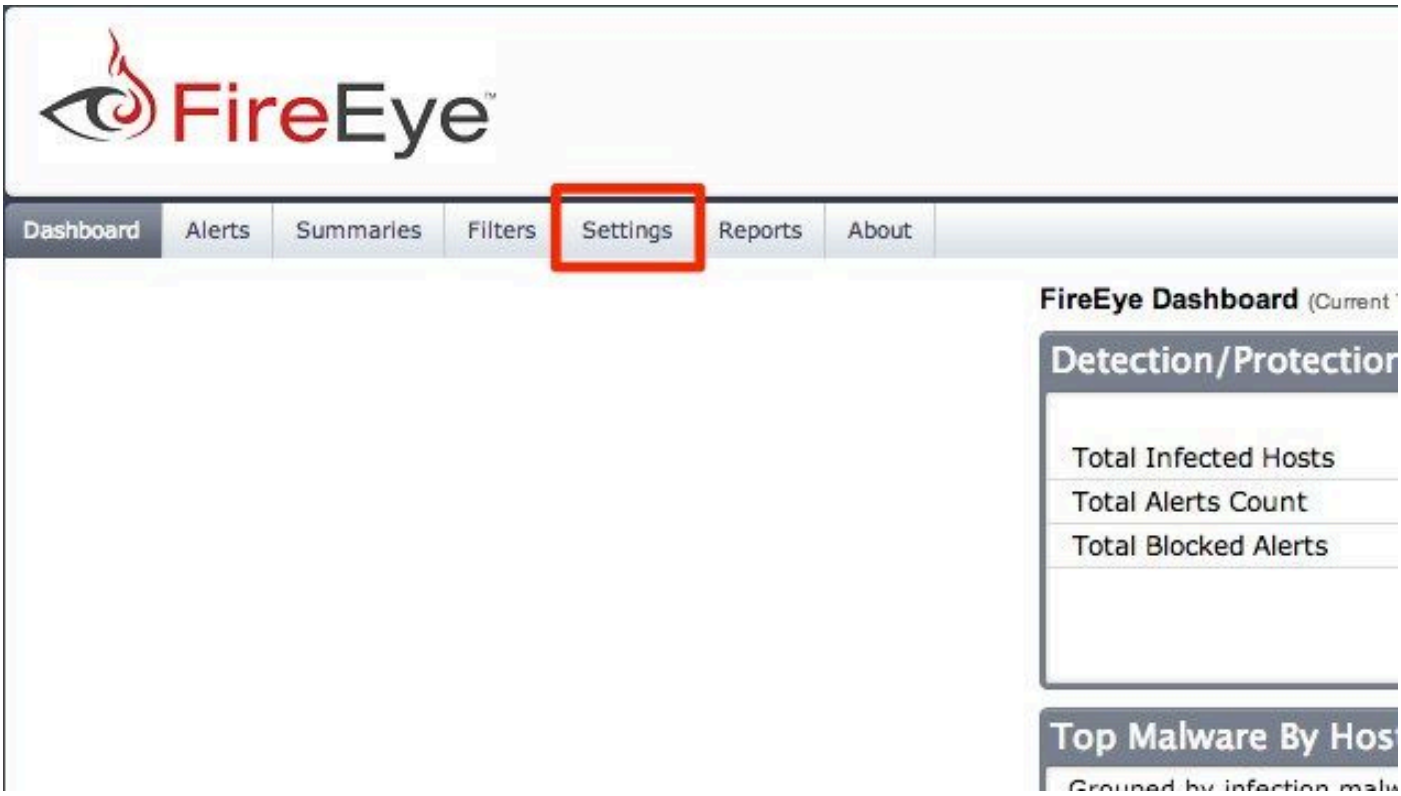


您可以稍后使用此URL配置FireEye设备以向Cisco Umbrella发送数据，因此请务必复制URL。

配置FireEye与Cisco Umbrella通信

要开始将流量从FireEye设备发送到Cisco Umbrella，您必须使用上一节中生成的URL信息配置FireEye。

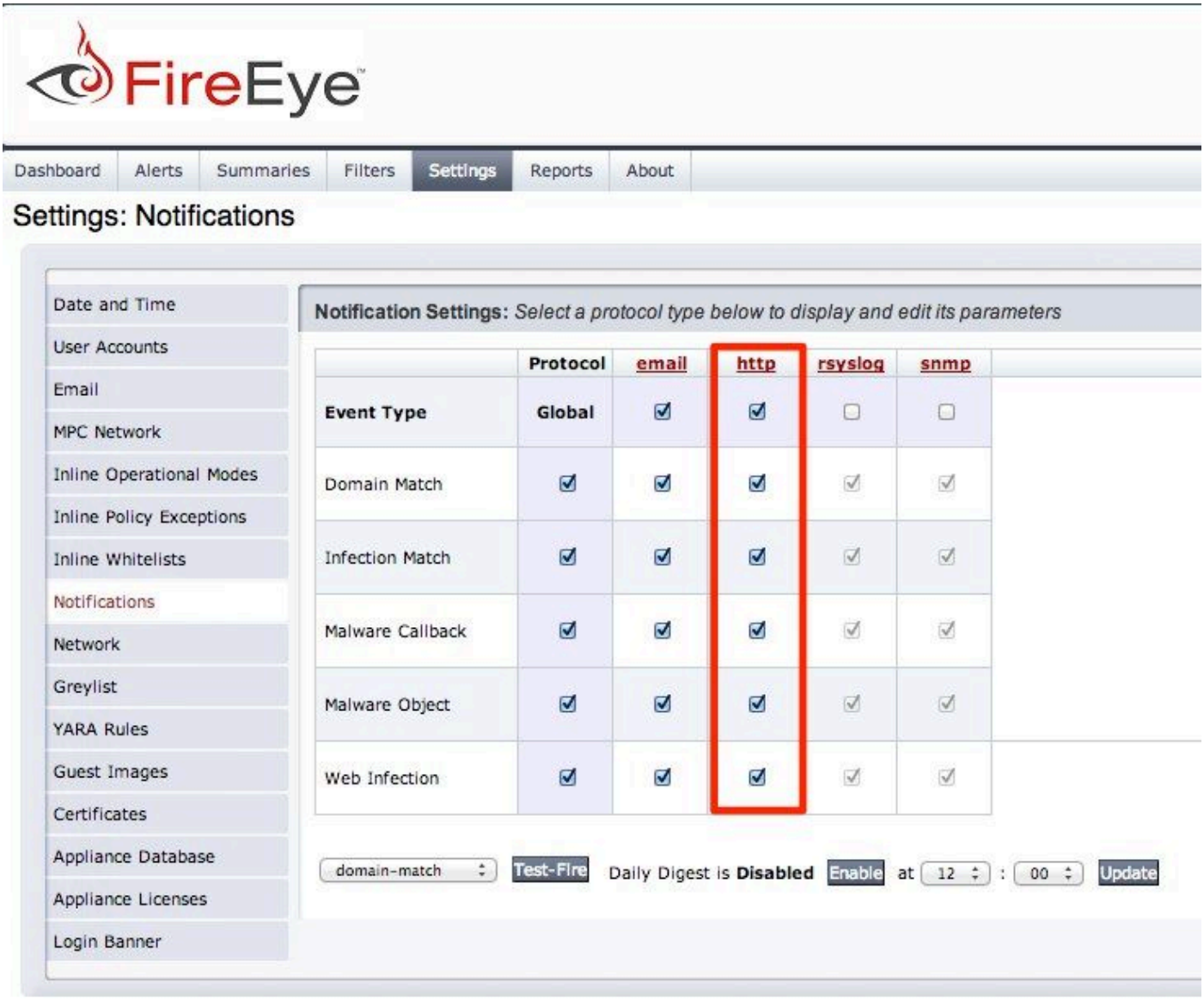
1.登录到FireEye，然后选择设置。



2.从设置列表中选择通知:

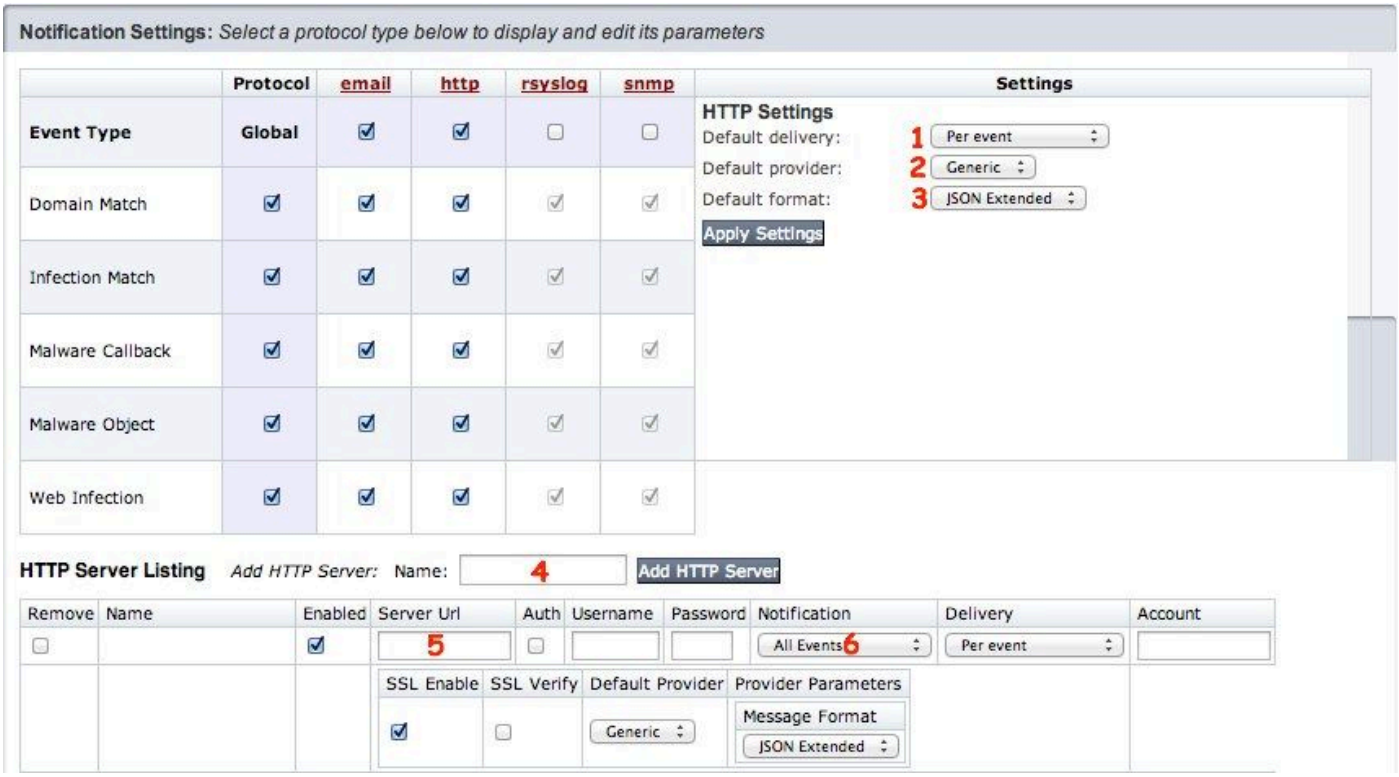

FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance Licenses
Login Banner
Date and Time Settings
Manually set the date, time, and time zone. Or, op
synchronization.
(Current Time: 11/11/13 17:29:24 UTC)
Set Manually:
November
11
2013
17
Enable NTP:
Add NTP Server:
NTP Server
Delete
Update T
pool.ntp.org
Update T
time.nist.gov
Update T
Remove Selected NTP Servers
Set Time Zone:
UTC
Set Time Zone

3.确保选中要发送到Cisco Umbrella的所有事件类型（Umbrella建议从all开始），然后选择列顶部的HTTP链接。



4.在菜单展开时，选择这些选项以启用“事件通知”。屏幕截图概述了采用数字编号的步骤：

1. 默认传送：每个事件
2. 默认提供程序：通用
3. 默认格式：扩展的JSON
4. 将HTTP服务器命名为“OpenDNS”。
5. 服务器 URL：粘贴您在此之前从Cisco Umbrella控制面板生成的Cisco Umbrella URL。
6. 通知下拉列表：选择All Events以确保最大覆盖范围。



5.确保Delivery、Default Provider和Provider Parameters下拉列表均与默认设置匹配，或者如果使用了多个通知服务器：

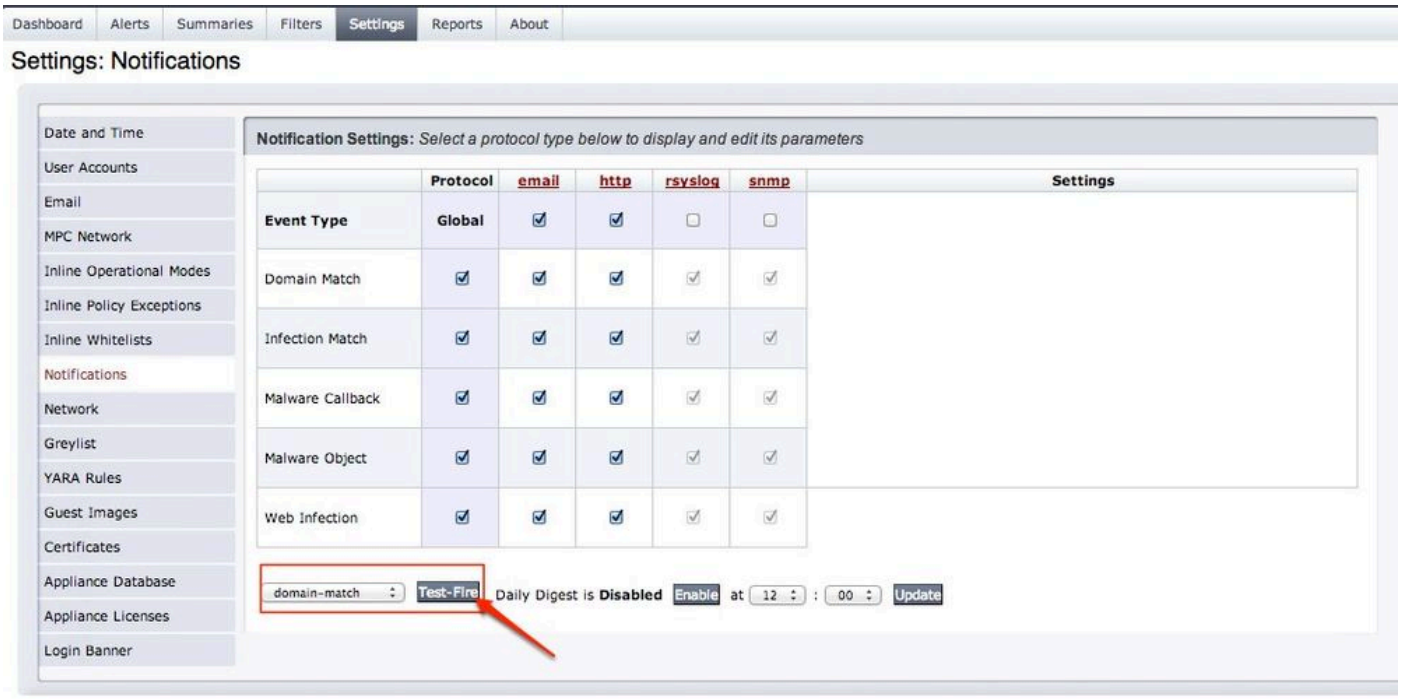
- 交付：基于每个事件
- 默认提供程序：通用
- 提供程序参数：消息格式JSON扩展
- （可选）如果您希望通过SSL发送流量，请选择SSL Enable。

此时，您的FireEye设备已设置为将选定的事件类型发送到Cisco Umbrella。接下来，了解如何在Cisco Umbrella控制面板中查看此信息并设置策略以阻止此流量。

确保连接：FireEye和Cisco Umbrella之间的“测试攻击”

此时，最好测试连通性并确保所有设备都设置正确：

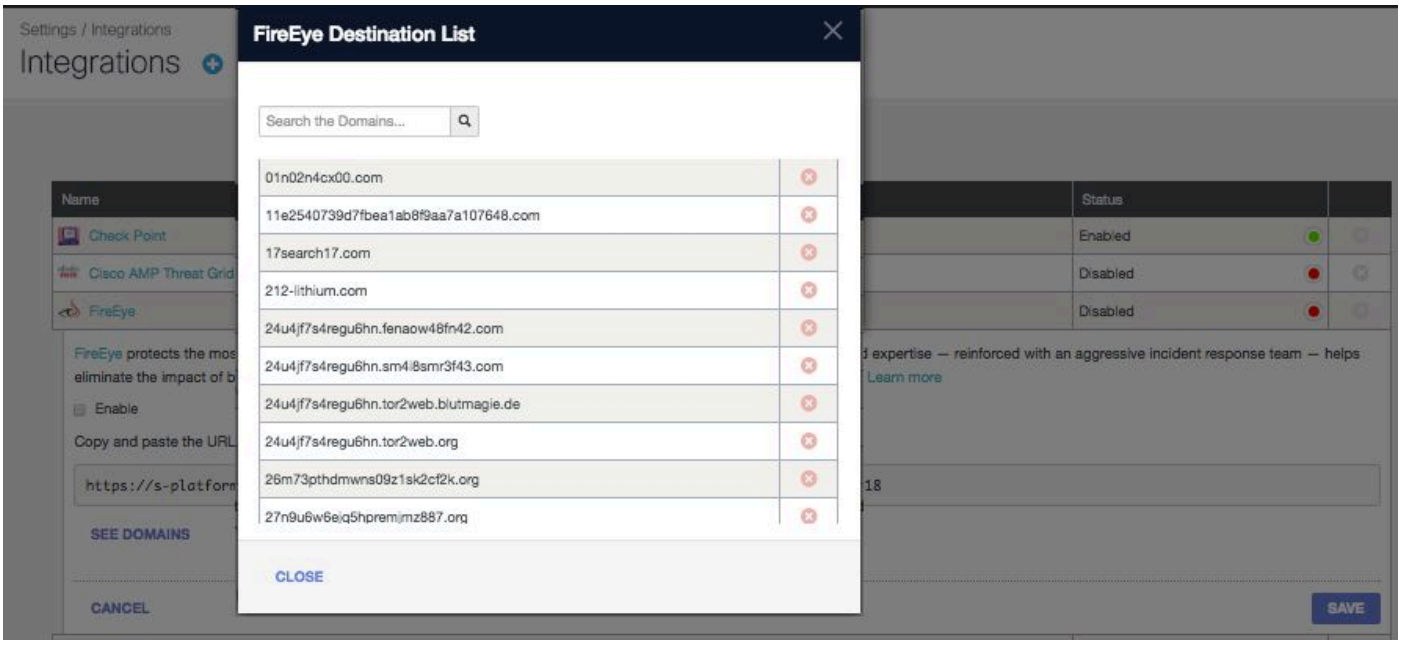
1.在FireEye中，从Test Fire下拉列表中选择domain-match，然后选择Test Fire:



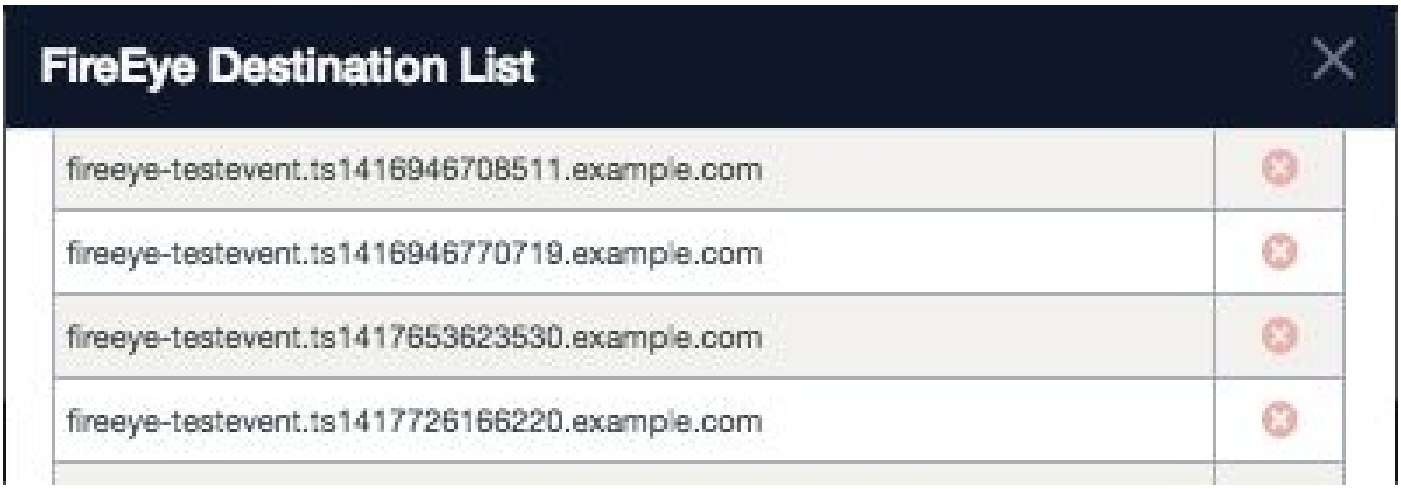
在Cisco Umbrella中，FireEye集成包括FireEye设备提供的域列表，以查看哪些域正在被主动添加。

2.选择Test Fire后，在Cisco Umbrella中导航到Settings > Integrations，然后在表中选择FireEye以展开它。

3.选择查看域。



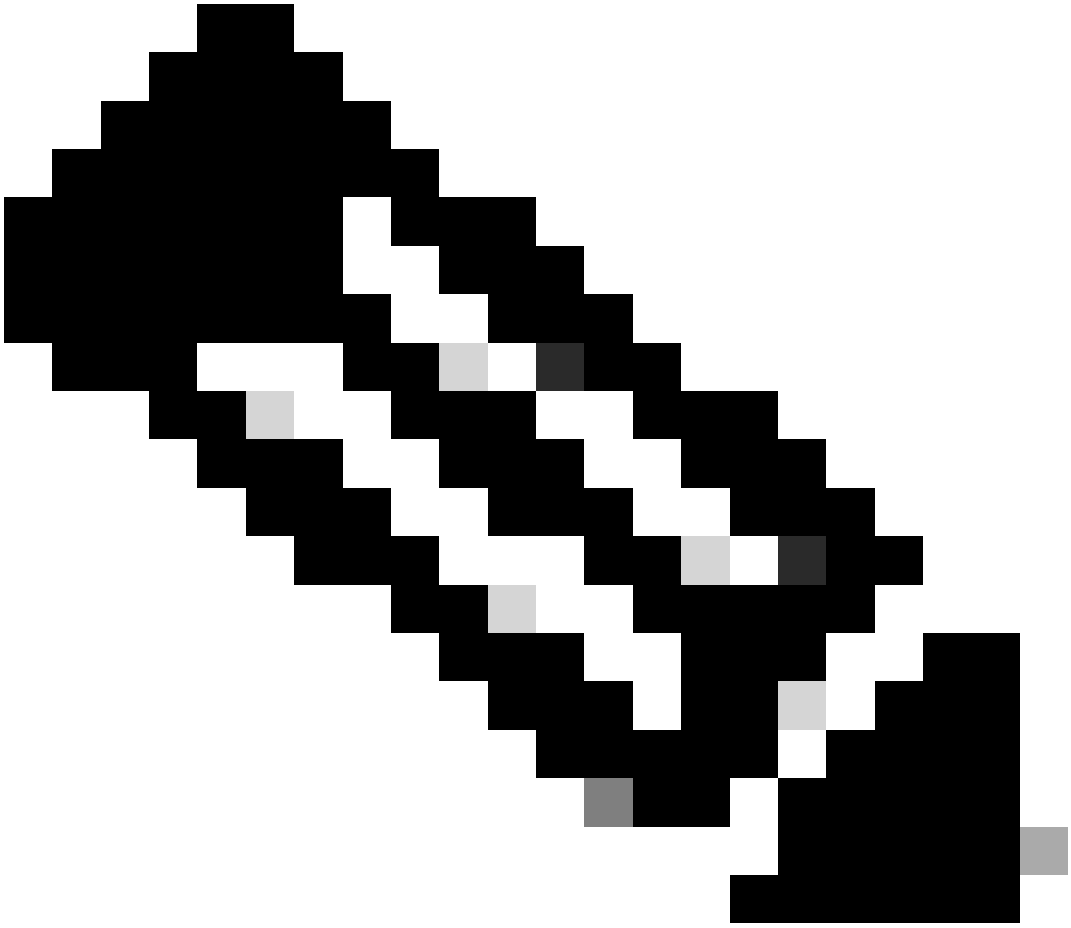
选择Test Fire会在FireEye目标列表中生成一个名为“fireeye-testevent.example.com-[date]”的域。每次在FireEye中选择Test Fire时，它都会创建一个唯一的域，该域的日期以UNIX Epoch时间为附加到测试的日期，因此将来的测试可以具有唯一的测试域名。



如果Test Fire成功，FireEye会向Cisco Umbrella发送更多事件，并开始填充和增加可搜索列表。

观察在“审核模式”下添加到FireEye安全设置的事件

FireEye设备中的事件开始填充特定目标列表，该列表可作为FireEye安全类别应用到策略。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，且不会导致对现有Cisco Umbrella策略进行任何更改。



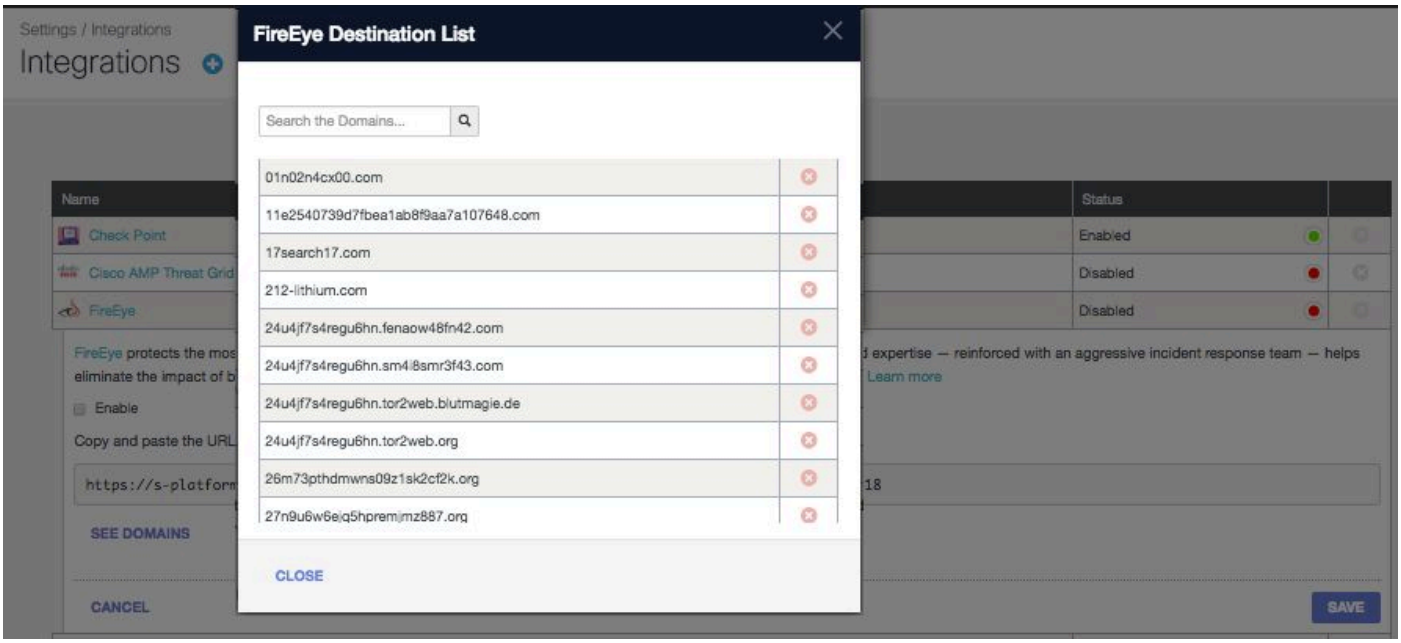
注意：根据您的部署配置文件和网络配置，可以启用“审核模式”，但必须持续很长时间。

查看目标列表

您可以随时查看FireEye目标列表：

1.定位至策略>策略组件>集成。

2.展开表中的FireEye，然后选择See Domains。

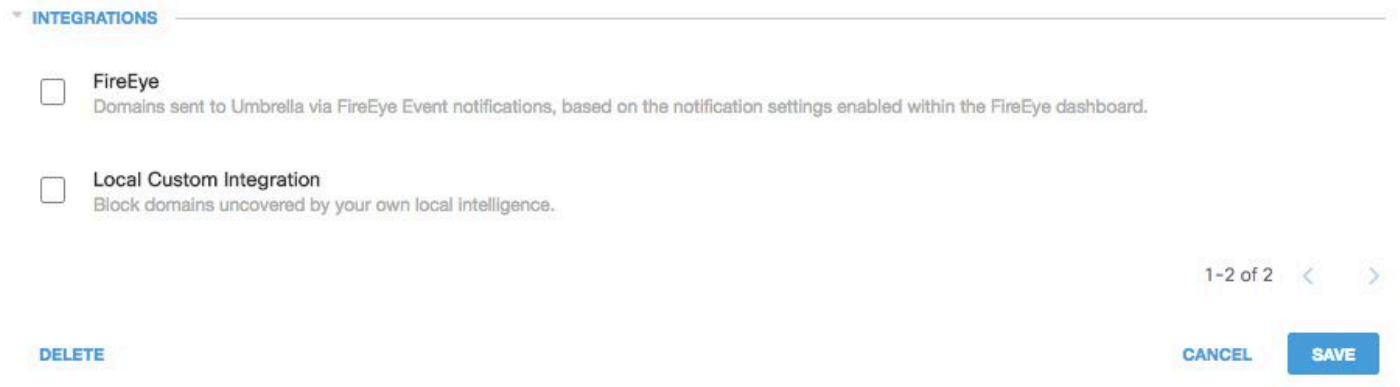


查看策略的安全设置

您可以查看可随时添加到策略的安全设置：

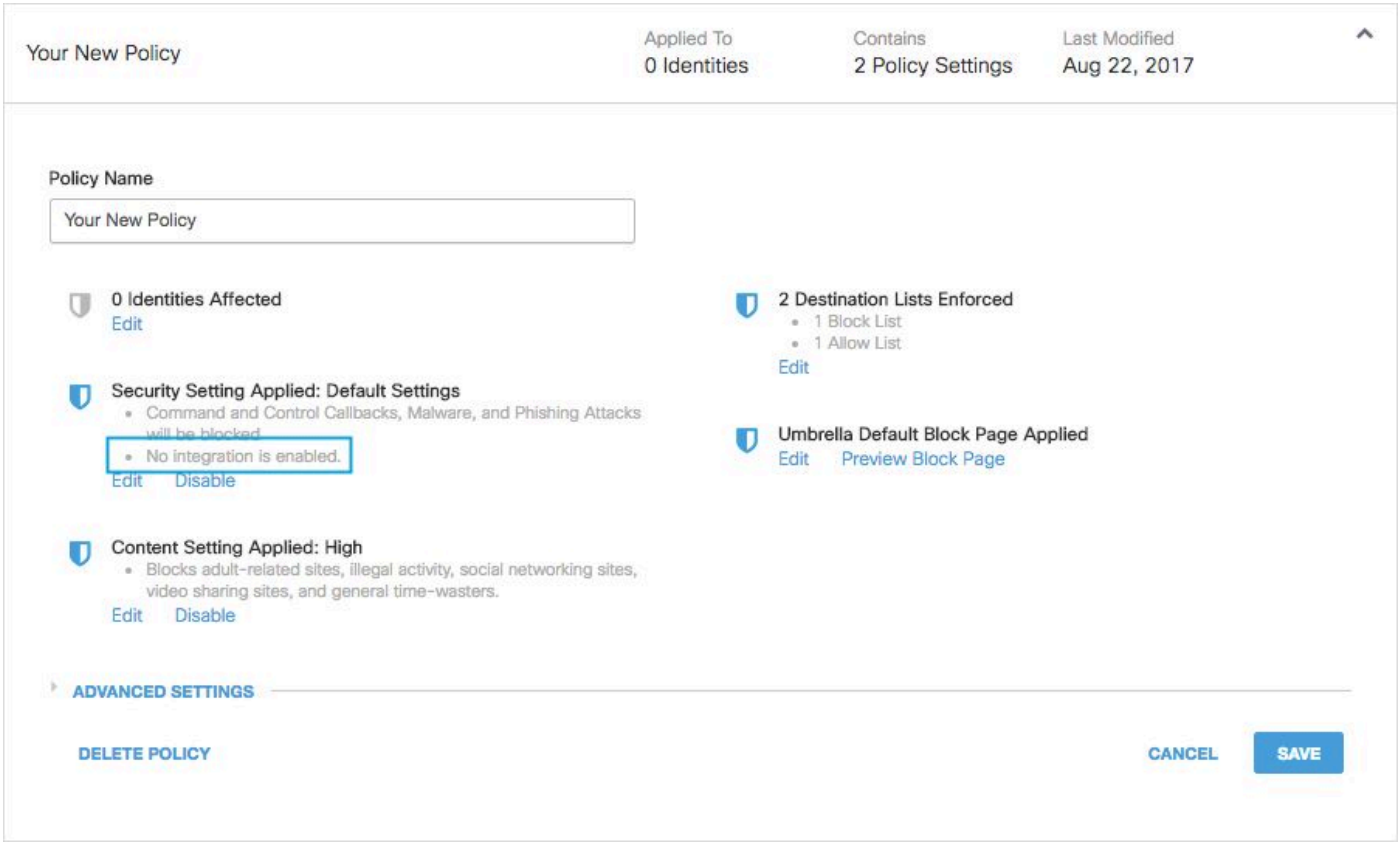
1.导航到策略>策略组件>安全设置。

2.选择表中的安全设置将其展开，然后滚动到集成以查找FireEye设置。



115014080803

您还可以通过“安全设置摘要”页面查看集成信息。



115013920526

开始使用时，最好清除此安全设置，以确保在“审核模式”下正确填充域。

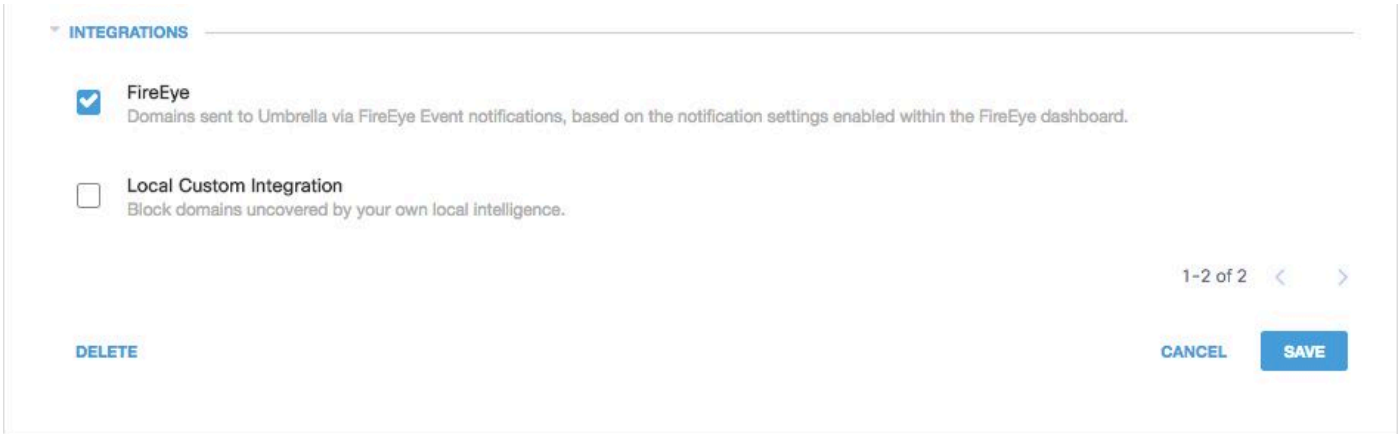
将“阻止模式”下的FireEye安全设置应用于托管客户端的策略

当您准备好让这些附加安全威胁由Cisco Umbrella管理的客户端实施后，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。

首先，创建或更新安全设置：

1.定位至“策略”>“策略组件”>“安全设置”。

2.在集成下，选择FireEye，然后选择保存。



115013921406

接下来，在策略向导中，将此安全设置添加到正在编辑的策略中：

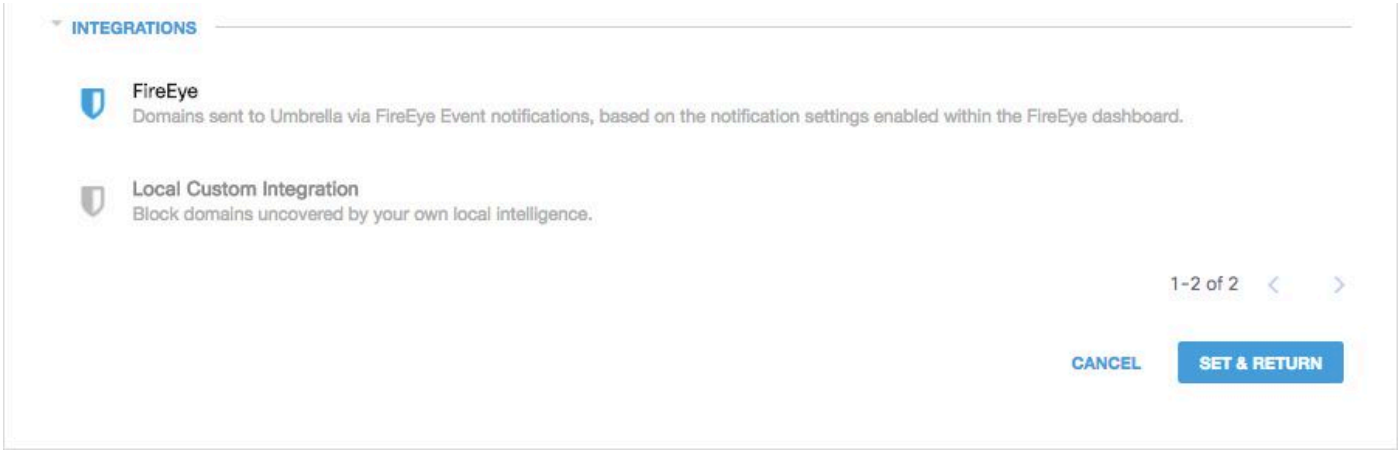
1.定位至策略>策略列表。

2.展开策略，并在Security Setting Applied下选择Edit。

3.在安全设置下拉列表中，选择包含FireEye设置的安全设置。

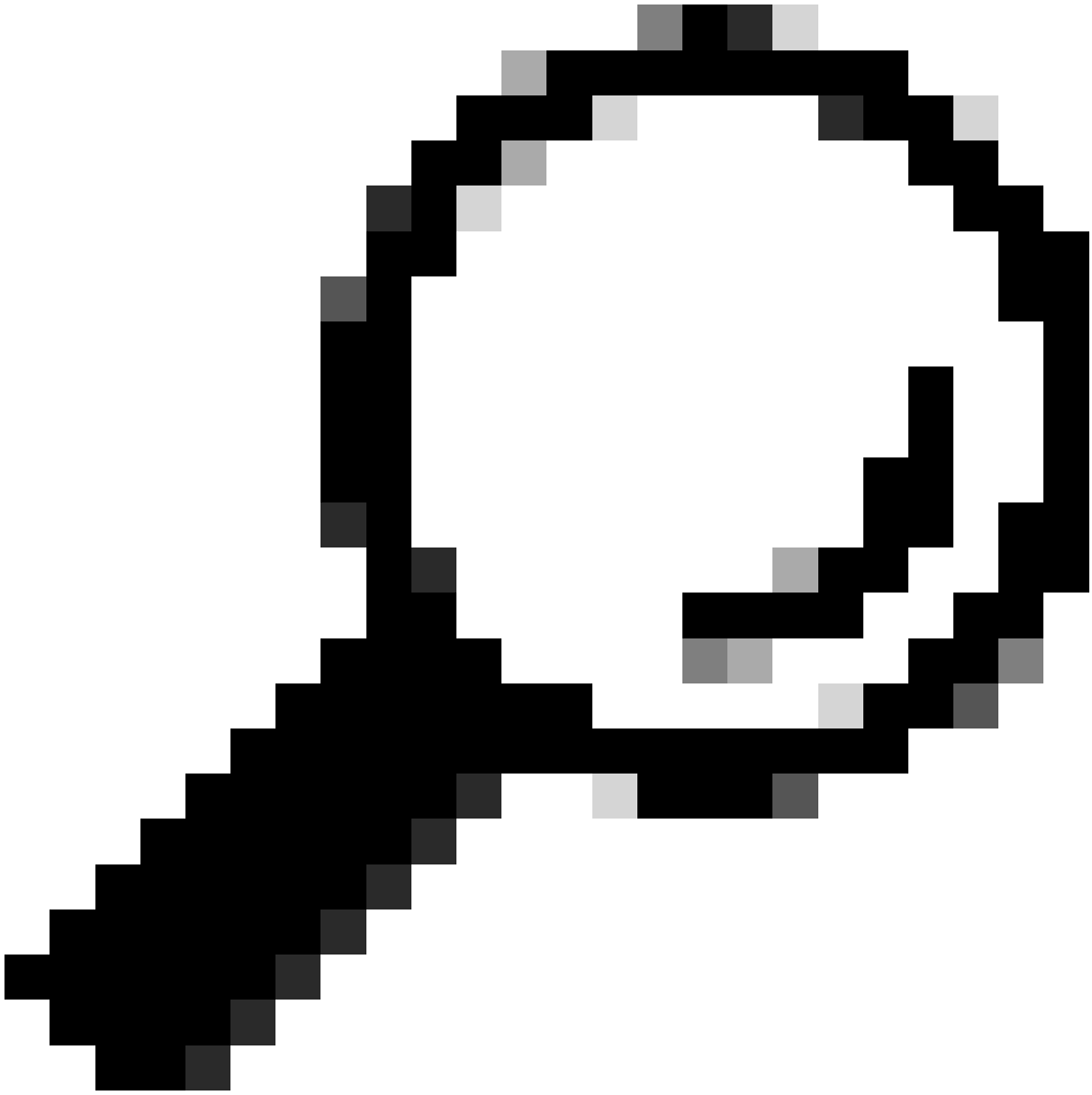
115014083083

“集成”(Integrations)下的屏蔽图标将更新为蓝色。



115013922146

4.选择设置&返回。



提示：也可以通过策略向导编辑安全设置。

FireEye的安全设置中包含的FireEye域会使用此策略阻止身份识别。

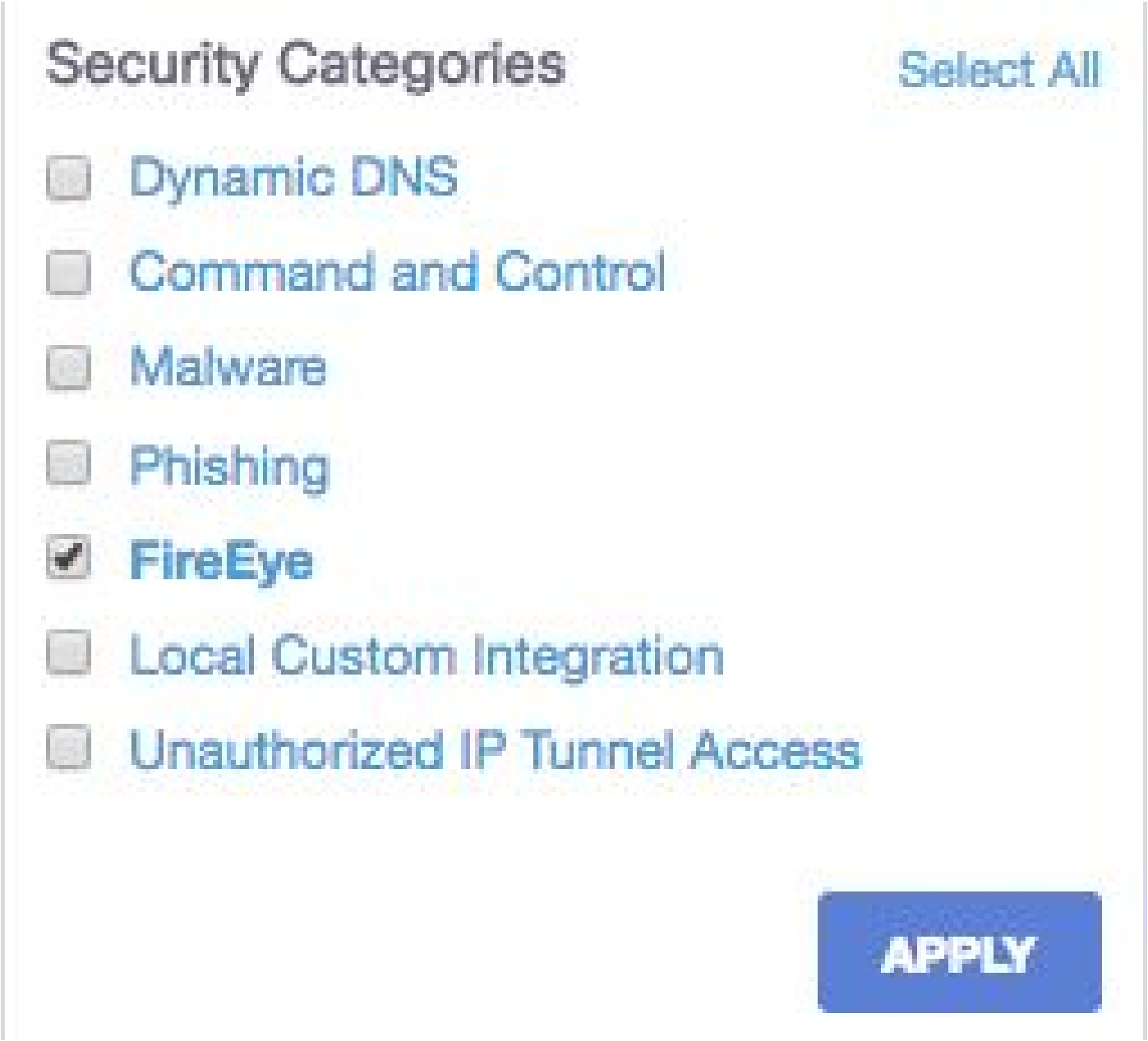
Cisco Umbrella for FireEye事件报告

FireEye安全事件报告

FireEye目标列表是可供报告使用的安全类别之一。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，以仅显示与FireEye相关的活动：

1.定位至“报告”>“活动搜索”。

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



115013924986

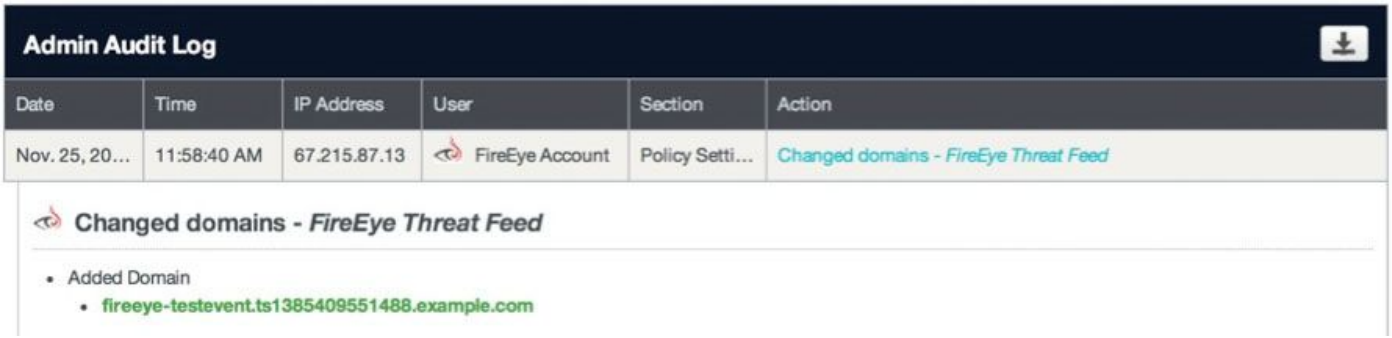
3.选择应用以查看报表中所选期间与FireEye相关的活动。

报告何时将域添加到FireEye目标列表

管理员审核日志包含FireEye设备中的事件，因为它将域添加到目标列表。名为“FireEye Account”（也带有FireEye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。

通过为“FireEye帐户”用户应用过滤器，您可以过滤以仅包括FireEye更改。

如果之前执行了“测试激活”步骤，则在审核日志中可能会显示添加FireEye测试域。



处理不需要的检测或误报

允许列表

尽管可能性不大，但FireEye设备自动添加的域可能会触发不必要的检测，阻止用户访问特定网站。在这种情况下，Umbrella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。

这一方法更可取的原因有两个。

- 首先，如果FireEye设备在删除域后重新添加该域，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。

如果阻止模式中的FireEye安全设置仅应用于受管Cisco Umbrella身份的子集（例如，它仅应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.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FireEye目标列表中删除域

FireEye目标列表中的每个域名旁边都有一个Delete图标。通过删除域，可以在发生意外检测时清除FireEye目标列表。

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

删除域的步骤：

1.定位至“设置”>“集成”，然后选择“FireEye”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。

在出现不需要的检测或误报时，Umbrella建议立即在Cisco Umbrella中创建允许列表，然后在FireEye设备中修复误报。稍后，您可以从FireEye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）。