將Umbrella與FireEye整合

目錄

簡介

本檔案介紹如何將Cisco Umbrella與FireEye整合。

必要條件

需求

思科建議您瞭解以下主題：

- 可訪問公共網際網路的FireEye裝置。
- Cisco Umbrella Dashboard管理許可權。
- Cisco Umbrella Dashboard必須啟用FireEye整合。

採用元件

本檔案中的資訊是根據Cisco Umbrella。

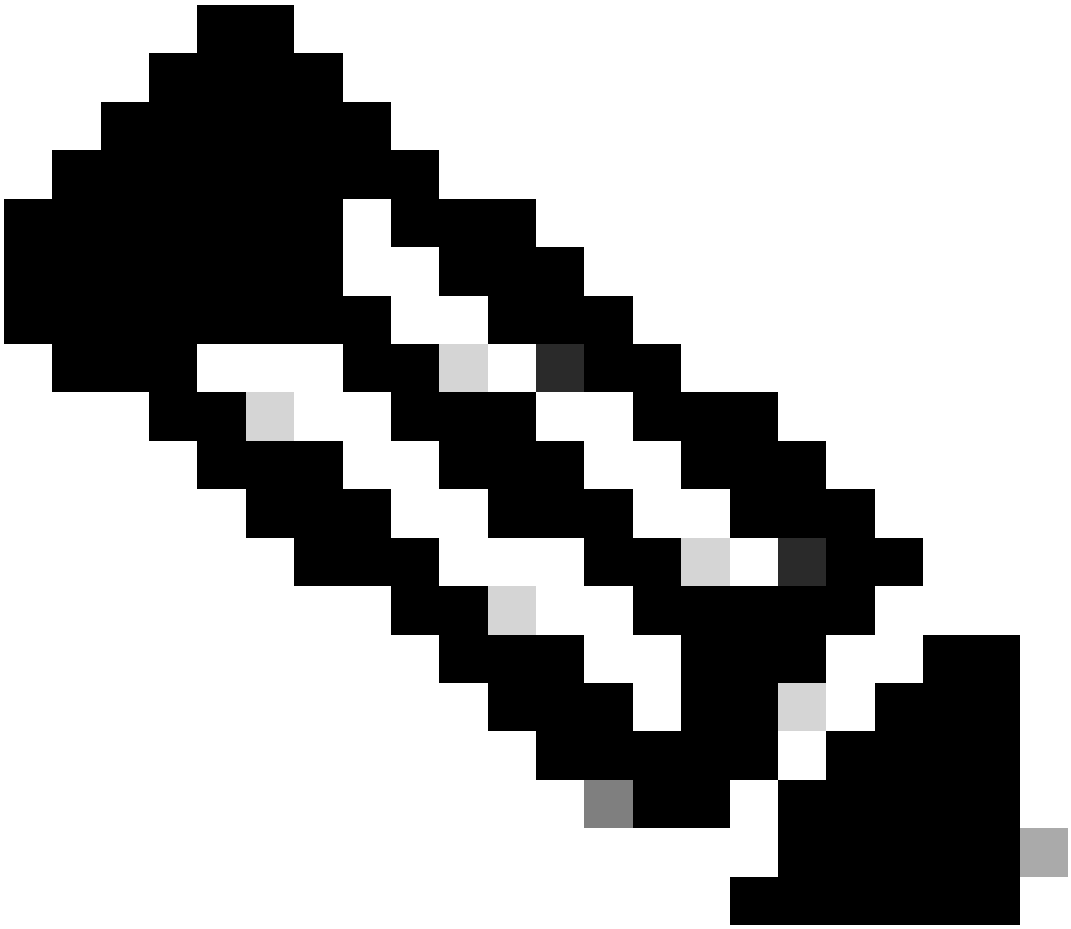
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

通過FireEye安全裝置與Cisco Umbrella之間的整合，安全人員和管理員現在可以針對漫遊的筆記型電腦、平板電腦或電話的高級威脅提供保護，同時為分散式企業網路提供另一層實施。

本指南概述如何配置FireEye以與Cisco Umbrella通訊，以便將FireEye的安全事件整合到策略中，這些策略可以應用於受Cisco Umbrella保護的客戶端。



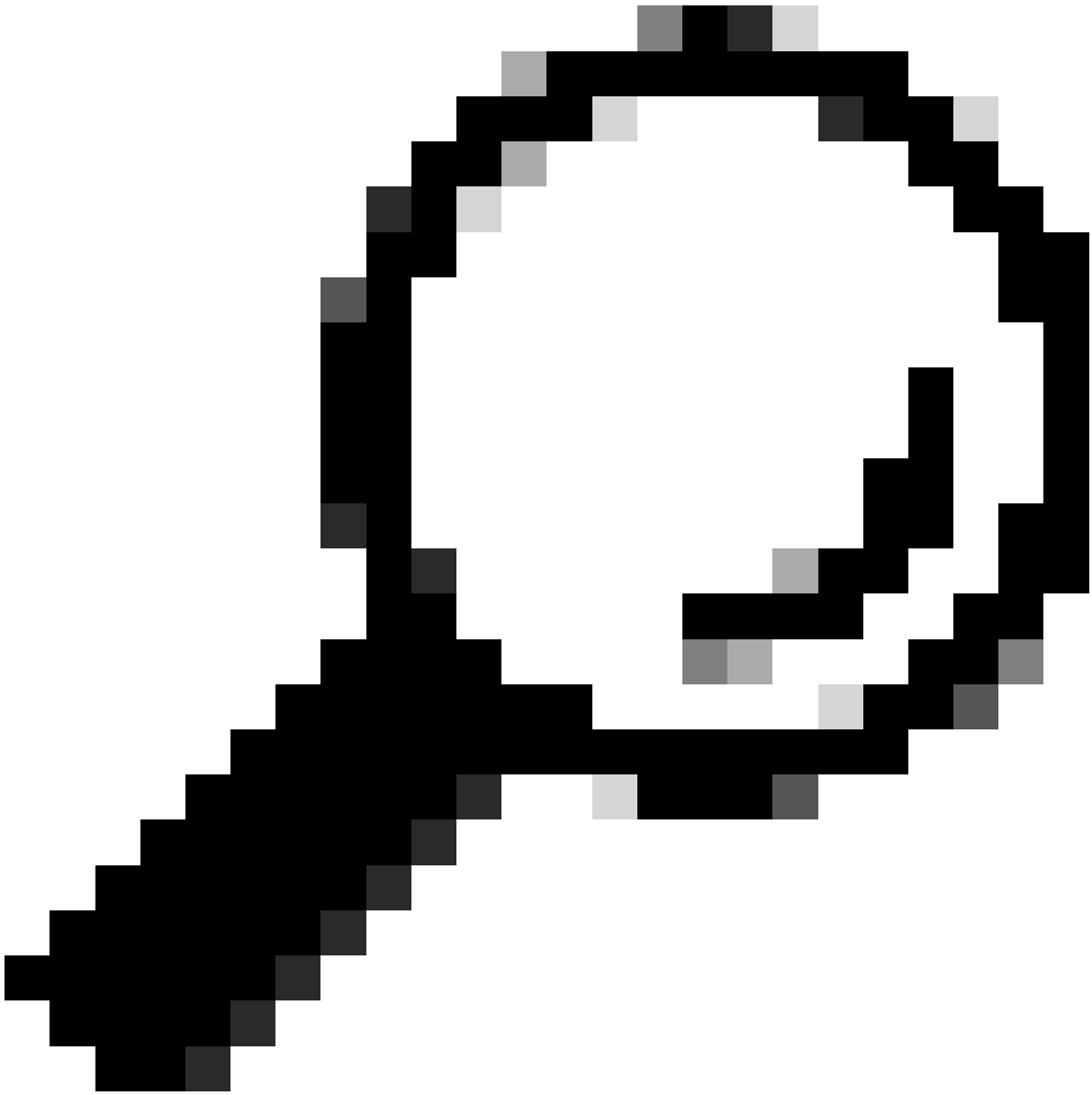
附註：FireEye整合僅包含在Cisco Umbrella包中，例如DNS Essentials、DNS Advantage、SIG Essentials或SIG Advantage。如果您沒有這些軟體包之一，並且希望整合FireEye，請聯絡您的思科Umbrella客戶經理。如果您有正確的Cisco Umbrella包，但並未將FireEye視為控制板的整合，請與Cisco Umbrella支援聯絡。

整合功能

FireEye裝置首先將其發現的基於網際網路的威脅（例如託管惡意軟體的域、殭屍網路的命令和控制或網路釣魚站點）傳送到Cisco Umbrella。

然後，Cisco Umbrella會驗證傳遞到Cisco Umbrella的資訊，以確保其有效並可新增到策略中。如果確認來自FireEye的資訊格式正確（例如，它不是檔案、複雜的URL或高度流行的域），則域地址會作為可應用於任何Cisco Umbrella策略的安全設定的一部分新增到FireEye目標清單中。該策略會立即應用於使用具有FireEye目標清單的策略從裝置發出的任何請求。

接下來，Cisco Umbrella會自動分析FireEye警報，並將惡意站點新增到FireEye目標清單。這會將FireEye保護擴展到所有遠端使用者和裝置，並為您的公司網路提供另一層實施。



提示：雖然Cisco Umbrella會儘量驗證和允許已知安全域（例如Google和Salesforce），以避免不必要的中斷，我們建議您根據您的策略將您從未希望阻止的域新增到全域性允許清單或其他目標清單中。示例包括：

- 您組織的首頁
- 表示您提供的服務的域，可以同時具有內部和外部記錄。例如，「mail.myservicedomain.com」和「portal.myotherservicedomain.com」。
- 您依賴於Cisco Umbrella的不太知名的基於雲的應用程式不包括在自動域驗證中。例如，「localcloudservice.com」。

這些網域可新增到Cisco Umbrella中Policies > Destination Lists下的Global Allow List。

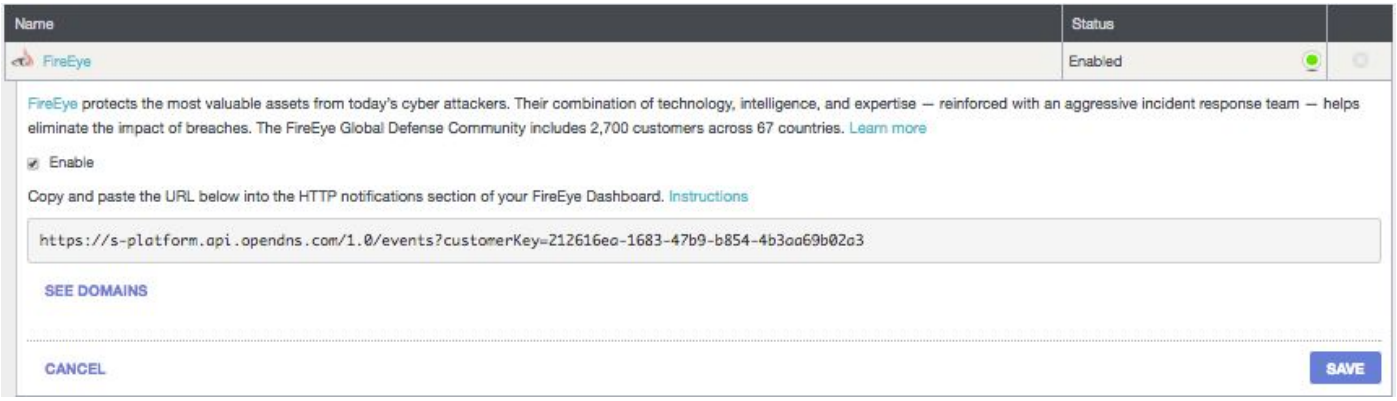
配置Cisco Umbrella控制面板以從FireEye接收資訊

第一步是在Cisco Umbrella中查詢您的唯一URL，以便FireEye裝置與其通訊。

1.以管理員身份登入Cisco Umbrella Dashboard。

2.定位至Policies > Policy Components > Integrations，然後在表中選擇FireEye將其展開。

3.選擇啟用框，然後選擇儲存。這會為您在Cisco Umbrella中的組織生成唯一的特定URL。

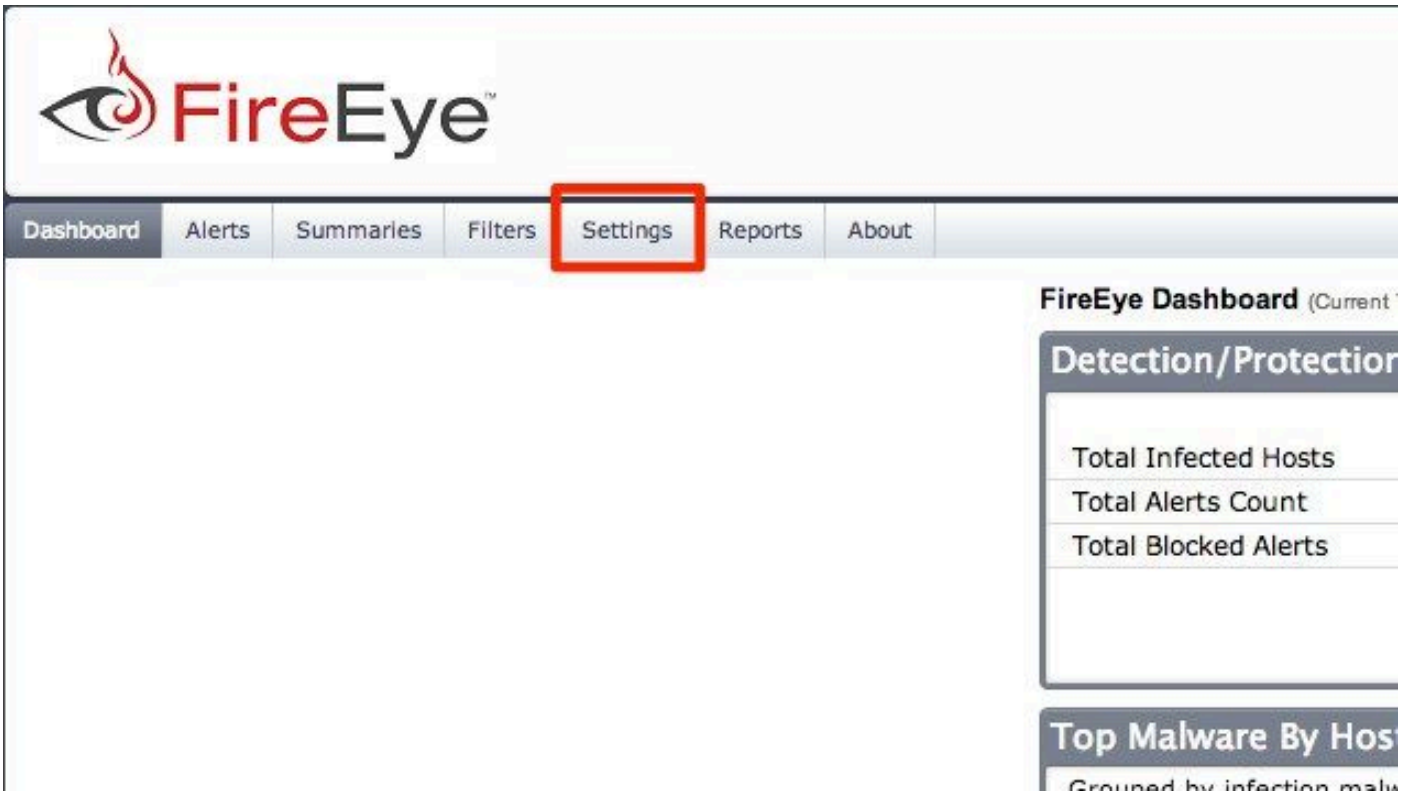


您可以稍後使用此URL配置FireEye裝置將資料傳送到Cisco Umbrella，因此請確保複製該URL。

配置FireEye與Cisco Umbrella通訊

若要開始將流量從FireEye裝置傳送到Cisco Umbrella，必須使用上一節中生成的URL資訊配置FireEye。

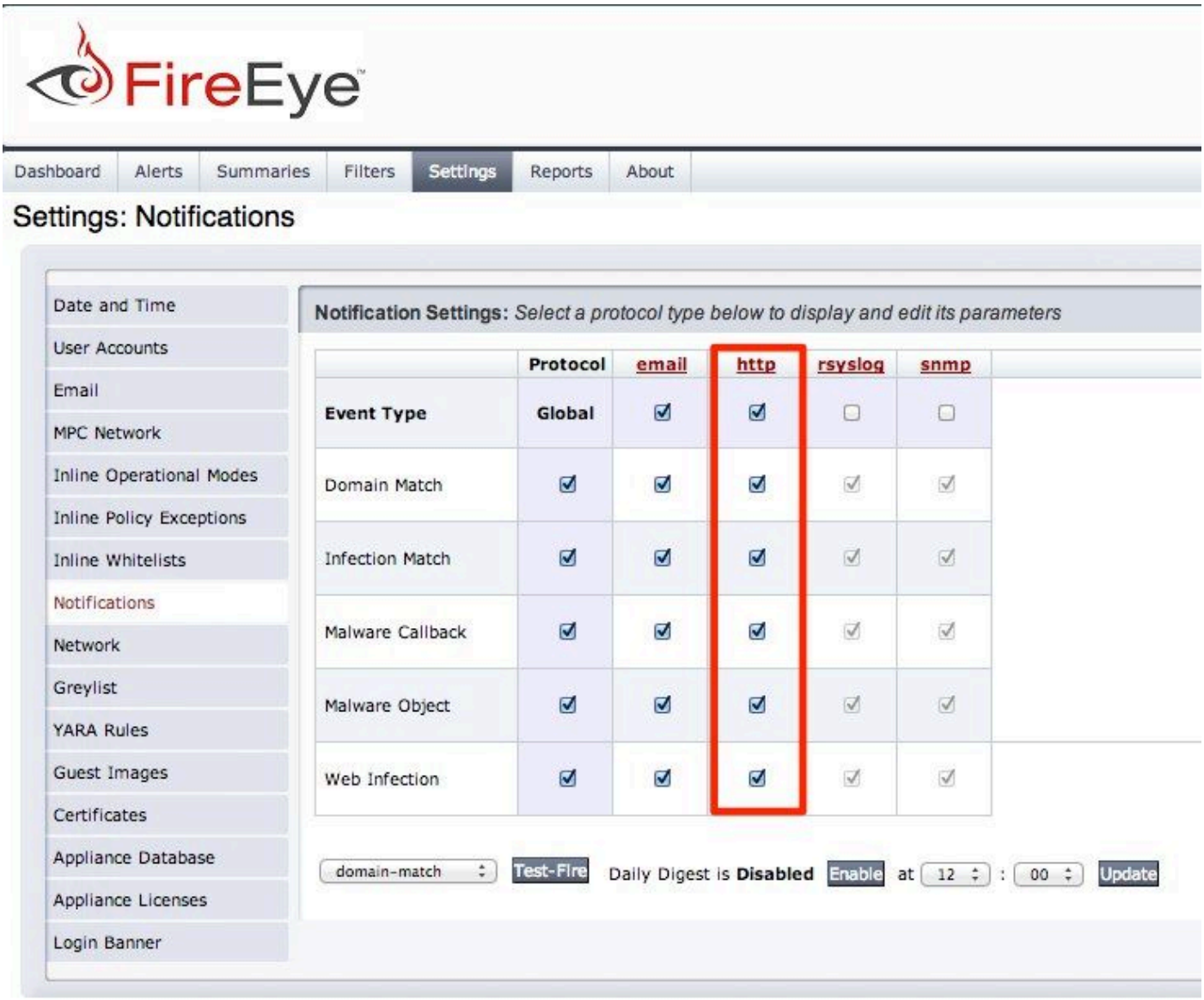
1.登入到FireEye，然後選擇設定。



2.從設定清單中選擇Notifications:

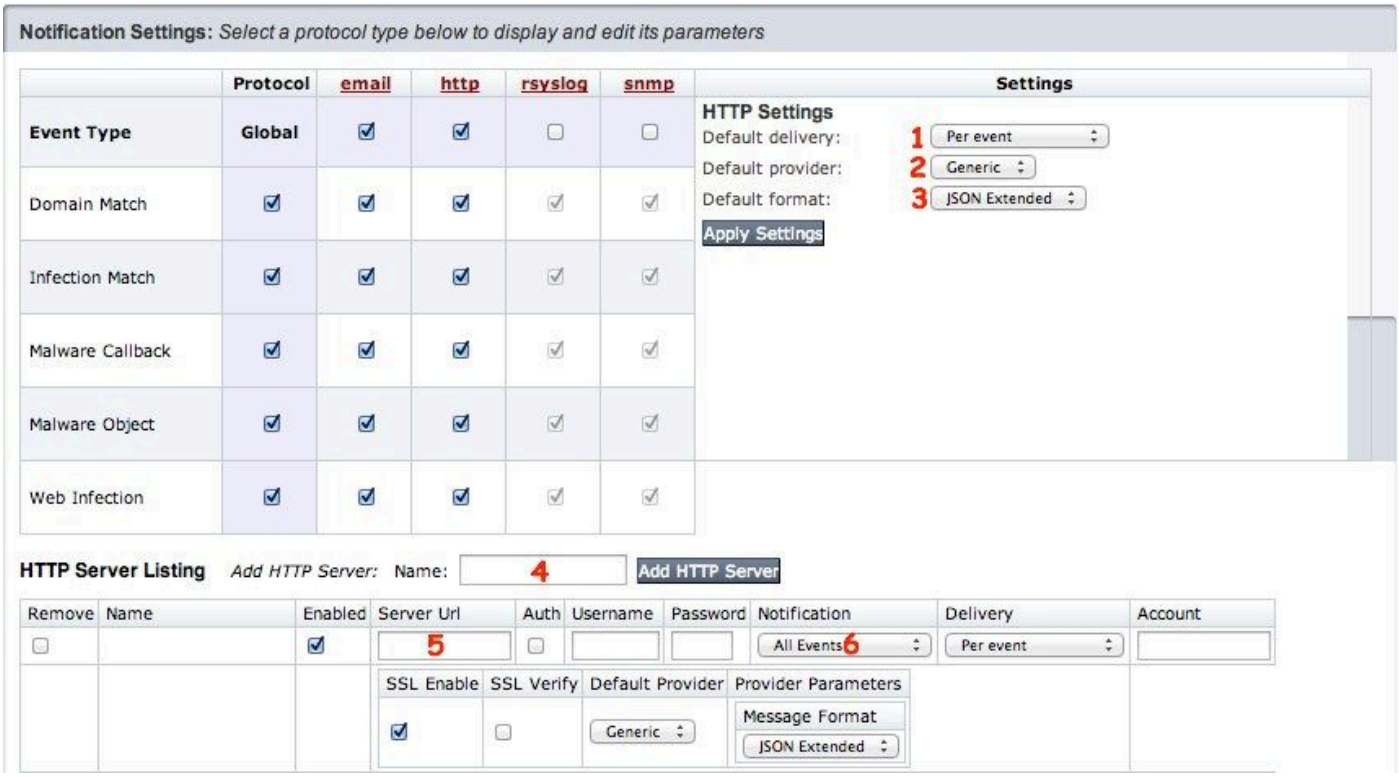

FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance 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.確保選擇了要傳送到Cisco Umbrella的所有事件型別（Umbrella建議從all開始），然後選擇列頂部的HTTP連結。



4.在選單展開時，選擇這些選項以啟用「事件通知」。螢幕截圖概述了編號步驟：

1. 預設傳送：每個事件
2. 預設提供程式：一般
3. 預設格式：擴展的JSON
4. 將HTTP服務器命名為「OpenDNS」。
5. 伺服器Url:在此之前貼上您從Cisco Umbrella控制面板中生成的Cisco Umbrella URL。
6. Notification（通知）下拉選單：選擇All Events以確保最大覆蓋範圍。



5.確保Delivery、Default Provider和Provider Parameters下拉選單均與預設設定匹配，或者如果使用了多個通知伺服器：

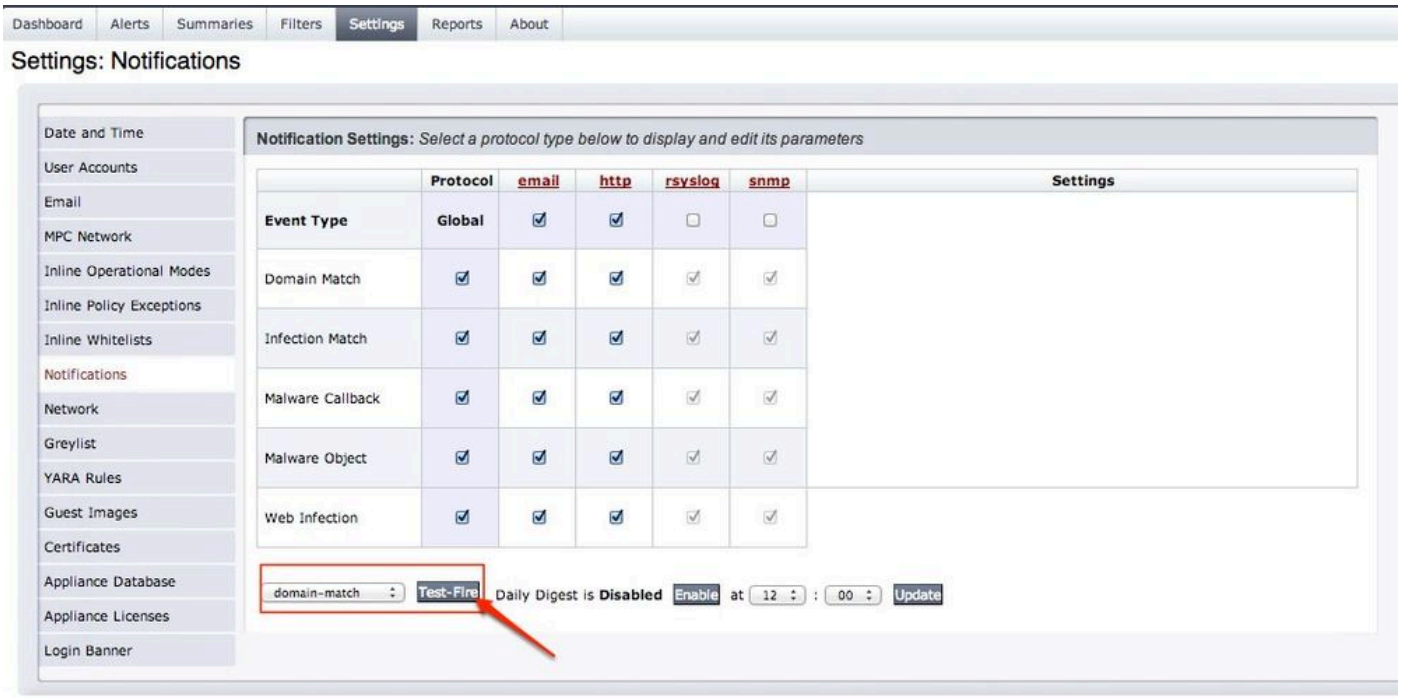
- 交付：基於每個事件
- 預設提供程式：一般
- 提供程式引數：消息格式JSON擴展
- （可選）如果您希望通過SSL傳送流量，請選擇SSL Enable。

此時，您的FireEye裝置已設定為將選定的事件型別傳送到Cisco Umbrella。接下來，瞭解如何在Cisco Umbrella控制面板中檢視此資訊並設定策略以阻止此流量。

確保連線：FireEye和Cisco Umbrella之間的「Test Fire」

此時，最好測試您的連線並確保所有裝置都設定正確：

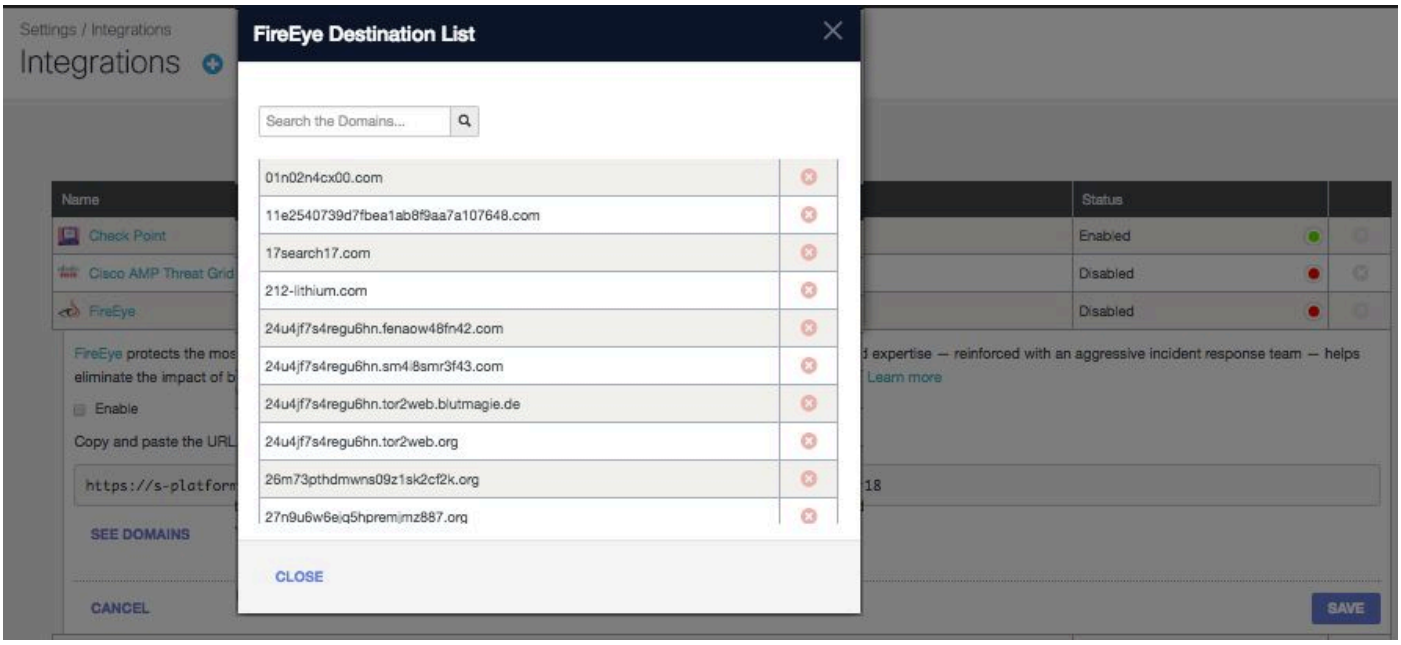
1.在FireEye中，從Test Fire下拉選單中選擇domain-match，然後選擇Test Fire:



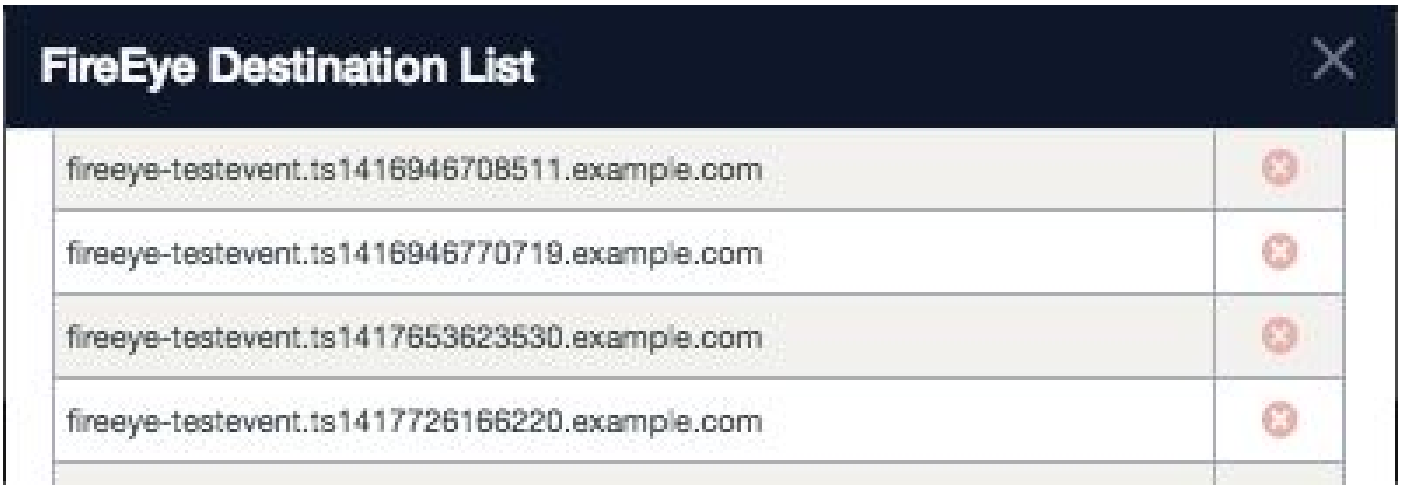
在Cisco Umbrella中，FireEye整合包括FireEye裝置提供的域清單，以檢視哪些域正在被主動新增。

2.選擇Test Fire後，在Cisco Umbrella中導航到Settings > Integrations，然後在表格中選擇FireEye以展開該選項。

3.選擇檢視域。



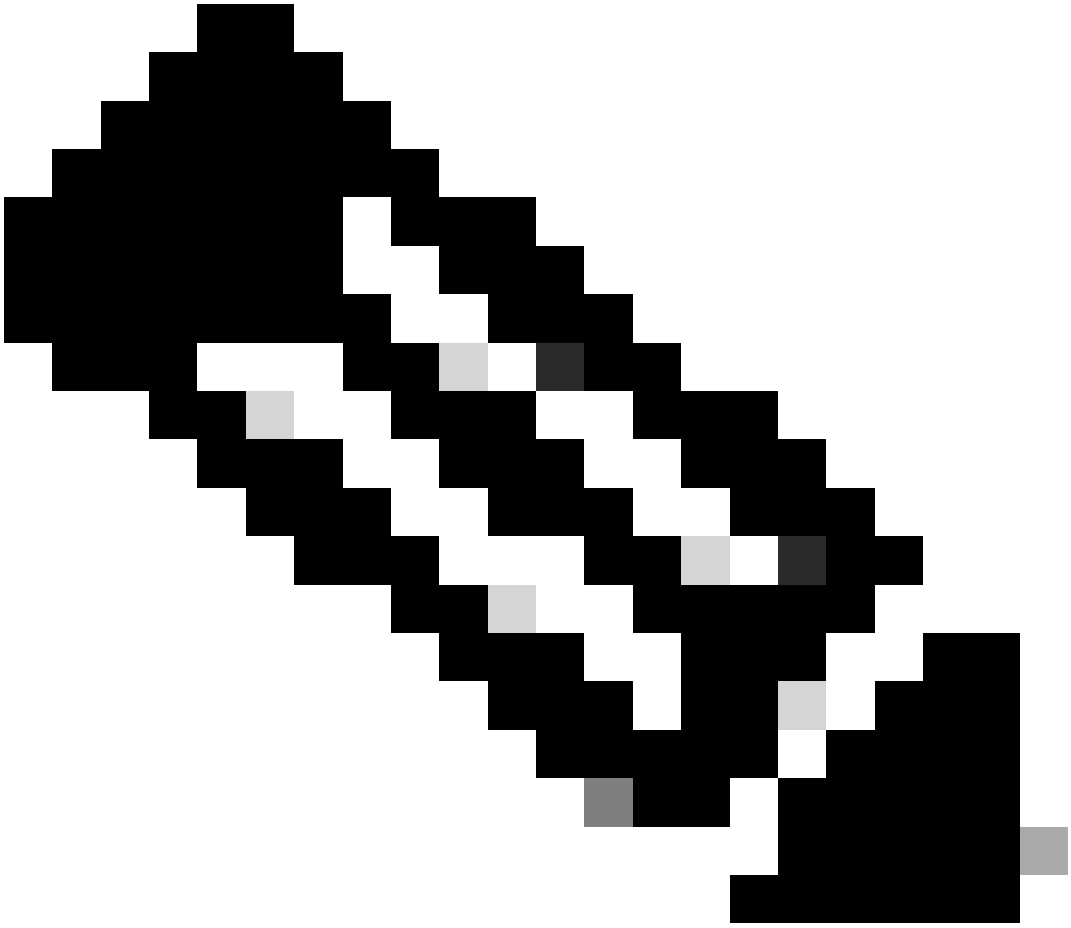
選擇Test Fire將在FireEye目標清單中生成名為「fireeye-testevent.example.com-[date]」的域。每次選擇FireEye中的Test Fire時，它都會建立一個唯一的域，該域的日期在UNIX Epoch時間內，該日期附加在測試上，因此將來的測試可以有一個唯一的測試域名。



如果Test Fire成功，FireEye會向Cisco Umbrella傳送更多事件，並開始填充和增加可搜尋清單。

觀察在「稽核模式」下新增到FireEye安全設定的事件

FireEye裝置中的事件開始填充一個特定目標清單，該清單可以作為FireEye安全類別應用到策略。預設情況下，目標清單和安全類別處於「稽核模式」，不應用於任何策略，並且不能導致對現有Cisco Umbrella策略進行任何更改。



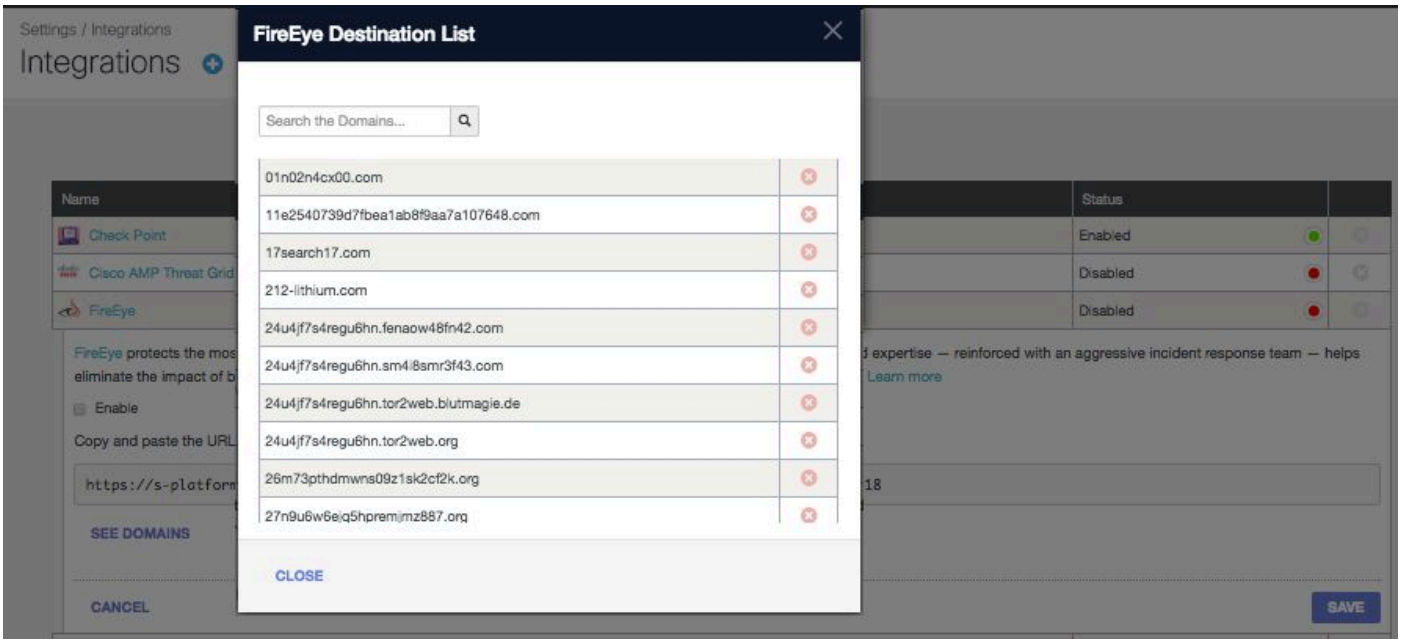
附註：根據您的部署配置檔案和網路配置，可以啟用「稽核模式」，無論需要多長時間。

檢視目標清單

您可以隨時檢視FireEye目標清單：

1.定位至策略>策略元件>整合。

2.展開表中的FireEye，然後選擇See Domains。

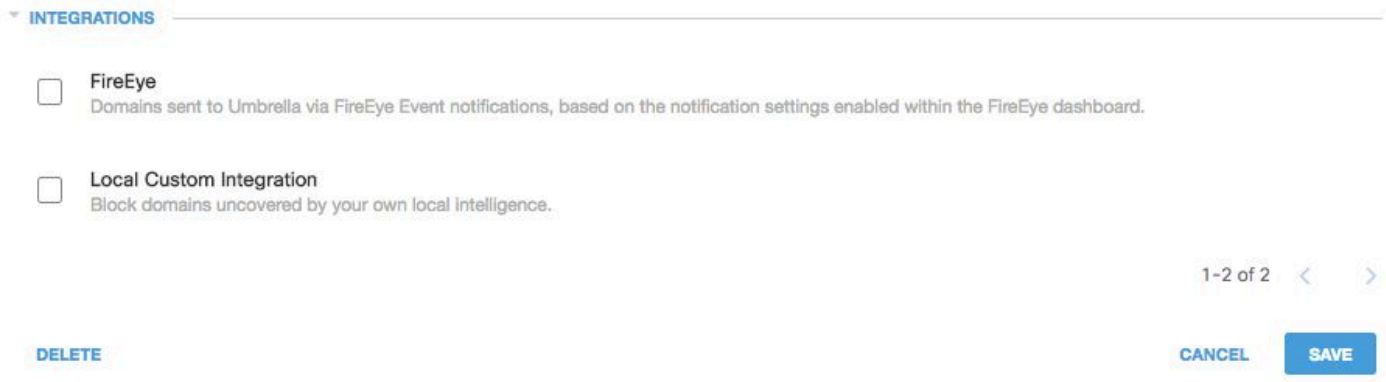


檢視策略的安全設定

您可以檢視可隨時新增到策略的安全設定：

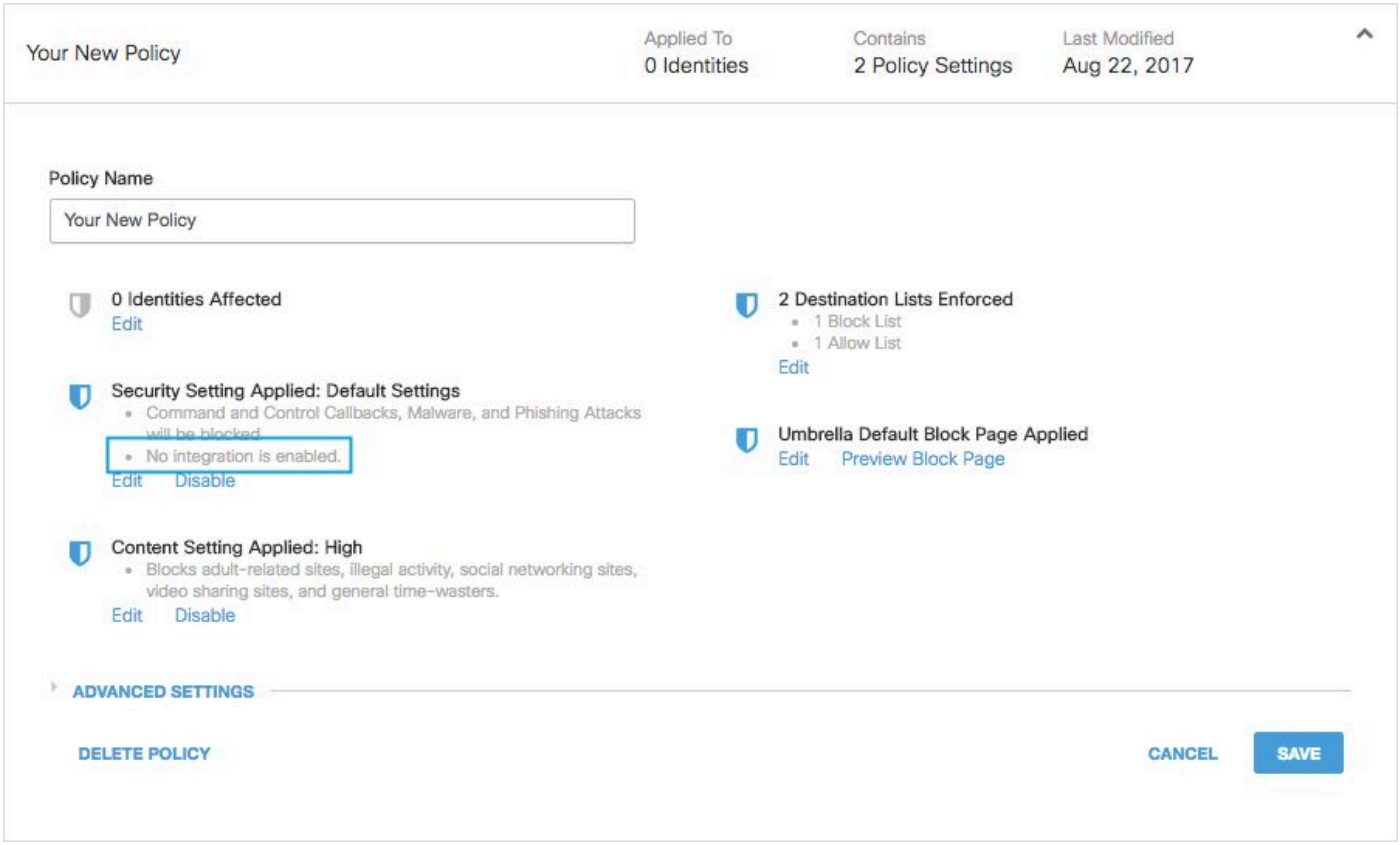
1.導航至策略>策略元件>安全設定。

2.選擇表中的安全設定將其展開，然後滾動到整合以查詢FireEye設定。



115014080803

您還可以通過「安全設定摘要」頁面檢視整合資訊。



115013920526

開始使用時，最好清除此安全設定，以確保域在「稽核模式」下正確填充。

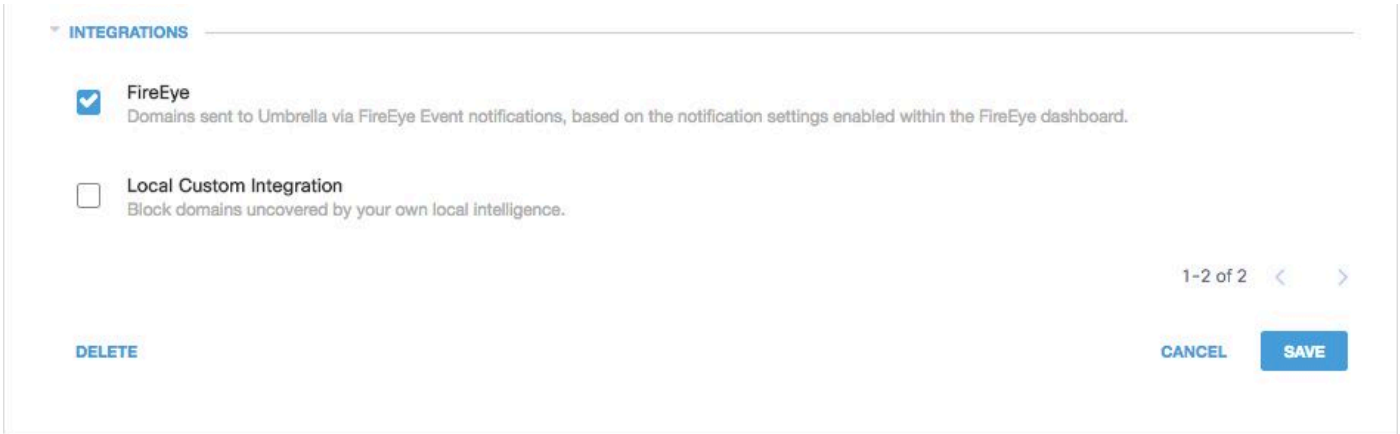
將「阻止模式」下的FireEye安全設定應用於託管客戶端的策略

一旦您準備好讓這些附加安全威脅由Cisco Umbrella管理的客戶端實施，請更改現有策略的安全設定，或建立位於預設策略上方的新策略以確保首先實施該策略。

首先，建立或更新安全設定：

1.導航到策略>策略元件>安全設定。

2.在Integrations下，選擇FireEye，然後選擇Save。



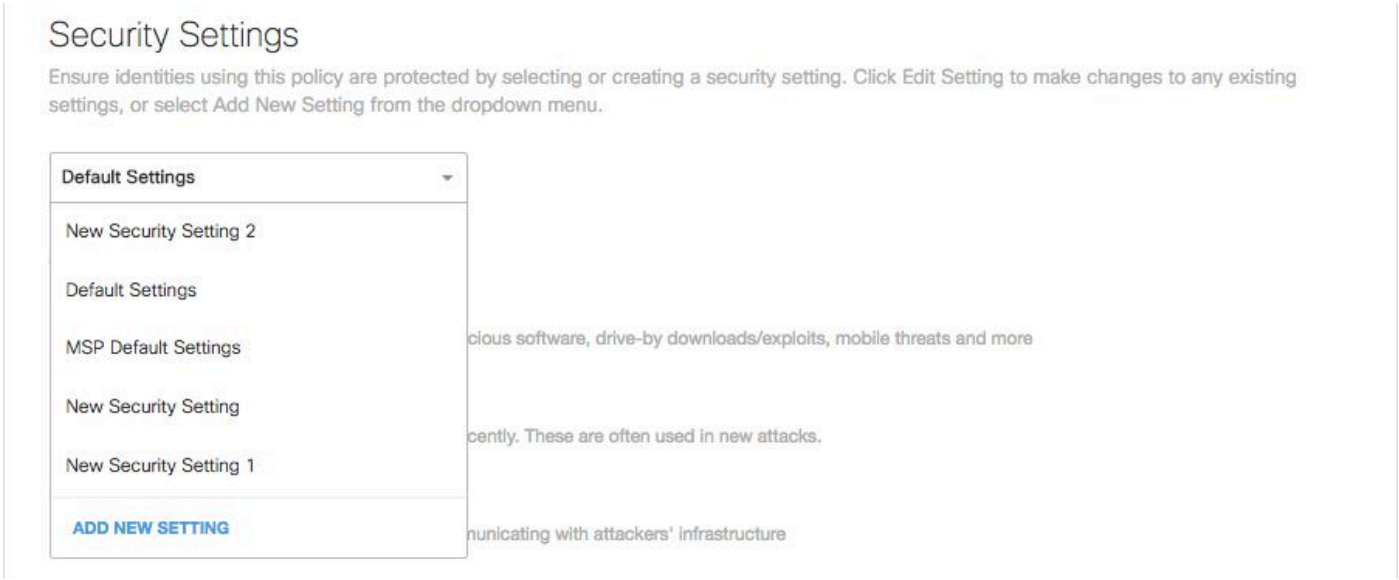
115013921406

接下來，在「策略」嚮導中，將此安全設定新增到正在編輯的策略中：

1.定位至Policies > Policy List。

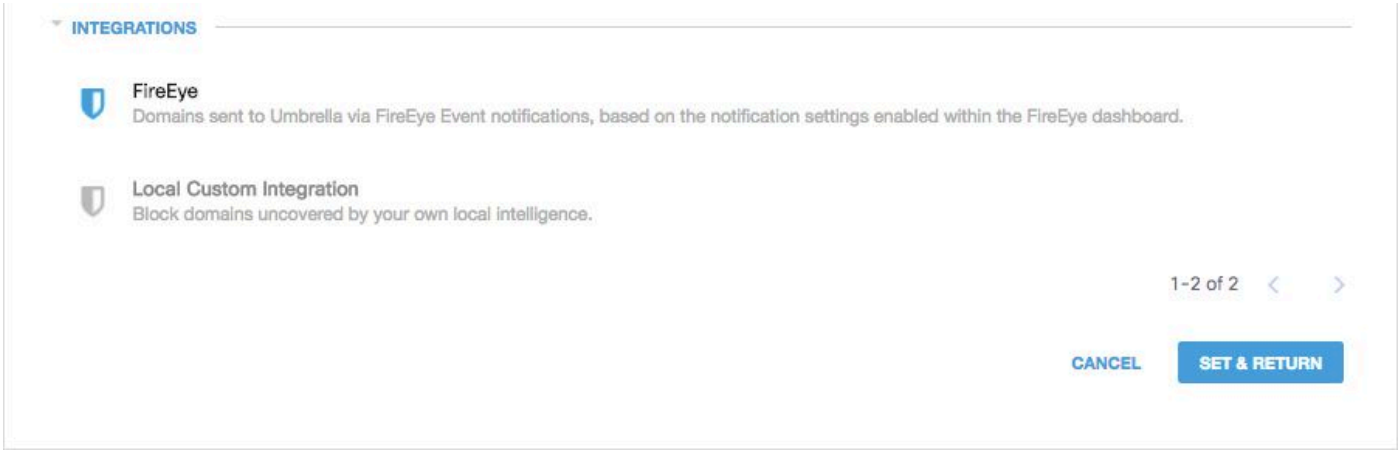
2.展開策略，然後在Security Setting Applied下選擇Edit。

3.在「Security Settings」下拉選單中，選擇包含FireEye設定的安全設定。



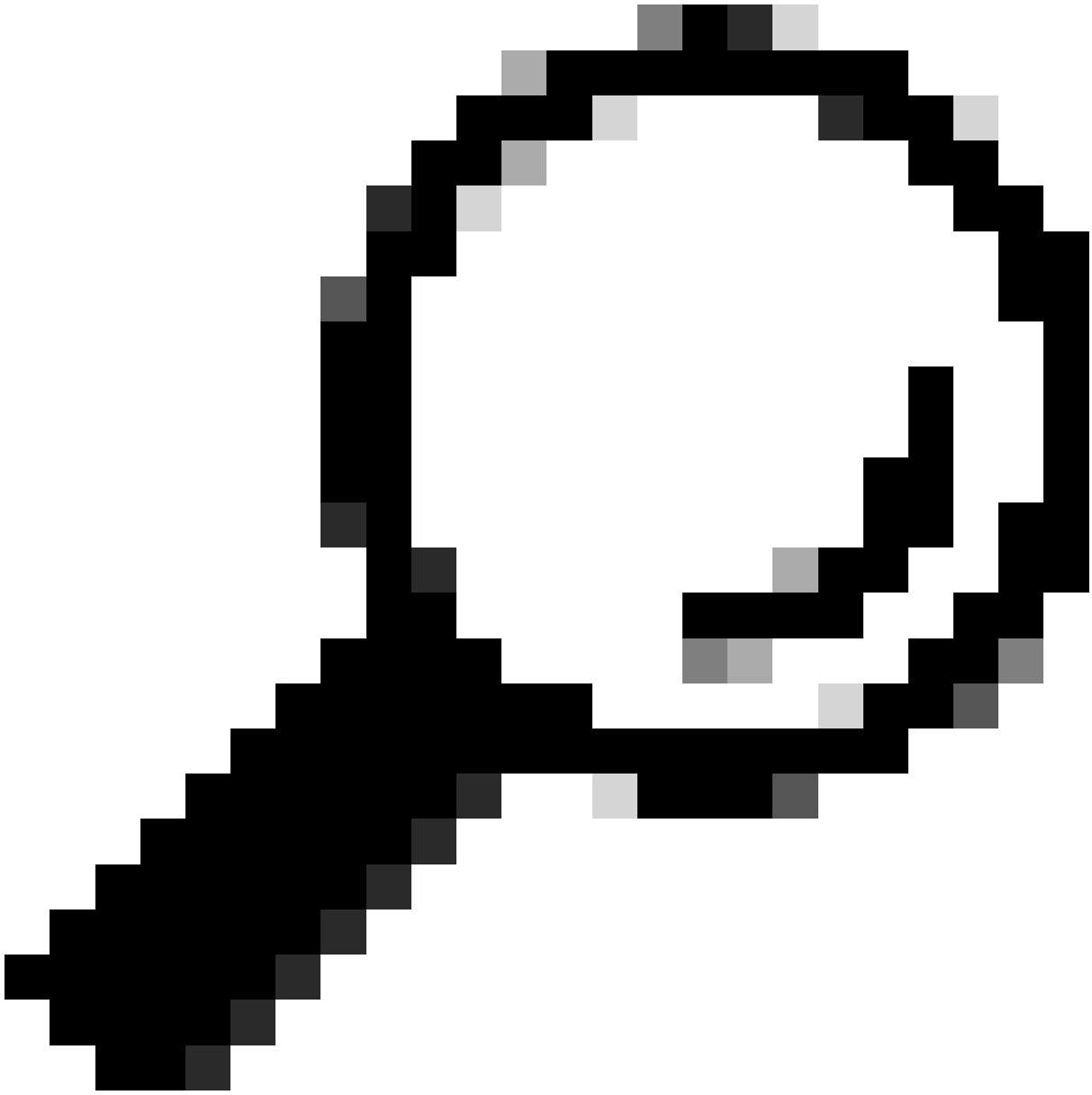
115014083083

「整合」(Integrations)下的遮蔽圖示將更新為藍色。



115013922146

4.選擇「設定&返回」。



提示：也可以通過「策略」嚮導編輯您的安全設定。

FireEye的安全設定中包含的FireEye域被阻止，以便使用該策略識別身份。

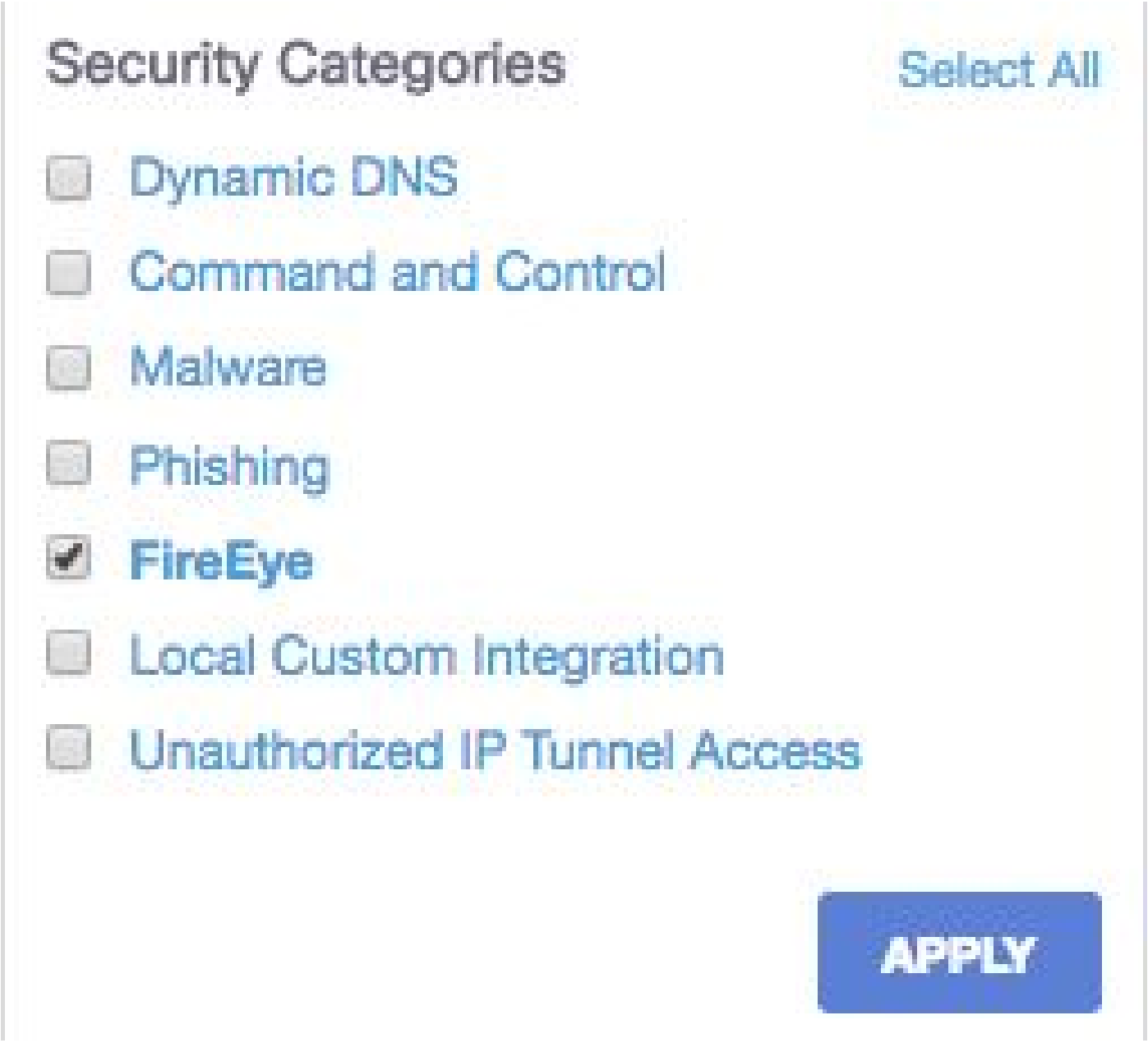
在Cisco Umbrella中報告FireEye事件

報告FireEye安全事件

FireEye目標清單是可用於報告的安全類別之一。大多數或全部報告使用安全類別作為過濾器。例如，您可以過濾安全類別，以便只顯示與FireEye相關的活動：

1.定位至報告>活動搜尋。

2.在安全類別下，選擇FireEye以篩選報表，以便僅顯示FireEye的安全類別。



115013924986

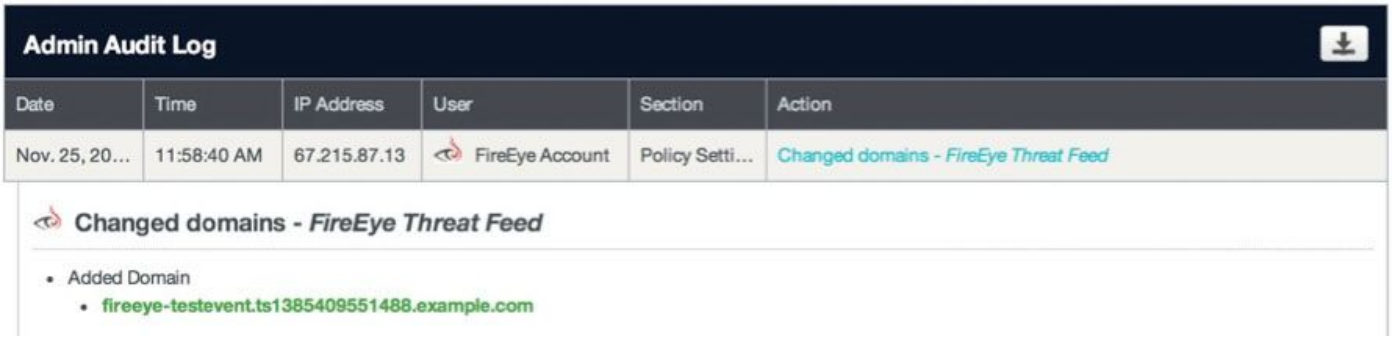
3.選擇應用以檢視報表中所選期間與FireEye相關的活動。

報告何時將域新增到FireEye目標清單

管理員稽核日誌包含FireEye裝置中的事件，因為它將域新增到目標清單。名為「FireEye Account」（也帶有FireEye徽標）的使用者生成事件。這些事件包括所新增的域和新增該域的時間。

通過為「FireEye帳戶」使用者應用篩選器，可以篩選為僅包括FireEye更改。

如果之前執行了「測試激發」(Test Fire)步驟，那麼FireEye測試域的新增就可能會出現在稽核日誌中。



處理不需要的檢測或誤報

允許清單

儘管可能性不大，但您的FireEye裝置自動新增的域可能會觸發不需要的檢測，阻止您的使用者訪問特定網站。在這種情況下，Umbrella建議將網域新增到允許清單(Policies > Destination Lists)，此清單優先於所有其他型別的封鎖清單，包括安全設定。

這一方針更可取，原因有二。

- 首先，如果FireEye裝置在域被移除後要重新新增域，則允許清單可防止出現進一步的問題。
- 其次，允許清單顯示了問題域的歷史記錄，這些域可用於調查分析或審計報告。

預設情況下，全域性允許清單應用於所有策略。將域新增到全域性允許清單會導致在所有策略中允許該域。

如果阻止模式中的FireEye安全設定僅應用於託管的Cisco Umbrella標識的子集（例如，它僅應用於漫遊電腦和流動裝置），則可以為這些標識或策略建立特定的允許清單。

要建立允許清單，請執行以下操作：

1.定位至策略>目標清單，然後選擇新增圖示。

2.選擇Allow，然後將您的域新增到清單中。

3.選擇儲存。

一旦儲存了目標清單，您就可以將其新增到覆蓋那些受不需要的阻止影響的客戶端的現有策略中。

從FireEye目標清單中刪除域

FireEye目標清單中的每個域名旁邊都有一個Delete圖示。通過刪除域，可以在發生意外檢測時清除FireEye目標清單。

但是，如果FireEye裝置將域重新傳送到Cisco Umbrella，則刪除操作不是永久性的。

刪除域：

1.定位至「設置」>「整合」，然後選擇「FireEye」將其展開。

2.選擇檢視域。

3.搜尋要刪除的域名。

4.選擇刪除圖示。

5.選擇關閉。

6.選擇「儲存」。

如果出現不需要的檢測或誤報，Umbrella建議立即在Cisco Umbrella中建立允許清單，然後在FireEye裝置內修正誤報。稍後，您可以從FireEye目標清單中刪除該域。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。