傘とFireEyeの統合

内容

はじめに

このドキュメントでは、Cisco UmbrellaとFireEyeを統合する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 公衆インターネットにアクセスできるFireEyeアプライアンス。
- Cisco Umbrellaダッシュボードの管理者権限
- Cisco UmbrellaダッシュボードでFireEye統合を有効にする必要がある

使用するコンポーネント

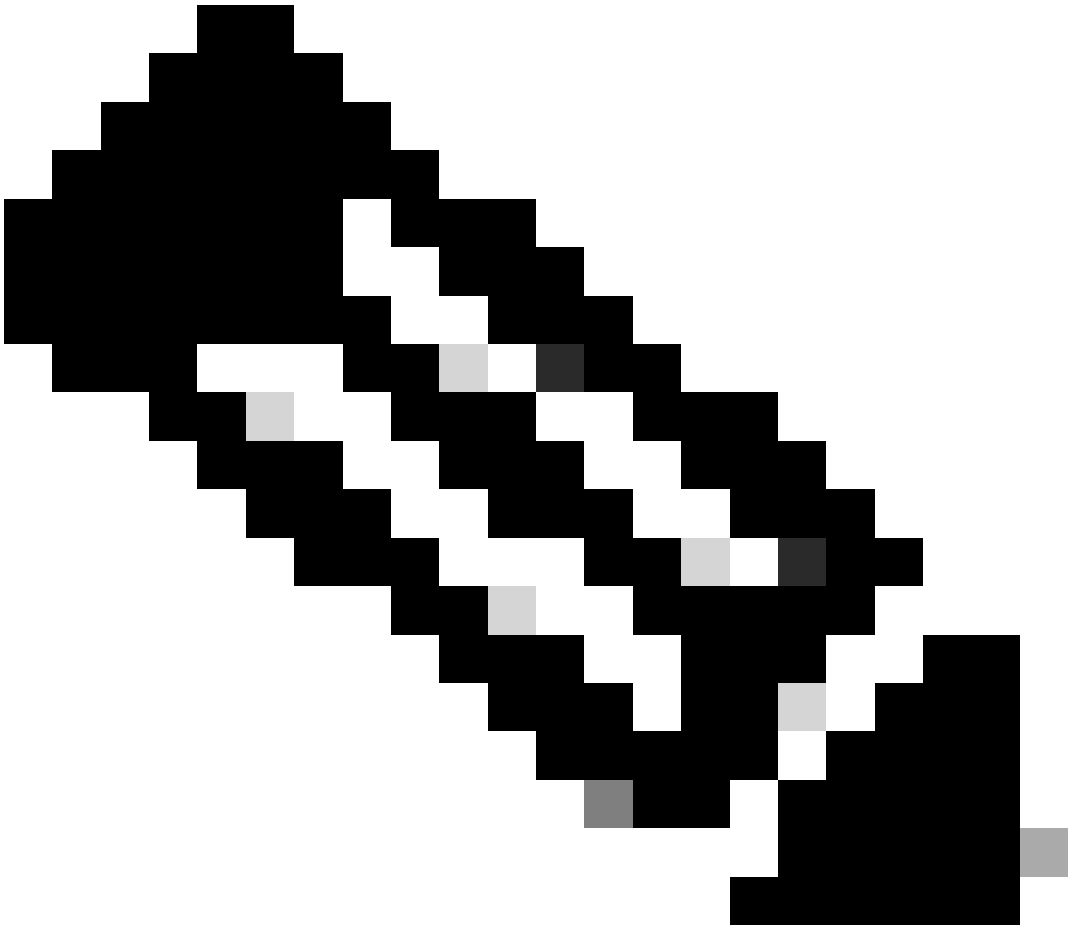
このドキュメントの情報は、Cisco Umbrellaに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

概要

FireEyeセキュリティアプライアンスとCisco Umbrellaの統合により、セキュリティ担当者と管理者は、分散した企業ネットワークに別の適用レイヤを提供しながら、ローミングするラップトップ、タブレット、または電話への高度な脅威に対する保護を拡張できます。

このガイドでは、Cisco Umbrellaと通信するようにFireEyeを設定し、FireEyeのセキュリティイベントをCisco Umbrellaで保護されているクライアントに適用できるポリシーに統合する方法について説明します。



注：FireEye統合は、DNS Essentials、DNS Advantage、SIG Essentials、SIG AdvantageなどのCisco Umbrellaパッケージにのみ含まれています。これらのパッケージ

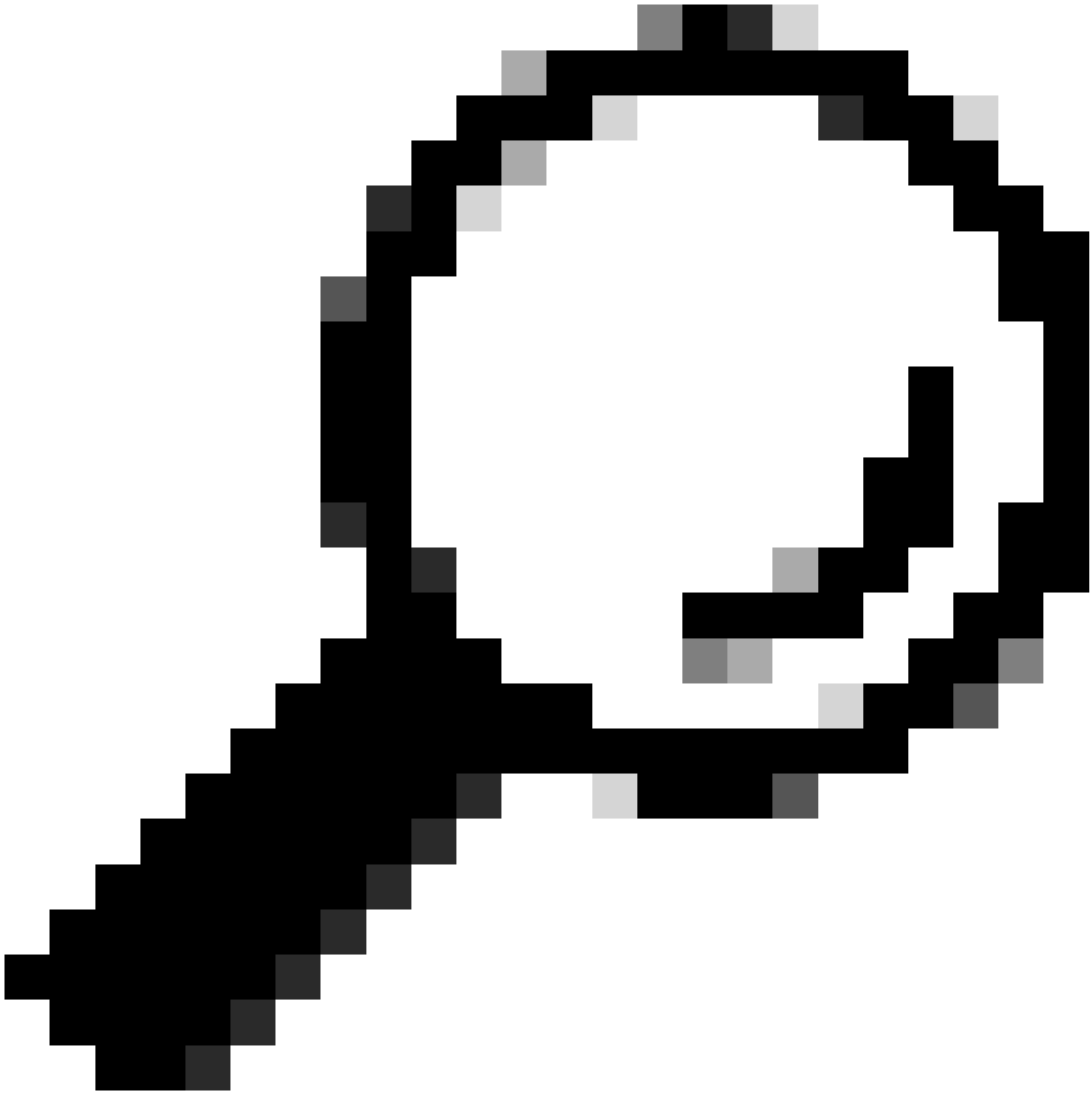
がなく、FireEye統合を希望する場合は、Cisco Umbrellaアカウントマネージャにお問い合わせください。正しいCisco Umbrellaパッケージがあっても、ダッシュボードの統合としてFireEyeが表示されない場合は、Cisco Umbrellaサポートにお問い合わせください。

統合機能

FireEyeアプライアンスは、最初に、検出したインターネットベースの脅威（マルウェアをホストするドメイン、ボットネットのコマンドと制御、フィッシングサイトなど）をCisco Umbrellaに送信します。

次に、Cisco Umbrellaに渡された情報が検証され、有効でポリシーに追加可能であることが確認されます。FireEyeからの情報が正しくフォーマットされていることが確認された場合（ファイル、複雑なURL、人気の高いドメインではない場合など）、任意のCisco Umbrellaポリシーに適用可能なセキュリティ設定の一部として、ドメインアドレスがFireEye宛先リストに追加されます。このポリシーは、FireEye宛先リストを持つポリシーを使用してデバイスから行われるすべての要求にただちに適用されます。

今後、Cisco UmbrellaはFireEyeアラートを自動的に解析し、悪意のあるサイトをFireEye宛先リストに追加します。これにより、すべてのリモートユーザとデバイスにFireEye保護が拡張され、企業ネットワークに別の適用レイヤが提供されます。



ヒント:Cisco Umbrellaは、一般的に安全であることが知られているドメイン（GoogleやSalesforceなど）の検証と許可に最善を尽くしますが、不要な中断を回避するために、ポリシーに従って、ブロックしたことがないドメインをGlobal Allow Listまたは他の宛先リストに追加することをお勧めします。次に例を示します。

- 組織のホームページ
- 内部レコードと外部レコードの両方を持つことができる、提供するサービスを表すドメイン。たとえば、「mail.myservicedomain.com」や「portal.myotherservicedomain.com」などです。
- Cisco Umbrellaに依存しているあまり知られていないクラウドベースのアプリケーションは、ドメインの自動検証に含まれません。例：「localcloudservice.com」。

これらのドメインは、Cisco UmbrellaのPolicies > Destination ListsにあるGlobal Allow Listに追加できます。

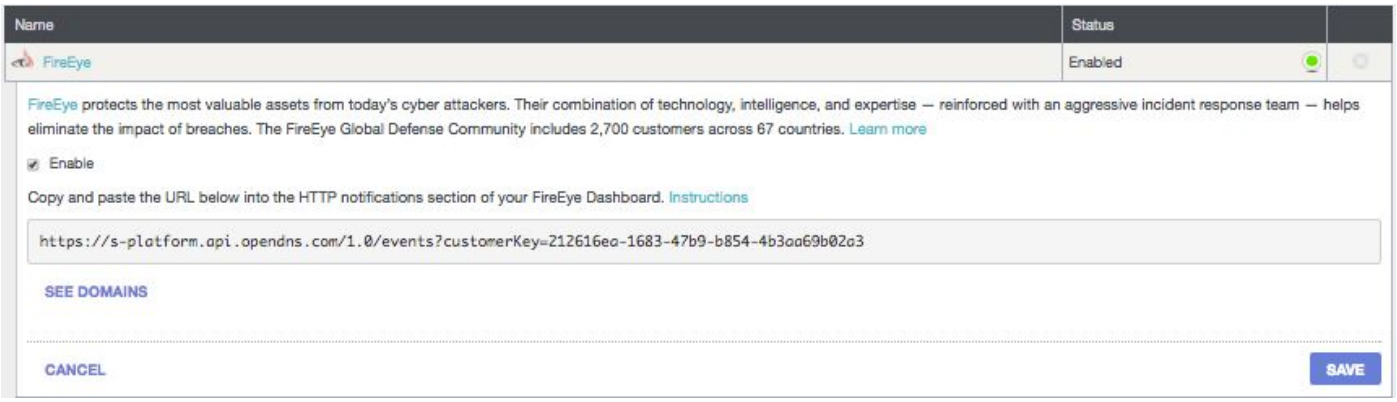
FireEyeから情報を受信するためのCisco Umbrellaダッシュボードの設定

最初に、FireEyeアプライアンスと通信するための固有のURLをCisco Umbrellaで見つけます。

1. Cisco Umbrellaダッシュボードに管理者として口グインします。

2. Policies > Policy Components > Integrationsの順に移動し、テーブル内でFireEyeを選択して展開します。

3. Enableボックスを選択してから、Saveを選択します。これにより、Cisco Umbrella内の組織固有のURLが生成されます。

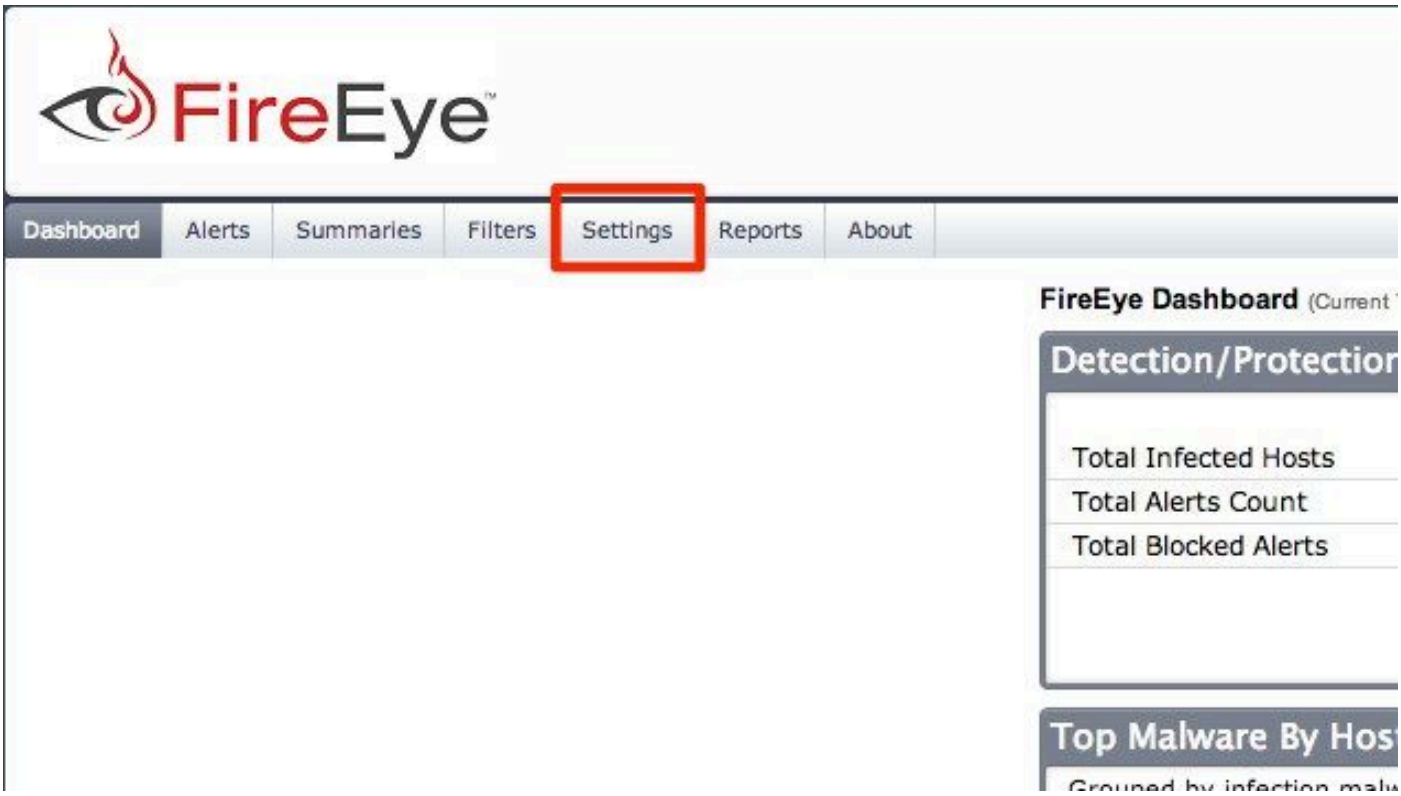


後でこのURLを使用して、FireEyeアプライアンスがCisco Umbrellaにデータを送信するように設定できるため、URLをコピーしてください。

Cisco Umbrellaと通信するためのFireEyeの設定

FireEyeアプライアンスからCisco Umbrellaへのトラフィックの送信を開始するには、前のセクションで生成されたURL情報でFireEyeを設定する必要があります。

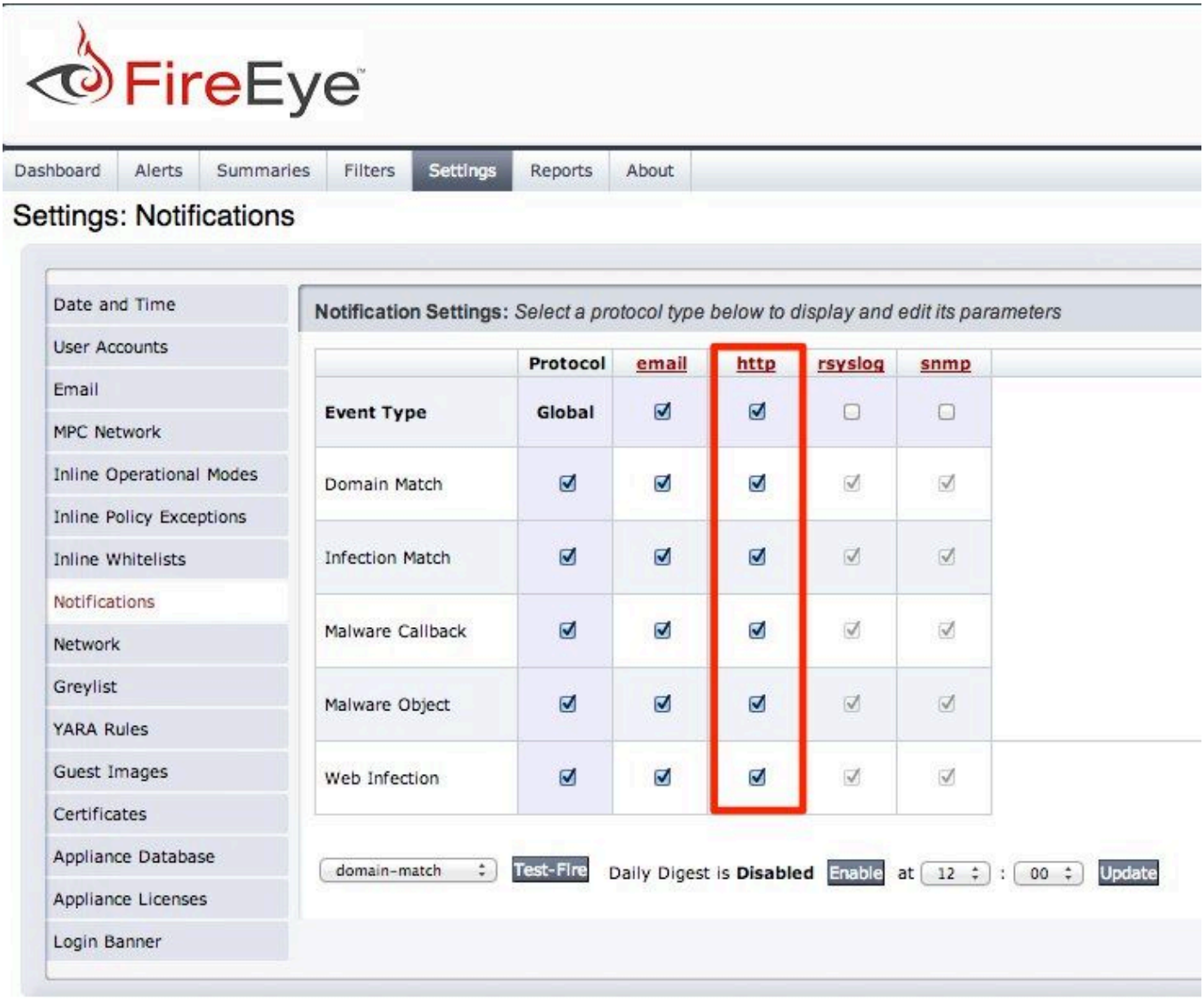
1. FireEyeに口グインし、Settingsを選択します。



2. 設定のリストからNotificationsを選択します。

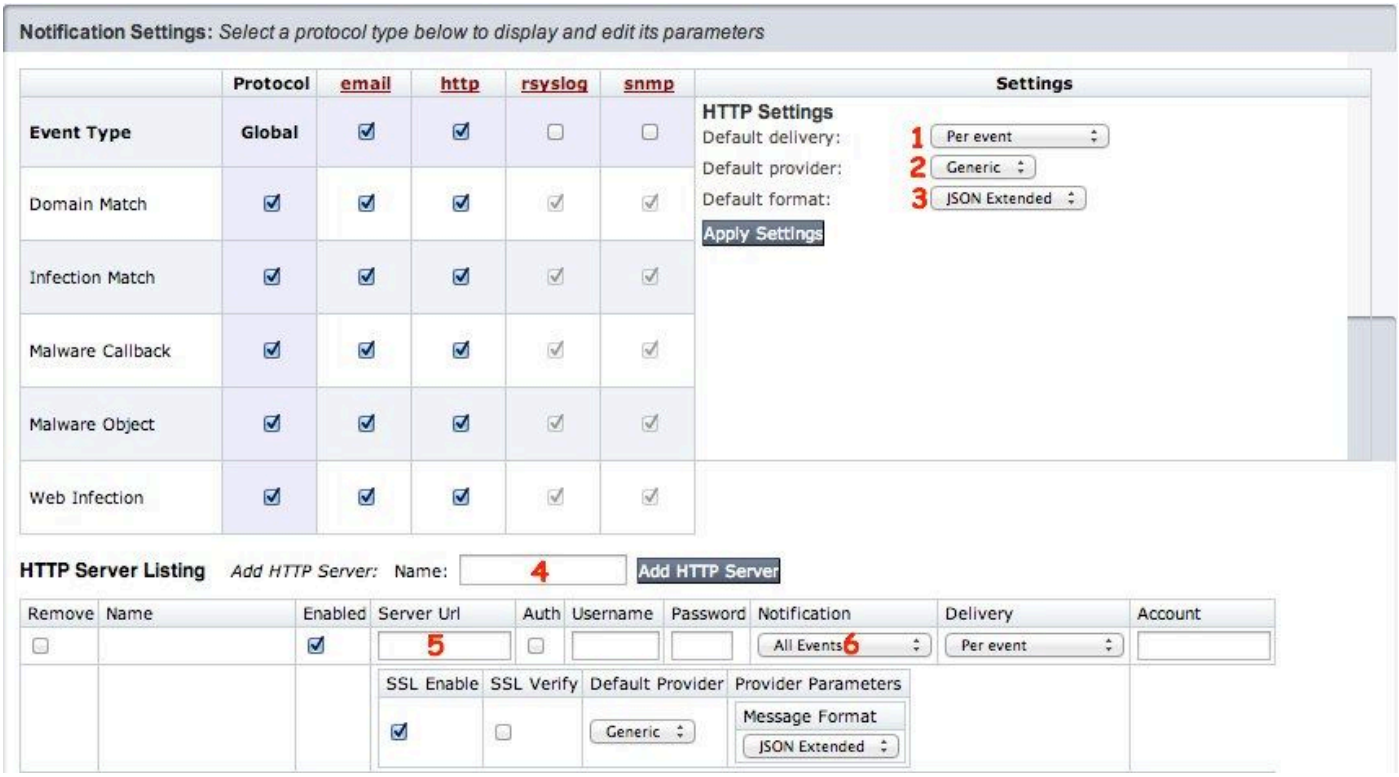

FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance 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. Cisco Umbrellaに送信されるすべてのイベントタイプが選択されていることを確認します（Umbrellaではallから開始することを推奨します）。次に、列の上部にあるHTTP リンクを選択します。



4. メニューが展開されたら、次のオプションを選択してイベント通知を使用可能にします。番号付きの手順がスクリーンショットに示されています。

1. デフォルトの配信：イベント単位
2. 既定のプロバイダ：汎用
3. デフォルトの形式：JSON拡張
4. HTTP Serverに「OpenDNS」という名前を付けます。
5. サーバURL:前の手順でCisco Umbrellaダッシュボードから生成したCisco Umbrella URLをここに貼り付けます。
6. 通知ドロップダウン：カバレッジを最大にするには、すべてのイベントを選択します。



5. Delivery、Default Provider、およびProvider Parametersのドロップダウンがすべてデフォルト設定に一致していることを確認します。一致していない場合は複数の通知サーバが使用されています。

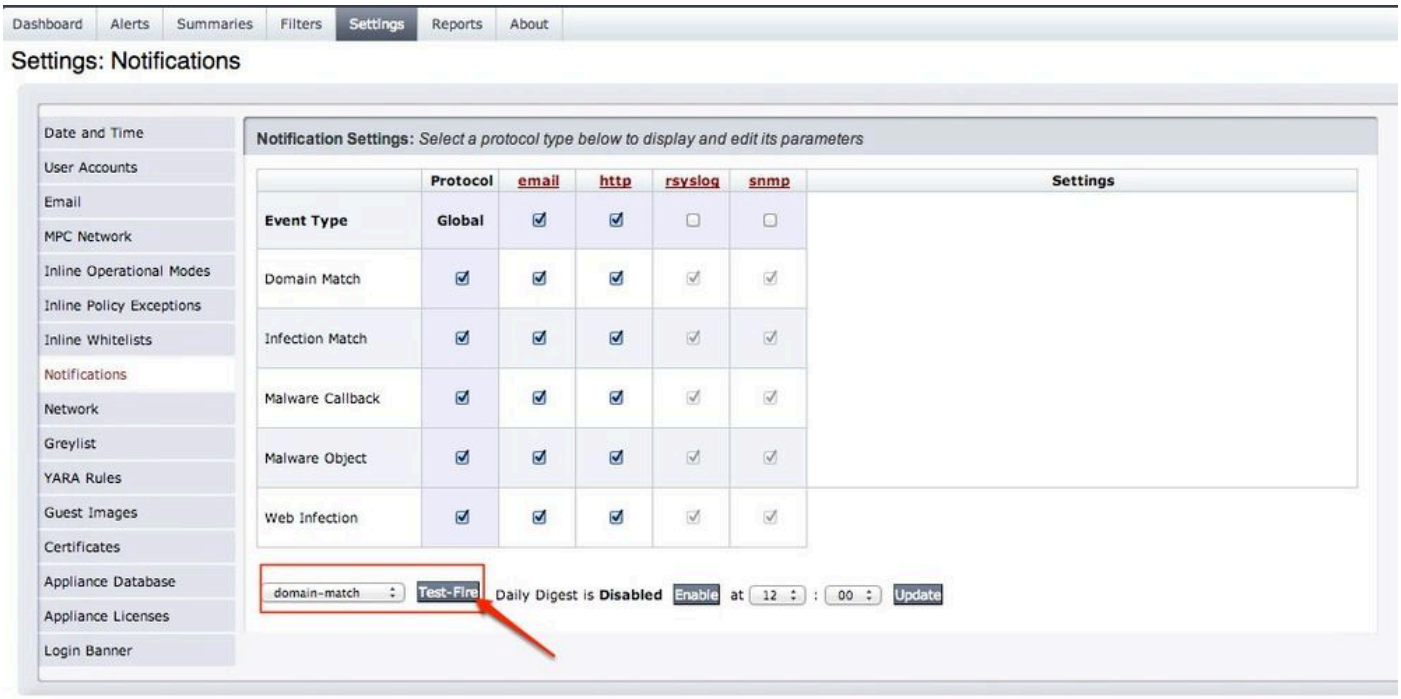
- 配信：イベント単位
- 既定のプロバイダ：汎用
- プロバイダーパラメーター：メッセージ形式JSON拡張
- （オプション）SSL経由でトラフィックを送信する場合は、SSL Enableを選択します。

この時点で、選択したイベントタイプをCisco Umbrellaに送信するようにFireEyeアプライアンスが設定されます。次に、この情報をCisco Umbrellaダッシュボードで確認し、このトラフィックをブロックするポリシーを設定する方法について説明します。

接続の確認：FireEyeとCisco Umbrellaの間の「テストファイア」

この時点で、接続をテストし、すべてが正しく設定されていることを確認することをお勧めします。

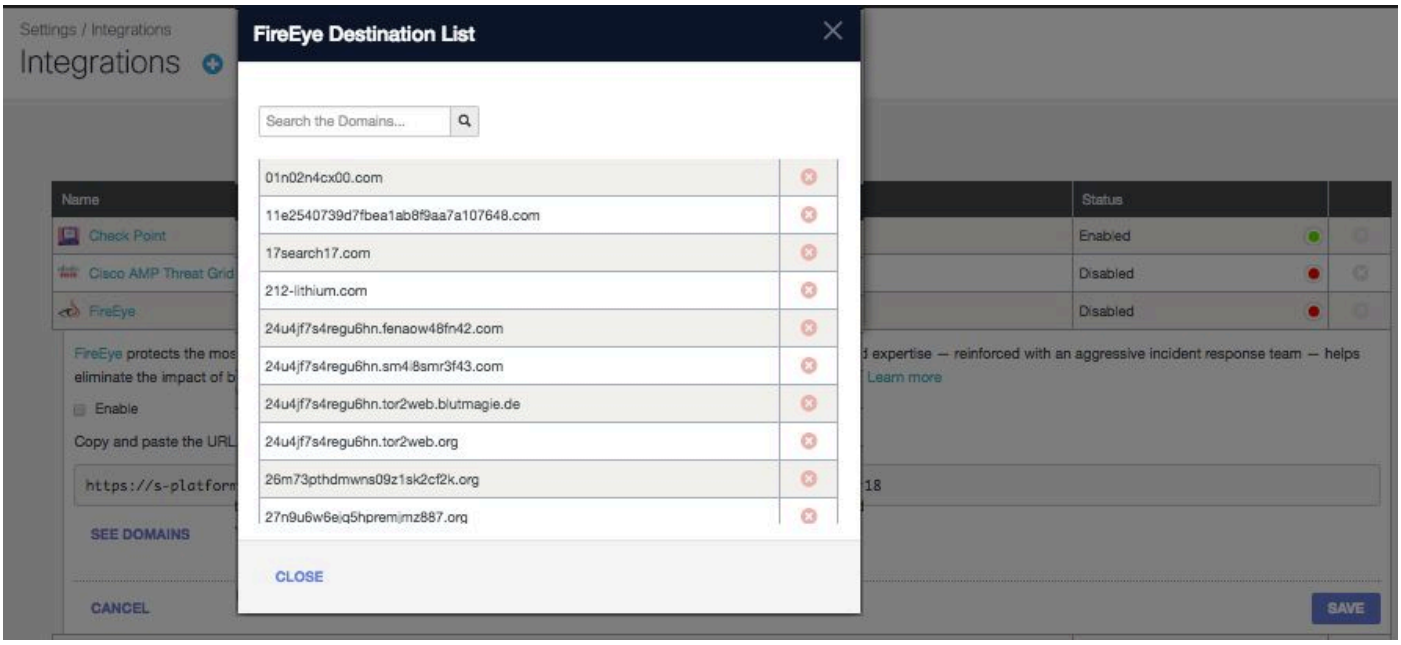
1. FireEyeで、Test Fireドロップダウンからdomain-matchを選択し、Test Fireを選択します。



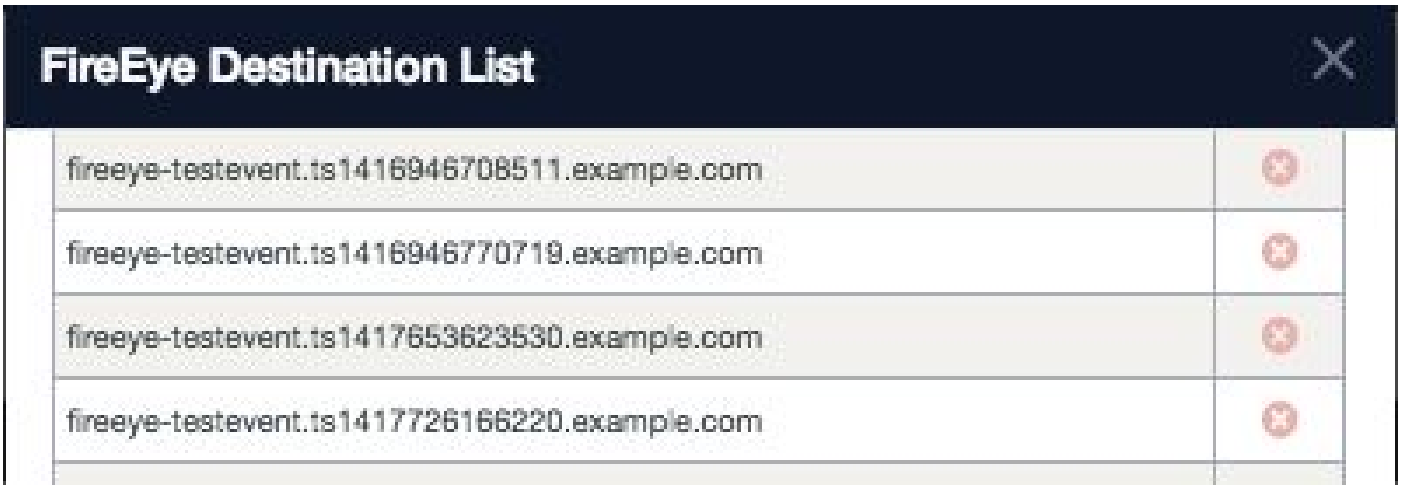
Cisco Umbrellaでは、FireEye統合には、どのドメインがアクティブに追加されているかを確認するためにFireEyeアプライアンスから提供されるドメインのリストが含まれます。

2. Test Fireを選択した後、Cisco UmbrellaでSettings > Integrations に移動し、テーブルでFireEyeを選択して展開します。

3. 「ドメインを表示」を選択します。



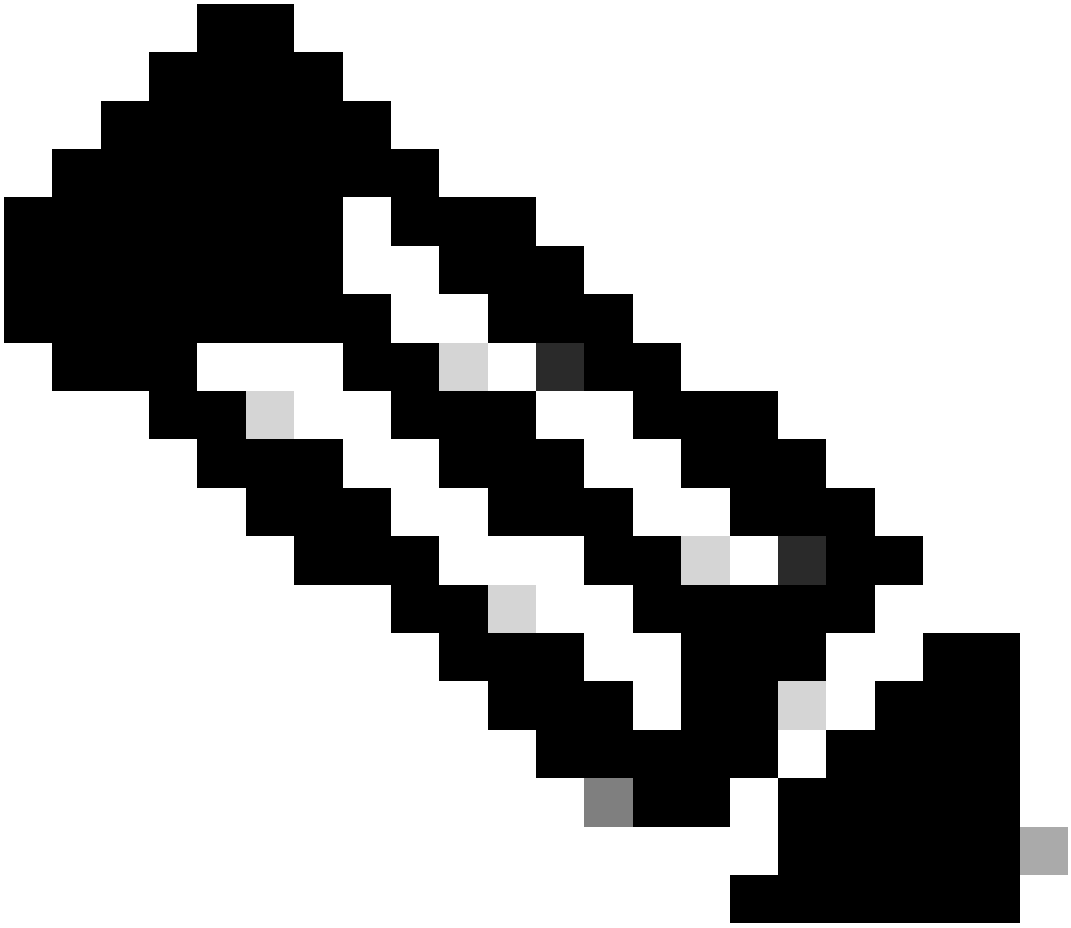
Test Fireを選択すると、FireEye Destinations Listに「fireeye-testevent.example.com-[date]」という名前のドメインが生成されます。FireEyeでTest Fireを選択するたびに、テストに添付されるUNIX工ポック時間の日付を持つ一意のドメインが作成されるため、以降のテストでは一意のテストドメイン名を持つことができます。



Test Fireが成功すると、FireEyeからさらに多くのイベントがCisco Umbrellaに送信され、検索可能なリストが作成されて拡大し始めます。

「監査モード」でFireEyeセキュリティ設定に追加されたイベントの監視

FireEyeアプライアンスからのイベントは、FireEyeセキュリティカテゴリとしてポリシーに適用できる特定の宛先リストへの入力を開始します。デフォルトでは、宛先リストとセキュリティカテゴリは「監査モード」であり、ポリシーには適用されず、既存のCisco Umbrellaポリシーを変更することはできません。



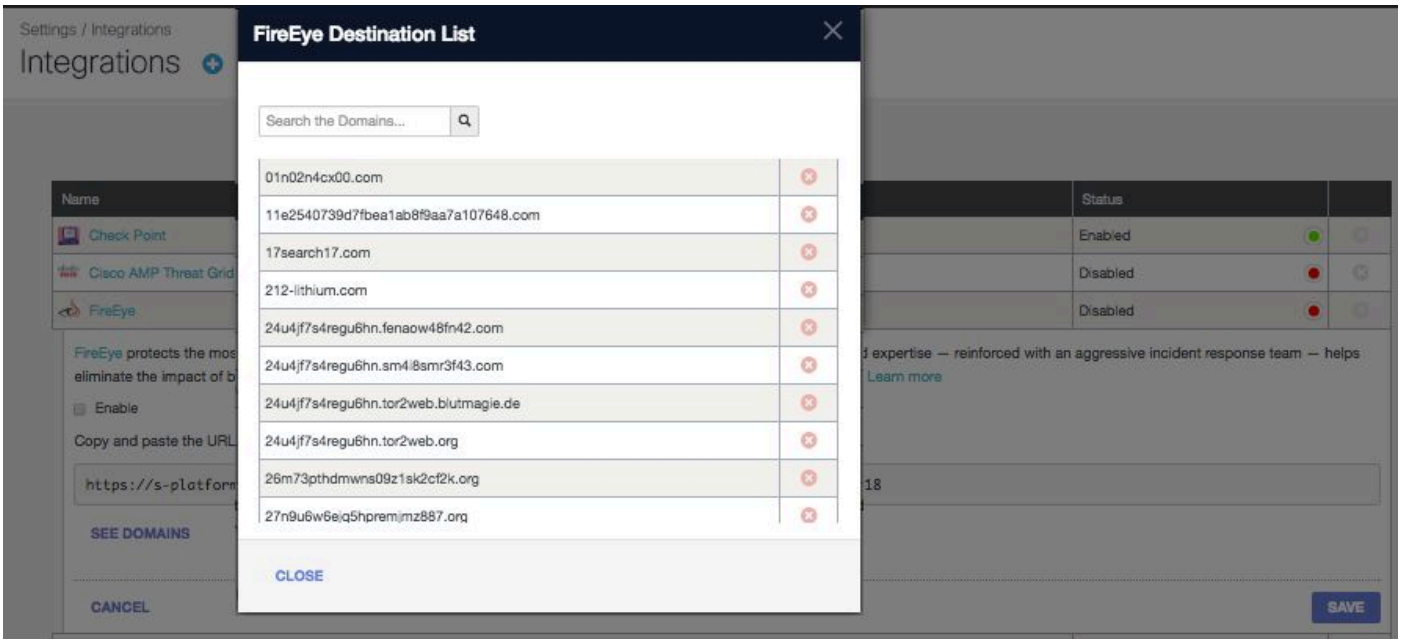
注:「監査モード」は、導入プロファイルとネットワーク設定に基づいて、必要な期間だけ有効にできます。

宛先リストの確認

FireEyeの宛先リストは、次の操作を実行していつでも確認できます。

1. 「ポリシー」>「ポリシー・コンポーネント」>「統合」に移動します。

2. テーブル内でFireEyeを展開し、See Domainsを選択します。

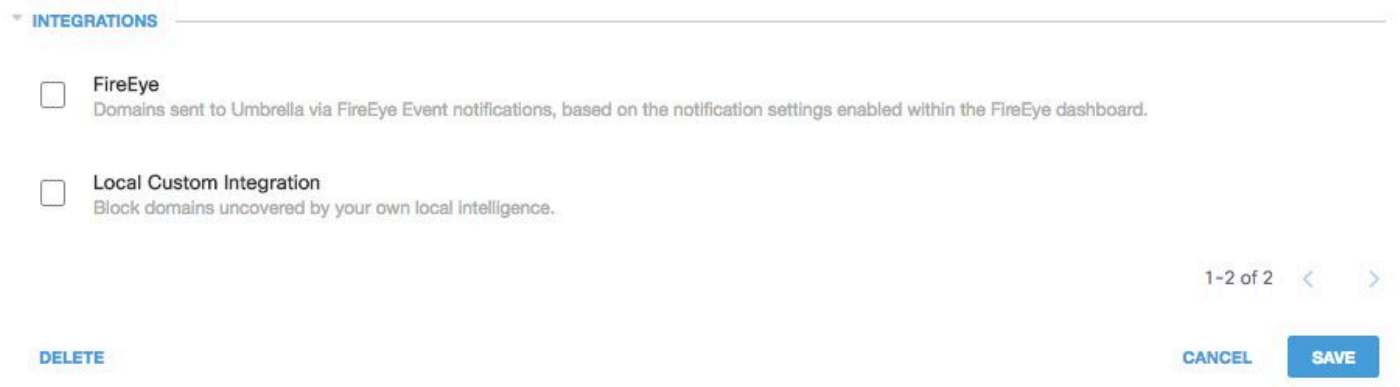


ポリシーのセキュリティ設定の確認

ポリシーに追加できるセキュリティ設定は、いつでも確認できます。

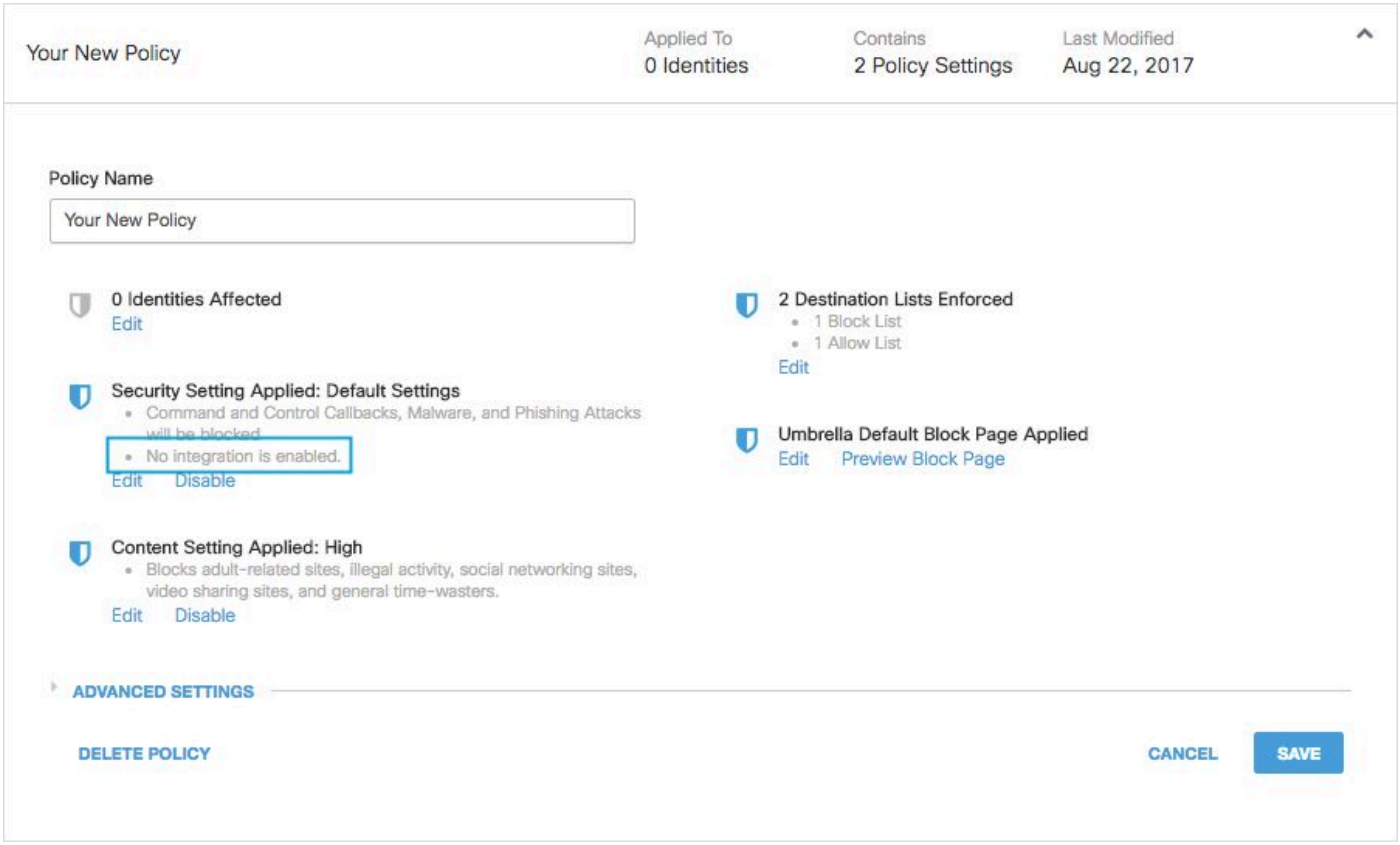
1. [ポリシー] > [ポリシーコンポーネント] > [セキュリティ設定] に移動します。

2. 表内のセキュリティ設定を選択して展開し、「統合」までスクロールしてFireEye設定を見つけます。



115014080803

統合情報は、[セキュリティ設定の概要]ページでも確認できます。



115013920526

作業を開始する際は、ドメインが「監査モード」で正しく入力されていることを確認するために、このセキュリティ設定をオフにしておくことをお勧めします。

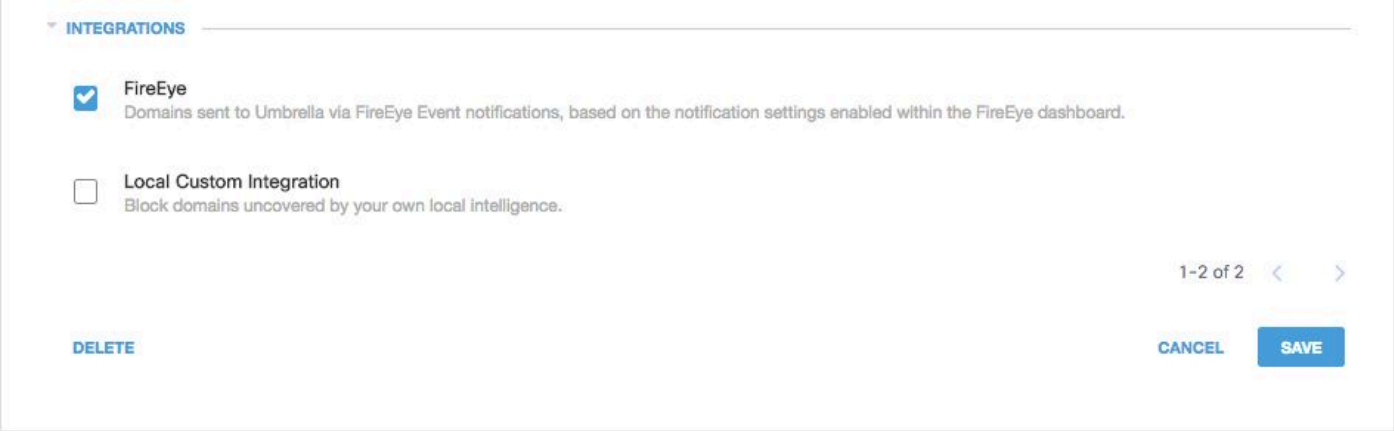
「ブロックモード」でのFireEyeセキュリティ設定の管理対象クライアントのポリシーへの適用

Cisco Umbrellaによって管理されるクライアントによってこれらの追加のセキュリティ脅威を適用する準備ができたら、既存のポリシーのセキュリティ設定を変更するか、または最初に確実に適用されるようにデフォルトポリシーの上に配置される新しいポリシーを作成します。

最初に、セキュリティ設定を作成または更新します。

1. 「ポリシー」>「ポリシー・コンポーネント」>「セキュリティ設定」に移動します。

2. Integrationsで、FireEyeを選択し、Saveを選択します。



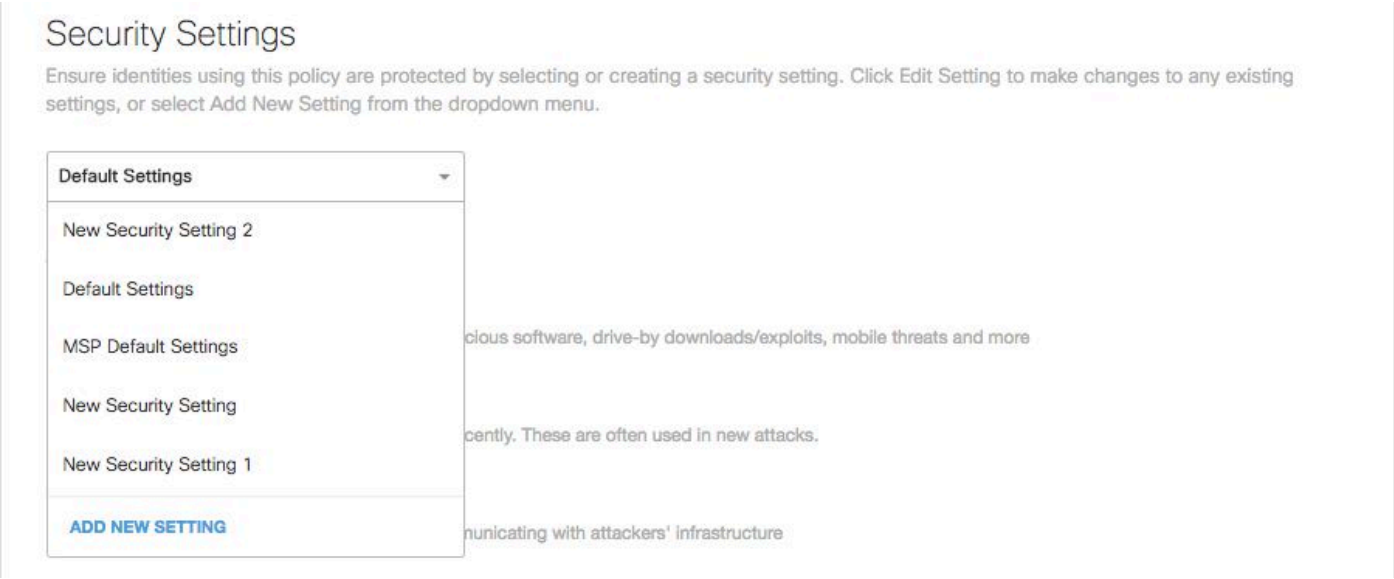
115013921406

次に、ポリシーウィザードで、編集中のポリシーにこのセキュリティ設定を追加します。

1. Policies > Policy Listの順に移動します。

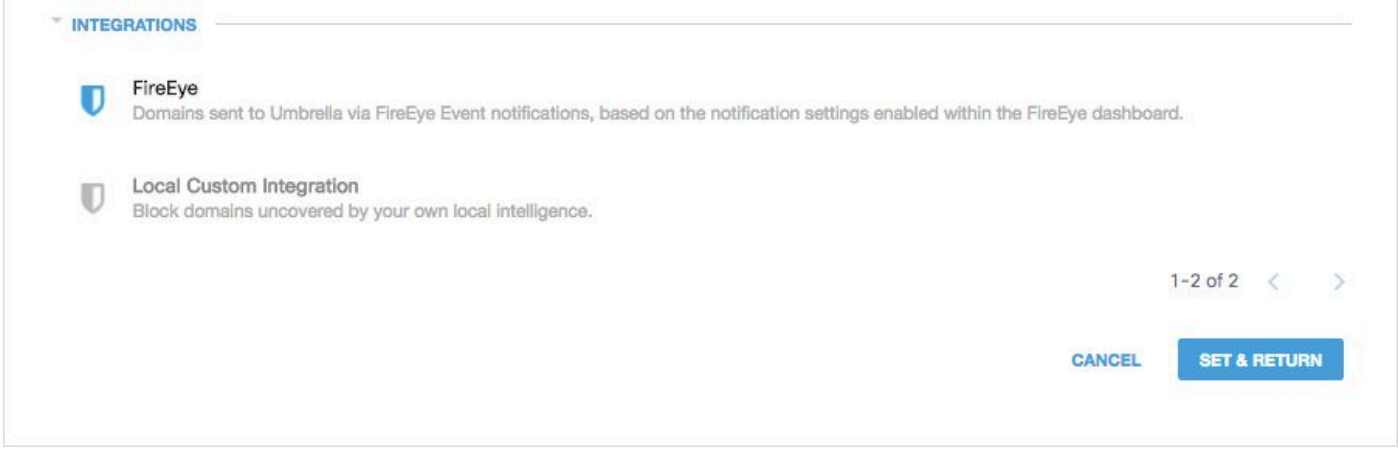
2. ポリシーを展開し、Security Setting Appliedの下でEditを選択します。

3. [セキュリティ設定] ドロップダウンで、FireEye設定を含むセキュリティ設定を選択します。



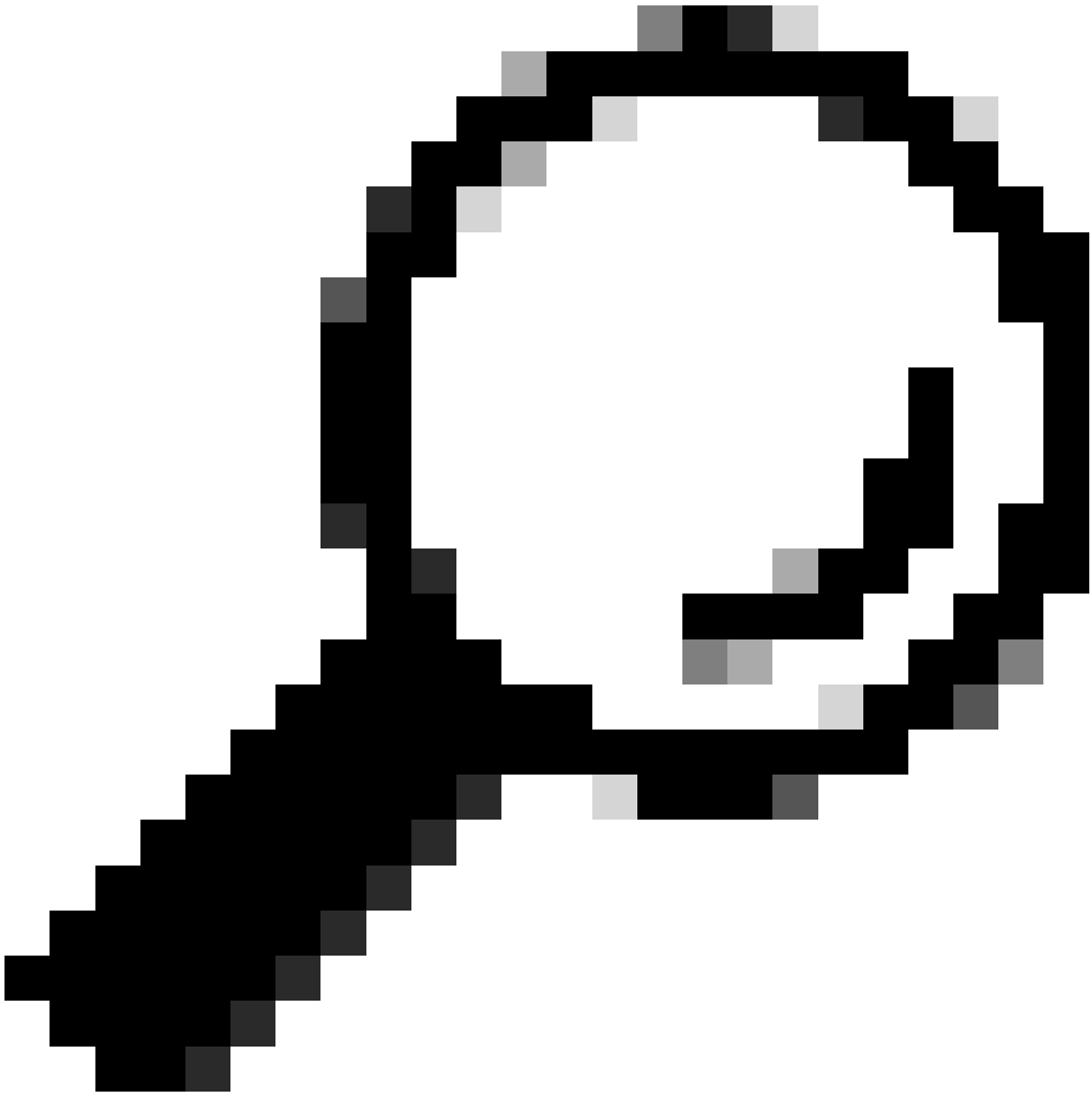
115014083083

「統合」の下のシールドアイコンが青色に更新されます。



115013922146

4. Set &Returnを選択します。



ヒント：ポリシーウィザードでセキュリティ設定を編集することもできます。

FireEyeのセキュリティ設定内に含まれるFireEyeドメインは、ポリシーを使用してIDに対してブロックされます。

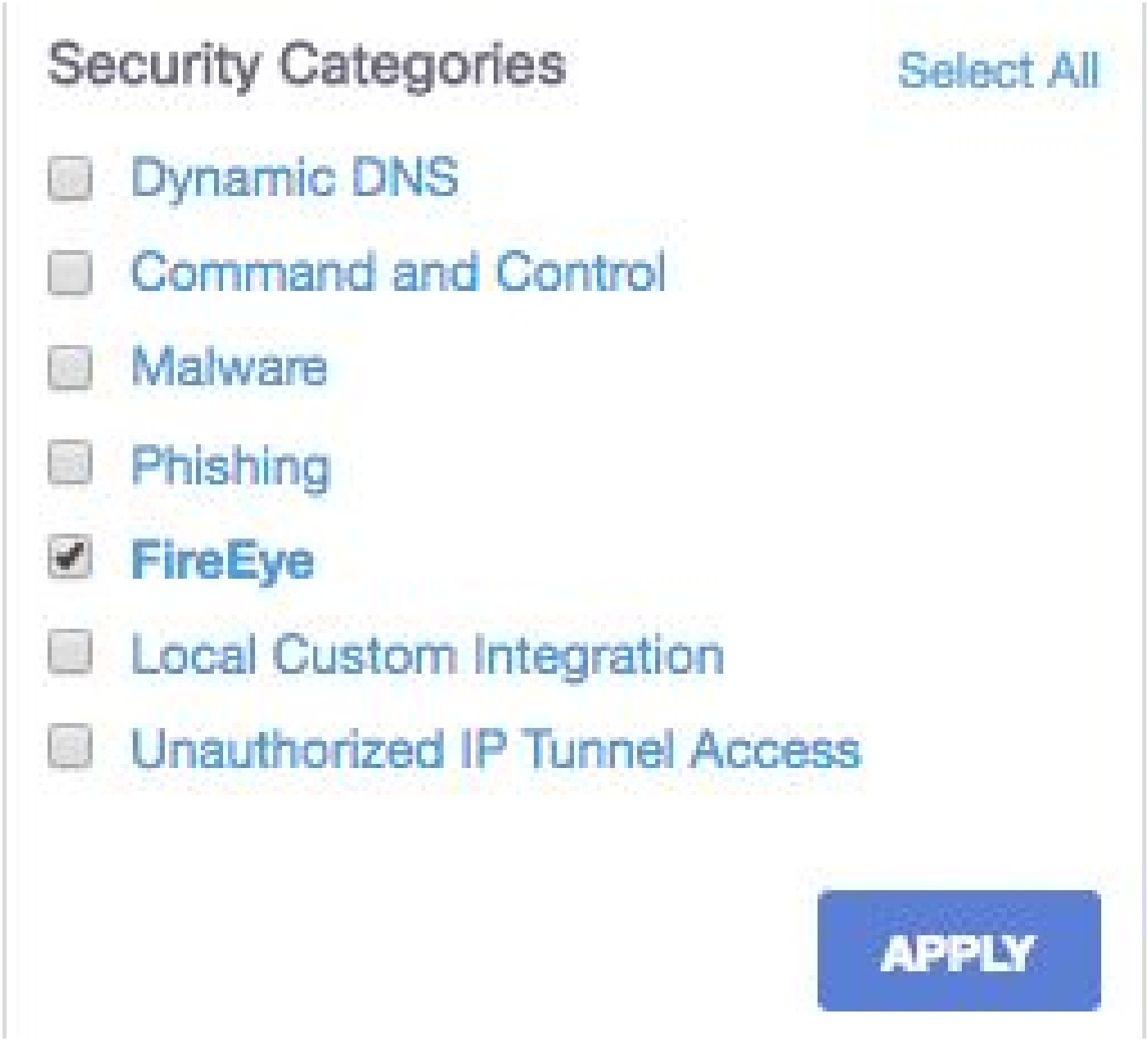
FireEyeイベントに関するCisco Umbrella内のレポート

FireEyeセキュリティイベントのレポート

FireEye宛先リストは、レポートに使用できるセキュリティカテゴリの1つです。ほとんどのレポートまたはすべてのレポートでは、セキュリティカテゴリがフィルタとして使用されます。たとえば、セキュリティカテゴリをフィルタリングして、FireEye関連のアクティビティのみを表示できます。

1. 「レポート」 > 「活動検索」にナビゲートします。

2. [Security Categories] で、[FireEye]を選択して、FireEyeのセキュリティカテゴリのみを表示するようにレポートをフィルタ処理します。



115013924986

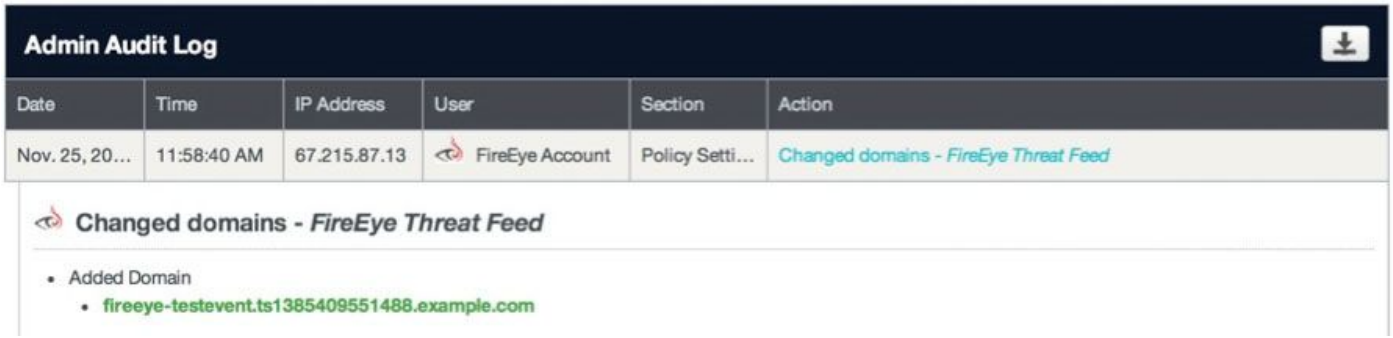
3. 「適用」を選択して、レポートで選択した期間のFireEye関連のアクティビティを表示します。

FireEye宛先リストにドメインが追加された日時のレポート

管理監査ログには、宛先リストにドメインを追加する際のFireEyeアプライアンスからのイベントが含まれます。FireEye口ゴが付いた「FireEye Account」という名前のユーザがイベントを生成します。これらのイベントには、追加されたドメインと追加時刻が含まれます。

「FireEyeアカウント」ユーザのフィルタを適用することで、FireEyeの変更のみを含めるようにフィルタリングできます。

前述の「Test Fire」ステップを実行した場合、FireEyeテストドメインの追加が監査ログに表示される可能性があります。



不要な検出や誤検出の処理

許可リスト

まれに、FireEyeアプライアンスによって自動的に追加されたドメインが、ユーザによる特定のWebサイトへのアクセスをブロックする不要な検出をトリガーする可能性があります。このような状況では、Umbrellaは許可リスト(Policies > Destination Lists)にドメインを追加することを推奨します。この許可リストは、セキュリティ設定を含め、他のすべてのタイプのブロックリストよりも優先されます。

このアプローチが望ましい理由は2つあります。

- まず、FireEyeアプライアンスがドメインを削除した後にドメインを再追加する場合、許可リストは、この問題を引き起こすさらなる問題を防ぎます。
- 2番目に、許可リストは、調査または監査レポートに使用できる問題のあるドメインの履歴レコードを示します。

デフォルトでは、すべてのポリシーに適用されるグローバル許可リストがあります。グローバル許可リストにドメインを追加すると、ドメインはすべてのポリシーで許可されます。

ブロックモードのFireEyeセキュリティ設定が、管理対象のCisco Umbrellaアイデンティティのサブセットにのみ適用される（たとえば、ローミングコンピュータやモバイルデバイスにのみ適用される）場合、これらのアイデンティティまたはポリシーの特定の許可リストを作成できます。

許可リストを作成するには、次の手順を実行します。

1. Policies > Destination Listsの順に移動し、Addアイコンを選択します。

2. Allowを選択し、リストにドメインを追加します。

3. Saveを選択します。

宛先リストを保存したら、不要なブロックの影響を受けるクライアントをカバーする既存のポリシーに追加できます。

FireEye宛先リストからのドメインの削除

FireEye宛先リストの各ドメイン名の横に、削除アイコンが表示されます。ドメインを削除すると、不必要な検出が発生した場合にFireEye宛先リストをクリーンアップできます。

ただし、FireEyeアプライアンスがドメインをCisco Umbrellaに再送信する場合、この削除は永続的にはありません。

ドメインを削除するには

1. [設定] > [統合]に移動し、[FireEye]を選択して展開します。

2. 「ドメインを表示」を選択します。

3. 削除するドメイン名を検索します。

4. 「削除」アイコンを選択します。

5. Closeを選択します。

6. 「保存」を選択します。

不必要な検出または誤検出の場合、Umbrellaは、Cisco Umbrellaで許可リストを即座に作成し、FireEyeアプライアンス内で誤検出を修復することを推奨します。後で、FireEye宛先リストからドメインを削除できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。