Integration von Umbrella mit FireEye

Inhalt

Einleitung

In diesem Dokument wird die Integration von Cisco Umbrella mit FireEye beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Eine FireEye-Appliance mit Zugriff auf das öffentliche Internet.
- Administratorrechte für das Cisco Umbrella Dashboard
- Auf dem Cisco Umbrella Dashboard muss die FireEye-Integration aktiviert sein.

Verwendete Komponenten

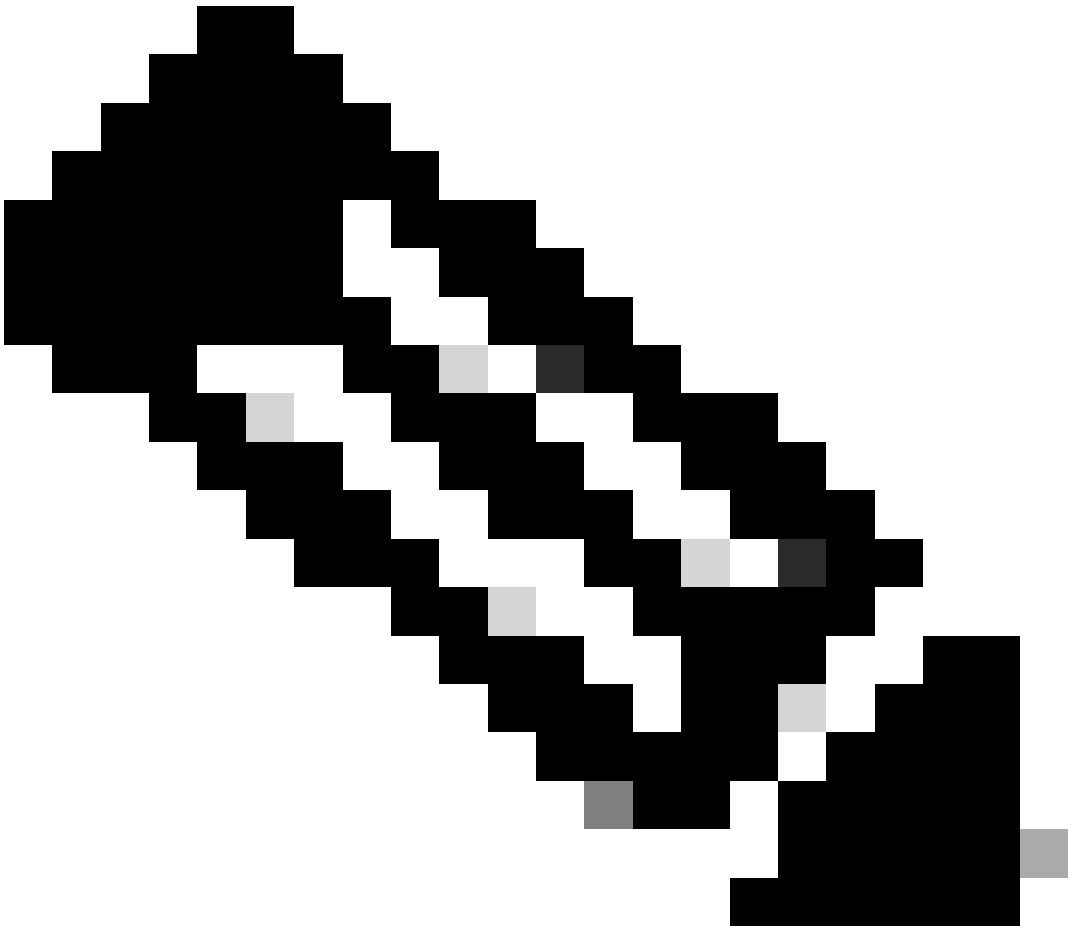
Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Durch die Integration der FireEye Security Appliance mit Cisco Umbrella können Sicherheitsbeauftragte und Administratoren jetzt den Schutz vor komplexen Bedrohungen auf Laptops, Tablets oder Telefone ausdehnen und gleichzeitig eine weitere Durchsetzungsebene für ein verteiltes Unternehmensnetzwerk bereitstellen.

In diesem Leitfaden wird erläutert, wie Sie FireEye für die Kommunikation mit Cisco Umbrella konfigurieren, damit Sicherheitsereignisse aus FireEye in Richtlinien integriert werden, die auf Clients angewendet werden können, die durch Cisco Umbrella geschützt sind.



Anmerkung: Die FireEye-Integration ist nur in Cisco Umbrella-Paketen wie DNS

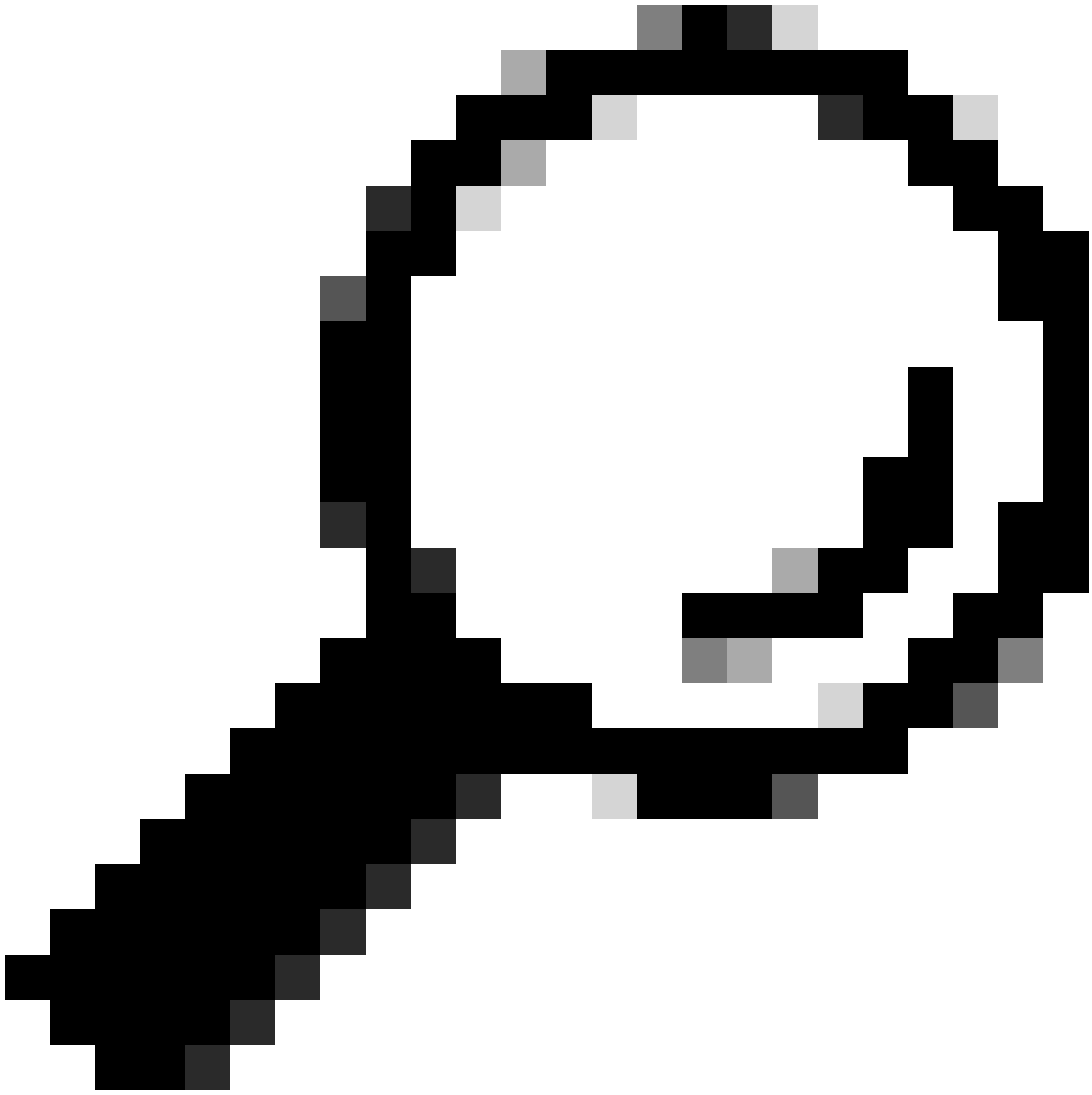
Essentials, DNS Advantage, SIG Essentials oder SIG Advantage enthalten. Wenn Sie keines dieser Pakete nutzen und die FireEye-Integration nutzen möchten, wenden Sie sich an Ihren Cisco Umbrella Account Manager. Wenn Sie über das richtige Cisco Umbrella-Paket verfügen, FireEye aber nicht als Integrationslösung für Ihr Dashboard sehen, wenden Sie sich an den Cisco Umbrella Support.

Integrationsfunktion

Die FireEye-Appliance sendet zunächst gefundene internetbasierte Bedrohungen, wie Domänen, die Malware hosten, Command-and-Control-Funktionen für Botnet- oder Phishing-Websites, an Cisco Umbrella.

Cisco Umbrella validiert die an Cisco Umbrella übergebenen Informationen, um sicherzustellen, dass sie gültig sind und einer Richtlinie hinzugefügt werden können. Wenn die Informationen von FireEye als korrekt formatiert bestätigt werden (es sich beispielsweise nicht um eine Datei, eine komplexe URL oder eine sehr beliebte Domäne handelt), wird die Domänenadresse der FireEye-Zielliste als Teil einer Sicherheitseinstellung hinzugefügt, die auf eine beliebige Cisco Umbrella-Richtlinie angewendet werden kann. Diese Richtlinie wird sofort auf alle Anforderungen angewendet, die von Geräten mithilfe von Richtlinien mit der FireEye-Zielliste gestellt werden.

In Zukunft analysiert Cisco Umbrella automatisch FireEye-Warnungen und fügt der FireEye-Zielliste bösartige Websites hinzu. Dadurch wird der FireEye-Schutz auf alle Remote-Benutzer und -Geräte ausgedehnt und eine weitere Durchsetzungsebene für Ihr Unternehmensnetzwerk geschaffen.



Tipp: Während Cisco Umbrella nach besten Kräften versucht, bekanntermaßen sichere Domains (z. B. Google und Salesforce) zu validieren und zuzulassen, empfehlen wir, Domains, die niemals blockiert werden sollen, der globalen Zulassungsliste oder anderen Ziellisten gemäß Ihrer Richtlinie hinzuzufügen, um unerwünschte Unterbrechungen zu vermeiden. Beispiele:

- Die Startseite Ihres Unternehmens
- Domänen, die von Ihnen bereitgestellte Dienste darstellen und sowohl interne als auch externe Datensätze enthalten können. Beispiel: "mail.myservicedomain.com" und "portal.myotherservicedomain.com".
- Weniger bekannte Cloud-basierte Anwendungen, von denen Cisco Umbrella abhängt, werden nicht automatisch für die Domänenvalidierung validiert. Beispiel: "localcloudservice.com".

Diese Domänen können der globalen Zulassungsliste hinzugefügt werden, die unter

Richtlinien > Ziellisten in Cisco Umbrella zu finden ist.

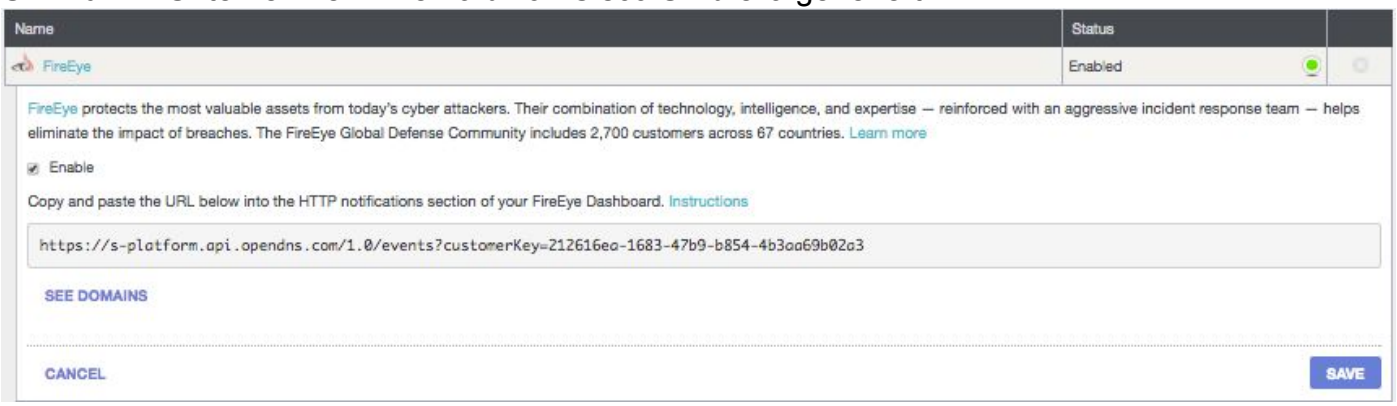
Konfigurieren des Cisco Umbrella Dashboards zum Empfangen von Informationen von FireEye

Der erste Schritt besteht darin, Ihre eindeutige URL in Cisco Umbrella für die FireEye-Appliance zu finden.

1. Melden Sie sich als Administrator beim Cisco Umbrella Dashboard an.

2. Navigieren Sie zu Richtlinien > Richtlinienkomponenten > Integrationen, und wählen Sie FireEye in der Tabelle aus, um die Liste zu erweitern.

3. Wählen Sie das Feld Aktivieren und dann Speichern. Dadurch wird eine eindeutige, spezifische URL für Ihr Unternehmen innerhalb von Cisco Umbrella generiert.

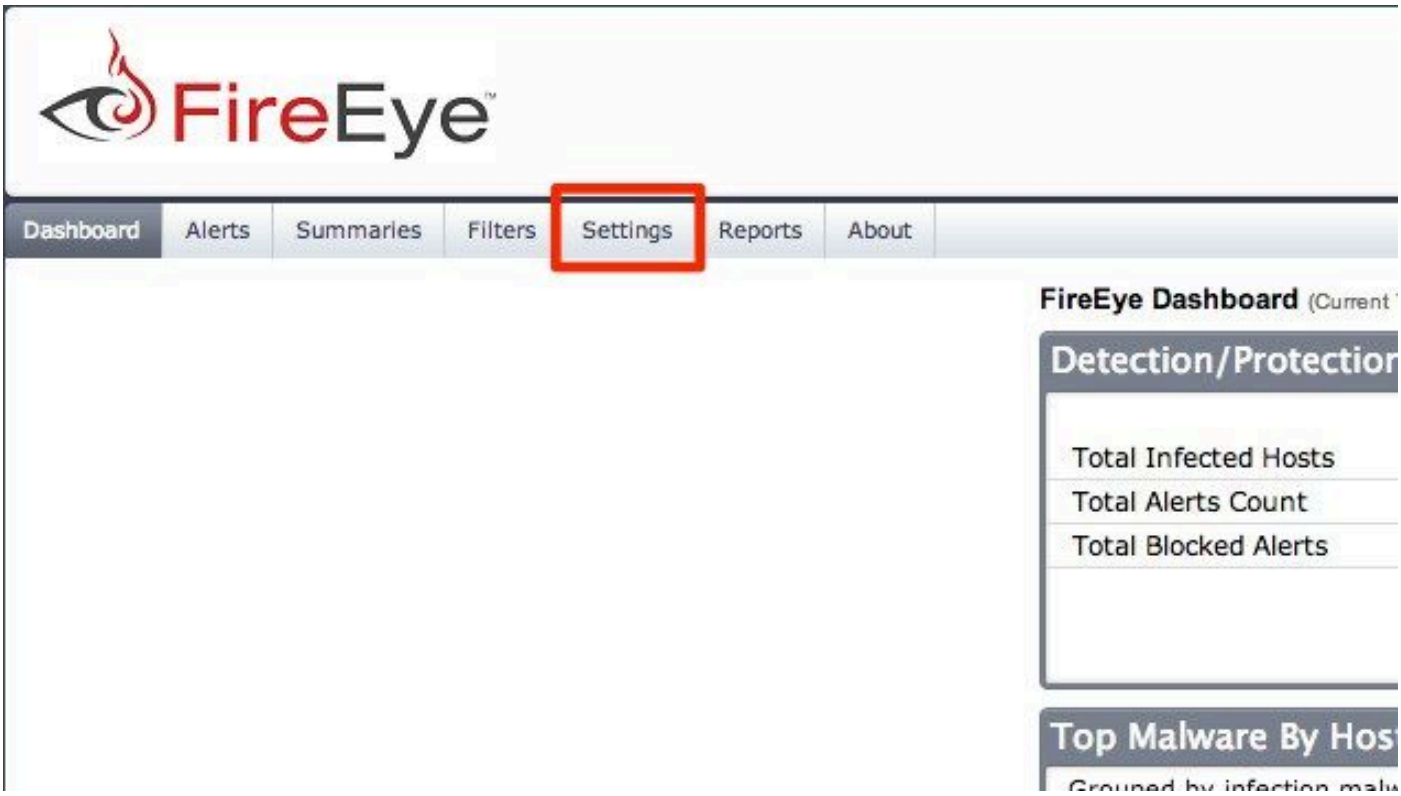


Sie können diese URL später verwenden, um die FireEye-Appliance so zu konfigurieren, dass sie Daten an Cisco Umbrella sendet. Kopieren Sie die URL daher unbedingt.

Konfigurieren von FireEye für die Kommunikation mit Cisco Umbrella

Um Datenverkehr von Ihrer FireEye-Appliance an Cisco Umbrella zu senden, müssen Sie FireEye mit den URL-Informationen konfigurieren, die im vorherigen Abschnitt generiert wurden.

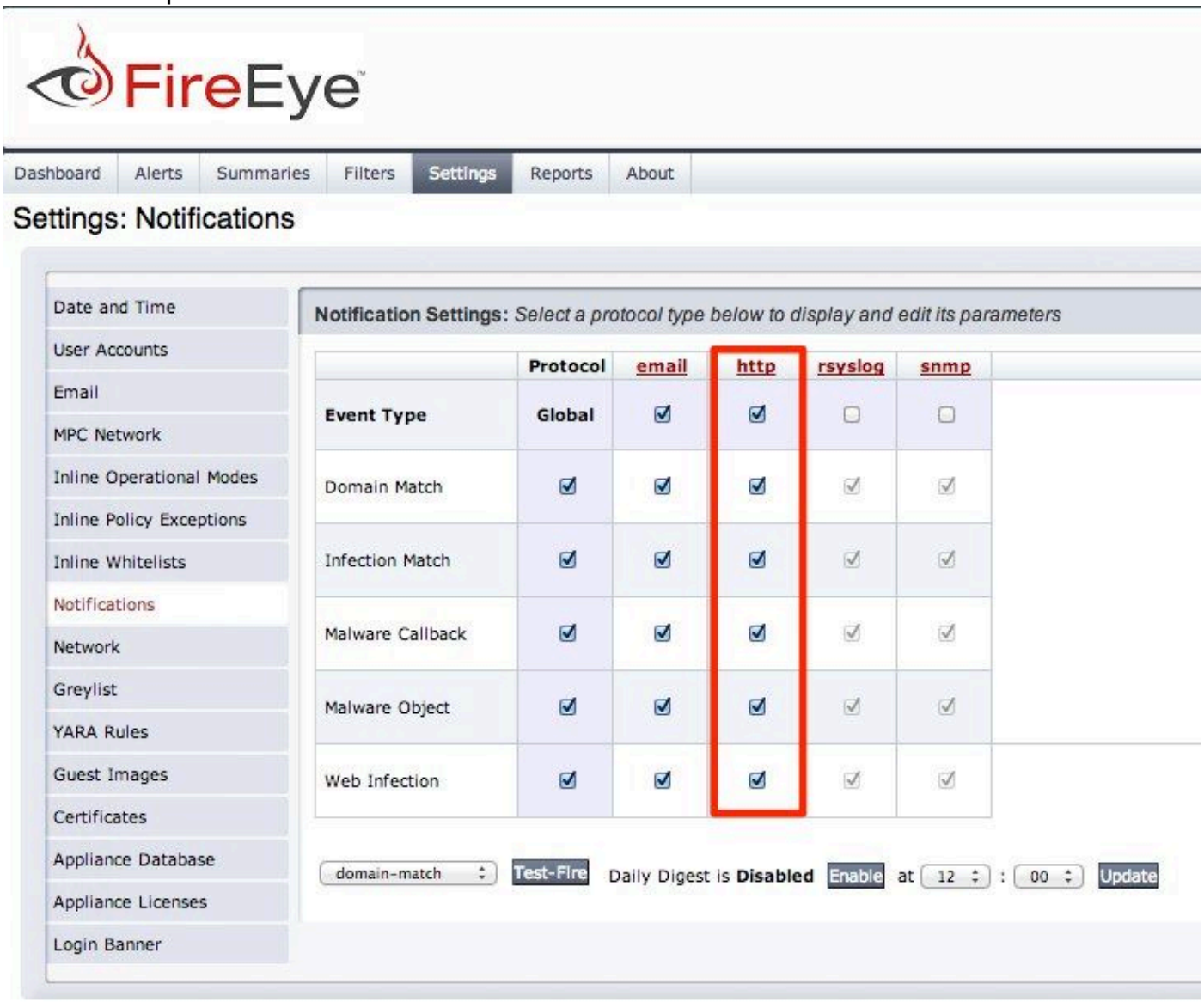
1. Melden Sie sich bei FireEye an, und wählen Sie Einstellungen aus.



2. Wählen Sie Benachrichtigungen aus der Einstellungsliste:

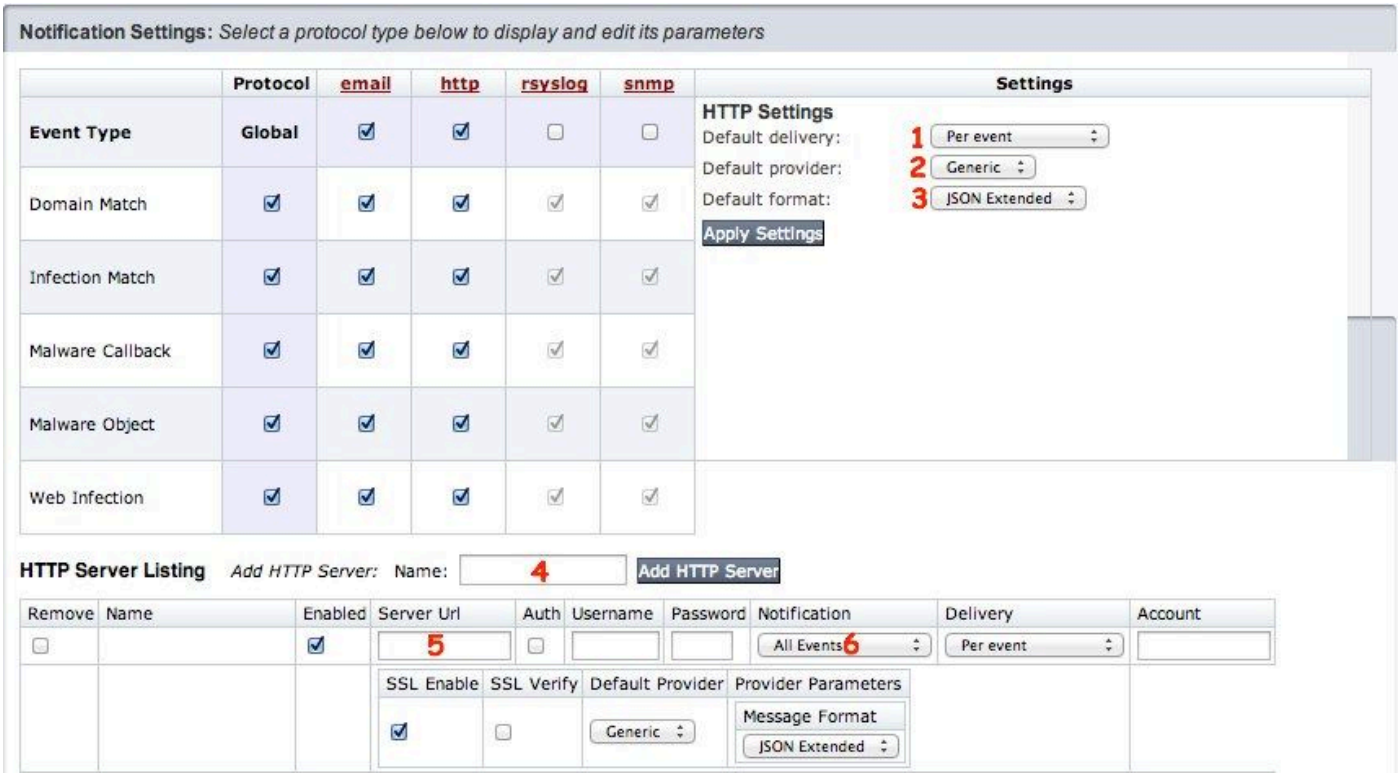

FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance 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. Stellen Sie sicher, dass alle Ereignistypen, die an Cisco Umbrella gesendet werden sollen, ausgewählt sind (Umbrella empfiehlt, mit allen zu beginnen), und wählen Sie dann den HTTP-Link oben in der Spalte aus.



4. Wenn sich das Menü erweitert, wählen Sie diese Optionen aus, um die Ereignisbenachrichtigung zu aktivieren. Die nummerierten Schritte sind im Screenshot umrissen:

1. Standardlieferung: Pro Veranstaltung
2. Standardanbieter: Allgemein
3. Standardformat: Erweiterter JSON
4. Nennen Sie den HTTP-Server "OpenDNS".
5. Server-URL: Fügen Sie hier die Cisco Umbrella URL ein, die Sie von Ihrem Cisco Umbrella Dashboard generiert haben.
6. Dropdown-Menü "Notification" (Benachrichtigung): Wählen Sie Alle Veranstaltungen aus, um eine maximale Abdeckung zu gewährleisten.



5. Stellen Sie sicher, dass die Dropdown-Menüs Delivery, Default Provider und Provider Parameters mit den Standardeinstellungen übereinstimmen, oder wenn mehrere Benachrichtigungsserver verwendet werden:

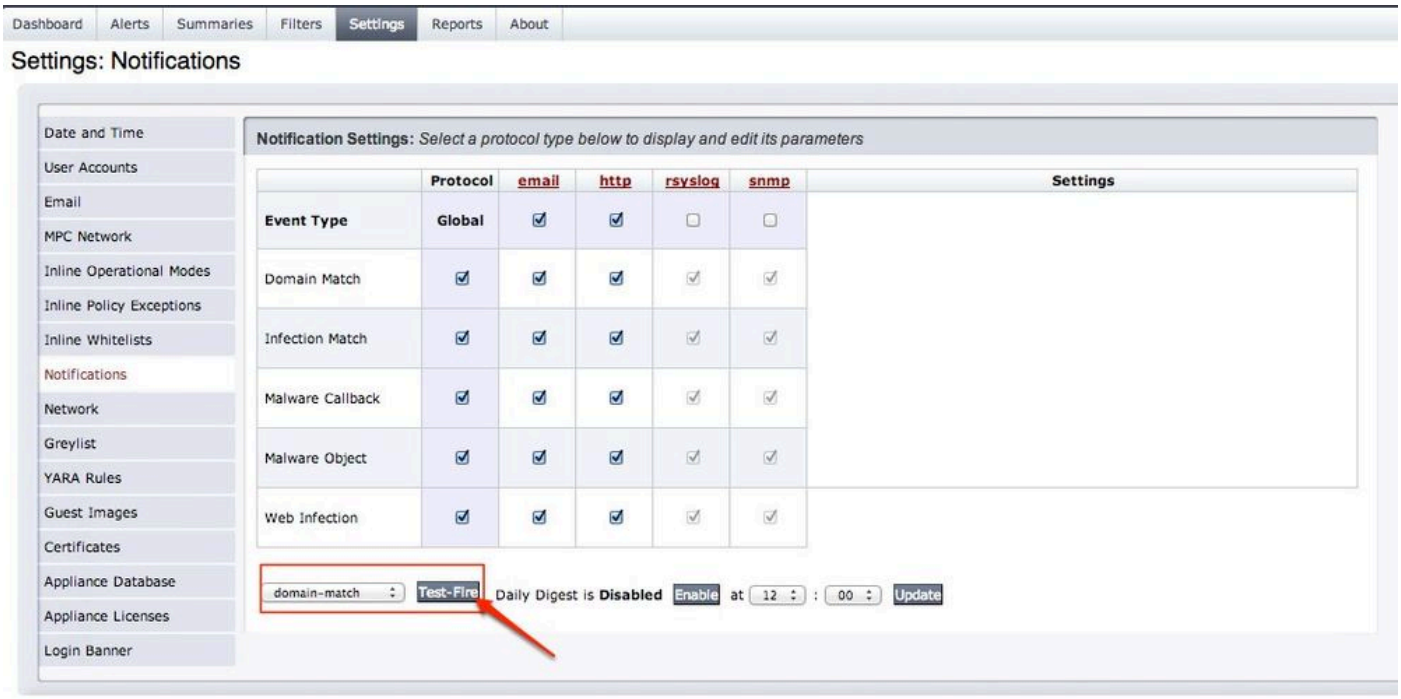
- Bereitstellung: Basis für jede Veranstaltung
- Standardanbieter: Allgemein
- Anbieterparameter: Nachrichtenformat JSON Extended
- (Optional) Wenn Sie Datenverkehr über SSL senden möchten, wählen Sie SSL Enable (SSL aktivieren).

Zu diesem Zeitpunkt ist Ihre FireEye-Appliance so konfiguriert, dass die ausgewählten Ereignistypen an Cisco Umbrella gesendet werden. Sehen wir uns diese Informationen in Ihrem Cisco Umbrella Dashboard an und legen Sie eine Richtlinie zur Blockierung dieses Datenverkehrs fest.

Sicherstellen der Anbindung: "Test Fire" zwischen FireEye und Cisco Umbrella

An dieser Stelle ist es sinnvoll, die Verbindung zu testen und sicherzustellen, dass alles ordnungsgemäß eingerichtet ist:

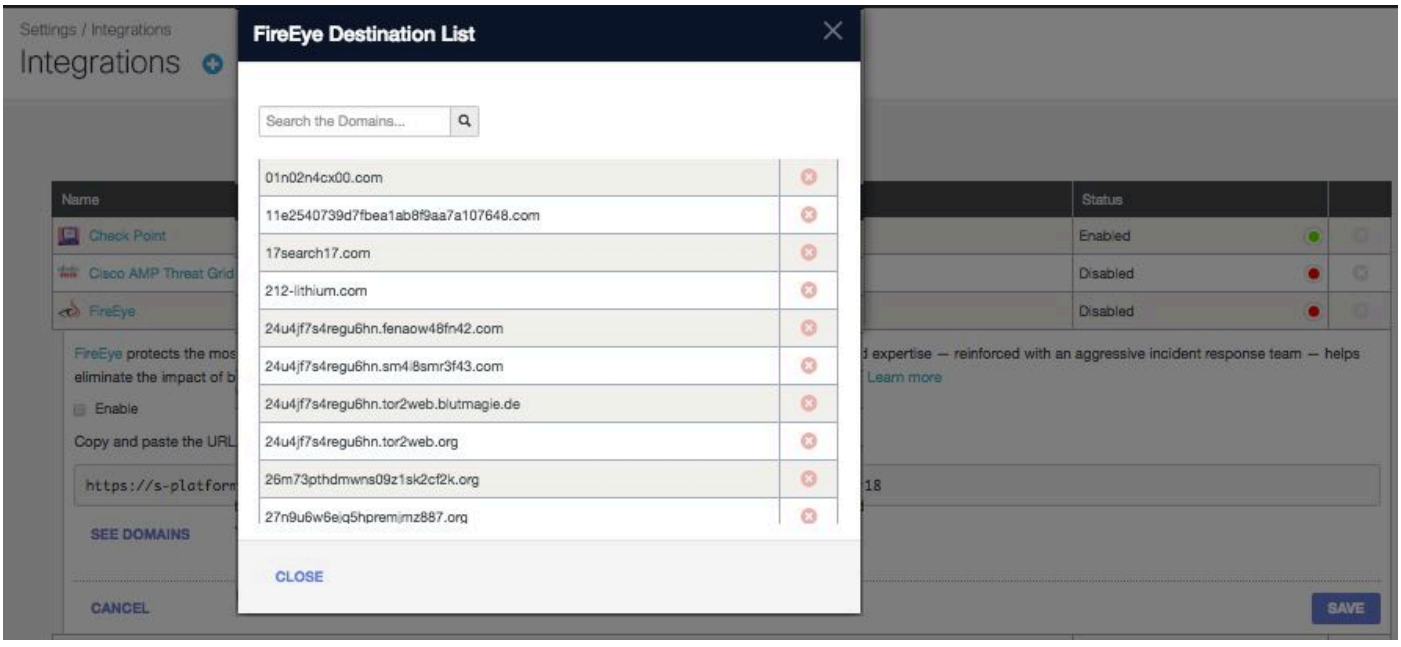
1. Wählen Sie in FireEye im Dropdown-Menü Test Fire die Option domain-match aus, und wählen Sie Test Fire:



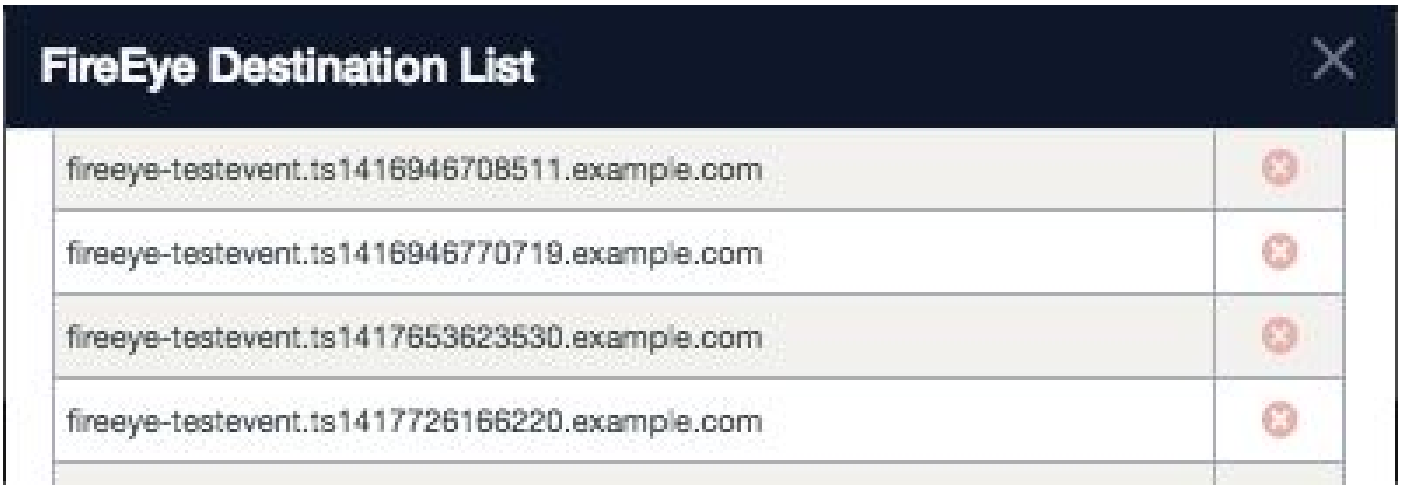
Bei Cisco Umbrella enthält die FireEye-Integration eine Liste der Domänen, die von der FireEye-Appliance bereitgestellt werden, um festzustellen, welche Domänen aktiv hinzugefügt werden.

2. Nachdem Sie Test Fire ausgewählt haben, navigieren Sie in Cisco Umbrella zu Einstellungen > Integrationen und wählen Sie FireEye in der Tabelle aus, um es zu erweitern.

3. Wählen Sie Siehe Domänen.



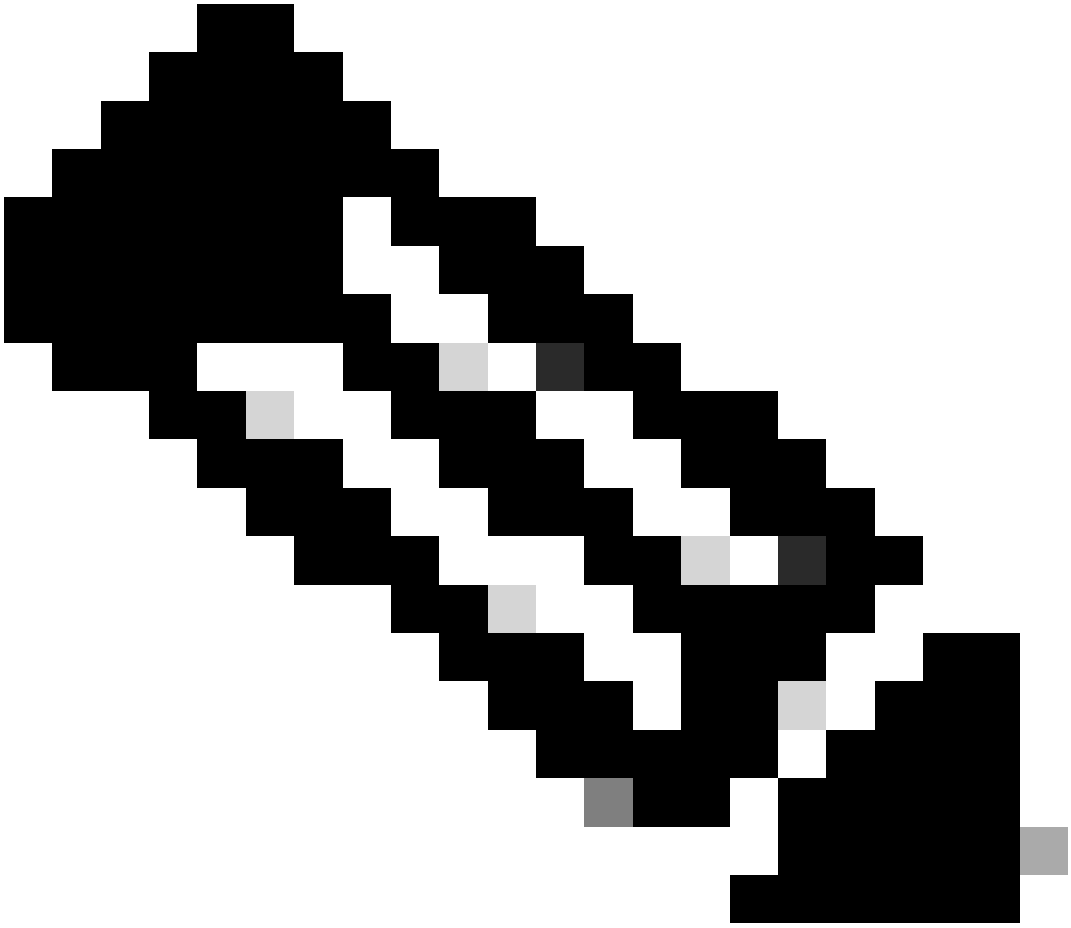
Bei Auswahl von Test Fire wird eine Domäne in der Liste der FireEye-Ziele mit dem Namen "fireeye-testevent.example.com-[date]" generiert. Jedes Mal, wenn Sie Test Fire in FireEye auswählen, wird eine eindeutige Domäne erstellt, deren Datum in der UNIX-Epoche an den Test angefügt ist. So können zukünftige Tests einen eindeutigen Testdomänennamen haben.



Wenn der Test Fire erfolgreich ist, werden weitere Ereignisse von FireEye an Cisco Umbrella gesendet, und eine durchsuchbare Liste beginnt zu füllen und zu wachsen.

Beobachten von Ereignissen, die der FireEye-Sicherheitseinstellung im "Überwachungsmodus" hinzugefügt wurden

Die Ereignisse in Ihrer FireEye-Appliance beginnen, eine bestimmte Zielliste auszufüllen, die als FireEye-Sicherheitskategorie auf Richtlinien angewendet werden kann. Standardmäßig befinden sich die Zielliste und die Sicherheitskategorie im "Überwachungsmodus". Sie werden nicht auf Richtlinien angewendet und können keine Änderungen an Ihren vorhandenen Cisco Umbrella-Richtlinien zur Folge haben.



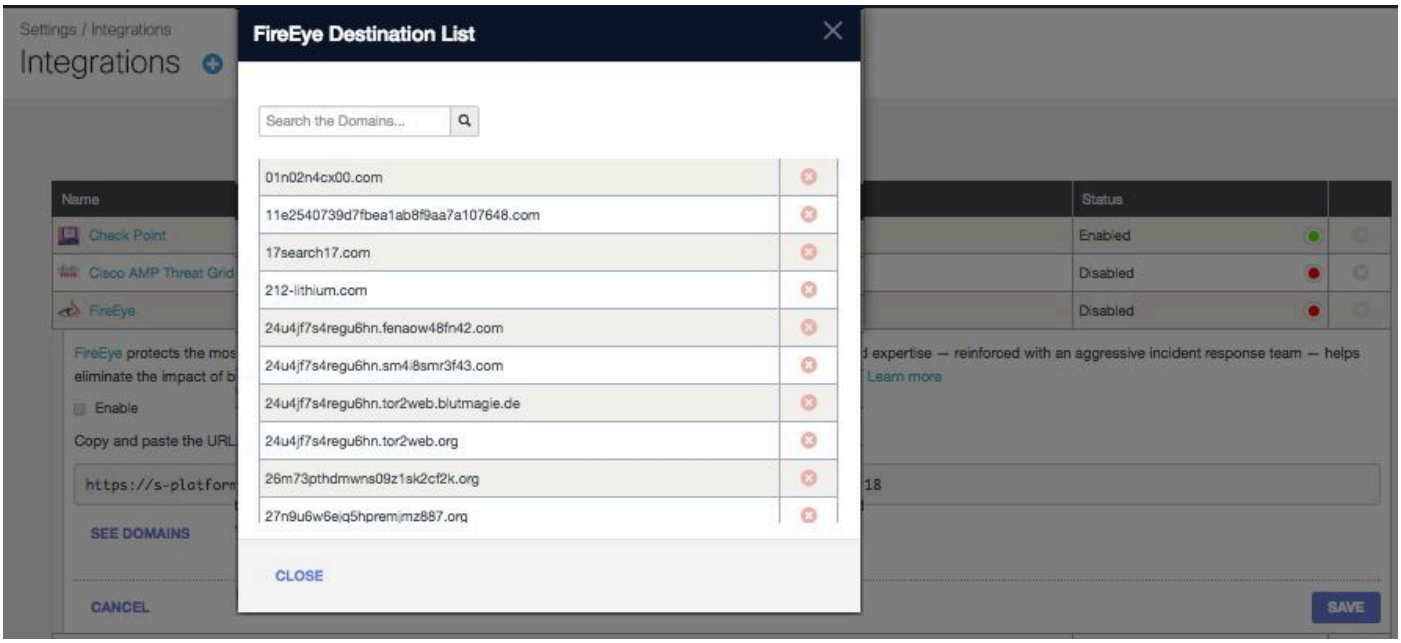
Anmerkung: Je nach Bereitstellungsprofil und Netzwerkkonfiguration kann der "Überwachungsmodus" aktiviert werden, allerdings so lange, wie dies erforderlich ist.

Zielliste überprüfen

Sie können die FireEye-Zielliste jederzeit einsehen:

1. Navigieren Sie zu Richtlinien > Richtlinienkomponenten > Integrationen.

2. Erweitern Sie FireEye in der Tabelle, und wählen Sie Domains anzeigen aus.

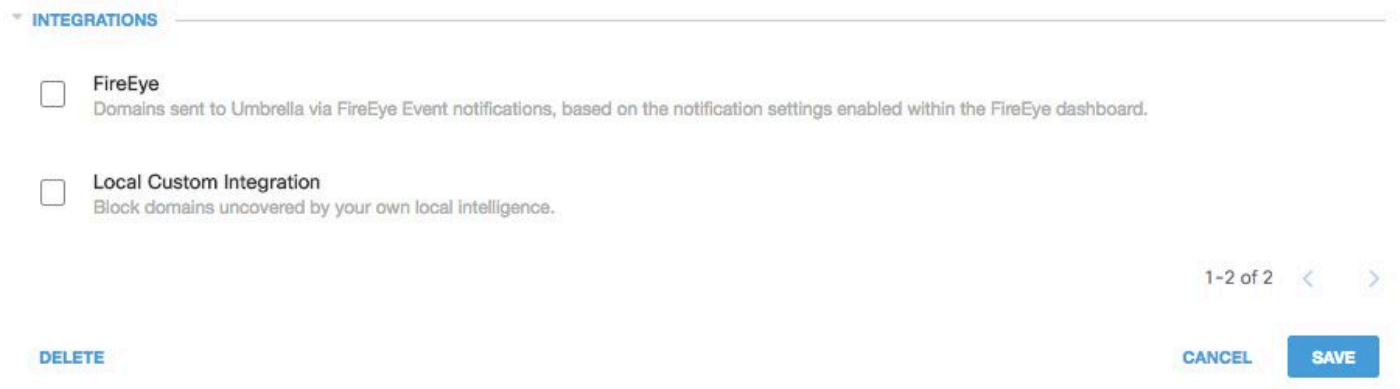


Sicherheitseinstellungen für eine Richtlinie überprüfen

Sie können die Sicherheitseinstellungen, die einer Richtlinie hinzugefügt werden können, jederzeit überprüfen:

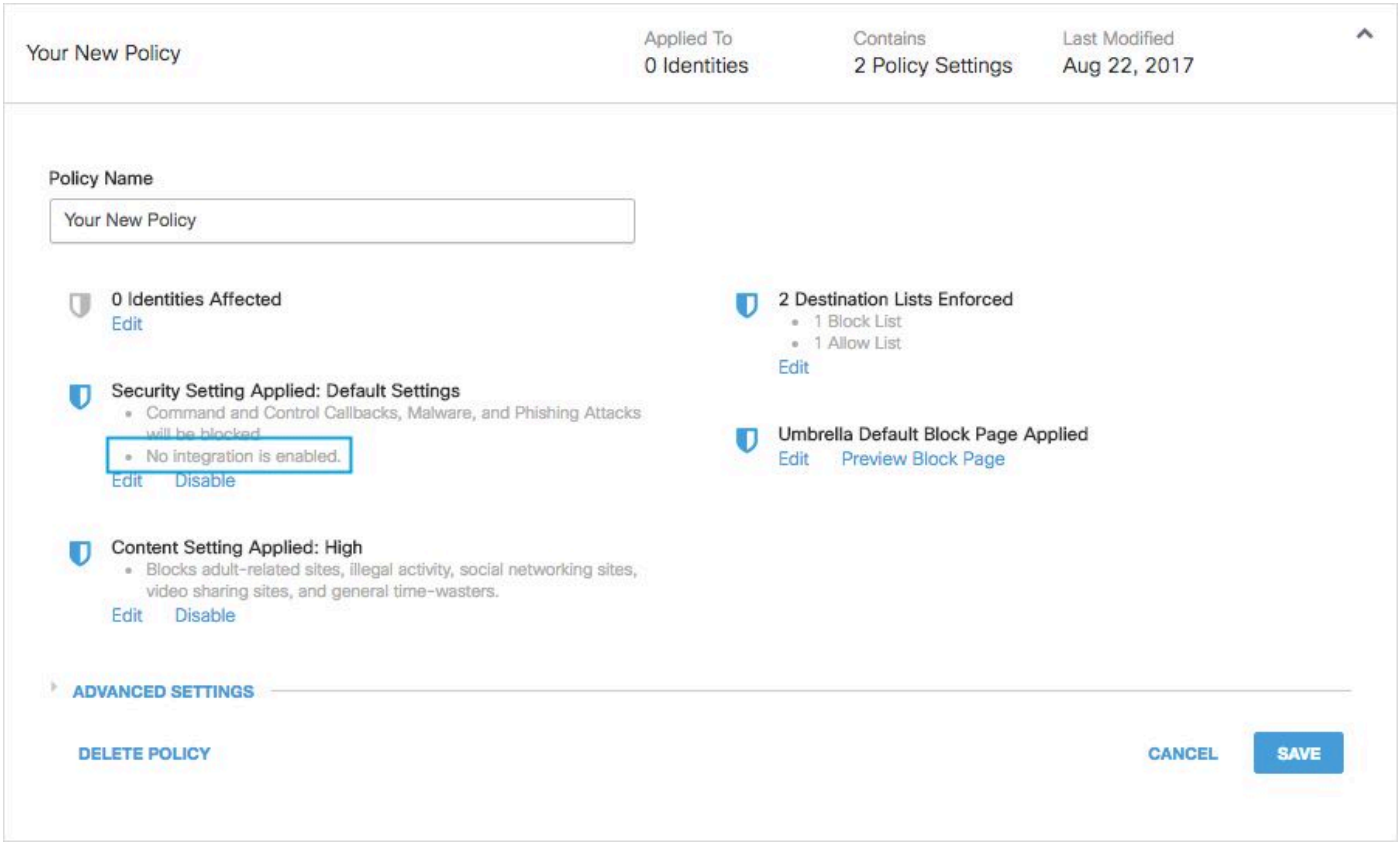
1. Navigieren Sie zu Richtlinien > Richtlinienkomponenten > Sicherheitseinstellungen.

2. Wählen Sie eine Sicherheitseinstellung in der Tabelle aus, um sie zu erweitern, und blättern Sie zu Integrations, um die FireEye-Einstellung zu finden.



115014080803

Sie können die Integrationsinformationen auch auf der Seite Zusammenfassung der Sicherheitseinstellungen überprüfen.



115013920526

Zu Beginn sollten Sie diese Sicherheitseinstellung deaktivieren, um sicherzustellen, dass die Domänen im Überwachungsmodus korrekt ausgefüllt werden.

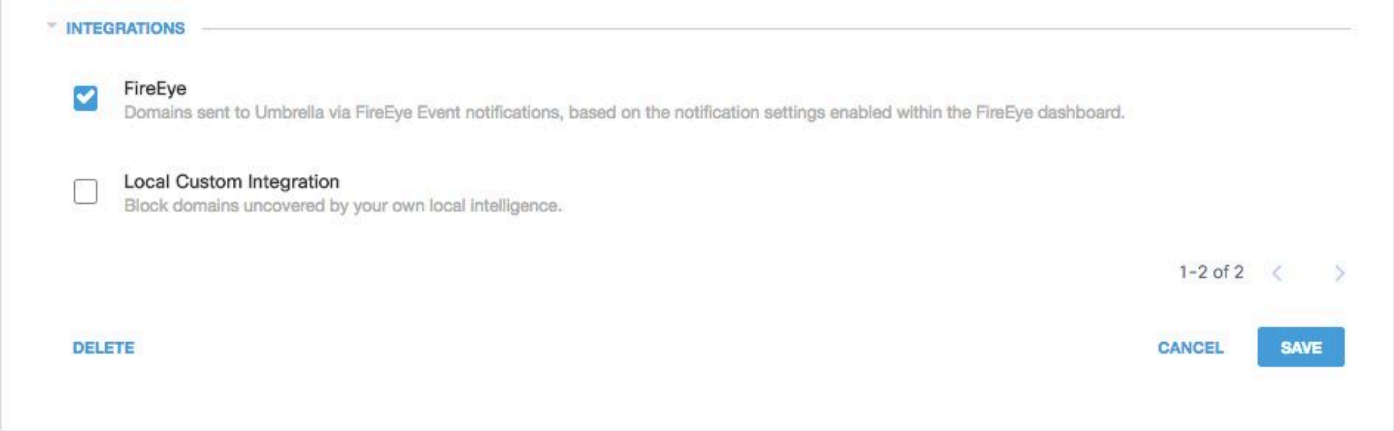
Anwenden der FireEye-Sicherheitseinstellungen im "Blockmodus" auf eine Richtlinie für verwaltete Clients

Wenn Sie diese zusätzlichen Sicherheitsbedrohungen durch Clients erzwingen möchten, die von Cisco Umbrella verwaltet werden, ändern Sie die Sicherheitseinstellung in einer vorhandenen Richtlinie, oder erstellen Sie eine neue Richtlinie, die über Ihrer Standardrichtlinie liegt, um sicherzustellen, dass sie zuerst erzwungen wird.

Erstellen oder aktualisieren Sie zunächst eine Sicherheitseinstellung:

1. Navigieren Sie zu Richtlinien > Richtlinienkomponenten > Sicherheitseinstellungen.

2. Wählen Sie unter Integrationen FireEye aus, und wählen Sie Speichern aus.



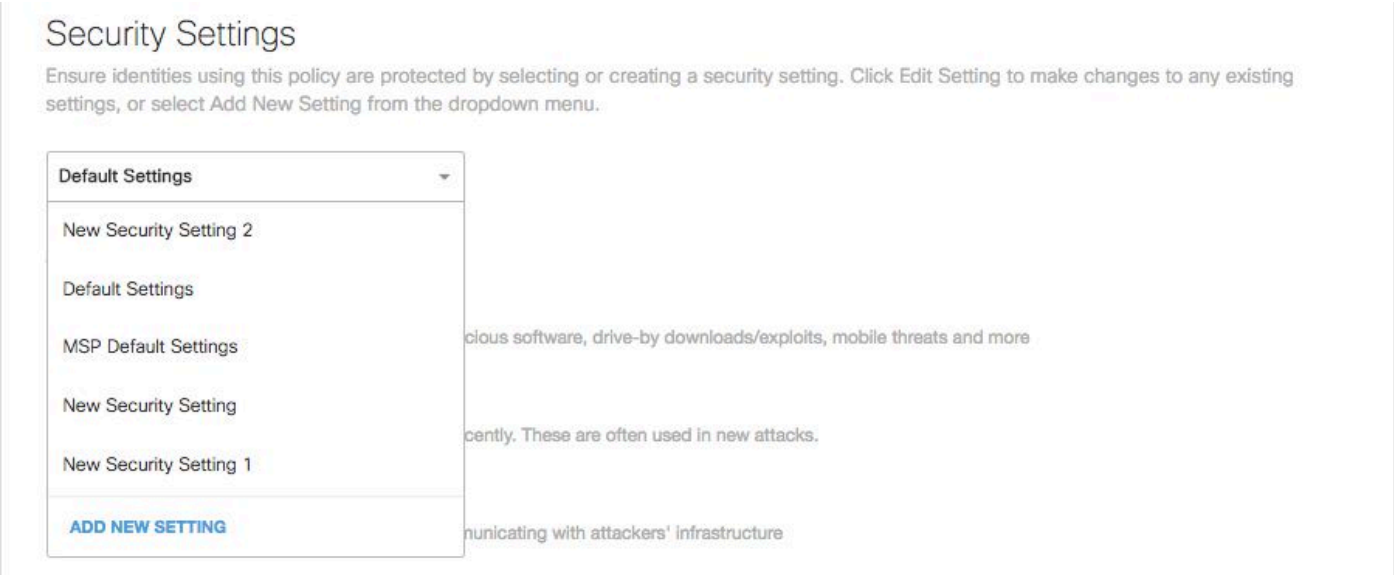
115013921406

Fügen Sie anschließend im Richtlinien-Assistenten der Richtlinie, die Sie bearbeiten, die folgende Sicherheitseinstellung hinzu:

1. Navigieren Sie zu Richtlinien > Richtlinienliste.

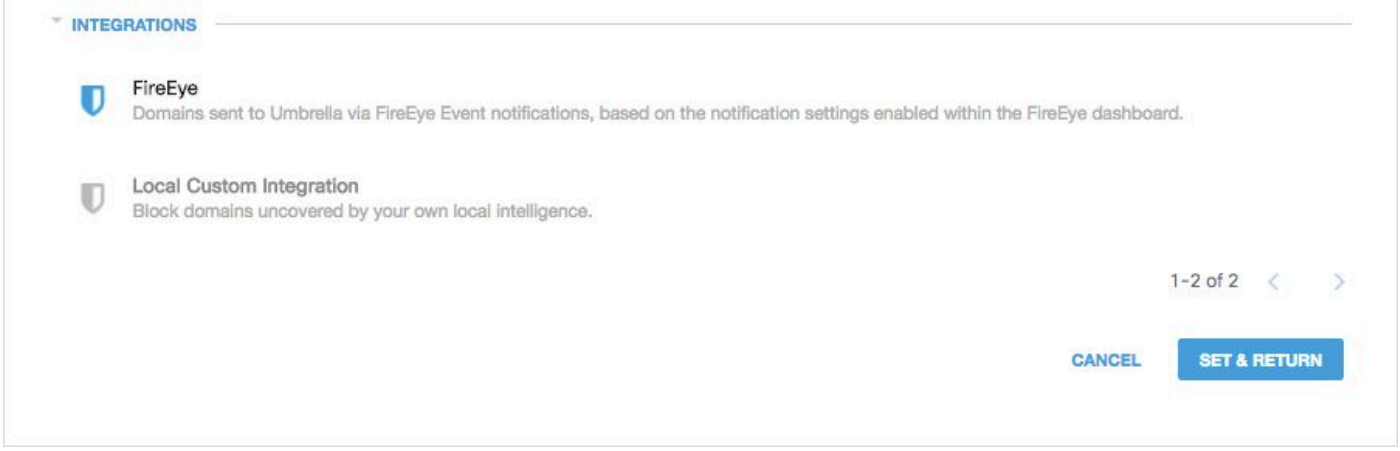
2. Erweitern Sie eine Richtlinie, und wählen Sie unter Sicherheitseinstellung angewendet die Option Bearbeiten aus.

3. Wählen Sie in der Dropdown-Liste Sicherheitseinstellungen eine Sicherheitseinstellung aus, die auch die FireEye-Einstellung enthält.



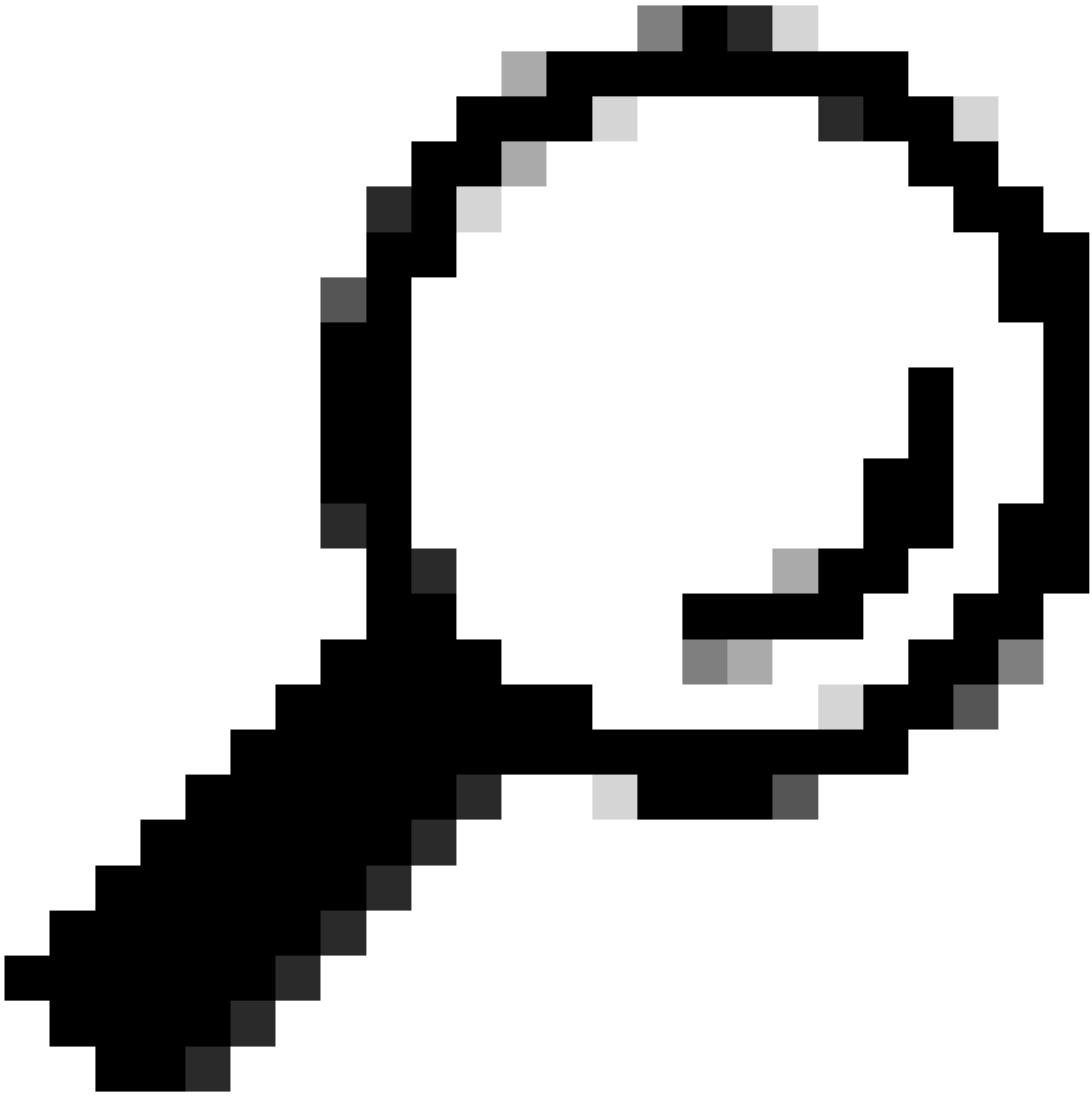
115014083083

Das Schildsymbol unter Integrationen wird auf blau aktualisiert.



115013922146

4. Wählen Sie Festlegen &Zurücksenden.



Tipp: Sie können Ihre Sicherheitseinstellungen auch über den Richtlinien-Assistenten bearbeiten.

FireEye-Domänen, die in den Sicherheitseinstellungen für FireEye enthalten sind, werden mithilfe der Richtlinie für Identitäten gesperrt.

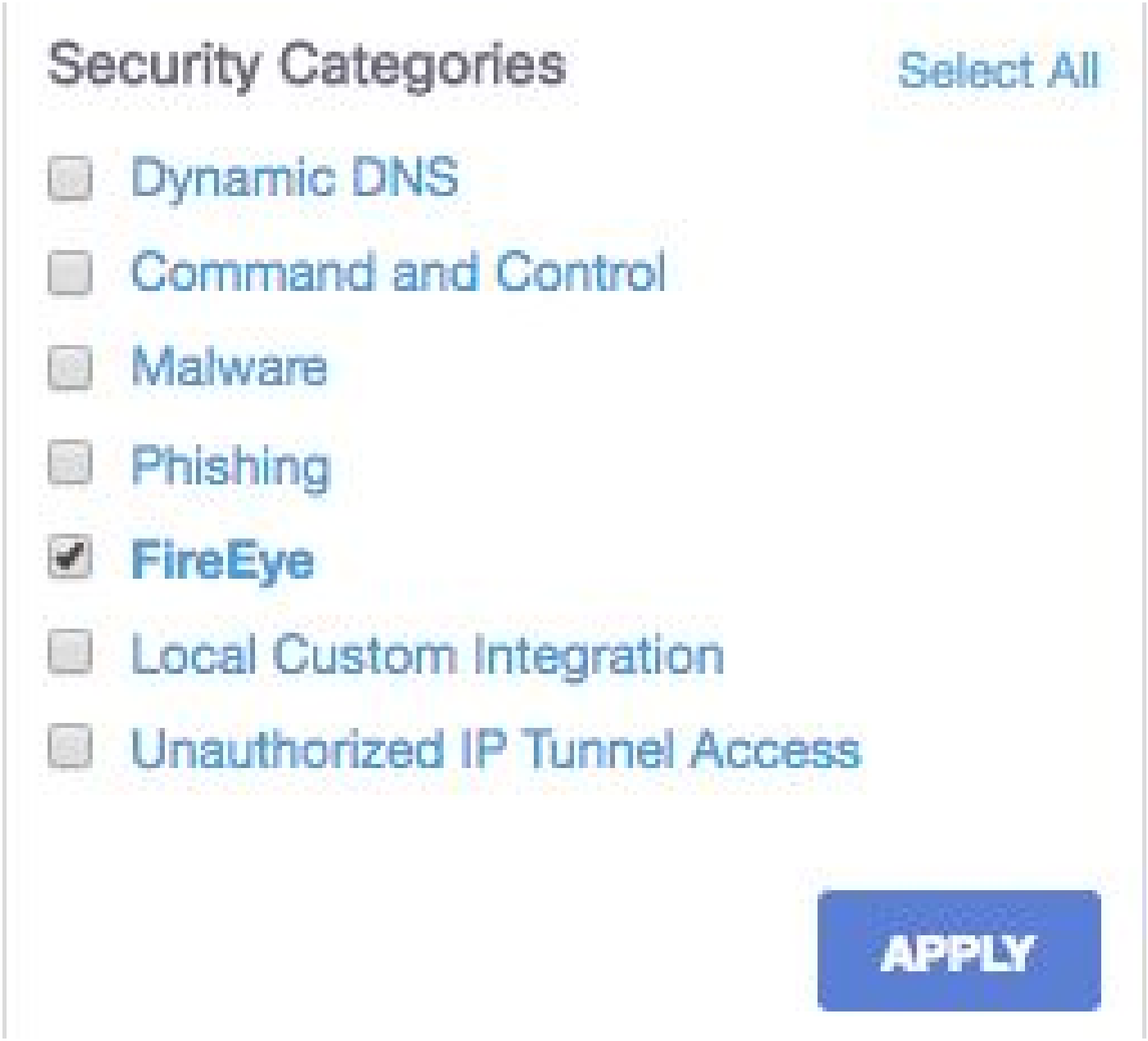
Reporting innerhalb von Cisco Umbrella für FireEye-Ereignisse

Berichte zu FireEye Security-Ereignissen

Die FireEye-Zielliste ist eine der für Berichte verfügbaren Sicherheitskategorien. Die meisten oder alle Berichte verwenden die Sicherheitskategorien als Filter. So können Sie beispielsweise Sicherheitskategorien filtern, sodass nur FireEye-bezogene Aktivitäten angezeigt werden:

1. Navigieren Sie zu Auswertung > Aktivitätssuche.

2. Wählen Sie unter Sicherheitskategorien FireEye aus, um den Bericht so zu filtern, dass nur die Sicherheitskategorie für FireEye angezeigt wird.



115013924986

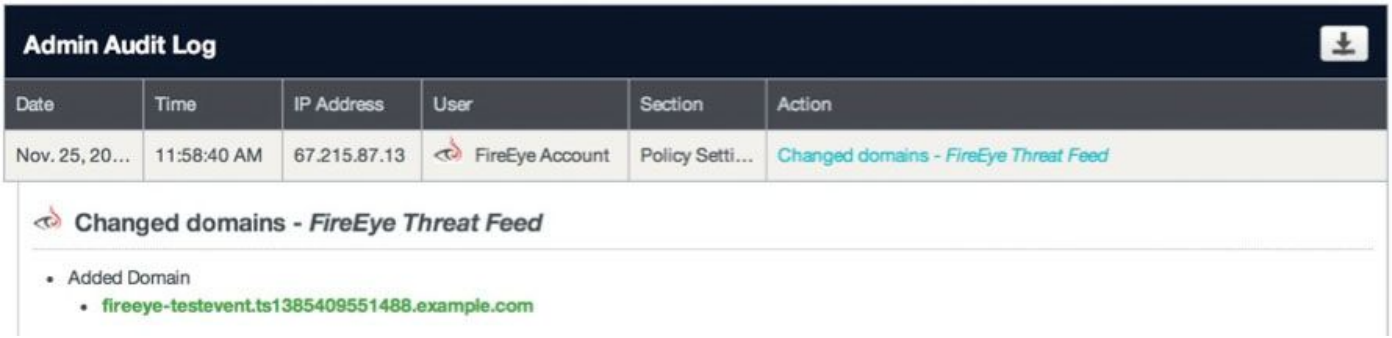
3. Wählen Sie Anwenden, um die FireEye-bezogenen Aktivitäten für den im Bericht ausgewählten Zeitraum anzuzeigen.

Berichte über das Hinzufügen von Domänen zur FireEye-Zielliste

Das Admin-Audit-Protokoll enthält Ereignisse von der FireEye-Appliance, da Domänen zur Zielliste hinzugefügt werden. Ein Benutzer mit dem Namen "FireEye Account", der ebenfalls mit dem FireEye-Logo versehen ist, generiert die Veranstaltungen. Zu diesen Ereignissen gehören die hinzugefügte Domäne und der Zeitpunkt, zu dem sie hinzugefügt wurde.

Sie können filtern, um nur FireEye-Änderungen einzubeziehen, indem Sie einen Filter für den Benutzer "FireEye-Konto" anwenden.

Wenn der "Test Fire"-Schritt früher ausgeführt wurde, kann die FireEye-Testdomäne im Audit Log angezeigt werden.



Umgang mit unerwünschten Erkennungen oder Fehlalarmen

Zulassungslisten

Obwohl unwahrscheinlich, ist es möglich, dass automatisch von Ihrer FireEye-Appliance hinzugefügte Domains eine unerwünschte Erkennung auslösen, die Ihre Benutzer daran hindert, auf bestimmte Websites zuzugreifen. In einer solchen Situation empfiehlt Umbrella, die Domäne(n) einer Zulassungsliste hinzuzufügen (Richtlinien > Ziellisten), die Vorrang vor allen anderen Typen von Sperrlisten hat, einschließlich Sicherheitseinstellungen.

Es gibt zwei Gründe, warum dieser Ansatz vorzuziehen ist.

- Wenn die FireEye-Appliance die Domäne nach dem Entfernen erneut hinzufügen sollte, schützt die Zulassungsliste vor weiteren Problemen.
- Zweitens zeigt die Zulassungsliste einen Verlaufsdatensatz problematischer Domänen an, die für forensische Untersuchungen oder Prüfberichte verwendet werden können.

Standardmäßig gibt es eine globale Zulassungsliste, die auf alle Richtlinien angewendet wird. Durch Hinzufügen einer Domäne zur globalen Zulassungsliste wird die Domäne in allen Richtlinien zugelassen.

Wenn die FireEye-Sicherheitseinstellung im Blockmodus nur auf eine Teilmenge Ihrer verwalteten Cisco Umbrella-Identitäten angewendet wird (z. B. nur auf Roaming-Computer und mobile Geräte), können Sie eine spezifische Zulassungsliste für diese Identitäten oder Richtlinien erstellen.

So erstellen Sie eine Zulassungsliste:

1. Navigieren Sie zu Policys > Ziellisten, und wählen Sie das Symbol Hinzufügen aus.

2. Wählen Sie Zulassen, und fügen Sie Ihre Domäne zur Liste hinzu.

3. Wählen Sie Speichern.

Nachdem die Zielliste gespeichert wurde, können Sie sie einer vorhandenen Richtlinie hinzufügen, die die Clients abdeckt, die von dem unerwünschten Block betroffen sind.

Löschen von Domänen aus der FireEye-Zielliste

Neben jedem Domänennamen in der FireEye-Zielliste befindet sich ein Symbol zum Löschen. Durch das Löschen von Domänen können Sie die FireEye-Zielliste bereinigen, wenn eine unerwünschte Erkennung auftritt.

Der Löschvorgang ist jedoch nicht dauerhaft, wenn die FireEye-Appliance die Domäne erneut an Cisco Umbrella sendet.

So löschen Sie eine Domäne:

1. Navigieren Sie zu Einstellungen > Integrationen, und wählen Sie dann "FireEye", um es zu erweitern.

2. Wählen Sie Siehe Domänen.

3. Suchen Sie nach dem Domänennamen, den Sie löschen möchten.

4. Wählen Sie das Symbol Löschen.

5. Wählen Sie Schließen.

6. Wählen Sie Speichern.

Im Fall einer unerwünschten Erkennung oder eines Fehlalarms empfiehlt Umbrella, sofort eine Zulassungsliste in Cisco Umbrella zu erstellen und anschließend das Fehlalarmen in der FireEye-Appliance zu beheben. Später können Sie die Domäne aus der FireEye-Zielliste entfernen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.