

Integrate Umbrella with FireEye

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Overview](#)

[Integration Functionality](#)

[Configuring Your Cisco Umbrella Dashboard to Receive Information from FireEye](#)

[Configuring FireEye to Communicate with Cisco Umbrella](#)

[Ensuring Connectivity: "Test Fire" Between FireEye and Cisco Umbrella](#)

[Observing Events Added to the FireEye Security Setting in "Audit Mode"](#)

[Review Destination List](#)

[Review Security Settings for a Policy](#)

[Applying the FireEye Security Settings in "Block Mode" to a Policy for Managed Clients](#)

[Reporting within Cisco Umbrella for FireEye Events](#)

[Reporting on FireEye Security Events](#)

[Reporting on when Domains Were Added to the FireEye Destination List](#)

[Handling Unwanted Detections or False Positives](#)

[Allow Lists](#)

[Deleting Domains from the FireEye Destination List](#)

Introduction

This document describes how to integrate Cisco Umbrella with FireEye.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- A FireEye appliance with access to the public Internet.
- Cisco Umbrella Dashboard administrative rights.
- The Cisco Umbrella Dashboard must have the FireEye integration enabled.

Components Used

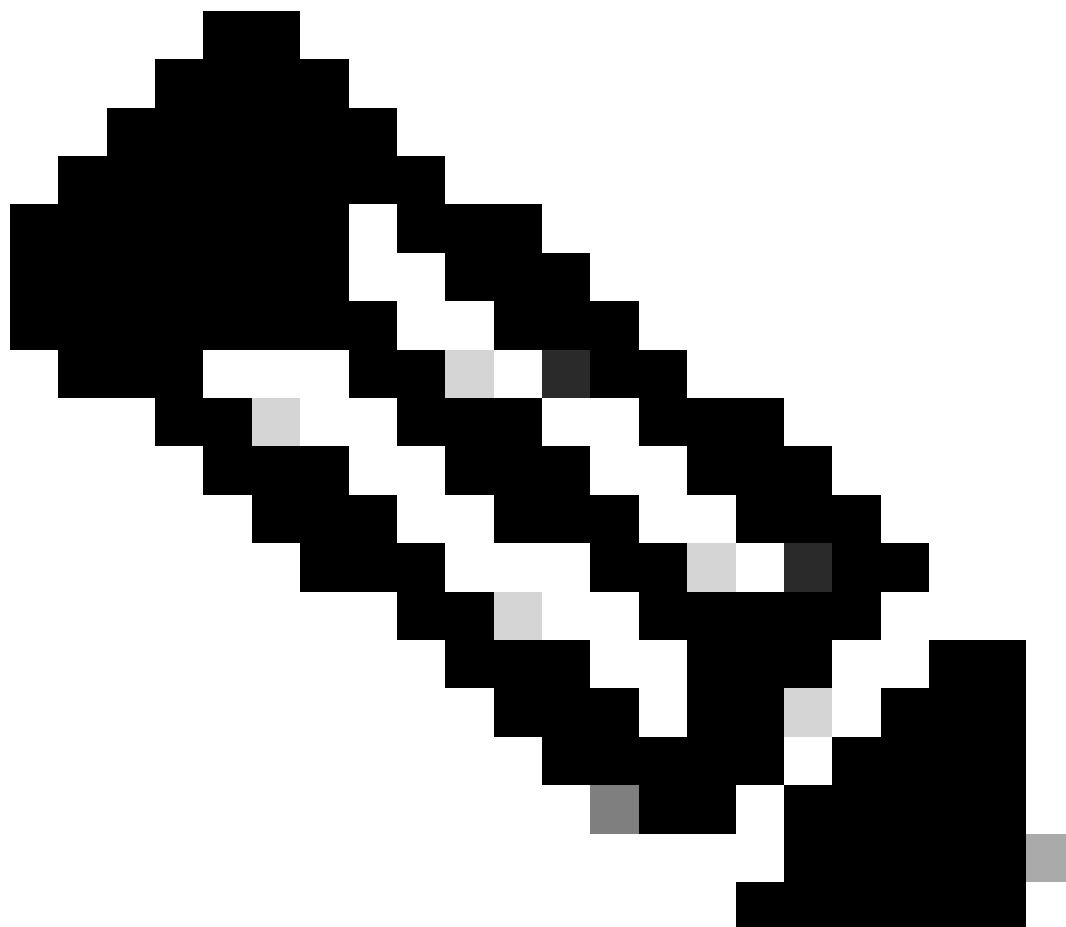
The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

With integration between the [FireEye security appliance and Cisco Umbrella](#), security officers and administrators are now able to extend protection against advanced threats to roaming laptops, tablets, or phones while also providing another layer of enforcement to a distributed corporate network.

This guide outlines how to configure your FireEye to communicate with Cisco Umbrella so security events from FireEye are integrated into policies that can be applied to clients protected by Cisco Umbrella.



Note: The FireEye integration is only included in [Cisco Umbrella packages](#) like DNS Essentials, DNS Advantage, SIG Essentials, or SIG Advantage. If you do not have one of these packages and would like to have the FireEye integration, please contact your Cisco Umbrella Account Manager. If you have the correct Cisco Umbrella package but do not see FireEye as an integration for your dashboard, please [contact Cisco Umbrella Support](#).

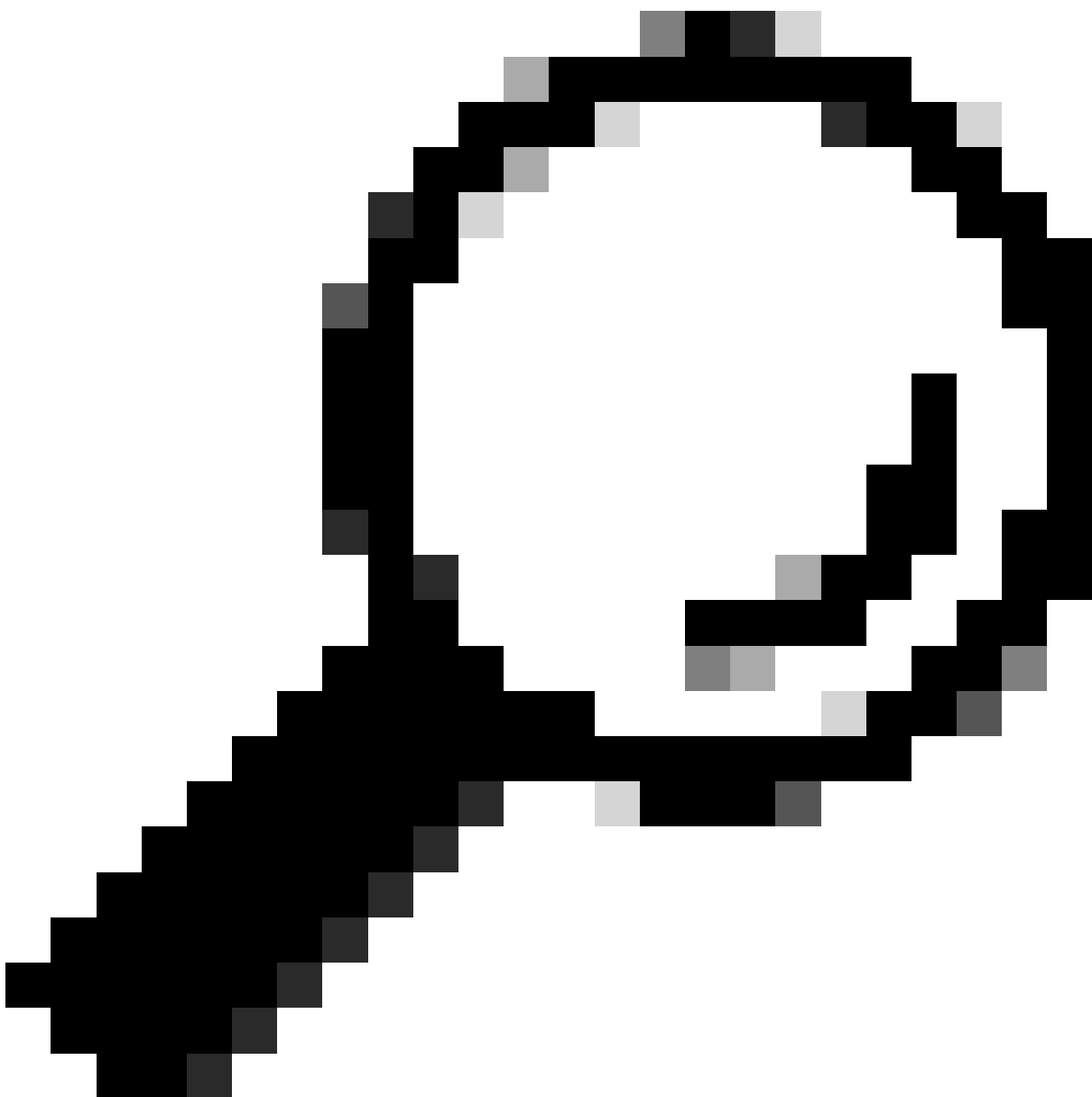
Integration Functionality

The FireEye appliance first sends Internet-based threats it has found, such as domains that host malware,

command and control for botnet, or phishing sites, to Cisco Umbrella.

Cisco Umbrella then validates the information passed to Cisco Umbrella to ensure it is valid and can be added to a policy. If the information from FireEye is confirmed to be formatted correctly (for example, it is not a file, a complex URL, or a highly popular domain) the domain address is added to the FireEye destination list as part of a security setting that can be applied to any Cisco Umbrella policy. That policy is immediately applied to any requests being made from devices using policies with the FireEye destination list.

Going forward, Cisco Umbrella automatically parses FireEye alerts and adds malicious sites to the FireEye destination list. This extends FireEye protection to all remote users and devices and providing another layer of enforcement to your corporate network.



Tip: While Cisco Umbrella tries its best to validate and allow domains which are known to be generally safe (for example, Google and Salesforce), to avoid unwanted interruptions, we suggest adding domains you never wish to have blocked to the Global Allow List or other destination lists as per your policy. Examples include:



- The home page for your organization
- Domains representing services you provide that can have both internal and external records. For example, "mail.myservicedomain.com" and "portal.myotherservicedomain.com".
- Lesser-known cloud-based applications you depend on that Cisco Umbrella does not include in automatic domain validation. For example, "localcloudservice.com".

These domains can be added to the [Global Allow List](#), which is found under **Policies > Destination Lists** in Cisco Umbrella.

Configuring Your Cisco Umbrella Dashboard to Receive Information from FireEye

The first step is to find your unique URL in Cisco Umbrella for the FireEye appliance to communicate with.

1. Log into the Cisco Umbrella Dashboard as an Administrator.
2. Navigate to **Policies > Policy Components > Integrations** and select **FireEye** in the table to expand it.
3. Select the **Enable** box and then select **Save**. This generates a unique, specific URL for your organization within Cisco Umbrella.

Name	Status
 FireEye	Enabled 

FireEye protects the most valuable assets from today's cyber attackers. Their combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 2,700 customers across 67 countries. [Learn more](#)

☒ Enable

Copy and paste the URL below into the HTTP notifications section of your FireEye Dashboard. [Instructions](#)

https://s-platform.api.opendns.com/1.0/events?customerKey=212616ea-1683-47b9-b854-4b3aa69b02a3

[SEE DOMAINS](#)

[CANCEL](#) [SAVE](#)

You can use this URL later to configure the FireEye appliance to send data to Cisco Umbrella, so be sure to copy the URL.

Configuring FireEye to Communicate with Cisco Umbrella

To begin sending traffic from your FireEye appliance to Cisco Umbrella, you must configure FireEye with the URL information generated in the previous section.

1. Log into FireEye and select **Settings**.



2. Select **Notifications** from the list of settings:



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, opt for 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	<input type="checkbox"/>	Update T
time.nist.gov	<input type="checkbox"/>	Update T

Remove Selected NTP Servers

Set Time Zone:

UTC Set Time Zone

3. Ensure all **Event Types** to be sent to Cisco Umbrella are selected (Umbrella recommends starting with all), and then select the **HTTP** link at the top of the column.

FireEye

Dashboard Alerts Summaries Filters **Settings** Reports About

Settings: Notifications

Notification Settings: Select a protocol type below to display and edit its parameters

	Protocol	email	http	rsyslog	snmp
Event Type	Global	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Domain Match	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Infection Match	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Malware Callback	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Malware Object	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Web Infection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

domain-match Test-Fire Daily Digest is **Disabled** **Enable** at 12 : 00 **Update**

4. When the menu expands, select these options to enable Event Notification. The numbered steps are outlined in the screenshot:

1. **Default delivery:** Per Event
2. **Default provider:** Generic
3. **Default format:** JSON Extended
4. Name the **HTTP Server** "OpenDNS".
5. **Server Url:** Paste the Cisco Umbrella URL you generated from your Cisco Umbrella dashboard earlier here.
6. **Notification** drop-down: Select **All Events** to ensure maximum coverage.

Notification Settings: Select a protocol type below to display and edit its parameters

	Protocol	email	http	rsyslog	snmp	Settings
Event Type	Global	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HTTP Settings Default delivery: 1 Per event Default provider: 2 Generic Default format: 3 JSON Extended <input type="button" value="Apply Settings"/>
Domain Match	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Infection Match	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Malware Callback	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Malware Object	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Web Infection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

HTTP Server Listing Add HTTP Server: Name: **4**

Remove	Name	Enabled	Server Url	Auth	Username	Password	Notification	Delivery	Account
<input type="checkbox"/>		<input checked="" type="checkbox"/>	5	<input type="checkbox"/>			All Events 6	Per event	
			SSL Enable	SSL Verify	Default Provider	Provider Parameters			
			<input checked="" type="checkbox"/>	<input type="checkbox"/>	Generic	Message Format JSON Extended			

5. Ensure the **Delivery**, **Default Provider**, and **Provider Parameters** drop-downs all match the default settings, or if multiple notification servers are being used:

- **Delivery:** Per Event basis
- **Default Provider:** Generic
- **Provider Parameters:** Message format JSON Extended
- (Optional) If you prefer to send traffic over SSL, select **SSL Enable**.

At this point, your FireEye appliance is set to send the selected Event Types to Cisco Umbrella. Next, learn how to see this information in your Cisco Umbrella Dashboard and set a policy to block against this traffic.

Ensuring Connectivity: “Test Fire” Between FireEye and Cisco Umbrella

At this point, it is a good idea to test your connectivity and ensure that everything is set up properly:

1. In FireEye, select **domain-match** from the **Test Fire** dropdown and select **Test Fire**:

Dashboard Alerts Summaries Filters **Settings** Reports About

Settings: Notifications

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

Notification Settings: Select a protocol type below to display and edit its parameters

	Protocol	email	http	rsyslog	snmp	Settings
Event Type	Global	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Domain Match	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Infection Match	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Malware Callback	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Malware Object	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Web Infection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

domain-match
Test-Fire
Daily Digest is Disabled
Enable
at 12 : 00
Update

In Cisco Umbrella, the FireEye integration includes a list of domains provided by the FireEye Appliance to see which domain(s) are being actively added.

2. After you select **Test Fire**, in Cisco Umbrella navigate to **Settings > Integrations** and select **FireEye** in the table to expand it.

3. Select **See Domains**.

Settings / Integrations
Integrations

Name
Check Point
Cisco AMP Threat Grid
FireEye

FireEye protects the most...
eliminate the impact of b...
☐ Enable
Copy and paste the URL
https://s-platform...
SEE DOMAINS
CANCEL

FireEye Destination List

Search the Domains...

01n02n4cx00.com	✖
11e2540739d7fba1ab8f9aa7a107648.com	✖
17search17.com	✖
212-lithium.com	✖
24u4jf7s4regu6hn.fenaow48fn42.com	✖
24u4jf7s4regu6hn.sm4l8smr3f43.com	✖
24u4jf7s4regu6hn.tor2web.blutmagie.de	✖
24u4jf7s4regu6hn.tor2web.org	✖
26m73pthdmwns09z1sk2cf2k.org	✖
27n9u6w6eiq5hpremjzm887.org	✖

CLOSE

Status	
Enabled	●
Disabled	●
Disabled	●

d expertise — reinforced with an aggressive incident response team — helps
[Learn more](#)

18

SAVE

Selecting **Test Fire** generates a domain in the FireEye Destinations List named “fireeye-testevent.example.com-[date]”. Each time you select **Test Fire** in FireEye, it creates a unique domain with the date in UNIX Epoch time attached to the test, so future tests can have a unique test domain name.

FireEye Destination List		
fireeye-testevent.ts1416946708511.example.com		
fireeye-testevent.ts1416946770719.example.com		
fireeye-testevent.ts1417653623530.example.com		
fireeye-testevent.ts1417726166220.example.com		

If the Test Fire is successful, more events from FireEye is sent to Cisco Umbrella, and a searchable list begins to be populated and grow.

Observing Events Added to the FireEye Security Setting in "Audit Mode"

The events from your FireEye appliance begin to populate a specific destination list that can be applied to policies as a FireEye security category. By default, the destination list and the security category are in "audit mode" and are not applied to any policies and cannot result in any change to your existing Cisco Umbrella policies.

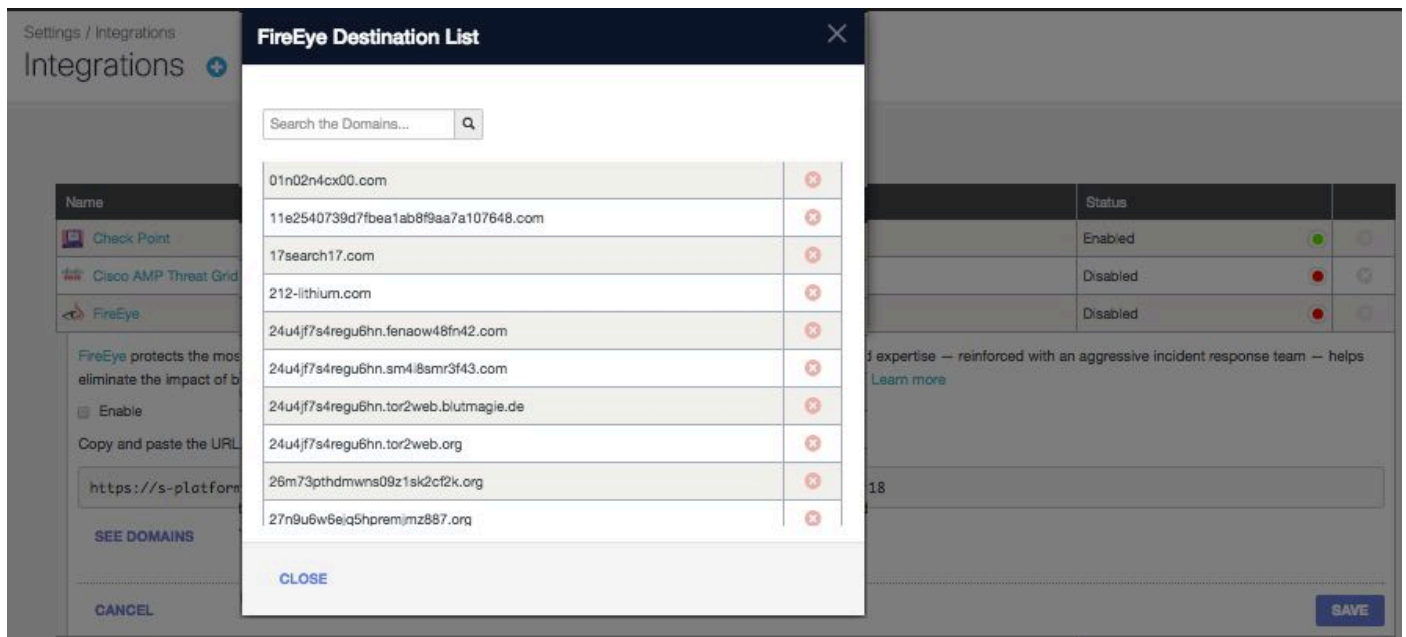


Note: "Audit mode" can be enabled for however long is necessary based on your deployment profile and network configuration.

Review Destination List

You can review the FireEye destination list at any time:

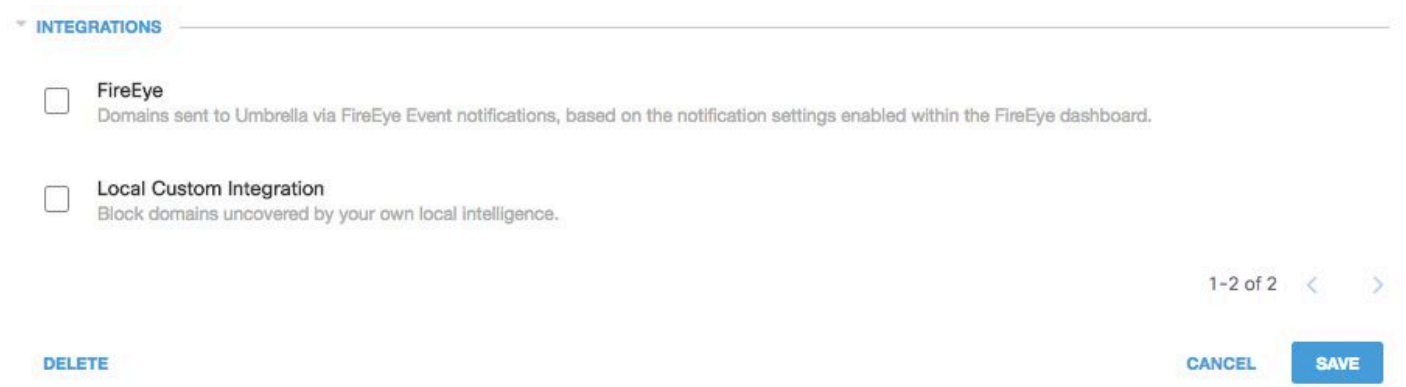
1. Navigate to **Policies > Policy Components > Integrations**.
2. Expand **FireEye** in the table and select **See Domains**.



Review Security Settings for a Policy

You can review the security settings that can be added to a policy at any time:

1. Navigate to **Policies > Policy Components > Security Settings**.
2. Select a security setting in the table to expand it and scroll to **Integrations** to locate the FireEye setting.



115014080803

You can also review integration information through the Security Settings Summary page.

Your New Policy
Applied To
0 Identities
Contains
2 Policy Settings
Last Modified
Aug 22, 2017

Policy Name
Your New Policy

0 Identities Affected
[Edit](#)

2 Destination Lists Enforced

- 1 Block List
- 1 Allow List

[Edit](#)

Security Setting Applied: Default Settings

- Command and Control Callbacks, Malware, and Phishing Attacks will be blocked
- No integration is enabled.

[Edit](#) [Disable](#)

Umbrella Default Block Page Applied
[Edit](#) [Preview Block Page](#)

Content Setting Applied: High

- Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

[Edit](#) [Disable](#)

ADVANCED SETTINGS

[DELETE POLICY](#)
[CANCEL](#)
[SAVE](#)

115013920526

When getting started, it is best to leave this security setting cleared in order to ensure domains are correctly populating in an "audit mode."

Applying the FireEye Security Settings in "Block Mode" to a Policy for Managed Clients

Once you are ready to have these additional security threats enforced by clients managed by Cisco Umbrella, change the security setting on an existing policy, or create a new policy that sits above your default policy to ensure it is enforced first.

First, create or update a security settings:

1. Navigate to **Policies > Policy Components > Security Settings**.
2. Under **Integrations**, select **FireEye** and select **Save**.

INTEGRATIONS

☒ **FireEye**
Domains sent to Umbrella via FireEye Event notifications, based on the notification settings enabled within the FireEye dashboard.

☐ **Local Custom Integration**
Block domains uncovered by your own local intelligence.

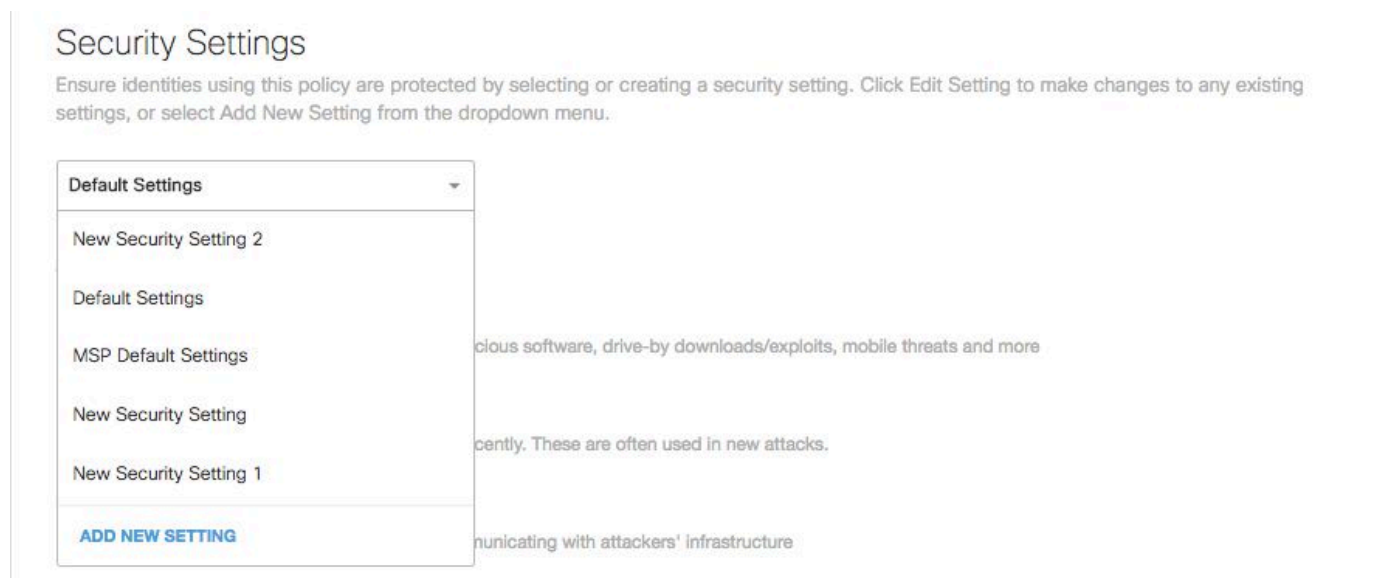
1-2 of 2

[DELETE](#)
[CANCEL](#)
[SAVE](#)

115013921406

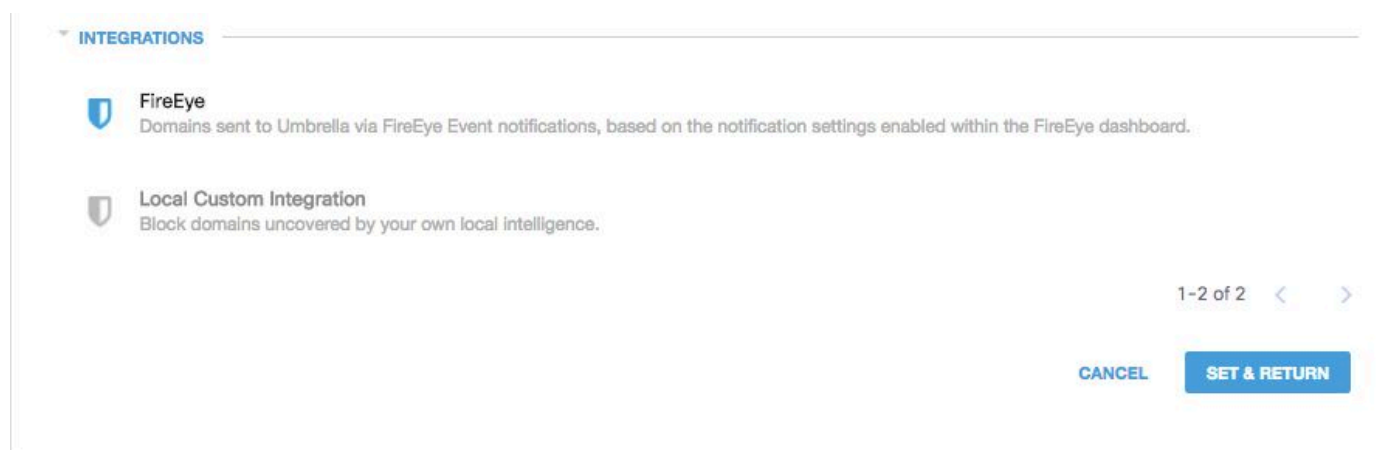
Next, in the Policy wizard, add this security setting to the policy you are editing:

1. Navigate to **Policies > Policy List**.
2. Expand a policy and under **Security Setting Applied** and select **Edit**.
3. In the **Security Settings** dropdown, select a security setting that includes the FireEye setting.



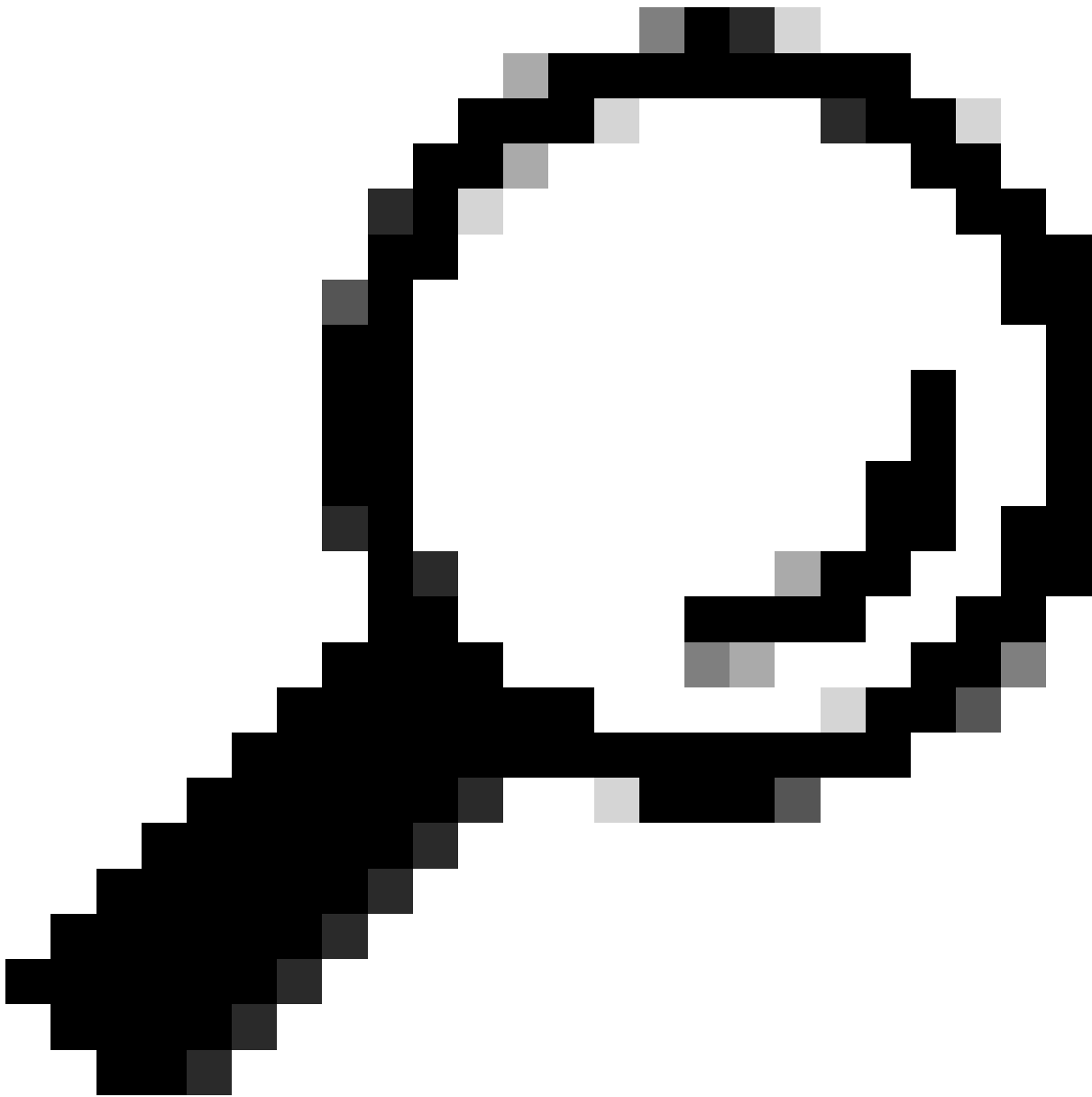
115014083083

The shield icon under Integrations updates to blue.



115013922146

4. Select **Set & Return**.



Tip: It is also possible to edit your Security Settings from the Policy wizard.

FireEye domains contained within the security setting for FireEye are blocked for identities using the policy.


Reporting within Cisco Umbrella for FireEye Events

Reporting on FireEye Security Events

The FireEye destination list is one of the security categories available for reports. Most or all of the reports use the Security Categories as a filter. For instance, you can filter security categories to only show FireEye-related activity:

1. Navigate to **Reporting > Activity Search**.

2. Under **Security Categories**, select **FireEye** to filter the report to only show the security category for FireEye.



Security Categories [Select All](#)

- ☐ Dynamic DNS
- ☐ Command and Control
- ☐ Malware
- ☐ Phishing
- ☒ **FireEye**
- ☐ Local Custom Integration
- ☐ Unauthorized IP Tunnel Access

APPLY

115013924986




3. Select **Apply** to see FireEye-related activity for the period selected in the report.

Reporting on when Domains Were Added to the FireEye Destination List

The Admin Audit log includes events from the FireEye appliance as it adds domains to the destination list. A user named “FireEye Account”, which is also branded with the FireEye logo, generates the events. These events include the domain that was added and the time at which it was added.

You can filter to only include FireEye changes by applying a filter for the “FireEye Account” user.

If the “Test Fire” step earlier was performed, the addition of the FireEye test domain can appear in the Audit Log.

Admin Audit Log 					
Date	Time	IP Address	User	Section	Action
Nov. 25, 20...	11:58:40 AM	67.215.87.13	 FireEye Account	Policy Setti...	Changed domains - FireEye Threat Feed
 Changed domains - FireEye Threat Feed					
<ul style="list-style-type: none"> Added Domain <ul style="list-style-type: none"> fireeye-testevent.ts1385409551488.example.com 					

Handling Unwanted Detections or False Positives

Allow Lists

Although unlikely, it is possible that domains added automatically by your FireEye appliance could potentially trigger an unwanted detection that blocks your users from accessing particular websites. In a situation like this, Umbrella recommends adding the domain(s) to an allow list (**Policies > Destination Lists**), which takes precedence over all other types of block lists, including security settings.

There are two reasons why this approach is preferable.

- First, in case the FireEye appliance was to re-add the domain after it was removed, the allow list safeguards against this causing further issues.
- Second, the allow list shows a historical record of problematic domains that can be used for forensics or audit reports.

By default, there is a Global Allow List that is applied to all policies. Adding a domain to the Global Allow List results in the domain being allowed in all policies.

If the FireEye security setting in block mode is only applied to a subset of your managed Cisco Umbrella identities (for instance, it is only applied to roaming computers and mobile devices), you can create a specific allow list for those identities or policies.

To create an allow list:

1. Navigate to **Policies > Destination Lists** and select the **Add** icon.
2. Select **Allow**, and add your domain to the list.
3. Select **Save**.

Once the destination list has been saved, you can add it to an existing policy covering those clients that have been affected by the unwanted block.

Deleting Domains from the FireEye Destination List

Next to each domain name in the FireEye destination list is a **Delete** icon. Deleting domains lets you clean up the FireEye destination list in the event of an unwanted detection.

However, the delete is **not** permanent if the FireEye appliance resends the domain to Cisco Umbrella.

To delete a domain:

1. Navigate to **Settings > Integrations**, then select "FireEye" to expand it.

2. Select **See Domains**.

3. Search for the domain name you want to delete.

4. Select the **Delete** icon.



5. Select **Close**.

6. Select **Save**.

In the instance of an unwanted detection or false positive, Umbrella recommends creating an allow list in Cisco Umbrella immediately and then remediating the false positive within the FireEye appliance. Later, you can remove the domain from the FireEye destination list.