

Integreer paraplu met FireEye

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Integratiefunctie](#)

[Uw Cisco Umbrella Dashboard configureren om informatie van FireEye te ontvangen](#)

[FireEye configureren voor communicatie met Cisco-paraplu](#)

[Zorgen voor connectiviteit: "Test Fire" tussen FireEye en Cisco Umbrella](#)

[Gebeurtenissen observeren toegevoegd aan de beveiligingsinstelling van FireEye in "Controlemodus"](#)

[Bestemmingslijst bekijken](#)

[Beveiligingsinstellingen voor een beleid bekijken](#)

[De beveiligingsinstellingen van FireEye toepassen in de "blokkmodus" op een beleid voor beheerde clients](#)

[Rapportage binnen Cisco Umbrella voor FireEye-evenementen](#)

[Rapportage over FireEye-beveiligingsgebeurtenissen](#)

[Rapportage over wanneer domeinen werden toegevoegd aan de bestemmingslijst van FireEye](#)

[Omgaan met ongewenste detecties of valse positieven](#)

[Lijsten toestaan](#)

[Domeinen verwijderen uit de bestemmingslijst van FireEye](#)

Inleiding

In dit document wordt beschreven hoe Cisco Umbrella met FireEye kan worden geïntegreerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Een FireEye-apparaat met toegang tot het openbare internet.
- Administratieve rechten Cisco Umbrella Dashboard.
- Het Cisco Umbrella Dashboard moet de FireEye-integratie hebben ingeschakeld.

Gebruikte componenten

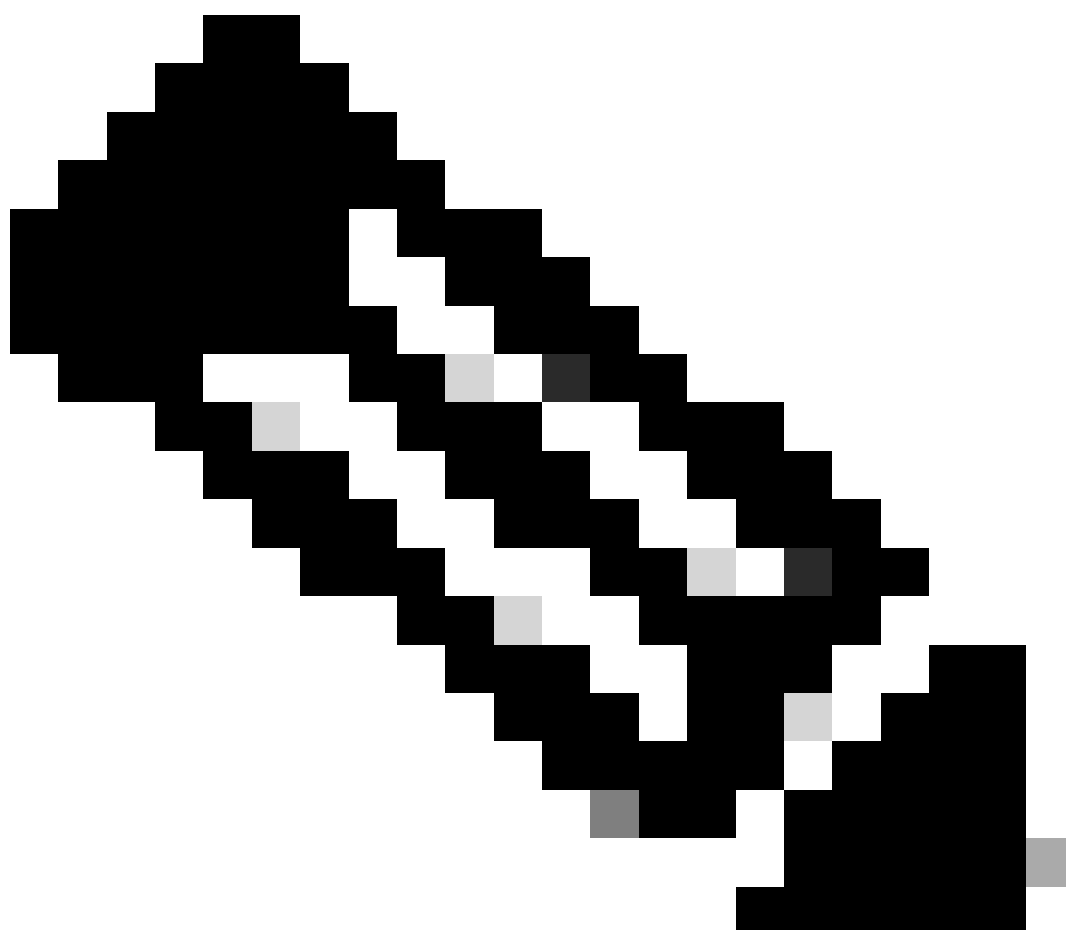
De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Met de integratie tussen het [FireEye-beveiligingstoestel en Cisco Umbrella](#), kunnen beveiligingsmedewerkers en beheerders nu de bescherming tegen geavanceerde bedreigingen uitbreiden naar zwervende laptops, tablets of telefoons, terwijl ze ook een andere handavingslaag bieden aan een gedistribueerd bedrijfsnetwerk.

In deze handleiding wordt beschreven hoe u uw FireEye kunt configureren om te communiceren met Cisco Umbrella, zodat beveiligingsgebeurtenissen van FireEye worden geïntegreerd in beleid dat kan worden toegepast op clients die worden beschermd door Cisco Umbrella.



Opmerking: de FireEye-integratie is alleen inbegrepen in [Cisco Umbrella-pakketten](#) zoals

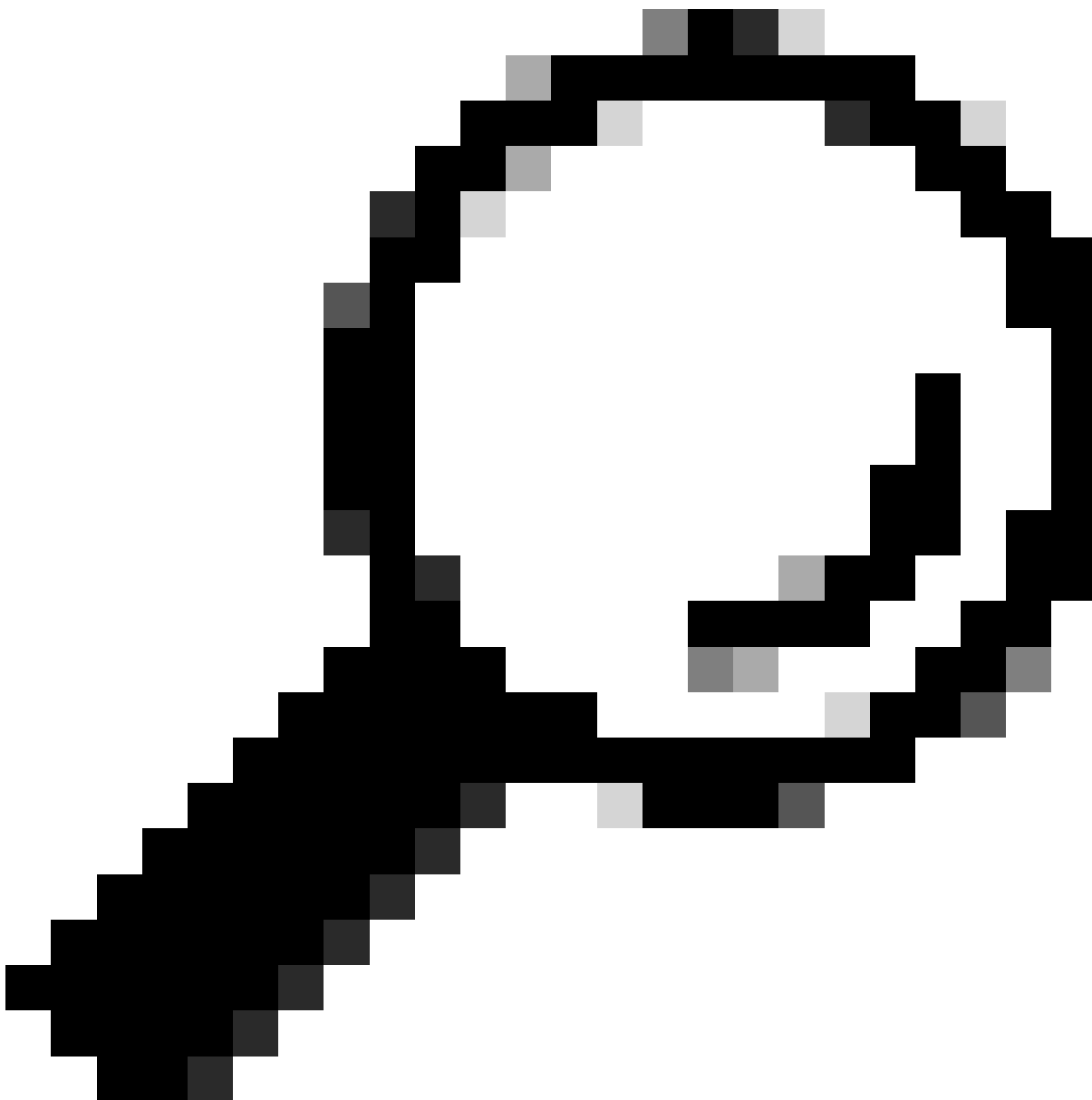
DNS Essentials, DNS Advantage, SIG Essentials of SIG Advantage. Als u niet over een van deze pakketten beschikt en de FireEye-integratie wilt gebruiken, neemt u contact op met uw Cisco Umbrella-accountmanager. Als u het juiste Cisco Umbrella-pakket hebt, maar FireEye niet als een integratie voor uw dashboard ziet, [neemt u contact op met Cisco Umbrella Support](#).

Integratiefunctionaliteit

Het FireEye-apparaat verzendt eerst op internet gebaseerde bedreigingen die het heeft gevonden, zoals domeinen die malware hosten, commando en controle voor botnet- of phishingsites, naar Cisco Umbrella.

Cisco Umbrella valideert vervolgens de informatie die aan Cisco Umbrella is doorgegeven om ervoor te zorgen dat deze geldig is en kan worden toegevoegd aan een beleid. Als wordt bevestigd dat de informatie van FireEye correct is geformatteerd (het is bijvoorbeeld geen bestand, een complexe URL of een zeer populair domein), wordt het domeinadres toegevoegd aan de bestemmingslijst van FireEye als onderdeel van een beveiligingsinstelling die kan worden toegepast op elk Cisco Umbrella-beleid. Dat beleid wordt onmiddellijk toegepast op alle verzoeken die worden gedaan vanaf apparaten met behulp van beleid met de bestemmingslijst van FireEye.

In de toekomst parseert Cisco Umbrella automatisch FireEye-waarschuwingen en voegt het kwaadaardige sites toe aan de FireEye-bestemmingslijst. Dit breidt FireEye-bescherming uit naar alle externe gebruikers en apparaten en biedt een andere laag van handhaving voor uw bedrijfsnetwerk.



Tip: Terwijl Cisco Umbrella zijn best doet om domeinen waarvan bekend is dat ze over het algemeen veilig zijn (bijvoorbeeld Google en Salesforce) te valideren en toe te staan, om ongewenste onderbrekingen te voorkomen, raden we aan domeinen toe te voegen die u nooit wilt hebben geblokkeerd in de Global Allow List of andere bestemmingslijsten volgens uw beleid. Voorbeelden zijn:

- De homepage voor uw organisatie
- Domeinen die diensten vertegenwoordigen die u levert en die zowel interne als externe records kunnen hebben. Bijvoorbeeld "mail.myservicedomain.com" en "portal.myotherservicedomain.com".
- Minder bekende cloudgebaseerde toepassingen waarvan u afhankelijk bent, zijn niet inbegrepen in automatische domeininvalidatie. Bijvoorbeeld "localcloudservice.com".

Deze domeinen kunnen worden toegevoegd aan de [Global Allow List](#), die te vinden is onder Beleid > Bestemmingslijsten in Cisco Umbrella.

Uw Cisco Umbrella Dashboard configureren om informatie van FireEye te ontvangen

De eerste stap is om uw unieke URL te vinden in Cisco Umbrella voor het FireEye-apparaat om mee te communiceren.

1. Meld u aan bij het Cisco Umbrella Dashboard als beheerder.
2. Navigeer naar **Beleid > Beleidscomponenten > Integraties** en selecteer FireEye in de tabel om deze uit te vouwen.
3. Selecteer het vak **Inschakelen** en selecteer vervolgens **Opslaan**. Dit genereert een unieke, specifieke URL voor uw organisatie binnen 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=Z12616ea-1683-47b9-b854-4b3aa69b02a3`

[SEE DOMAINS](#)

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

U kunt deze URL later gebruiken om het FireEye-toestel te configureren voor het verzenden van gegevens naar Cisco Umbrella, dus zorg ervoor dat u de URL kopieert.

FireEye configureren voor communicatie met Cisco-paraplu

Om te beginnen met het verzenden van verkeer van uw FireEye-toestel naar Cisco Umbrella, moet u FireEye configureren met de URL-informatie die in de vorige sectie is gegenereerd.

1. Meld u aan bij FireEye en selecteer **Instellingen**.

[Dashboard](#)[Alerts](#)[Summaries](#)[Filters](#)[Settings](#)[Reports](#)[About](#)

FireEye Dashboard (Current)

Detection/Protection

Total Infected Hosts

Total Alerts Count

Total Blocked Alerts

Top Malware By Host

Grouped by infection malw

2. Selecteer Meldingen in de lijst met instellingen:

[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:

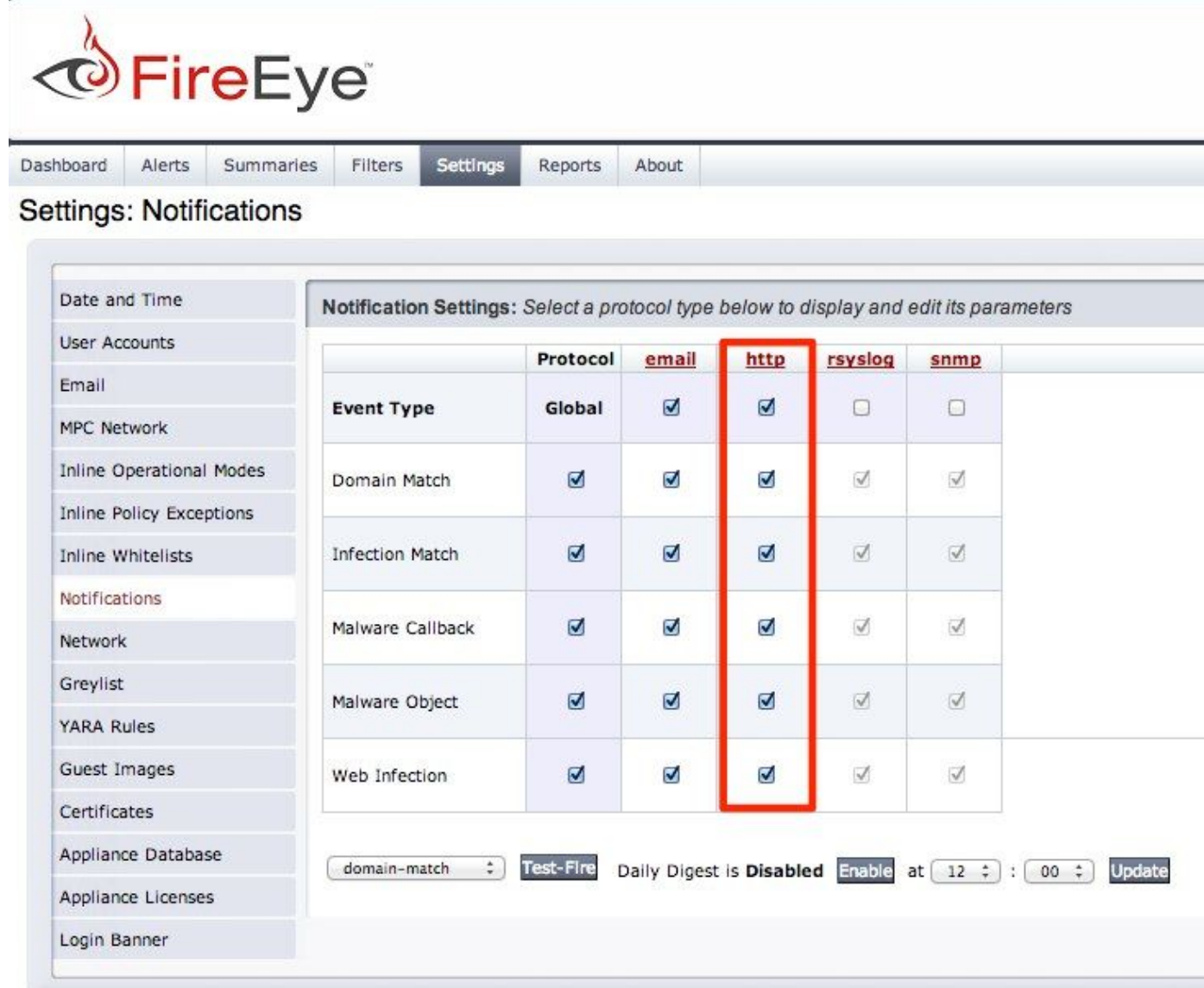
NTP Server	Delete	Update T
pool.ntp.org	☐	Update T
time.nist.gov	☐	Update T

Remove Selected NTP Servers

Set Time Zone:

UTC Set Time Zone

3. Zorg ervoor dat alle gebeurtenistypen die naar Cisco Umbrella worden verzonden, zijn geselecteerd (Umbrella beveelt aan om met alle te beginnen) en selecteer vervolgens de HTTP-koppeling boven aan de kolom.



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	☒	☒	☐	☐
Domain Match	☒	☒	☒	☒	☒
Infection Match	☒	☒	☒	☒	☒
Malware Callback	☒	☒	☒	☒	☒
Malware Object	☒	☒	☒	☒	☒
Web Infection	☒	☒	☒	☒	☒

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

4. Wanneer het menu wordt uitgebreid, selecteert u deze opties om Gebeurtenismelding in te schakelen. De genummerde stappen worden beschreven in de screenshot:

1. Standaardlevering: per gebeurtenis
2. Standaardprovider: Algemeen
3. Standaardformaat: JSON Extended
4. Noem de HTTP-server "OpenDNS".
5. Server-URL: Plak de Cisco Umbrella URL die u eerder op uw Cisco Umbrella-dashboard hebt gegenereerd.
6. Melding vervolgkeuzelijst: Selecteer Alle gebeurtenissen om maximale dekking te garanderen.

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

	Protocol	email	http	rsyslog	snmp	Settings
Event Type	Global	☒	☒	☐	☐	HTTP Settings Default delivery: 1 Per event Default provider: 2 Generic Default format: 3 JSON Extended Apply Settings
Domain Match	☒	☒	☒	☒	☒	
Infection Match	☒	☒	☒	☒	☒	
Malware Callback	☒	☒	☒	☒	☒	
Malware Object	☒	☒	☒	☒	☒	
Web Infection	☒	☒	☒	☒	☒	

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

Remove	Name	Enabled	Server Url	Auth	Username	Password	Notification	Delivery	Account
☐		☒	5	☐			All Events 6	Per event	
			SSL Enable	SSL Verify	Default Provider	Provider Parameters			
			☒	☐	Generic	Message Format JSON Extended			

5. Zorg ervoor dat de vervolgkeuzelijsten Levering, Standaardprovider en Leveranciersparameters allemaal overeenkomen met de standaardinstellingen of dat er meerdere meldingsservers worden gebruikt:

- Levering: per event basis
- Standaardprovider: Algemeen
- Provider-parameters: berichtindeling JSON Extended
- (Optioneel) Als u liever verkeer via SSL verzendt, selecteert u SSL inschakelen.

Op dit punt is uw FireEye-toestel ingesteld om de geselecteerde gebeurtenistypen naar Cisco Umbrella te verzenden. Leer vervolgens hoe u deze informatie kunt zien in uw Cisco Umbrella Dashboard en stel een beleid in om dit verkeer te blokkeren.

Zorgen voor connectiviteit: "Test Fire" tussen FireEye en Cisco Umbrella

Op dit punt is het een goed idee om uw connectiviteit te testen en ervoor te zorgen dat alles goed is ingesteld:

1. Selecteer in FireEye domeinovereenkomst in de vervolgkeuzelijst Test Fire en selecteer 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	☒	☒	☐	☐	
Domain Match	☒	☒	☒	☒	☒	
Infection Match	☒	☒	☒	☒	☒	
Malware Callback	☒	☒	☒	☒	☒	
Malware Object	☒	☒	☒	☒	☒	
Web Infection	☒	☒	☒	☒	☒	

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

In Cisco Umbrella bevat de FireEye-integratie een lijst met domeinen die door de FireEye Appliance worden verstrekt om te zien welke domein(en) actief worden toegevoegd.

2. Nadat u Test Fire hebt geselecteerd, navigeert u in Cisco Umbrella naar Instellingen > Integraties en selecteert u FireEye in de tabel om deze uit te vouwen.

3. Selecteer Zie domeinen.

Settings / Integrations
Integrations

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	✖
27n9u6w6eiq5hpremjmz887.org	✖

CLOSE

Status
Enabled
Disabled
Disabled

Learn more

18

SAVE

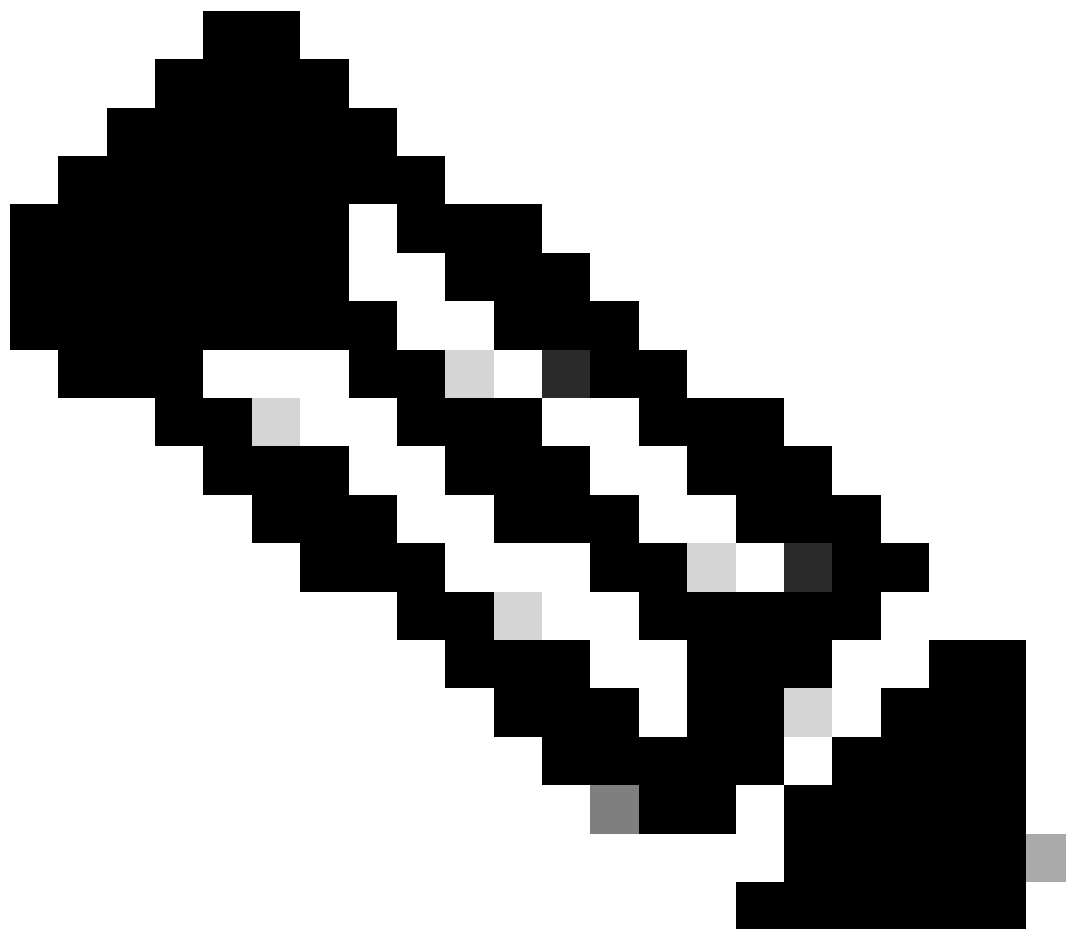
Als u Testbrand selecteert, wordt een domein gegenereerd in de lijst met bestemmingen van FireEye met de naam "fireeye-testevent.example.com-[date]". Elke keer dat u Test Fire in FireEye selecteert, wordt een uniek domein gemaakt met de datum in UNIX Epoch-tijd gekoppeld aan de test, zodat toekomstige tests een unieke testdomeinnaam kunnen hebben.

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

Als de Test Fire succesvol is, worden meer gebeurtenissen van FireEye naar Cisco Umbrella verzonden en begint een doorzoekbare lijst te worden ingevuld en te groeien.

Gebeurtenissen observeren toegevoegd aan de beveiligingsinstelling van FireEye in "Controlemodus"

De gebeurtenissen van uw FireEye-apparaat beginnen een specifieke bestemmingslijst te vullen die kan worden toegepast op beleid als een FireEye-beveiligingscategorie. De doellijst en de beveiligingscategorie bevinden zich standaard in de "controlemodus" en worden niet toegepast op beleidsregels. Dit kan niet leiden tot wijzigingen in uw bestaande Cisco-beleidsregels.

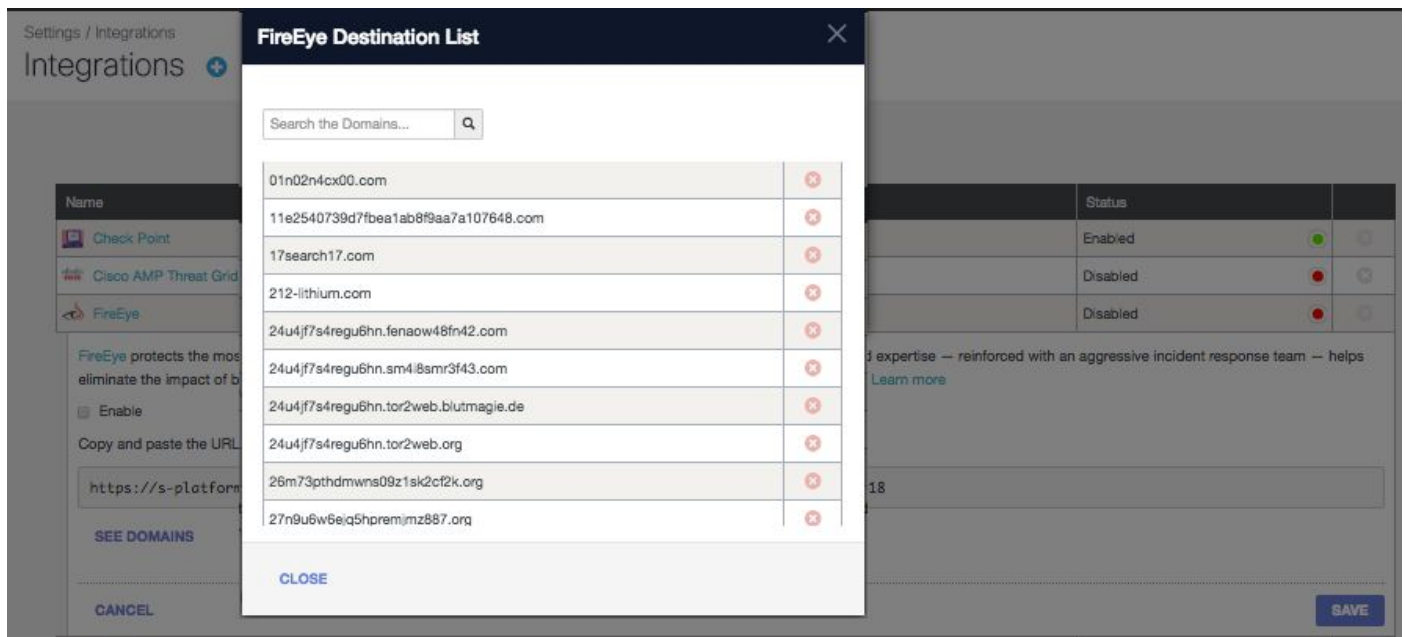


Opmerking: de "Controlemodus" kan worden ingeschakeld zolang dit nodig is op basis van uw implementatieprofiel en netwerkconfiguratie.

Bestemmingslijst bekijken

U kunt de FireEye-bestemmingslijst op elk gewenst moment bekijken:

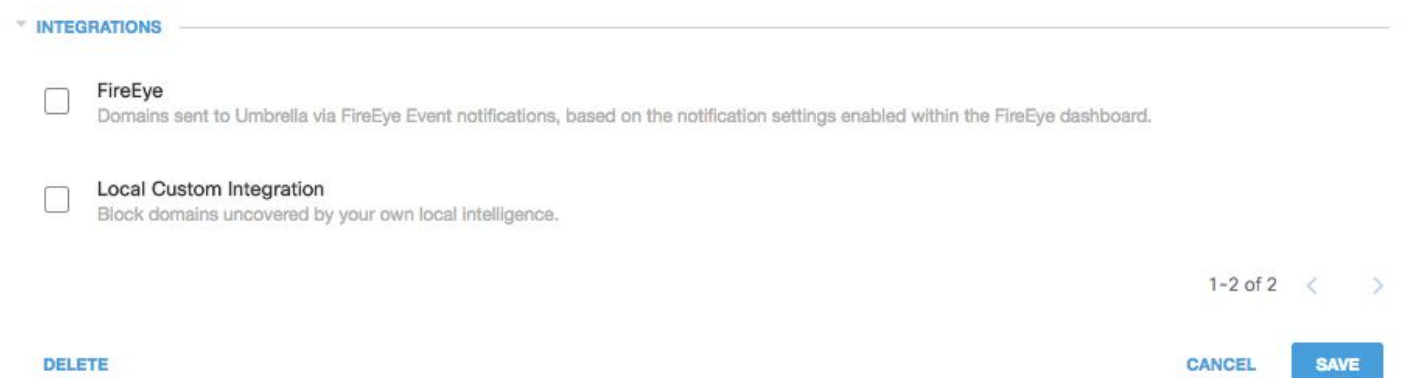
1. Ga naar **Beleid > Beleidscomponenten > Integraties**.
2. Vouw FireEye in de tabel uit en selecteer **Zie domeinen**.



Beveiligingsinstellingen voor een beleid bekijken

U kunt de beveiligingsinstellingen bekijken die op elk gewenst moment aan een beleid kunnen worden toegevoegd:

1. Navigeer naar Beleid > Beleidscomponenten > Beveiligingsinstellingen.
2. Selecteer een beveiligingsinstelling in de tabel om deze uit te vouwen en blader naar Integraties om de FireEye-instelling te vinden.



115014080803

U kunt ook integratiegegevens bekijken via de overzichtspagina Beveiligingsinstellingen.

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

Security Setting Applied: Default Settings

• Command and Control Callbacks, Malware, and Phishing Attacks will be blocked

• No integration is enabled.

Edit Disable

Content Setting Applied: High

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

Edit Disable

2 Destination Lists Enforced

• 1 Block List

• 1 Allow List

Edit

Umbrella Default Block Page Applied

Edit Preview Block Page

ADVANCED SETTINGS

DELETE POLICY

CANCEL

SAVE

115013920526

Wanneer u aan de slag gaat, kunt u deze beveiligingsinstelling het beste leeg laten om ervoor te zorgen dat domeinen correct worden ingevuld in een "auditmodus".

De beveiligingsinstellingen van FireEye toepassen in de "blokmodus" op een beleid voor beheerde clients

Zodra u klaar bent om deze extra beveiligingsbedreigingen te laten afdwingen door clients die worden beheerd door Cisco Umbrella, wijzigt u de beveiligingsinstelling voor een bestaand beleid of maakt u een nieuw beleid dat boven uw standaardbeleid staat om ervoor te zorgen dat het eerst wordt afgedwongen.

Maak of werk eerst een beveiligingsinstelling bij:

1. Navigeer naar Beleid > Beleidscomponenten > Beveiligingsinstellingen.
2. Selecteer onder Integraties de optie FireEye en selecteer Opslaan.

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

Voeg vervolgens in de wizard Beleid deze beveiligingsinstelling toe aan het beleid dat u bewerkt:

1. Navigeer naar Beleid > Beleidslijst.
2. Vouw een beleid uit onder Beveiligingsinstelling toegepast en selecteer Bewerken.
3. Selecteer in de vervolgkeuzelijst Beveiligingsinstellingen een beveiligingsinstelling die de instelling FireEye bevat.

Security Settings

Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.

Default Settings

New Security Setting 2

Default Settings

MSP Default Settings

New Security Setting

New Security Setting 1

ADD NEW SETTING

icious software, drive-by downloads/exploits, mobile threats and more

cently. These are often used in new attacks.

nunicating with attackers' infrastructure

115014083083

Het schildpictogram onder Integraties wordt bijgewerkt naar blauw.

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.

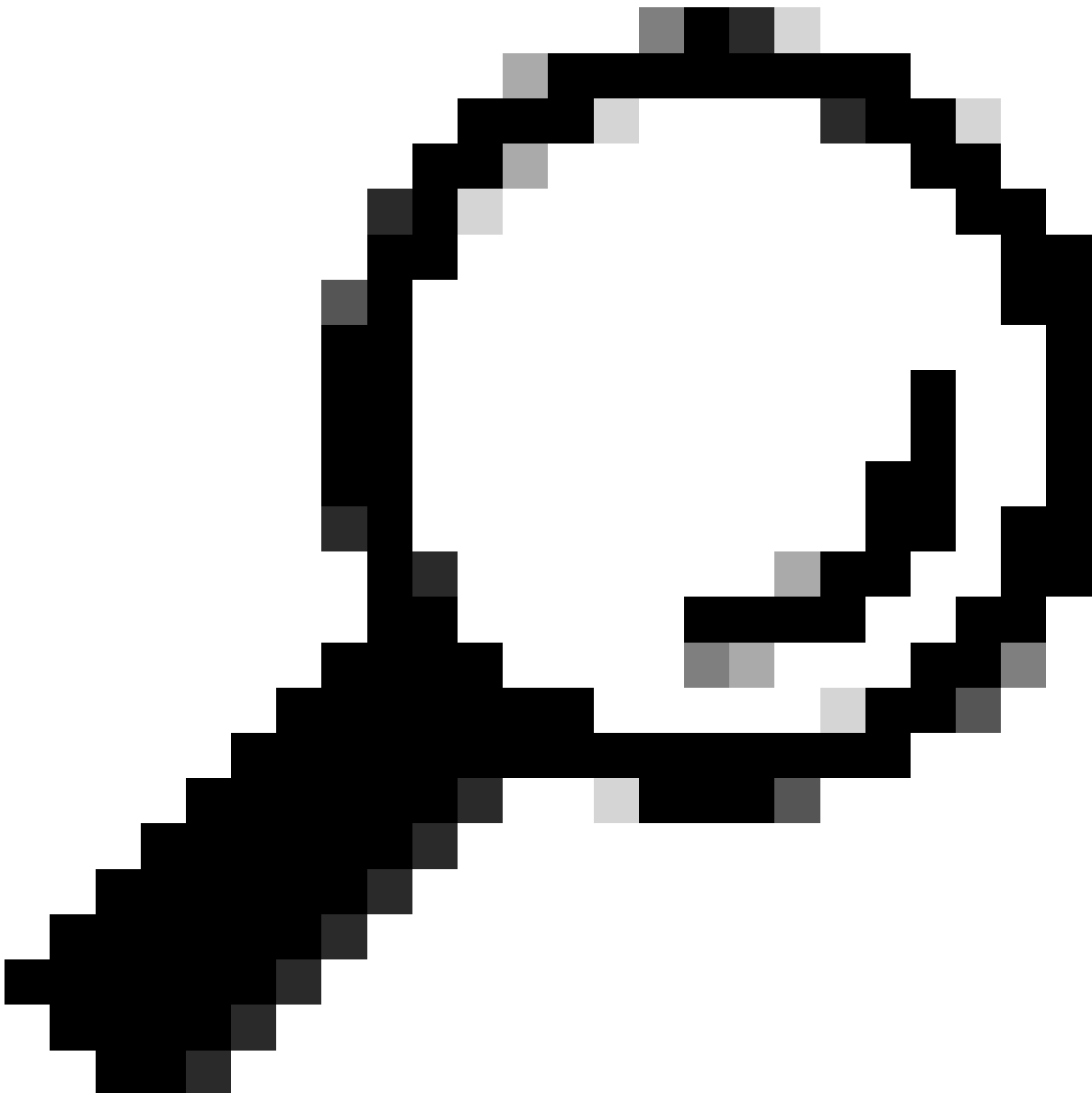
1-2 of 2 < >

CANCEL

SET & RETURN

115013922146

4. Selecter Set & Return.



Tip: Het is ook mogelijk om uw beveiligingsinstellingen te bewerken vanuit de wizard Beleid.

FireEye-domeinen die zich in de beveiligingsinstelling voor FireEye bevinden, worden geblokkeerd voor identiteiten die het beleid gebruiken.

Rapportage binnen Cisco Umbrella voor FireEye-evenementen

Rapportage over FireEye-beveiligingsgebeurtenissen

De bestemmingslijst van FireEye is een van de beveiligingscategorieën die beschikbaar zijn voor rapporten. De meeste of alle rapporten gebruiken de beveiligingscategorieën als filter. U kunt bijvoorbeeld beveiligingscategorieën filteren om alleen FireEye-gerelateerde activiteiten weer te geven:

1. Navigeer naar Rapportage > Zoeken naar activiteiten.
2. Selecteer onder Beveiligingscategorieën FireEye om het rapport te filteren zodat alleen de beveiligingscategorie voor FireEye wordt weergegeven.

Security Categories

Select All

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

APPLY

115013924986

3. Selecteer Toepassen om FireEye-gerelateerde activiteiten te bekijken voor de periode die in het rapport is geselecteerd.

Rapportage over wanneer domeinen werden toegevoegd aan de bestemmingslijst van FireEye

Het Admin Audit-logboek bevat gebeurtenissen uit het FireEye-toestel, omdat het domeinen toevoegt aan de bestemmingslijst. Een gebruiker met de naam "FireEye Account", die ook wordt gebrandmerkt met het FireEye-logo, genereert de evenementen. Deze gebeurtenissen omvatten het domein dat is toegevoegd en het moment waarop het is toegevoegd.

U kunt filteren om alleen FireEye-wijzigingen op te nemen door een filter toe te passen voor de gebruiker "FireEye-account".

Als de "Test Fire"-stap eerder is uitgevoerd, kan de toevoeging van het FireEye-testdomein

worden weergegeven in het auditlogboek.

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					
• Added Domain					
• fireeye-testevent.ts1385409551488.example.com					

Omgaan met ongewenste detecties of valse positieven

Lijsten toestaan

Hoewel onwaarschijnlijk, is het mogelijk dat domeinen die automatisch door uw FireEye-apparaat worden toegevoegd, mogelijk een ongewenste detectie kunnen veroorzaken die uw gebruikers blokkeert om toegang te krijgen tot bepaalde websites. In een dergelijke situatie raadt Umbrella aan om het domein toe te voegen aan een lijst met machtigingen (Beleid > Bestemmingslijsten), die voorrang heeft op alle andere soorten blokkeringslijsten, inclusief beveiligingsinstellingen.

Er zijn twee redenen waarom deze aanpak de voorkeur verdient.

- Ten eerste, in het geval dat het FireEye-apparaat het domein opnieuw zou toevoegen nadat het was verwijderd, staat de lijst beveiligingen toe tegen dit veroorzaken van verdere problemen.
- Ten tweede toont de allow-lijst een historisch record van problematische domeinen die kunnen worden gebruikt voor forensisch onderzoek of auditrapporten.

Standaard is er een algemene lijst met toegestane items die wordt toegepast op alle beleidsregels. Als u een domein toevoegt aan de algemene machtigingslijst, wordt het domein toegestaan in alle beleidsregels.

Als de FireEye-beveiligingsinstelling in de blokmodus alleen wordt toegepast op een subset van uw beheerde Cisco Umbrella-identiteiten (deze wordt bijvoorbeeld alleen toegepast op zwervende computers en mobiele apparaten), kunt u een specifieke machtigingslijst maken voor die identiteiten of beleidsregels.

U maakt als volgt een lijst met machtigingen:

1. Navigeer naar Beleid > Bestemmingslijsten en selecteer het pictogram Toevoegen.
2. Selecteer Toestaan en voeg uw domein toe aan de lijst.
3. Selecteer Opslaan.

Zodra de bestemmingslijst is opgeslagen, kunt u deze toevoegen aan een bestaand beleid voor die clients die zijn getroffen door het ongewenste blok.

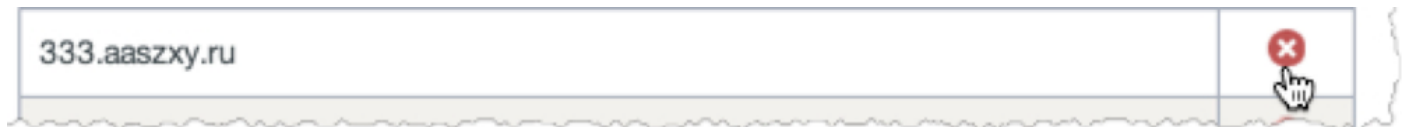
Domeinen verwijderen uit de bestemmingslijst van FireEye

Naast elke domeinnaam in de bestemmingslijst van FireEye staat een pictogram Verwijderen. Als u domeinen verwijdert, kunt u de bestemmingslijst van FireEye opschonen in het geval van een ongewenste detectie.

De verwijdering is echter niet permanent als het FireEye-toestel het domein opnieuw doorstuurt naar Cisco Umbrella.

Een domein verwijderen:

1. Navigeer naar Instellingen > Integraties en selecteer vervolgens "FireEye" om het uit te vouwen.
2. Selecteer Zie domeinen.
3. Zoek naar de domeinnaam die u wilt verwijderen.
4. Selecteer het pictogram Verwijderen.



5. Selecteer Sluiten.
6. Selecteer Opslaan.

In het geval van een ongewenste detectie of vals-positief, raadt Umbrella aan om onmiddellijk een allow-lijst in Cisco Umbrella te maken en vervolgens het vals-positieve in het FireEye-apparaat te herstellen. Later kunt u het domein verwijderen uit de bestemmingslijst van FireEye.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.