

Integre o Umbrella com o FireEye

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Funcionalidade de integração](#)

[Configurando seu painel do Cisco Umbrella para receber informações do FireEye](#)

[Configurando o FireEye para se comunicar com o Cisco Umbrella](#)

[Garantindo a conectividade: "Teste de fogo" entre o FireEye e o Cisco Umbrella](#)

[Observação de eventos adicionados à configuração de segurança do FireEye em "Modo de auditoria"](#)

[Revisar lista de destinos](#)

[Revisar Configurações de Segurança para uma Política](#)

[Aplicação das configurações de segurança do FireEye no "modo de bloqueio" a uma política para clientes gerenciados](#)

[Relatórios dentro do Cisco Umbrella para eventos FireEye](#)

[Relatórios sobre eventos de segurança do FireEye](#)

[Relatórios sobre quando os domínios foram adicionados à lista de destinos do FireEye](#)

[Lidando com detecções indesejadas ou falsos positivos](#)

[Listas de permissão](#)

[Excluindo domínios da lista de destinos do FireEye](#)

Introdução

Este documento descreve como integrar o Cisco Umbrella com FireEye.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Um dispositivo FireEye com acesso à Internet pública.
- Direitos administrativos do Cisco Umbrella Dashboard.
- O Cisco Umbrella Dashboard deve ter a integração do FireEye habilitada.

Componentes Utilizados

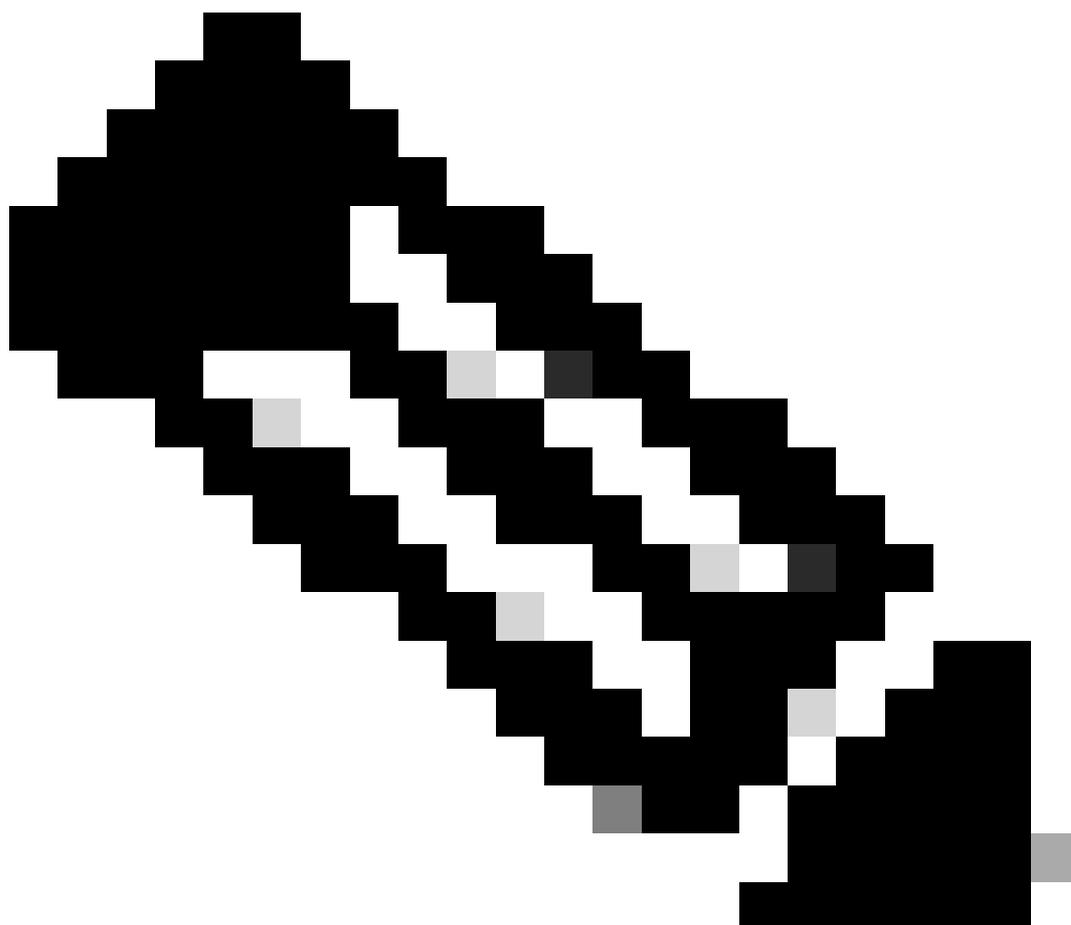
As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Com a integração entre o [dispositivo de segurança FireEye e o Cisco Umbrella](#), os administradores e os responsáveis pela segurança agora podem estender a proteção contra ameaças avançadas a laptops, tablets ou telefones móveis e, ao mesmo tempo, fornecer outra camada de aplicação a uma rede corporativa distribuída.

Este guia descreve como configurar seu FireEye para se comunicar com o Cisco Umbrella para que os eventos de segurança do FireEye sejam integrados em políticas que possam ser aplicadas a clientes protegidos pelo Cisco Umbrella.



Note: A integração do FireEye está incluída apenas nos [pacotes do Cisco Umbrella](#) como

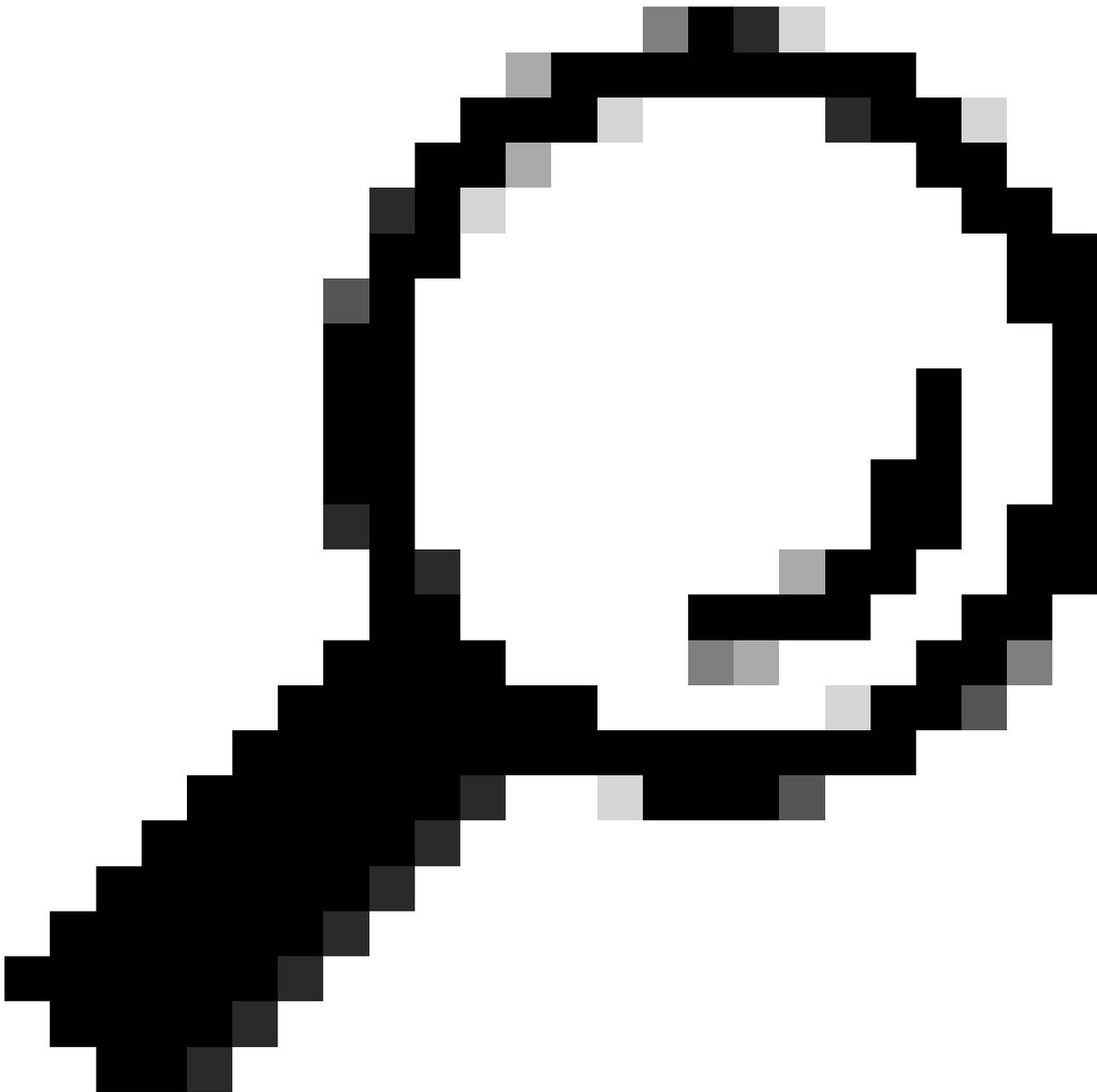
DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage. Se você não tiver um desses pacotes e quiser ter a integração com o FireEye, entre em contato com o seu Cisco Umbrella Account Manager. Se você tiver o pacote Cisco Umbrella correto, mas não vir o FireEye como uma integração para seu painel, entre em [contato com o Suporte do Cisco Umbrella](#).

Funcionalidade de integração

O dispositivo FireEye envia primeiro ameaças com base na Internet que encontrou, como domínios que hospedam malware, comandos e controles para botnet ou sites de phishing, para o Cisco Umbrella.

Em seguida, o Cisco Umbrella valida as informações passadas ao Cisco Umbrella para garantir que sejam válidas e possam ser adicionadas a uma política. Se for confirmado que as informações do FireEye estão formatadas corretamente (por exemplo, não é um arquivo, uma URL complexa ou um domínio altamente popular), o endereço de domínio será adicionado à lista de destinos do FireEye como parte de uma configuração de segurança que pode ser aplicada a qualquer política do Cisco Umbrella. Essa política é aplicada imediatamente a todas as solicitações feitas de dispositivos que usam políticas com a lista de destino do FireEye.

No futuro, o Cisco Umbrella analisa automaticamente os alertas do FireEye e adiciona sites mal-intencionados à lista de destinos do FireEye. Isso estende a proteção do FireEye a todos os usuários e dispositivos remotos e fornece outra camada de aplicação à rede corporativa.



Tip: Embora o Cisco Umbrella faça o possível para validar e permitir domínios que são conhecidos como seguros em geral (por exemplo, Google e Salesforce), para evitar interrupções indesejadas, sugerimos adicionar domínios que você nunca deseja ter bloqueado à Lista de Permissões Global ou a outras listas de destino de acordo com sua política. Por exemplo:

- A página inicial da sua organização
- Domínios que representam os serviços que você fornece e que podem ter registros internos e externos. Por exemplo, "mail.myservicedomain.com" e "portal.myotherservicedomain.com".
- Os aplicativos menos conhecidos baseados em nuvem dos quais você depende não fazem parte da validação automática de domínio do Cisco Umbrella. Por exemplo, "localcloudservice.com".

Esses domínios podem ser adicionados à [Lista de permissões global](#), que é encontrada

em Políticas > Listas de destino no Cisco Umbrella.

Configurando seu painel do Cisco Umbrella para receber informações do FireEye

A primeira etapa é encontrar sua URL exclusiva no Cisco Umbrella para que o dispositivo FireEye se comunique com o.

1. Efetue login no Cisco Umbrella Dashboard como Administrador.
2. Navegue até Políticas > Policy Components > Integrations e selecione FireEye na tabela para expandi-la.
3. Selecione a caixa Ativar e, em seguida, selecione Salvar. Isso gera um URL exclusivo e específico para sua empresa no 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](#)

Você pode usar esse URL posteriormente para configurar o dispositivo FireEye para enviar dados ao Cisco Umbrella, portanto, copie o URL.

Configurando o FireEye para se comunicar com o Cisco Umbrella

Para começar a enviar tráfego do seu dispositivo FireEye para o Cisco Umbrella, você deve configurar o FireEye com as informações de URL geradas na seção anterior.

1. Faça login no FireEye e selecione Settings.



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. Selecione Notificações na lista de configurações:



- 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:

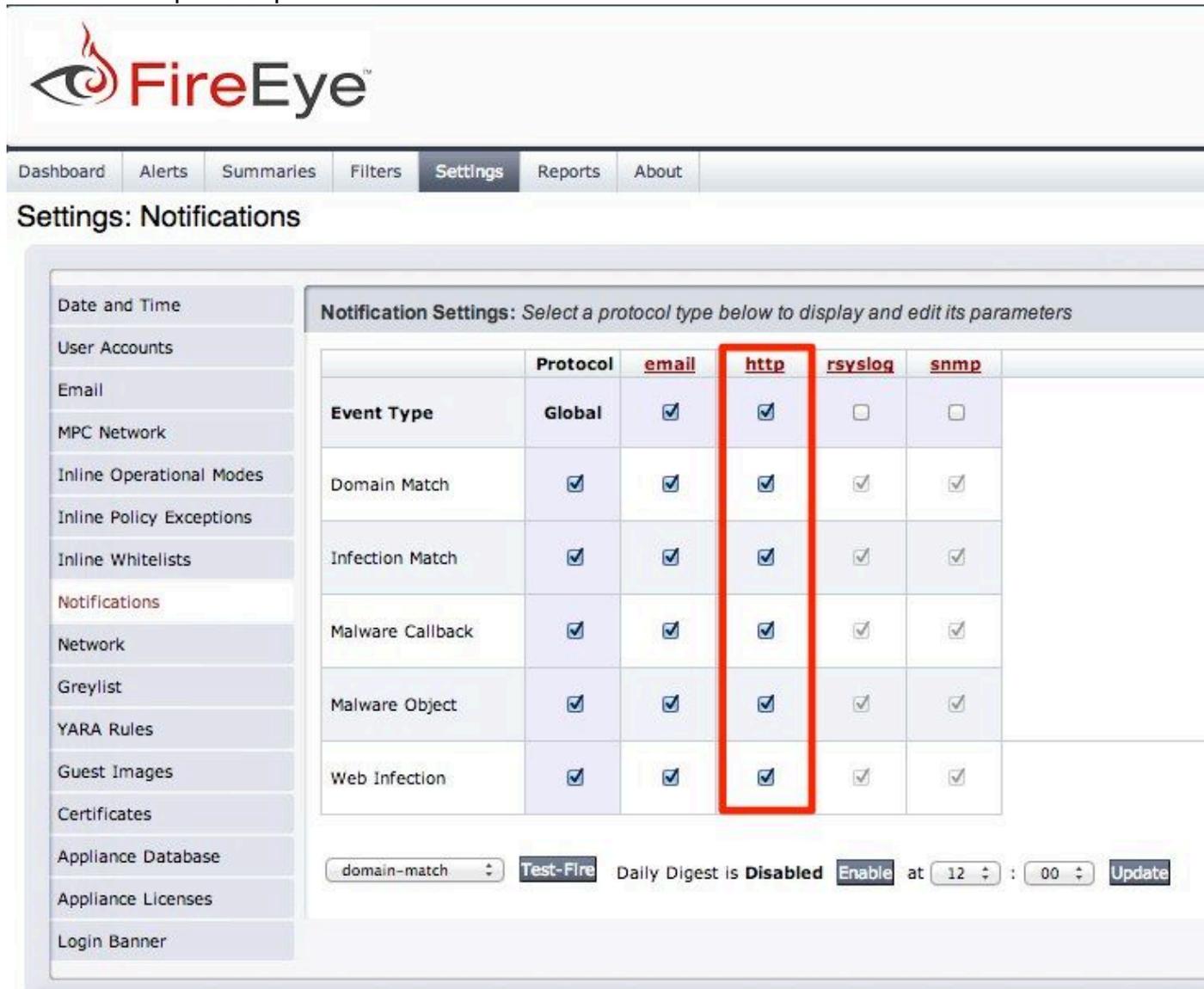
NTP Server	Delete	Update T
pool.ntp.org	<input type="checkbox"/>	Update T
time.nist.gov	<input type="checkbox"/>	Update T

Remove Selected NTP Servers

Set Time Zone:

UTC **Set Time Zone**

3. Certifique-se de que todos os Tipos de Evento a serem enviados para o Cisco Umbrella estejam selecionados (o Umbrella recomenda começar com todos) e, em seguida, selecione o link HTTP na parte superior da coluna.



The screenshot shows the FireEye interface with the 'Settings: Notifications' page. A sidebar on the left lists various configuration categories, with 'Notifications' selected. The main content area displays a table of notification settings. The 'http' column is highlighted with a red box. Below the table, there are controls for a specific event type, including a dropdown menu, a 'Test-Fire' button, and a 'Daily Digest' toggle set to 'Disabled'.

	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"/>				
Infection Match	<input checked="" type="checkbox"/>				
Malware Callback	<input checked="" type="checkbox"/>				
Malware Object	<input checked="" type="checkbox"/>				
Web Infection	<input checked="" type="checkbox"/>				

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

4. Quando o menu se expandir, selecione estas opções para ativar a Notificação de Eventos. As etapas numeradas estão descritas na captura de tela:

1. Entrega padrão: Por evento
2. Provedor padrão: GENÉRICO
3. Formato padrão: JSON estendido
4. Nomeie o HTTP Server como "OpenDNS".
5. Url Do Servidor: Cole aqui a URL do Cisco Umbrella que você gerou do painel do Cisco Umbrella anteriormente.
6. Menu suspenso Notificação: Selecione All Events para garantir cobertura máxima.

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"/>	Settings 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"/>					
Infection Match	<input checked="" type="checkbox"/>					
Malware Callback	<input checked="" type="checkbox"/>					
Malware Object	<input checked="" type="checkbox"/>					
Web Infection	<input checked="" type="checkbox"/>					

HTTP Server Listing Add HTTP Server: Name:

Remove	Name	Enabled	Server Url	Auth	Username	Password	Notification	Delivery	Account
<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="text" value="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. Certifique-se de que as listas suspensas Delivery, Default Provider e Provider Parameters correspondam às configurações padrão ou se vários servidores de notificação estiverem sendo usados:

- Entrega: Base por evento
- Provedor padrão: GENÉRICO
- Parâmetros do provedor: Formato de mensagem estendido JSON
- (Opcional) Se você preferir enviar tráfego por SSL, selecione SSL Enable.

Neste ponto, seu dispositivo FireEye está configurado para enviar os tipos de evento selecionados para o Cisco Umbrella. Em seguida, saiba como visualizar essas informações no Cisco Umbrella Dashboard e defina uma política para bloquear esse tráfego.

Garantindo a conectividade: "Teste de fogo" entre o FireEye e o Cisco Umbrella

Neste ponto, é recomendável testar a conectividade e garantir que tudo esteja configurado corretamente:

1. No FireEye, selecione domain-match no menu suspenso Test Fire e selecione Test Fire:

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"/>					
Infection Match	<input checked="" type="checkbox"/>					
Malware Callback	<input checked="" type="checkbox"/>					
Malware Object	<input checked="" type="checkbox"/>					
Web Infection	<input checked="" type="checkbox"/>					

domain-match ▾ **Test-Fire**

Daily Digest is **Disabled** **Enable** at 12 : 00 **Update**

No Cisco Umbrella, a integração do FireEye inclui uma lista de domínios fornecidos pelo dispositivo FireEye para ver quais domínios estão sendo adicionados ativamente.

2. Depois de selecionar Testar fogo, no Cisco Umbrella, navegue para Configurações > Integrações e selecione FireEye na tabela para expandi-la.

3. Selecione Ver Domínios.

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.sm48smr3f43.com	✕
24u4jf7s4regu6hn.tor2web.blutmagle.de	✕
24u4jf7s4regu6hn.tor2web.org	✕
26m73pthdmwns09z1sk2cf2k.org	✕
27n9u6w6eiq5hpremjz887.org	✕

CLOSE

Status	
Enabled	● <input type="checkbox"/>
Disabled	● <input type="checkbox"/>
Disabled	● <input type="checkbox"/>

of expertise — reinforced with an aggressive incident response team — helps
Learn more

18

SAVE

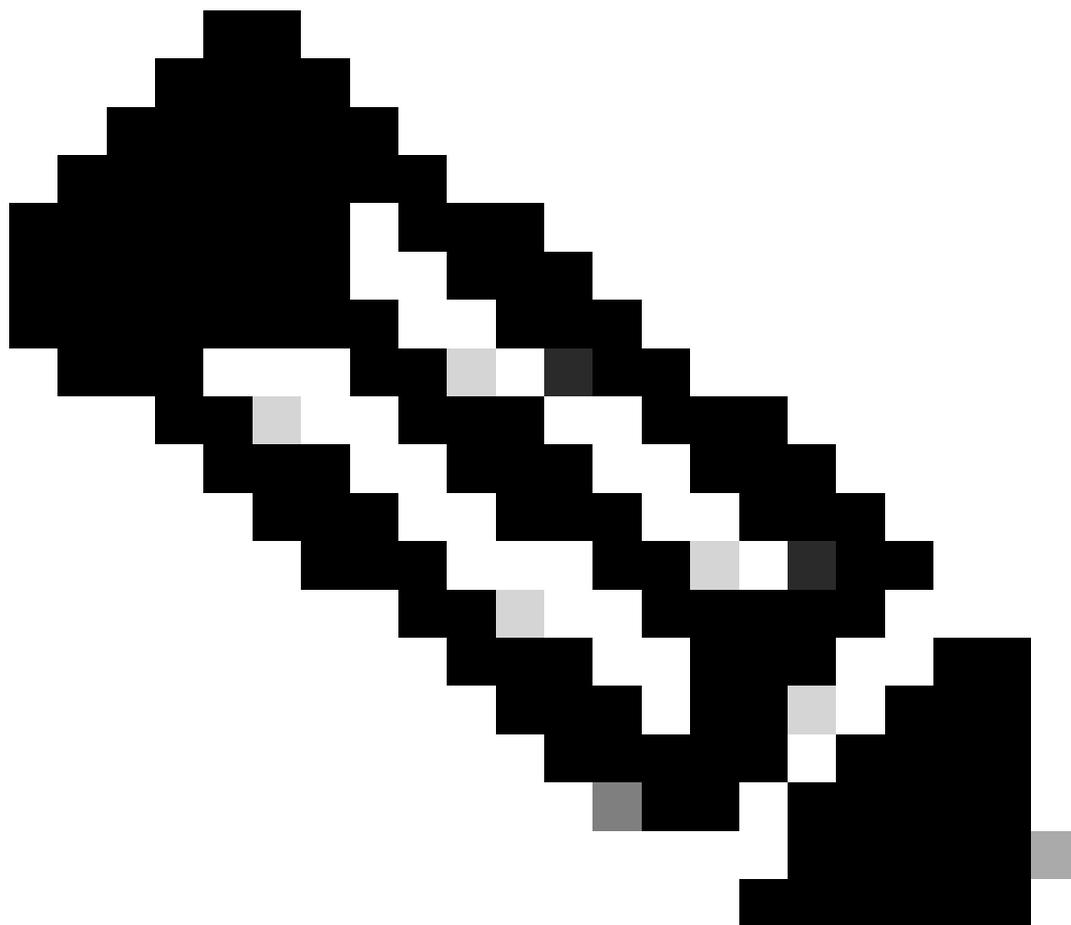
Selecionar Test Fire gera um domínio na lista de destinos do FireEye chamado "fireeye-testevent.example.com-[date]". Cada vez que você seleciona Test Fire no FireEye, ele cria um domínio exclusivo com a data no UNIX Epoch time anexada ao teste, para que os testes futuros possam ter um nome de domínio de teste exclusivo.

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

Se o teste de fogo for bem-sucedido, mais eventos do FireEye serão enviados ao Cisco Umbrella e uma lista pesquisável começará a ser preenchida e a crescer.

Observação de eventos adicionados à configuração de segurança do FireEye em "Modo de auditoria"

Os eventos do seu dispositivo FireEye começam a preencher uma lista de destinos específica que pode ser aplicada às políticas como uma categoria de segurança FireEye. Por padrão, a lista de destino e a categoria de segurança estão no "modo de auditoria" e não são aplicadas a nenhuma política e não podem resultar em nenhuma alteração nas políticas atuais do Cisco Umbrella.

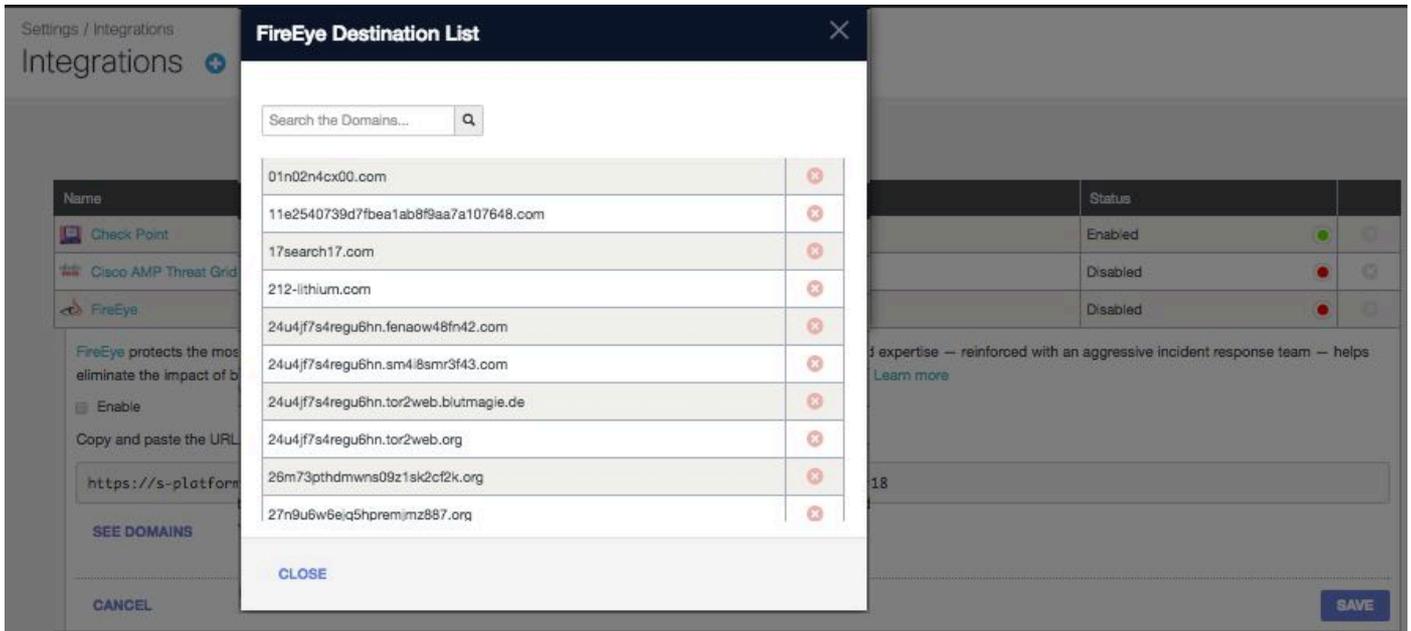


Note: O "modo de auditoria" pode ser ativado por quanto tempo for necessário, com base no perfil de implantação e na configuração da rede.

Revisar lista de destinos

Você pode revisar a lista de destinos do FireEye a qualquer momento:

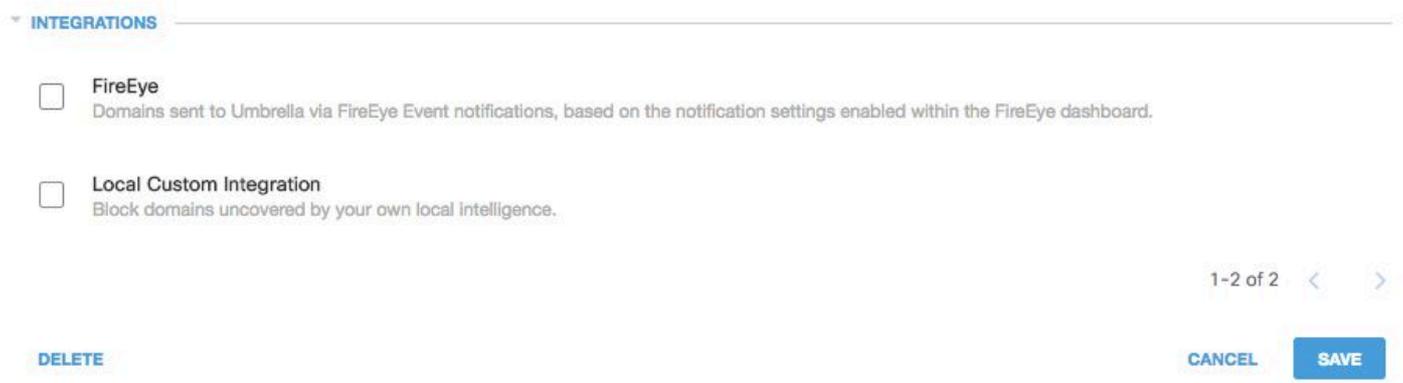
1. Navegue até **Policies > Policy Components > Integrations**.
2. Expanda FireEye na tabela e selecione **See Domains**.



Revisar Configurações de Segurança para uma Política

Você pode revisar as configurações de segurança que podem ser adicionadas a uma diretiva a qualquer momento:

1. Navegue até Políticas > Policy Components > Security Settings.
2. Selecione uma configuração de segurança na tabela para expandi-la e role até Integrations para localizar a configuração FireEye.



115014080803

Você também pode revisar as informações de integração através da página Resumo das configurações de segurança.

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

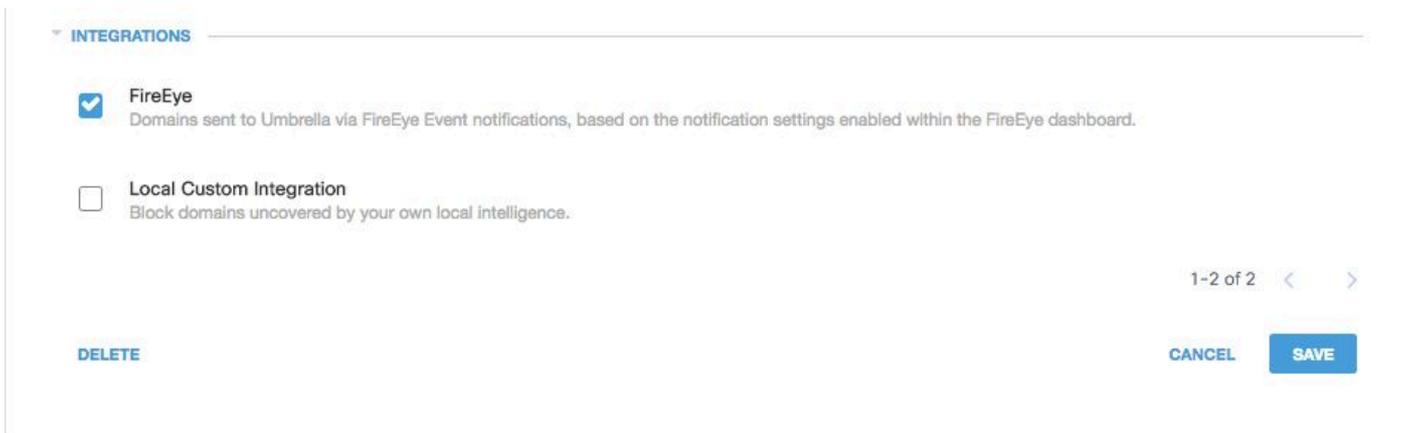
Ao começar, é melhor deixar essa configuração de segurança desmarcada para garantir que os domínios sejam preenchidos corretamente em um "modo de auditoria".

Aplicação das configurações de segurança do FireEye no "modo de bloqueio" a uma política para clientes gerenciados

Quando estiver pronto para que essas ameaças de segurança adicionais sejam aplicadas pelos clientes gerenciados pelo Cisco Umbrella, altere a configuração de segurança em uma política existente ou crie uma nova política que esteja acima da sua política padrão para garantir que ela seja aplicada primeiro.

Primeiro, crie ou atualize uma configuração de segurança:

1. Navegue até Policies > Policy Components > Security Settings.
2. Em Integrações, selecione FireEye e Salvar.



115013921406

Em seguida, no Assistente de política, adicione esta configuração de segurança à política que você está editando:

1. Navegue até Políticas > Policy List.
2. Expanda uma política e, em Configuração de segurança aplicada e selecione Editar.
3. No menu suspenso Configurações de segurança, selecione uma configuração de segurança que inclua a configuração FireEye.



115014083083

O ícone de escudo em Integrações é atualizado para azul.

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.

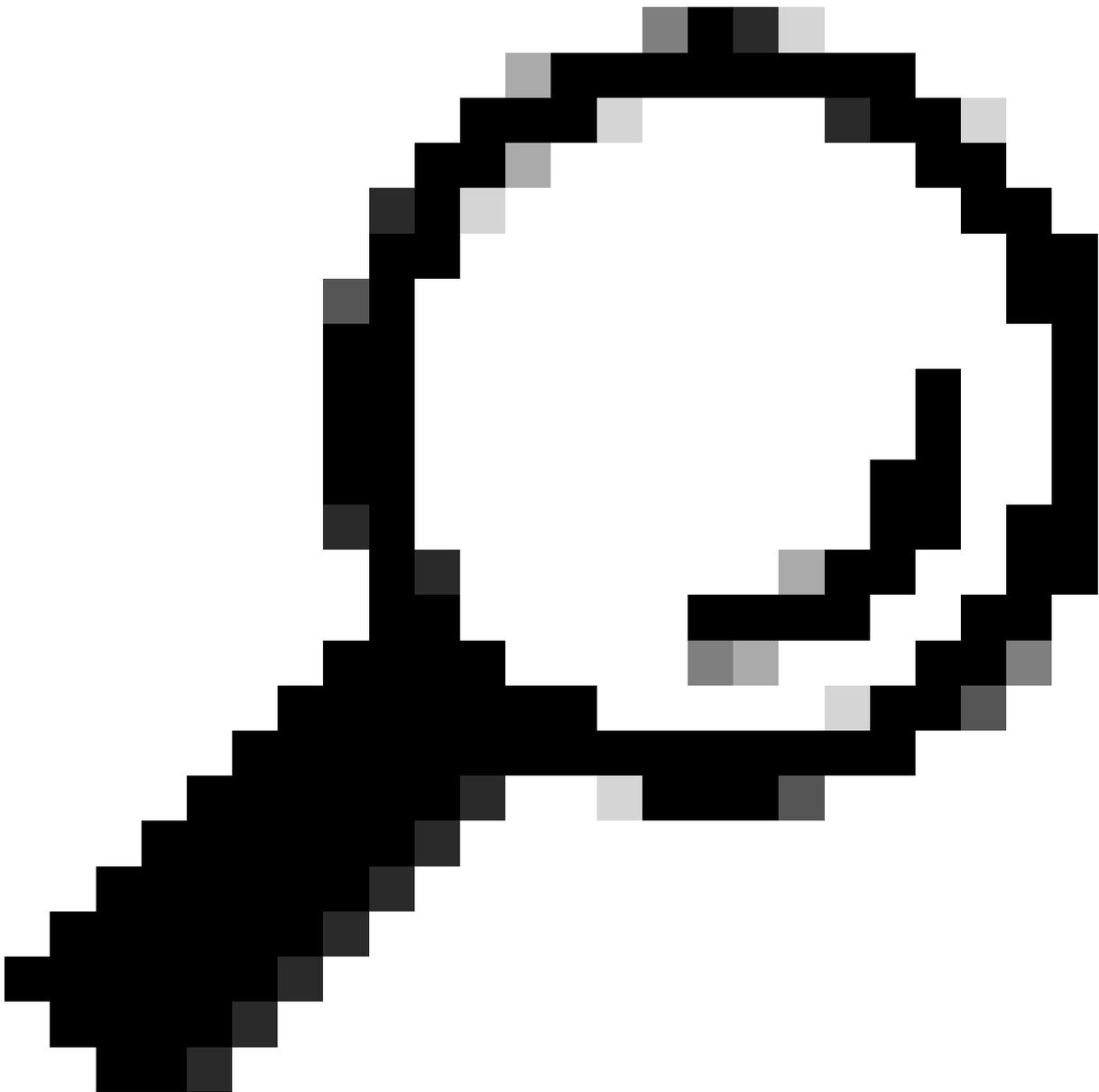
1-2 of 2 < >

CANCEL

SET & RETURN

115013922146

4. Seleccione Definir &Retorno.



Tip: Também é possível editar as Configurações de segurança no Assistente de política.

Os domínios FireEye contidos na configuração de segurança do FireEye são bloqueados para identidades usando a política.

Relatórios dentro do Cisco Umbrella para eventos FireEye

Relatórios sobre eventos de segurança do FireEye

A lista de destinos do FireEye é uma das categorias de segurança disponíveis para relatórios. A maioria ou todos os relatórios usam as Categorias de segurança como um filtro. Por exemplo, você pode filtrar as categorias de segurança para mostrar apenas as atividades relacionadas ao FireEye:

1. Navegue até Relatórios > Pesquisa de Atividade.
2. Em Categorias de Segurança, selecione FireEye para filtrar o relatório para mostrar apenas a categoria de segurança do FireEye.

Security Categories

Select All

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

APPLY

115013924986

3. Selecione Aplicar para ver as atividades relacionadas ao FireEye para o período selecionado no relatório.

Relatórios sobre quando os domínios foram adicionados à lista de destinos do FireEye

O log de auditoria Admin inclui eventos do dispositivo FireEye enquanto adiciona domínios à lista de destino. Um usuário chamado "FireEye Account", que também é marcado com o logotipo do FireEye, gera os eventos. Esses eventos incluem o domínio que foi adicionado e a hora em que ele foi adicionado.

Você pode filtrar para incluir apenas alterações do FireEye aplicando um filtro para o usuário da "Conta do FireEye".

Se a etapa "Testar fogo" tiver sido executada anteriormente, a adição do domínio de teste do

FireEye poderá aparecer no Registro de auditoria.

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 - <i>FireEye Threat Feed</i>

 **Changed domains - *FireEye Threat Feed***

- Added Domain
 - [fireeye-testevent.ts1385409551488.example.com](#)

Lidando com detecções indesejadas ou falsos positivos

Listas de permissão

Embora seja improvável, é possível que os domínios adicionados automaticamente pelo dispositivo FireEye possam disparar uma detecção indesejada que bloqueie o acesso de usuários a sites específicos. Em uma situação como essa, a Umbrella recomenda adicionar o(s) domínio(s) a uma lista de permissão (Políticas > Listas de Destino), que tem precedência sobre todos os outros tipos de listas de bloqueio, incluindo as configurações de segurança.

Há duas razões pelas quais esta abordagem é preferível.

- Primeiro, caso o dispositivo FireEye fosse readicionar o domínio após sua remoção, a lista de permissões protegerá contra esse problema.
- Em segundo lugar, a lista de permissão mostra um registro histórico de domínios problemáticos que podem ser usados para computação forense ou relatórios de auditoria.

Por padrão, há uma Lista de Permissões Global que é aplicada a todas as políticas. Adicionar um domínio à Lista de Permissões Global resulta na permissão do domínio em todas as políticas.

Se a configuração de segurança do FireEye no modo de bloqueio for aplicada apenas a um subconjunto de suas identidades gerenciadas do Cisco Umbrella (por exemplo, ela só é aplicada a computadores e dispositivos móveis em roaming), você poderá criar uma lista de permissões específica para essas identidades ou políticas.

Para criar uma lista de permissões:

1. Navegue até Políticas > Destination Lists e selecione o ícone Add.
2. Selecione Permitir e adicione seu domínio à lista.
3. Selecione Salvar.

Depois que a lista de destino tiver sido salva, você poderá adicioná-la a uma política existente que abranja os clientes que foram afetados pelo bloqueio indesejado.

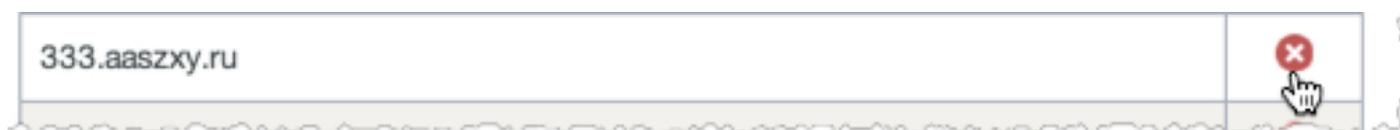
Excluindo domínios da lista de destinos do FireEye

Ao lado de cada nome de domínio na lista de destino do FireEye, há um ícone Delete. A exclusão de domínios permite que você limpe a lista de destinos do FireEye caso ocorra uma detecção indesejada.

No entanto, a exclusão não será permanente se o dispositivo FireEye reenviar o domínio para o Cisco Umbrella.

Para excluir um domínio:

1. Navegue até Configurações > Integrações e selecione "FireEye" para expandi-lo.
2. Selecione Ver Domínios.
3. Procure o nome de domínio que deseja deletar.
4. Selecione o ícone Deletar.



5. Selecione Fechar.

6. Selecione Salvar.

No caso de uma detecção indesejada ou falso positivo, a Umbrella recomenda criar imediatamente uma lista de permissões no Cisco Umbrella e, em seguida, corrigir o falso positivo no dispositivo FireEye. Posteriormente, você poderá remover o domínio da lista de destinos do FireEye.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.