Integre o Umbrella com o FireEye

Contents

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

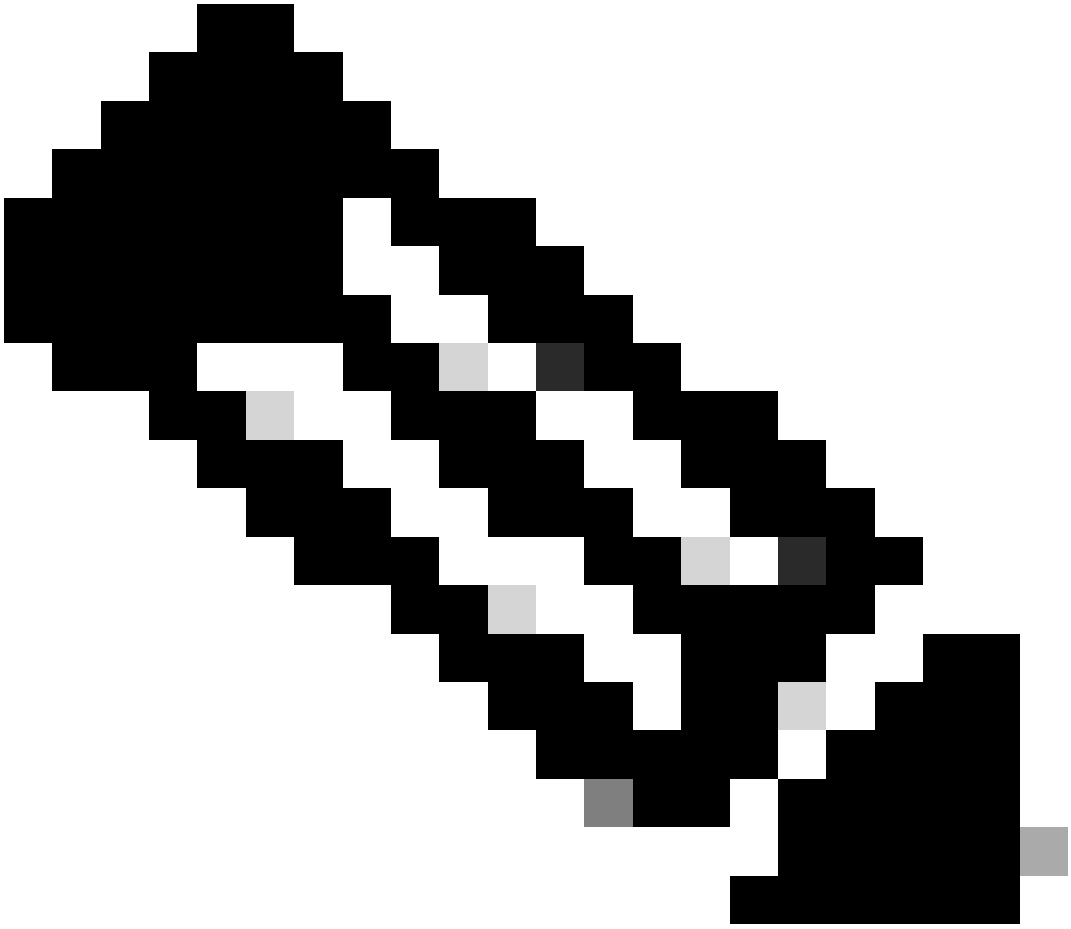
As informações neste documento são baseadas no Cisco Umbrella.

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

---

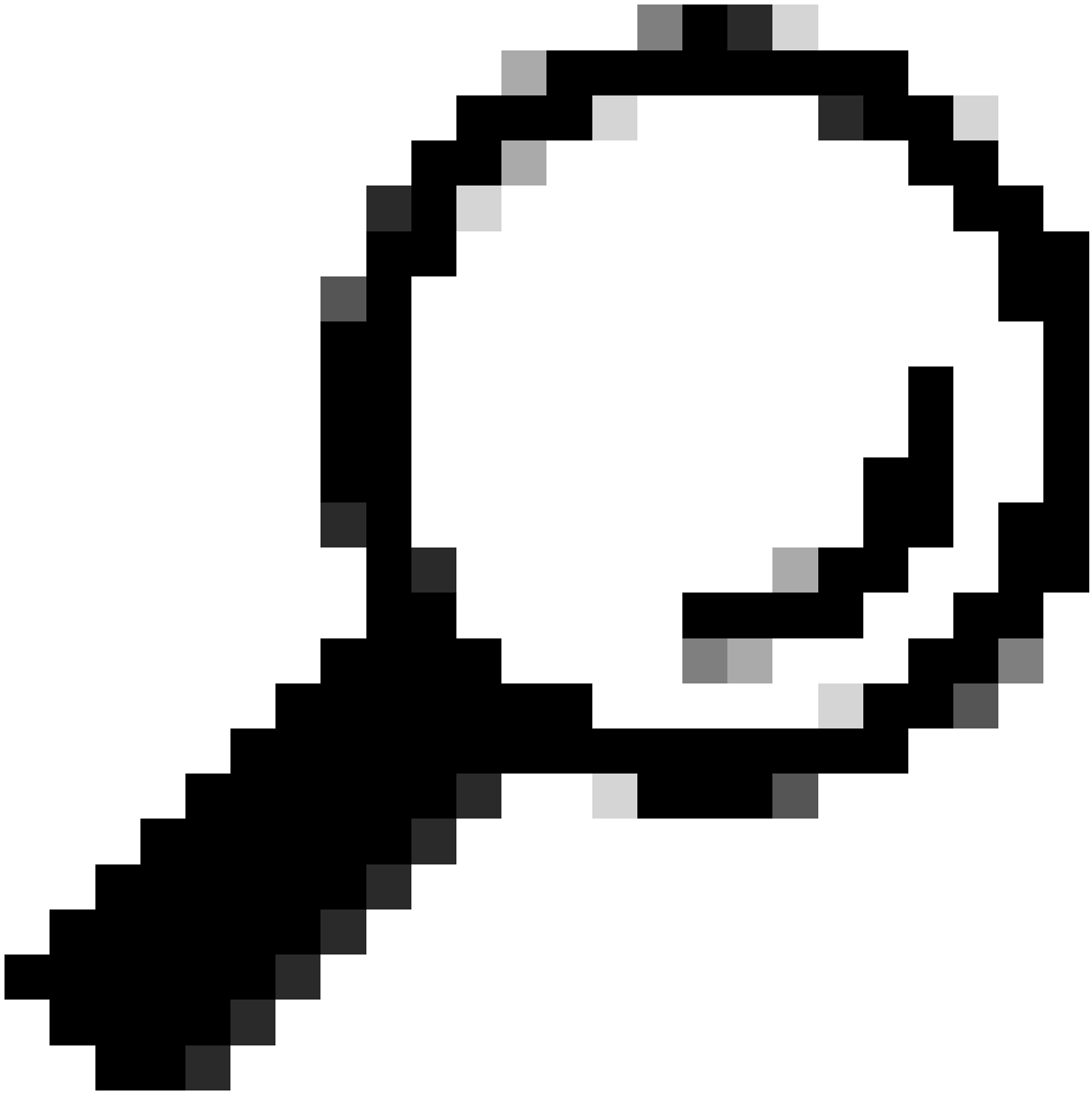
DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage. Se você não tiver um desses pacotes e quiser ter a integração com o FireEye, entre em contato com o seu Cisco Umbrella Account Manager. Se você tiver o pacote Cisco Umbrella correto, mas não vir o FireEye como uma integração para seu painel,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

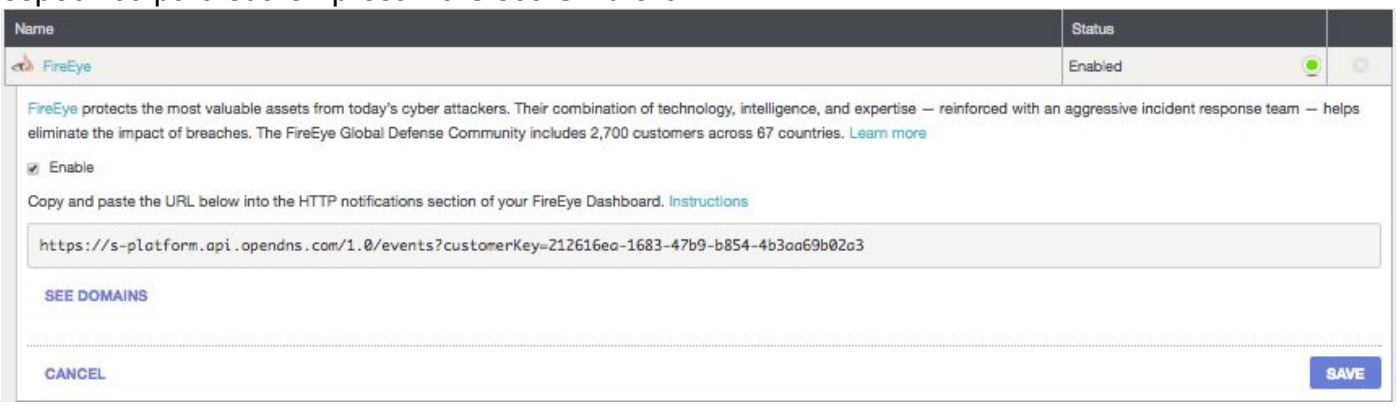
Configurando seu painel do Cisco Umbrella para receber informações do FireEye

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 Policies > 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.

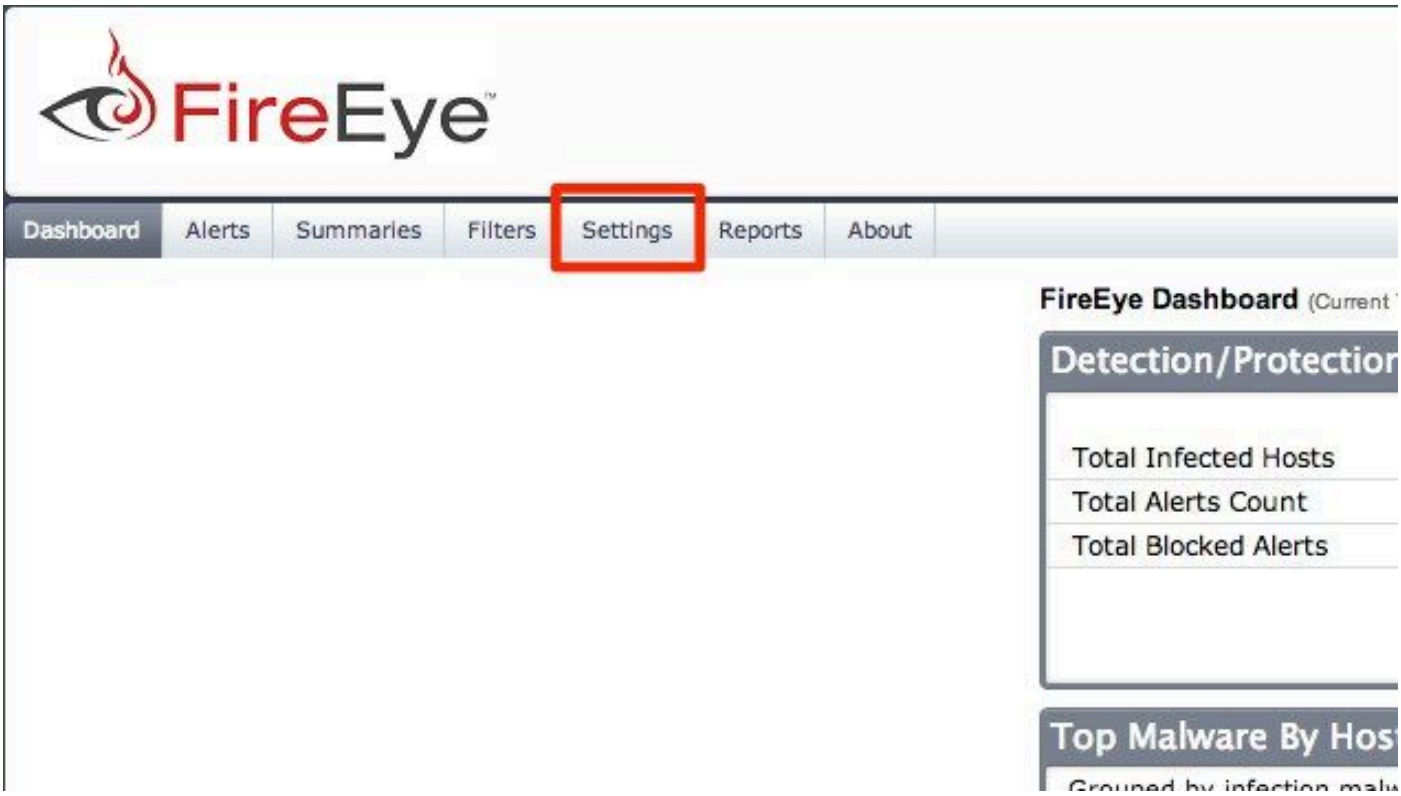


Você pode usar esse URL posteriormente para configurar o dispositivo FireEye para enviar dados ao Cisco Umbrella, portanto, copie o URL.

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.

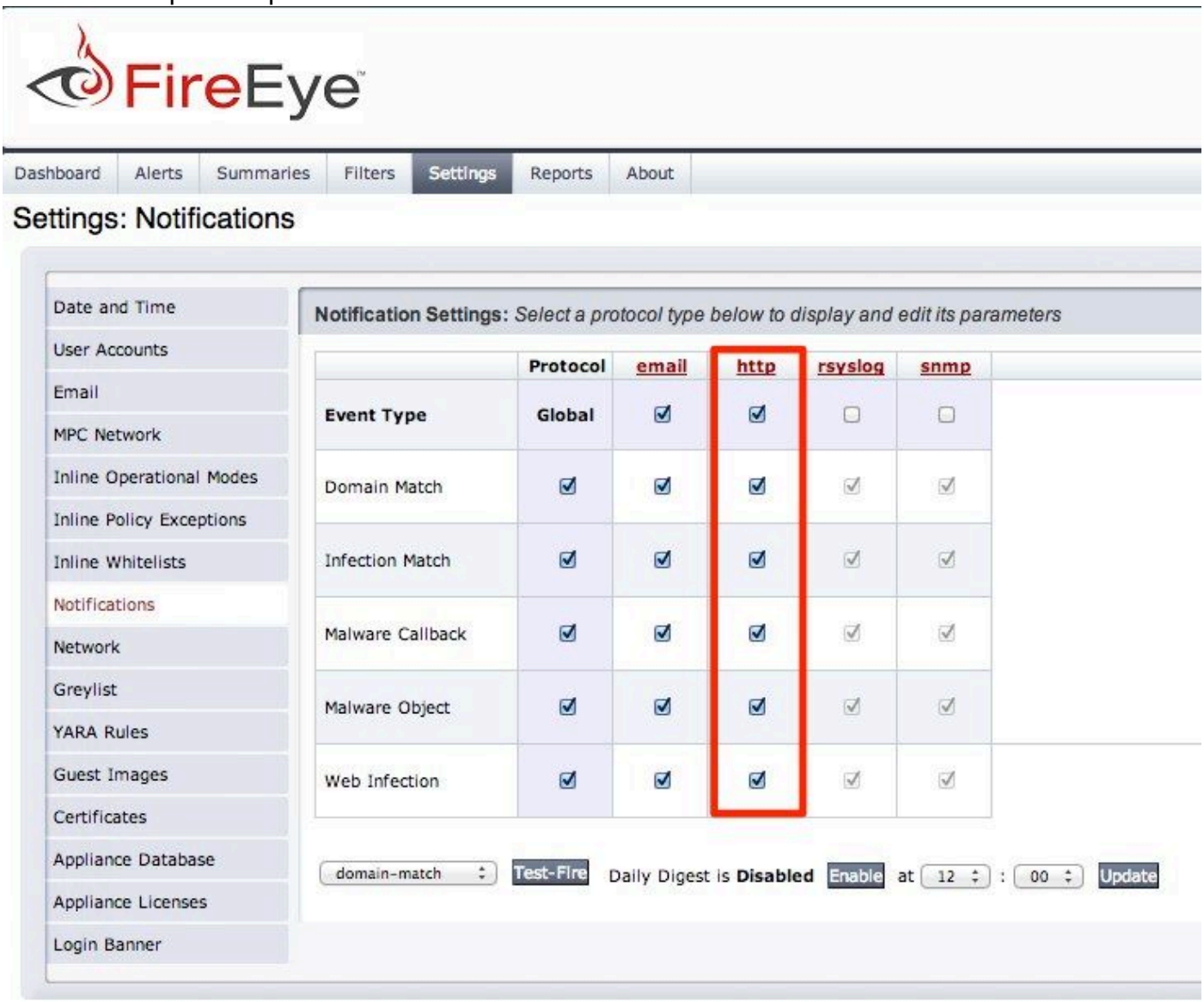
1. Faça login no FireEye e selecione Settings.



2. Selecione Notificações na lista de configurações:

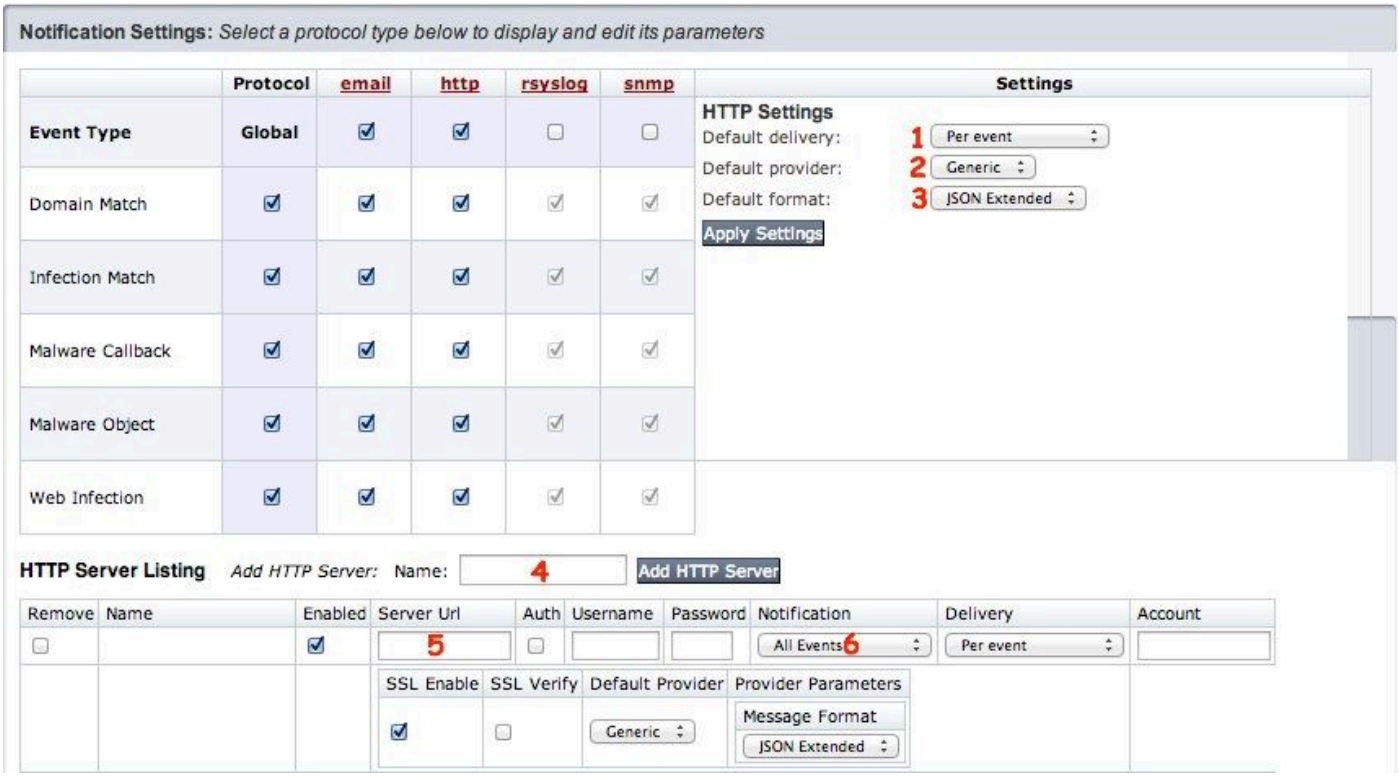

FireEye
Dashboard
Alerts
Summaries
Filters
Settings
Reports
About
Settings: Date and Time
Date and Time
User Accounts
Email
MPC Network
Inline Operational Modes
Inline Policy Exceptions
Inline Whitelists
Notifications
Network
Greylist
YARA Rules
Guest Images
Certificates
Appliance Database
Appliance 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. 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.



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.



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:

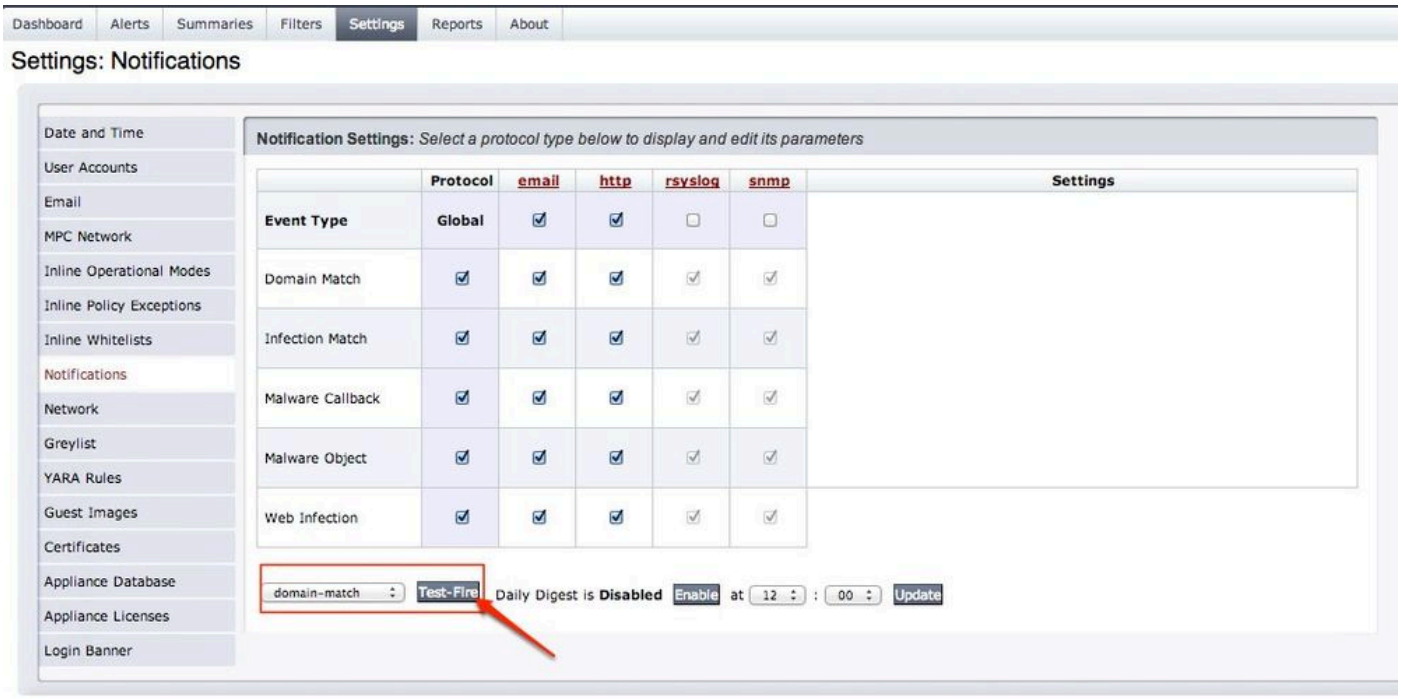
- Entrega: Base por evento
- Provedor padrão: GENÉRICO
- Parâmetros do provedor: Formato de mensagem estendido JSON
- (Opcional) Se você preferir enviar tráfego por SSL, selecione SSL Enable.

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:

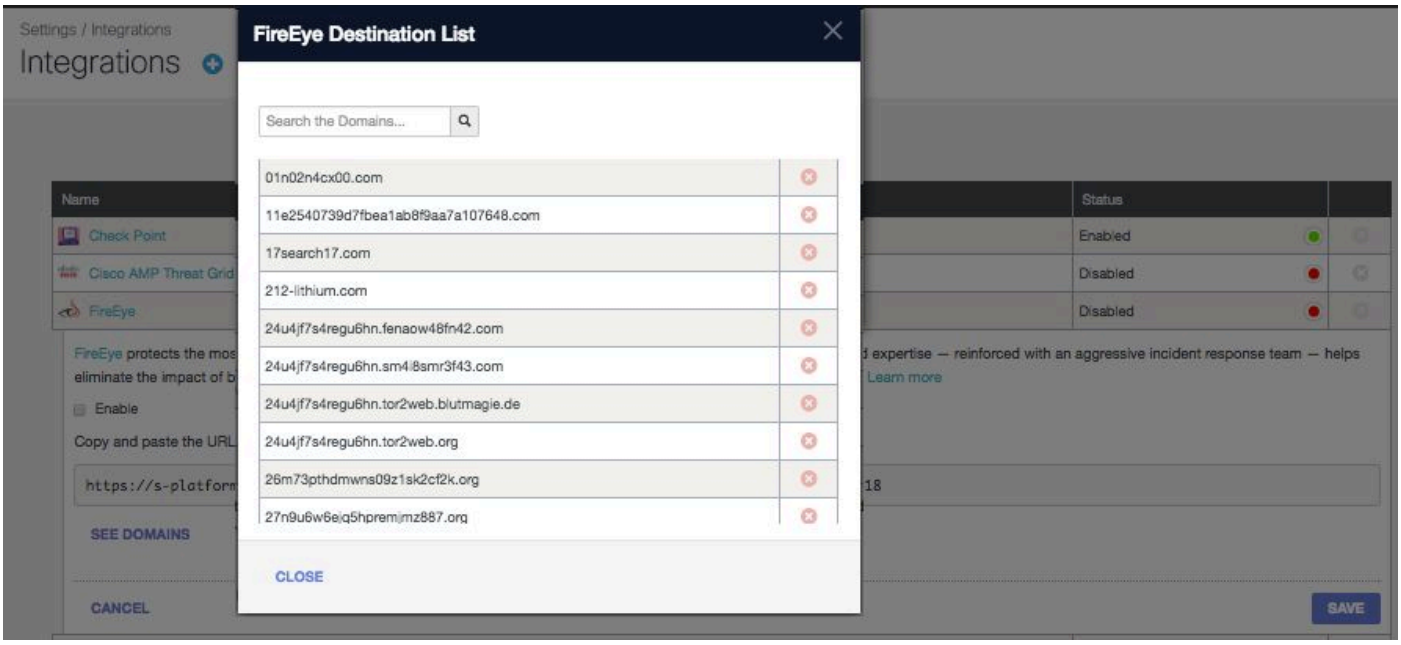
1. No FireEye, selecione domain-match no menu suspenso Test Fire e selecione Test Fire:



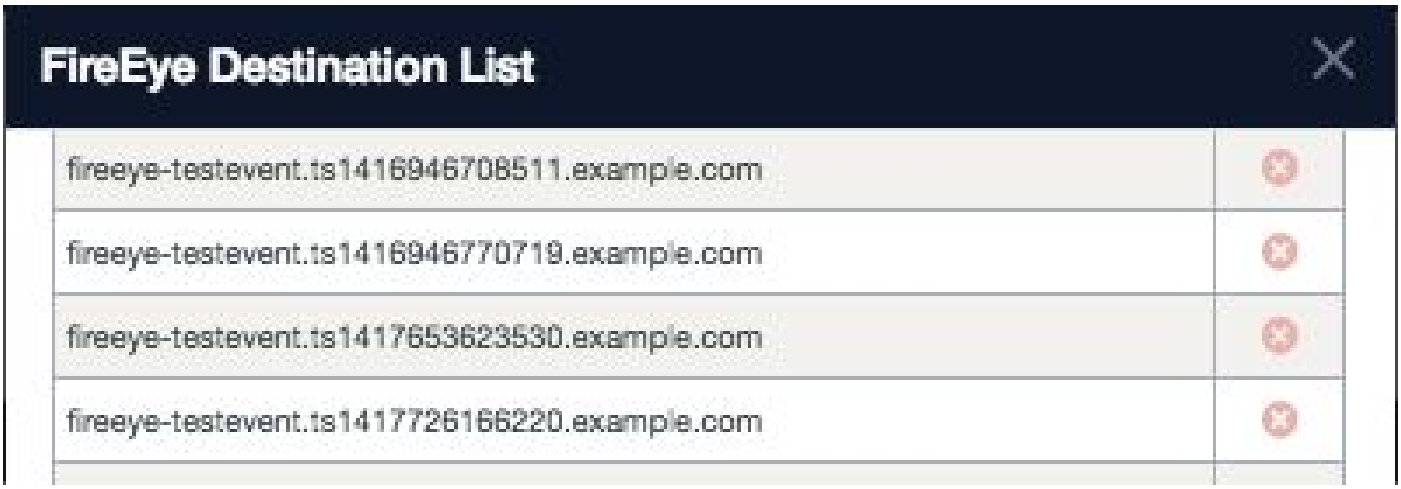
No Cisco Umbrella, a integração do FireEye inclui uma lista de domínios fornecidos pelo dispositivo FireEye para ver quais domínios estão sendo adicionados ativamente.

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.



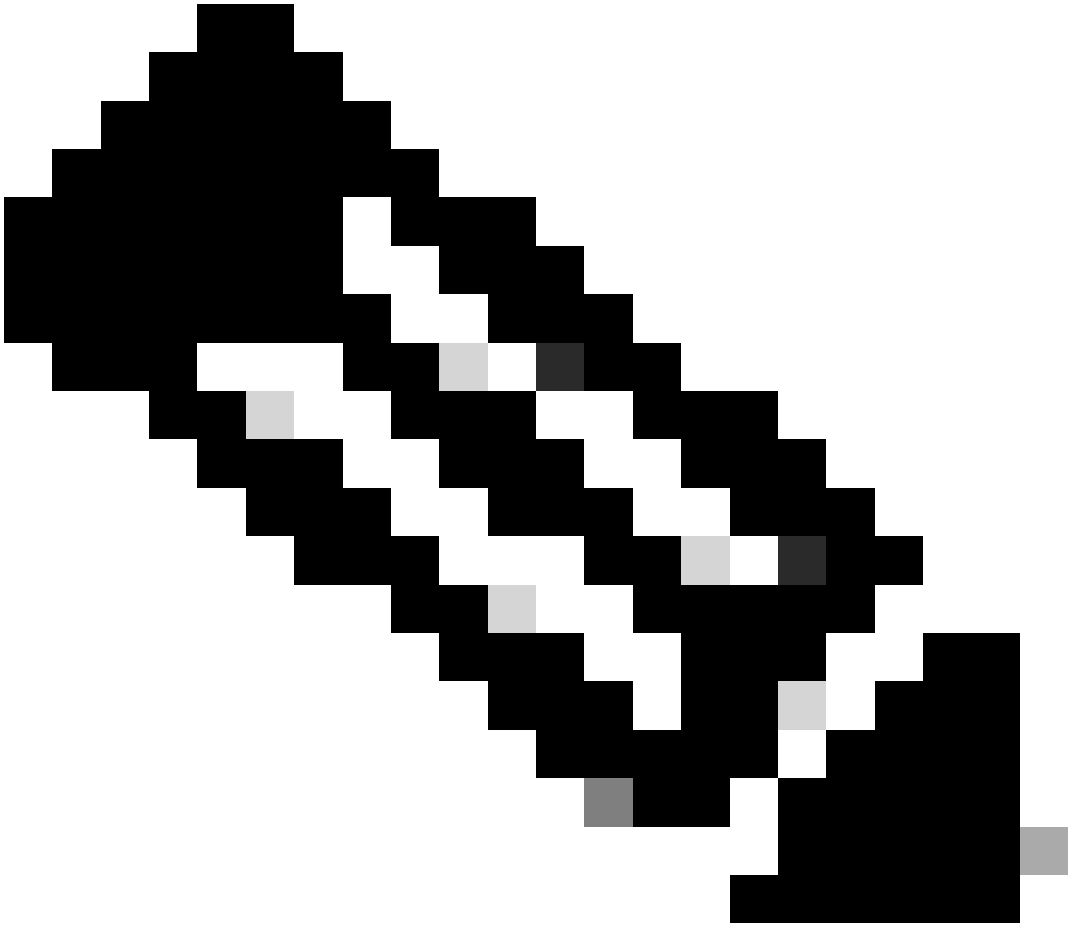
Selecionar Test Fire gera um domínio na lista de destinos do FireEye chamado "fireeye-testevent.example.com-[date]". Cada vez que você seleciona Test Fire no FireEye, ele cria um domínio exclusivo com a data no UNIX Epoch time anexada ao teste, para que os testes futuros possam ter um nome de domínio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



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.



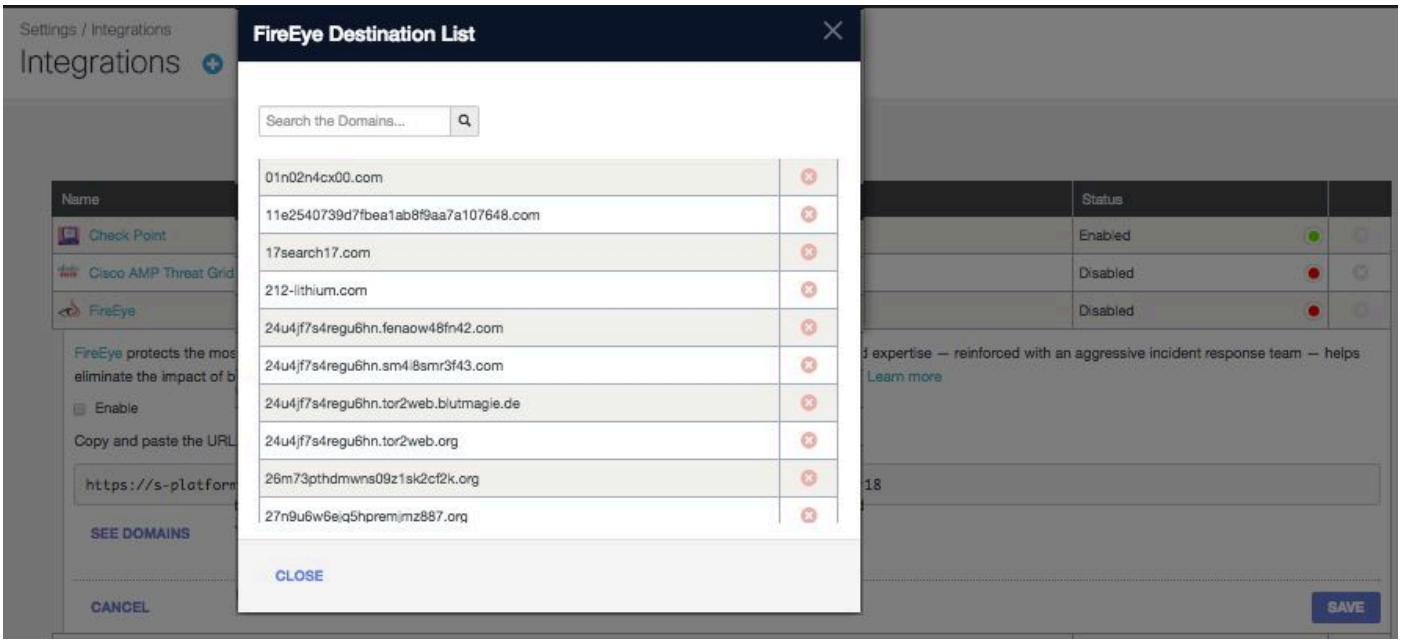
Note: O "modo de auditoria" pode ser ativado por quanto tempo for necessário, com base no perfil de implantação e na configuração da rede.

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.

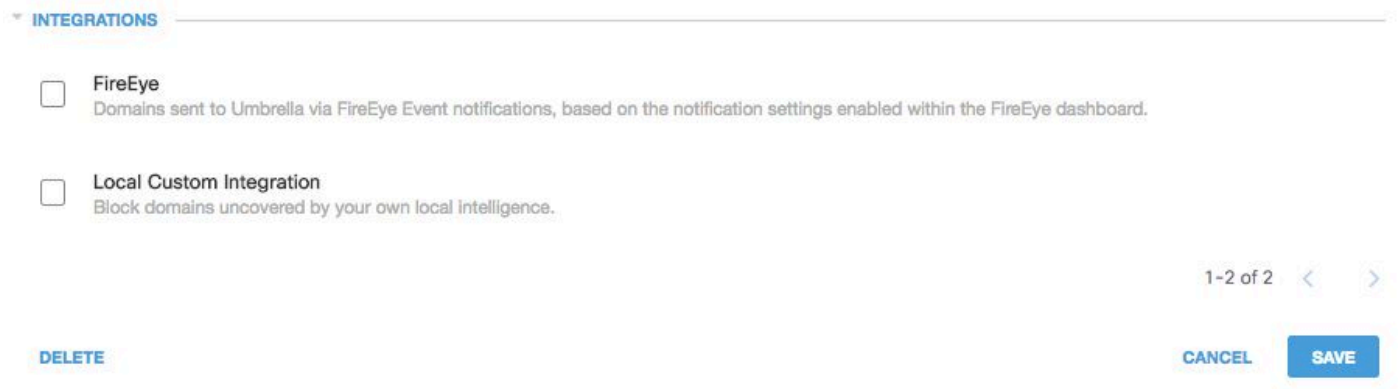


Revisar Configurações de Segurança para uma Política

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

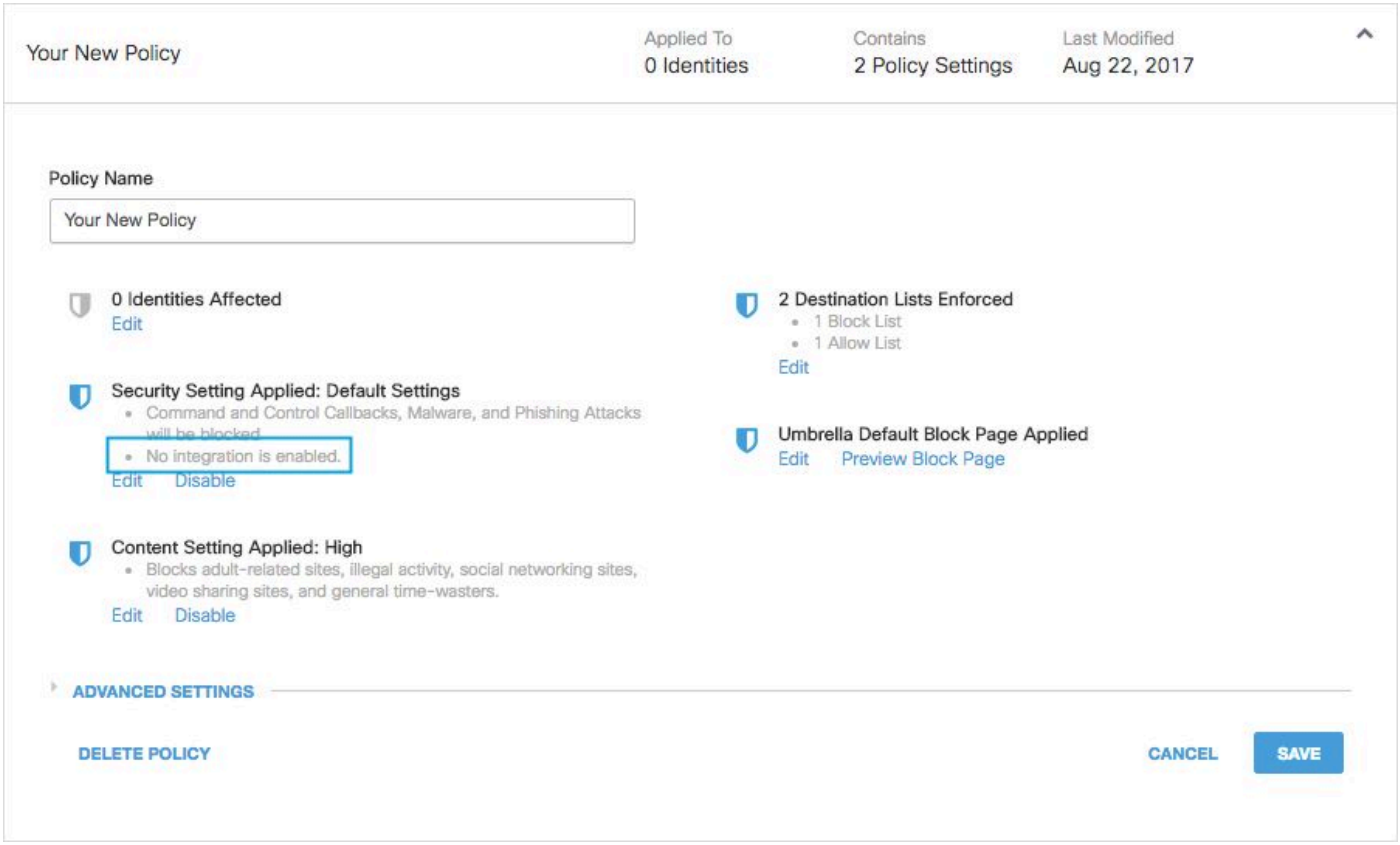
1. Navegue até Policies > Policy Components > Security Settings.

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.



115013920526

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

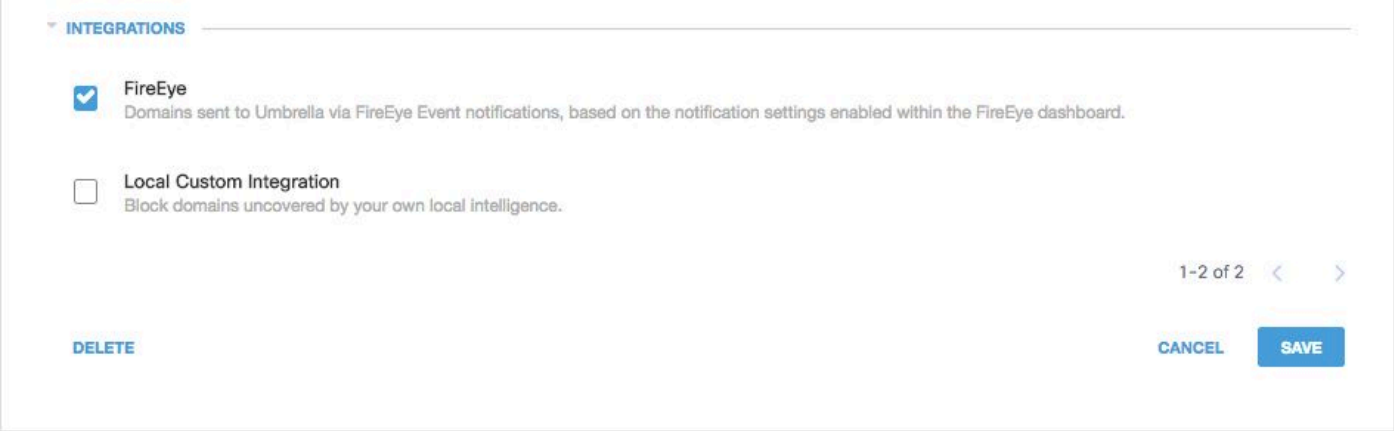
Aplicação das configurações de segurança do FireEye no "modo de bloqueio" a uma política para clientes gerenciados

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.



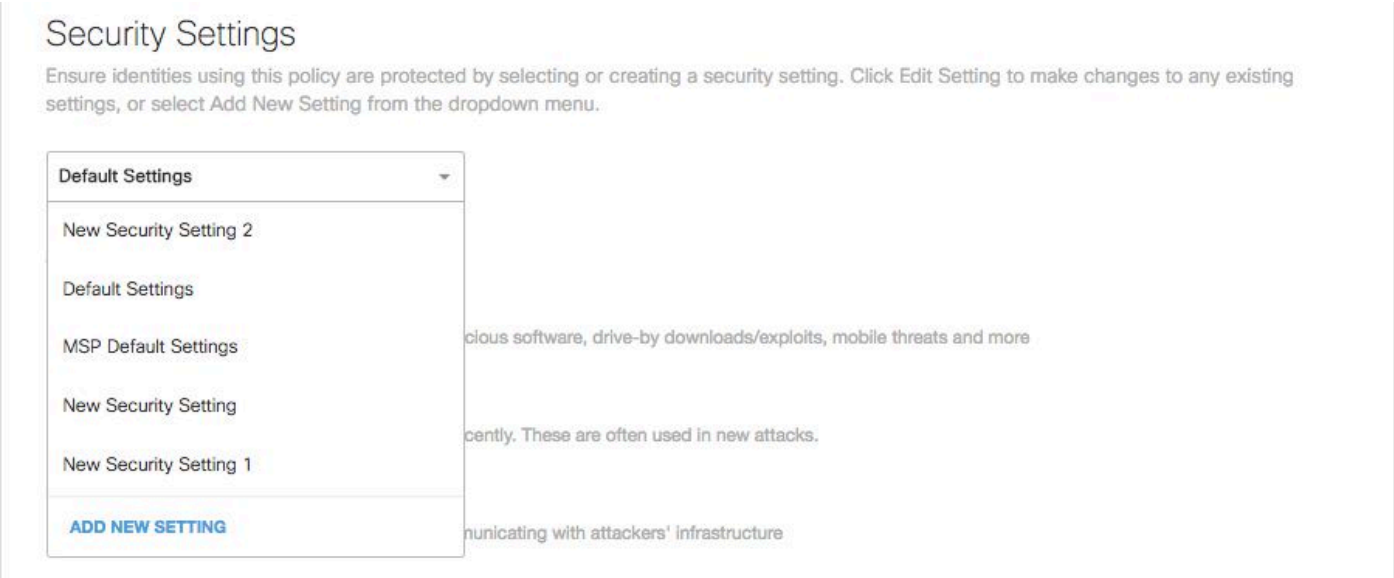
115013921406

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

1. Navegue até Policies > Policy List.

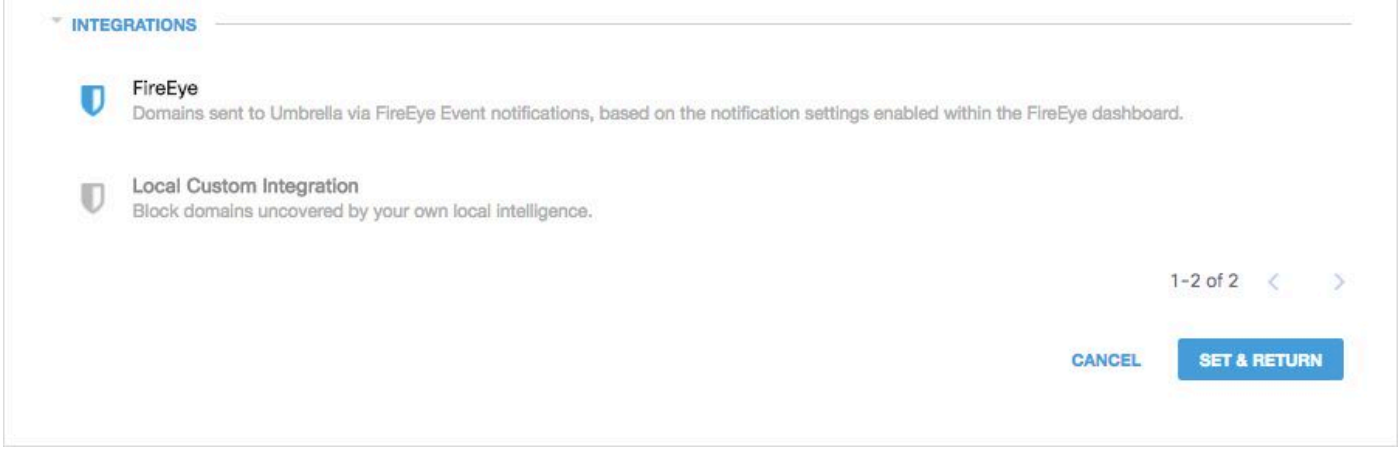
2. Expanda uma política e, em Configuração de segurança aplicada e selecione Editar.

3. No menu suspenso Configurações de segurança, selecione uma configuração de segurança que inclua a configuração FireEye.



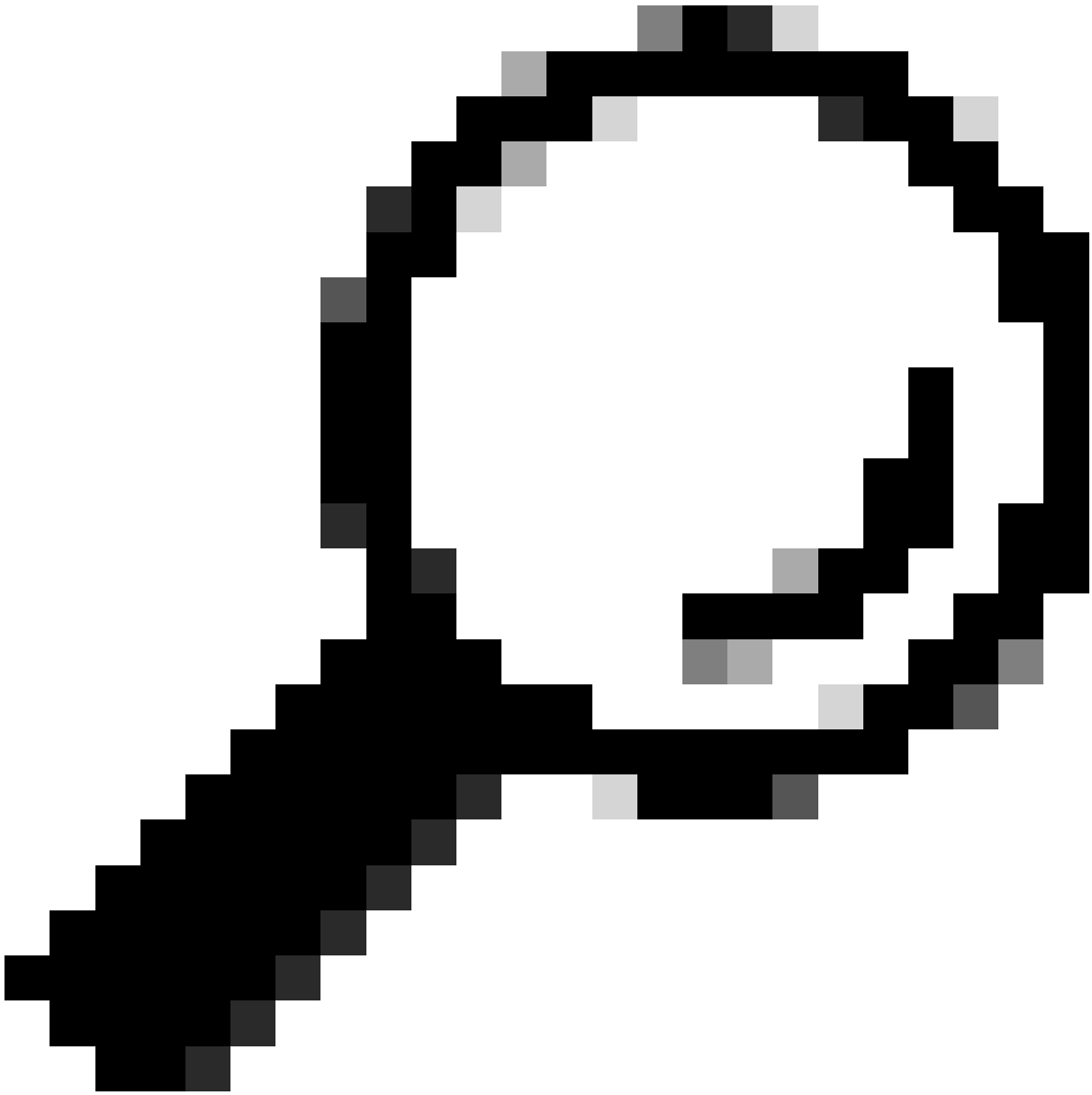
115014083083

O ícone de escudo em Integrações é atualizado para azul.



115013922146

4. Selecione 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.

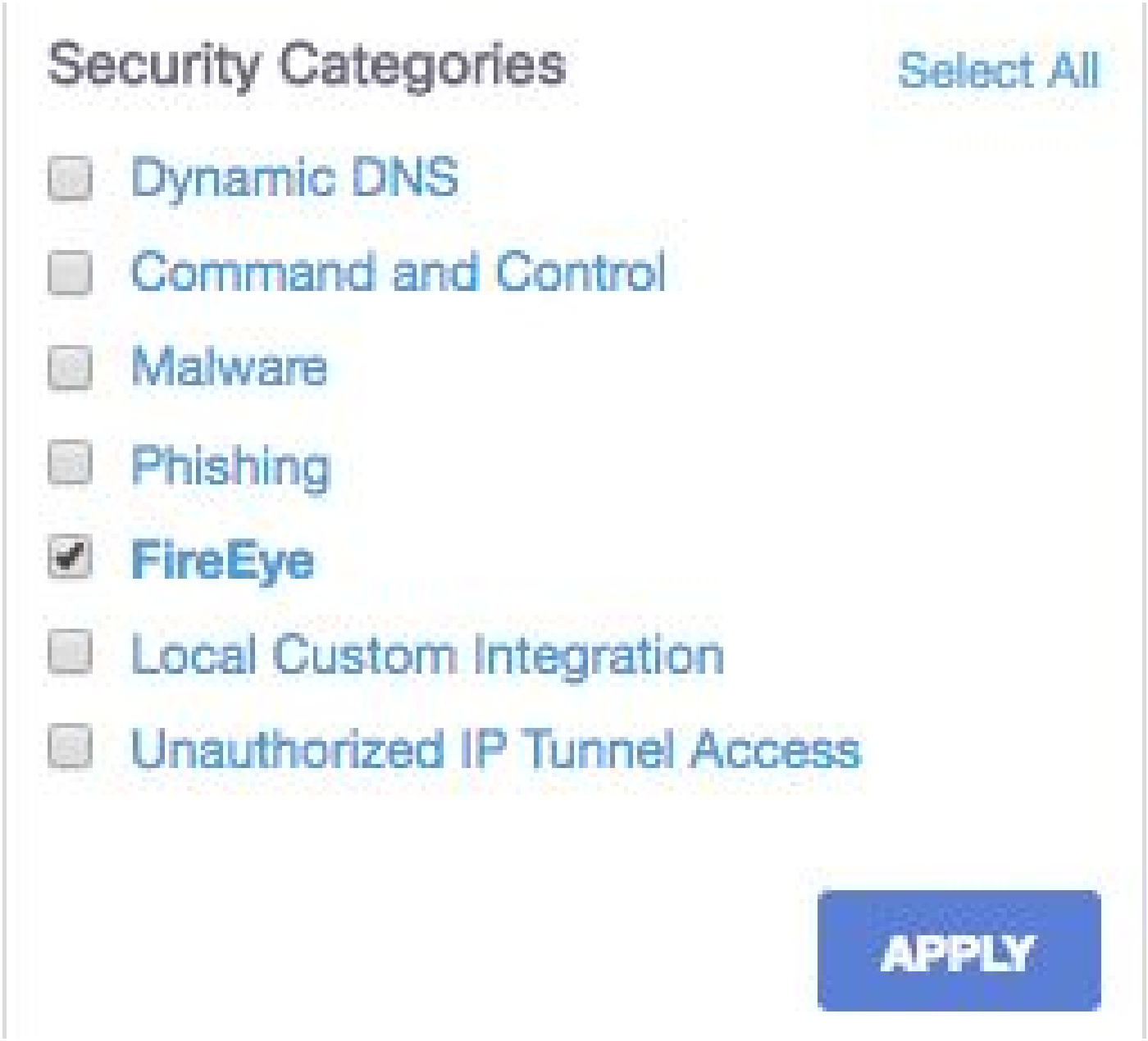
Relatórios dentro do Cisco Umbrella para eventos FireEye

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.



115013924986

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

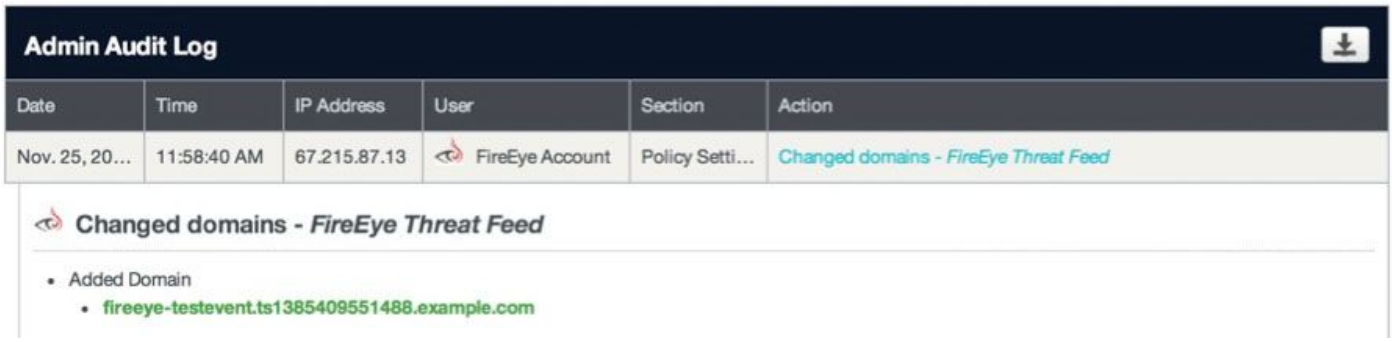
Relatórios sobre quando os domínios foram adicionados à lista de destinos do FireEye

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.



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 Policies > 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.