Configuración de la integración de Secure Malware Analytics (antes Threat Grid) con Umbrella

Contenido

Introducción

Este documento describe cómo integrar Secure Malware Analytics (anteriormente Threat Grid) con Umbrella.

Descripción general de Cisco Secure Malware Analytics (Threat Grid) Integration para Cisco Umbrella

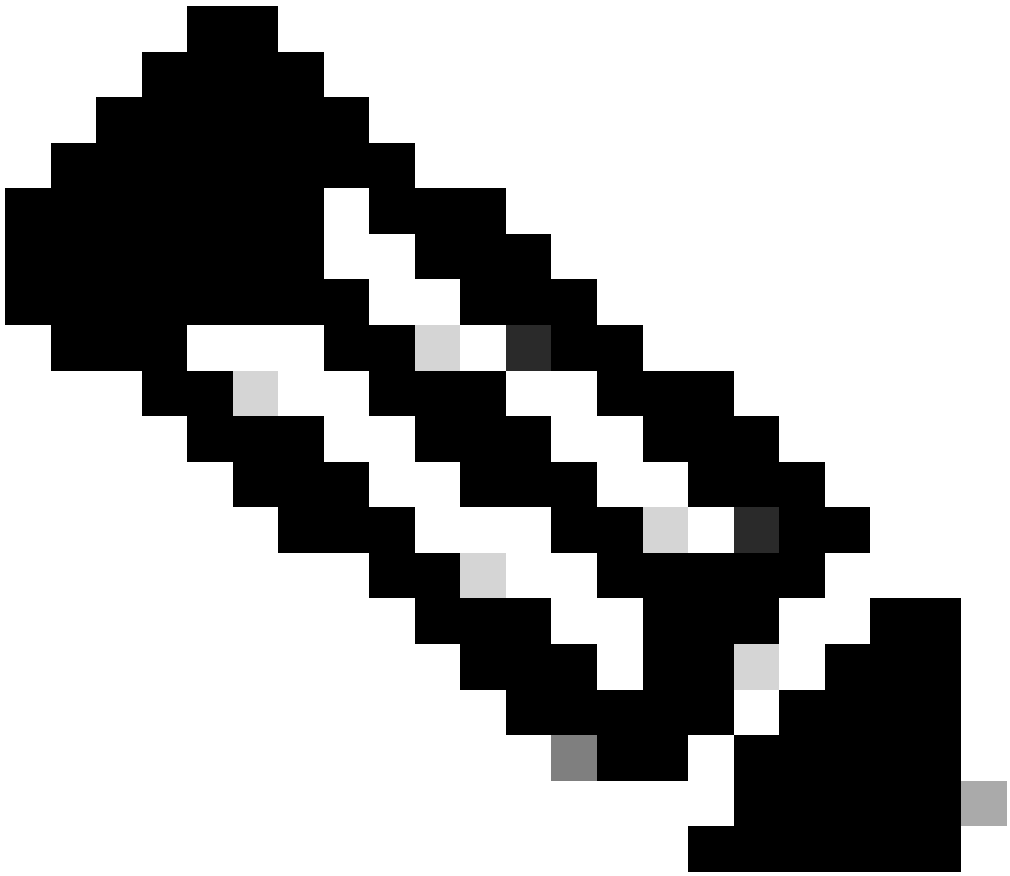
Gracias a la integración entre Cisco Secure Malware Analytics (anteriormente Threat Grid) y Cisco Umbrella, los equipos de seguridad ahora pueden ampliar su visibilidad y aplicar la protección frente a las amenazas avanzadas actuales en portátiles, tablets o teléfonos móviles, a la vez que proporcionan otro nivel de aplicación a una red corporativa distribuida.

Esta guía describe cómo configurar Cisco Secure Malware Analytics (Threat Grid) para

comunicarse con Cisco Umbrella, de modo que la inteligencia de amenazas generada por Cisco Secure Malware Analytics (Threat Grid) se pueda integrar automáticamente en políticas que puedan proteger a los clientes bajo Cisco Umbrella.

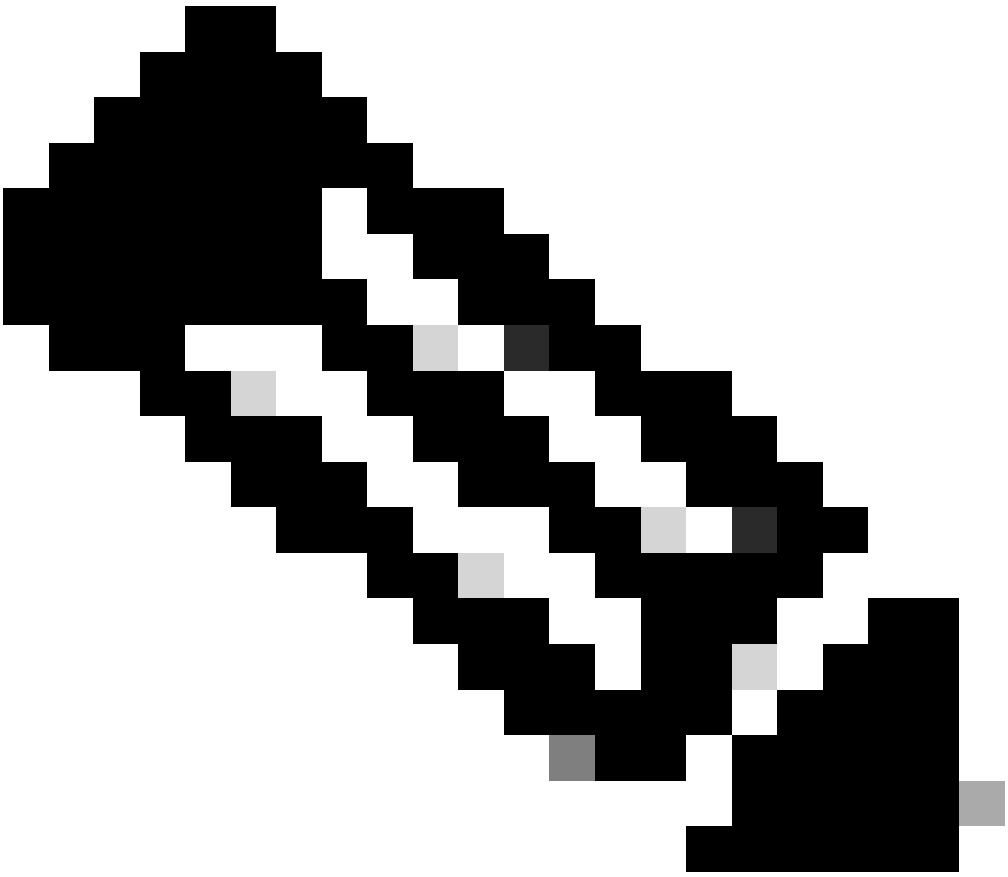
Prerequisites

- Un panel funcional de Cisco Secure Malware Analytics (Threat Grid) con acceso a la clave de la API de su cuenta.



Nota: Los dispositivos y terminales de Cisco Secure Malware Analytics (Threat Grid) no son compatibles en este momento.

- Derechos administrativos de Cisco Umbrella Dashboard.
- El panel de Cisco Umbrella debe tener habilitada la integración de Cisco Secure Malware Analytics (Threat Grid).



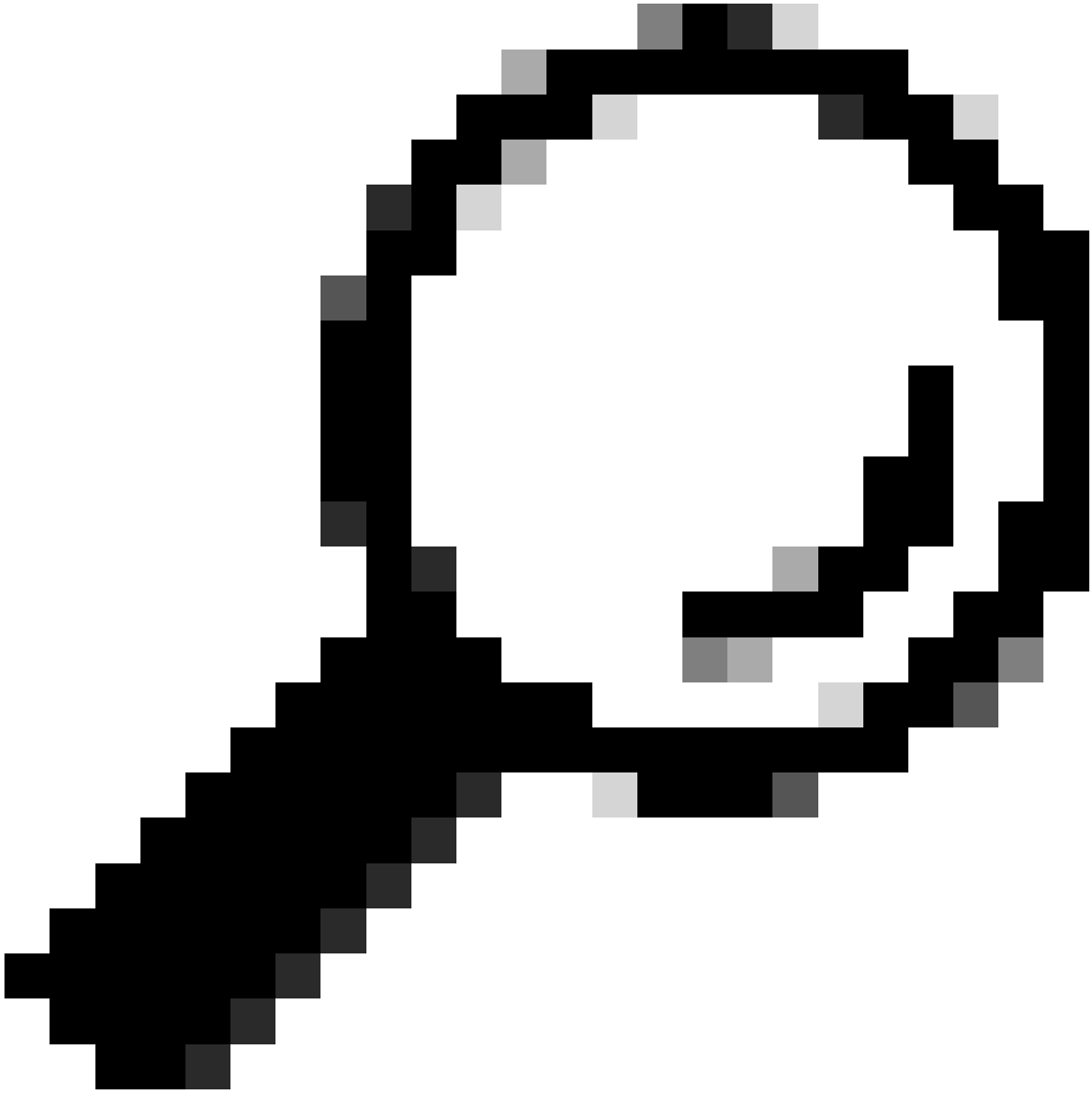
Nota: La integración de Cisco Secure Malware Analytics (Threat Grid) solo se incluye en paquetes de Cisco Umbrella como DNS Essentials, DNS Advantage, SIG Essentials o SIG Advantage. Si no tiene un paquete de Cisco Umbrella y le gustaría tener esta integración, póngase en contacto con su Cisco Umbrella Account Manager. Si tiene un paquete de Cisco Umbrella pero no ve Cisco Secure Malware Analytics (Threat Grid) como una integración para su panel, póngase en contacto con el servicio de asistencia de Cisco Umbrella.

¿Cómo funciona esta integración?

Cisco Umbrella se pone en contacto con la API Cisco Secure Malware Analytics (Threat Grid) y recupera listas de dominios que se generan a partir del análisis de muestras malintencionadas. Cisco Umbrella importa esta lista a través de la API de Cisco Umbrella Enforcement. Este enfoque es diferente de cómo funcionan otras integraciones en las que Cisco Umbrella aprovecha la inteligencia de amenazas realizando consultas de API a la API de Cisco Secure Malware Analytics (Threat Grid), en lugar de aceptar incidentes de otros sistemas que llevan la inteligencia de amenazas al servicio Cisco Umbrella.

A continuación, Cisco Umbrella valida la amenaza para garantizar que se pueda agregar a su política. Si se confirma que la información de Cisco Secure Malware Analytics (Threat Grid) es una amenaza o que no es un dominio de funcionalidad comprobada, la dirección del dominio se agrega a la lista de destino de Cisco Secure Malware Analytics (Threat Grid) como parte de una configuración de seguridad que se puede aplicar a cualquier política de Cisco Umbrella. Esta política se aplica inmediatamente a cualquier solicitud que se realice desde dispositivos que utilicen políticas que aprovechen la integración de Cisco Secure Malware Analytics (Threat Grid).

Cisco Umbrella obtiene dos fuentes independientes de Cisco Secure Malware Analytics (Threat Grid): una fuente Public (global) y una fuente Customer Only (private, específica de un único cliente).



Consejo: Aunque Cisco Umbrella hace todo lo posible por validar y permitir dominios que se sabe que son seguros en general (por ejemplo, Google y Salesforce), para evitar

---

interrupciones no deseadas, le sugerimos que agregue dominios que nunca desee bloquear a la Lista global de permitidos u otras listas de destinos según su política.

Entre los ejemplos, se encuentran los siguientes:

- La página de inicio de su organización.
- Dominios que representan servicios proporcionados que pueden tener registros internos y externos. Por ejemplo, "mail.myservicedomain.com" y "portal.myotherservicedomain.com".
- Aplicaciones en la nube menos conocidas de las que depende en gran medida que Cisco Umbrella no conozca o no incluya en su validación automática de dominio. Por ejemplo, "localcloudservice.com".

Estos dominios deben agregarse a la Lista global de permitidos, que se encuentra en Políticas > Listas de destino en Cisco Umbrella.

Configuración de Cisco Umbrella Dashboard para obtener información de Cisco Secure Malware Analytics (Threat Grid)

El primer paso consiste en buscar o generar la clave de la API en el panel de análisis de malware seguro de Cisco (Threat Grid):

1. Inicie sesión en el panel de Cisco Secure Malware Analytics (Threat Grid) y seleccione los detalles de su cuenta.
2. En Detalles de cuenta, es posible que ya esté visible una clave de API si ya ha creado una. Si no lo ha hecho, seleccione "Generar nueva clave de API".

   Su clave de API está visible en Detalles del usuario > Clave de API.

A continuación, agregue la clave de la API a Cisco Umbrella Dashboard para que pueda extraer datos de Cisco Secure Malware Analytics (Threat Grid):

1. Inicie sesión en el panel de Cisco Umbrella como administrador.
2. , vaya a Políticas > Componentes de política > Integraciones y seleccione "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) en la tabla para ampliarla.
3. Seleccione Enable, pegue su API Key en el cuadro API Key y, a continuación, seleccione Save.

En este momento, si recibe un error, es probable que exista un problema con la clave de la API o las comunicaciones entre los servicios. Compruebe la clave de la API e inténtelo de nuevo. Si sigue fallando, póngase en contacto con el servicio de asistencia de Cisco Umbrella.

Si recibe un mensaje de confirmación, indica que el servicio Cisco Umbrella ha podido utilizar la clave de la API para establecer una conexión inicial con la API de Cisco Secure Malware Analytics (Threat Grid). El servicio Cisco Umbrella utiliza un intervalo de sondeo de cinco minutos para recuperar datos de Cisco Secure Malware Analytics (Threat Grid).

Incluso después del intervalo de cinco minutos, si no hay datos válidos o eventos de amenaza válidos disponibles para ser extraídos por Cisco Umbrella Dashboard, es posible que la información no aparezca. Cuando la integración se habilita por primera vez, solo comienza retrocediendo cinco minutos tanto para la fuente global como para la fuente de solo organización y la primera vez que obtiene datos es en el siguiente intervalo de cinco minutos, por lo que es posible que los datos no aparezcan inmediatamente.

Si se desactivara o eliminara la clave de la API en el lado de Cisco Secure Malware Analytics (Threat Grid), la integración se desactivaría. Para restaurar la integración, se debe proporcionar una nueva clave de API en el panel de Cisco Umbrella. Si se produce un error de tiempo de espera o de servicio interno entre Cisco Umbrella y Cisco Secure Malware Analytics (Threat Grid), se genera un tipo de excepción diferente y la integración no se deshabilita; en su lugar, las conexiones se siguen intentando cada cinco minutos, como en condiciones normales.

Detalles técnicos

A continuación se enumeran las consultas de API exactas que se utilizan para obtener información de Cisco Secure Malware Analytics (Threat Grid). Tenga en cuenta que sólo se recopilan eventos con una gravedad superior a 90, una confianza superior a 90 y del tipo Dominios. El tiempo en este ejemplo es un rango de cinco minutos que se incrementa para la siguiente consulta. La `api_key` proporcionada en Cisco Umbrella se utiliza en lugar de la variable `<key>`:

- Público (fuente global):

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- Solo cliente (fuente privada):

```
hxxps://panacea.threatgrid.com/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

or:

- Público (fuente global):

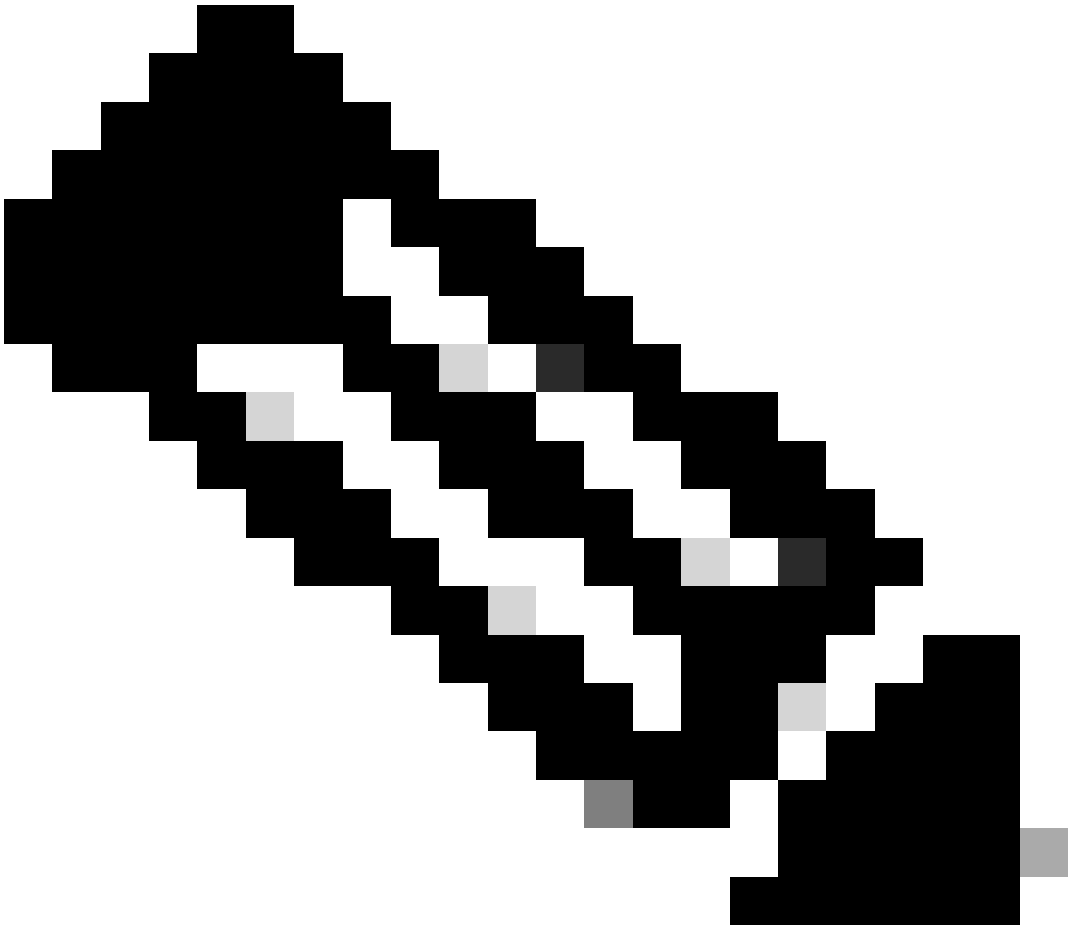
```
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
```

- Solo cliente (fuente privada):

```
hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence=
```

Observación de eventos agregados a Cisco Secure Malware Analytics (Threat Grid) en "modo auditoría"

Con el tiempo, los eventos de Cisco Secure Malware Analytics (Threat Grid) comienzan a rellenar una lista de destinos específicos que se pueden aplicar a políticas como la categoría Cisco Secure Malware Analytics (Threat Grid). De forma predeterminada, la lista de destino y la categoría de seguridad están en "modo auditoría" y no se aplican a ninguna política, por lo que no se bloquea ninguna solicitud. Sin embargo, puede ver qué solicitudes están asociadas (y podrían haberse bloqueado) a la categoría de seguridad de Cisco AMP Threat Grid.



Nota: El "modo auditoría" puede activarse el tiempo que sea necesario, o incluso de forma indefinida, en función del perfil de implementación y de la configuración de la red.

Revisar lista de destinos

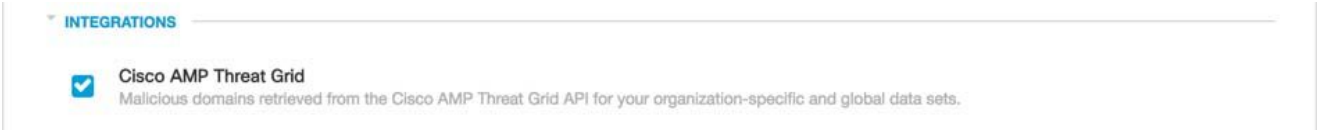
Puede consultar la lista de destinos de Cisco Secure Malware Analytics (Threat Grid) en cualquier momento.

1. Vaya a Políticas > Componentes de política > Integraciones.
2. Expanda "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) en la tabla y seleccione "Ver dominios".

Revisar la configuración de seguridad de una directiva

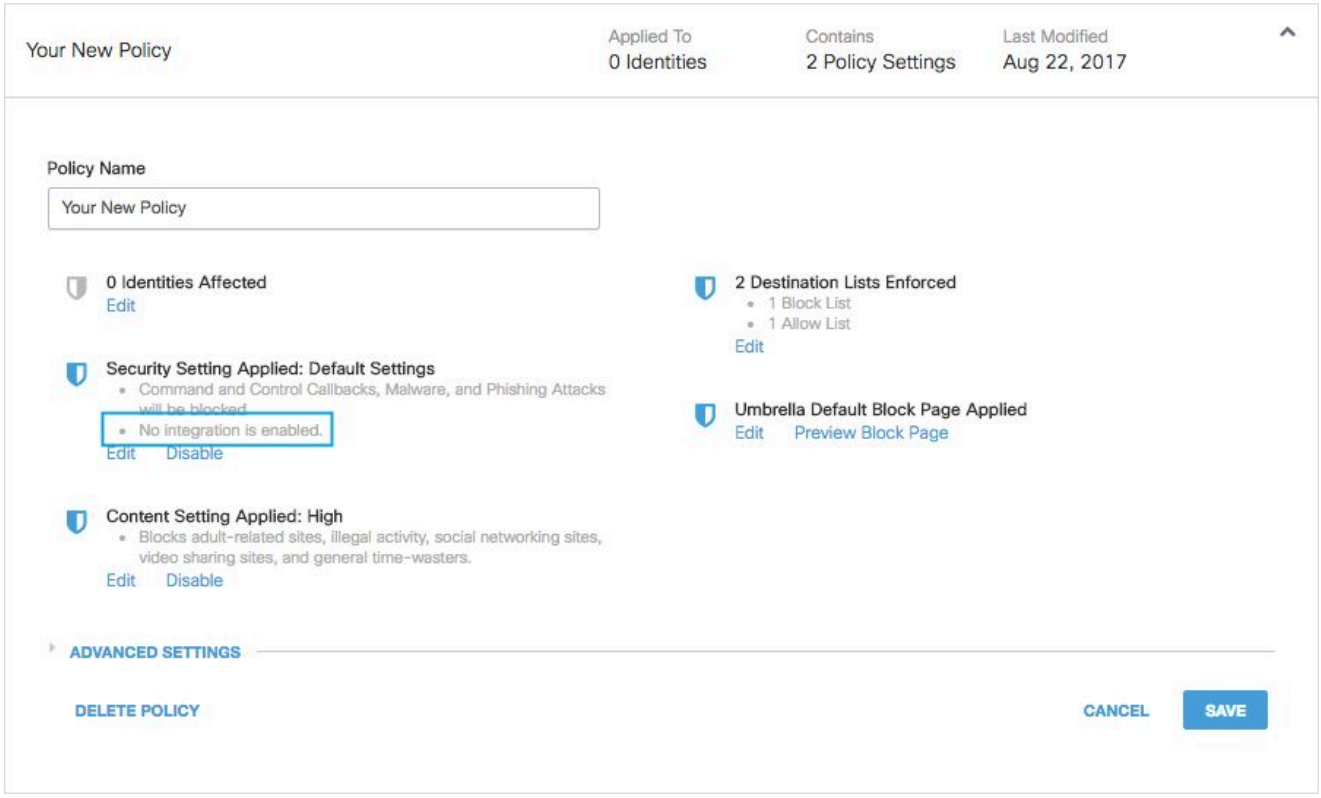
Puede revisar la configuración de seguridad que se puede habilitar para una política en cualquier momento en Cisco Umbrella:

1. Vaya a Políticas > Componentes de política > Configuración de seguridad.
2. Haga clic en una configuración de seguridad de la tabla para expandirla.
3. Desplácese hasta la sección Integraciones y expanda la sección para mostrar la integración de Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)).
4. Seleccione la casilla de la integración de Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)) y, a continuación, seleccione Guardar.

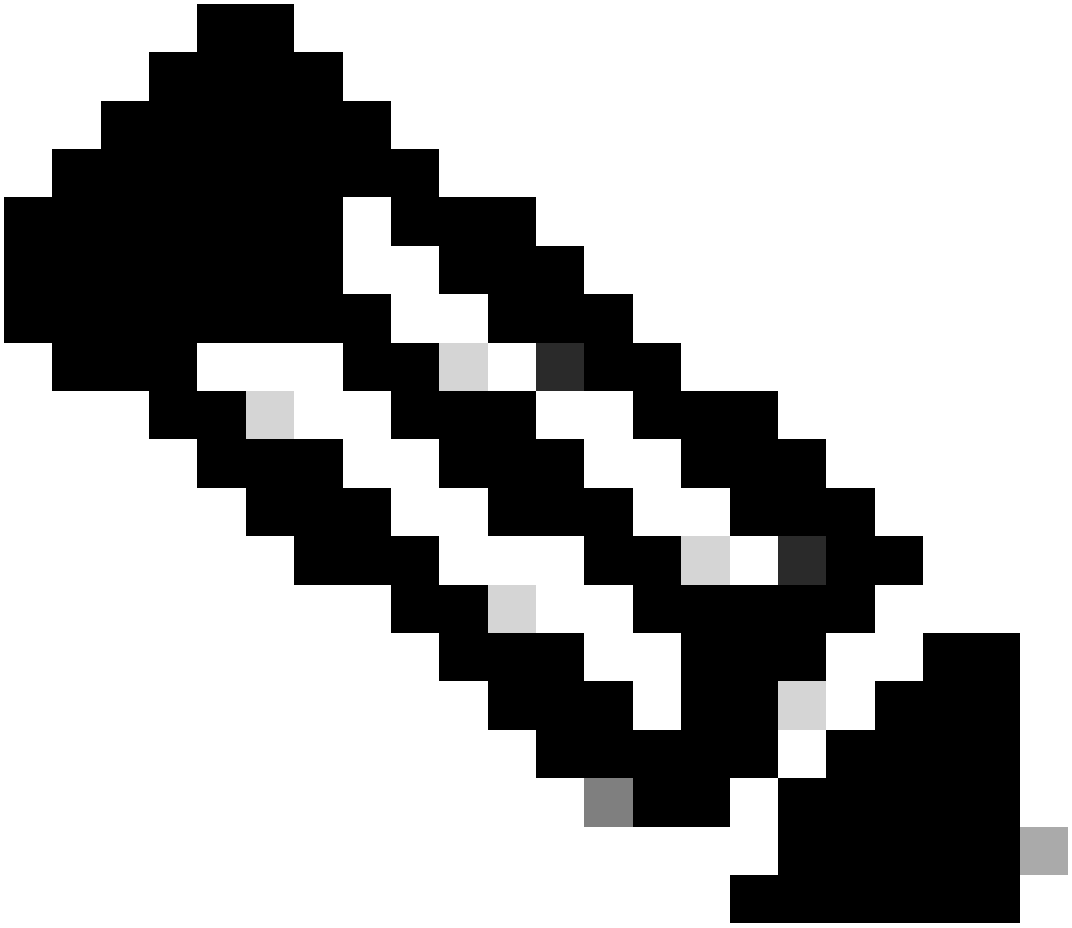


115014151543

También puede revisar la información de integración a través de la página Resumen de parámetros de seguridad.



20993269073556



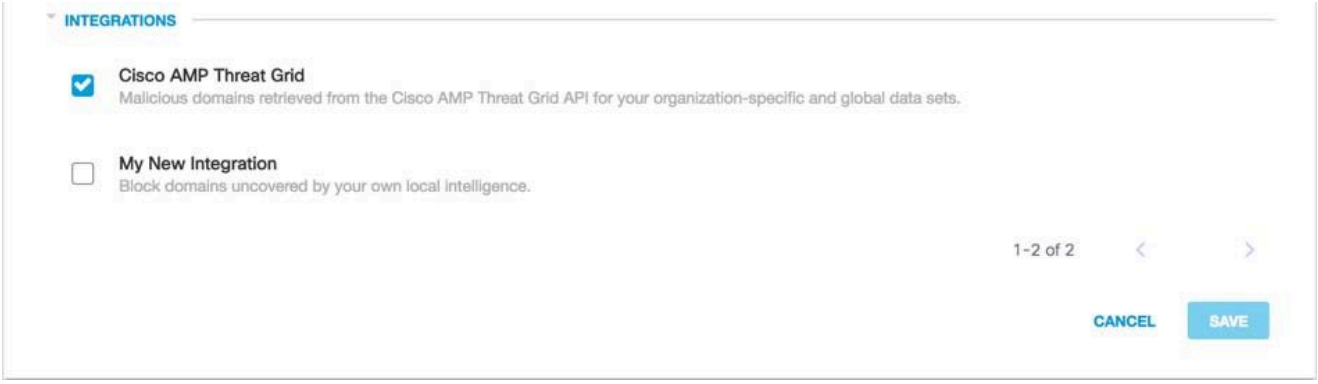
Nota: La aplicación de la configuración puede tardar hasta cinco minutos y, si no se introducen nuevos eventos en el sistema Cisco Secure Malware Analytics (Threat Grid), es posible que no vea cómo se agregan nuevos dominios a la integración.

Aplicación de la configuración de seguridad de Cisco Secure Malware Analytics (Threat Grid) en "modo de bloqueo" a una política para clientes gestionados

Una vez que esté listo para bloquear estos dominios para los clientes gestionados por Cisco Umbrella, cambie la configuración de seguridad de una política existente o cree una nueva política que se sitúe por encima de la política predeterminada para asegurarse de que se aplica en primer lugar.

1. Vaya a Políticas > Componentes de política > Configuración de seguridad.
2. En Integraciones, compruebe que el cuadro "Cisco AMP Threat Grid" está seleccionado. Si

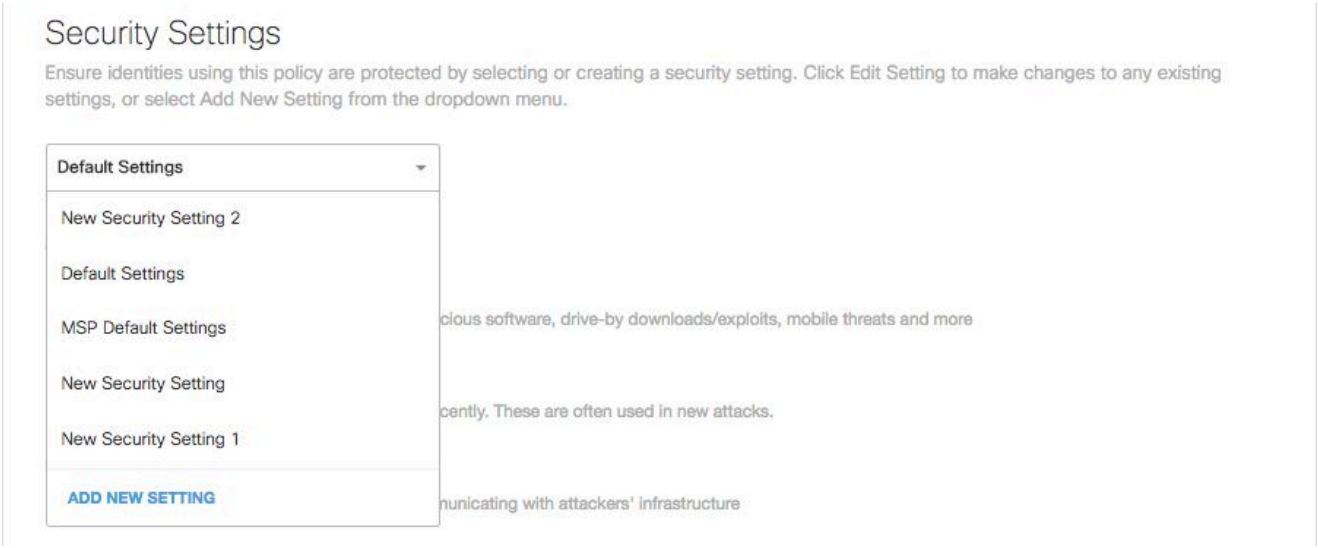
no es así, active la casilla y seleccione Guardar.



115013987086

A continuación, en el Asistente de directivas de Cisco Umbrella, agregue una configuración de seguridad a la directiva que está editando:

1. Vaya a Políticas > Administración > Todas las políticas.
2. Expanda una directiva y en Configuración de seguridad aplicada y, a continuación, seleccione Editar.
3. En el menú desplegable Security Settings, seleccione una configuración de seguridad que incluya la configuración "Cisco AMP Threat Grid".



20993282642708

El icono de escudo de Integraciones se actualiza a azul.

115013987446

4. Seleccione Set & Return.

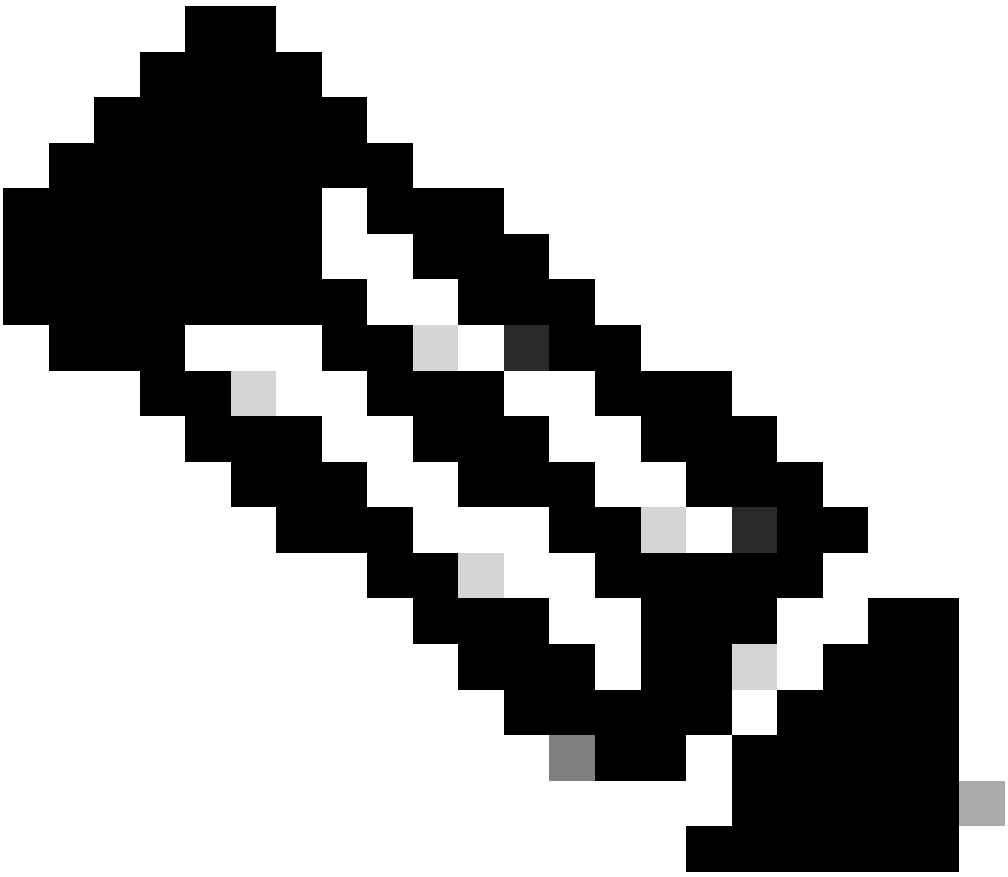
   Los dominios de Cisco Secure Malware Analytics (Threat Grid) incluidos en la configuración de seguridad de Cisco Secure Malware Analytics (Threat Grid) se bloquean para las identidades que utilizan la política.

Informes dentro de Cisco Umbrella para eventos de Cisco Secure Malware Analytics

Informes sobre eventos de seguridad de Cisco Secure Malware Analytics (Threat Grid)

La lista de destino de Cisco Secure Malware Analytics (Threat Grid) es una de las listas de categorías de seguridad sobre las que puede informar. La mayoría de los informes, o todos ellos, utilizan las categorías de seguridad como filtro. Por ejemplo, puede filtrar las categorías de seguridad para mostrar solo la actividad relacionada con Cisco Secure Malware Analytics (Threat Grid).

1. Navegue hasta Informes > Informes principales > Búsqueda de actividad y en Categorías de seguridad seleccione "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics [Threat Grid]) para filtrar el informe y mostrar solo la categoría de seguridad para Cisco Secure Malware Analytics (Threat Grid).



Nota: Si la integración de Cisco AMP Threat Grid está desactivada, no aparecerá en el filtro Categorías de seguridad.

115014210123

2. Seleccione Apply.

Informes sobre cuándo se agregaron los dominios a la lista de destino de Cisco Secure Malware Analytics (Threat Grid)

El registro de auditoría de administración de Cisco Umbrella incluye eventos del panel de análisis de malware seguro de Cisco (Threat Grid) a medida que agrega dominios a la lista de destinos. Un usuario llamado "Cisco AMP Threat Grid Domain List", que también lleva la marca del logotipo de Cisco, genera los eventos. Estos eventos incluyen el dominio que se agregó y la hora en que se agregó.

Al seleccionar la entrada del registro de auditoría de administración, se amplía para mostrar detalles, incluido el dominio específico que se agregó.

Puede filtrar para incluir solo los cambios de Cisco Secure Malware Analytics (Threat Grid) aplicando un filtro para el usuario "Cisco AMP Threat Grid Domain List".

Gestión de detecciones no deseadas o falsos positivos

Dos tipos de detecciones de Cisco Secure Malware Analytics (Threat Grid) y dos soluciones

Actualmente, existen dos tipos de bloques de Cisco Secure Malware Analytics (Threat Grid): Uno con una posible resolución y otro con una resolución actual para una detección no deseada.

1. Entrada de Global Threat Grid (pública): En este momento, el único método para permitir el dominio es agregarlo a la lista de permitidos.
2. Fuente solo para clientes (privada): se puede abordar con una entrada de lista de permitidos o eliminando de la lista de integración de AMP Threat Grid.

Permitir listas

Aunque es poco probable, es posible que los dominios agregados automáticamente por la integración de Cisco Secure Malware Analytics (Threat Grid) puedan activar potencialmente una detección no deseada que bloquee el acceso de los usuarios a sitios web concretos. En una situación como esta, se recomienda agregar los dominios a una lista de permitidos (Políticas > Listas de destino), que tiene prioridad sobre todos los demás tipos de listas de bloqueo, incluida la configuración de seguridad.

Hay dos razones por las que se prefiere este enfoque. En primer lugar, en caso de que el panel de Cisco Secure Malware Analytics (Threat Grid) tuviera que volver a agregar el dominio después de que se haya eliminado, la lista de permitidos protege frente a este problema y genera más problemas. En segundo lugar, la lista de permitidos muestra un registro histórico de dominios problemáticos que pueden utilizarse para informes de diagnóstico o auditoría.

De forma predeterminada, existe una lista global de permitidos que se aplica a todas las políticas. Al agregar un dominio a la lista global de permitidos, el dominio se permite en todas las directivas.

Si la configuración de seguridad de Cisco Secure Malware Analytics (Threat Grid) en modo de bloqueo solo se aplica a un subconjunto de las identidades de Cisco Umbrella gestionadas (por ejemplo, solo se aplica a los equipos móviles y a los equipos móviles), puede crear una lista de permitidos específica para estas identidades o políticas.

Para crear una lista de permitidos:

1. Navegue hasta Políticas > Componentes de política > Listas de destino y seleccione 

("Agregar").
2. Seleccione Allow y agregue su dominio a la lista.
3. Seleccione Guardar.

Una vez guardada la lista, puede agregarla a una directiva existente que cubra los clientes afectados por el bloqueo no deseado.

Eliminación de dominios de la lista de destino de Cisco Secure Malware Analytics (Threat Grid)

Junto a cada nombre de dominio de la lista Cisco Secure Malware Analytics (Threat Grid) hay un icono ("Eliminar"). La eliminación de dominios le permite limpiar la lista de destinos de Cisco Secure Malware Analytics (Threat Grid) en caso de que se produzca una detección no deseada.

La eliminación no es permanente si el panel de Cisco Secure Malware Analytics (Threat Grid) reenvía el dominio a Cisco Umbrella.

1. Navegue hasta Políticas > Componentes de política > Integraciones y seleccione "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) para expandirlo.
2. Seleccione Consulte Dominios.
3. Busque el nombre de dominio que desea eliminar.
4. Seleccione el icono ("Eliminar").
5. Seleccione Cerrar.
6. Seleccione Guardar.

En caso de que se produzca una detección no deseada o un falso positivo, se recomienda crear una lista de permitidos en Cisco Umbrella inmediatamente y, a continuación, remediar el falso positivo en el panel de Cisco Secure Malware Analytics (Threat Grid). Posteriormente, puede eliminar el dominio de la lista de destinos de Cisco Secure Malware Analytics (Threat Grid).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).