Configure the Integration of Secure Malware Analytics (Formerly Threat Grid) with Umbrella

Contents

Introduction

This document describes how to integrate Secure Malware Analytics (formerly Threat Grid) with Umbrella.

Cisco Secure Malware Analytics (Threat Grid) Integration for Cisco Umbrella Overview

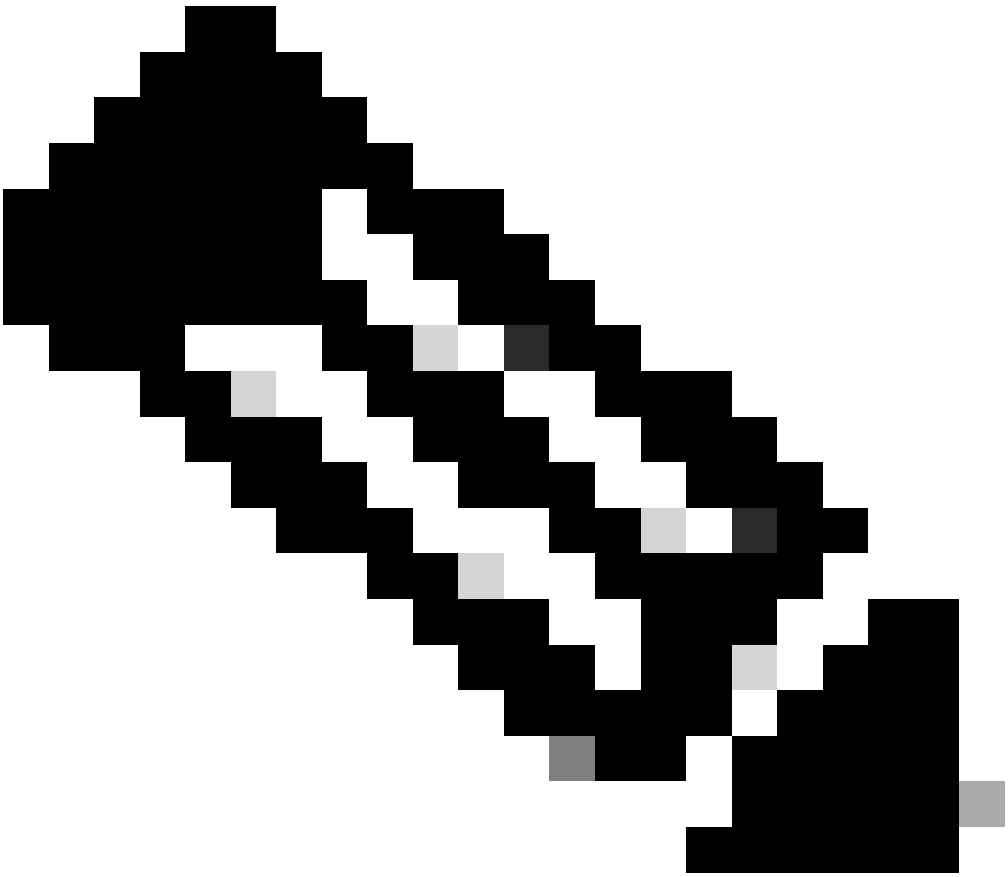
With the integration between Cisco Secure Malware Analytics (formerly Threat Grid) and Cisco Umbrella, security teams are now able to extend their visibility and enforce protection against today's advanced threats to roaming laptops, tablets, or phones while also providing another layer of enforcement to a distributed corporate network.

This guide outlines how to configure Cisco Secure Malware Analytics (Threat Grid) to communicate with Cisco Umbrella so that threat intelligence generated by Cisco Secure Malware Analytics (Threat Grid) can be automatically integrated into policies that can protect clients under your Cisco Umbrella.

Prerequisites

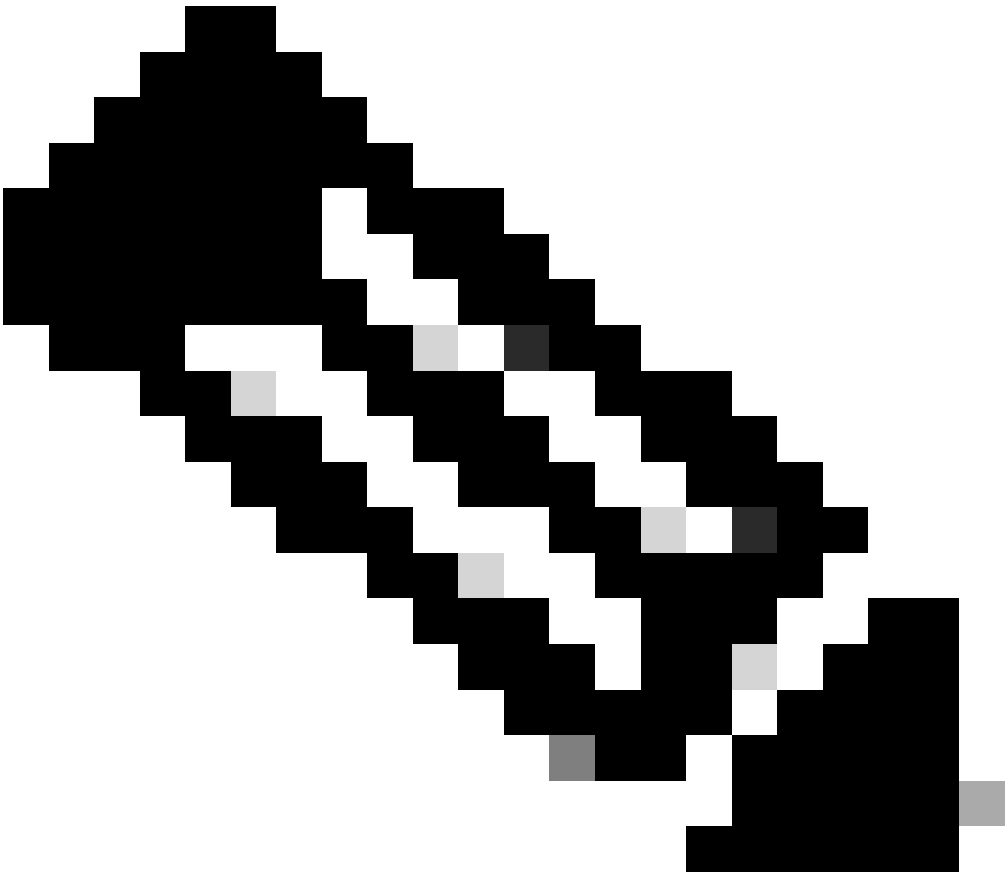
- A functional Cisco Secure Malware Analytics (Threat Grid) dashboard with access to your account's

API key.



Note: Cisco Secure Malware Analytics (Threat Grid) appliances and endpoints are not supported at this time.

- Cisco Umbrella Dashboard administrative rights.
- The Cisco Umbrella dashboard must have the Cisco Secure Malware Analytics (Threat Grid) integration enabled.



Note: The Cisco Secure Malware Analytics (Threat Grid) integration is only included in Cisco Umbrella packages like DNS Essentials, DNS Advantage, SIG Essentials, or SIG Advantage. If you do not have a Cisco Umbrella package and would like to have this integration, please contact your Cisco Umbrella Account Manager. If you have a Cisco Umbrella package but do not see Cisco Secure Malware Analytics (Threat Grid) as an integration for your Dashboard, please contact Cisco Umbrella Support.

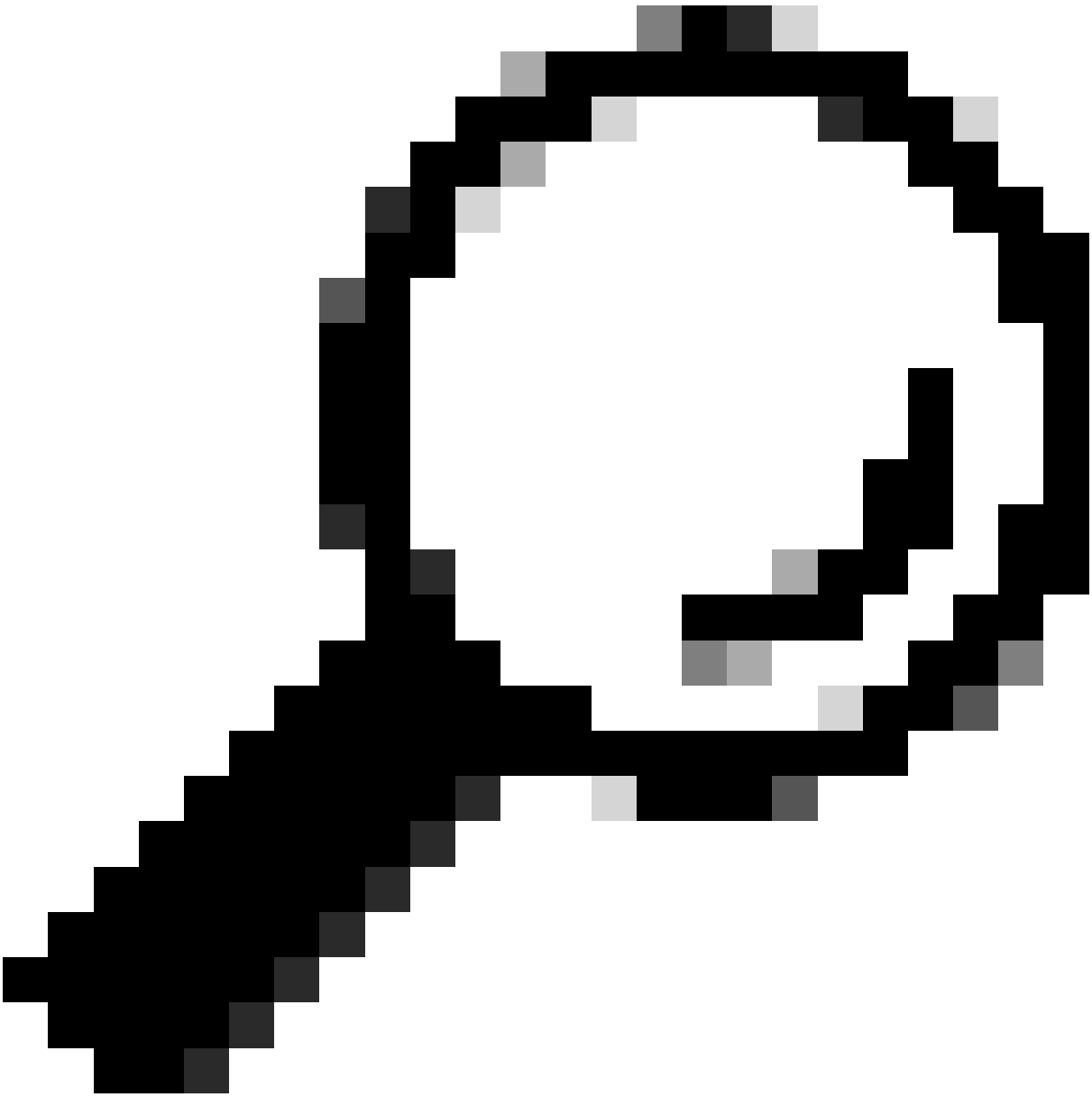
How does This Integration Work?

Cisco Umbrella reaches out to the Cisco Secure Malware Analytics (Threat Grid) API and retrieves lists of domains that are generated from the analysis of malicious samples. Cisco Umbrella then imports this list via the Cisco Umbrella Enforcement API. This approach is different from how other integrations work in that Cisco Umbrella **pulls** the threat intelligence in by making API queries to the Cisco Secure Malware Analytics (Threat Grid) API, rather than accepting incidents from other systems that **push** threat intelligence into the Cisco Umbrella service.

Cisco Umbrella then validates the threat to ensure it can be added to your policy. If the information from Cisco Secure Malware Analytics (Threat Grid) is confirmed to be a threat or is not a known good domain, the domain address is added to the Cisco Secure Malware Analytics (Threat Grid) 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 leveraging the Cisco Secure Malware Analytics (Threat Grid) integration.

Cisco Umbrella pulls two separate feeds from Cisco Secure Malware Analytics (Threat Grid): a Public (global) feed, and a Customer Only (private, specific to a single customer) feed.



Tip: While Cisco Umbrella tries its best to validate and allow domains that are known to be generally safe (for example, Google and Salesforce), to avoid any unwanted interruptions, we suggest adding any 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 might have both internal and external records. For example, "mail.myservicedomain.com" and "portal.myotherservicedomain.com".

- Lesser-known cloud applications you depend on heavily that Cisco Umbrella might not be aware of or include in their automatic domain validation. For example, "localcloudservice.com".

These domains must be added to the Global Allow List, which is found under **Policies > Destination Lists** in Cisco Umbrella.

Configuring your Cisco Umbrella Dashboard to obtain information from Cisco Secure Malware Analytics (Threat Grid)

The first step is to find or generate the API key in your Cisco Secure Malware Analytics (Threat Grid) dashboard:

1. Log into your Cisco Secure Malware Analytics (Threat Grid) dashboard and select your account details.
2. Under your **Account Details**, an API key might already be visible if you have created one already. If you have not, select "Generate New API Key."

   Your API key is then visible under **User Details > API Key**.

Next, add the API key to the Cisco Umbrella Dashboard for it to pull data from Cisco Secure Malware Analytics (Threat Grid):

1. Log into your Cisco Umbrella dashboard as an Administrator.
2. , navigate to **Policies > Policy Components > Integrations** and select "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) in the table to expand it.
3. Select **Enable**, paste your API Key into the **API Key** box, and then select **Save**.

At this point, if you receive an error, there is likely a problem with your API key or communications between the services. Check your API key and try again, and if it still fails contact Cisco Umbrella Support.

If you receive a success message, it indicates that the Cisco Umbrella service was able to use the API key to make an initial connection to the Cisco Secure Malware Analytics (Threat Grid) API. The Cisco Umbrella service uses a polling interval of five minutes to retrieve data from Cisco Secure Malware Analytics (Threat Grid).

Even after the five-minute interval, if there is no valid data or valid threat events available to be pulled by the Cisco Umbrella Dashboard, information might not appear. When the integration is first enabled, it just starts by going back five minutes for both the global and org-only feeds and the first time it gets data is at the next five-minute interval, so data might not appear immediately.

If the API key on the Cisco Secure Malware Analytics (Threat Grid) side were deactivated or removed, the integration would be disabled. To restore the integration, a new API key must be provided in the Cisco Umbrella Dashboard. If there is a timeout or internal service error between Cisco Umbrella and Cisco Secure Malware Analytics (Threat Grid), a different sort of exception is raised and the integration is not disabled, but instead, connections continue to be attempted every five minutes as in normal conditions.

Technical Details

The exact API queries being used to pull information from the Cisco Secure Malware Analytics (Threat Grid) are listed below. Note that only events with a severity greater than 90, a confidence greater than 90, and of the type Domains are being gathered. The time in this example is a five-minute range which is

incremented for the next query. The `api_key` provided in Cisco Umbrella is used in place of the `<key>` variable:

- Public (global feed):

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

- Customer Only (private feed):

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

or:

- Public (global feed):

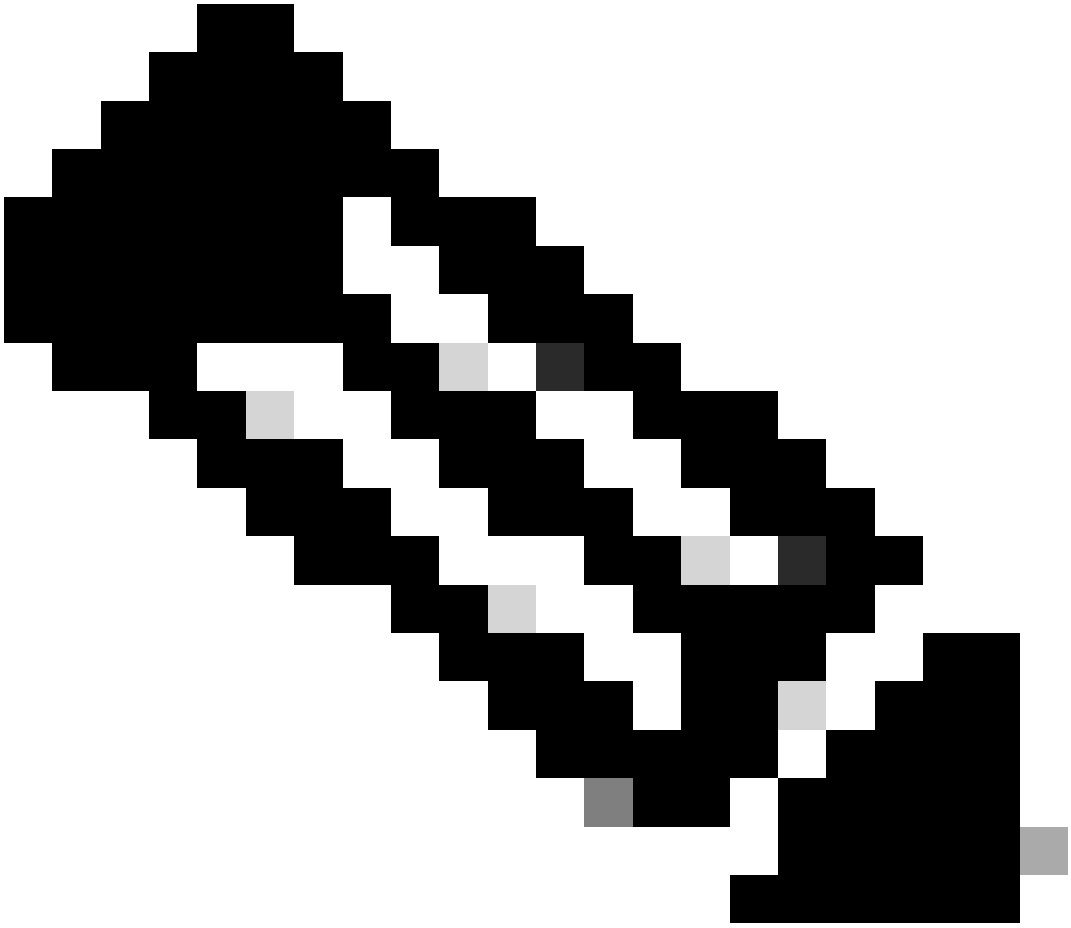
  ```
  hxxps://panacea.threatgrid.eu/api/v2/iocs/feeds/domains?limit=100&offset=0&severity=90&confidence
  ```

- Customer Only (private feed):

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

Observing events added to the Cisco Secure Malware Analytics (Threat Grid) in "audit mode"

Over time, the events from Cisco Secure Malware Analytics (Threat Grid) begins to populate a specific destinations list that can be applied to policies as the Cisco Secure Malware Analytics (Threat Grid) Category. By default, the destination list and the security category are in "audit mode" and are not applied to any policies, and thus does not result in any requests being blocked. However, you are able to see what requests are associated (and could have been blocked) by the Cisco AMP Threat Grid Security Category.



Note: "Audit mode" can be enabled as long as necessary, or even indefinitely, depending on your deployment profile and network configuration.

Review Destination List

You can review the Cisco Secure Malware Analytics (Threat Grid)Destination List at any time.

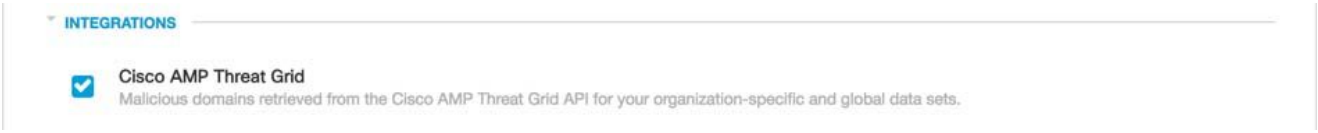
1. Navigate to **Policies > Policy Components > Integrations**.
2. Expand "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) in the table and select"See Domains."

Review Security Settings for a Policy

You can review the security settings that can be enabled for a policy at any time in Cisco Umbrella:

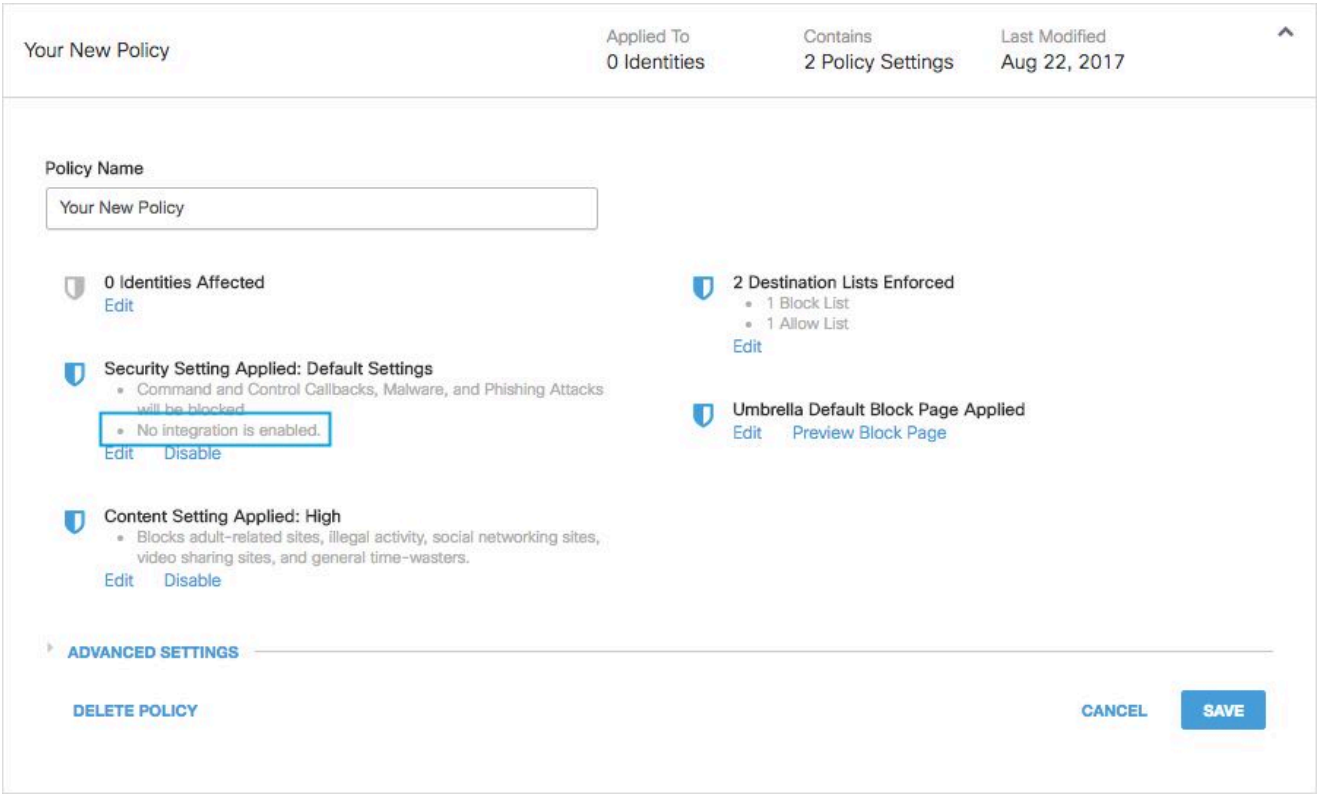
1. Navigate to **Policies > Policy Components > Security Settings**.
2. Click a security setting in the table to expand it.
3. Scroll to the **Integrations** section and expand the section to display the Cisco AMP Threat Grid (Cisco Secure Malware Analytics (Threat Grid)) integration.

4. Select the box for the Cisco AMP Threat Grid integration (Cisco Secure Malware Analytics (Threat Grid)), then select **Save**.

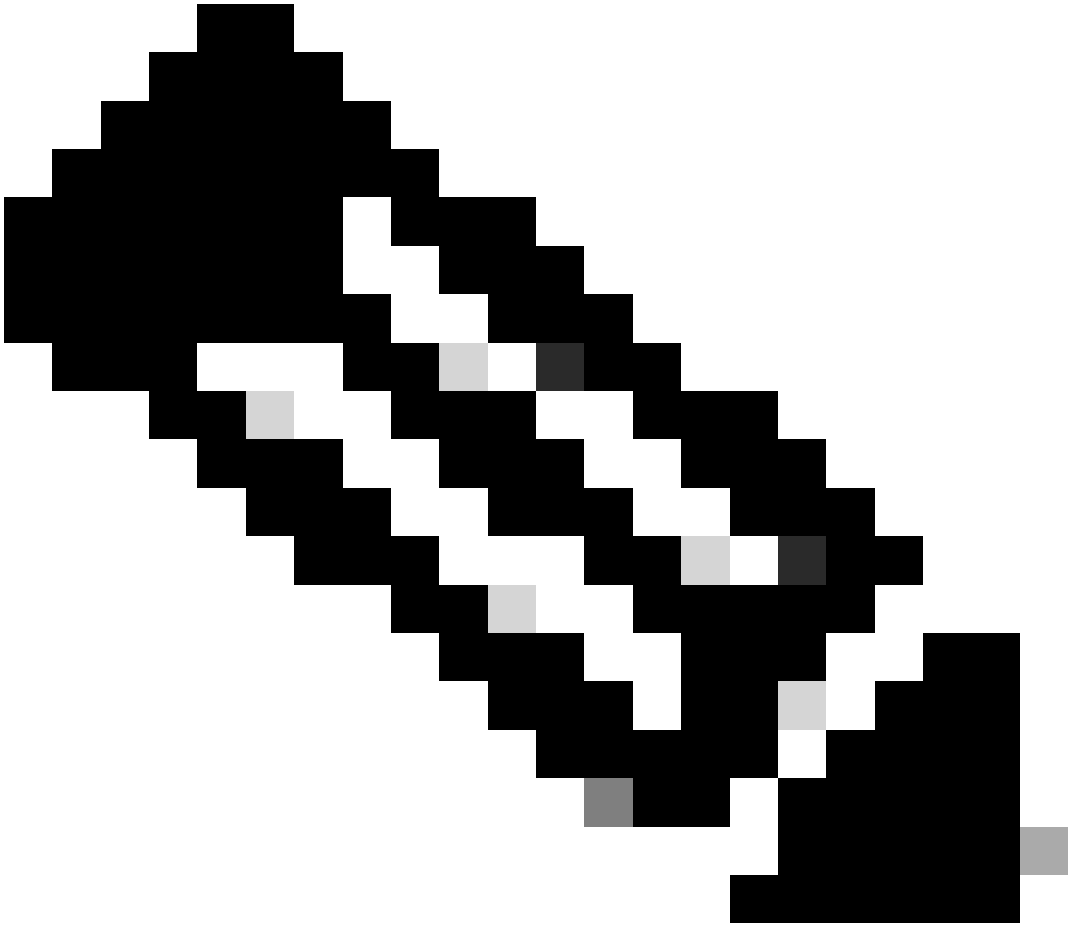


115014151543

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



20993269073556



Note: It can take up to five minutes to apply settings, and if new events are not being injected into the Cisco Secure Malware Analytics (Threat Grid) system, you might not see new domains being added to your integration.

Applying the Cisco Secure Malware Analytics (Threat Grid) Security Setting in "block mode" to a Policy for Managed Clients

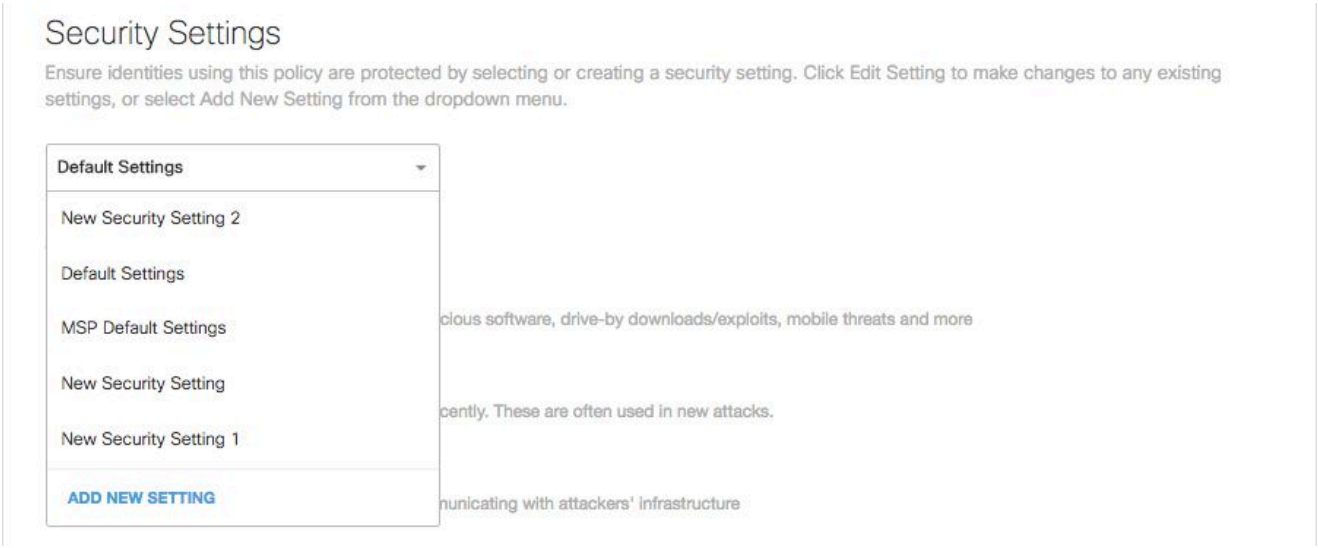
Once you are ready to have these domains blocked for clients managed by Cisco Umbrella, change the security setting on an existing policy, or create a new policy that sits above your default policy to ensure it is enforced first.

1. Navigate to **Policies > Policy Components > Security Settings.**
2. Under **Integrations**, verify that the "Cisco AMP Threat Grid" box is selected. If not, select the box and select **Save**.

115013987086

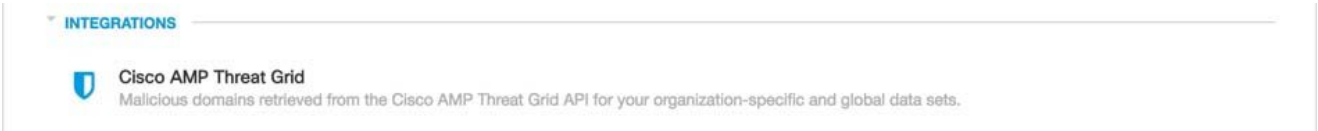
Next, in the Cisco Umbrella Policy wizard, add a security setting to the policy you are editing:

1. Navigate to **Policies > Management > All Policies**.
2. Expand a policy and under **Security Setting Applied** and then select **Edit**.
3. In the **Security Settings** pull-down, select a security setting that includes the "Cisco AMP Threat Grid" setting.



20993282642708

The shield icon under Integrations updates to blue.



115013987446

4. Select **Set & Return**.

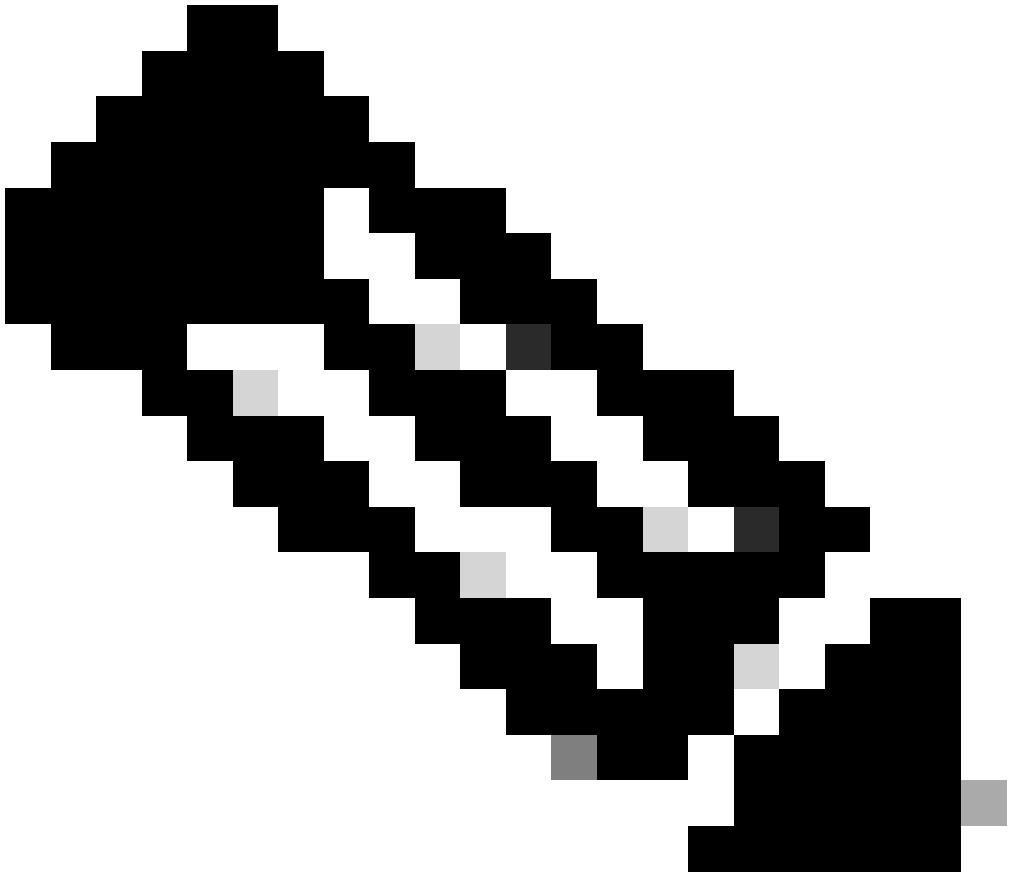
Cisco Secure Malware Analytics (Threat Grid) domains contained within the security setting for Cisco Secure Malware Analytics (Threat Grid) is blocked for those identities using the policy.

Reporting within Cisco Umbrella for Cisco Secure Malware Analytics events

Reporting on Cisco Secure Malware Analytics (Threat Grid) Security Events

The Cisco Secure Malware Analytics (Threat Grid) Destination List is one of the Security Categories lists you can report on. Most or all of the reports use the Security Categories as a filter. For instance, you can filter security categories to only show Cisco Secure Malware Analytics (Threat Grid)-related activity.

1. Navigate to **Reporting > Core Reports > Activity Search** and under **Security Categories** select "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) to filter the report to only show the security category for Cisco Secure Malware Analytics (Threat Grid).



Note: If the Cisco AMP Threat Grid integration is disabled, it does not appear in the Security Categories filter.

115014210123

2. Select **Apply**.

Reporting on When Domains Were Added to the Cisco Secure Malware Analytics (Threat Grid) Destination List

The Cisco Umbrella Admin Audit log includes events from the Cisco Secure Malware Analytics (Threat Grid) dashboard as it adds domains to the destination list. A user named “Cisco AMP Threat Grid Domain List”, which is also branded with the Cisco logo, generates the events. These events include the domain that was added and the time when it was added.

Selecting the Admin Audit Log entry expands it to show details, including the specific domain that was added.

You can filter to only include Cisco Secure Malware Analytics (Threat Grid) changes by applying a filter for the “Cisco AMP Threat Grid Domain List” user.

Handling Unwanted Detections or False Positives

Two types of Cisco Secure Malware Analytics (Threat Grid) Detections and Two Resolutions

Currently, there are two types of Cisco Secure Malware Analytics (Threat Grid)blocks: One with one possible resolution and a second with one current resolution to an unwanted detection.

1. **Global Threat Grid entry (Public):** At this time, the only method to allow the domain is to add it to your allow list.
2. **Customer only feed (Private):** Can be addressed with an allow list entry or deleting from the AMP Threat Grid integration list.

Allow Lists

Although unlikely, it is possible that domains added automatically by your Cisco Secure Malware Analytics (Threat Grid) integration could potentially trigger an unwanted detection that blocks your users from accessing particular websites. In a situation like this, we recommend 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 preferred. First, in case the Cisco Secure Malware Analytics (Threat Grid) dashboard was to re-add the domain again after it was removed, the allow list safeguards against this causing further issues. Secondly, the allow list shows a historical record of problematic domains that can be used for forensic 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 Cisco Secure Malware Analytics (Threat Grid) 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 these identities or policies.

To create an allow list:

1. Navigate to **Policies > Policy Components > Destination Lists** andselect 

("Add").
2. Select **Allow** and add your domain to the list.
3. Select **Save**.

Once the 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 Cisco Secure Malware Analytics (Threat Grid) Destination List

Next to each domain name in the Cisco Secure Malware Analytics (Threat Grid) list is a ("Delete") icon. Deleting domains lets you clean up the Cisco Secure Malware Analytics (Threat Grid) Destination List in the event of an unwanted detection.

The delete is **not** permanent if the Cisco Secure Malware Analytics (Threat Grid) dashboard were to resend the domain to Cisco Umbrella.

1. Navigate to **Policies > Policy Components > Integrations** and select "Cisco AMP Threat Grid" (Cisco Secure Malware Analytics (Threat Grid)) 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, we recommend creating an allow list in Cisco Umbrella immediately and then remediating the false positive within the Cisco Secure Malware Analytics (Threat Grid) dashboard. Later, you can remove the domain from the Cisco Secure Malware Analytics (Threat Grid) Destination List.