

# Integrate Cisco SecureX with Cisco Umbrella

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Create Module](#)

[Investigate API](#)

[Enforcement API](#)

[Reporting API](#)

[Save Module](#)

[Create SecureX Dashboard](#)

[Verify](#)

[Investigate](#)

[Enforcement](#)

[Reporting](#)

[Video](#)

[Related Information](#)

## Introduction

This document describes the process to configure and verify the Umbrella integration with SecureX with the 3 available APIs.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Umbrella
- Cisco Secure X
- Cisco Threat Response

### Components Used

The information in this document is based on these software and hardware versions:

- Umbrella account with DNS Advantage License
- Secure X

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Background Information

In order to fully configure this integration with all of its functionalities, you need access to the 3 following APIs

- Reporting API (included in all licenses)
- Enforcement API
- Investigate API

In order to configure the Umbrella integration, you must first gather some information from your Umbrella instances and then complete the **Add New Umbrella Module** form.

## Configure

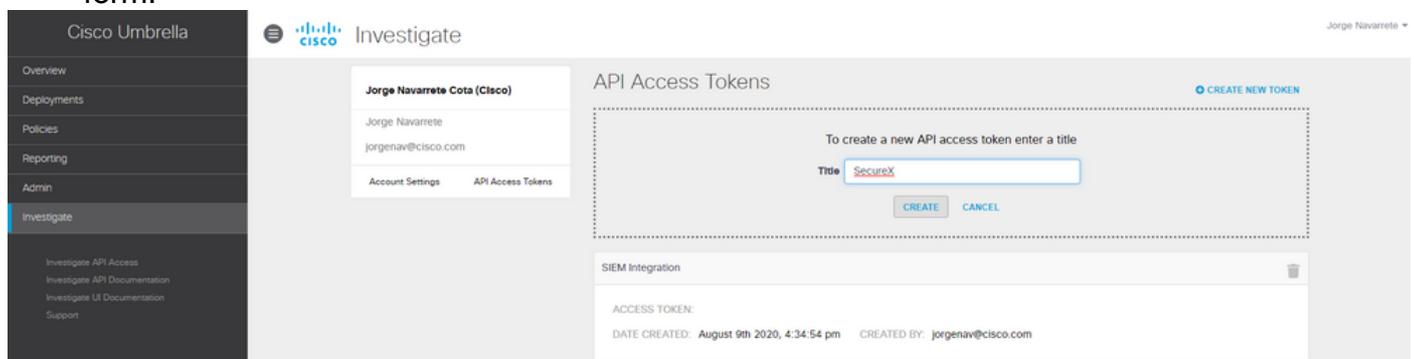
### Create Module

1. Log in to your Secure X account. If you don't have an account yet, you can create one with [Cisco Secure Sign-On](#).
2. Navigate to **Integrations > Add New Module**. In the Available Integrations page scroll down to the Umbrella option and click **Add New Module**.

Follow the below steps to collect the necessary information from your Umbrella Account to submit in the **Add New Umbrella Module** form.

### Investigate API

1. In Umbrella, navigate to **Investigate > Investigate API Access**, click **Create New Token** and enter a title for the token, and then click **Create New Token** again.
2. Copy the Access Token value into the API Token field on the Add New Umbrella Module form.



### Enforcement API

1. In Umbrella, navigate to **Policies > Policy Components > Integrations**, click **Add** and enter a name, and click **Create**.
2. Click the newly created **integration name** link, check the **Enable** checkbox, and **Save**.

3. Click the **integration name** to display the integration URL. Copy the integration URL into the **Custom Umbrella Integration URL** field on the **Add New Umbrella Module** form.

Name	Status	
Check Point	Disabled	● ○
Cisco AMP Threat Grid	Disabled	● ○
CTR -- Enforcement	Disabled	● ○
FireEye	Disabled	● ○
SecureX	Enabled	● ○
SecureX-elseo	Enabled	● ○
test	Disabled	● ○
ThreatConnect	Disabled	● ○
ThreatIQ	Disabled	● ○
ZeroFOX	Disabled	● ○

Create a custom integration between Umbrella and other parts of your security stack (e.g. SIEM, threat intelligence platform (TIP), or homegrown systems) using the Cisco Umbrella API to instantly operationalize your threat intelligence into visibility and enforcement. [Learn more](#)

SecureX

Enable

Create an integration for a custom threat intelligence feed using the Cisco Umbrella API and the URL below. [Instructions](#)

https://s-platform.api.opendns.com/1.0/events?customerKey=f32505aa-3247-487c-9f34

SEE DOMAINS

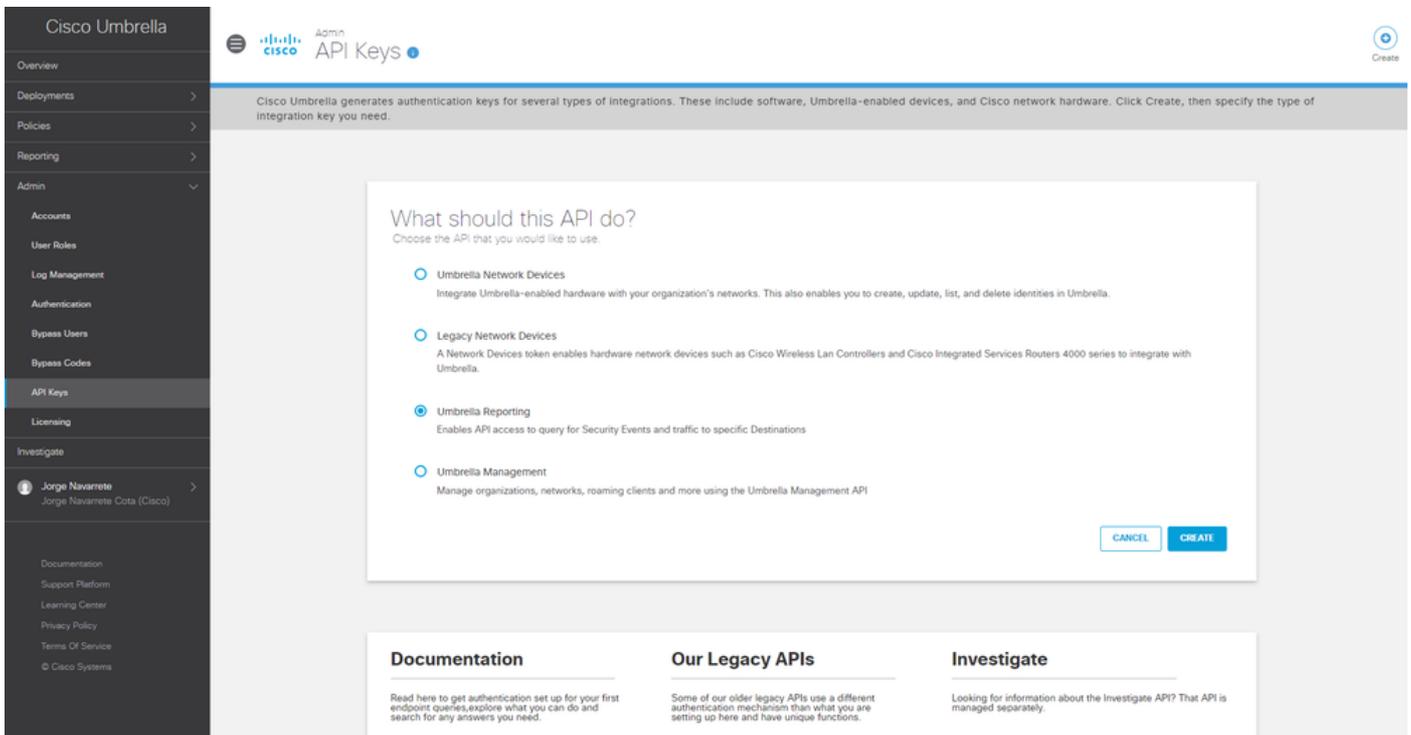
CANCEL

SAVE

**Note:** In order to integrate the Umbrella Enforcement API, you must be an admin in an Umbrella standalone org or child org instead of an admin of an Umbrella console.

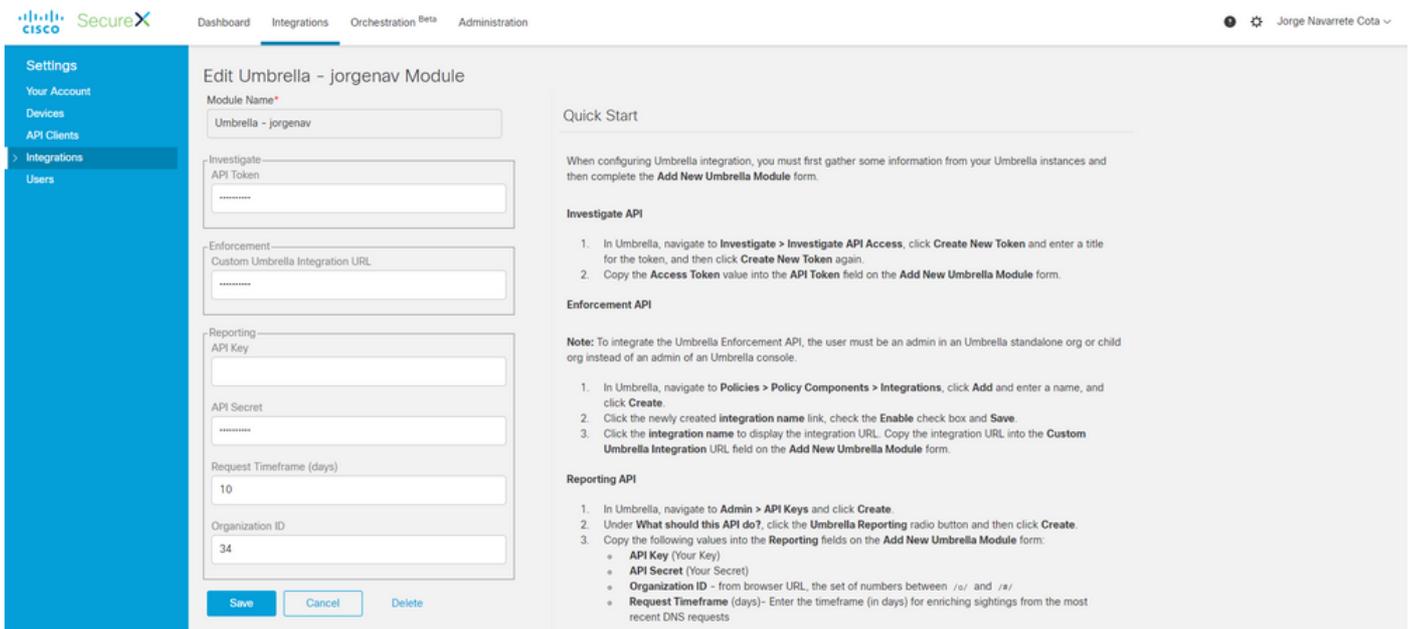
## Reporting API

1. In Umbrella, navigate to **Admin > API Keys** and click **Create**.
2. Under **What should this API do?**, click the **Umbrella Reporting** radio button and then click **Create**.
3. Copy the next values into the **Reporting** fields on the **Add New Umbrella Module** form: **API Key** (Your Key) **API Secret** (Your Secret) **Organization ID** - from browser URL, the set of numbers between /o/ and /#/ **Request Timeframe** (days) - Enter the timeframe (in days) for enriching sightings from the most recent DNS requests



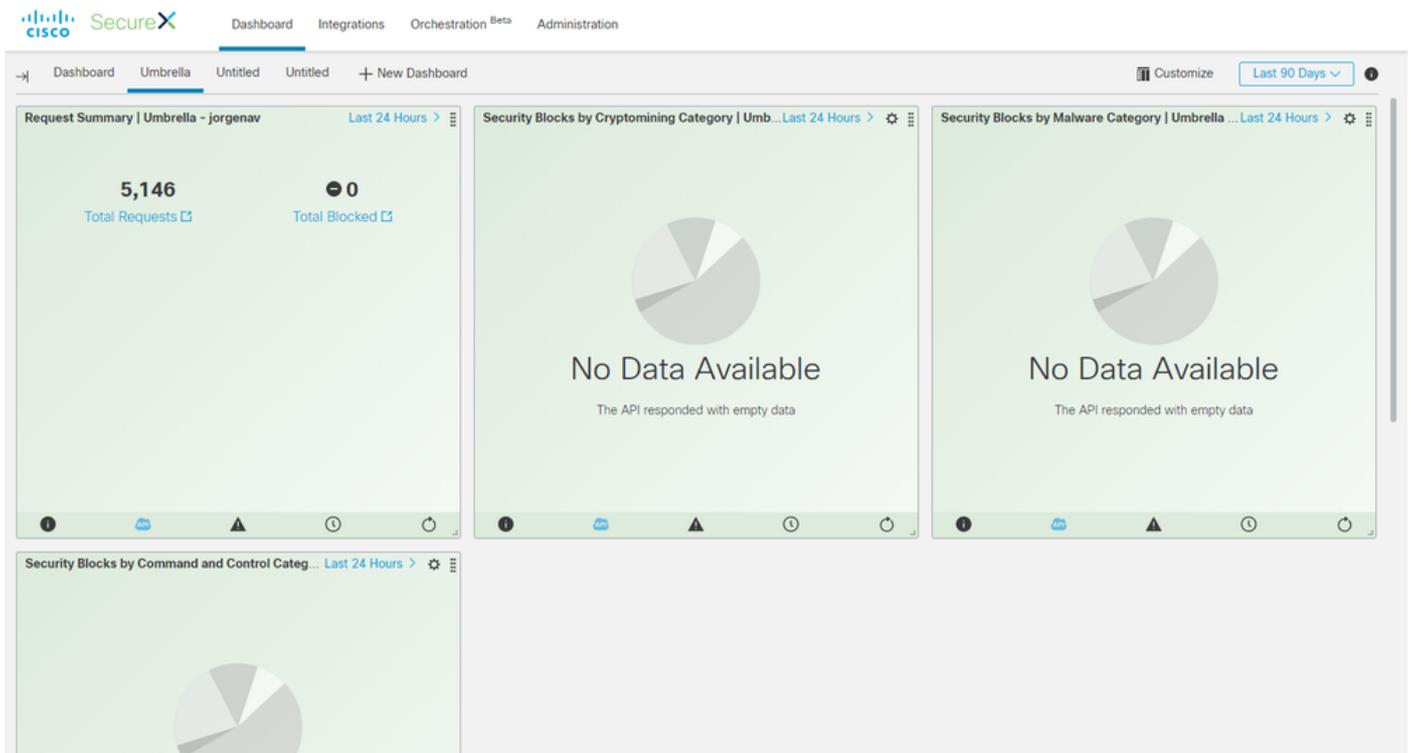
## Save Module

1. Fill out the API information in your Umbrella Module, click **Save**.



## Create SecureX Dashboard

1. Once you added your module, you can navigate to Secure X and create a **New Dashboard**.
2. Under the available Dashboards, select your Umbrella module and add the Categories you are interested in seeing.
3. Click **Save**, and see your information populated via the API.



## Verify

Use this section in order to confirm that your configuration works properly.

## Investigate

The Investigate API, allows you to add a feed to a CTR investigation, to see the disposition of a domain and enrich the investigation with other modules.

1. In order to verify this integration, make a new investigation in [Cisco Threat Response](#). Search for a known domain such as cisco.com and you should see a Disposition provided by Umbrella.
2. If you click under the domain in the Relations Graph, you also can pivot from there to the Investigate Dashboard in Umbrella.

Investigation: 1 of 1 enrichments complete

domain: cisco.com

Investigate Clear Reset What can I search for?

Relations Graph - Dispositions: All - Types: All - Mode: Simplified - Showing 4 of 73 nodes

3 IPs

Clean Domain

cisco.com

2 SHA-256s

Sightings

Observables

cisco.com

Clean Domain

My Environment Global

0 Sightings in My Environment

Aug 9, 2020 22:21:17

Module	Observable	Disposition	Reason	Source
Umbrella - jorgenav	DOMAIN: cisco.com	Clean	Good Cisco Umbrella reputation status	Umbrella Investigate API
Talos Intelligence	DOMAIN: cisco.com	Clean	Good Talos Intelligence reputation score	Talos Intelligence

## Enforcement

With the Enforcement API, you can block or unblock a domain directly from an investigation.

1. In order to verify that the API works, you can block a domain seen in an investigation and that adds the domain to the policy block list in Umbrella.
2. In order to verify that the URL has been added to the block list, navigate to **Policies > Policy Components > Integrations**. Select your SecureX integration, and click **See Domains**. A window displays the added domains from CTR.

Relations Graph - Dispositions: All - Types: All - Mode: Expanded - Showing 1 node

Domain

malicioushackers.com

malicioushackers.com

Domain

KEVIN TG

Submit URL to Threat Grid

Brandon Plays with Teams

vivings4\_Perimeter Block

Move Computer to AMP Triage Group

Perimeter Block

Talos Intelligence

Search for this domain

ThreatGrid\_jesum2

Browse malicioushackers.com

Search malicioushackers.com

Umbrella - jorgenav

Domain view for malicioushackers.c...

Block this domain

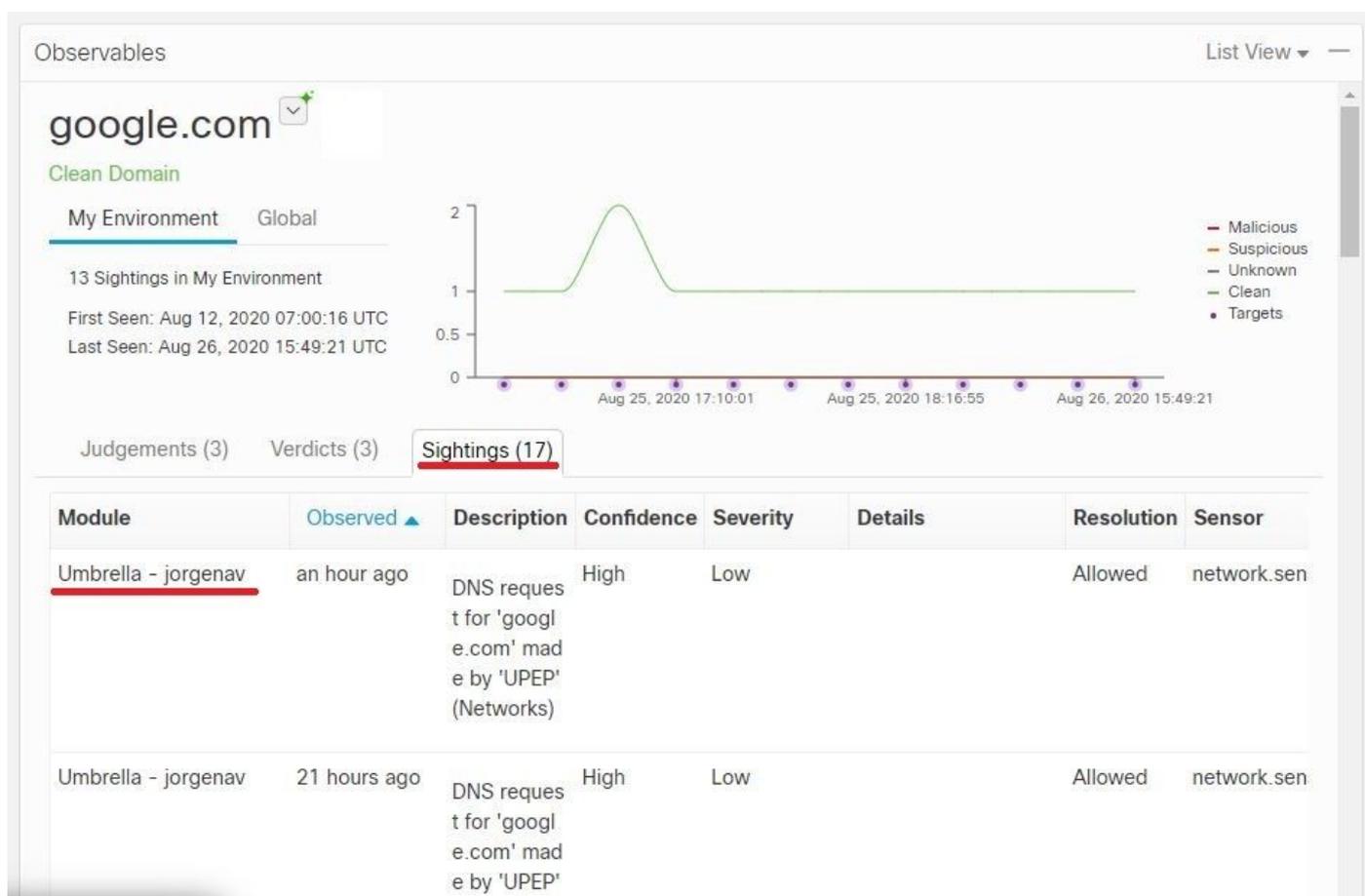
3. If the domains are not blocked, on your Umbrella dashboard navigate to **Policies > Policy Components > Security Settings**. Under **Integrations** make sure that you have applied your desired list.

## Reporting

The Reporting API allows you to see the information of your Umbrella deployments within SecureX.

You can verify the integration with an investigation of a domain you know has been seen in your environment in CTR.

In the CTR Investigation, the list of computers that have accessed a particular domain is displayed under **Sightings**.



## Video

You can find the configuration information contained in this article in the following video.

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)