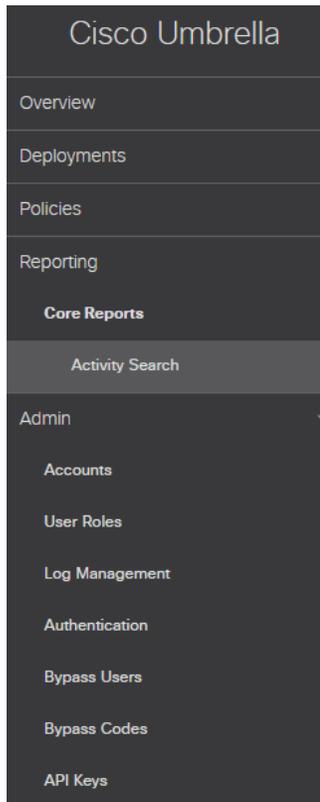
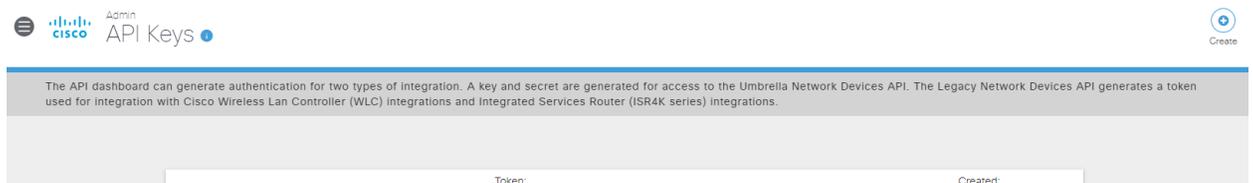


# CISCO UMBRELLA INTEGRATION THREAT RESPONSE

- 1- Inicia sesion en la consola de Umbrella , seleccionar Admin > API Keys



- 2- Hacer clic en el boton Crear , se abra un formulario ,
  - a. Seleccionar Umbrella Reporting y dar clic en Crear



What should this API do?  
Choose the API that you would like to use.

Umbrella Network Devices  
To be used to integrate Umbrella-enabled hardware with your organization. In addition, allows you to create, update, list and delete identities in Umbrella.

Legacy Network Devices  
A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.  
You can only generate one token. Refresh your current token to get a new token.

Umbrella Reporting  
Enables API access to query for Security Events and traffic to specific Destinations.  
You can only generate one token. Refresh your current token to get a new token.

Umbrella Management  
Manage organizations, networks, roaming clients and more using the Umbrella Management API

CANCEL CREATE

Umbrella Reporting Key: [REDACTED] Created: Jul 24, 2019

The API key and secret here are used to perform API requests against your Umbrella organization.

Your Key: [REDACTED]

Your Secret: [REDACTED]

To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

[Check out the documentation](#) for step by step instructions.

DELETE REFRESH CLOSE

- 3- Copiar Key y Secret para poder agregar al modulo de Threat Response
- 4- Guarda tu ID de Umbrella que encontraras en la barra de URL , tu ID es el numero que se encuentra entre /o/ y /#/ en la barra de URL.

← → ↻ [https://dashboard.umbrella.com/o/\[REDACTED\]/#/admin/apikeys](https://dashboard.umbrella.com/o/[REDACTED]/#/admin/apikeys)

Apps [REDACTED]

Cisco Umbrella

Overview

Deployments >

Admin API Keys i

The API dashboard can generate used for integration with Cisco V

- 5- Inicia sesion en Cisco Threat Response > Modules > Configure Modules> Umbrella> Cisco Umbrella.

Settings

Your Account

Devices

API Clients

Integration Modules

Users

# Integration Modules

[Configure Modules](#) [How do I configure modules?](#)

## AMP Global Intel - AMP Global Intel - Adv

*This module comes with Cisco Threat Response and cannot be edited.*

### Configure New Module

MODULE TYPE: Umbrella - Cisco Umbrella

MODULE NAME: Umbrella

Investigate

API TOKEN:

Enforcement

CUSTOM UMBRELLA INTEGRATION URL:

Reporting

#### Tips

Connect Cisco Umbrella

**Enrichment**

Add the API Token for the Umbrella API. If the Umbrella navigation menu is not visible, expand it using the menu icon in the upper left corner of the Cisco Umbrella page at <https://dashboard.umbrella.com/>. Click the Investigate option. A new tab will open with several options listed beneath Investigate. Click Investigate API Access. From the resulting page you can create a new or retrieve an existing API Token.



**Response**

Umbrella comes with the response capability to add and remove Domains in your domain list. To enable it, you'll need to provide

- 6- En la seccion de Reporting ingresas la llave , el numero secreto y tu ID guardades en los pasos anteriores.
- 7- El time frame es dias de los mas recientes consultas de DNS.
- 8- Clic en Create module.

### Configure New Module

Enforcement

CUSTOM UMBRELLA INTEGRATION URL:

Reporting

API KEY: [REDACTED]

API SECRET: [REDACTED]

REQUEST TIMEFRAME (DAYS): 2

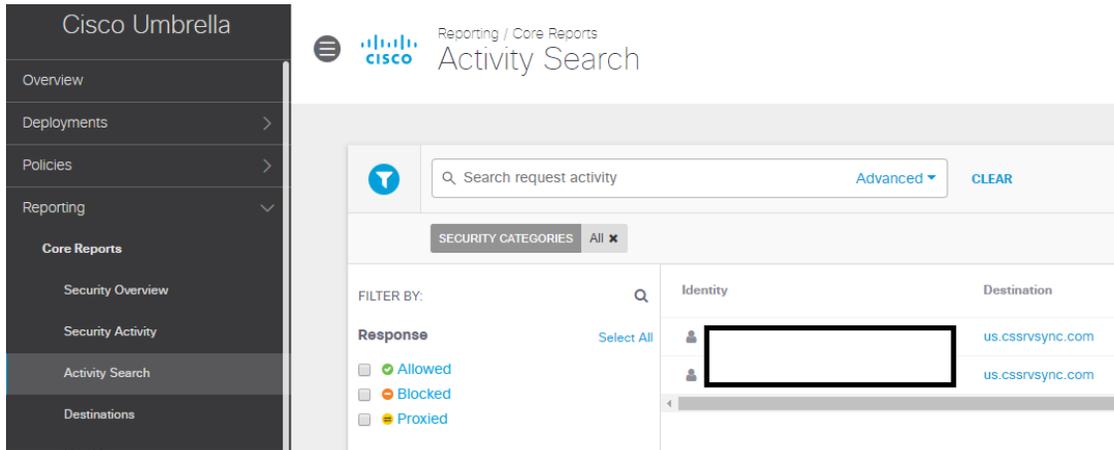
ORGANIZATION ID: [REDACTED]

\* Required

[Cancel](#) [Create Module](#)

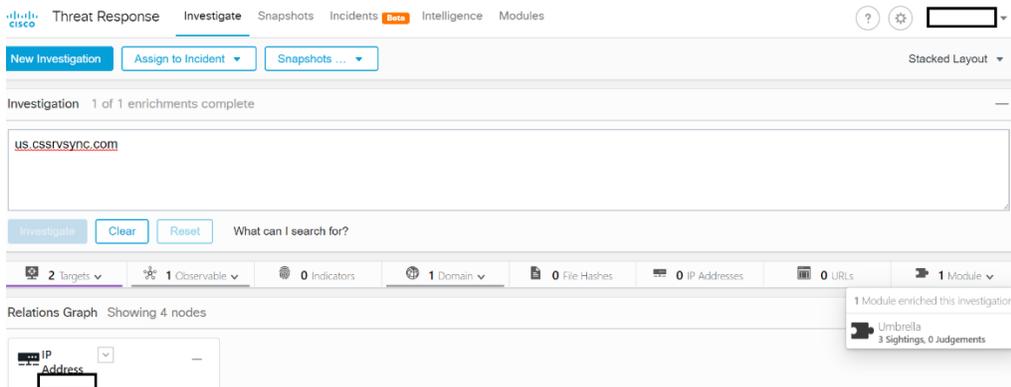
# VALIDAR MODULO DE UMBRELLA EN CISCO THREAT RESPONSE

1- Inicia sesion en Umbrella > Reporting > Activity Search



2- Selecciona un destino para investigacion, en este caso seleccionare us.cssrvsync.com

3- En Threat response ingreso el dominio para investigar.



Confirmaras que la Fuente de la informacion proviene de Umbrella.

