Cisco Umbrella™ Integration Configuration Guide

Software Version 3.0

Integration Guide

April 19, 2023

30053-03 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

The Cisco Umbrella integration allows Host and URL Indicators in ThreatConnect® to be added and removed from the Cisco Umbrella Platform over the Cisco Umbrella API.

Dependencies

ThreatConnect Dependencies

- ThreatConnect version 6.4 or newer
- Active ThreatConnect Application Programming Interface (API) key

Note: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Customers on Dedicated Cloud and On Premises instances can enable these settings on the **Account Settings** screen within their ThreatConnect instance.

Cisco Umbrella Dependencies

- Active Cisco Umbrella Platform subscription with API access. The API is available only in the Platform-level subscription of Cisco Umbrella.

Configuration Parameters

Parameter Definitions

The parameters defined in Table 1 apply to the configuration parameters during the Job-creation process.

Table 1

Name	Description	Required?
Api User	The ThreatConnect API User.	Yes
Cisco Umbrella API key (customer_key)	The Cisco Umbrella API key.	Yes
ThreatConnect Indicator Types	The type(s) of Indicators that will be sent to Cisco Umbrella. Accepted values include the following: • Host • URL	No
ThreatConnect Owners	The ThreatConnect owner(s) whose Indicators will be sent to Cisco Umbrella.	No
Last Run	The last time the App ran. Data modified since this date will be included on the first run. Thereafter, the date will be automatically updated each time the Job successfully completes. The default value is **30 days ago**.	No
TQL	A custom ThreatConnect Query Language (TQL) query for filtering Indicators. If using this parameter, do not use any other filter-based parameters (**Indicator Types**, **ThreatConnect Owners**, **Tag Filter**, **Minimum ThreatAssess Score**, **Minimum Threat Rating**, **Minimum Confidence Rating**, and **Maximum False Positive Count**), as doing so will cause the App to error out.	No
Tag Filter	The Tag(s) that Indicators must include in order to be sent to Cisco Umbrella. Indicators must include **at least one** of the specified Tags in order to be sent.	No

Minimum ThreatAssess Score	The minimum ThreatAssess score that Indicators must have in order to be sent to Cisco Umbrella.	No
Minimum Threat Rating	The minimum Threat Rating that Indicators must have in order to be sent to Cisco Umbrella.	No
Minimum Confidence Rating	The minimum Confidence Rating that Indicators must have in order to be sent to Cisco Umbrella.	No
Maximum False Positive Count	The maximum number of false positives that Indicators can have in order to be sent to Cisco Umbrella. When used, only Indicators with a false positive count less than or equal to the specified value will be sent.	No
Logging Level	Determines the verbosity of the logging output for the application.	Yes