ThreatConnect® Indicator CSV Integration Installation and Configuration Guide

Software Version 3.0

Integration Guide

February 27, 2023

30049-03 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 **ThreatConnect Indicator CSV** integration produces a custom comma-separated values (CSV) file of Indicators on a schedule for download by third-party tools over HTTPS. The App allows users to define the columns to include in the CSV file, filters for retrieving data from ThreatConnect, and how frequently the file should be updated.

Dependencies

ThreatConnect Dependencies

- 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.

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 username of the ThreatConnect API account.	Yes
TQL	Use this parameter to filter Indicators based on a custom ThreatConnect Query Language (TQL) query. When used, all other filter-based parameters will be ignored.	No

Field Mapping	A comma-separated list of field mappings for each column that will be included in the CSV file. **Available Field Values:** @tc.attribute=Attribute Name @tc.dateAdded @tc.id @tc.lastModified @tc.ownerName @tc.tags @tc.threatAssessRating @tc.threatAssessConfidence @tc.threatAssessScore @tc.type @tc.type_specific @tc.value @tc.webLink **Format:** Header Name::@tc.field **Default Mapping:** Value::@tc.value Type::@tc.type Type Specific::@tc.type_specific Owner::@tc.ownerName Description::@tc.attribute=Description Date Added::@tc.dateAdded ID::@tc.id Date Last Modified::@tc.lastModified Tags::@tc.tags ThreatAssess Rating::@tc.threatAssessRating ThreatAssess Confidence::@tc.threatAssessConfidence Web Link::@tc.webLink	Yes
Include Tags	Use this parameter to filter Indicators by the specified Tag(s). When used, only Indicators that include **at least one** of the specified Tags will be exported.	No

Indicator Types	Use this parameter to filter Indicators by type. When used, only Indicators of the selected type(s) will be exported.	No
Last Run	The last time the Job ran, which determines the interval for which data are retrieved.	No
Do not update Last Run Field	Select this checkbox to prevent the **Last Run** field from being updated when the App runs.	No
Maximum False Positive Count	Use this parameter to filter Indicators by false positive count. When used, only Indicators with a false positive count less than or equal to the specified value will be exported.	No
Minimum Confidence Rating	Use this parameter to filter Indicators by Confidence Rating. When used, only Indicators with a Confidence Rating greater than or equal to the specified value will be exported.	No
Minimum Threat Rating	Use this parameter to filter Indicators by Threat Rating. When used, only Indicators with a Threat Rating greater than or equal to the specified value will be exported.	No
Minimum ThreatAssess Score	Use this parameter to filter Indicators by ThreatAssess score. When used, only Indicators with a ThreatAssess score greater than or equal to the specified value will be exported.	No
ThreatConnect Owners	Use this parameter to filter Indicators by owner. When used, only Indicators belonging to the selected owner(s) will be exported.	No
Attributes with Multiple Values	Specifies which Attribute value to export for Indicators that contain multiple Attributes of the same Attribute Type.	Yes
Field Delimiter	The delimiter used between fields in the CSV file.	Yes

Duplicate indicators	Determines how the App will handle duplicate Indicators.	No
Write Field Headers	Enables a header row to be written for each column. If this parameter is enabled and the header name is not specified in the Field Mapping, then the default field name from ThreatConnect will be used.	No
Logging Level	Determines the verbosity of the logging output for the application.	Yes

Accessing Published CVS Files

After the App has created and published the CSV files, the files can be accessed and downloaded via URLs. To access these URLs, navigate to the **Apps** tab of the **Organization Settings** screen, click the vertical ellipsis ⋮ in the **Options** column for the Job, and select **Published Files** from the menu that is displayed (Figure 1).

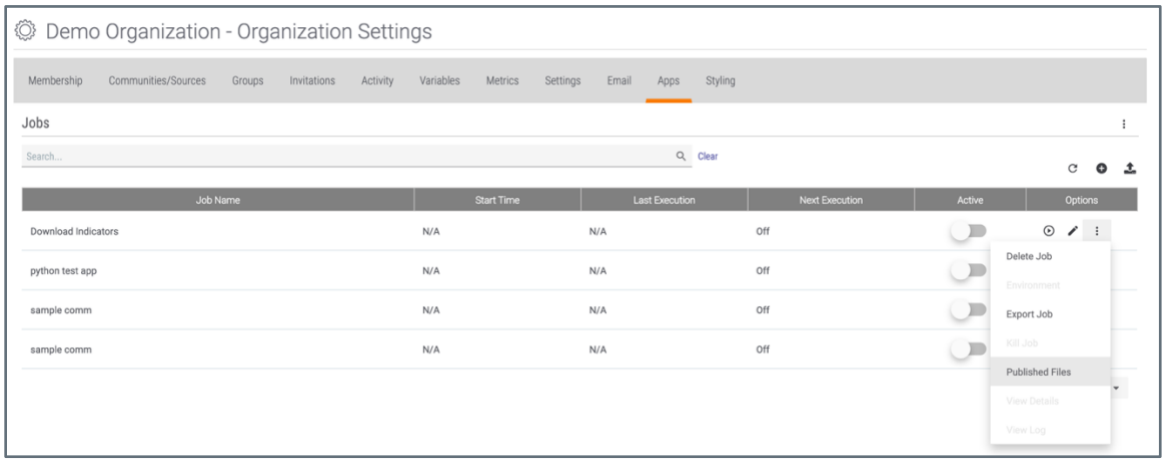

Figure 1

The **Published Files** window will be displayed, providing the URLs to download the published files (Figure 2). These URLs can be used with a third-party integration or for manual download.

Figure 2