



# Fidelis® Network Extract Integration Configuration Guide

Software Version 2.0

Integration Guide

April 27, 2023

30072-02 EN Rev. A



©2023 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.

Fidelis® is a registered trademark of Fidelis Cybersecurity, Inc.



# Table of Contents

---

<b>Overview .....</b>	<b>4</b>
<b>Dependencies .....</b>	<b>4</b>
ThreatConnect Dependencies .....	4
Fidelis Dependencies .....	4
<b>Configuration Parameters .....</b>	<b>4</b>
Parameter Definitions .....	4



# Overview

The ThreatConnect® integration with Fidelis Network Extract publishes a CSV file of IOCs based on the parameters configured in the Job, using ThreatConnect as a web server for Fidelis to retrieve. The Basic Authentication username and password are placed into the configuration within Fidelis, along with the URL of the CSV files, which can be retrieved by clicking on the three dots to the right of the Jobs entry.

## 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.

### Fidelis Dependencies

- Active Fidelis subscription

## 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 account.	Yes
Indicator Types	The type(s) of Indicators that will be sent to Fidelis. Accepted values include the following: <ul style="list-style-type: none"><li>• Address</li><li>• EmailAddress</li><li>• File</li><li>• Host</li><li>• URL</li></ul>	No
ThreatConnect Owners	The ThreatConnect owner(s) whose Indicators will be sent to Fidelis.	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 updated automatically each time the Job completes successfully. The default value is <b>30 days ago</b> .	No
TQL	A custom <a href="#">ThreatConnect Query Language (TQL)</a> query for filtering Indicators. If using this parameter, do not use any other filter-based parameters ( <b>Indicator Types, ThreatConnect Owners, Include Tags, Minimum ThreatAssess Score, Minimum Threat Rating, Minimum Confidence Rating, and Maximum False Positive Count</b> ), as doing so will cause the App to error out.	No



Include Tags	The Tag(s) that Indicators must have in order to be sent to Fidelis. Indicators must include <b>at least one</b> 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 Fidelis.	No
Minimum Threat Rating	The minimum Threat Rating that Indicators must have in order to be sent to Fidelis.	No
Minimum Confidence Rating	The minimum Confidence Rating that Indicators must have in order to be sent to Fidelis.	No
Minimum False Positive Count	The maximum number of false positives that Indicators can have in order to be sent to Fidelis. 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