CrowdStrike
Intel Indicators Add-on

Installation and Configuration Guide

V2-7-20-TS

Overview

This document outlines the deployment and configuration of the technology add-on for CrowdStrike Falcon Intel Indicators.

This technical add-on (TA) facilitates establishing a connecting to CrowdStrike's OAuth2 authentication-based Intel Indicators API to collect and index intelligence indicator data into Splunk for further analysis and utilization. This is a replacement for the previous TA "CrowdStrike Falcon Intelligence Add-on" (https://splunkbase.splunk.com/app/3945/#/overview) and does not serve nor install as an upgrade.

The major differences for the Intel Indicators Add-on vs the Intelligence Add-on are:

	Intel Indicators Add-on	Intelligence Add-on
API Credentials	OAuth2 Only	Legacy Only
Cloud Environments	US Commercial US Commercial 2 US GovCloud EU Cloud	US Commercial
Include Deleted Indicators	Supported	n/a
Indicator Update Field	Provided	n/a
Splunk: Python 3	Supported	Not Supported

Multitenancy - This TA is able to have multiple independent inputs enabled at the same time, each collecting data from different Falcon Instances and storing it in independent indexes.

Contents:

Getting Started

Prior to deploying the CrowdStrike Falcon Intel Indicators Add-on ensure the following:

1. The latest version of the TA has been downloaded from Splunkbase
2. All Splunk systems that the TA will be deployed to have been identified
3. An account with proper access to identified Splunk systems is available
4. CrowdStrike support has enabled the Event Streams API for the instance (this API is disabled by default)
5. Properly scoped API credentials have been created and recorded from the Falcon UI
6. Any custom indexes being used have been created on the appropriate systems
7. (optional) – If the communication between Splunk and the Falcon platform will traverse a proxy server then appropriate configurations should be taken into account. If the connection will need to authenticate to the proxy then appropriate credentials should be created and available.

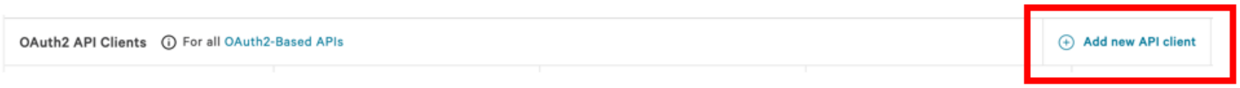
Enable Access to the Intel Indicators API

*Note this process is not required if there is an existing API client with proper access but it is recommended to leverage a dedicated account for the TA.

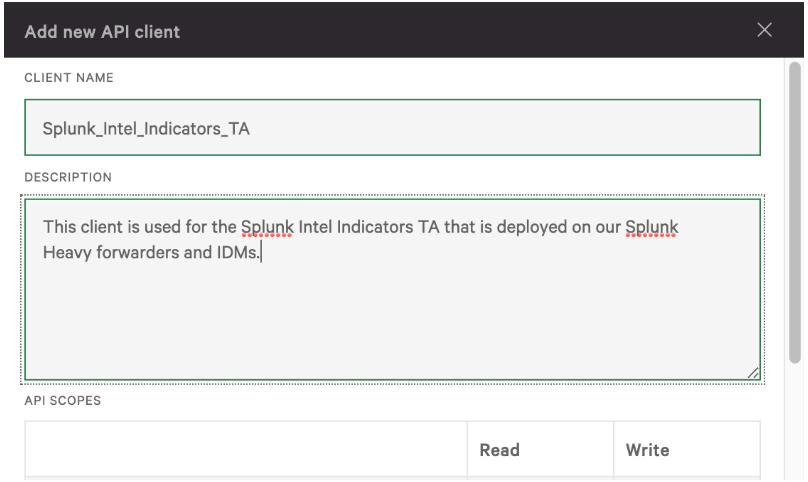
1. Log into the Falcon UI with an account that has administrator level permissions

2. Navigate to ‘Support’, ‘API Clients and Keys’ in the Falcon menu:

3. Select ‘Add new API Client’ to the right of ‘OAuth2 API Clients’:



4. Provide a client name and description (recommended):



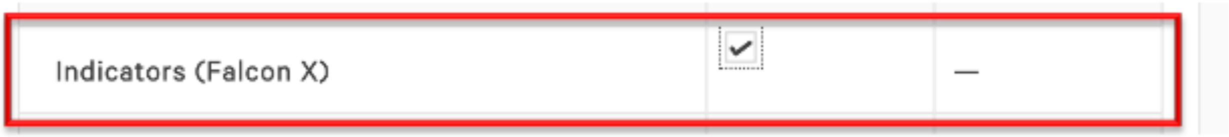
CLIENT NAME

Splunk_Intel_Indicators_TA

DESCRIPTION

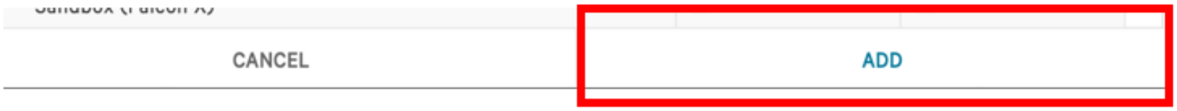
This client is used for the Splunk Intel Indicators TA that is deployed on our Splunk Heavy forwarders and IDMs.

5. Under ‘API Scopes’ select the ‘Read’ check box next to ‘Indicators (Falcon X)’:

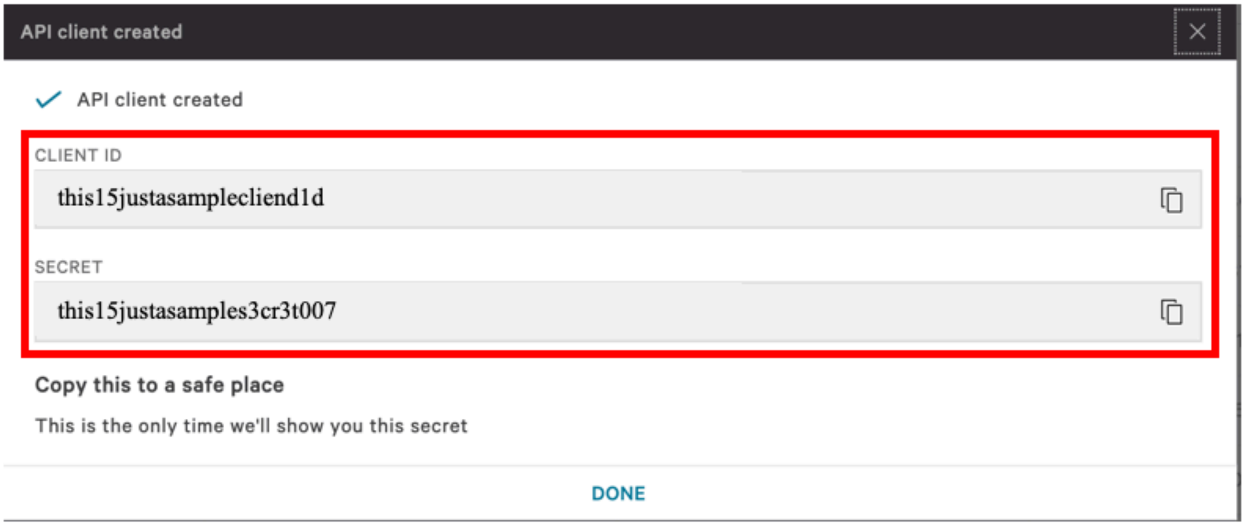


Indicators (Falcon X) ☑ —

6. Click ‘ADD’ to create the client:



7. A pop-up window will appear with the newly created Client ID and Secret. **Ensure to record the secret correctly and store it in a safe place as this is the only time it will be visible.**



API client created

✓ API client created

CLIENT ID

this15justasamplecliend1d

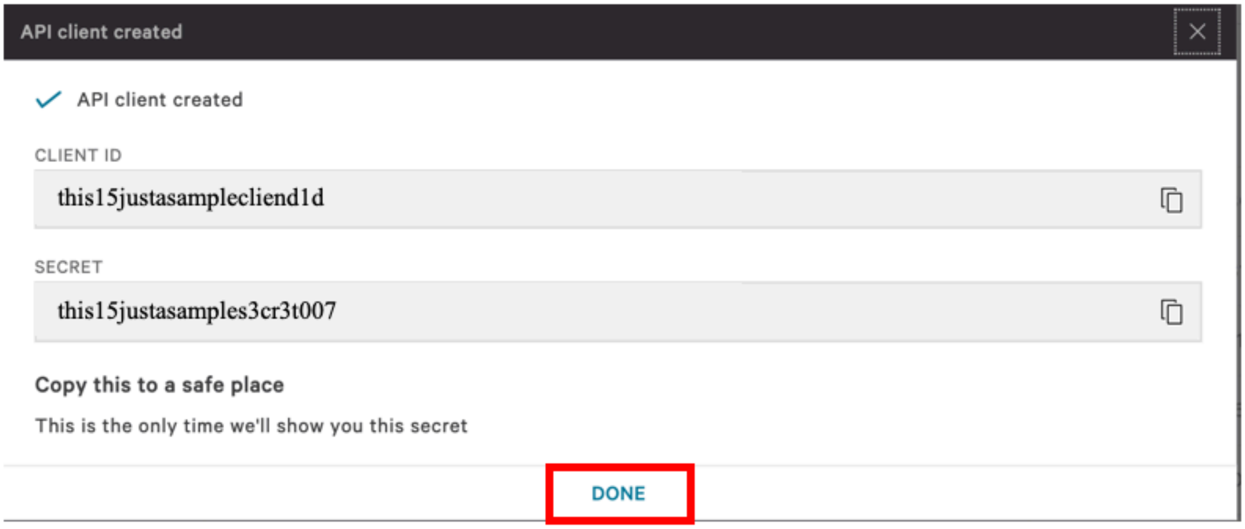
SECRET

this15justasamples3cr3t007

Copy this to a safe place

This is the only time we'll show you this secret

8. Once the credentials have successfully be copied to a safe and secure location click ‘DONE’ to close the window:



API client created

✓ API client created

CLIENT ID

this15justasamplecliend1d

SECRET

this15justasamples3cr3t007

Copy this to a safe place

This is the only time we'll show you this secret

Proxy Considerations

The CrowdStrike Technical Add-On establishes a secure persistent connection with the Falcon cloud platform. In some environments network devices may impact the ability to establish and maintain a secure persistent connection and as such these devices should be taken into account and configuration modifications should be done when necessary.

Ensure that the API URLs/IPs for the CrowdStrike Cloud environment(s) are accessible by the Splunk Heavy forwarder. For a complete list of URLs and IP address please reference CrowdStrike's API documentation.

The current base URLs for OAuth2 Authentication per cloud are:

US Commercial Cloud	: https://api.crowdstrike.com
US Commercial Cloud 2	: https://api.us-2.crowdstrike.com
US GovCloud	: https://api.laggar.gcw.crowdstrike.com
EU Cloud	: https://api.eu-1.crowdstrike.com

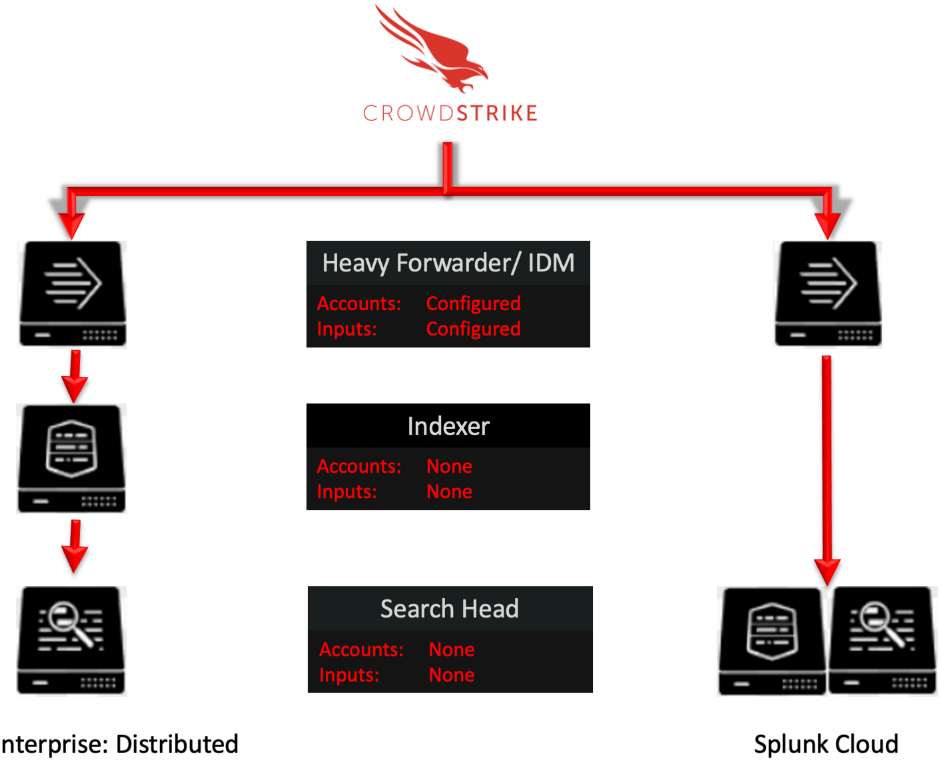
Splunk Architecture

Splunk Search Head(s) and Splunk Cloud: The TA should be installed to provide field mapping and search macro support. These are often required to support CrowdStrike Apps. The TA should be deployed without any accounts or inputs configured and any search macros should be properly configured for use.

Splunk Indexer(s): The TA can be installed to provide field mapping and search macro support. The TA should be deployed without any accounts or inputs configured and any search macros should be properly configured for use. If a custom index is going to be used, then it should be created here.

Splunk Heavy Forwarder(s) & Information Data Managers (IDMs): The TA should be installed here as this is where the data from the Streaming API will be collected. The appropriate accounts or inputs should be properly configured for data collection. If the Heavy Forwarder is storing events prior to forwarding them to the Indexer and a custom index is being used, ensure that the index has been created on both the Heavy Forwarder as well as the Indexer(s).
Note: Due to python requirements the TA can only be installed on Heavy Forwarders and IDMs.

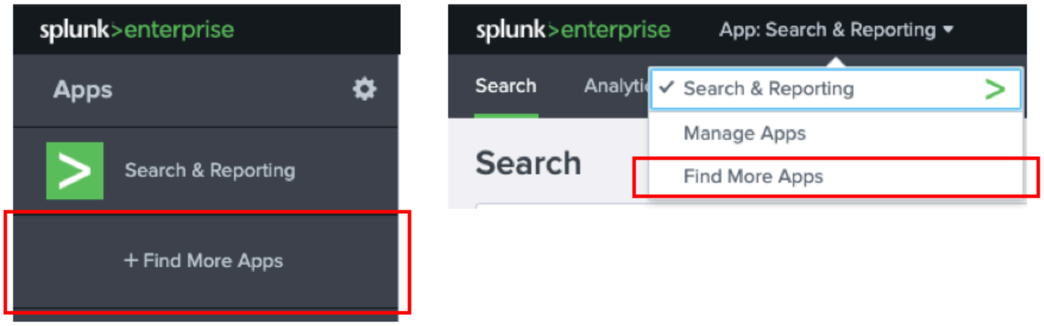
The following diagram shows the flow of data from the Streaming API and the Event Streams TA configuration within a distributed Splunk Enterprise and Splunk Cloud environment:



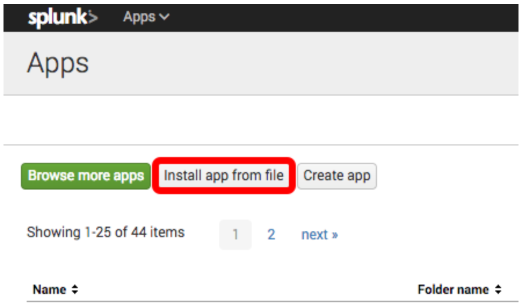
Initial Installation: Heavy Forwarders, Information Data Managers and Search Heads

PERFORMING THIS ACTION REQUIRES A SYSTEM RESTART

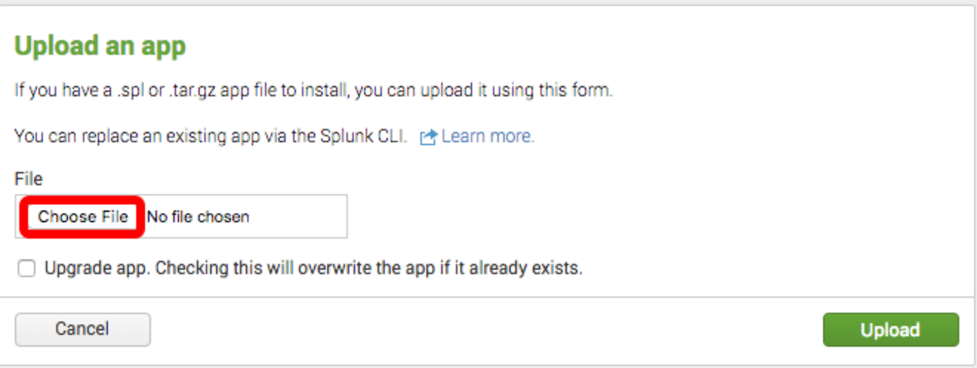
1. From the Splunk menu select 'Manage Apps'



2. From the Manage Apps menu select 'Install app from file'



3. From the 'Upload an app' window, select 'Choose File' *note if this action will upgrade an existing installation check the 'Upgrade app' selection as well.



Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

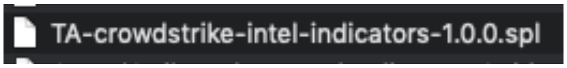
You can replace an existing app via the Splunk CLI. Learn more.

File

Choose File No file chosen

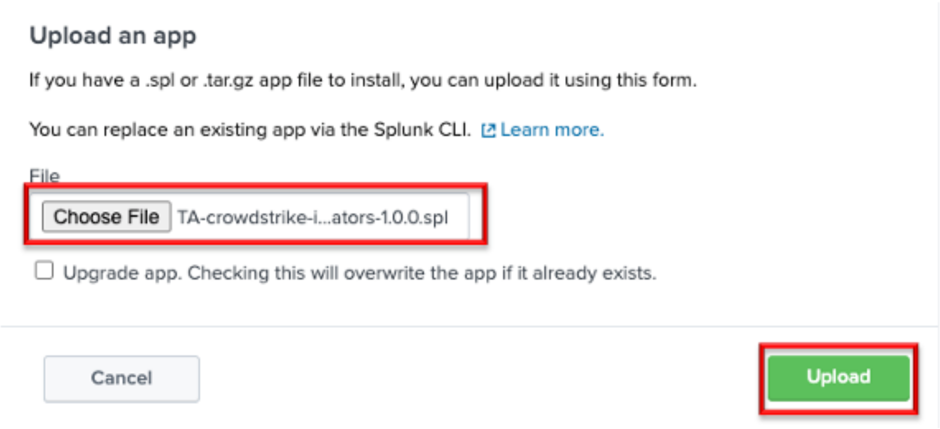
□ Upgrade app. Checking this will overwrite the app if it already exists.

4. Select the downloaded Falcon Event Streams add-on file



TA-crowdstrike-intel-indicators-1.0.0.spl

5. Once the file is selected click ‘Upload’ to upload the add-on to system. *Note this will need to be performed on all in-scope Heavy Forwarders and Search Heads identified in the prerequisite section.



Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. Learn more.

File

Choose File TA-crowdstrike-i...ators-1.0.0.spl

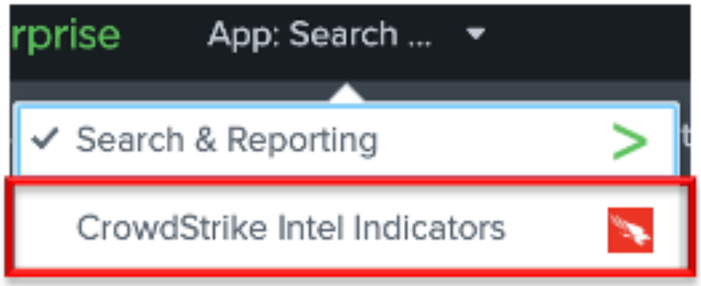
□ Upgrade app. Checking this will overwrite the app if it already exists.

6. Once the add-on has been installed the system will require a restart for the add-on to complete installation.

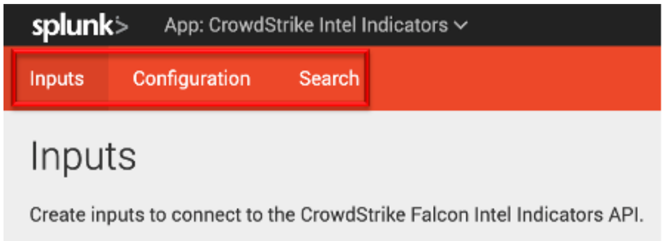
----This concludes the Initial Installation / Re-Installation / Manual Update process----

Heavy Forwarder/ Information Data Manager Configuration

1. From the Splunk drop down menu select the ‘Technical Add-on from CrowdStrike’



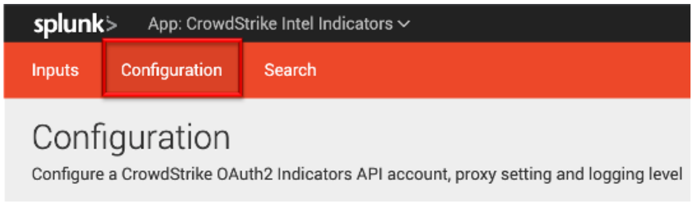
2. There are three sub menus within the add-on: ‘Inputs’, ‘Configuration’ and ‘Search’



Inputs

Create inputs to connect to the CrowdStrike Falcon Intel Indicators API.

3. Select the submenu ‘Configuration’

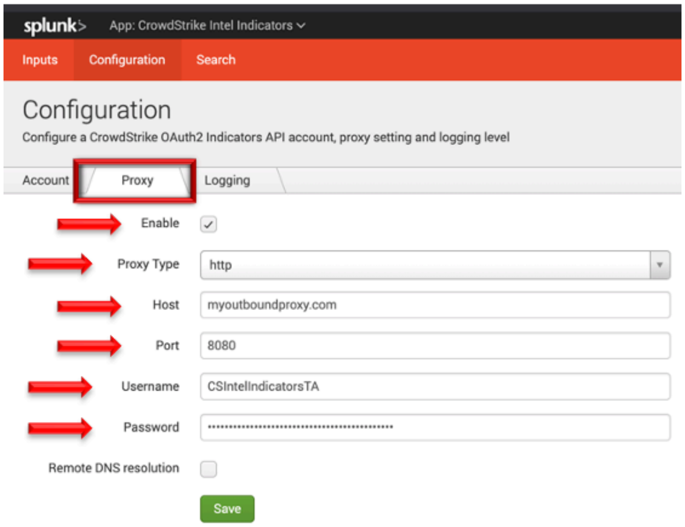


Configuration

Configure a CrowdStrike OAuth2 Indicators API account, proxy setting and logging level

Proxy Configuration (Optional)

Select the 'Proxy' tab under 'Configuration' - Check the 'Enable' checkbox, select the Proxy Type from the drop down, enter the proxy host name, the proxy port and the credentials to allow communication.



Configuration

Configure a CrowdStrike OAuth2 Indicators API account, proxy setting and logging level

Enable ☑

Proxy Type: http

Host: myoutboundproxy.com

Port: 8080

Username: CSIntelIndicatorsTA

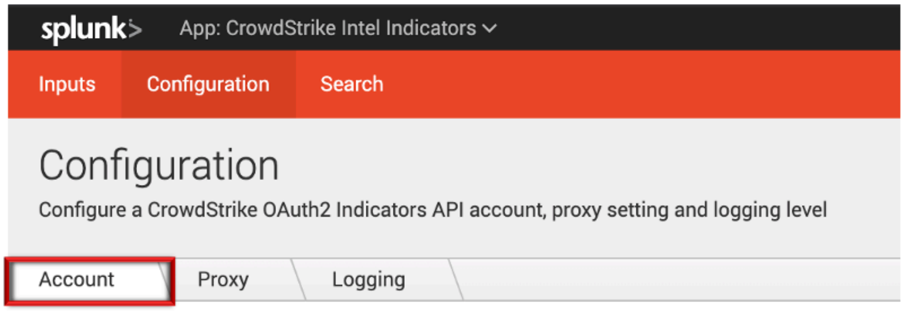
Password: ••

Remote DNS resolution ☐

Intel Indicators Account Configuration

This TA only supports connections to the Event Streams OAuth2 based API.

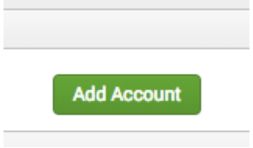
1. Select the 'CrowdStrike Account' tab under 'Configuration'



Configuration

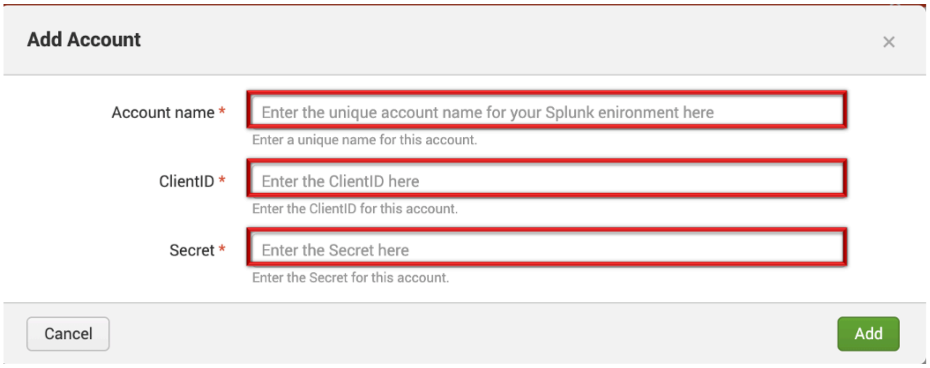
Configure a CrowdStrike OAuth2 Indicators API account, proxy setting and logging level

2. On the right-hand side select 'Add Account'



3. Configure the account for the Event Stream by providing the following:

    - **Account Name** – This is a unique name for the account within Splunk
    - **ClientID** – This is the ClientID for the API credential created
    - **Secret** – This is the Secret for the API credential created



Add Account

Account name * Enter the unique account name for your Splunk enironment here

Enter a unique name for this account.

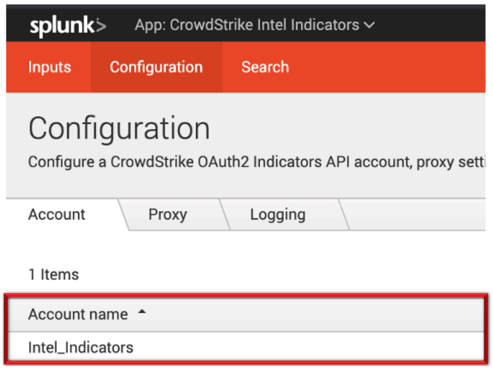
ClientID * Enter the ClientID here

Enter the ClientID for this account.

Secret * Enter the Secret here

Enter the Secret for this account.

4. Once the information has been entered correctly click ‘Add’ to create the account. ***Note the TA does not authenticate or validate the credentials entered.**



Configuration

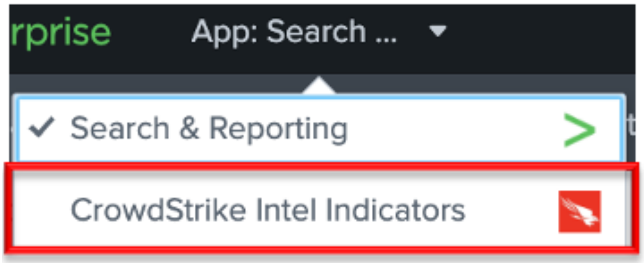
Configure a CrowdStrike OAuth2 Indicators API account, proxy setti

1 Items

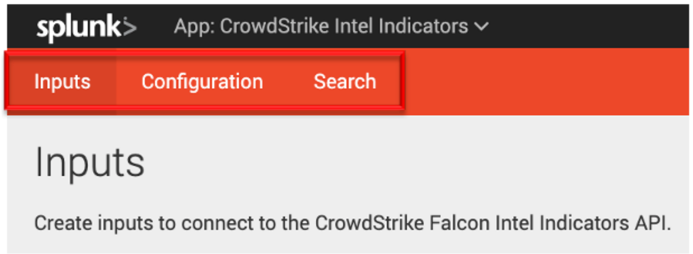
Account name
Intel_Indicators

Intelligence Indicators TA Inputs Configuration

1. From the Splunk drop down menu select the ‘CrowdStrike Intel Indicators’

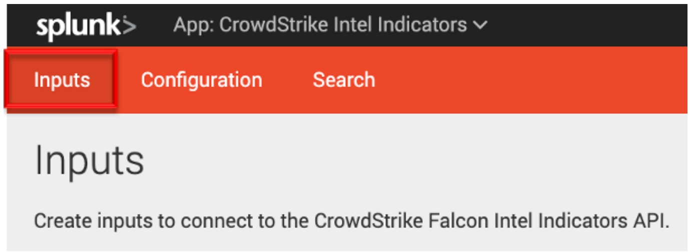


2. There are three sub menus within the add-on: ‘Inputs’, ‘Configuration’ and ‘Search’



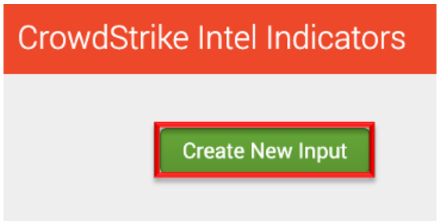
Create inputs to connect to the CrowdStrike Falcon Intel Indicators API.

3. Select the ‘Inputs’ sub menu

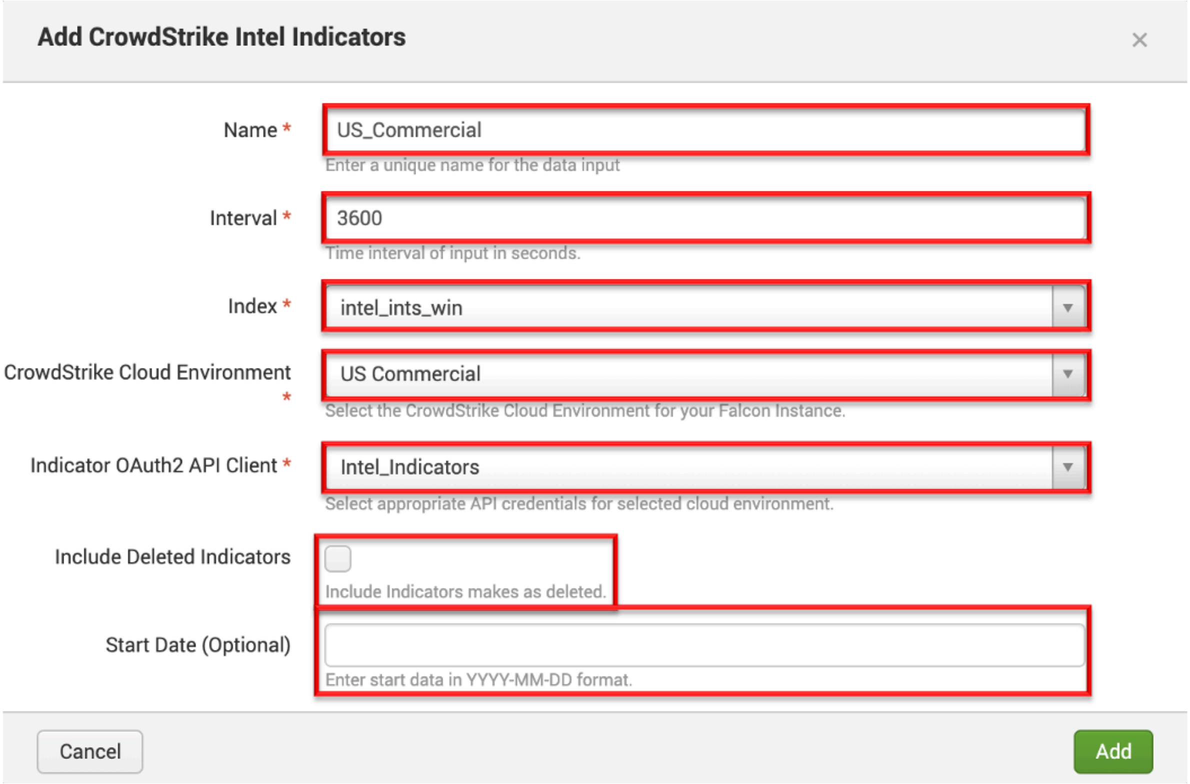


Create inputs to connect to the CrowdStrike Falcon Intel Indicators API.

4. Select the ‘Create New Input’ from the top right



5. Configure the Intel Indicator input by indicating the following:
   - **Name** – The Splunk unique name for the input being configured
   - **Interval** – Enter how often the TA should query the API (represented in seconds) *Note it is not recommended to run the TA at intervals shorter than 5 minutes
   - **Index** – The index that the data will be stored in (must an existing index)
   - **Cloud Environment** – The CrowdStrike cloud environment the Falcon instance being connected to resides in
   - **OAuth2 API Client** – The corresponding API credential for the Falcon instance in the select Cloud Environment
   - **Include Deleted Indicators** – Select to include indicators that are marked as 'Deleted'
   - **Start Date** – (optional and only for new inputs) Enter a date in YYYY-MM-DD format to begin the collection starting on that specific date



Add CrowdStrike Intel Indicators

Name * US_Commercial
Enter a unique name for the data input

Interval * 3600
Time interval of input in seconds.

Index * intel_ints_win

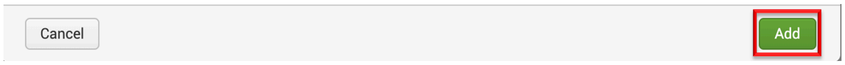
CrowdStrike Cloud Environment * US Commercial
Select the CrowdStrike Cloud Environment for your Falcon Instance.

Indicator OAuth2 API Client * Intel_Indicators
Select appropriate API credentials for selected cloud environment.

Include Deleted Indicators □
Include Indicators makes as deleted.

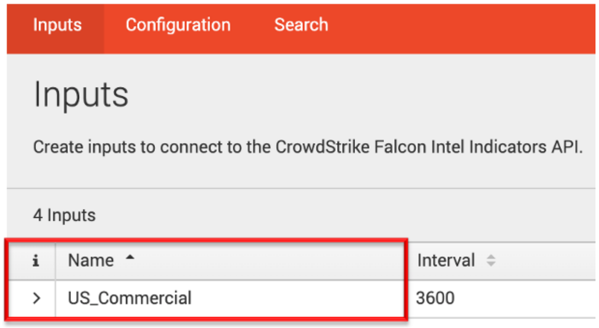
Start Date (Optional)
Enter start data in YYYY-MM-DD format.

6. Once the Input parameters have been correctly configured click ‘add’*



***Newly created inputs are enabled by default**

7. Validate the newly created input information and ensure it is set to enabled/disabled as appropriate



Inputs

Create inputs to connect to the CrowdStrike Falcon Intel Indicators API.

4 Inputs

i	Name ▲	Interval ⇕
>	US_Commercial	3600

This concludes the Heavy Forwarder/Information Data Manager Configuration process

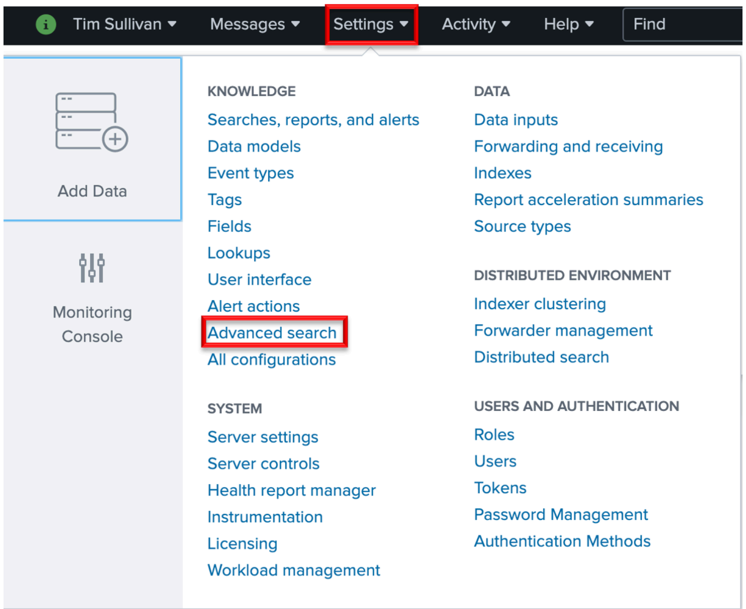
Search Macro Configuration

Search macros are reusable chunks of Search Processing Language (SPL) that you can insert into other searches. Search macros can be any part of a search, such as an eval statement or search term, and do not need to be a complete command. You can also specify whether the macro field takes any arguments.
https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros

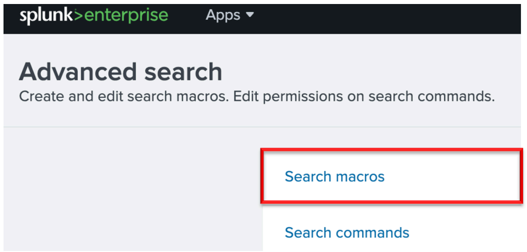
The Intel Indicator TA contains a search macro named `cs_ii_get_index` (CrowdStrike Intel Indicator get index) that points to the index(es) that contain the data received from the Intel Indicator API. The default for this search macro is to point to all indexes to search for data but should be adjusted to reflect the specific index(es) that the Heavy Forwarder/IDMs are pushing the data to.

The search macro can be modified as follows:

1. Select the 'Settings' dropdown menu in the Splunk bar and select 'Advanced Search'



2. Select 'Search macros'

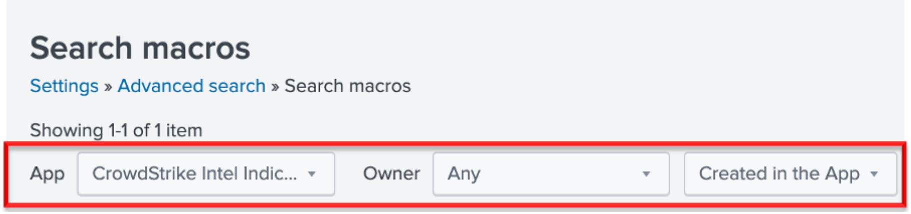


Advanced search

Create and edit search macros. Edit permissions on search commands.

3. Configure the search settings as follows:

- **App** - CrowdStrike Intel Indicators
- **Owner** - Any
  - Created in the App



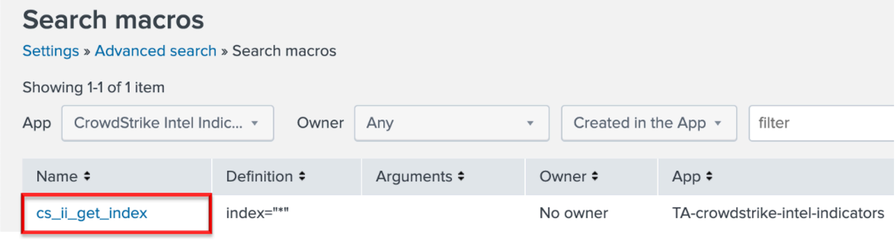
Search macros

Settings » Advanced search » Search macros

Showing 1-1 of 1 item

App CrowdStrike Intel Indic... Owner Any Created in the App

4. To modify the search macro, click on the name: “cs_ii_get_index”



Search macros

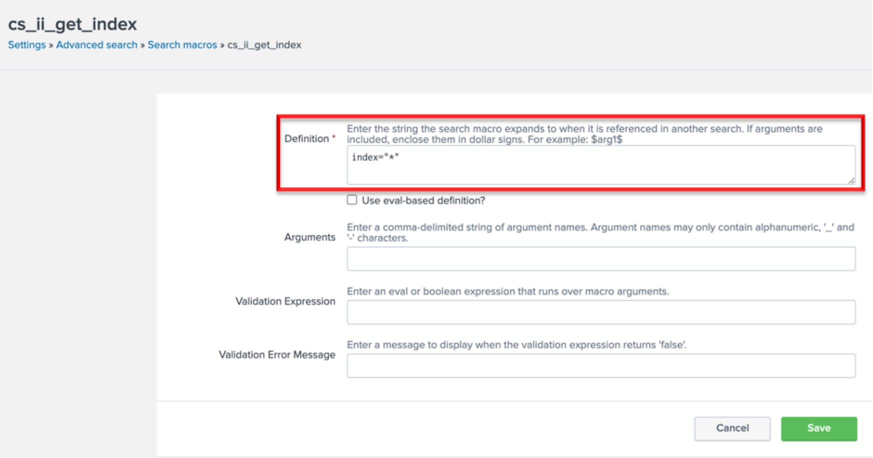
Settings » Advanced search » Search macros

Showing 1-1 of 1 item

App CrowdStrike Intel Indic... Owner Any Created in the App filter

Name ⬍	Definition ⬍	Arguments ⬍	Owner ⬍	App ⬍
cs_ii_get_index	index="*"		No owner	TA-crowdstrike-intel-indicators

5. Under ‘Definition’ enter the index or indexes that contain the Event Stream data to the right of “index=” – separate multiple indexes with the “OR” Boolean.



cs_ii_get_index

Settings » Advanced search » Search macros » cs_ii_get_index

Definition * Enter the string the search macro expands to when it is referenced in another search. If arguments are included, enclose them in dollar signs. For example: $arg1$

```
index="*"
```

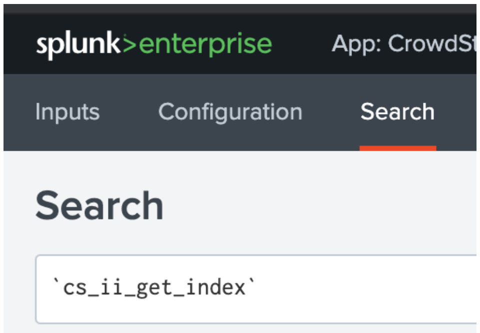
□ Use eval-based definition?

Arguments Enter a comma-delimited string of argument names. Argument names may only contain alphanumeric, '_' and '-' characters.

Validation Expression Enter an eval or boolean expression that runs over macro arguments.

Validation Error Message Enter a message to display when the validation expression returns 'false'.

6. To leverage the search macro, open a search window within Splunk and enter the search macro enclose with backquotes: `cs_get_ii_index` (the backquote key is the same key as a tilde on a US keyboard layout and should not be confused with a single quote)



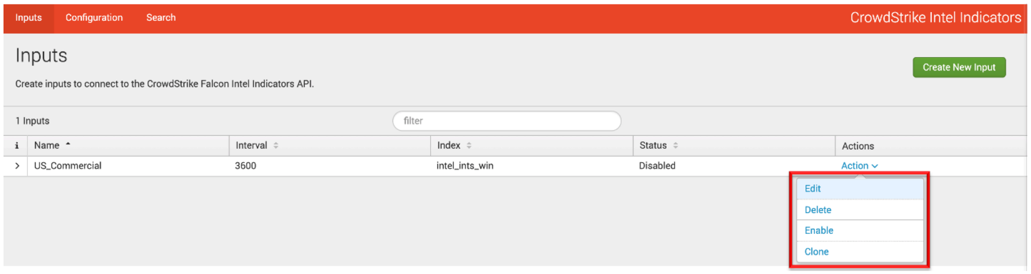
```
`cs_ii_get_index`
```

This concludes the Search Macro Configuration process

Modify, Remove or Clone Existing Settings

Configuration: Inputs

1. Under the "Inputs" tab, under the "Action" column for an input, there is a pull-down menu with the options for "Edit", "Delete", "Enable" / "Disable" or "Clone"



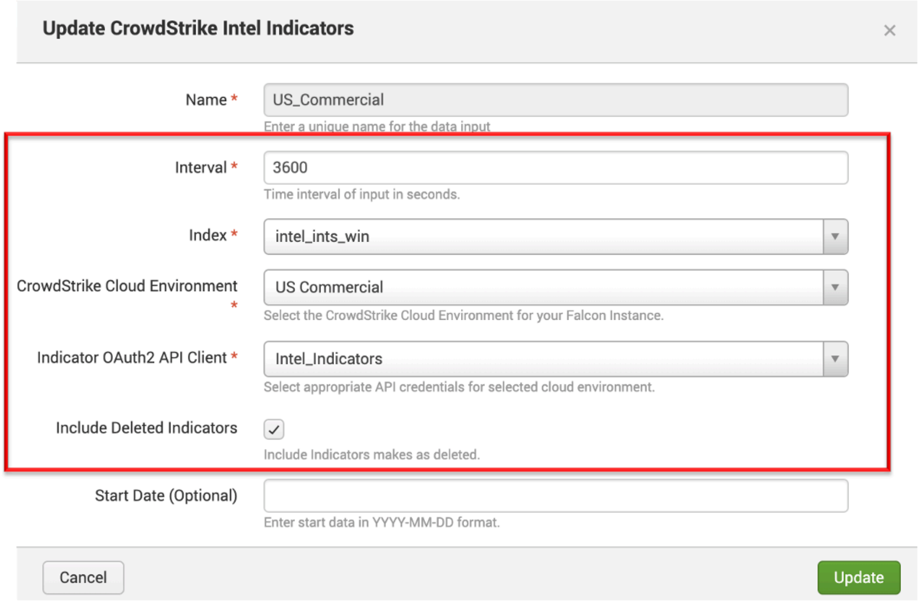
Inputs

Create inputs to connect to the CrowdStrike Falcon Intel Indicators API.

1 Inputs

i	Name	Interval	Index	Status	Actions
>	US_Commercial	3600	intel_ints_win	Disabled	Action

2. **Editing:** allows for changing all the input fields with the exception of the input's original name - *note editing the 'Start Date' field will have no impact on the Input



Update CrowdStrike Intel Indicators

Name * US_Commercial
Enter a unique name for the data input

Interval * 3600
Time interval of input in seconds.

Index * intel_ints_win

CrowdStrike Cloud Environment * US Commercial
Select the CrowdStrike Cloud Environment for your Falcon Instance.

Indicator OAuth2 API Client * Intel_Indicators
Select appropriate API credentials for selected cloud environment.

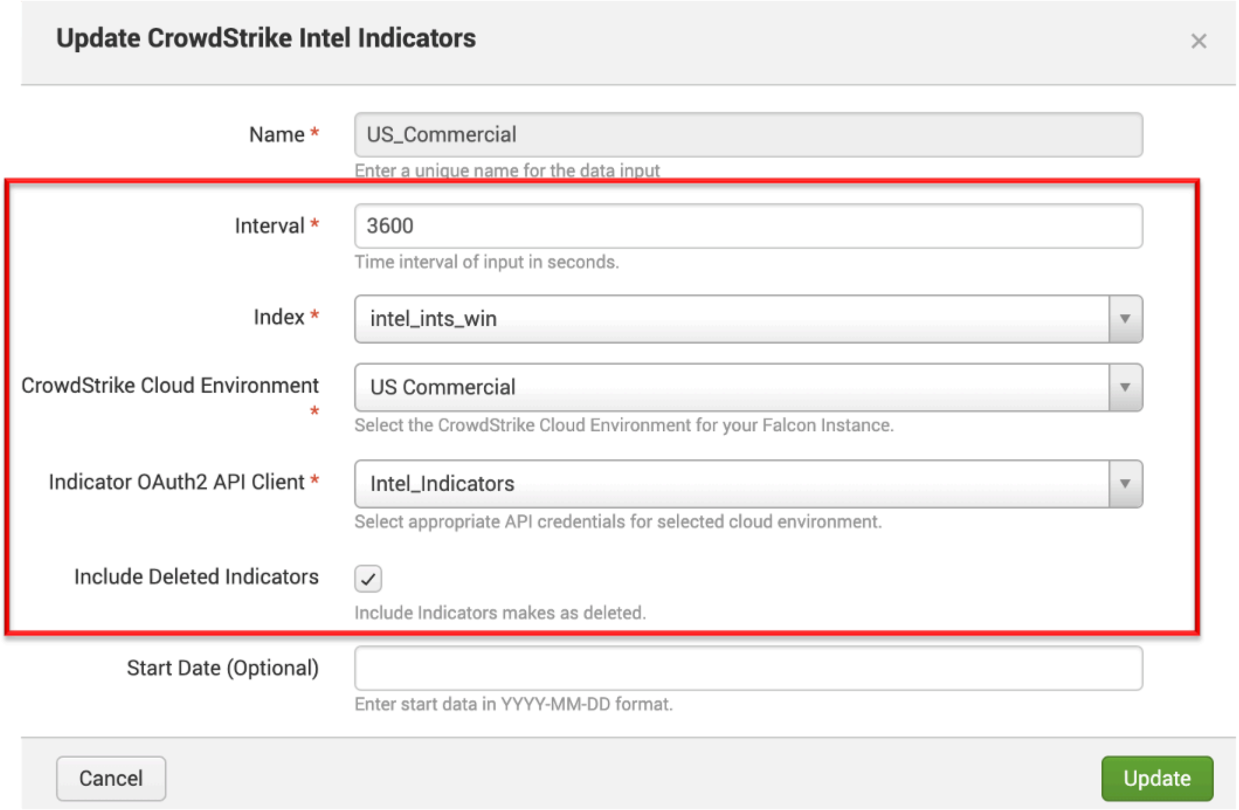
Include Deleted Indicators ☑
Include Indicators makes as deleted.

Start Date (Optional)
Enter start data in YYYY-MM-DD format.

3. **Deleting:** allows for the input to be deleted

4. **Enabling/Disabling:** allows the input to enabled or disabled depending on the current state – the initial state is enabled

5. **Cloning**: allows all the settings of the input to be replicated with the exception of the "name" – field



Update CrowdStrike Intel Indicators

Name * US_Commercial
Enter a unique name for the data input

Interval * 3600
Time interval of input in seconds.

Index * intel_ints_win

CrowdStrike Cloud Environment * US Commercial
Select the CrowdStrike Cloud Environment for your Falcon Instance.

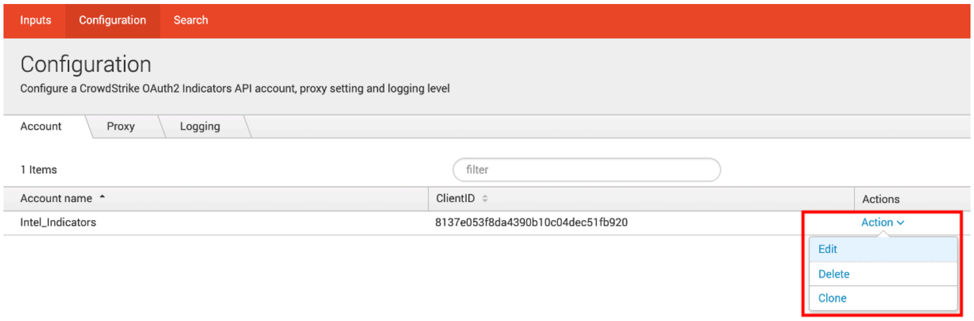
Indicator OAuth2 API Client * Intel_Indicators
Select appropriate API credentials for selected cloud environment.

Include Deleted Indicators ☑
Include Indicators makes as deleted.

Start Date (Optional)
Enter start data in YYYY-MM-DD format.

Configuration: Accounts

1. Under the “Configuration” sub menu, “Account” tab, and the “Actions” column for an account, there is a pull-down menu with the options for “Edit”, “Delete” or “Clone



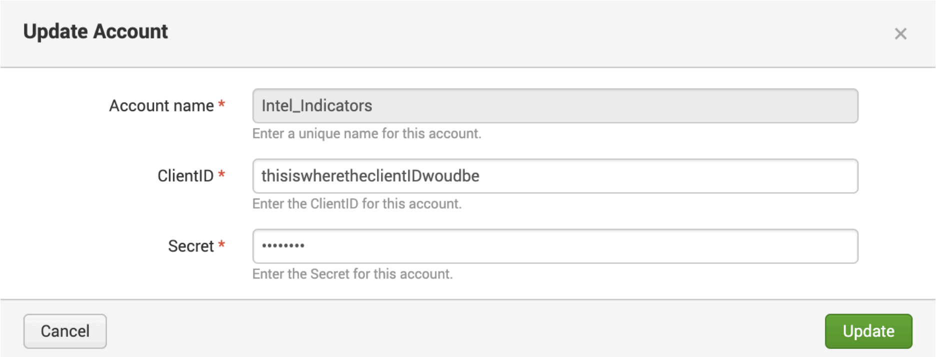
Configuration

Configure a CrowdStrike OAuth2 Indicators API account, proxy setting and logging level

1 Items

Account name	ClientID	Actions
Intel_Indicators	8137e053f8da4390b10c04dec51fb920	Action

2. **Editing:** allows for the changing of the ClientID and Secret - the account name is NOT able to be edited once created



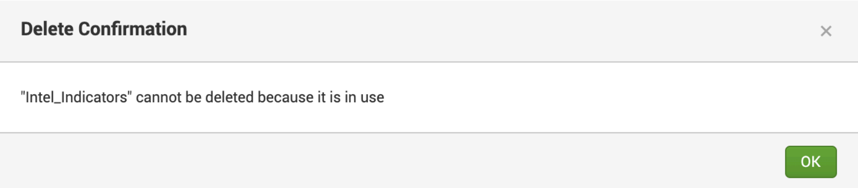
Update Account

Account name * Intel_Indicators
Enter a unique name for this account.

ClientID * thisiswheretheclientIDwoudbe
Enter the ClientID for this account.

Secret * ••••••••
Enter the Secret for this account.

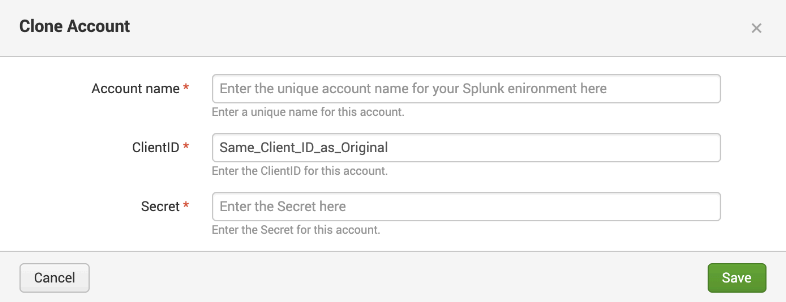
3. **Deleting:** allows a configuration to be deleted however it has to be removed from all inputs before this can be accomplished



Delete Confirmation

"Intel_Indicators" cannot be deleted because it is in use

4. **Cloning**: allows for a second account to be created with the same ClientID as the original but requires a new Account Name and Secret to be entered



Clone Account

Account name * Enter the unique account name for your Splunk eironment here

Enter a unique name for this account.

ClientID * Same_Client_ID_as_Original

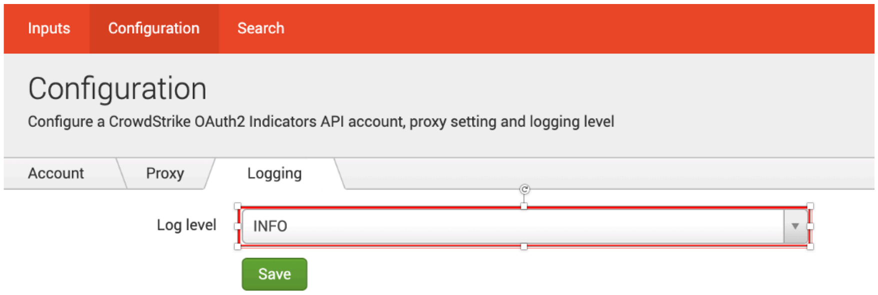
Enter the ClientID for this account.

Secret * Enter the Secret here

Enter the Secret for this account.

Configuration: Logging

1. Under the “Configuration” sub menu, “Account” tab, and the “Actions” column for an account, there is a pull-down menu for setting the Log Level – which is ‘INFO’ by default

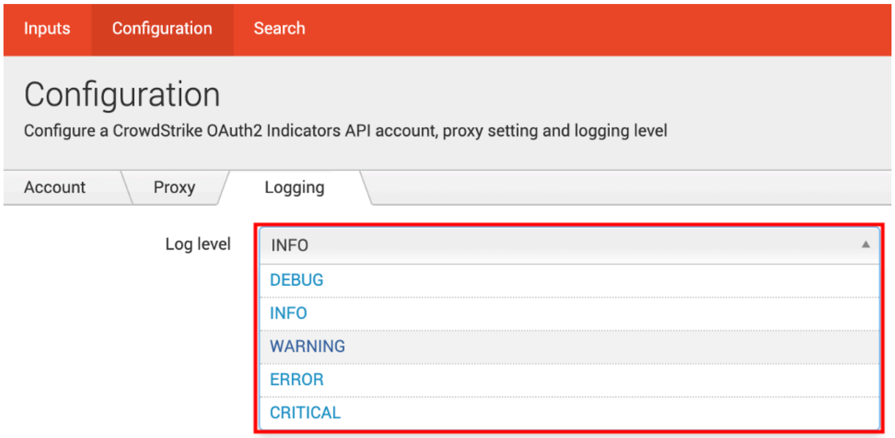


Configuration

Configure a CrowdStrike OAuth2 Indicators API account, proxy setting and logging level

Log level INFO

2. The TA provides the typical log levels available for a modular input. Those levels are (from most to least verbose): DEBUG, INFO, WARN, ERROR, FATAL.

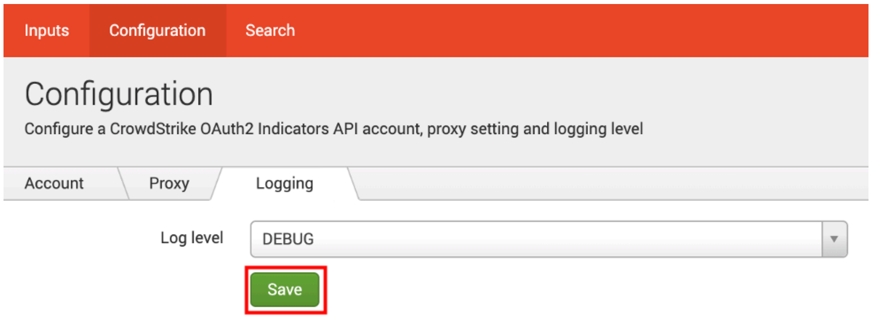


Configuration

Configure a CrowdStrike OAuth2 Indicators API account, proxy setting and logging level

Log level INFO

3. Select the desired Log Level from the drop down and click “Save”



Configuration

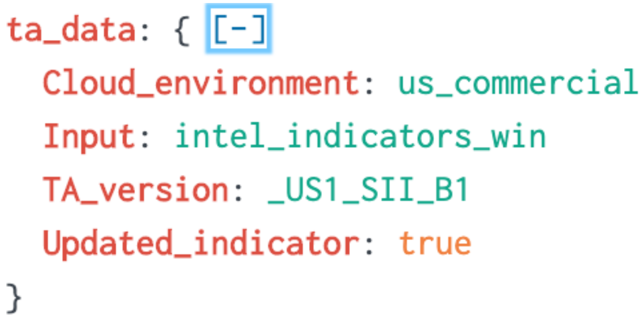
Configure a CrowdStrike OAuth2 Indicators API account, proxy setting and logging level

Log level DEBUG

Custom Fields

Custom Fields: ta_data

The Event Streams TA creates a custom information section and adds into all events to provide valuable information on the origin of the data and to assist in troubleshooting.



```
ta_data: { [-]
  Cloud_environment: us_commercial
  Input: intel_indicators_win
  TA_version: _US1_SII_B1
  Updated_indicator: true
}
```

- **ta_data** - The name of the data section that provides the custom TA data
- **Cloud_environment** – The cloud environment selected for the Input
- **Input** – The name of the configured Input that received the data
- **TA_version** – Data pulled from the TA configuration file and indicates the version of the TA
- **Updated_indicator** – Shows if the indicator was updated by checking if the last_updated field is greater than the published_date field

Troubleshooting and Support

CrowdStrike provides support for the TA's code, the functionality of that code and authentication to the API endpoint(s). The following topics fall outside of that scope:

1. Network connectivity issues unrelated to authentication response from the CrowdStrike API endpoint
2. Tagging and CIM mapping (these are considered feature requests and will be evaluated by the integrations team)

Checking Configuration

Unable to establish connection:

1. Ensure that the Event Stream API has been enabled for the CID
2. Ensure that the proper Cloud Environment has been selected
3. Ensure that the OAuth2 credential has been scoped correctly
4. Ensure that the OAuth2 credential has been entered correctly
5. Ensure that network devices aren't blocking or tearing down the connection

No data is present:

1. Ensure that the Input is enabled
2. Ensure that the Index has been created on the Indexer(s)
3. If leveraging the Search Macro ensure that it's been configured correctly
4. Ensure that events have taken place since the connection was established

Getting Support

Prior to contacting CrowdStrike support please review the following:

Initial Deployment

1. Ensure that the OAuth2 credential information have been entered correctly
2. Ensure that the OAuth2 credential has been scoped correctly
3. Set the TA log level to 'DEBUG'
4. Repeat and record the action(s) that are associated with the issue you are reporting
5. Download the all log files containing 'ta_crowdstrike_intel_indicators' under the $Splunk/var/log/splunk/ directory
6. Record the following information about the Splunk system:
    - Splunk environment type
    - Splunk version
    - TA version
7. Identify the types of networks devices that the connection will traverse and ensure that they have been properly configured
8. Collect API audit logs from the Falcon instance for the time frame when the issue is occurring
9. Navigate to https://supportportal.crowdstrike.com/
10. Provide (at a minimum) the information from steps 4-9

Existing Deployment

1. Set the TA log level to 'DEBUG'
2. Disable and re-enable TA Inputs
3. Download the all log files containing 'ta_crowdstrike_intel_indicators' under the $Splunk/var/log/splunk/ directory
4. Record the following information about the Splunk system:
    - When was the last successful connection
    - If a TA or Splunk update performed around the same time frame
    - Splunk environment type
    - Splunk version
    - TA version
5. Identify the types of networks devices that the connection will traverse and ensure that they are still properly configured
6. Collect API audit logs from the Falcon instance for the time frame when the issue began occurring
7. Navigate to https://supportportal.crowdstrike.com/
8. Provide (at a minimum) the information from steps 3-6