CROWDSTRIKE

CrowdStrike Falcon Devices Add-on for Splunk

Installation and Configuration Guide v3.1+

TPS822310

Table of Contents

Introduction

This guide covers the deployment, configuration and usage of the CrowdStrike Falcon Devices Technical Add-on (TA) for Splunk.

The CrowdStrike Falcon Devices Technical Add-on for Splunk allows CrowdStrike customers to retrieve Falcon device data from the CrowdStrike Hosts API and index it into Splunk.

To get more information about this API, please refer to the API documentation which can be found in the CrowdStrike Falcon UI: https://falcon.crowdstrike.com/support/documentation/84/host-and-host-group-management-apis.

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. It also provides an input type that can be used by Falcon Flight Control customers.

Requirements

The following are the requirements to leverage this technical add-on:

1. An active subscription to the CrowdStrike Insight or Prevent modules.

2. A Splunk Heavy forwarder, input Data Manager (IDM) or Splunk Cloud instance that supports modular input data ingestion.

3. A Splunk account with proper access to deploy and configure technical add-ons.

4. A properly scoped API credential or proper access to the CrowdStrike Falcon instance to create one.

5. The base URL for the CrowdStrike Cloud environment that the Falcon instance resides in.

Major Modifications

The following are some of the major modifications made to this version of the add-on that differ from previous versions:

1. All input timestamps are now use the 'modified_timestamp' value for the event time as well as checkpoint values.

2. 'On-line Only' selections no longer use a time-based determination to only collect devices that have been on-line since the last collection but instead use a dedicated API endpoint to identify systems on-line at the time of the collection.

Getting Started

API Endpoint(s), Filter(s) and Timestamp(s):

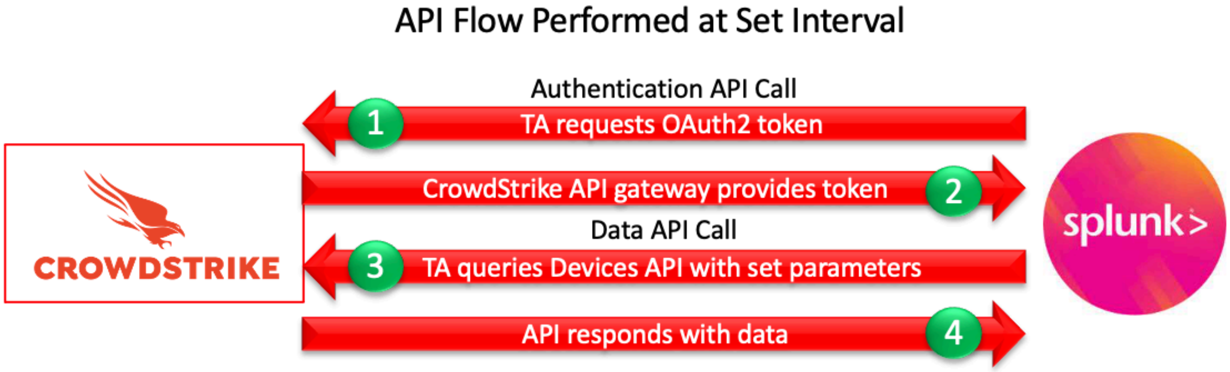
The TA will make API calls to some or all of the following endpoints. Some API calls may leverage different filter fields depending on the selected options.

API Endpoint	Filter fields(s)
/oauth2/token	
/devices/queries/devices-scroll/v1	modified_timestamp
/devices/entities/online-state/v1	
/devices/entities/devices/v1	

The event timestamp used by the TA is the '**modified_timestamp**' value. This value will be what Splunk uses for the _time value and can be found in the event data under '**falcon_device.modified_timestamp**'.

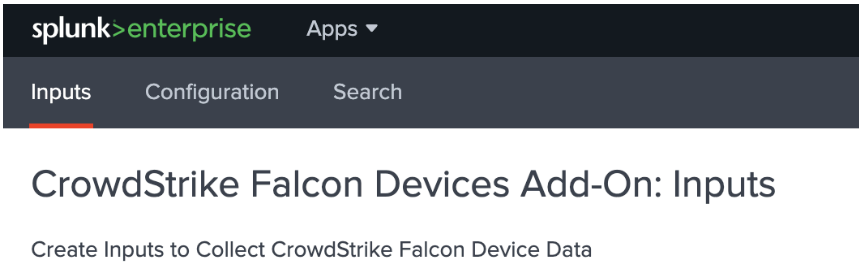
High Level API Call Flow

The CrowdStrike Falcon Devices TA performs the same API calls at each time interval that's configured within the TA input:


API Flow Performed at Set Interval
Authentication API Call
1
TA requests OAuth2 token
CROWDSTRIKE
CrowdStrike API gateway provides token
2
splunk>
Data API Call
3
TA queries Devices API with set parameters
API responds with data
4

1. The TA will call the CrowdStrike API gateway with the configured credentials and request an OAuth2 authentication token that is valid for 30 minutes.
2. If the API credentials are valid the API gateway will respond to the TA with an Oauth2 token.
3. The TA will use the OAuth2 token to call the Devices API with the configured parameters.
4. The API will respond with whatever appropriate data matches the configured parameters.

Technical Add-On Layout



CrowdStrike Falcon Devices Add-On: Inputs

Create Inputs to Collect CrowdStrike Falcon Device Data

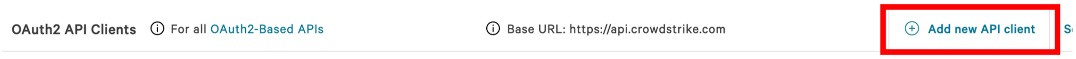
The CrowdStrike Falcon Devices TA has 3 tabs associated with it:

1. **Inputs** – The Inputs tab (only configure on a Splunk Heavy Forwarder or IDM) contains the connection configuration(s) that the TA uses to communicate with the API.
2. **Configuration** – The Configuration tab contains the API credential information, proxy server configuration information and logging level.
3. **Search** – A link to Splunk search that's specific to the TA.

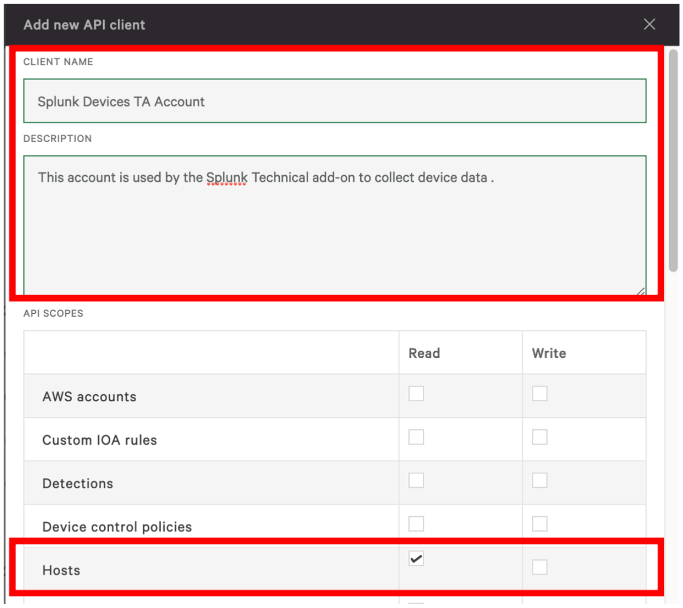
Creating/Validating the API Credential Scope

While the CrowdStrike Falcon Devices TA can leverage an existing OAuth2 based API credential, it is recommended that a dedicated credential be created and used. This can be accomplished by the following:

1. Access the CrowdStrike Falcon user interface (UI) with an account that is able to create API clients and keys
2. Navigate to ‘Support’>’API Client and Keys’ page
3. Create a new API client by selecting ‘Add new API client’ in the OAuth2 API client’s area


OAuth2 API Clients
For all OAuth2-Based APIs
Base URL: https://api.crowdstrike.com
Add new API client

4. Give the new API client a name and description (recommended) and under ‘API Scopes’ select the ‘Hosts’ scope and the ‘Read’ capability



CLIENT NAME

Splunk Devices TA Account

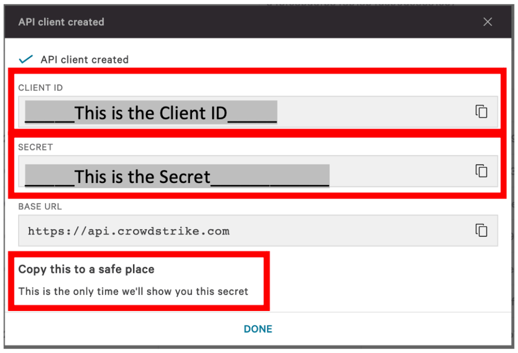
DESCRIPTION

This account is used by the Splunk Technical add-on to collect device data .

API SCOPES

	Read	Write
AWS accounts	□	□
Custom IOA rules	□	□
Detections	□	□
Device control policies	□	□
Hosts	☑	□

5. Select ‘Add’ once completed and a window will appear with the Client ID, Secret and the Base URL. NOTE: This is the only time the Secret will be visible – ensure it is recorded in a protected location.



API client created

✓ API client created

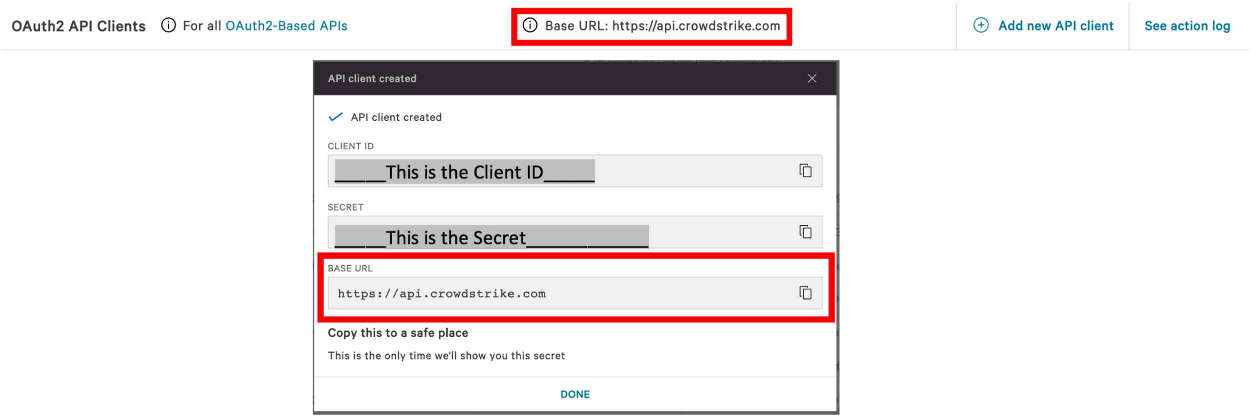
CLIENT ID
_____This is the Client ID_____

SECRET
_____This is the Secret____________

BASE URL
https://api.crowdstrike.com

Copy this to a safe place
This is the only time we'll show you this secret

6. In addition, make note of the ‘BASE URL’ value in either the API client created window or the ‘OAuth2 API client’ area as this will be used to determine the CrowdStrike Cloud the instance is in



ⓘ Base URL: https://api.crowdstrike.com

API client created

✓ API client created

CLIENT ID
_____This is the Client ID_____

SECRET
_____This is the Secret____________

BASE URL
https://api.crowdstrike.com

Copy this to a safe place
This is the only time we'll show you this secret

7. Select ‘Done’ to close the window and finish creating the credential

Proxy Considerations

The CrowdStrike Devices Technical Add-On establishes a secure connection with the Falcon cloud platform. In some environments network devices may impact the ability to establish and maintain a secure 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.

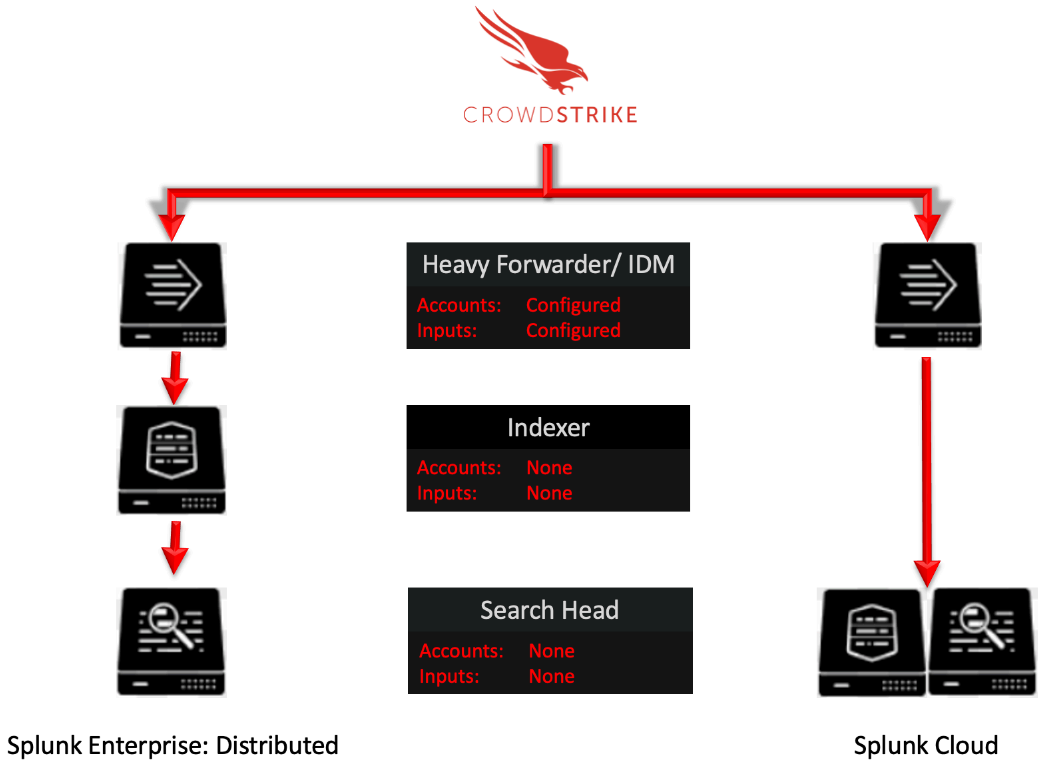
Splunk Indexer(s): The TA can be installed to provide field mapping and search macro support. The TA should be deployed without any accounts or inputs configured and any search macros should be properly configured for use. If a custom index is going to be used, then it should be created here.

Splunk Heavy Forwarder(s) & Information Data Managers (IDMs): The TA is required to be installed here as this is where the data from the Devices API will be collected. The appropriate accounts and inputs should be properly configured for data collection. Ensure that if a customer index is being used, which is highly recommended, that the index has been created on the indexer tier. If the Heavy Forwarder is storing events (not required but is an optional Splunk configuration) 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 configured for data collection on Heavy Forwarders and IDMs.

The following diagram shows the flow of data from the Devices API and the Falcon Device TA configuration within a distributed Splunk Enterprise and Splunk Cloud environment:

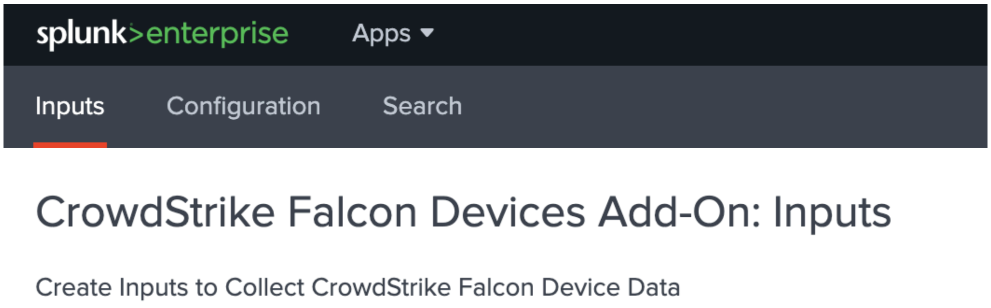


	Accounts:	Inputs:
Heavy Forwarder/ IDM	Configured	Configured
Indexer	None	None
Search Head	None	None

Configuring the TA

TA Layout

The TA contains 3 sections:



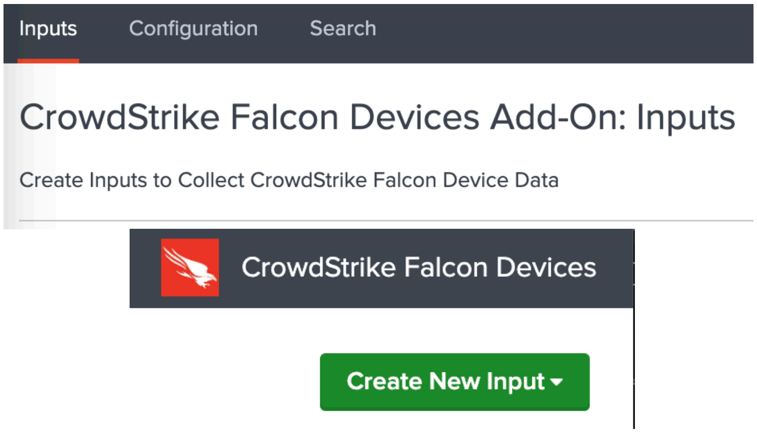
CrowdStrike Falcon Devices Add-On: Inputs

Create Inputs to Collect CrowdStrike Falcon Device Data

- The Inputs section
- The Configuration section
- The Search section

Inputs Section

The Inputs section is where inputs are configured, modified and listed. Prior to configuring any inputs an account needs to be created under the Configuration section (see below). The Inputs section contains a 'button' that will create a new input configuration in the far-right corner.

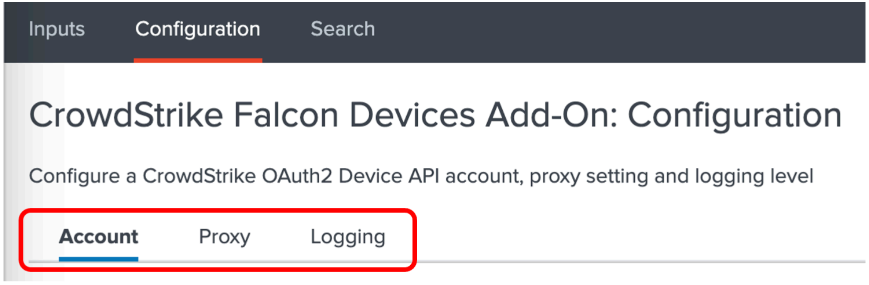


CrowdStrike Falcon Devices Add-On: Inputs

Create Inputs to Collect CrowdStrike Falcon Device Data

Configuration Section

The Configuration section contains 3 configuration tabs:



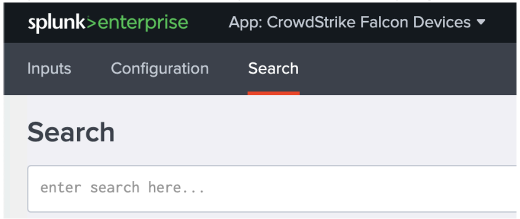
CrowdStrike Falcon Devices Add-On: Configuration

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

- **Account Tab**: This is where the OAuth2 API credentials are entered.
- **Proxy Tab**: This is where proxy server configurations are entered.
- **Logging Tab**: This is where the logging level is configured.

Search Section

The Search section opens a standard Splunk search page within the context of the TA:

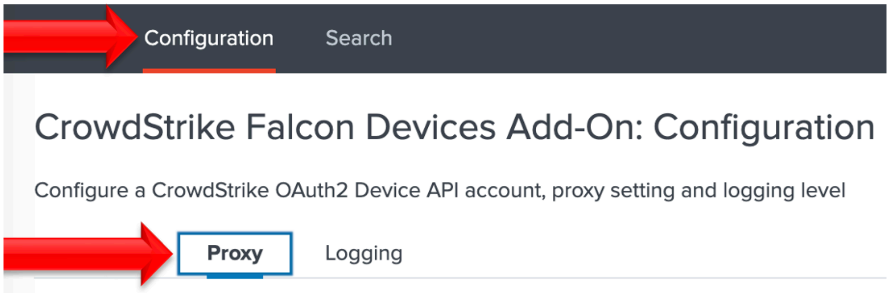


Configuring the TA to collect data

***NOTE* This action should only be performed on a Splunk instance designed for collecting data**

Configure Proxy Settings (optional)

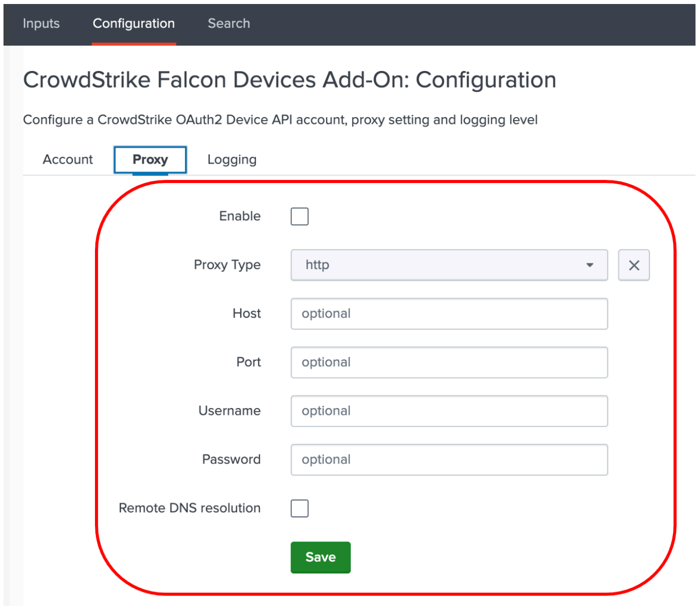
1. Proxy settings are configured under the Configuration section, Proxy tab. Proxies can cause authentication issue if not configured correctly, the proxy should not perform SSL/TLS proxying on any API calls.



CrowdStrike Falcon Devices Add-On: Configuration

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

2. Configure the following fields as appropriate:



CrowdStrike Falcon Devices Add-On: Configuration

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

Enable □

Proxy Type: http

Host: optional

Port: optional

Username: optional

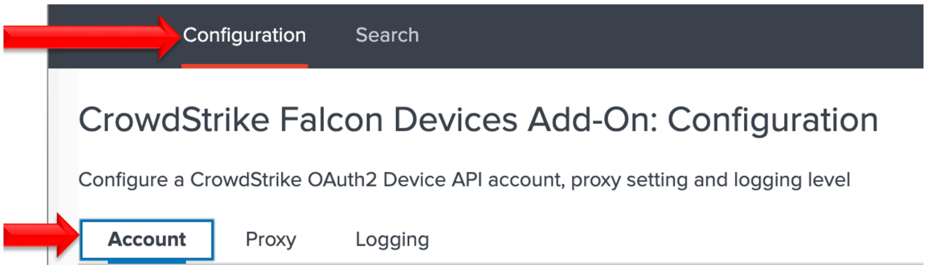
Password: optional

Remote DNS resolution □

- **Enable**: This checkbox is used to enable/disable the proxy settings
- **Proxy Type**: This dropdown is used to select the proxy type
- **Host**: The hostname/IP address for the proxy server
- **Port**: The communication port for the proxy server
- **Username**: The authentication username for the proxy (optional)
- **Password**: The authentication password for the proxy (optional)
- **Save**: This button is used to safe the configuration

Configure an Account

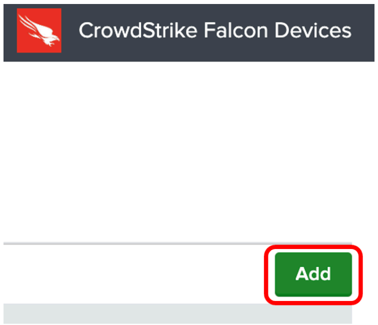
1. An account is configured using a properly scoped OAuth2 API credential.
2. An account is created under the Configuration section, Account tab:



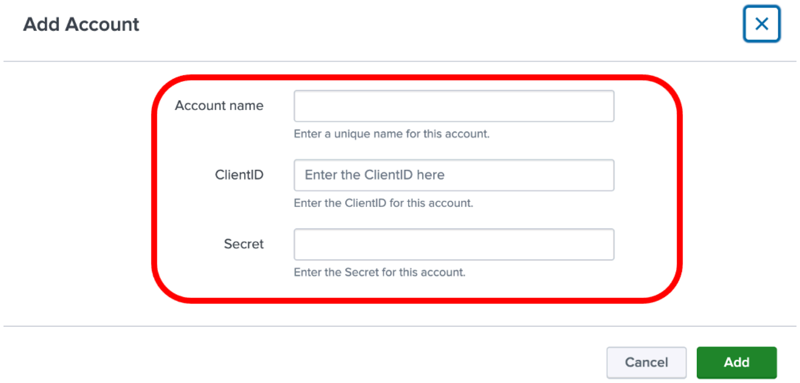
CrowdStrike Falcon Devices Add-On: Configuration

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

3. On the right side of the screen click the “Add” button:



4. Configure the following fields:



Enter a unique name for this account.

Enter the ClientID for this account.

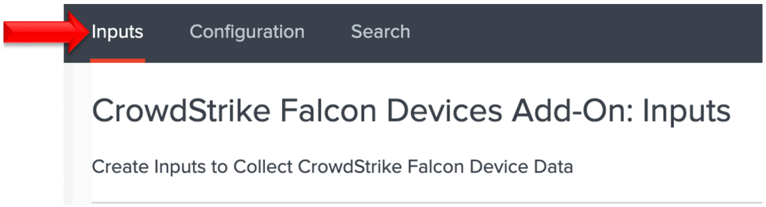
Enter the Secret for this account.

- **Account Name**: A name unique for the Splunk instance
- **ClientID**: The ClientID of the API credential created in the CrowdStrike Falcon UI
- **Secret**: The Secret of the API credential created in CrowdStrike Falcon UI

5. Click the ‘Add’ button in the bottom right corner to save the account.

Configure an Input

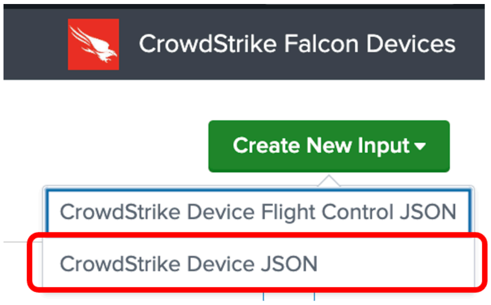
1. An input will require a valid account be already created.
2. An input is created under the Inputs section:



CrowdStrike Falcon Devices Add-On: Inputs

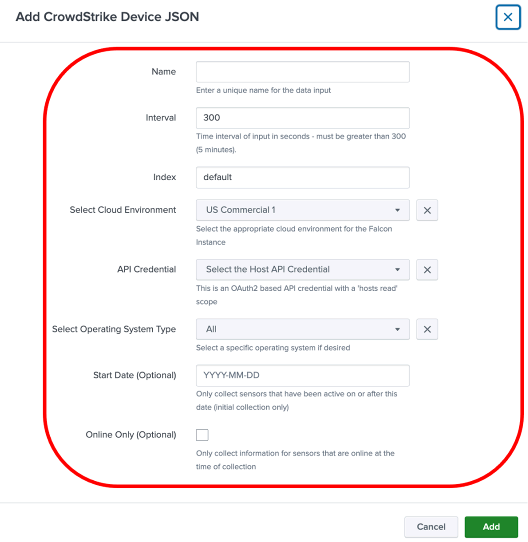
Create Inputs to Collect CrowdStrike Falcon Device Data

3. From the dropdown‘Create New Input’ in the top right corner select ‘CrowdStrike Device JSON’



CrowdStrike Falcon Devices
Create New Input ▾
CrowdStrike Device Flight Control JSON
CrowdStrike Device JSON

4. Configure the appropriate fields:



Add CrowdStrike Device JSON

Name:

Enter a unique name for the data input

Interval: 300

Time interval of input in seconds - must be greater than 300 (5 minutes).

Index: default

Select Cloud Environment: US Commercial 1

Select the appropriate cloud environment for the Falcon Instance

API Credential: Select the Host API Credential

This is an OAuth2 based API credential with a 'hosts read' scope

Select Operating System Type: All

Select a specific operating system if desired

Start Date (Optional): YYYY-MM-DD

Only collect sensors that have been active on or after this date (initial collection only)

Online Only (Optional): □

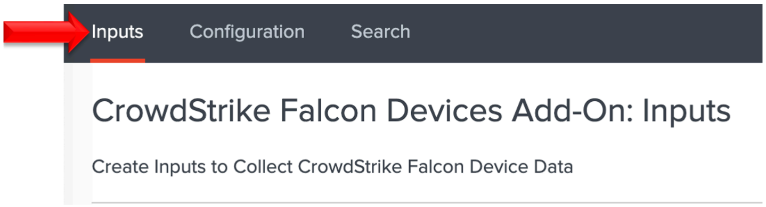
Only collect information for sensors that are online at the time of collection

- **Name**: (required) A name unique to the Splunk Environment
- **Interval**: (required) How often the TA will collect data, expressed in seconds (the default and minimum is 300)
- **Index**: (required) The Splunk Index that the data will be stored in
- **Cloud Environment**: (required) The CrowdStrike cloud environment that that API call will be made to (match the URL indicated in the Falcon UI ’API Client and Keys’ page):
    - **US Commercial 1**: https://api.crowdstrike.com
    - **US Commecial 2**: https://api.us-2.crowdstrike.com
    - **GovCloud**: https://api.laggar.gcw.crowdstrike.com
    - **EUCloud**: https://api.eu-1.crowdstrike.com
- **API Credential**: (required) The account that will be used to authenticate to the CrowdStrike API
- **Operating System Type**: (required) Indicates the operating system types to collect
    - **All**: Collects all operating system types
    - **MAC**: Collects only Apple OSX based systems
    - **Windows**: Collects only Windows based systems
    - **Linux**: Collects only Linux based systems
- **Start Date**: (optional) A date in YYYY-MM-DD format that serves as a starting point from which to collect device data. Devices must have been online on or after the date to be collected
- **Online Only**: (optional) Only data for devices that are online at the time of the collection will be collected

5. Click the ‘Add’ button in the bottom right corner to save and active the input.

Configure an Input: Flight Control

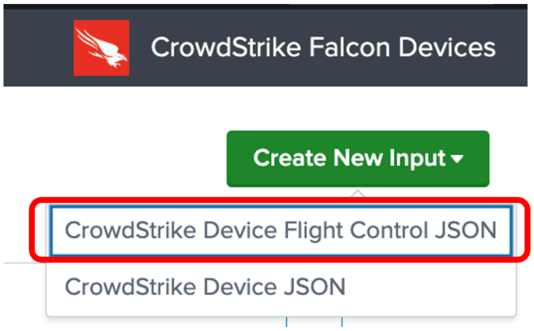
1. An input will require a valid account be created already.
2. An input is created under the Inputs section:



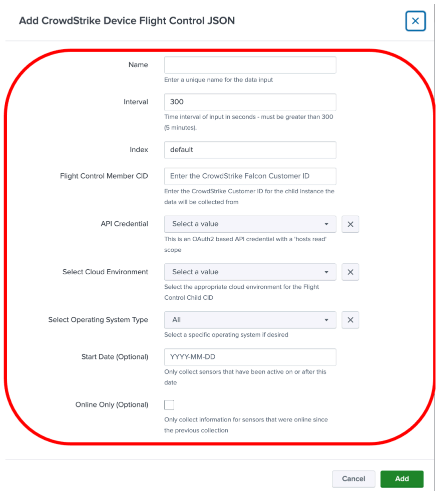
CrowdStrike Falcon Devices Add-On: Inputs

Create Inputs to Collect CrowdStrike Falcon Device Data

3. From the dropdown'Create New Input' in the top right corner select 'CrowdStrike Device JSON'


CrowdStrike Falcon Devices
Create New Input ▾
CrowdStrike Device Flight Control JSON
CrowdStrike Device JSON

4. Configure the appropriate fields:



Add CrowdStrike Device Flight Control JSON

Name:
Enter a unique name for the data input

Interval: 300
Time interval of input in seconds - must be greater than 300 (5 minutes).

Index: default

Flight Control Member CID: Enter the CrowdStrike Falcon Customer ID
Enter the CrowdStrike Customer ID for the child instance the data will be collected from

API Credential: Select a value
This is an OAuth2 based API credential with a 'hosts read' scope

Select Cloud Environment: Select a value
Select the appropriate cloud environment for the Flight Control Child CID

Select Operating System Type: All
Select a specific operating system if desired

Start Date (Optional): YYYY-MM-DD
Only collect sensors that have been active on or after this date

Online Only (Optional): □
Only collect information for sensors that were online since the previous collection

- **Name**: (required) A name unique to the Splunk Environment
- **Interval**: (required) How often the TA will collect data, expressed in seconds (the default and minimum is 300)
- **Index**: (required) The Splunk Index that the data will be stored in
- **Flight Control Member CID**: Falcon Customer ID for the Falcon Flight Control child instance
- **Cloud Environment**: (required) The CrowdStrike cloud environment that that API call will be made to (match the URL indicated in the Falcon UI 'API Client and Keys' page):
  - **US Commercial 1**: https://api.crowdstrike.com
  - **US Commecial 2**: https://api.us-2.crowdstrike.com
  - **GovCloud**: https://api.laggar.gcw.crowdstrike.com
  - **EUCloud**: https://api.eu-1.crowdstrike.com
- **API Credential**: (required) The account that will be used to authenticate to the CrowdStrike API of the Falcon Flight Control Parent instance
- **Operating System Type**: (required) Indicates the operating system types to collect
  - **All**: Collects all operating system types
  - **MAC**: Collects only Apple OSX based systems
  - **Windows**: Collects only Windows based systems
  - **Linux**: Collects only Linux based systems
- **Start Date**: (optional) A date in YYYY-MM-DD format that serves as a starting point from which to collect device data. Devices must have been online on or after the date to be collected
- **Online Only**: (optional) Only data for devices that are online at the time of the collection will be collected

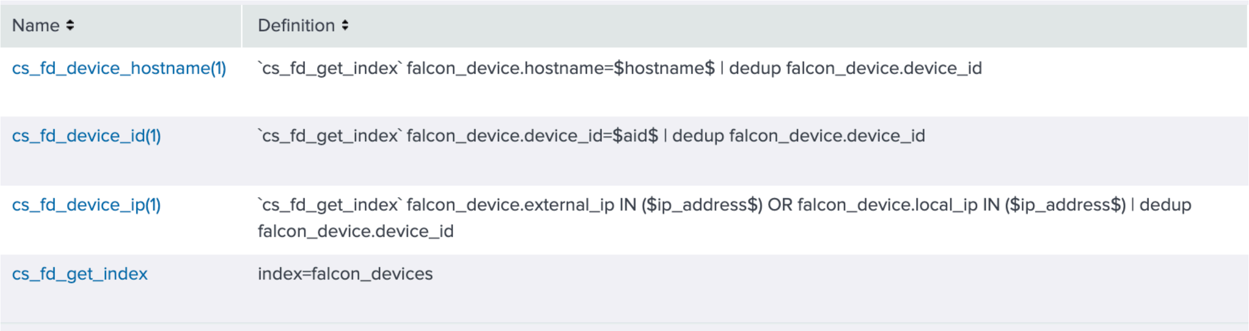
5. Click the 'Add' button in the bottom right corner to save and active the input.

Search Macros

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

This TA contains search macros to assist in examining and associating the data collected as quickly and efficiently as possible.

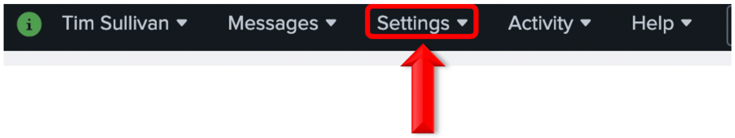


Name ⇕	Definition ⇕
cs_fd_device_hostname(1)	\`cs_fd_get_index\` falcon_device.hostname=$hostname$ | dedup falcon_device.device_id
cs_fd_device_id(1)	\`cs_fd_get_index\` falcon_device.device_id=aid | dedup falcon_device.device_id
cs_fd_device_ip(1)	\`cs_fd_get_index\` falcon_device.external_ip IN ($ip_address$) OR falcon_device.local_ip IN ($ip_address$) | dedup falcon_device.device_id
cs_fd_get_index	index=falcon_devices

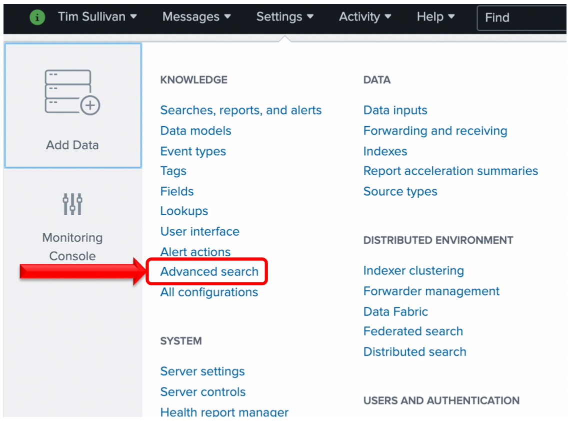
Locating the Search Macros

The search macros can be located by navigating to:

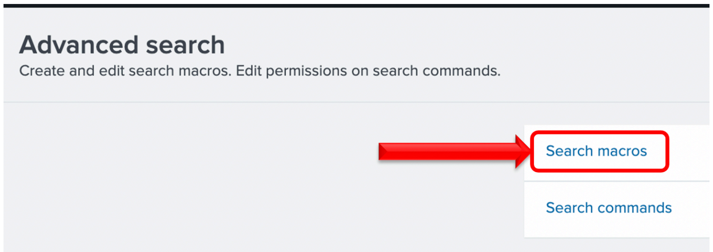
1. Select that ‘Settings’ dropdown in the Splunkbar :



2. Select ‘Advanced Search’ from the dropdown menu:



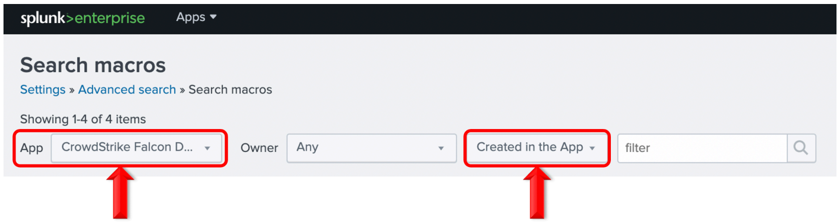
3. Under ‘Advanced Search’ select ‘Search Macros:



Advanced search

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

4. Ensure the ‘CrowdStrike Falcon Device Technical Add-on’ is selected in the ‘App’ selection and ‘Created in App’ is selected from the pulldown selection:



Search macros

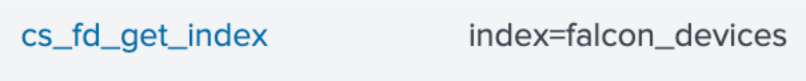
Settings » Advanced search » Search macros

Showing 1-4 of 4 items

App: CrowdStrike Falcon D... Owner: Any Created in the App

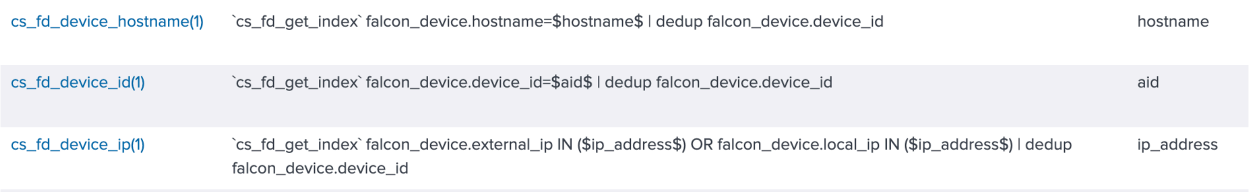
Configuring and Leveraging the Search Macros

There currently is only 1 search macro that requires configuration but this search macro must be configured for the other search macros to function.



cs_fd_get_index index=falcon_devices

- **`cs_fd_get_index`** (CrowdStrike Falcon Device get index) A search macro that points to the index(es) that contain the data received by the TA inputs. The default for this search macro is to point to an index named ‘falcon_devices’ and should be adjusted to reflect the specific index(es) that the Heavy Forwarder/IDMs are pushing the data to.



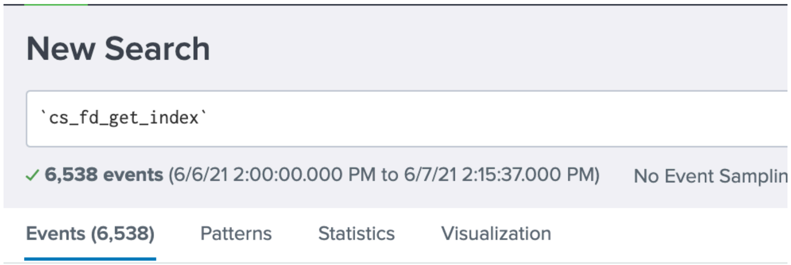
cs_fd_device_hostname(1)	\`cs_fd_get_index\` falcon_device.hostname=$hostname$ | dedup falcon_device.device_id	hostname
cs_fd_device_id(1)	\`cs_fd_get_index\` falcon_device.device_id=aid | dedup falcon_device.device_id	aid
cs_fd_device_ip(1)	\`cs_fd_get_index\` falcon_device.external_ip IN ($ip_address$) OR falcon_device.local_ip IN ($ip_address$) | dedup falcon_device.device_id	ip_address

- **\`cs_fd_device_hostname(1)\`** A search macro that takes 1 input (a hostname). This search macro will search the configured index(es) for the hostname contained in the parenthesis.
- **\`cs_fd_get_device_id(1)\`** A search macro that takes 1 input (a Falcon device/agent ID). This search macro will search the configured index(es) for the Falcon device/agent ID contained in the parenthesis.
- **\`cs_fd_get_ip(1)\`** A search macro that takes 1 input (a IP address). This search macro will search the configured index(es) for the IP address contained in the parenthesis. This search will include both the internal and external addresses.

NOTE: These search macros will not function correctly if the \`cs_fd_get_index\` search macro is not configured correctly and all search macros must be contained in backticks (they are not single quotation marks).

Search Macro Examples

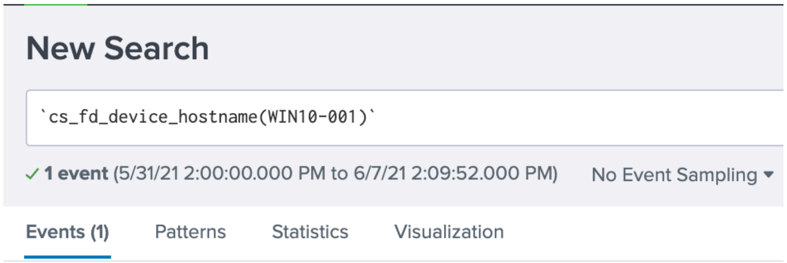
`cs_fd_get_index`



```
`cs_fd_get_index`
```

✓ **6,538 events** (6/6/21 2:00:00.000 PM to 6/7/21 2:15:37.000 PM)

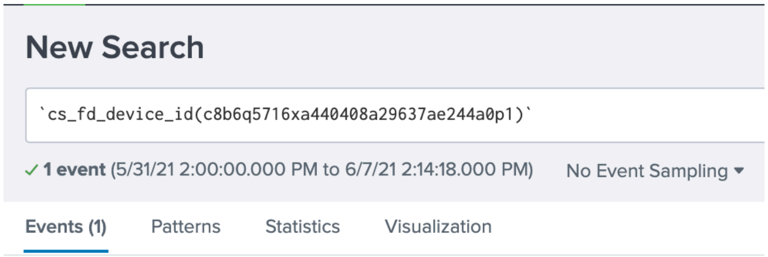
`cs_fd_device_hostname(Win10-001)`



```
`cs_fd_device_hostname(WIN10-001)`
```

✓ **1 event** (5/31/21 2:00:00.000 PM to 6/7/21 2:09:52.000 PM)

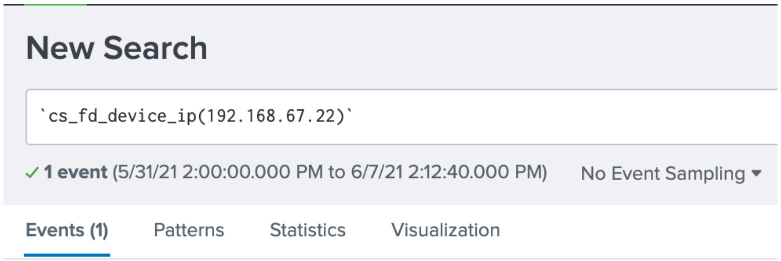
`cs_fd_get_device_id(c8b6q5716xa440408a29637ae244a0p1)`



```
`cs_fd_device_id(c8b6q5716xa440408a29637ae244a0p1)`
```

✓ **1 event** (5/31/21 2:00:00.000 PM to 6/7/21 2:14:18.000 PM)

`cs_fd_get_ip(192.168.67.22)`



```
`cs_fd_device_ip(192.168.67.22)`
```

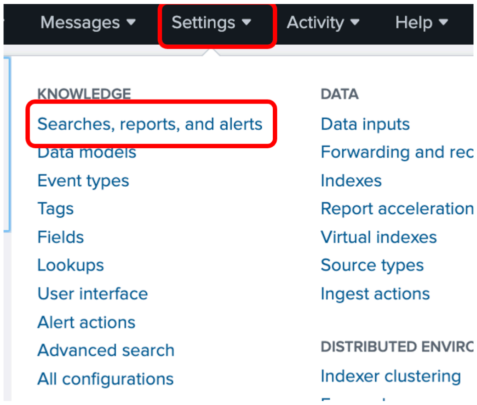
✓ **1 event** (5/31/21 2:00:00.000 PM to 6/7/21 2:12:40.000 PM)

Reports

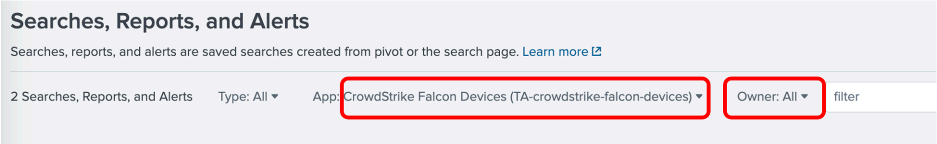
Locating the Reports

The reports included in the TA can be found by navigating to:

1. Open the Settings menu, under ‘knowledge’ select ‘Searches, reports and alerts’:



2. In the ‘App’ dropdown ensure that the ‘CrowdStrike Falcon Devices’ is selected and under the ‘Owner’ dropdown ensure that ‘All’ is selected

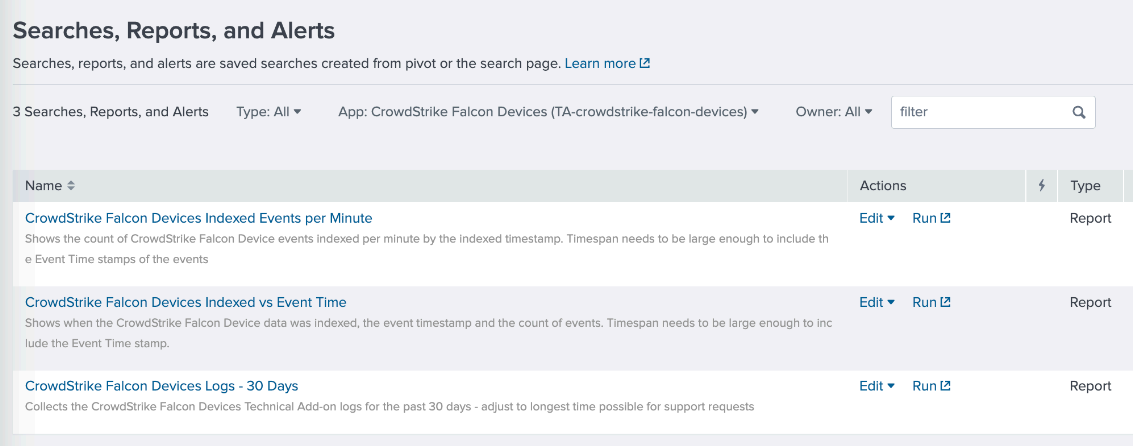


Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more

2 Searches, Reports, and Alerts   Type: All ▾   App: CrowdStrike Falcon Devices (TA-crowdstrike-falcon-devices) ▾   Owner: All ▾   filter

3. The reports that are included with the TA should be visible:



Searches, Reports, and Alerts

Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more

3 Searches, Reports, and Alerts   Type: All ▾   App: CrowdStrike Falcon Devices (TA-crowdstrike-falcon-devices) ▾   Owner: All ▾   filter

Name	Actions		Type
CrowdStrike Falcon Devices Indexed Events per Minute Shows the count of CrowdStrike Falcon Device events indexed per minute by the indexed timestamp. Timespan needs to be large enough to include the Event Time stamps of the events	Edit ▾ Run		Report
CrowdStrike Falcon Devices Indexed vs Event Time Shows when the CrowdStrike Falcon Device data was indexed, the event timestamp and the count of events. Timespan needs to be large enough to include the Event Time stamp.	Edit ▾ Run		Report
CrowdStrike Falcon Devices Logs - 30 Days Collects the CrowdStrike Falcon Devices Technical Add-on logs for the past 30 days - adjust to longest time possible for support requests	Edit ▾ Run		Report

Understanding the Reports

These reports require the index search macro be correctly configured

- **<u>CrowdStrike Falcon Devices Indexed Events per Minute</u>**: Shows the number of events, per minute by default, that have been indexed by Splunk by the _indextime timestamp.
- **<u>CrowdStrike Falcon Devices Indexed vs Event Time</u>**: Shows the number of events that have been indexed per minute into Splunk by the _indextime timestamp and also shows event timestamp.

This report should be used to collected data for support tickets, export data in JSON

- **<u>CrowdStrike Falcon Devices Logs – 30Days</u>**: Collects events from the internal index for sourcetypes that contain the TA name string for the last 30 days by default. This report can be used to collect log data for support cases and should be set to ‘all time’ and exported in JSON format for those instances.

Recommendations

The following are general recommendations. They may not be optimal in all situations and should be evaluated on an environment-by-environment basis.

Custom Indexes

The use of a dedicated custom index is strongly recommended for the CrowdStrike device data. If data inputs are configured for specific operating system types, it is also recommended that this data be put into dedicated indexes based on the specific operating system. ie Windows devices would be stored in index 'Windows', MAC OSX devices would be stored in index 'OSX' and Linux devices would be stored in index 'Linux'.

This enables the index to be queried specifically as part of either an individual search or a more complex search. It also allows multiple teams to reference the data without exposing other data sets that may be more sensitive.

Dedicated API Credential

The use of a dedicated API credential for this integration is recommended to prevent issues should the credentials secret need to be regenerated and/or to ensure that the client is only scoped for the specific API endpoints used.

Interval Setting

The interval setting for inputs should take into account the amount of data that the input could potentially process. Setting an interval to low may result in a collection being interrupted and/or the data being collected having minimal changes. In most environments collection interval over 1 hour is recommended for standard inputs. Depending on the use case and the number of potential hosts involved, on-line inputs maybe slightly shorter.

Troubleshooting

CrowdStrike only provides support for:

- TA code-based functionality errors
- API/Gateway based errors

Examples of issues that are outside the scope of CrowdStrike support:

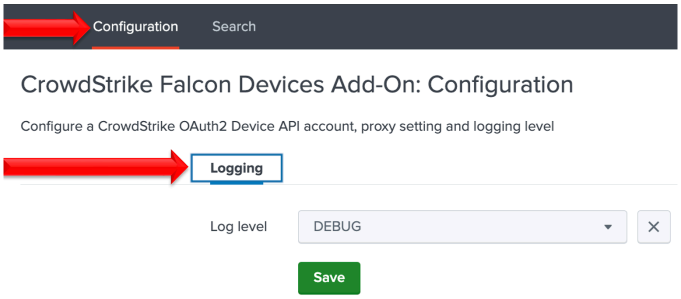
- Proxy based issues
- Firewall based issues
- Network connectivity issues
- Authentication issues (based on misconfigured credentials)
- Splunk CIM field mapping
- Splunk environmental/configuration-based issues

Configuring the TA to collect log data

The TA logging level is set to 'info' by default and will only log a minimal amount of information. To properly troubleshoot issues with the TA the logging level should be set to 'debug'.

Change Logging Level

1. Navigate to the Configuration section, Logging tab:

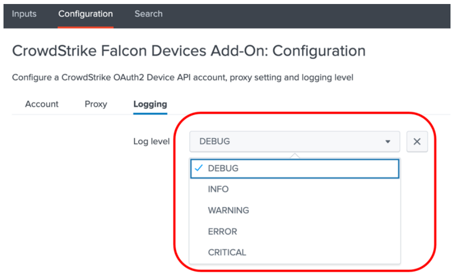


CrowdStrike Falcon Devices Add-On: Configuration

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

Log level DEBUG

2. Select the logging level from the drop-down menu:



CrowdStrike Falcon Devices Add-On: Configuration

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

Log level DEBUG

3. Click 'Save' to save the logging level.

Review Log Data in Splunk

1. Run and review the **CrowdStrike Falcon Devices Logs – 30 Days** Report to determine if there are any errors being reported by the TA.
2. Review Splunkd logs to determine if there's any internal issues within Splunk that could be causing issues with the proper collection and processing of data. If events related to a possible issue are found please include export them in JSON format and include them in any support requests.

Examples of Troubleshooting Situations and Remediation Steps

1. It doesn't look like any data is being collected:

1.1. Ensure that the credentials have been properly scoped for the API and have been properly entered

1.2. Ensure that the time picker selection is set to either 'all time' or that the time window is large enough to include the event timestamp. If the TA may be collecting events that are timestamped outside the currently selected time window

1.3. Run one of the reports or a search query that shows the events by _indextime to determine if and when events are being or have been indexed. Ensure that the time window is set to 'all time' to avoid not capturing data that has an event time outside the time window. Indexed time and event time can be drastically different

1.4. Examine log data to determine if any API calls are getting 401 or 403 responses indicating a potential issue with authentication, credential input

1.5. Ensure that firewalls, proxies and other network devices are not interfering with the communications between the TA and CrowdStrike API(s) and the TA and Splunk APIs

2. Data looks like it is coming in 'delayed':

Data collected by the TA can be delayed in indexing because of factors outside of the control of the TA's functionality and may ***not*** *be able to be identified or rectified by CrowdStrike*

2.1. Determine if there is potentially any latency in data communication between the Splunk system doing the data collection and the indexer tier

2.2. Determine if there's any latency in data being indexed at the indexing tier

2.3. Run one of the reports or a search query that shows the events by _indextime to determine if and when events are being or have been indexed. Ensure that the time window is set to 'all time' to avoid not capturing data that has an event time outside the time window. Indexed time and event time can be drastically different

2.4. Example the TA log data and compare it against the indexing time data to determine if they are aligning

3. **The data being collected does not look ‘complete’:**

   3.1. Review the input settings to ensure that the settings reflect that data collection requirements

   3.2. Review the interval setting to ensure that there is enough time to collect the required data and that data collections are not being interrupted

   3.3. Ensure that the Splunk search and the associated time window will encompass all the potential data

   3.4. Ensure that any potential discrepancy does not take into account hosts that may have been deleted

   3.5. Review the TA logs and the internal Splunk logs for any errors that may have impacted data collection

   3.6. Validate that there is not an internal Splunk issue that could be delaying the indexing of data

Support

This TA Is designed to help facilitate the collection of device data provided by the CrowdStrike API(s). CrowdStrike provides support for the TA code functionality as it was designed. Example of instances that would fall outside of CrowdStrike's support:

- Environment caused network connectivity issues
- Issues related to certain Splunk configurations or internal Splunk connectivity issues
- Modifying the TA configuration outside of what's outlined in this documentation
- Support requests without the appropriate data outlined below
- Splunk CIM field mapping or custom data modification requests

Prior to Contacting CrowdStrike Support

1. Ensure that the OAuth2 credential has been scoped and entered correctly
2. Ensure that it is not an issue with the TA communicating with Splunk, modular inputs post data to API endpoints within Splunk so things like host firewalls can block this communication as can permission issues.
3. Ensure that the issue is not a network connectivity issue, if the API calls being made by the TA cannot properly communicate with the CrowdStrike API those issues should be resolved before contacting CrowdStrike support
4. Set the TA log level to 'DEBUG'
5. Repeat and record the action(s) that are associated with the issue you are reporting
6. Collect all appropriate log information
    a. Run the **CrowdStrike Falcon Devices Logs – 30 Days** Report with the time picker set to 'All Time' and export all the results in JSON format
    b. (If possible) Download the all log files containing 'ta_crowdstrike_falcon_devices' under the $Splunk/var/log/splunk/ directory
    c. Collect any relevant logs from Splunk's internal log index related to the TA and the issue you're reporting
7. Record the following information about the Splunk system:
    - Splunk environment type
    - Splunk version
    - TA version
    - If this is was a new deployment/upgrade or if there was no change to the TA
    - The approximate date(s) and time(s) of examples of when the specific issue(s) occurred

Contacting CrowdStrike Support

1. Navigate to https://supportportal.crowdstrike.com/
2. Open a support ticket, provide the data collected in steps 6 & 7 above as well as any modifications that have been made to the TA outside of the processed outlined in this documentation

NOTE:

CrowdStrike technical support engineers (TSE) are required to evaluate Splunk integration support requests. In addition, CrowdStrike TSE are required to perform troubleshooting workflows to help identify potential issues and evaluate those issues for potential escalations to other teams. This may include, but is not limited to, requesting additional information/data/logs and requesting results from specific search queries or configurations modifications. The inability or unwillingness to supply the required/requested information and/or make request modifications/actions may result in CrowdStrike not being able to troubleshoot the reported issue and result in the inability to provide support for the reported issue.

Additional Resources

CrowdStrike Host and Host Group Management API Documentation
CrowdStrike FalconPy SDK

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

There's only one thing to remember about CrowdStrike: **We stop breaches**.