



CROWDSTRIKE

CrowdStrike Scheduled Search Add-on for Splunk

Installation and Configuration Guide v2.2.0+

Table of Contents

Introduction	1
Requirements	1
Getting Started.....	2
API Endpoint(s), Filter(s) and Timestamp(s).....	2
High Level API Call Flow	3
Technical Add-On Layout	4
Creating/Validating the API Credential Scope	5
TA_Data Section	7
Proxy Considerations	8
Splunk Architecture	8
Creating the Scheduled Search.....	10
Creating a Scheduled Search – Events Page:.....	11
Creating a Scheduled Search – Scheduled Search Page:.....	12
Configuring the TA.....	15
TA Layout.....	15
Inputs Section.....	15
Configuration Section	16
Search Section	16
Dashboards Section	17
Reports Section.....	17
CrowdStrike Resources Section	18
Configuring the TA to collect data	19
Configure Proxy Settings (optional).....	19
Configure an Account.....	20
Configure an Input.....	21
Search Macros.....	23
Locating the Search Macros	24
Configuring and Leveraging the Search Macro(s).....	25
Search Macro Examples	26
Reports.....	27
Locating the Reports	27

Current Reports	27
Report: CrowdStrike Scheduled Search Logs – 30 Days	27
Report: CrowdStrike Scheduled Search Report and Execution Event Counts	27
Dashboards	28
Locating the Dashboards.....	28
CrowdStrike Schedules Search TA: Admin and Operations Dashboard	28
CrowdStrike Schedules Search TA: TA Log Search – BETA Dashboard	29
Recommendations.....	30
Custom Indexes	30
Dedicated API Credential	30
Interval Setting	30
Troubleshooting	31
Configuring the TA to collect log data.....	32
Change Logging Level	32
Review Log Data in Splunk	32
Examples of Troubleshooting Situations and Remediation Steps.....	33
Support	35
Prior to Contacting CrowdStrike Support	35
Contacting CrowdStrike Support	36

Introduction

This guide covers the deployment, configuration and usage of the CrowdStrike Scheduled Search Technical Add-on (TA) for Splunk version 2.0.5 and up.

The CrowdStrike Scheduled Search Technical Add-on for Splunk allows CrowdStrike customers to retrieve Scheduled Searches that they have configured and index that data into Splunk.

PLEASE NOTE:

This TA does not support collection of 'Scheduled Reports', which are preconfigured scheduled searches in the Falcon UI. This data type will be added in a future release.

Requirements

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

1. An active subscription to the CrowdStrike modules that produce the desired data.
2. The name of an active scheduled search collecting the desired data.
3. A Splunk Heavy forwarder, input Data Manager (IDM) or Splunk Cloud instance that supports modular input data ingestion.
4. A Splunk account with proper access to deploy and configure technical add-ons.
5. A properly scoped API credential or proper access to the CrowdStrike Falcon instance to create one.
6. The base URL for the CrowdStrike Cloud environment that the Falcon instance resides in.

Getting Started

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

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

API Scope	Read	Write
Scheduled Reports		

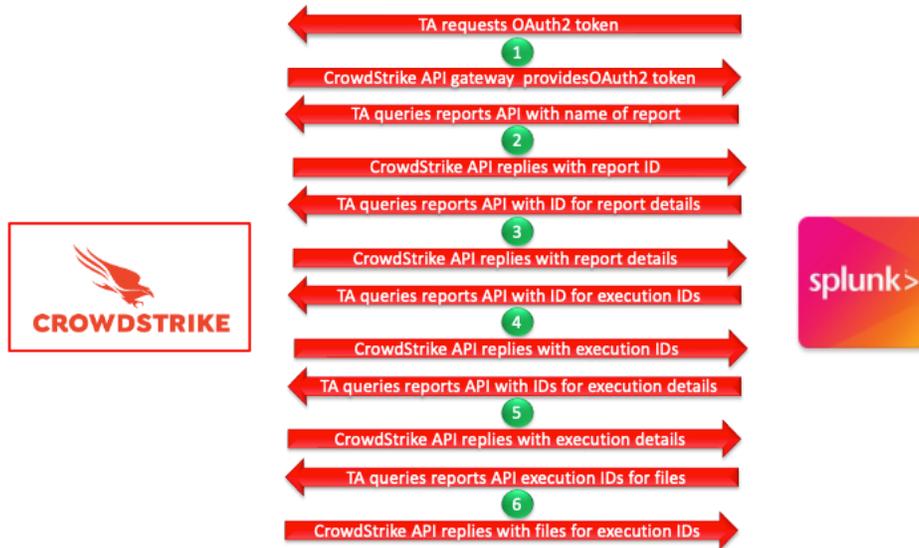
API Endpoint	Potential fields(s)
/oauth2/token	
/reports/queries/scheduled-reports/v1	name
/reports/entities/scheduled-reports/v1	
/reports/queries/report-executions/v1	scheduled_report_id, result_metadata.report_finish
/reports/entities/report-executions/v1	
/reports/entities/report-executions-download/v1	

For more information about these API endpoints please refer to the *Scheduled reports and searches APIs* documentation in the Falcon console.

The TA will use the `_time` field value in the event data as the timestamp of the event. This is the timestamp directly from Falcon search UI and is in UTC.

The TA will use the `'report_finish'` field value in the execution data results as a filtering field and as the checkpoint value. As data is collected the TA will record this field value and leverage it for follow on data collections. For example, if the last collection had a `'report_finish'` value of `'2023-04-27T17:15:24.264903909Z'`, then the next collection interval would request report-executions that happened after `'2023-04-27T17:15:24.26Z'`. This value can be located in the `'ta_data'` section of the event under `'Execution_Data'`, `'result_metadata'`.

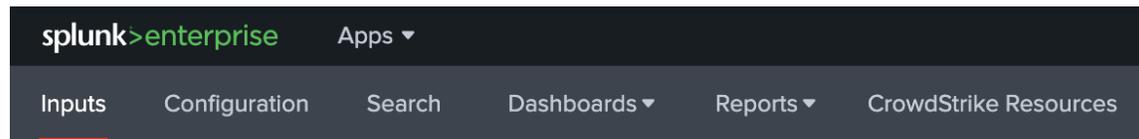
High Level API Call Flow



1. TA will call the CrowdStrike API gateway with the configured credentials and request an OAuth2 authentication token that is valid for 30 minutes.
If the API credential are valid the API gateway will respond to the TA with an OAuth2 token.
2. The TA will call the reports API endpoint with the name of the report in the configuration to get the report's ID.
If the name of the report is valid, the API will return the report's ID.
****NOTE: report names are case sensitive.**
3. The TA will call the reports API with the report ID to get the details about the report.
The API returns the detailed information about the report.
4. The TA will call the reports API with the report ID to get the execution IDs associated with that report and within the timeframe of the data collection.
The API returns a list of any execution IDs for the report ID within the indicated timeframe.
5. The TA will call the report API for each of the execution IDs to get the details about the execution.
The API returns the details about the execution ID.
6. The TA will call the report API for each of the execution IDs to get the data file for the events
The API will return the binary file information for the events

Once this process has been completed, the data will be pushed to the internal Splunk API for the TA so that the data can be sent to the indexer for indexing. In addition, the TA will record the latest 'report_finish' field value into the Splunk KVStore.

Technical Add-On Layout



CrowdStrike Scheduled Search: Inputs

The CrowdStrike Scheduled Search TA has 6 selections 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.
4. **Dashboards** - A dropdown menu that will auto-populate with any available view containing 'crowdstrike_scheduled_search' in the name, by default the CrowdStrike provided dashboards will be listed.
5. **Reports** – A dropdown menu that will auto-populate with any available report containing 'CrowdStrike Scheduled Search' in the name, by default the CrowdStrike provided reports will be listed.
6. **CrowdStrike Resources** – A dashboard that provides links to additional information about the TA, the FalconPy SDK and the CrowdStrike support process.

Creating/Validating the API Credential Scope

While the CrowdStrike Scheduled Search TA can leverage an existing OAuth2 based API credential, but it's often preferred to create a dedicated credential. This can be accomplished by the following:

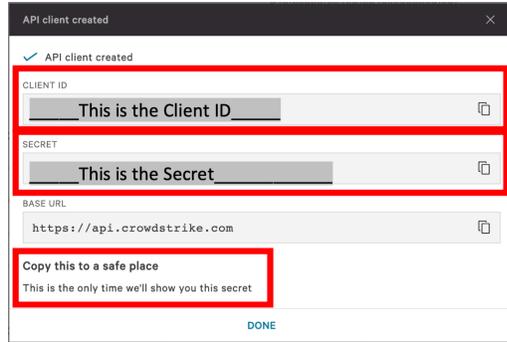
1. Access the CrowdStrike Falcon user interface (UI) with an account that is able to create API clients and keys
2. Navigate to 'Support' > 'API Client and Keys' page
3. Create a new API client by selecting 'Add new API client' in the OAuth2 API client's area

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

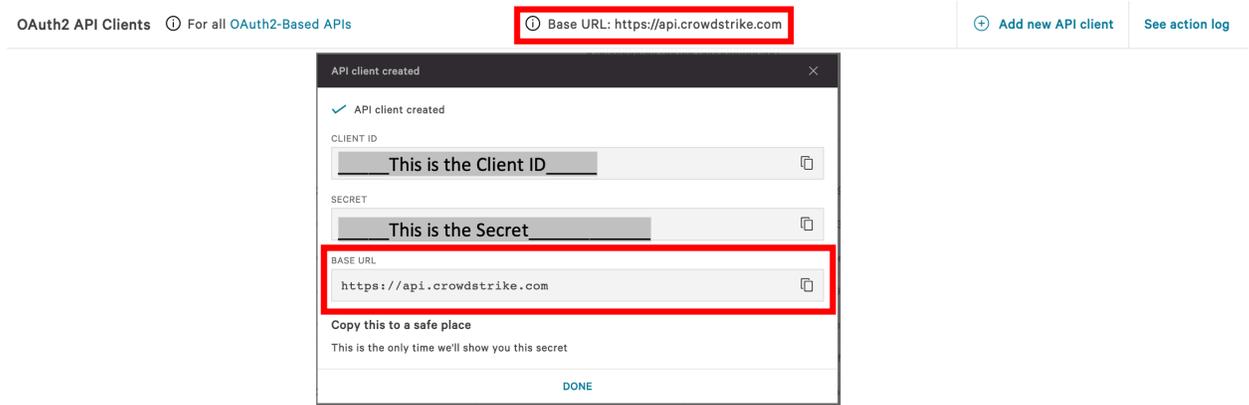
4. Give the new API client a name and description (recommended) and under 'API Scopes' select the 'Scheduled Reports' scope and the 'Read' scope:

Scope	Read	Write
Response policies	<input type="checkbox"/>	<input type="checkbox"/>
Sample uploads	<input type="checkbox"/>	<input type="checkbox"/>
Scheduled Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IOA Exclusions	<input type="checkbox"/>	<input type="checkbox"/>
Sensor Download	<input type="checkbox"/>	<input type="checkbox"/>
Sensor update policies	<input type="checkbox"/>	<input type="checkbox"/>

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.**



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



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

TA_Data Section

The `ta_data` section of the event(s) is created by the TA and added to each event that's ingested. This section contains information about the TA, the collecting input's configuration and may also include API response data.

```
ta_data: { [-]
  Cloud_environment: us_commercial2
  Collection_option: historic_search
  Collection_time: 2023-05-09T19:30:27Z
  Execution_Data: { [+]
  }
  Input_name: Fast_FIM_US2
  Report_Data: { [+]
  }
  Search_name: Fast_FIM_US2
  TA_version: 2.1.0
}
```

The diagram shows the following annotations:

- `Cloud_environment: us_commercial2` is annotated as "Input Configuration: CrowdStrike Cloud Environment".
- `Collection_option: historic_search` is annotated as "Input Configuration: Collection Option Selection".
- `Collection_time: 2023-05-09T19:30:27Z` is annotated as "Timestamp for when Input collection started".
- `Execution_Data: { [+] }` is annotated as "Execution Details Returned by the API".
- `Input_name: Fast_FIM_US2` is annotated as "Input Configuration: Input Name".
- `Report_Data: { [+] }` is annotated as "Report Details Returned by the API".
- `Search_name: Fast_FIM_US2` is annotated as "Input Configuration: Search Name".
- `TA_version: 2.1.0` is annotated as "Version of the TA used for collection".

- **Cloud Environment:** The CrowdStrike Cloud selected in the input configuration.
- **Collection_option:** Indicates if the input configuration was historic or most recent.
- **Collection_time:** A timestamp of when the input began data collection.
- **Execution_Data:** The API data returned from the execution details API call.
- **Input_name:** The name of the configured input.
- **Report_Data:** The API data returned from the report details API call.
- **Search_name:** The name of the search configured for the input.
- **TA_version:** The version of the TA that did the data collection.

Proxy Considerations

The CrowdStrike Scheduled Search 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.

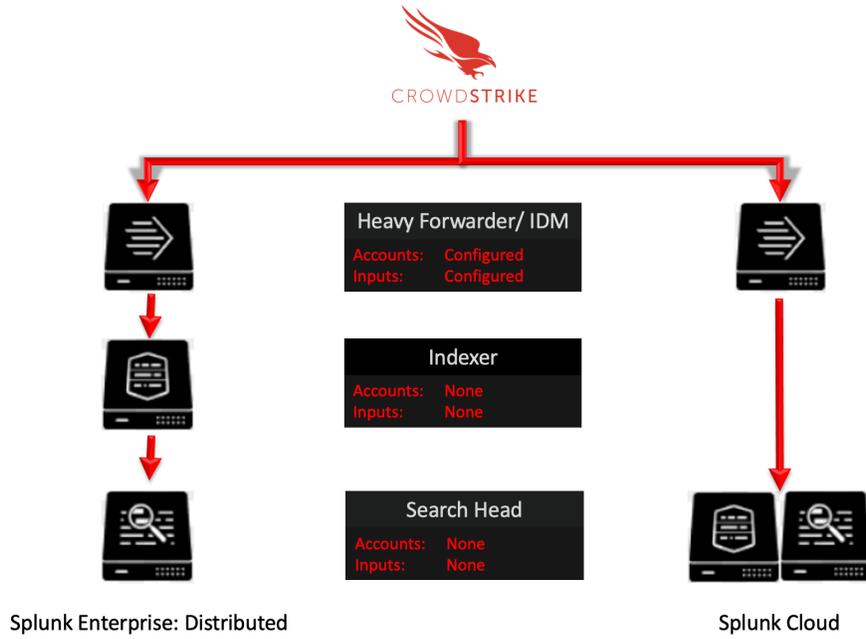
Splunk Indexer(s): The TA can be installed to provide field mapping and search macro support. The TA should be deployed without any accounts or inputs configured and any search macros should be properly configured for use. If a custom index is going to be used, then it should be created here.

Splunk Heavy Forwarder(s) & Information Data Managers (IDMs): The TA is required to be installed here as this is where the data from the 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:

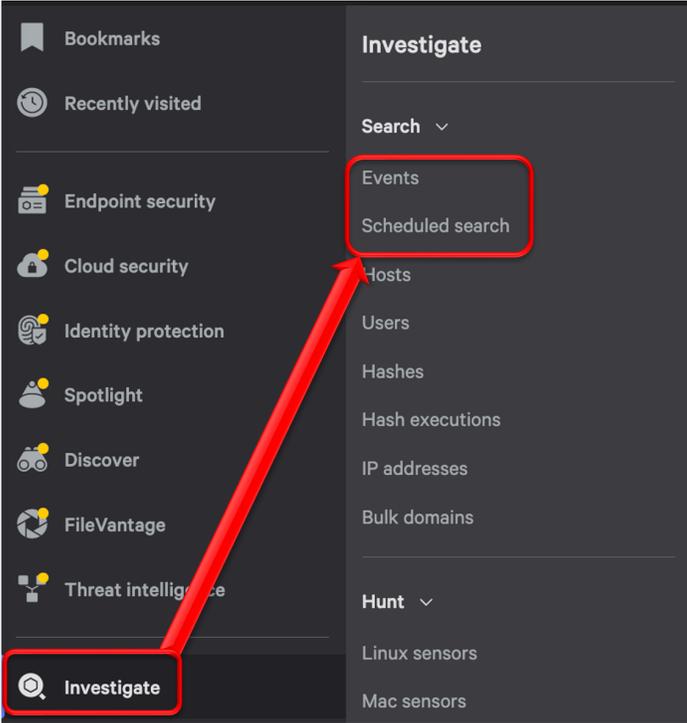
Due to python requirements the TA can only be configured for data collection on Heavy Forwarders, IDMs or Splunk Cloud deployments capable of support modular inputs.

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



Creating the Scheduled Search

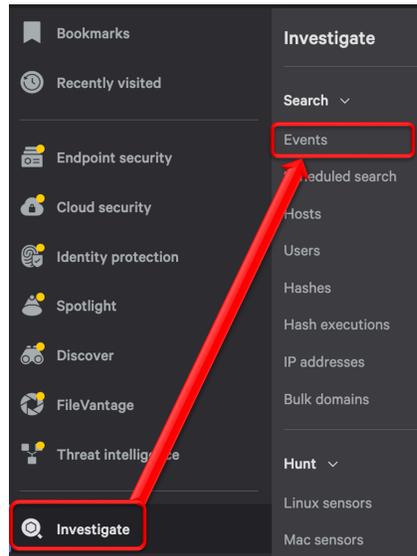
A scheduled searches are typically created in one of two ways. The two selections are both located under the 'Investigate' selection in the Falcon UI and are 'Events' and 'Scheduled Search':



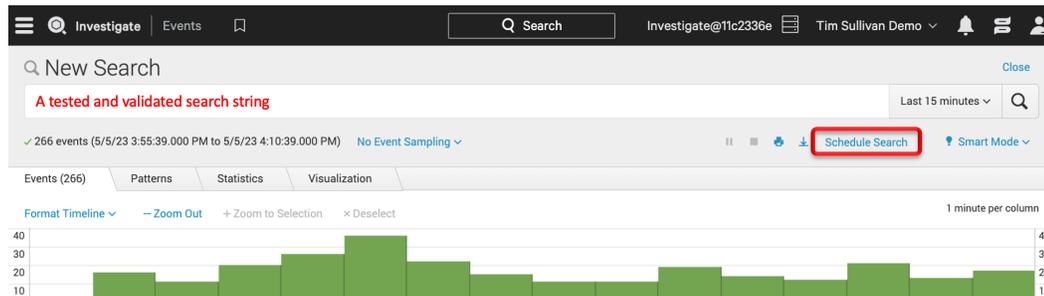
Creating a Scheduled Search – Events Page:

This is the recommended initial step if there isn't an existing and validated search string available. If there is an existing and validated search string available the 'Scheduled Search' process can be leveraged.

1. Navigate to 'Investigate' -> 'Events' in the Flacon UI



2. Create, test and validate a search to run that will collect the desired data. Once the search results have been validated select 'Schedule Search':

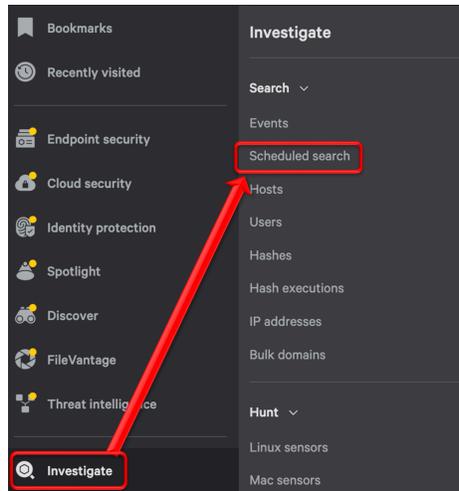


3. The 'Schedule Search' option will navigate to a process in the 'Scheduled Search' page under 'Investigate' described in the 'Creating A Scheduled Search – Scheduled Search Page' part of this document.

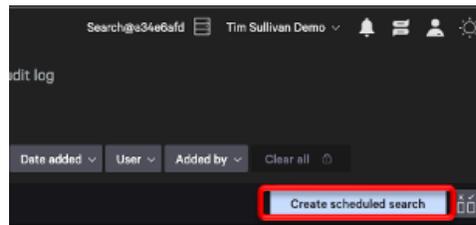
Creating a Scheduled Search – Scheduled Search Page:

This is the recommended process for an existing and validated search string.

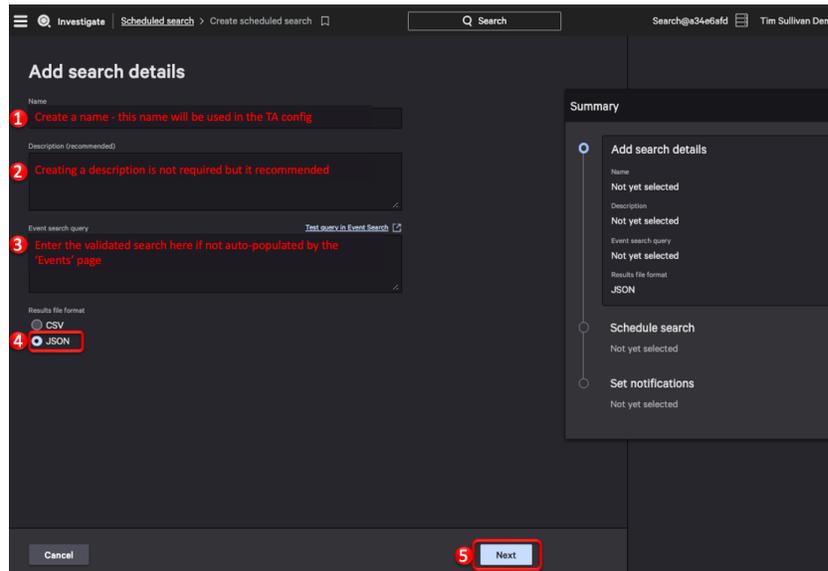
1. Navigate to 'Investigate' -> 'Scheduled Search' in the Flacon UI.



2. To create a new Scheduled Search, select 'Create scheduled search'

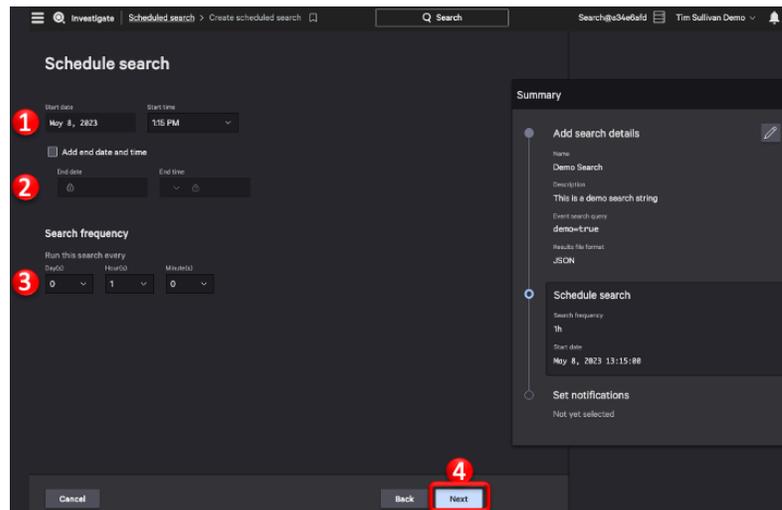


3. Create the search details as follows:



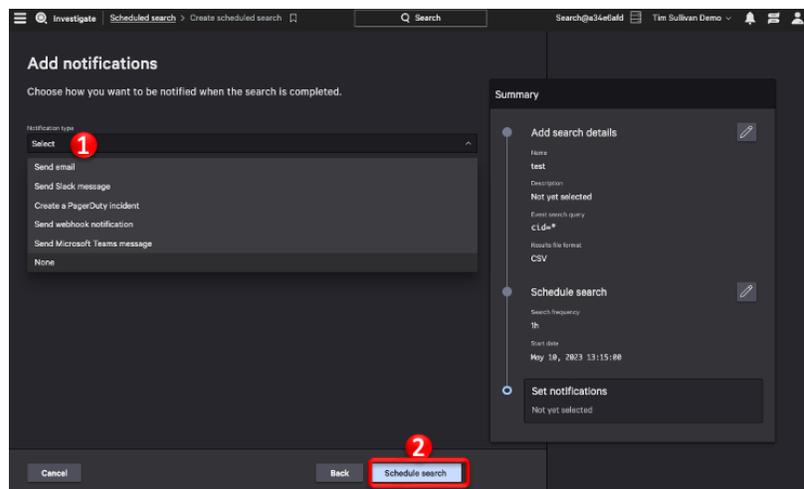
1. **Name:** This will be the name of the scheduled search
2. **Description:** This is an optional but recommended field to describe the search
3. **Event Search Query:** The actual query that will be run on the scheduled basis, if this search is being imported from the Events page, then this field will already be populated.
4. **Results file format:** This should be set to JSON; the TA will attempt to convert CSV to JSON but the format should be configured as JSON.
5. **Next:** Select next to schedule the search

4. Configure the schedule for the search as follows:



1. **Start Date and Time:** Select the start date and time for the first search.
2. **End Date and Time:** Optional – Configure an end date and time for the search.
3. **Search Frequency:** Configure how often the search should run
4. **Next:** Select next to set the notifications

5. Add notifications:

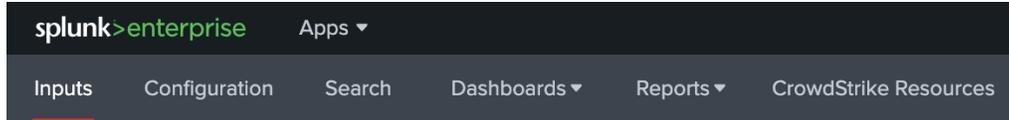


1. **Notifications:** The TA does not require notifications so this can be set to 'none' if desired.
2. **Schedule search:** Select to complete and schedule the search.

Configuring the TA

TA Layout

The TA contains 6 sections:

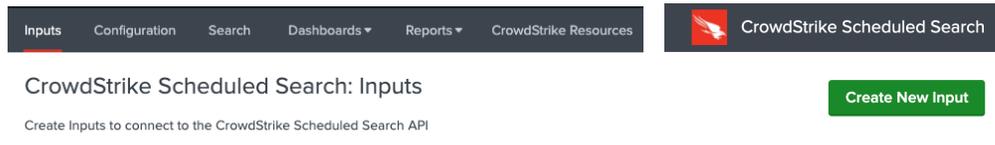


CrowdStrike Scheduled Search: Inputs

- Inputs
- Configuration
- Search
- Dashboards
- Reports
- CrowdStrike Resources

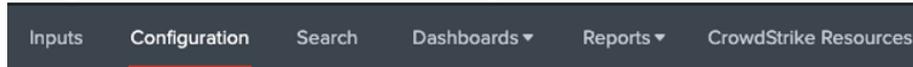
Inputs Section

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 the Configuration Section of this document). The Inputs section contains a 'button' that will create a new input configuration in the far-right corner.



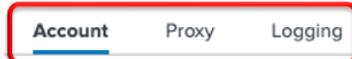
Configuration Section

The Configuration section contains 3 configuration tabs:



CrowdStrike Scheduled Search: Configuration

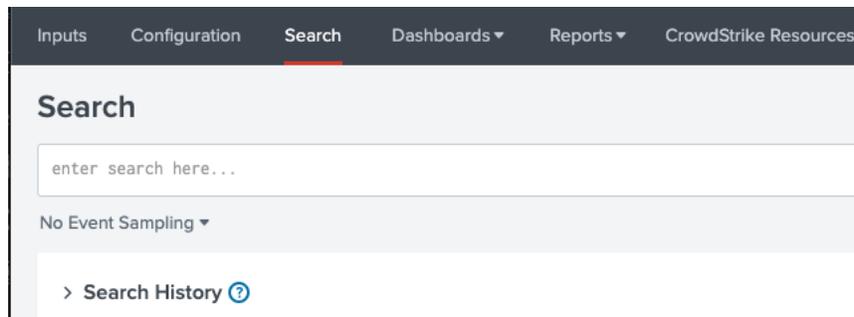
Configure a CrowdStrike OAuth2 Scheduled Search API account, proxy setting and logging level



- **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.

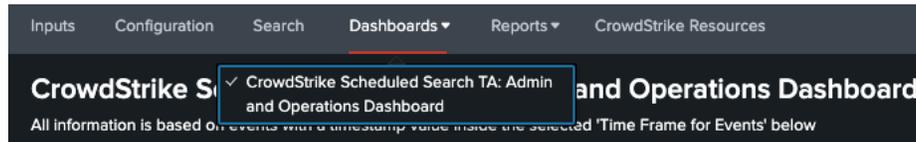
Search Section

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



Dashboards Section

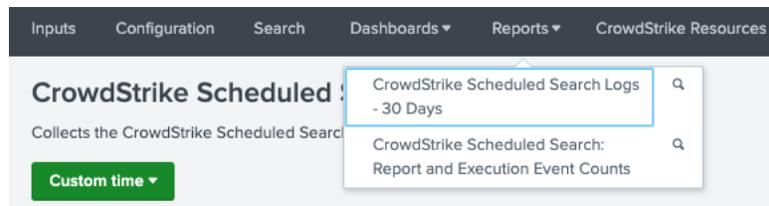
The Dashboards section is a dynamic dropdown that will display any views containing the phrase 'crowdstrike_scheduled_search' and by default will contain a single dashboard called 'CrowdStrike Scheduled Search TA: Admin and Operations Dashboard'. This dashboard is a simple example of a monitoring dashboard to assist customer with getting insight into the TA's current operations.



Since this is a dynamic listing, if the default dashboard is not accessible, is removed and/or there are no other views meeting the criteria, then the section will not be present. Similarly, if additional dashboards are added that meet the naming criteria and are accessible by the TA and user, they should be displayed in this dropdown.

Reports Section

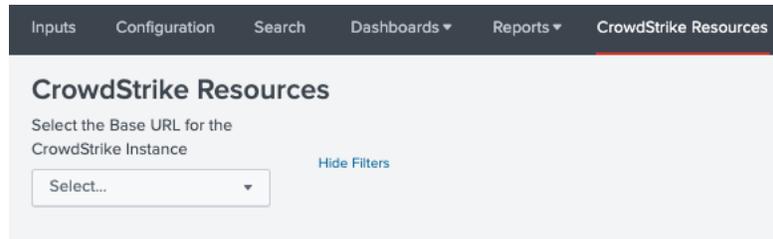
The Reports section is a dynamic dropdown that will display and reports containing the phrase 'CrowdStrike Scheduled Search' and by default will contain searches provided by CrowdStrike.



Since this is a dynamic listing, if the default reports are not accessible, are removed and/or there are no other report meeting the criteria, then the section will not be present. Similarly, if additional reports are added that meet the naming criteria and are accessible by the TA and user, they should be displayed in this dropdown.

CrowdStrike Resources Section

The CrowdStrike Resources Section contains resources around the specific TA, the CrowdStrike SDKs and an overview of the process to contact CrowdStrike support.



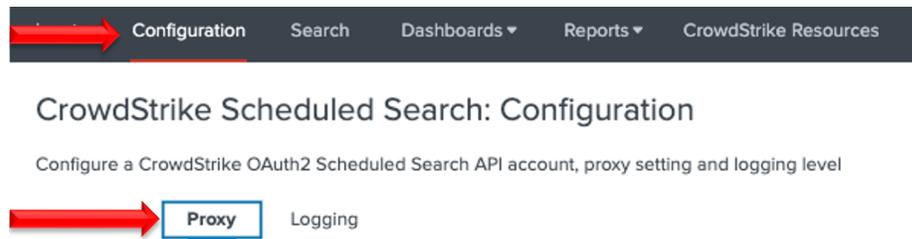
In order for some of the links to the documentation in the Falcon console to work properly please ensure that the correct base URL has been selected from the dropdown.

Configuring the TA to collect data

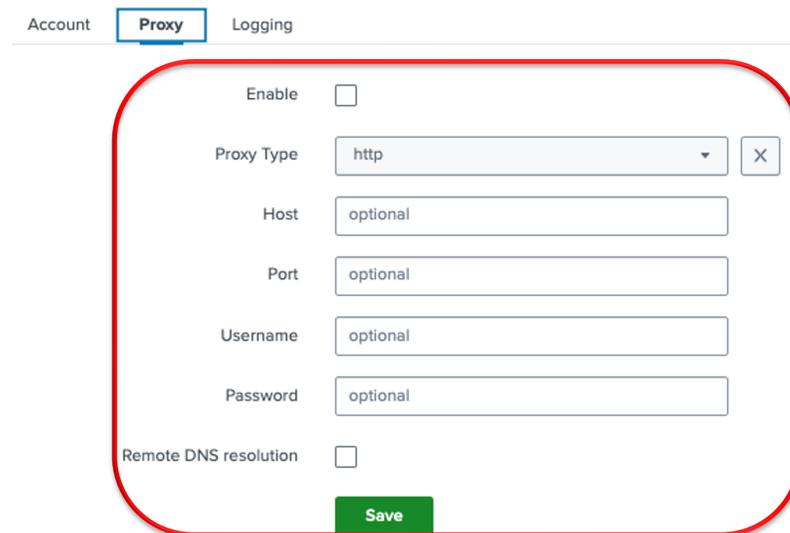
***NOTE* This action should only be performed on a Splunk instance designed for collecting data**

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.



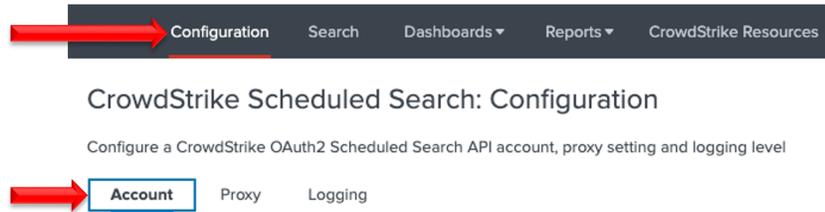
2. Configure the following fields as appropriate:

A screenshot of the "Proxy" configuration form in the Splunk interface. The form is enclosed in a red rounded rectangle. It contains the following fields: "Enable" (checkbox), "Proxy Type" (dropdown menu with "http" selected), "Host" (text input field with "optional" placeholder), "Port" (text input field with "optional" placeholder), "Username" (text input field with "optional" placeholder), "Password" (text input field with "optional" placeholder), and "Remote DNS resolution" (checkbox). A green "Save" button is located at the bottom right of the form.

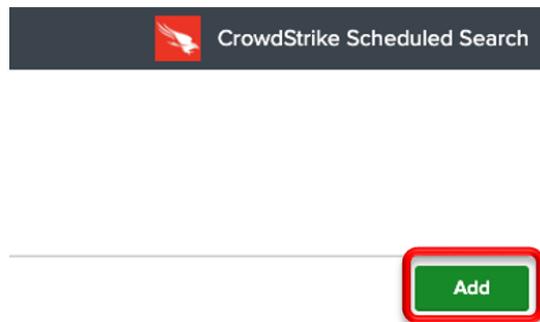
- **Enable:** This checkbox is used to enable/disable the proxy settings
- **Proxy Type:** This dropdown is used to select the proxy type
- **Host:** The hostname/IP address for the proxy server
- **Port:** The communication port for the proxy server
- **Username:** The authentication username for the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



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



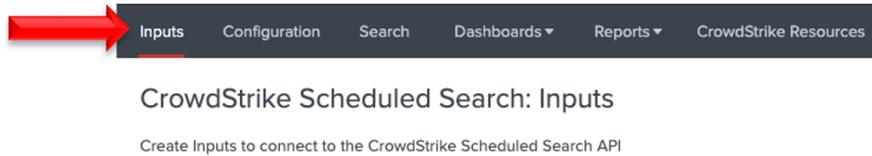
4. Configure the following fields:

- **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

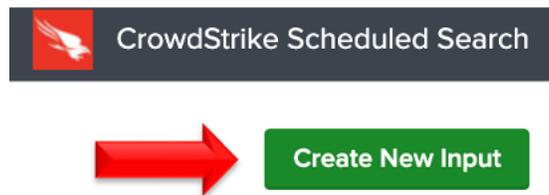
5. Click the ‘Add’ button in the bottom right corner to save the account.

Configure an Input

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



3. In the top right corner select 'Create New Input'



4. Configure the appropriate fields

Add CrowdStrike Scheduled Search×

[CrowdStrike Scheduled Search TA Guide](#)
[CrowdStrike FalconPy SDK Wiki](#)

*Name
Enter a unique name for the data input

*Interval
Time Interval of input in seconds - must be greater than or equal to 300 (5 Minutes)

*Index

*Select Cloud Environment
Select the appropriate cloud environment for the Falcon Instance

*API Credential
This is an OAuth2 based API credential with a Scheduled Reports 'Read' scope

*Scheduled Search Name
Enter the full name of the scheduled search from the Falcon UI

*Collection Options
Configure to collect historic or most recent search events

- **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 Commercial 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
- **Scheduled Search Name:** (required) The name of the scheduled search configured in the Falcon UI
- **Collection Options:** (required) Select one of two options
 - **Historic** – collects up to 499 searches done since the last collection
 - **Most Recent** – collects the most recent search since the last collection

Search Macros

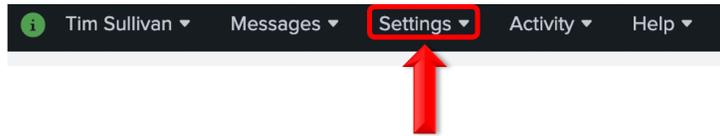
Search macros are reusable chunks of Search Processing Language (SPL) that you can insert into other searches. Search macros can be any part of a search, such as an eval statement or search term, and do not need to be a complete command. You can also specify whether the macro field takes any arguments.

<https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Definesearchmacros>

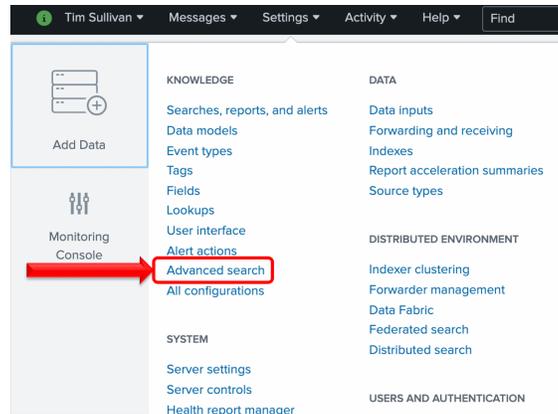
Locating the Search Macros

The search macros can be located by navigating to:

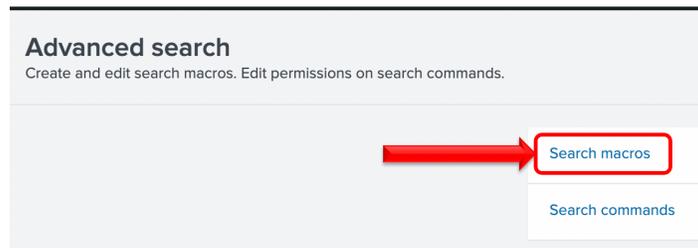
1. Select that 'Settings' dropdown in the Splunkbar :



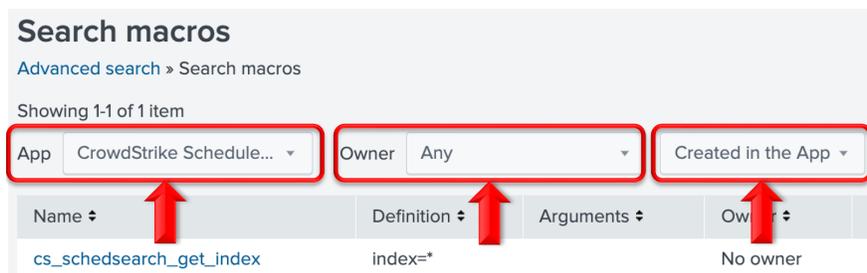
2. Select 'Advanced Search' from the dropdown menu:



3. Under 'Advanced Search' select 'Search Macros':



4. Ensure the 'CrowdStrike Scheduled Search Technical Add-on' is selected in the 'App' selection, 'Owner' is set to 'Any' and 'Created in App' is selected from the pulldown selection:



Configuring and Leveraging the Search Macro(s)

There currently is only 1 search macro that requires configuration.

Name ↕	Definition ↕	Arguments ↕
<code>cs_schedsearch_get_index</code>	<code>index=*</code>	

- ``cs_schedsearch_get_index`` (CrowdStrike Schedule Search 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 `'*` and should be adjusted to reflect the specific index(es) that the data is being pushed to.

The other search macros that are available once the required search macro has been properly configured:

<code>cs_schedsearch_get_execution()</code>	<code>`cs_schedsearch_get_index` spath "ta_data.Execution_Data.id" search "ta_data.Execution_Data.id"=\$Execution_ID\$</code>	Execution_ID	No owner	TA-crowdstrike-scheduled-search	Global Permissions	Enabled Disable
<code>cs_schedsearch_get_report()</code>	<code>`cs_schedsearch_get_index` spath "ta_data.Report_Data.id" search "ta_data.Report_Data.id"=\$Report_ID\$</code>	Report_ID	No owner	TA-crowdstrike-scheduled-search	Global Permissions	Enabled Disable

- ``cs_schedsearch_get_execution(1)`` A search macro that takes 1 input, the execution id (ta_data.Execution_Data.id). This search macro will search the configured index(es) for the execution if contained in the parenthesis.
- ``cs_schedsearch_get_report(1)`` A search macro that takes 1 input, the report id (ta_data.Report_Data.id). This search macro will search the configured index(es) for the report id contained in the parenthesis.

NOTE: These search macros will not function efficiently if the ``cs_schedsearch_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_schedsearch_get_index``

New Search

``cs_schedsearch_get_index``

✓ **1,929 events** (5/1/23 8:00:00.000 AM to 5/2/23 8:19:18.000 AM) No Event Sampling ▾

``cs_schedsearch_get_execution(afcd62f77c18476ca9ac81e409e75da0)``

New Search

``cs_schedsearch_get_execution(afcd62f77c18476ca9ac81e409e75da0)``

✓ **101 events** (5/1/23 8:00:00.000 AM to 5/2/23 8:26:49.000 AM) No Event Sampling ▾

``cs_schedsearch_get_report(8faebdd436542d7b07f6287a4c6b2f1)``

New Search

``cs_schedsearch_get_report(8faebdd436542d7b07f6287a4c6b2f1)``

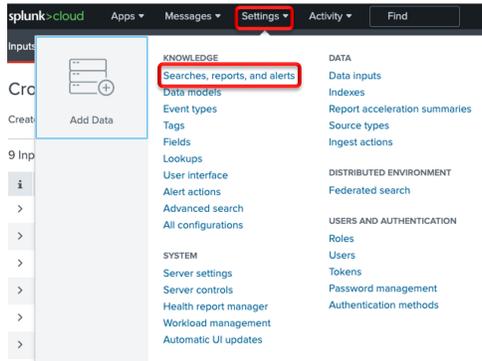
✓ **315 events** (5/1/23 8:00:00.000 AM to 5/2/23 8:23:00.000 AM) No Event Sampling ▾

Reports

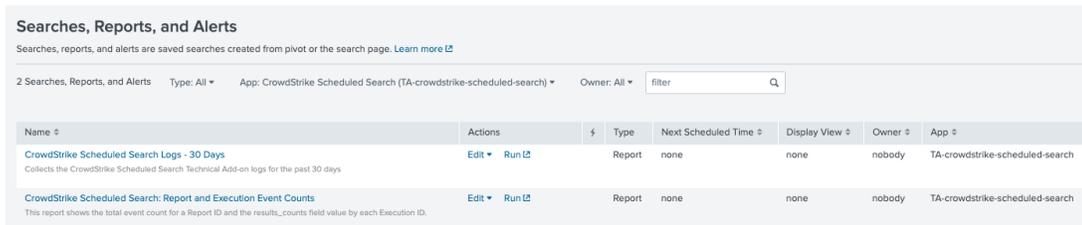
Locating the Reports

The reports included in the TA can be found using the dynamic dropdown in the TA navigation bar or by navigating to them in the Splunk Settings.

- Open the Settings menu, under 'knowledge' select 'Searches, reports and alerts':



- In the 'App' dropdown ensure that the 'CrowdStrike Scheduled Search' 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 Scheduled Search (TA-crowdstrike-scheduled-search) Owner: All filter

Name	Actions	Type	Next Scheduled Time	Display View	Owner	App
CrowdStrike Scheduled Search Logs - 30 Days <small>Collects the CrowdStrike Scheduled Search Technical Add-on logs for the past 30 days</small>	Edit Run	Report	none	none	nobody	TA-crowdstrike-scheduled-search
CrowdStrike Scheduled Search: Report and Execution Event Counts <small>This report shows the total event count for a Report ID and the results_counts field value by each Execution ID.</small>	Edit Run	Report	none	none	nobody	TA-crowdstrike-scheduled-search

Current Reports

There are currently 2 reports included with the TA.

Report: CrowdStrike Scheduled Search Logs – 30 Days

The Search Logs – 30 Days report will search for TA logs for the past 30 days. This report should be run and the results provided to CrowdStrike support when opening a support request, ensure that the timeframe encompasses the timeframe of the issue and the logging is in debug.



CrowdStrike Scheduled Search Logs - 30 Days Edit Run Report

Collects the CrowdStrike Scheduled Search Technical Add-on logs for the past 30 days

Report: CrowdStrike Scheduled Search Report and Execution Event Counts



CrowdStrike Scheduled Search: Report and Execution Event Counts Edit Run Report

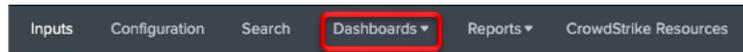
This report shows the total event count for a Report ID and the results_counts field value by each Execution ID.

Report and Execution Event Counts report shows a total count of events for a report ID and also shows the 'results_count' field value for associated execution IDs within the timeframe.

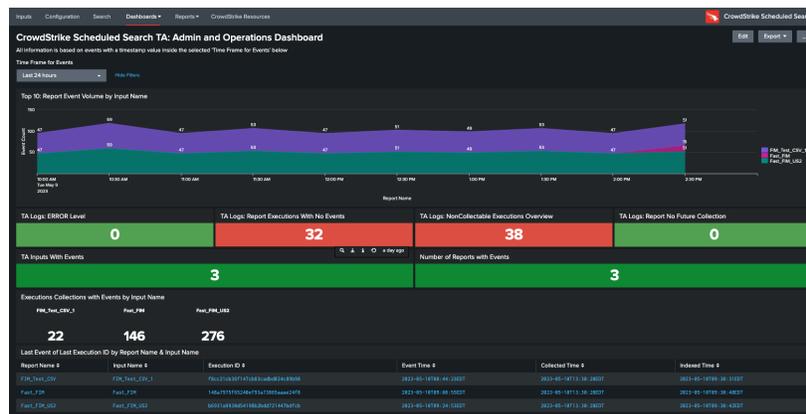
Dashboards

Locating the Dashboards

The dashboards included in the TA can be found using the dynamic dropdown in the TA navigation bar.



CrowdStrike Schedules Search TA: Admin and Operations Dashboard

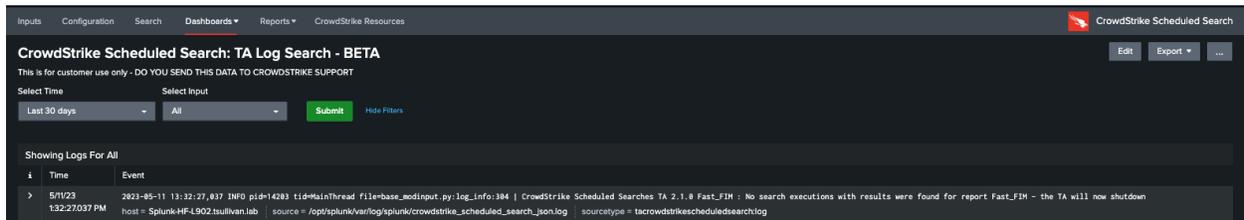


- **Time Frame for Events:** Selects the time frame to search for events and logs, all event-based data (reports/executions/event) must have events within this time frame.
- **Top 10 Report Event Columns by Input Name:** Shows the top 10 input event volumes by the name of the input.
- **TA Logs ERROR Level:** Shows the number of error log events in the TA logs.
- **TA Logs Report Executions with No Events:** Shows the number of logs reflecting a successful report execution that returned no events in the TA logs.
- **TA Logs NonCollectable Executions Overview:** Shows the number of logs reflecting report executions that did not have a successful status and the associated messages.
- **TA Logs: Report No Future Collections:** Shows the number of logs reflecting a report where the report details do not show a next scheduled collection.
- **TA Inputs with Events:** Counts the number of TA inputs that have events within the given timeframe.
- **Number of Reports with Events:** Counts the number of reports that have events within the given timeframe.
- **Executions Collections with Events by Input Name:** Shows the number of executions that have events within the given time frame by report name.
- **Last Event of Last Execution ID by Report Name & Input Name:** Shows the latest execution ID by the report and input names and provides the latest events event timestamp, collected timestamp and indexed timestamp.

CrowdStrike Schedules Search TA: TA Log Search – BETA Dashboard

NOTE: THIS DASHBOARD IS FOR CUSTOMER USE ONLY AND SHOULD NOT BE USED TO PROVIDE NECESSARY LOG DATA TO CROWDSTRIKE SUPPORT UNLESS SPECIFICALLY DIRECTED TO DO SO

This dashboard can be used for a quick check of the TA logs and can also filter the logs by the input name. However, filtering by the input name does not provide all the related debugging logs and as such this dashboard is not designed to be a replacement for the TA logs report. This dashboard also does not provide the level of information need for opening a support request and as cannot be used as a substitute for the 30 day log report.



- **Select Time:** Select the timeframe to view the TA logs.
- **Select Input:** This is a self-populating dropdown list that will do a search for input names within the TA logs for the selected timeframe. The default is to search for all inputs.

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 data. Depending on the use case(s) and the Splunk architecture, the use of dedicated indexes for specific schedule search inputs is often strongly recommended.

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 and well as the number of API calls being made per minute. The TA should have enough time to process the collected data and the frequency should be configured to avoid any API throttling.

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:

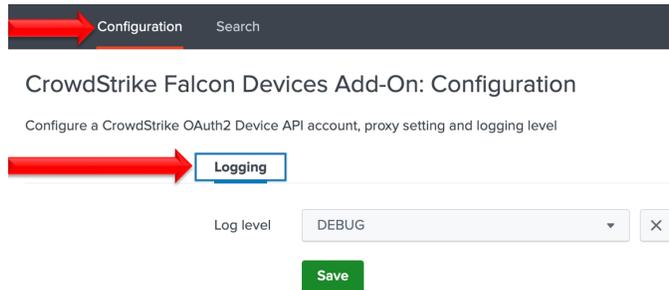
- Proxy based issues
- Firewall based issues
- Network connectivity issues
- Authentication issues (based on misconfigured credentials)
- Splunk CIM field mapping
- Splunk environmental/configuration-based issues

Configuring the TA to collect log data

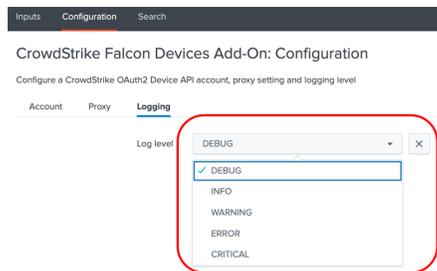
The TA logging level is set to 'info' by default and will only log a minimal amount of information. To properly troubleshoot issues with the TA the logging level should be set to 'debug'.

Change Logging Level

1. Navigate to the Configuration section, Logging tab:



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



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

Review Log Data in Splunk

1. Run and review the **CrowdStrike Scheduled Search 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 RAW format and include them in any support requests.

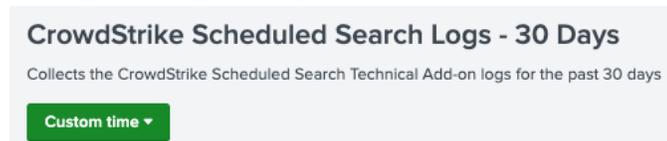
Examples of Troubleshooting Situations and Remediation Steps

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. 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.
- 1.4. Ensure that the scheduled search has run and that there were results for those runs.
- 1.5. Review the Admin and Operations Dashboard for log events that don't contain events or whose executions were completed. These are drilldowns and can be clicked on to see the underlying events.

TA Logs: Executions With No Events	TA Logs: NonCollectable Executions Overview
48	48

- 1.6. Review the TA logs for any indication of issues, these logs can be viewed using the log report in the Reports pulldown menu. For the best results it's recommended to set the logging level to 'debug' and repeat any actions that need to be examined.



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. Compare the 'Collection_time' field value under the 'ta_data' section of the event to the time that it was indexed. The collection time for the event is create when the input starts the process of collecting scheduled search data and then is added to the events.

3. The data being collected does not look 'complete':

- 3.1. 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.
- 3.2. Perform a count of the events by the execution id and compare the results to the count under 'ta_data'-'Execution_Data'-'result_metadata'-'results_count'.

```
result_metadata: {  
  execution_delay:  
  execution_durati  
  execution_finish  
  execution_start:  
  queue_duration: :  
  queue_start: 202:  
  report_file_name  
  report_finish: 21  
  result_count: 8  
  result_id:
```

In the event that the count number is multiples higher than the 'results_count' number, ensure that the execution has only been ingest once. Adding the 'Collection_time' and/or 'Input_name' can also be used to narrow the search.

4. There's more TA Inputs with Events than Number of Reports with Events in the Admin and Operations Dashboard:

- 4.1. This can happen if there are multiple inputs configured to collect the same report. If this is not by design delete one of the reports. This should not happen for a report with the same name as it's based on the report ID.

Support

This TA is designed to help facilitate the collection of scheduled search data provided by the CrowdStrike API(s). CrowdStrike provides support for the TA code functionality as it was designed.

Examples of instances that **would fall outside** of CrowdStrike's support:

- Trying to collect CrowdStrike Scheduled Reports
- Environment or configurations 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
- Deployments, configurations, modifications that do not align with what is outlined in this documentation
- Support requests without the appropriate data outlined below
- Splunk CIM field mapping or custom data modification requests
- Issues related to Splunk searches attempting to model the same data as found in the Falcon UI

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 Scheduled Search Logs – 30 Days** Report with the time picker set to 'All Time' and export all the results in RAW format
 - b. (If possible) Download the all-log files containing 'ta_crowdstrike_scheduled_search' 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 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.