CrowdStrike Unified Alerts Add-on for Splunk

Installation and Configuration Guide v2.3.0+

Table of Contents

Introduction

This guide covers the deployment, configuration and usage of the CrowdStrike Unified Alerts Technical Add-on (TA) for Splunk version 2.3.0 and up.

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

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. 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.

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
Alerts	✓	

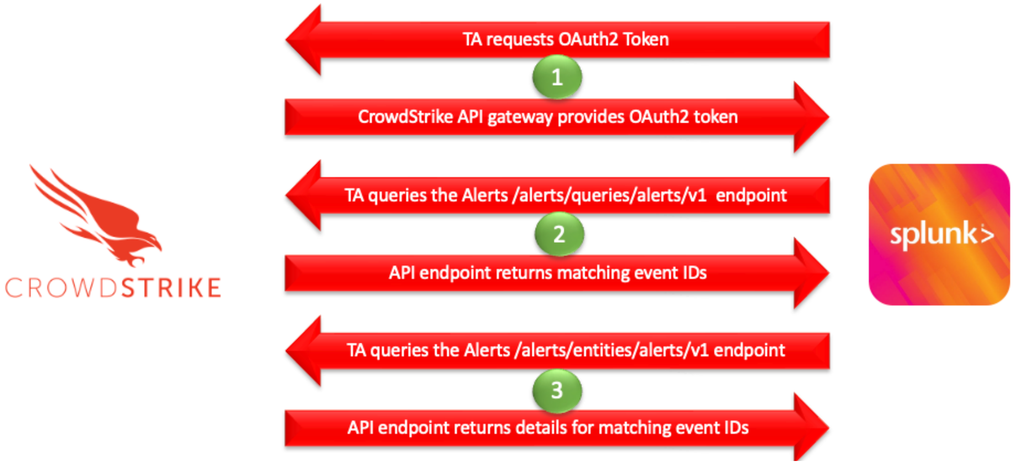
API Endpoint	Potential fields(s)
/oauth2/token	
/alerts/queries/alerts/v1	updated_timestamp
/alerts/entities/alerts/v1	ids

*Note: The value used for the 'ids' field is actually the 'composite_id' value in the event details.

For more information about these API endpoints please refer to the *Incident, Detection, and Alert Monitoring APIs* documentation in the Falcon console.

The TA will use the updated_timestamp field value in the event data as the timestamp of the event. The TA will also use the value 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 'updated_timestamp' value of '2023-04-27T17:15:24Z', then the next collection interval would request events that happened after '2023-04-27T17:15:24Z'. This value can be located in the 'ta_data' section of the event under 'Timestamp_value'.

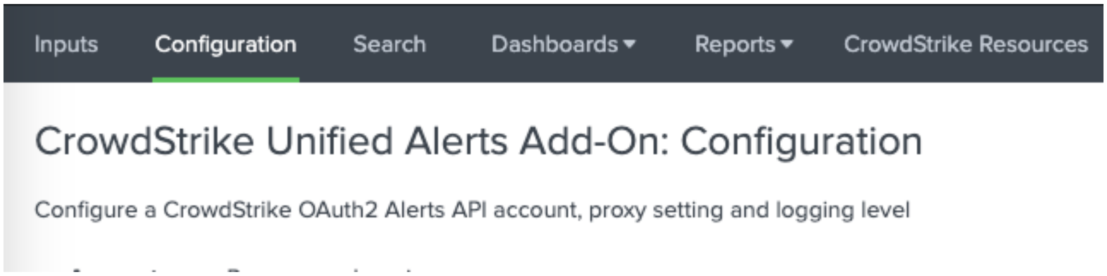
High Level API Call Flow


TA requests OAuth2 Token
1
CrowdStrike API gateway provides OAuth2 token
CROWDSTRIKE
TA queries the Alerts /alerts/queries/alerts/v1 endpoint
2
API endpoint returns matching event IDs
splunk>
TA queries the Alerts /alerts/entities/alerts/v1 endpoint
3
API endpoint returns details for matching event IDs

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 is valid the API gateway will respond to the TA with an OAuth2 token.
2. The TA will call the Alerts API to collect any event ids that match the search criteria.
3. The TA will take any event ids provided and call the Alerts API to get the available details on those ids.

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 timestamp field value into the Splunk KVStore.

Technical Add-On Layout



CrowdStrike Unified Alerts Add-On: Configuration

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

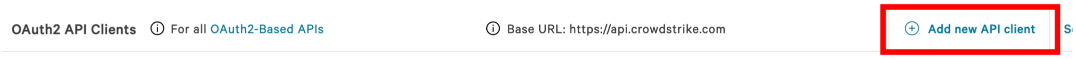
The CrowdStrike Unified ALerts TA has 6 selections associated with it:

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_Unified_Alerts' 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 Unified Alerts' in the name, by default the CrowdStrike provided reports will be listed.
6. **CrowdStrike Resources** – A dashboard that provides links to addition information about the TA, the FalconPy SDK and the CrowdStrike support process.

Creating/Validating the API Credential Scope

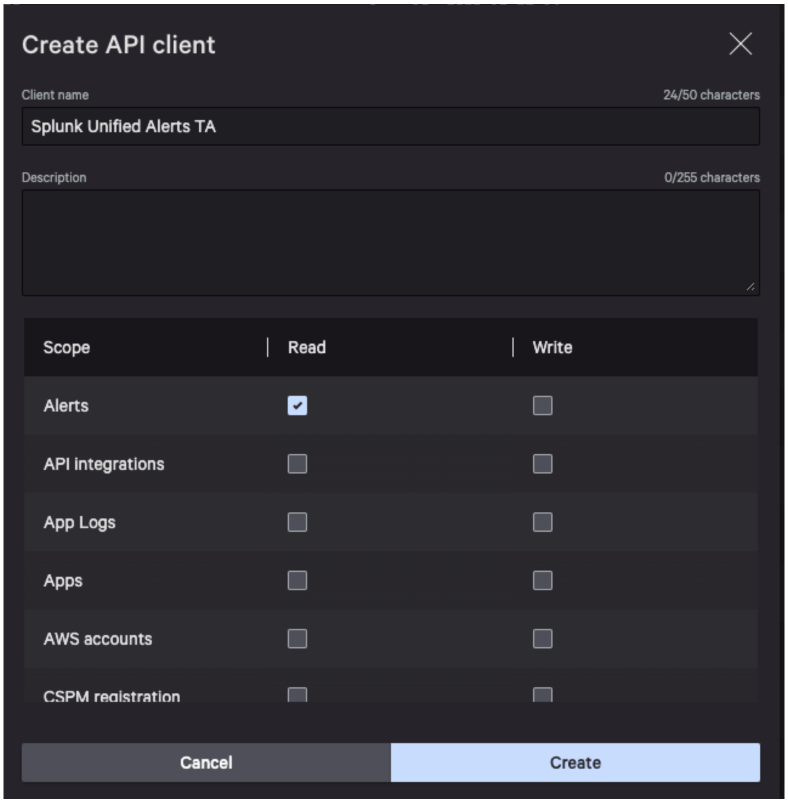
While the CrowdStrike Unified Alerts TA can leverage an existing OAuth2 based API credential, but it's often preferred to create a dedicated credential. This can be accomplished by the following:

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

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



Create API client

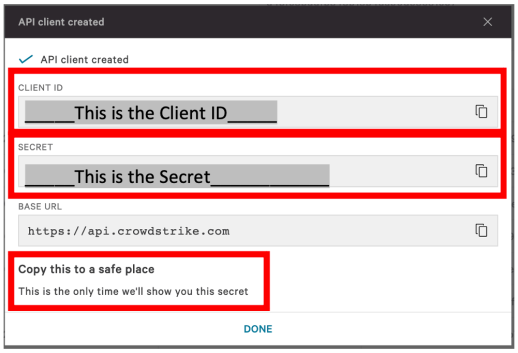
Client name 24/50 characters

Splunk Unified Alerts TA

Description 0/255 characters

Scope	Read	Write
Alerts	☑	□
API integrations	□	□
App Logs	□	□
Apps	□	□
AWS accounts	□	□
CSPM registration	□	□

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

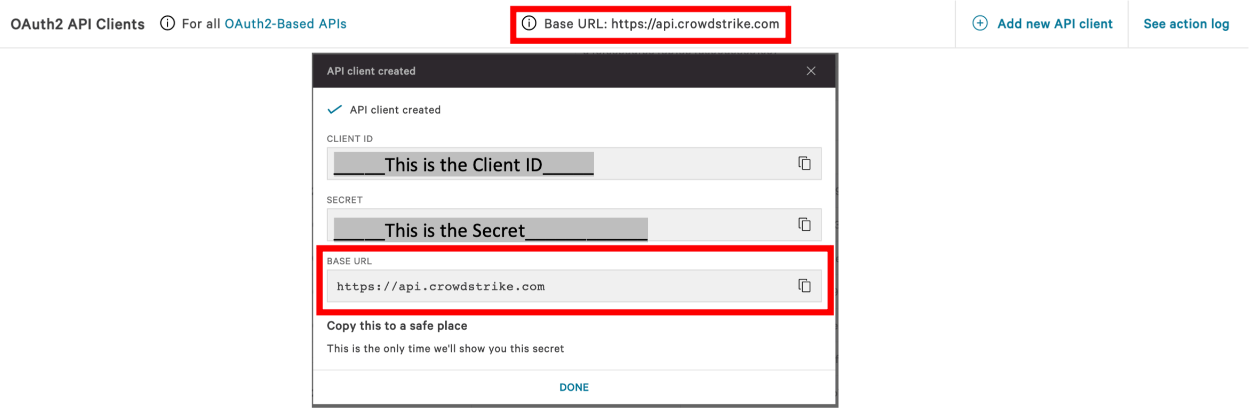
https://api.crowdstrike.com

Copy this to a safe place

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

DONE

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



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

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

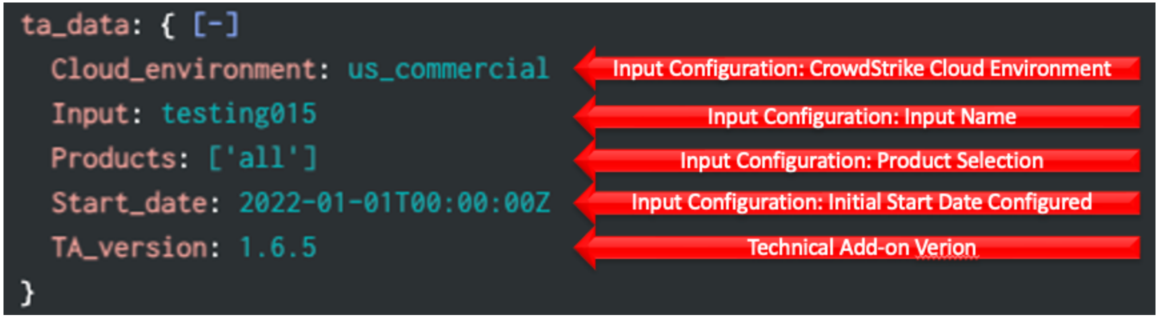
This is the only time we'll show you this secret

DONE

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_commercial
  Input: testing015
  Products: ['all']
  Start_date: 2022-01-01T00:00:00Z
  TA_version: 1.6.5
}
```

Input Configuration: CrowdStrike Cloud Environment
Input Configuration: Input Name
Input Configuration: Product Selection
Input Configuration: Initial Start Date Configured
Technical Add-on Verion

- **Cloud Environment**: The CrowdStrike Cloud selected in the input configuration.
- **Input_name**: The name of the configured input.
- **Products**: The products selected to collect alerts from.
- **Start_date**: The start date used in the configured input (optional).
- **TA_version**: The version of the TA that did the data collection.

Proxy Considerations

The CrowdStrike Unified Alerts 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.

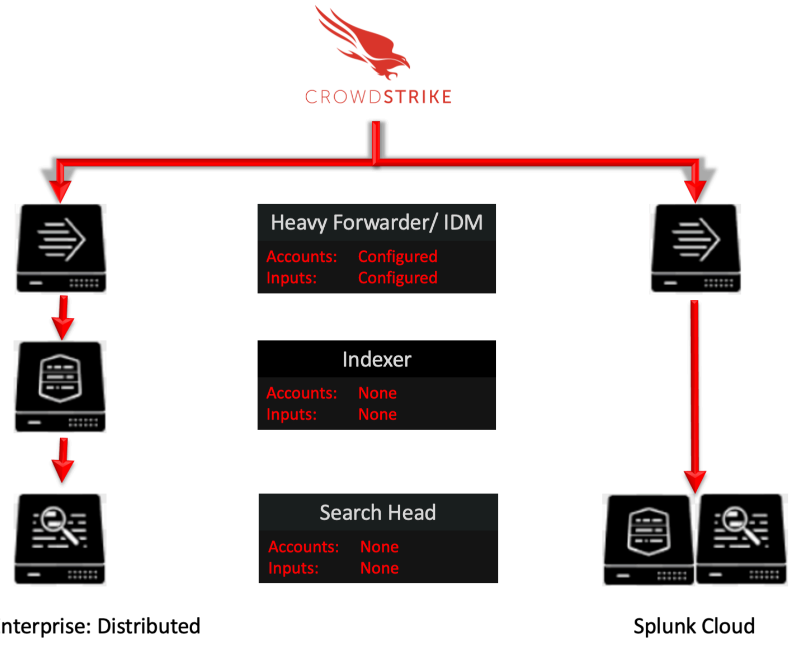
Splunk Indexer(s): The TA can be installed to provide field mapping and search macro support. The TA should be deployed without any accounts or inputs configured and any search macros should be properly configured for use. If a custom index is going to be used, then it should be created here.

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.

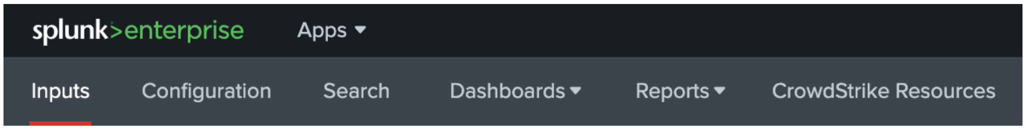
The following diagram shows the flow of data from the CrowdStrike API and the CrowdStrike TA configuration within a distributed Splunk Enterprise and Splunk Cloud environment:



Configuring the TA

TA Layout

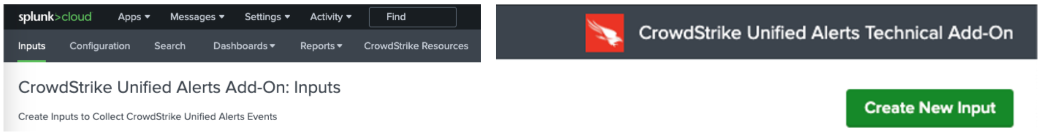
The TA contains 6 sections:



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

Inputs Section

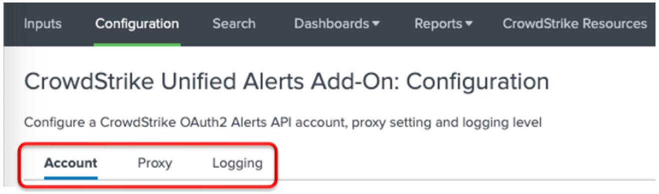
The Inputs section is where inputs are configured, modified and listed. Prior to configuring any inputs an account needs to be created under the Configuration section (see the Configuration Section of this document). The Inputs section contains a ‘button’ that will create a new input configuration in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



splunk>cloud
Apps ▾
Messages ▾
Settings ▾
Activity ▾
Find
Inputs
Configuration
Search
Dashboards ▾
Reports ▾
CrowdStrike Resources
CrowdStrike Unified Alerts Add-On: Inputs
Create Inputs to Collect CrowdStrike Unified Alerts Events
CrowdStrike Unified Alerts Technical Add-On
Create New Input

Configuration Section

The Configuration section contains 3 configuration tabs:

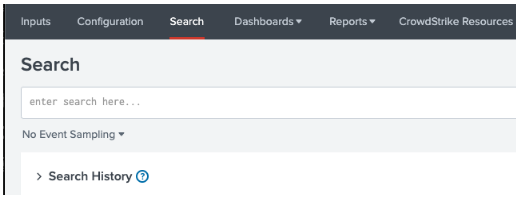


Inputs
Configuration
Search
Dashboards ▾
Reports ▾
CrowdStrike Resources
CrowdStrike Unified Alerts Add-On: Configuration
Configure a CrowdStrike OAuth2 Alerts API account, proxy setting and logging level
Account
Proxy
Logging

- **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.

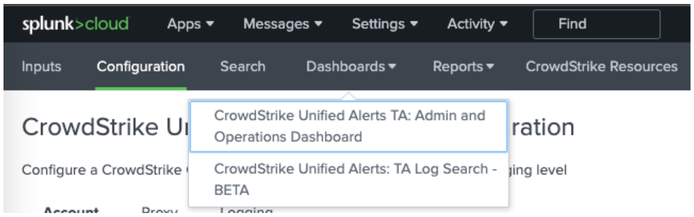
Search Section

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



Dashboards Section

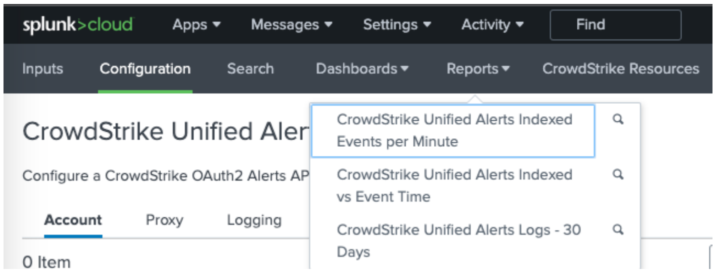
The Dashboards section is a dynamic dropdown that will display any views containing the phrase ‘Crowdstrike_Unified_Alerts’ and by default will contain 2 dashboards. The first is called the ‘CrowdStrike Unified Alerts TA: Admin and Operations Dashboard’ and is a simple example of a monitoring dashboard to assist customer with getting insight into the TA’s current operations. The second is a dashboard called ‘CrowdStrike Unified Alerts: TA Log Search – BETA’ and is a simple example of a log search to assist customer in reviewing TA related log files.



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

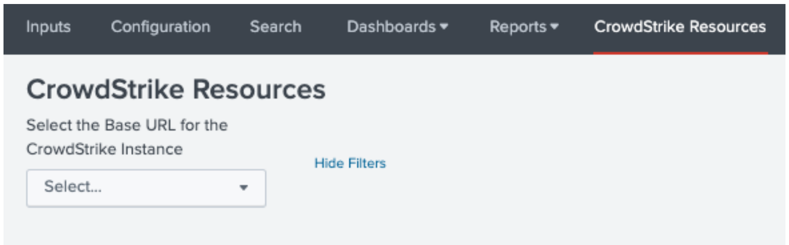
The Reports section is a dynamic dropdown that will display and reports containing the phrase ‘CrowdStrike Unified Alerts’ and by default will contain searches provided by CrowdStrike.


splunk>cloud
Apps
Messages
Settings
Activity
Find
Inputs
Configuration
Search
Dashboards
Reports
CrowdStrike Resources
CrowdStrike Unified Aler
Configure a CrowdStrike OAuth2 Alerts AP
Account
Proxy
Logging
0 Item
CrowdStrike Unified Alerts Indexed Events per Minute
CrowdStrike Unified Alerts Indexed vs Event Time
CrowdStrike Unified Alerts Logs - 30 Days

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.



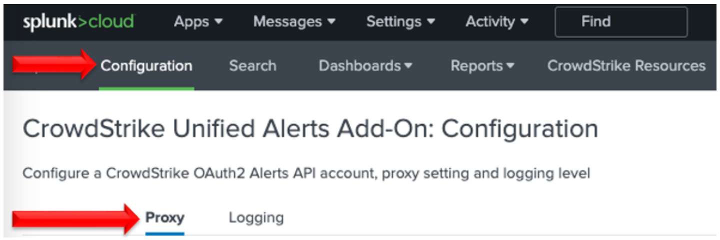
In order for some of the links to the documentation in the Falcon console to work properly please ensure that the correct base URL has been selected from the dropdown.

Configuring the TA to collect data

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

Configure Proxy Settings (optional)

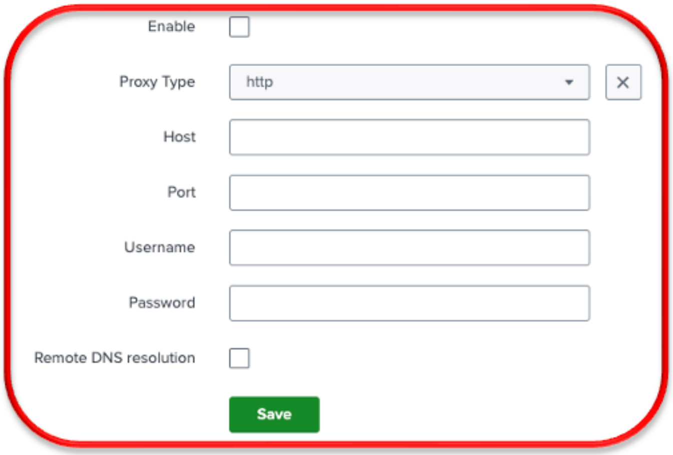
1. Proxy settings are configured under the Configuration section, Proxy tab. Proxies can cause authentication issue if not configured correctly, the proxy should not perform SSL/TLS proxying on any API calls.



CrowdStrike Unified Alerts Add-On: Configuration

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

2. Configure the following fields as appropriate:



Enable □

Proxy Type: http

Host

Port

Username

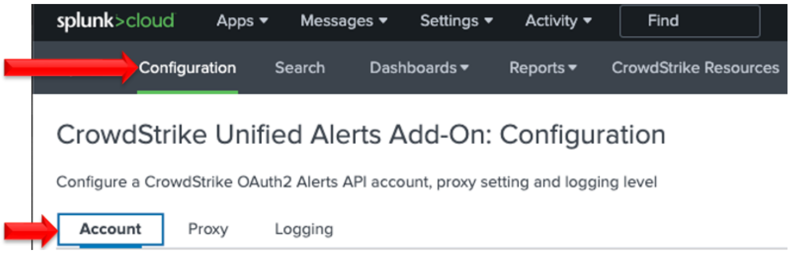
Password

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

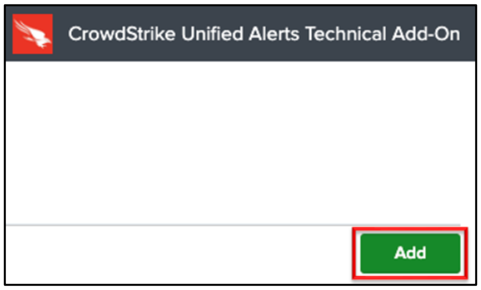
1. An account is configured using a properly scoped OAuth2 API credential.
2. An account is created under the Configuration section, Account tab:



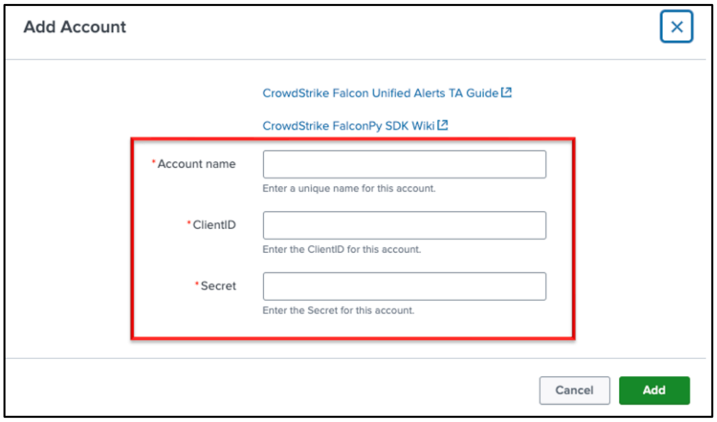
CrowdStrike Unified Alerts Add-On: Configuration

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

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



4. Configure the following fields:


Add Account
×
CrowdStrike Falcon Unified Alerts TA Guide
CrowdStrike FalconPy SDK Wiki
Cancel
Add

*Account name

Enter a unique name for this account.

*ClientID

Enter the ClientID for this account.

*Secret

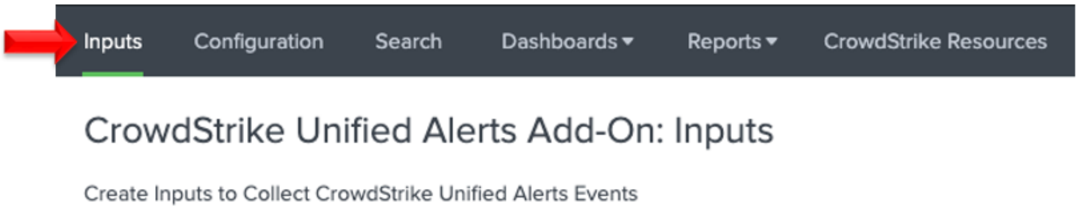
Enter the Secret for this account.

- **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

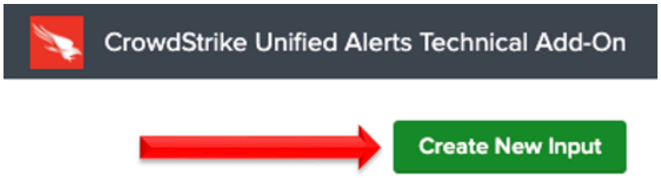
1. An input will require a valid account be already created.
2. An input is created under the Inputs section:



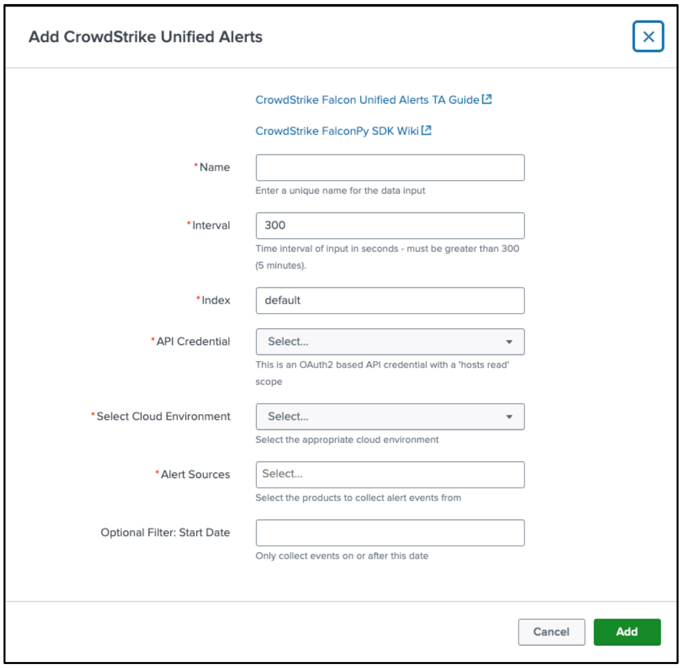
CrowdStrike Unified Alerts Add-On: Inputs

Create Inputs to Collect CrowdStrike Unified Alerts Events

3. In the top right corner select ‘Create New Input’



4. Configure the appropriate fields



Add CrowdStrike Unified Alerts

CrowdStrike Falcon Unified Alerts TA Guide

CrowdStrike FalconPy SDK Wiki

*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

*API Credential: Select...

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

*Select Cloud Environment: Select...

Select the appropriate cloud environment

*Alert Sources: Select...

Select the products to collect alert events from

Optional Filter: Start Date:

Only collect events on or after this date

Field Name	Configuration	Description
Name	required	A name unique to the Splunk Environment
Interval	required	How often the TA will collect data, expressed in seconds
Index	required	The Splunk Index that the data will be stored in
API Credential	required	The configured account used to authenticate to the CrowdStrike API
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
Alert Sources	required	The product types to collect alerts from
Start Date	optional	A date to start the initial collection on

Search Macros

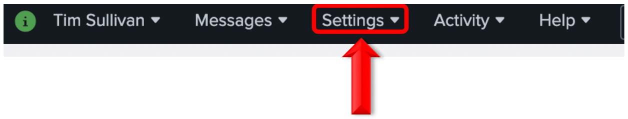
Search macros are reusable chunks of Search Processing Language (SPL) that you can insert into other searches. Search macros can be any part of a search, such as an eval statement or search term, and do not need to be a complete command. You can also specify whether the macro field takes any arguments.

https://docs.splunk.com/Documentation/Splunk/9.1.1/Knowledge/Definesearchmacros

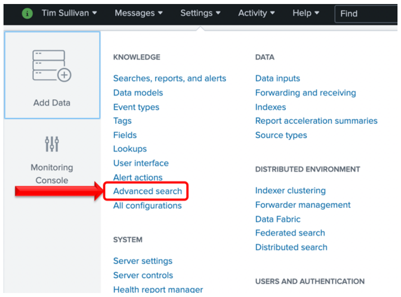
Locating the Search Macros

The search macros can be located by navigating to:

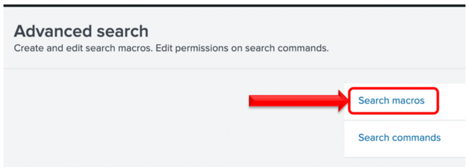
1. Select that 'Settings' dropdown in the Splunkbar:



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

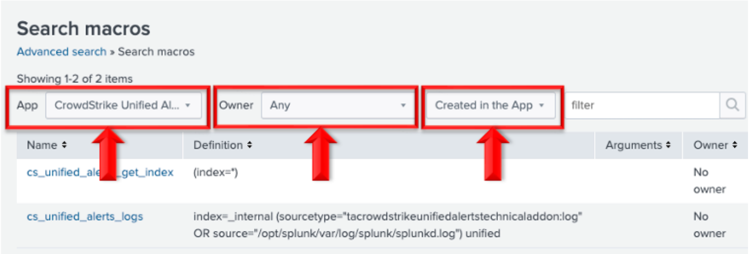


3. Under 'Advanced Search' select 'Search Macros:


Advanced search

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

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


Search macros

Advanced search » Search macros

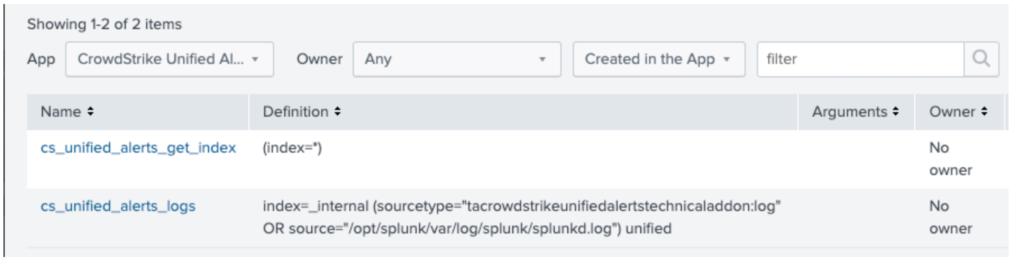
Showing 1-2 of 2 items

App: CrowdStrike Unified Al... ▾ Owner: Any ▾ Created in the App ▾ filter

Name ⬍	Definition ⬍	Arguments ⬍	Owner ⬍
cs_unified_ale_get_index	(index=*)		No owner
cs_unified_alerts_logs	index=_internal (sourcetype="tacrowdstrikeunifiedalertstechnicaladdon:log" OR source="/opt/splunk/var/log/splunk/splunkd.log") unified		No owner

Configuring and Leveraging the Search Macro(s)

There currently are 2 search macros, 1 of which requires configuration.



Showing 1-2 of 2 items

App: CrowdStrike Unified Al... | Owner: Any | Created in the App | filter

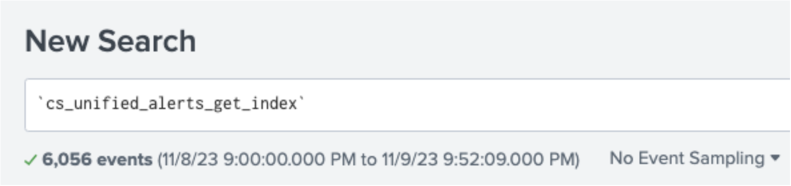
Name	Definition	Arguments	Owner
cs_unified_alerts_get_index	(index=*)		No owner
cs_unified_alerts_logs	index=_internal (sourcetype="tacrowdstrikeunifiedalertstechnicaladdon:log" OR source="/opt/splunk/var/log/splunk/splunkd.log") unified		No owner

- **`cs_unified_alerts_get_index`** (CrowdStrike Unified Alerts 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.
- **`cs_unified_alerts_logs`** A search macro that is used to collect TA logs from both the TA logs and the splunkd.log sources.

NOTE: Some TA reporting, dashboarding and other functionality will not function efficiently if the `cs_unified_alerts_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

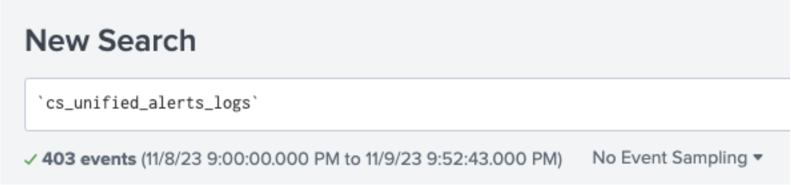
`cs_unified_alerts_get_index`



```
`cs_unified_alerts_get_index`
```

✓ **6,056 events** (11/8/23 9:00:00.000 PM to 11/9/23 9:52:09.000 PM)

`cs_unified_alerts_logs`



```
`cs_unified_alerts_logs`
```

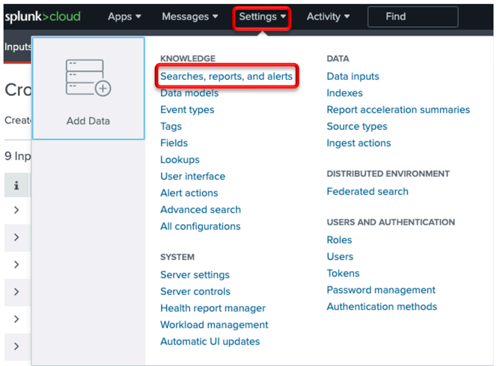
✓ **403 events** (11/8/23 9:00:00.000 PM to 11/9/23 9:52:43.000 PM)

Reports

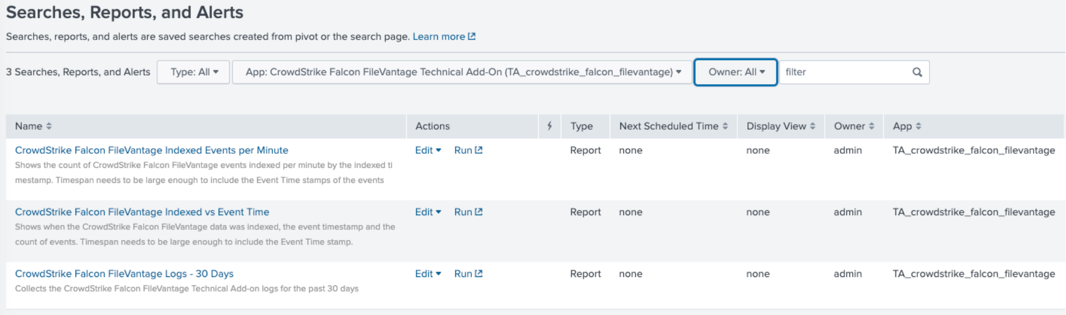
Locating the Reports

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

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



- In the ‘App’ dropdown ensure that the ‘CrowdStrike Unified Alerts’ 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

3 Searches, Reports, and Alerts | Type: All | App: CrowdStrike Falcon FileVantage Technical Add-On (TA_crowdstrike_falcon_filevantage) | Owner: All | filter

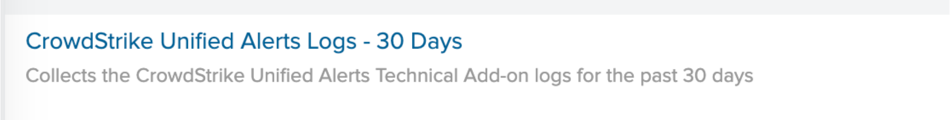
Name	Actions		Type	Next Scheduled Time	Display View	Owner	App
CrowdStrike Falcon FileVantage Indexed Events per Minute Shows the count of CrowdStrike Falcon FileVantage events indexed per minute by the indexed ti mestamp. Timespan needs to be large enough to include the Event Time stamps of the events	Edit Run		Report	none	none	admin	TA_crowdstrike_falcon_filevantage
CrowdStrike Falcon FileVantage Indexed vs Event Time Shows when the CrowdStrike Falcon FileVantage 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	none	none	admin	TA_crowdstrike_falcon_filevantage
CrowdStrike Falcon FileVantage Logs - 30 Days Collects the CrowdStrike Falcon FileVantage Technical Add-on logs for the past 30 days	Edit Run		Report	none	none	admin	TA_crowdstrike_falcon_filevantage

Current Reports

There are currently 3 reports included with the TA.

Report: CrowdStrike Unified Alerts Logs – 30 Days

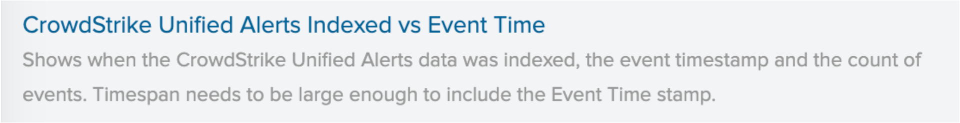
The Search Logs – 30 Days report will search for TA logs for the past 30 days. This report should be run and the results provided to CrowdStrike support when opening a support request, ensure that the timeframe encompasses the timeframe of the issue and the logging is in debug.



CrowdStrike Unified Alerts Logs - 30 Days

Collects the CrowdStrike Unified Alerts Technical Add-on logs for the past 30 days

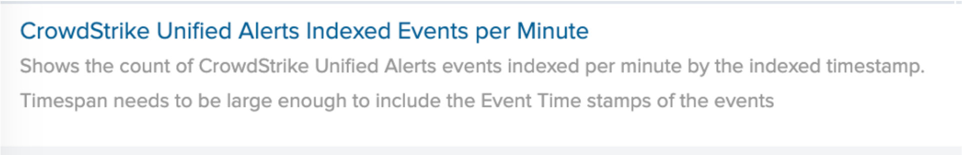
Report: CrowdStrike Unified Alerts Indexed Events per Minute



CrowdStrike Unified Alerts Indexed vs Event Time

Shows when the CrowdStrike Unified Alerts data was indexed, the event timestamp and the count of events. Timespan needs to be large enough to include the Event Time stamp.

Report: CrowdStrike Unified Alerts Indexed vs Event Time



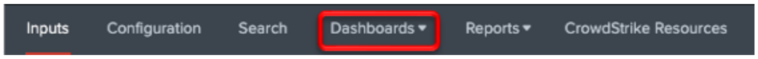
CrowdStrike Unified Alerts Indexed Events per Minute

Shows the count of CrowdStrike Unified Alerts events indexed per minute by the indexed timestamp. Timespan needs to be large enough to include the Event Time stamps of the events

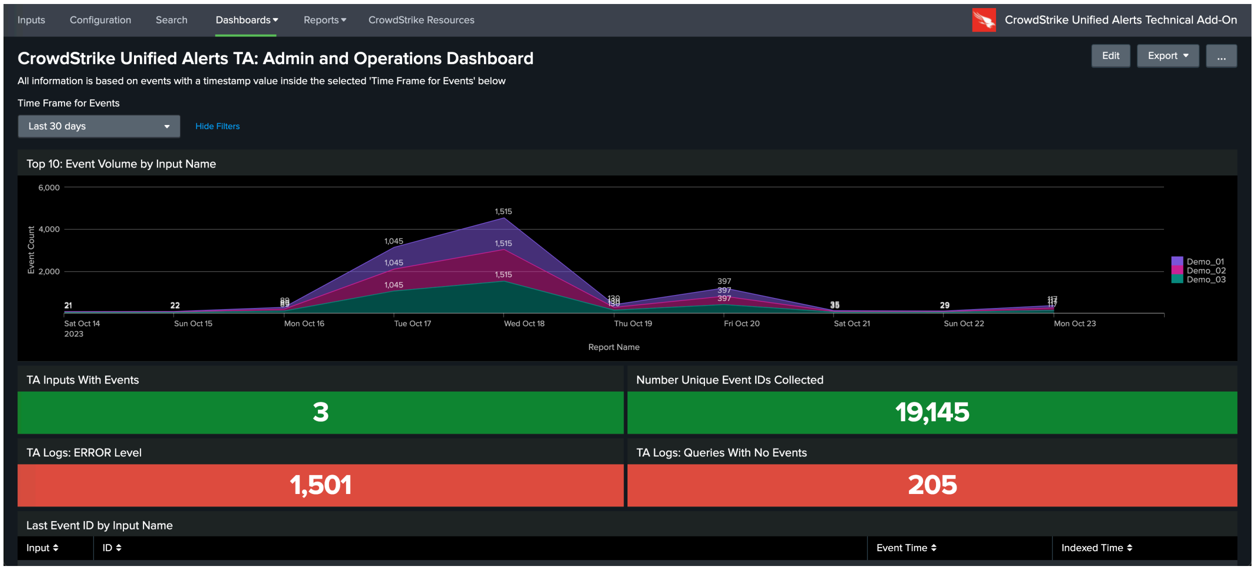
Dashboards

Locating the Dashboards

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



CrowdStrike Unified Alerts TA: Admin and Operations Dashboard



CrowdStrike Unified Alerts TA: Admin and Operations Dashboard

All information is based on events with a timestamp value inside the selected 'Time Frame for Events' below

Time Frame for Events: Last 30 days

Hide Filters

Top 10: Event Volume by Input Name

TA Inputs With Events: 3

Number Unique Event IDs Collected: 19,145

TA Logs: ERROR Level: 1,501

TA Logs: Queries With No Events: 205

Last Event ID by Input Name

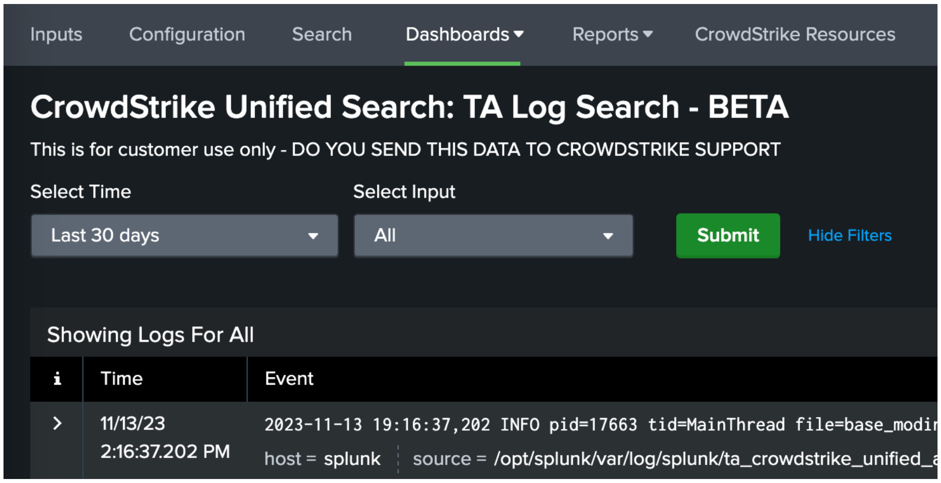
Input ⇕	ID ⇕	Event Time ⇕	Indexed Time ⇕

- **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 Inputs With Events:** Shows a count of inputs that have events within the select timeframe.
- **Number Unique Event IDs Collected:** Shows the number unique Unified Alert event composite_ids collected across all inputs in the given timeframe.
- **TA Logs: Error Level:** Shows a count of error level logs related to the TA in the given timeframe.
- **TA Logs: Queries With No Events:** Shows a count of API queries that did return any events. NOTE: This does not automatically indicate any issue with the TA's functioning.
- **Last Event ID by Input Name:** Shows the latest Unified Alert event composite_id per input, along with the event timestamp and the indexed timestamp.

CrowdStrike Unified Alerts 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.



CrowdStrike Unified Search: TA Log Search - BETA

This is for customer use only - DO YOU SEND THIS DATA TO CROWDSTRIKE SUPPORT

Select Time: Last 30 days

Select Input: All

Showing Logs For All

i	Time	Event
>	11/13/23 2:16:37.202 PM	2023-11-13 19:16:37,202 INFO pid=17663 tid=MainThread file=base_modi host = splunk source = /opt/splunk/var/log/splunk/ta_crowdstrike_unified_a

- **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 if 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:

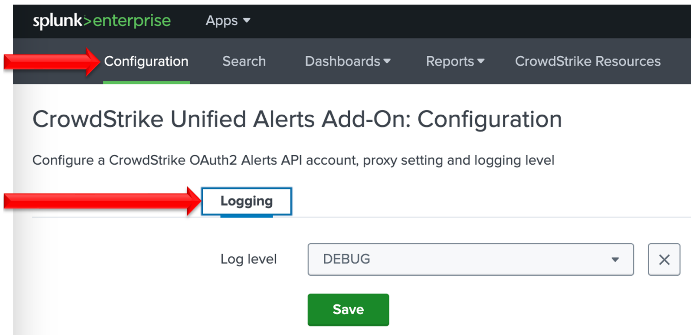
- Proxy based issues
- Firewall based issues
- Network connectivity issues
- Authentication issues (based on misconfigured credentials)
- Splunk CIM field mapping
- Splunk environmental/configuration-based issues

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:

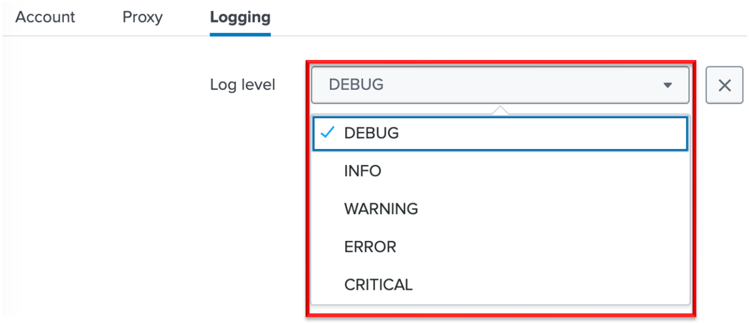


CrowdStrike Unified Alerts Add-On: Configuration

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

Log level: DEBUG

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



Log level: DEBUG

3. Click ‘Save’ to save the logging level.

Review Log Data in Splunk

1. Run and review the **CrowdStrike Unified Alerts 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:**

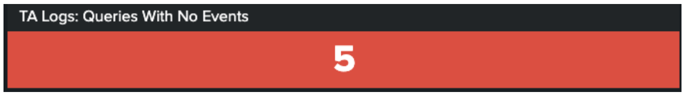
   1.1. Ensure that the credentials have been properly scoped for the API and have been properly entered.

   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.

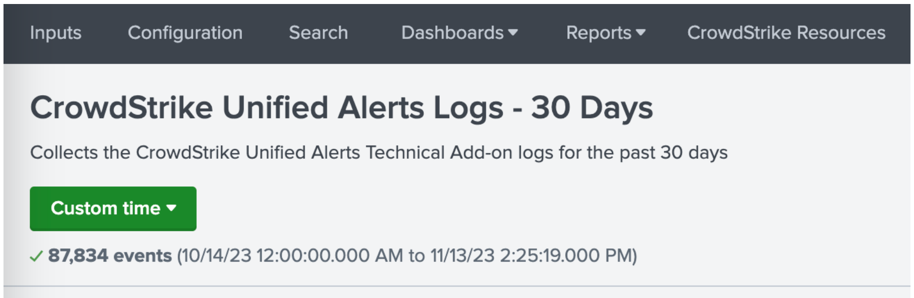
   1.3. Ensure that firewalls, proxies and other network devices are not interfering with the communications between the TA and CrowdStrike API(s) and the TA and Splunk APIs.

   1.4. Ensure that a Unified Alerts input 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.



   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.



CrowdStrike Unified Alerts Logs - 30 Days

Collects the CrowdStrike Unified Alerts Technical Add-on logs for the past 30 days

✓ **87,834 events** (10/14/23 12:00:00.000 AM to 11/13/23 2:25:19.000 PM)

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. If using the action timestamp, keep in mind that actions that happen while the sensor is not communicating with CrowdStrike may be delayed in being reported.

Support

This TA Is designed to help facilitate the collection of Unified Alerts 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:

- 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 Unified Alerts 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_unified_alerts' 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.