CROWDSTRIKE

CrowdStrike
Falcon Spotlight Vulnerability Data Add-on for Splunk

Installation and Configuration Guide v2.0+

Introduction

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

The CrowdStrike Falcon Spotlight Vulnerability Data Technical Add-on for Splunk allows CrowdStrike customers to retrieve CrowdStrike Spotlight Vulnerability data from CrowdStrike Falcon instance that have the Spotlight module enabled via API.

To get more information about this CrowdStrike Falcon Spotlight please refer to the documentation for the Spotlight module located in the CrowdStrike Falcon UI:
https://falcon.crowdstrike.com/documentation/43/falcon-spotlight

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.

This Technical Add-On does not currently support Falcon Flight Control Architectures. API access is direct to the Falcon Instance.

Requirements

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

1. An active subscription to the CrowdStrike Falcon Spotlight Vulnerability module
2. A Splunk Heavy forwarder or Input Data Manager (IDM)
3. A Splunk account with proper access to deploy and configure technical add-ons
4. An active API credential with the proper API scope or access to the CrowdStrike Falcon instance to create one
5. The CrowdStrike Cloud environment that the Falcon instance resides in

If you do not have a current CrowdStrike Spotlight subscription:

1. Contact your CrowdStrike sales team to acquire one
2. Navigate to the CrowdStrike store in your falcon instance and request a trial: Click Here to See the CrowdStrike Spotlight App in the CrowdStrike Store

This Technical Add-On does not currently support Falcon Flight Control Architectures. API access needs to be direct to the Falcon Instance.

Getting Started

Spotlight Data Communication Flow

The CrowdStrike Falcon Spotlight Vulnerability Technical Add-on for Splunk leverages the ‘combined’ Spotlight API endpoint to collect vulnerability data. The TA communication process is as follows:

1. The TA will authenticate to the CrowdStrike API gateway for the configured CrowdStrike Cloud environment to collect an OAuth2 token
2. The OAuth2 token will then be used by the TA to connect and collect Spotlight vulnerability data from the CrowdStrike Spotlight API combined endpoint: /spotlight/combined/vulnerabilities/v1 *
3. Up to 4000 vulnerabilities will be called per API call **
4. Once all relevant data has been retrieved the TA will process the data
5. The TA will post each event to Splunk to be indexed

* The credential used to create the OAuth2 token must be scoped correctly to be able to connect to the Spotlight API
** multiple API calls maybe required to collect all available data

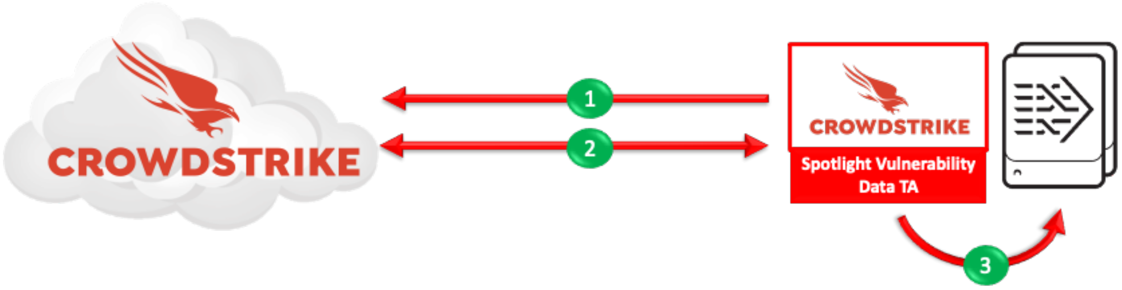
Data Volume Considerations

Spotlight Vulnerability data can be a large amount of data depending on the size of the environment and the time range of the data being collected. Some key considerations to take into account when collecting this data:

1. The amount of data that will be ingested
2. The available resources to collect and process the data
3. The time range or frequency of the data collection

High Level Data Flow

The CrowdStrike Falcon Spotlight Vulnerability Data TA leverages CrowdStrike API calls to collect data:

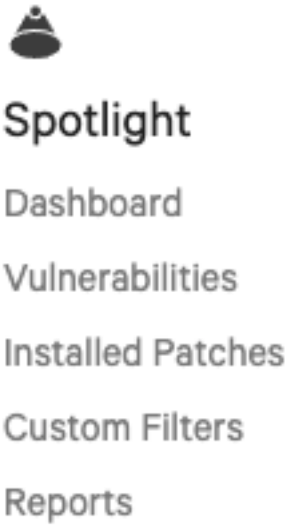


1. The TA acquires an OAuth2 token from the CrowdStrike API gateway
2. The TA uses the OAuth2 token to query and collect CrowdStrike Falcon Spotlight Vulnerability data
3. The TA posts the data to the internal Splunk API

***Note – The API Client must be scoped for access to the Spotlight API to be granted access**

Validating that Spotlight is Enabled

The CrowdStrike Falcon Spotlight Vulnerability Data TA requires a valid Spotlight subscription and that Spotlight has been enabled on the CrowdStrike instance.

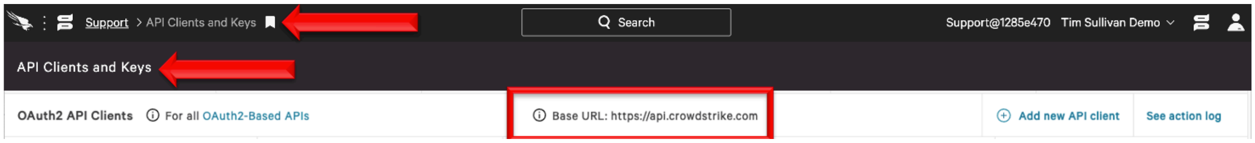


1. Access the CrowdStrike Falcon user interface (UI)
2. Ensure that ‘Spotlight’ is listed in the dropdown menu

If you have a Spotlight subscription but are not able to access it or create an API credential, please submit a support ticket though the support portal: https://supportportal.crowdstrike.com/

Identifying the CrowdStrike Cloud:

The Spotlight Vulnerability Data TA requires the CrowdStrike Cloud environment be identified when being configured. The cloud environment can be located in the CrowdStrike Falcon UI under the ‘Support’ > ‘API Clients and Keys’


Support > API Clients and Keys
Search
Support@1285e470 Tim Sullivan Demo
API Clients and Keys
OAuth2 API Clients
For all OAuth2-Based APIs
Add new API client
See action log

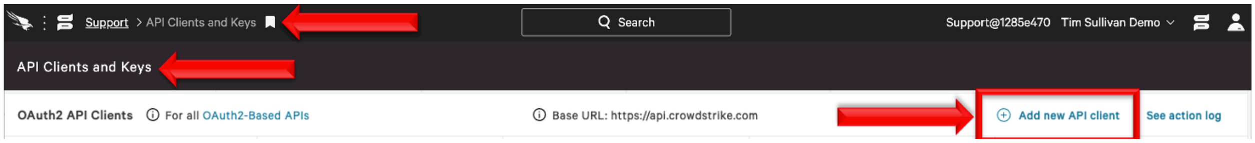
Base URL: https://api.crowdstrike.com

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

Generating and Scoping Credentials

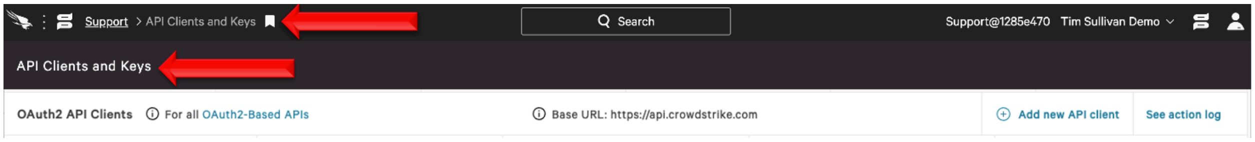
The Spotlight Vulnerability Data TA requires API credentials that are located in the CrowdStrike Falcon UI in order to access the APIs. These can be existing API credentials with the Spotlight scope or can be newly generated credentials.

Generating New API Credentials

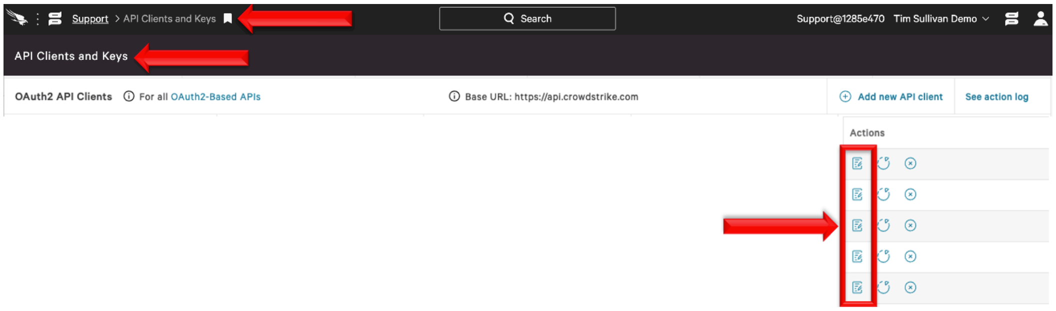

Support > API Clients and Keys
Search
Support@1285e470 Tim Sullivan Demo
API Clients and Keys
OAuth2 API Clients
For all OAuth2-Based APIs
Base URL: https://api.crowdstrike.com
Add new API client
See action log

1. Access the CrowdStrike Falcon user interface (UI) with an account that is able to view/create the API clients and keys page
2. Navigate to ‘Support’>’API Client and Keys’ page
3. On the same line as ‘OAuth2 API Clients’ select ‘Add new API client’
4. Give the client a name and assign the appropriate scope(s)
5. Select Add and save the credentials *NOTE: This is the only time the Secret appears, failure to capture it at this time will require that it be regenerated

Modifying Existing Credentials

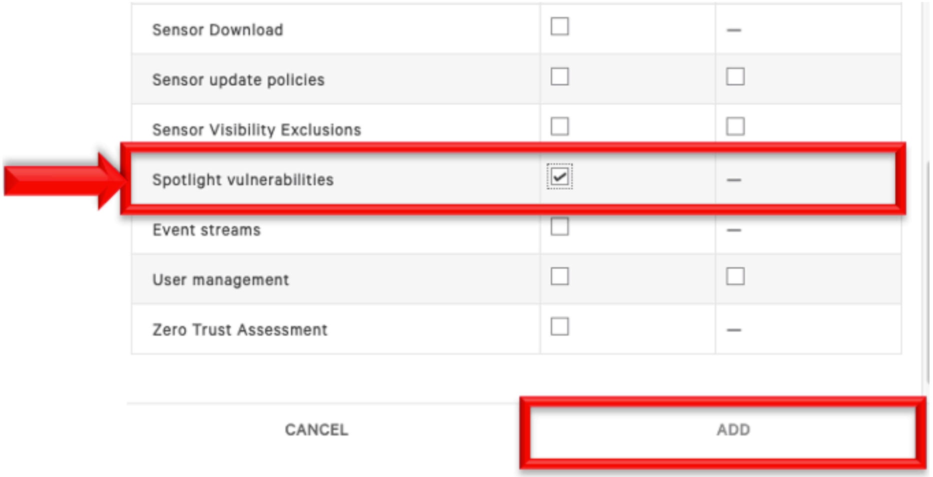

Support > API Clients and Keys
Search
Support@1285e470 Tim Sullivan Demo
API Clients and Keys
OAuth2 API Clients
For all OAuth2-Based APIs
Base URL: https://api.crowdstrike.com
Add new API client
See action log

1. Access the CrowdStrike Falcon user interface (UI) with an account that is able to view/create the API clients and keys page
2. Navigate to ‘Support’>’API Client and Keys’ page
3. Select the ‘edit’ icon for the API credential that will be modified


Support > API Clients and Keys
Search
Support@1285e470 Tim Sullivan Demo
API Clients and Keys
OAuth2 API Clients
For all OAuth2-Based APIs
Base URL: https://api.crowdstrike.com
Add new API client
See action log
Actions

Scoping the Credentials

The API credential, either new or existing, must be assigned the correct scope to be able to access the data.



Sensor Download	□	–
Sensor update policies	□	□
Sensor Visibility Exclusions	□	□
Spotlight vulnerabilities	☑	–
Event streams	□	–
User management	□	□
Zero Trust Assessment	□	–

1. Under the ‘API SCOPES’ selection located ‘Spotlight vulnerabilities’
2. Check the ‘READ’ scope for Spotlight vulnerabilities (Note: there is no ‘WRITE’ scope for this API.
3. Select ‘ADD’ to save this assignment

Proxy Considerations

The CrowdStrike Falcon Spotlight Vulnerability Data Add-On communicates with the CrowdStrike's APIs and any proxy systems in the environment should be configured to allow this communication.

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.

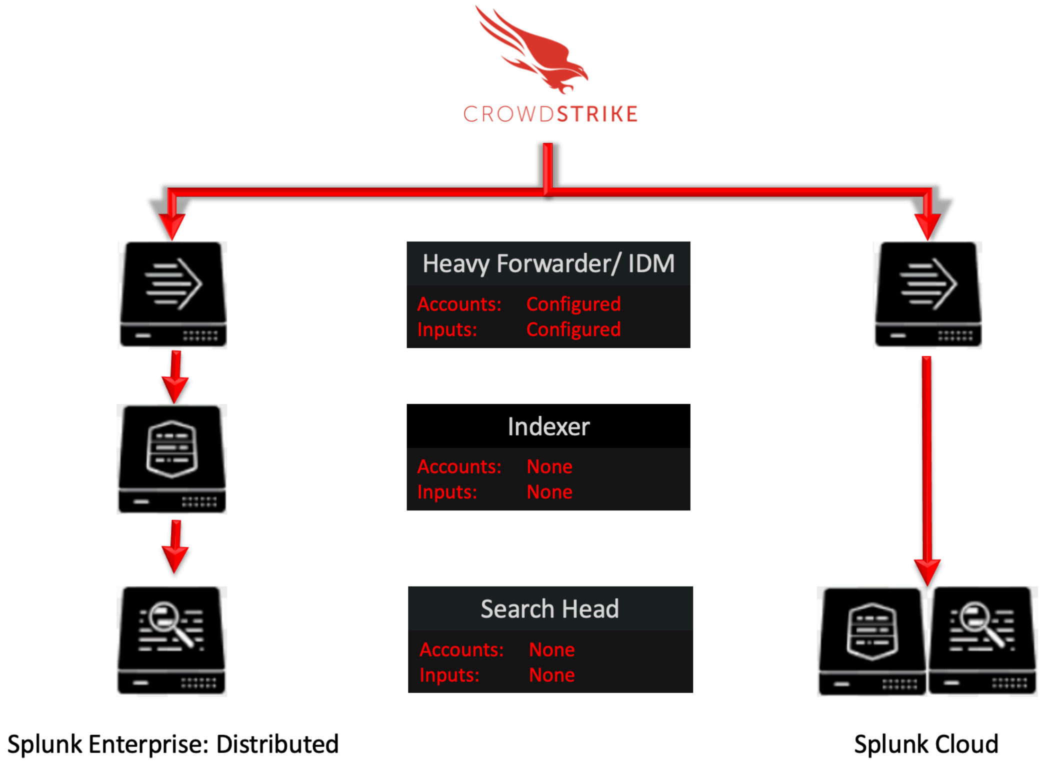
Splunk Indexer(s): The TA can be installed to provide field mapping and search macro support. The TA should be deployed without any accounts or inputs configured and any search macros should be properly configured for use. If a custom index is going to be used, then it should be created here.

Splunk Heavy Forwarder(s) & Information Data Managers (IDMs): The TA is required to be installed here as this is where the data will be collected. The appropriate accounts and inputs should be properly configured for data collection. Ensure that if a custom 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.

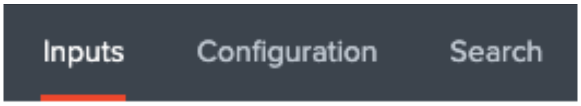
The following diagram shows the flow of data from CrowdStrike and CrowdStrike Falcon Spotlight Vulnerability TA configuration within a distributed Splunk Enterprise and Splunk Cloud environment:



Configuring the TA

TA Layout

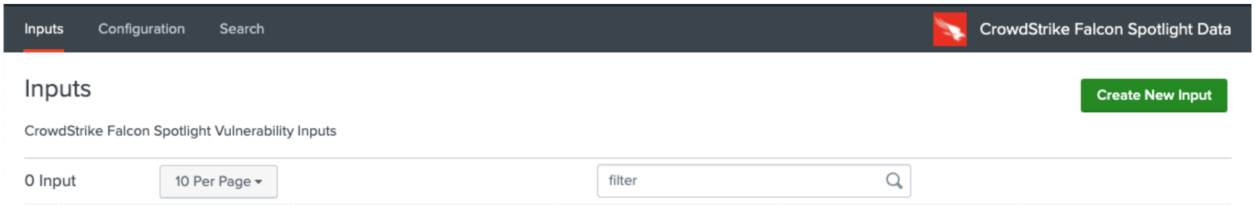
The TA contains 3 sections.



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

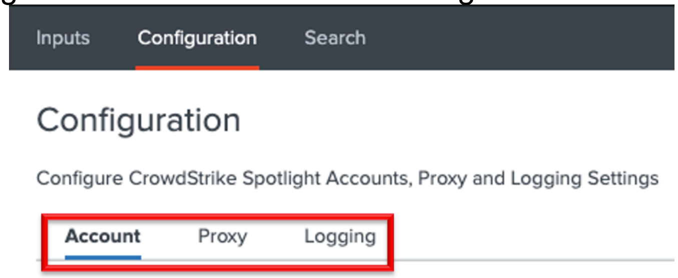
Inputs Section

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). In the far-right corner of the Inputs section contains select to create a new input configuration.


Inputs
Configuration
Search
CrowdStrike Falcon Spotlight Data
Inputs
CrowdStrike Falcon Spotlight Vulnerability Inputs
Create New Input
0 Input
10 Per Page ▾
filter

Configuration Section

The Configuration section contains 3 configuration tabs:



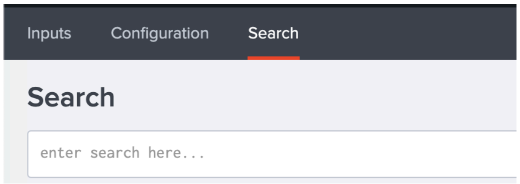
Configuration

Configure CrowdStrike Spotlight Accounts, Proxy and Logging Settings

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

Search Section

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



Search

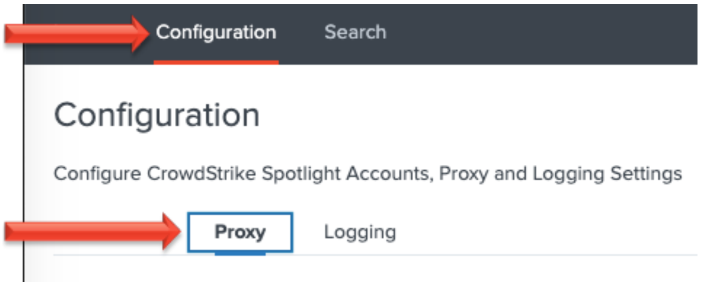
enter search here...

Configuring the TA to collect data

NOTE This action should only be performed on:
Splunk Heavy Forwarders and Splunk IDMs

Configure Proxy Settings (optional)

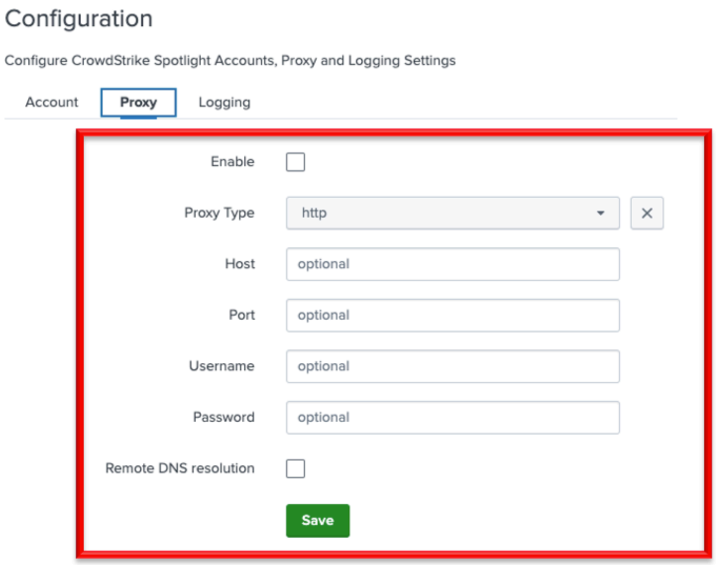
1. Proxy settings are configured under the Configuration section, Proxy tab. Proxies can cause authentication issue if not configured correctly, ensure that the proxy does not interfere with communication between the TA and the CrowdStrike APIs



Configuration

Configure CrowdStrike Spotlight Accounts, Proxy and Logging Settings

2. Configure the following fields as appropriate:



Configuration

Configure CrowdStrike Spotlight Accounts, Proxy and Logging Settings

Enable □

Proxy Type http

Host optional

Port optional

Username optional

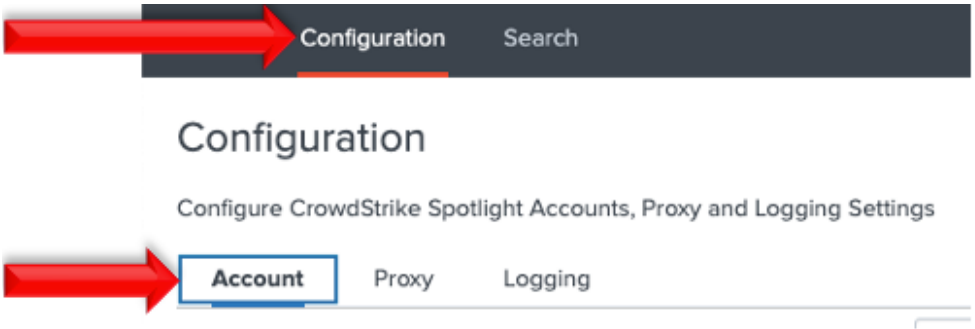
Password optional

Remote DNS resolution □

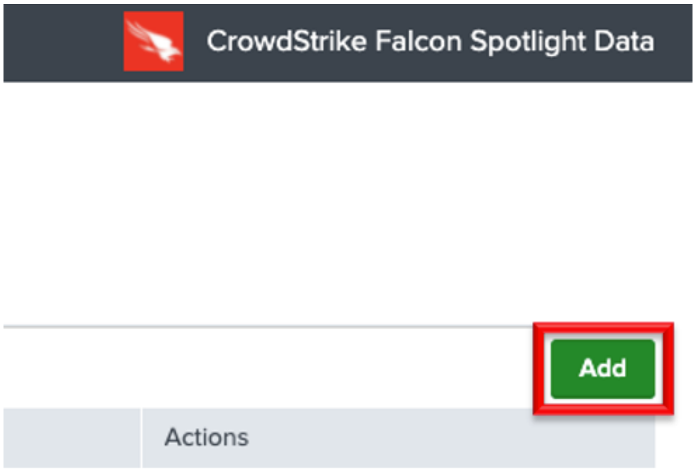
- **Enable**: This checkbox is used to enable/disable the proxy settings
- **Proxy Type**: This dropdown is used to select the proxy type
- **Host**: The hostname/IP address for the proxy server
- **Port**: The communication port for the proxy server
- **Username**: The authentication username for the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

Configure an Account

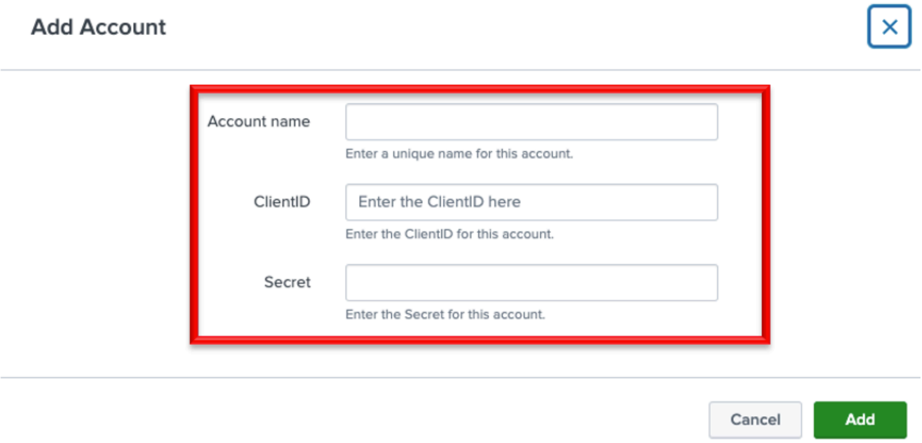
1. An account is configured using an API client credential from the CrowdStrike Falcon UI.
2. An account is created under the Configuration section, Account tab:


Configuration
Search
Configuration
Configure CrowdStrike Spotlight Accounts, Proxy and Logging Settings
Account
Proxy
Logging

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



4. Configure the following fields:


Add Account

Account name

Enter a unique name for this account.

ClientID: Enter the ClientID here

Enter the ClientID for this account.

Secret

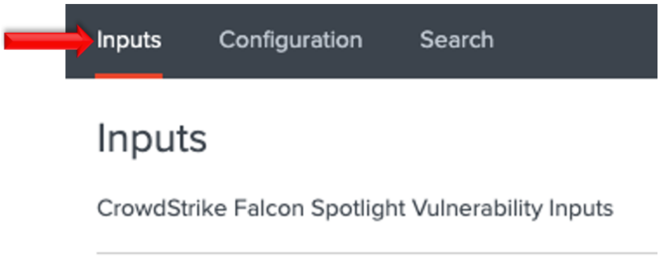
Enter the Secret for this account.

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

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

Creating an Input

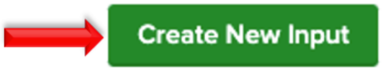
1. An input will require a valid Spotlight account be created already.
2. An input is created under the Inputs section:



Inputs

CrowdStrike Falcon Spotlight Vulnerability Inputs

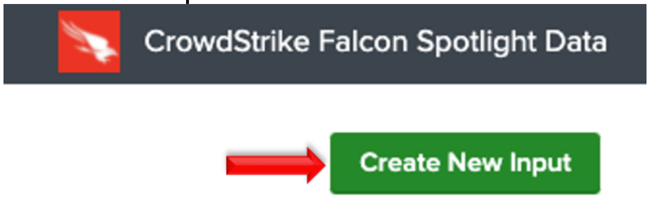
3. In the top right corner select the ‘Create New Input’ dropdown to display the available input types.



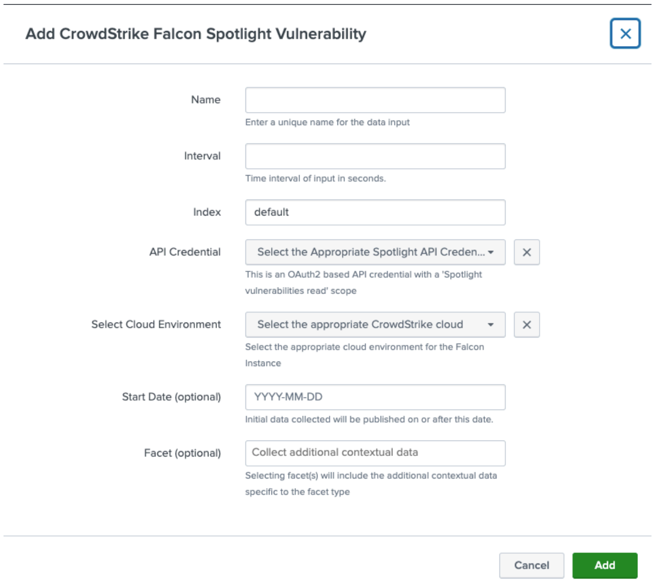
Configure an Input

The Spotlight Vulnerability Data TA can be configured with multiple inputs. These can be for the same of different CrowdStrike Falcon environments.

1. Select the 'Create New Input'



2. Configure the appropriate fields:



Add CrowdStrike Falcon Spotlight Vulnerability

Name
Enter a unique name for the data input

Interval
Time interval of input in seconds.

Index: default

API Credential: Select the Appropriate Spotlight API Creden...
This is an OAuth2 based API credential with a 'Spotlight vulnerabilities read' scope

Select Cloud Environment: Select the appropriate CrowdStrike cloud
Select the appropriate cloud environment for the Falcon Instance

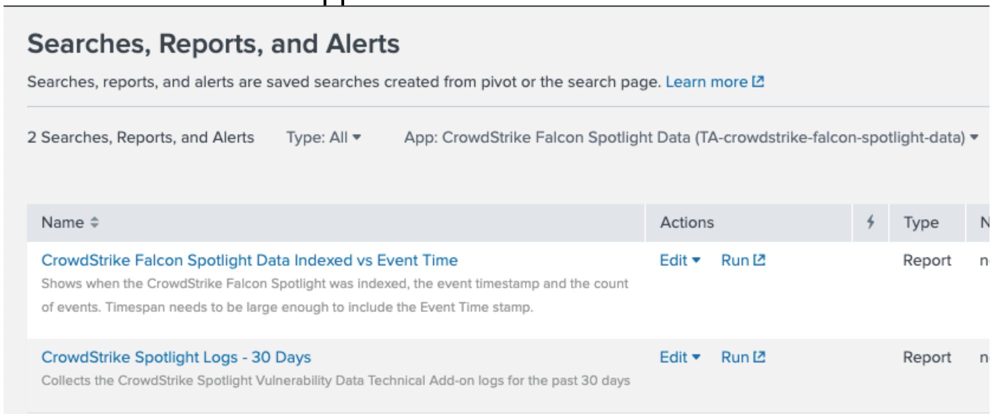
Start Date (optional): YYYY-MM-DD
Initial data collected will be published on or after this date.

Facet (optional): Collect additional contextual data
Selecting facet(s) will include the additional contextual data specific to the facet type

- **Name**: (required) A name unique to the Splunk Environment
- **Interval**: (required) How often the specific input will run, expressed in seconds
- **Index**: (required) The Splunk Index that the data will be stored in
- **API Credential**: (required) The appropriate account from the configuration tab
- **Select Cloud Environment**: (required) The CrowdStrike Cloud the instance resides in
- **Start Date**: (optional) The initial date to start data collection on
- **Facet**: (optional) Provides the option to include host, CVE, remediation data

Searches, Reports, and Alerts

The Spotlight Vulnerability Data TA contains saved reports that can be found under the ‘Searches, Reports, and Alerts’ section. Ensure that ‘CrowdStrike Falcons Spotlight Data’ is the selected app:



Searches, Reports, and Alerts

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

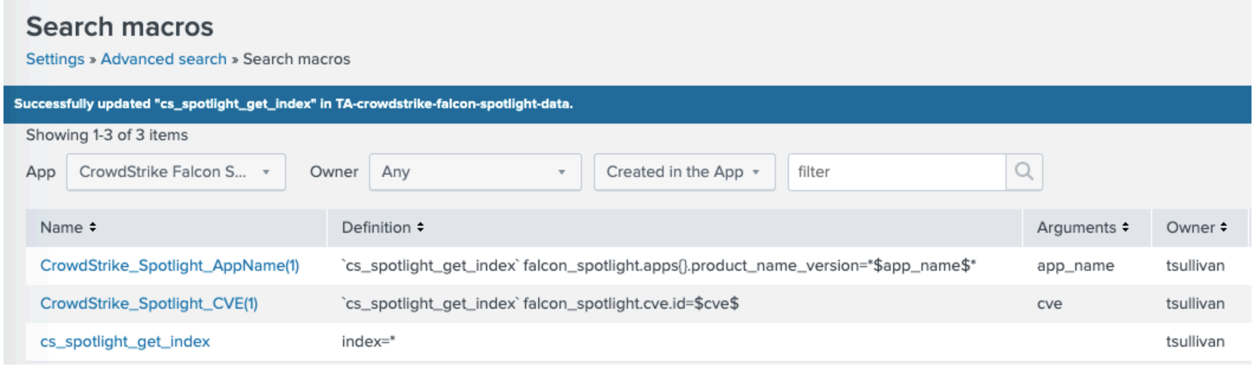
2 Searches, Reports, and Alerts   Type: All ▾   App: CrowdStrike Falcon Spotlight Data (TA-crowdstrike-falcon-spotlight-data) ▾

Name ⇕	Actions		⚡	Type	N
CrowdStrike Falcon Spotlight Data Indexed vs Event Time Shows when the CrowdStrike Falcon Spotlight 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	n
CrowdStrike Spotlight Logs - 30 Days Collects the CrowdStrike Spotlight Vulnerability Data Technical Add-on logs for the past 30 days	Edit ▾	Run ↗		Report	n

- **CrowdStrike Falcon Spotlight Data Indexed vs Event Time**: This report will show when the CrowdStrike Falcon Spotlight data was indexed by Splunk, the event timestamp and the number of events for that index time. This report helps show when the Spotlight data was actually indexed into Splunk
- **CrowdStrike Spotlight Logs – 30 days**: This report shows the TA’s logs for the past 30 days. This information show be provided, at a minimum, when requesting support from CrowdStrike.

Search Macros

The Spotlight Vulnerability Data TA contains configurable search macros:



Search macros

Settings » Advanced search » Search macros

Successfully updated "cs_spotlight_get_index" in TA-crowdstrike-falcon-spotlight-data.

Showing 1-3 of 3 items

App: CrowdStrike Falcon S... ▾ Owner: Any ▾ Created in the App ▾ filter

Name	Definition	Arguments	Owner
CrowdStrike_Spotlight_AppName(1)	`cs_spotlight_get_index` falcon_spotlight.apps{}.product_name_version=*app_name*	app_name	tsullivan
CrowdStrike_Spotlight_CVE(1)	`cs_spotlight_get_index` falcon_spotlight.cve.id=cve	cve	tsullivan
cs_spotlight_get_index	index=*		tsullivan

- **CS_spotlight_get_index**: This is configured to point to the index that is storing the CrowdStrike Spotlight Vulnerability data. The default configuration is to '*'. This search macro must be configured for the other search macros and reports to work
- **CrowdStrike_Spotlight_AppName(1):** This search macro allows for an app name to be entered in the variable position (replacing the '1') and will search the 'product_name_version' for that name
- **CrowdStrike_Spotlight_CVE(1):** This search macro allows for a CVE number to be entered in the variable position (replacing the '1') and will search the 'cve.id' field for that CVE number

Ensure the following:

1. Search Macros must be enclosed by 'back ticks', not single quotes. This key is located above the 'Tab' key, to the left of the number 1 on most US style keyboards.
2. Ensure that the account leveraging the macro has the correct permissions to use the macro or adjust the permission of the macro accordingly.
3. Ensure that the account leveraging the macro has the correct permissions to access the Spotlight Vulnerability data.
4. Ensure that the index(es) have been designated correctly.

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 Falcon Spotlight Vulnerability data.

Some examples of benefits that leveraging custom indexes can provides:

- Allows multiple teams to reference the data without exposing other data sets that may be more sensitive.
- Allows data collection types to be assigned to different Heavy Forwarders/IDM for access and resource allocation considerations.
- Improves searching response times and reduces resources needed.

Troubleshooting

CrowdStrike only provides support for:

- TA code-based functionality errors
- CrowdStrike API based access errors

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

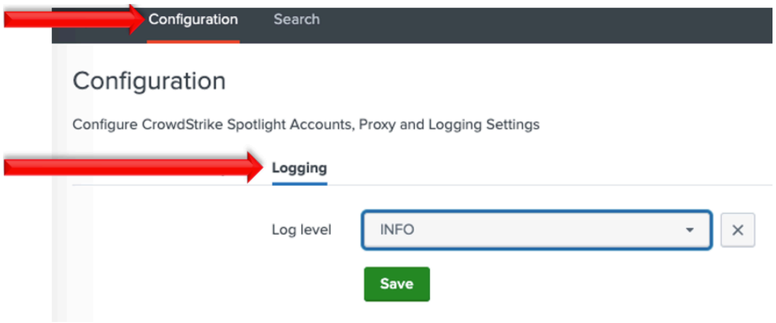
- Proxy based issues
- Firewall based issues
- Network connectivity issues
- Authentication issues (based on misconfigured credentials)
- Splunk CIM field mapping

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:

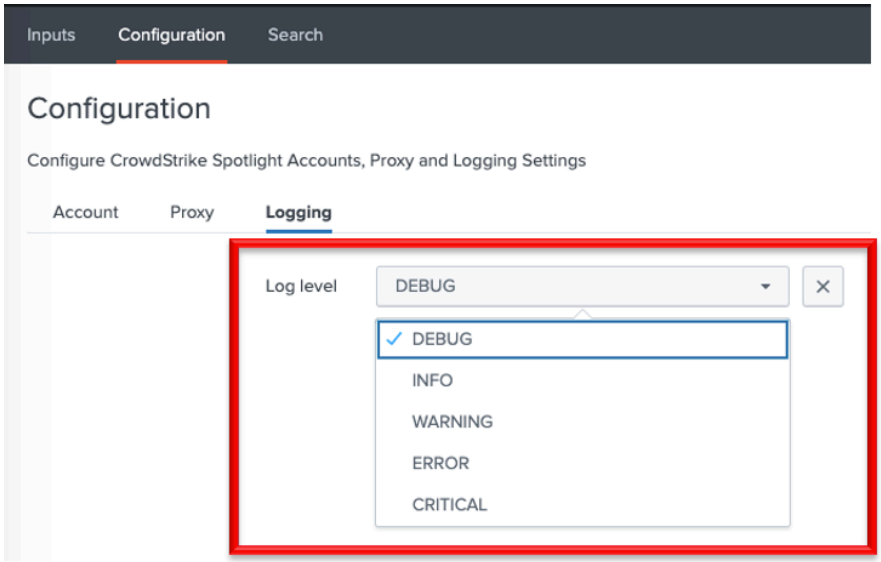


Configuration

Configure CrowdStrike Spotlight Accounts, Proxy and Logging Settings

Log level: INFO

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



Configuration

Configure CrowdStrike Spotlight Accounts, Proxy and Logging Settings

Log level: DEBUG

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

Obtaining and Contacting Support

1. Ensure that the OAuth2 credential has been scoped correctly
2. Set the TA log level to ‘DEBUG’
3. Repeat and record the action(s) that are associated with the issue you are reporting
4. Download the all log files containing ‘crowdstrike_falcon_spotlight_vulnerability’ under the $Splunk/var/log/splunk/ directory
   - The “**CrowdStrike Spotlight Logs – 30 days**” report can also be used to collect logs. Ensure that the timeframe in long enough to encompass all relevant information
5. Record the following information about the Splunk system:
   - Splunk environment type
   - Splunk version
   - TA version
6. Identify the types of networks devices that the connection will traverse and ensure that they have been properly configured
7. Collect API audit logs from the Falcon instance for the time frame when the issue is occurring
8. Navigate to https://supportportal.crowdstrike.com/
9. Provide (at a minimum) the information from steps 4-7

Additional Resources

(Access to the CrowdStrike Falcon UI Required)
CrowdStrike Spotlight Guide
Spotlight API Guide