SIEM Connector Feature Guide

Version 5.2 - Last updated: 09/18/2017

Contents:

Introduction

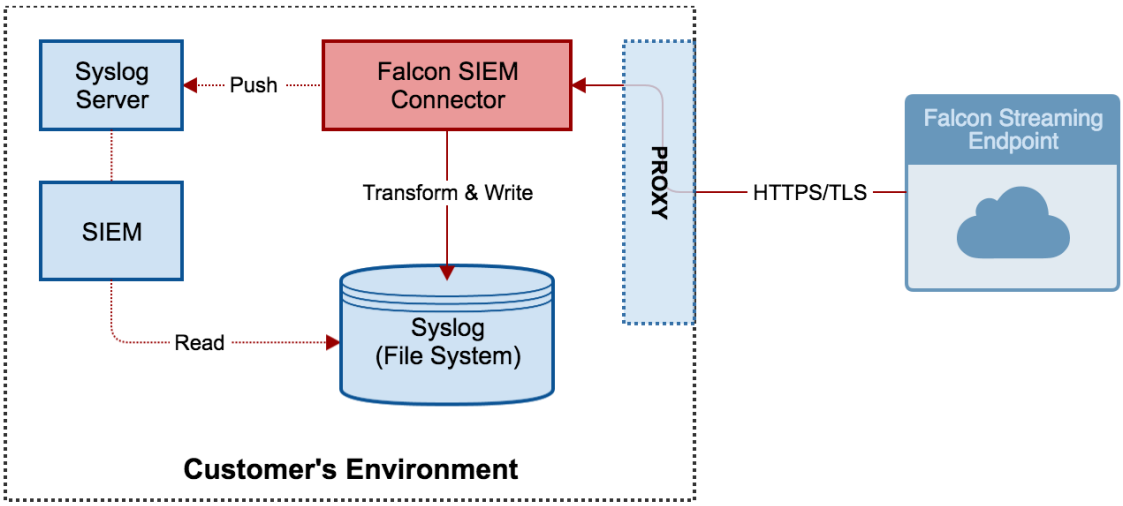
The Falcon SIEM Connector Feature Guide explains how to install and configure the Falcon SIEM Connector, which is available for download on the Downloads page. If you have any questions or experience issues during installation, contact support@crowdstrike.com.

Before You Begin

What is the Falcon SIEM Connector?

The Falcon SIEM Connector provides users a turnkey, SIEM-consumable data stream. The Falcon SIEM Connector:

- Transforms Falcon Streaming API data into a format that a SIEM can consume (for more information on the events that the Streaming API provides, see the Streaming API Reference)
- Maintains the connection to the Falcon Streaming API and your SIEM, in case either drops
- Manages the data-stream pointer to prevent data loss



The Falcon SIEM Connector can be placed behind a proxy within your environment and will connect to the Falcon Streaming endpoint to authorize and discover available feeds. This information will then be used to stream the data (event feed) into your environment through a syslog transport protocol (UDP/TCP). The Connector will then:

- Transform and spool events into syslog. The syslog will be consumed by SIEM.
- Transform and write events to syslog listener with a SIEM-agnostic payload.

> **Important:** While the SIEM Connector does support proxies, it is not designed to authenticate to a proxy service. In other words, the SIEM Connector can authenticate the the Streaming API through a proxy, but cannot authenticate to a proxy first and then authenticate with the Streaming API endpoint.

What are the features of the Falcon SIEM Connector?

- Handles the mechanics to auto connect and reconnect to the Falcon Streaming API
  - Open long-lived connection to the Falcon Streaming API to receive streamed `DetectionSummaryEvent`, `UserActivityAuditEvent`, and `LoginAuditEvent`
  - Save offset value of latest event received
  - When disconnected, automatically reconnect to the Falcon Streaming API and pass last offset value to continue receive events from that point
- Supports new Falcon authentication/authorization system
  - Uses an API key instead of previous API username/password
  - Processing of new user authentication events
- Built-in data transformation
  - By default, events are in nested JSON format
  - Options to transform data into Syslog, CEF, or LEEF format

- Flexible data integration options
  - Save nested JSON file to disk
  - Save Syslog/CEF/LEEF file to disk
  - Send Syslog/CEF/LEEF to Syslog listener

System Dependencies

- **OS**: CentOS/RHEL 6.x-7.x (64-bit) or or Ubuntu 14.x (64-bit)
- **Connectivity**: Internet connectivity and ability to connect the CrowdStrike Cloud
- **Time**: The date and time on the host running the Falcon SIEM Connector must be current
- **Communication**: Ability to communicate with Syslog Listener

There are no specific RAM or processor requirements for running the Falcon SIEM Connector. The required disk space will vary depending on how long you wish to store output logs.

Getting Started

Enable Access to the Falcon Streaming API

Before using the Falcon SIEM Connector, you must contact support@crowdstrike.com to enable access to the Falcon Streaming API (upon which the SIEM Connector is based). This is required to ensure that you can authenticate.

Obtaining Credentials

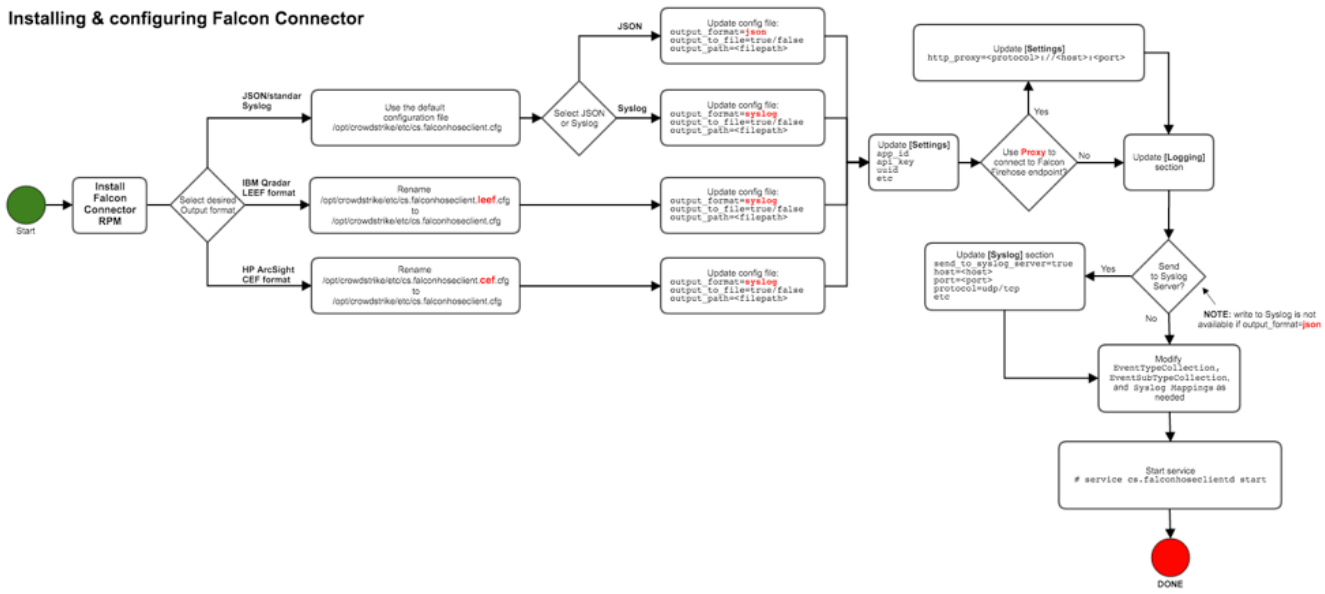
The Falcon SIEM Connector is built on top of the the Streaming API. You therefore need to obtain a Streaming API key to use it. Your API key and UUID are in the **Support App > API Key** page. There is one API key and UUID per customer ID:

1. Go to the Support App > API Key page.
2. Click **Reset API**. Copy the API key and UUID for safe keeping. Note that your API key and UUID are assigned one pair per customer account, not one pair per user. Thus, if you generate a new API key, you may be affecting existing applications in your environment. Note also that the API key will only appear in the UI the first time the key is generated.

RESETTING AN API KEY

To revoke an existing API key, follow the same process as described above to generate a new key, which invalidates the existing key.

Installation and Configuration



Using CentOS

STEP 1

Install the Falcon SIEM Connector using the provided RPM file which is available for download on the Downloads page. Administrative (root) permissions are required to install and configure the client.

```
# sudo rpm -Uvh /path/to/file/cs.falconhoseclient-1.0.70-1.el7.centos.x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:cs.falconhoseclient-1.0.70-1.el7.c################################# [ 50%]
Cleaning up / removing...
   2:cs.falconhoseclient-1.0.69-1.el7.c################################# [100%]
```

By default, the Falcon SIEM Connector will install in the `opt/crowdstrike` directory. The installer will also create a service script at `/etc/init.d/cs.falconhoseclientd`, and logs will be written to `/var/log/crowdstrike/falconhoseclient/` by default. If you have previous versions of the application installed, the existing Falcon SIEM Connector will upgrade automatically. However, upgrading will not replace your existing configuration file or your offset file.

To uninstall the SIEM Connector on CentOS, run:

```
# sudo rpm -e cs.falconhoseclient
```

STEP 2

After installing, choose which config file you want to use. The RPM file comes with three configurations that you can customize as you see fit. The client application will always use the `/opt/crowdstrike/etc/cs.falconhoseclient.cfg` as the default configuration. For this reason, you will need to rename any configuration file you want to use to `/opt/crowdstrike/etc/cs.falconhoseclient.cfg`.

Configuration Filename	Descriptions

`/opt/crowdstrike/etc/cs.falconhoseclient.cfg`	This is the default configuration that will be used out-of-the-box. By default, the client will output JSON to a file at `/var/log/crowdstrike/falconhoseclient/cs.falconhoseclient.log`, as specified under output_path configuration in [Settings]. **Note**: Currently when JSON output is specified, we will not be able to send to syslog/SIEM directly, so the send_to_syslog_server flag is not supported.
`/opt/crowdstrike/etc/cs.falconhoseclient.cef.cfg`	This is a configuration file to use Common Event Format (CEF). To enable syslog push to your syslog server, you will need to change the `send_to_syslog_server` flag to `true`. You will need to change the [Syslog] section of the configuration file to match your SIEM/syslog relay server's details. This configuration will also output events to the location specified in `output_path`. For more information, see the Additional Configuration section of this document.
`/opt/crowdstrike/etc/cs.falconhoseclient.leef.cfg`	This is a configuration file to use Log Event Extended Format (LEEF). To enable syslog push to syslog server, you will need to change the `send_to_syslog_server` flag to true. You will need to change the [Syslog] section of the configuration file to match your SIEM/syslog relay server's details. This configuration will also output message to location specified in `output_path`. For more information, see the Additional Configuration section of this document.

STEP 3

Provide the appropriate credentials by editing the [Settings] section of the configuration file at `/opt/crowdstrike/etc/cs.falconhoseclient.cfg`. The version must be set to `2` and you must also replace `your_unique_app_id`, `your_uuid` and `your_api_key` with the appropriate entries, as shown below:

```
[Settings]
version = 2
api_url = https://firehose.crowdstrike.com/sensors/entities/datafeed/v1
app_id = your_unique_app_id #max 18 char, must be unique for each instance of Connector
api_key = your_api_key
api_uuid = your_uuid
```

Using Ubuntu

STEP 1

As of version 1.0.70 of the SIEM Connector, we now support Debian/Ubuntu. Install the Falcon SIEM Connector using the provided DEB file which is available for download on the Downloads page. Administrative (root) permissions are required to install and configure the client.

```
# sudo dpkg -i crowdstrike-cs-falconhoseclient_70-siem-release-1.0_amd64.deb
(Reading database ... 63084 files and directories currently installed.)
Preparing to unpack crowdstrike-cs-falconhoseclient_70-siem-release-1.0_amd64.deb ...
Unpacking crowdstrike-cs-falconhoseclient (70-siem-release-1.0) over (69-siem-release-1.0) ...
Setting up crowdstrike-cs-falconhoseclient (70-siem-release-1.0) ...

Configuration file '/opt/crowdstrike/etc/cs.falconhoseclient.cfg'
 ==> Modified (by you or by a script) since installation.
 ==> Package distributor has shipped an updated version.
   What would you like to do about it ?  Your options are:
    Y or I  : install the package maintainer's version
    N or O  : keep your currently-installed version
      D     : show the differences between the versions
```

```
     Z     : start a shell to examine the situation
 The default action is to keep your current version.
*** cs.falconhoseclient.cfg (Y/I/N/O/D/Z) [default=N] ?
```

By default, all of the Falcon SIEM Connector's assets will be installed under `/opt/crowdstrike/`. The installer will also create a service script `/etc/init/cs.falconhoseclientd` and log directory `/var/log/crowdstrike/falconhoseclient/`.

To uninstall the SIEM Connector on Ubuntu, run:

```
# sudo dpkg --remove crowdstrike-cs-falconhoseclient
```

STEP 2

After installing, choose which config file you want to use. The DEB file comes with three configurations that you can customize as you see fit. The client application will always use the `/opt/crowdstrike/etc/cs.falconhoseclient.cfg` as the default configuration. For this reason, you will need to rename any configuration file you want to use to `/opt/crowdstrike/etc/cs.falconhoseclient.cfg`.

Configuration Filename	Descriptions
`/opt/crowdstrike/etc/cs.falconhoseclient.cfg`	This is the default configuration that will be used out-of-the-box. By default, amongst other things, the client will output JSON to a file at `/var/log/crowdstrike/falconhoseclient/cs.falconhoseclient.log`, as specified under output_path configuration in [Settings]. **Note**: Currently when JSON output is specified, we will not be able to send to syslog/SIEM directly, so the send_to_syslog_server flag is not supported.
`/opt/crowdstrike/etc/cs.falconhoseclient.cef.cfg`	This is a configuration file to use Common Event Format (CEF). To enable syslog push to your syslog server, you will need to change the `send_to_syslog_server` flag to `true`. You will need to change the [Syslog] section of the configuration file to match your SIEM/syslog relay server's details. This configuration will also output events to the location specified in `output_path`. For more information, see the Additional Configuration section of this document.
`/opt/crowdstrike/etc/cs.falconhoseclient.leef.cfg`	This is a configuration file to use Log Event Extended Format (LEEF). To enable syslog push to syslog server, you will need to change the `send_to_syslog_server` flag to true. You will need to change the [Syslog] section of the configuration file to match your SIEM/syslog relay server's details. This configuration will also output message to location specified in `output_path`. For more information, see the Additional Configuration section of this document.

STEP 3

Provide the appropriate credentials by editing the [Settings] section of the configuration file at `/opt/crowdstrike/etc/cs.falconhoseclient.cfg`. The version must be set to 2 and you must also replace `your_unique_app_id`, `your_uuid` and `your_api_key` with the appropriate entries, as shown below:

```
[Settings]
version = 2
api_url = https://firehose.crowdstrike.com/sensors/entities/datafeed/v1
app_id = your_unique_app_id #max 18 char, must be unique for each instance of Connector
api_uuid = your_uuid
api_key = your_api_key
```

Operation

By default, starting, stopping, and restarting the service all require root permission. Note that the event output file will be cleared out every time the Falcon SIEM Connector is stopped and started or restarted.

Starting the Service

CENTOS

Out of the box, the Falcon SIEM Connector comes with a service script pre-installed. The script will automatically start and restart to ensure client resiliency. However, the client service/daemon will not be started out of the box because it needs to be configured with appropriate credentials beforehand. Once the initial configuration is complete, you can start the service with the following command:

```
# sudo service cs.falconhoseclientd start
```

UBUNTU

You can use the following command to start the service:

```
# sudo start cs.falconhoseclientd
```

Stopping the Service

CENTOS

In some cases, you may want to stop the service which will stop the consumption of the Falcon Streaming API events. Note that the event output file will be cleared out every time the connector is restarted. To stop the service:

```
# sudo service cs.falconhoseclientd stop
```

UBUNTU

You can use the following command to stop the service:

```
# sudo stop cs.falconhoseclientd
```

Restarting the Service

CENTOS

When you change the configuration of the client, you will need to restart the client. Note that the event output file will be cleared out every time the connector is restarted. To restart the service, use the following command:

```
# sudo service cs.falconhoseclientd restart
```

UBUNTU

When you change the configuration of the client, you will need to restart the client. Note that the event output file will be cleared out every time the connector is restarted. To restart the service, use the following command:

```
# sudo restart cs.falconhoseclientd
```

Additional Configuration

Note: 'Section' refers to anything that is enclosed with square brackets [SectionName]. The order (where you put the section) does not matter

[Settings] Section

This section contains all the client runtime specific configurations.

Key	Value	Description	Required?	De
`version`	`1` or `2`	The version of authentication to be used. 1 = Basic Authentication (may be deprecated in the future). 2 = API Key Authentication. In order for the version 2 authentication to work, the system time will have to be in sync with actual time (i.e. through time server)	Y	
`api_url`	`<protocol>://<host>:<port>/<paths>`	The endpoint URL to which client application connect. The out-of-the-box value is https://firehose.crowdstrike.com/sensors/entities/datafeed/v1	Y	
`app_id`	string	Identifier to be used when connecting to Falcon Streaming API endpoint. This is an arbitrary string to be used to help us troubleshoot issues from server end.	Y	`FalconH`
`api_username`	string	User name to be used for client verification.	If version = 1	
`api_password`	string	Password to be used for client verification.	If version = 1	
`api_key`	string	API Key to be used for client verification.	If version = 2	
`api_uuid`	string	API UUID to be used for client verification.	If version = 2	
`connection_timeout`	number > 0 (seconds)	Amount of time (in seconds) client should wait for a connection to complete before considering a retry.	N	5 se
`read_timeout`	number > 0 (seconds)	Amount of time (in seconds) client should wait for server's response headers after fully writing the request.	N	8 se
`partition`	`all` or partition number (0-n)	Partition to be consumed by the running instance of the client application.	N	
`http_proxy`	`<protocol>://<host>:<port>`	HTTP proxy to be used to connect to Falcon Streaming API endpoint. This can also be set in the environment variable `$HTTP_PROXY`.	N	
`output_format`	`syslog` or `json`	`syslog`: will output syslog format with flat key=value pairs and uses the mapping configuration. Use syslog format if CEF/LEEF output is required. `json`: will output raw nested json format received from the Falcon Streaming API.	N	j
`output_to_file`	`true` or `false`	Enable/disable event output to file.	N	t
`output_path`	string	Location of file where event output should be written to.	N	`/var/log/crowdstrike/falconho`

[Logging] Section

Key	Value	Description	Required	Default
`verbose_log`	`true` or `false`	Enable/disable verbose logging.	N	true
`max_size`	number > 0 (MB)	Maximum individual log file size in Megabytes before rotation.	N	100MB
`max_backups`	number > 0 (count)	Number of backups to keep before purging.	N	10
`max_age`	number > 0 (days)	Maximum age (in days) of backup files before it is deleted.	N	30 days

[Syslog] Section

Key	Value	Description	Required	Default
`send_to_syslog_server`	`true` or `false`	Enable/disable push to syslog server.	Y	n/a
`host`	string (internet address)	Syslog/SIEM host address. It can be IP or host name.	If send_to_syslog_server is true	n/a
`port`	0-65535	Network port.	If send_to_syslog_server is true	n/a
`protocol`	`udp` or `tcp`	**udp**: User Datagram Protocol, connectionless transmission model \n . **tcp**: Transmission Control Protocol, guarantees delivery of data and sequence.	If send_to_syslog_server is true	n/a
`tag`	string	Syslog tag	N	n/a
`header_delim`	string	Header will be delimited by this value	N	n/a
`header_prefix`	string	Prefix that will be appended to syslog line	N	n/a
`key_val_delim`	string	Delimiter to be used between key and value i.e. if equal sign '=' is used then result will be key=value if a colon ':' is used then result will be key:value.	N	n/a
`field_delim`	string	Delimiter to be used to separate key and value pairs i.e. if pipe (¦) is used as `field_delim` and '=' is used as `key_val_delim`, then the result will be `key1=value1 PIPE key2=value2 PIPE key3=value3`	N	< space >
`val_enclosure`	string	String to be used to enclose the value of the key-value pairs i.e. if a single quote is used then the result will be key1='value1'	N	n/a
`time_fields`	comma-separated strings	Comma-separated strings of fields treated as times, to which the `time_format` configuration will be applied.	N	n/a
`time_format`	See Time Format Values table below.	See Time Format Values table below.	N	`yyyy-MM-dd HH:mm:ss`
`event_type_field`	string	Fields from nested JSON with dot notation e.g. metadata.eventType. This will be used for filtering and mapping. It is not recommended to change this field unless there is instruction to do so from CrowdStrike.	N	n/a

`event_subtype_field`	comma-separated strings	Fields from nested JSON with dot notation e.g. event.subType. This will be used for filtering and mapping. Please do not edit or adjust unless otherwise advised to do so by CrowdStrike.	N	n/a
`max_length`	number (bytes)	Maximum length of syslog line before being truncated. Truncation will happen atomically by field. Key-value pairs will not be appended unless the entire string will fit within the next line. No partial truncation will happen. The field will either show or not show.	N	n/a

TIME FORMAT VALUES

The following table shows values for the `time_format` syslog key above.

Key	Conversion
HH	2-digit hours
hh	2-digit hours
H	single digit hours
h	single digit hours
mm	minutes
ss	seconds
MMMM	Full month names e.g. January, February
MMM	3 characters month names e.g. Jan, Feb
MM	2 digit month i.e. 01, 02
M	1 digit month (when applicable) e.g. 1, 2, 12
pm	AM/PM
PM	AM/PM
ZZZZ	GMT Time offset e.g. -07:00
ZZZ	Timezone e.g. MST, PST
ZZ	Z notation of time offset e.g. Z07:00
yyyy	4-digit year
YYYY	4-digit year
YY	2-digit year
yy	2-digit year
DDDD	Full day name e.g. Monday, Tuesday
dddd	Full day name e.g. Monday, Tuesday
DDD	3-character day abbreviation e.g. Mon, Tue
ddd	3-character day abbreviation e.g. Mon, Tue
DD	2-digit day e.g. 02
dd	2-digit day e.g. 02
D	1-digit day e.g. 1
d	1-digit day e.g. 1

[EventTypeCollection] Section

This section specifies what event type to collect based on the event_type_field configuration in the [Syslog] section.

Key	Value	Description	Required	Default
The key is being derived from the value of events coming in of which key is specified by `event_type_field`.	`true` or `false`	Currently supported event types (as key) are `DetectionSummaryEvent`, `LoginAuditEvent`, `UserActivityAuditEvent`, `AuthActivityAuditEvent`, `CustomerIOCEvent` and `HashSpreadingEvent`. If true, the event will be collection. Otherwise the event will be skipped and not reported.	Y	n/a

[EventSubTypeCollection] Section

This section specifies what event type to collect based on the event_subtype_field configuration in the [Syslog] section.

Key	Value	Description	Required	Default
The key is being derived from the value of events coming in of which key is specified by `event_subtype_field`.	`true` or `false`	Currently supported event types (as key) are `DetectionSummaryEvent_DnsRequests`, `DetectionSummaryEvent_NetworkAccesses`, `DetectionSummaryEvent_DocumentAccessed`, `DetectionSummaryEvent_ScanResults`, and `DetectionSummaryEvent_ExecutablesWritten`. If true, event will be collection, otherwise event will be skipped and not reported.	Y	n/a

Syslog Mappings

MAPPING SECTION

The section names enclosed by square brackets e.g. [DetectionSummaryEvent], [DetectionSummaryEvent_DnsRequests] are derived from event types and event sub-types. The format is as follows.

Event:

```
[EventType]
```

Event sub-type:

```
[EventType_EventSubType] replace "EventType" and "EventSubType" with actual value
```

Example:

```
[DetectionSummaryEvent_DnsRequests]
```

MAPPING KEY-VALUE PAIRS

> **Important**: If the event type and/or event sub-type section is not specified, then the event WILL NOT be included. Additionally, if the field is not specified in the section for the event type and/or sub-type, the field will not be included.

The key is the value to which the field will be mapped. For example:

```
externalID = event.SensorID
```

means that the value of `event.SensorID` will be using 'externalID' as a key. Thus, if `event.SensorID` is `ThisIsMySensorID`, the result will be:

```
externalID = "ThisIsMySensorID"
```

In the example above, we would also specify `val_enclosure = "` and `key_val_delim` with an equal sign `=` as values.

If a configuration value is enclosed within a single quote, then the value will be taken as-is (literal). This is useful when we need to specify labels. For example:

```
aLiteralKey = 'This is a literal enclosed by single quote'
```

MAPPING HEADER

In order to specify the event type/sub-type headers, you can use the following notation:

```
__header.{n}
```

where {n} is a number starting with 0. The header has the same rules as the mappings:

1. If the value of the header configuration is not enclosed by a single quote, the value will be taken from the incoming event for the specific event type/sub-type.
2. If the value of header is enclosed by single quote, the value will be taken as-is from the value enclosed by single quote.

Example:

```
[DetectionSummaryEvent_DnsRequests]
__header.0 = metadata.eventType
__header.1 = 'DNS Request In A Detection Summary Event'
__header.2 = event.Severity

externalID = event.SensorId
spid = event.ProcessId
shost = event.ComputerName
suser = event.UserName
fname = event.FileName
filePath = event.FilePath
cs1Label = 'CommandLine'
cs1 = event.CommandLine
sntdom = event.MachineDomain
dhost = event.DnsRequests.DomainName
cs6Label = 'FalconHostLink'
cs6 = event.FalconHostLink
cn3Label = 'Offset'
cn3 = metadata.offset
deviceCustomDate1Label = 'DnsRequestTime'
deviceCustomDate1 = event.DnsRequests.LoadTime
```

Splunk Configuration for the Falcon SIEM Connector Log

The Falcon SIEM Connector log may be indexed in Splunk by adding the log file location to the `inputs.conf` file and adding the indexing properties to the `props.conf` file.

The default location for the Connector logs is `/var/log/crowdstrike/falconhoseclient/`. Using this as the location, add the following monitoring stanza to `inputs.conf`:

```
[monitor:///var/log/crowdstrike/falconhoseclient/cs.falconhoseclient.log]
disabled = false
sourcetype = firehose
```

To configure basic attributes for event line breaking, timestamp extraction, and max lines per event (MAX_EVENTS), add the following stanza to `props.conf`:

```
[firehose]
BREAK_ONLY_BEFORE = ^{
DATETIME_CONFIG =
MAX_EVENTS = 2048
NO_BINARY_CHECK = true
TIME_PREFIX = (\"LoginTime":\s)|(\"ProcessStartTime\":\s)|(\"UTCTimestamp\":\s)
TRUNCATE = 0
category = Custom
disabled = false
pulldown_type = true
```

The above configuration corresponds to the following event types:

1. `AuthActivityAuditEvent`
2. `DetectionSummaryEvent`
3. `LoginAuditEvent`
4. `UserActivityAuditEvent`

Additional event types may not be covered.

The output connector log contains events formatted in JSON. Splunk line breaking is configured via regular expression, expressed as the left most opening brace ("{") marking the start of a new JSON event: i.e. each JSON event begins with a left brace ("{") at column one.

Once the configurations are in place, Falcon SIEM Connector log events will be indexed. You may need to restart Splunk to enable indexing. The following basic search may be used to return raw connector log events:

```
index=main source="/var/log/crowdstrike/falconhoseclient/cs.falconhoseclient.log" sourcetype="firehose"
```

Be sure to select the search window in the time picker, or add earliest and latest times to the search, prior to running the above search.

Troubleshooting and Errors

When troubleshooting, refer to `/var/log/crowdstrike/cs.falconhoseclient.log` for error lines.

Configuration Errors

Configuration errors are prefixed with ERROR[config] in the log file. The following guide will attempt to describe and potentially help to point the right direction in resolving issues:

Error	Description/Resolution
`api_password setting is required`	Please specify valid `api_password` under [Settings] section.
`api_url setting is required`	Please specify valid `api_url` under [Settings] section.
`api_username setting is required`	Please specify valid `api_username` under [Settings] section.
`api_uuid setting is required`	Please specify valid `api_uuid` under [Settings] section.
`Invalid connection_timeout configuration value: <value>`	Please specify valid `connection_timeout` value under [Settings] section.
`Invalid log max size, defaulting to <size>MB`	Please specify valid `logging max_size` value under [Logging] section.
`Invalid partition configuration value: <value>`	Please specify valid partition value under [Settings] section.
`Invalid read_timeout configuration value: <value>`	Please specify valid `read_timeout` value under [Settings] section.
`Invalid send_to_syslog_server configuration value: <value>`	Please specify valid `send_to_syslog_server` value under [Syslog] section.
`Missing [Settings] section in configuration file. Unable to determine what format to produce`	Configuration file might be malformed. Please ensure that there is [Settings] section in the configuration file.
`Missing event_subtype_field configuration for Syslog.`	Please specify valid `event_subtype_field` value under [Syslog] section.
`Missing event_type_field configuration for Syslog.`	Please specify valid `event_type_field` value under [Syslog] section.
`Missing field_delim configuration for Syslog`	Please specify valid `field_delim` value under [Syslog] section.
`Missing header_delim configuration for Syslog`	Please specify valid `header_delim` value under [Syslog] section.
`Missing header_prefix configuration for Syslog`	Please specify valid `header_prefix` value under [Syslog] section.
`Missing host configuration for Syslog`	Please specify valid protocol host under [Syslog] section.
`Missing key_val_delim configuration for Syslog`	Please specify valid `key_val_delim` value under [Syslog] section.
`Missing max_length configuration for Syslog`	Please specify valid `max_length` value under [Syslog] section.
`Missing port configuration for Syslog`	Please specify valid port value under [Syslog] section.
`Missing protocol configuration for Syslog`	Please specify valid protocol setting under [Syslog] section.
`Missing send_to_syslog_server configuration`	Please specify valid `send_to_syslog_server` setting under [Syslog] section.
`Missing Settings section in configuration file.`	Configuration file might be malformed. Please ensure that there is [Settings] section in the configuration file.
`Missing tag configuration for Syslog`	Please specify valid tag value under [Syslog] section.
`Missing time_fields configuration for Syslog`	Please specify valid time_fields value under [Syslog] section.
`Missing val_enclosure configuration for Syslog`	Please specify valid `val_enclosure` value under [Syslog] section.
`Unable to check if we want to output to file through output_to_file configuration`	Missing `output_to_file` under [Settings] section to specify whether or not client should output the event to file.

`Unable to create output file: <output_file>, writing to service log: <service_log>`	Please specify valid output_path under [Settings] section to output event into and make sure that write permission is given to service.
`Unable to retrieve log max size, defaulting to <size>MB`	Please specify valid logging `max_size` under [Logging] section.
`Unable to retrieve output_path, default to service log`	Please specify valid `output_path` under [Settings] section to output event into and make sure that write permission is given to service.
`Unsupported protocol for Syslog. Supported protocols are udp or tcp`	Please specify to use udp/tcp for syslog protocol under [Syslog] section.
`Version setting '<version>' is invalid`	Invalid version setting under [Settings] section.
`Version setting is required`	Missing version setting under [Settings] section.

Connector/Client Errors

Error	Description/resolution
`Discovery failed with HTTP: <http_code>, Payload: <payload>`	Server is returning status code other than 200 during discovery stage. The `<http_code>` is usually in the 4xx range. In most cases, HTTP code will be 401 which means unauthorized access has been attempted. Retries will be performed. Please ensure that credentials provided are correct.
`Failed to convert offsets [<offsets>]`	Failure occurred while converting offset to be stored. Please contact CrowdStrike Customer Support with the log file.
`Failed to handle feed for partition <partition_no>: <event> - <message>`	Failure occurred while performing event transformation or posting to syslog remote server. `<message>` contains more information about this error. Please ensure that syslog remote server is configured properly and please contact CrowdStrike Customer Support with the log file.
`Failed to read from i/o buffer - <message>`	Failure occurred while digesting events. `<message>` contains more information about this error. This can occur for several reasons (1) Network interruption occurs during ingestion of event: Retries will be attempted. (2) Falcon Streaming Client service is interrupted by shutdown: Retries will be attempted after start up.
`Failed to retrieve partition/offset <partition_no> with last <format> data <event>`	Failure occurred while parsing event data to retrieve offset. Please contact CrowdStrike Customer Support with the log file.
`Failed to save offsets [<offsets>] to file`	Failure occurred while attempting to save offset to file. Please ensure that permission is granted to service to write to file system under `/opt/crowdstrike/*`.
`Missing data feed URL for <configuration>`	In some cases, when connector/client recovered from ungraceful disconnects i.e. power outage, hot reboot etc, server still maintains the existing session with the given `app_id`. Certain configurations in client's environment may maintain the opened connection to server longer than expected, this will in turn cause the endpoint to be unaware of client's disconnections. Falcon Streaming Client/Connector will keep retrying until streaming is successful. In order to get around this quicker, `app_id` can be modified into a different `app_id` and restart the service.

`No resource discovered for<configuration>`	In some cases, when connector/client recovered from ungraceful disconnects i.e. power outage, hot reboot etc, server still maintains the existing session with the given `app_id`. Certain configurations in client's environment may maintain the opened connection to server longer than expected, this will in turn cause the endpoint to be unaware of client's disconnections. Falcon Streaming Client/Connector will keep retrying until streaming is successful. In order to get around this quicker, `app_id` can be modified into a different `app_id` and restart the service.
`Partition streaming failed - HTTP: <http_code> - <message>`	Server is returning status code other than 200 during event streaming. The `<http_code>` is usually in the 4xx range. In most cases, HTTP code will be 401 which means unauthorized access has been attempted. `<message>` part contains more information about this error. Retries will be performed. Please ensure that credentials provided are correct.
`Partition streaming failed @ GET: <partition_no> - <message>`	Error returned during the attempt to stream partition from the underlying HTTP GET. Usually caused by underlying network connectivity which renders the client unable to reach the Falcon Streaming endpoint part contains more information about this error. Retries will be performed. Please ensure that endpoint is reachable from client machine.
`Timed out, last heartbeat received <time> ago`	Timed out occurred while waiting for Falcon Streaming endpoint heartbeat. Retries will be attempted. Please make sure client machine is able to reach Falcon Streaming endpoint.
`Unable to parse dataFeedURL from <configuration>`	This is cause by server returning unexpected URL format. Please contact CrowdStrike Customer Support with the log file.

Transformation/Syslog Errors

Configuration errors are prefixed with ERROR[syslog] in the log file. The following guide will attempt to describe and potentially help to point the right direction in resolving issues:

Error	Description/resolution
`Missing event (sub)type for <event>`	Please contact CrowdStrike Customer Support with the log file.
`Unable to obtain section key for event: <event>`	Please contact CrowdStrike Customer Support with the log file.
`Unable to parse <event_value> as time with format(<format>)`	Please review your time_fields configuration, the field might not have time value.
`Missing field name:<field_name> in the feed type: <feed_type>`	Please review your mapping configuration with the given `field_name` under `feed_type` section.
`Unexpected JSON value in array format from key <key>, value <value>`	Please contact CrowdStrike Customer Support with the log file.

Revision History

Date	Release	Notes	Completed by:
2/24/2016	1.0	Initial release.	Nick Cangie
2/25/2016	2.0	Added additional system requirements information. Added information about the impact of restarting the connector.	Nick Cangie
3/10/2016	3.0	Added info about obtaining credentials. Updated diagram.	Nick Cangie
3/31/2016	3.1	Updated the installation diagram.	Nick Cangie
5/18/2016	3.2	Rebranded as Falcon SIEM Connector. Removed references to Falcon Firehose API. Renamed to Falcon Streaming API.	Nick Cangie
5/31/2016	3.3	Updated SIEM Connector diagram.	Nick Cangie
6/7/2016	3.4	Updating styles.	Nick Cangie
10/24/2016	4.0	GA for new UI.	Nick Cangie
1/3/2017	4.1	Adding note about proxy authentication.	Nick Cangie
1/16/2017	5.0	Adding support for Ubuntu.	Nick Cangie
2/3/2017	5.1	Updating default values for `output_path`.	Nick Cangie
5.2	09/18/2017	Removing branded references to "Falcon Host"	Scott P