

CrowdStrike API Integration Guide

A step-by-step guide to integrate CrowdStrike with Securus360 services.

Overview

The Securus360 Cyber SOC has the ability to collect log files from CrowdStrike. These logs empower Securus360 to monitor and alert on potentially suspicious activity occurring on your CrowdStrike endpoints.

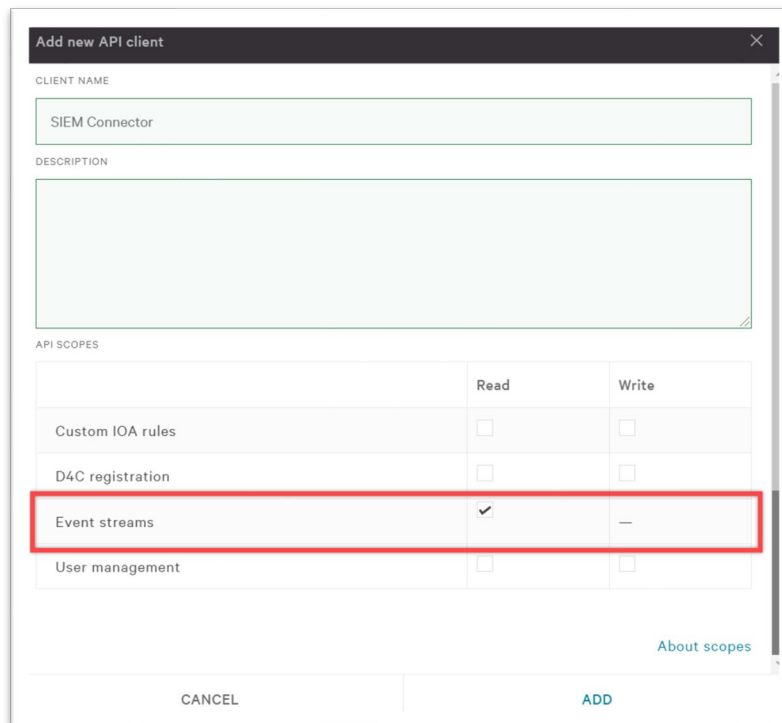
For this to work, you will need to configure a few things within CrowdStrike. This document will walk you through that process.

Supported Platform Version

- CrowdStrike Falcon SIEM-Connector-v2.0

Prerequisites

First, you'll want to define the API client using the Falcon SIEM Connector and set the scope. Refer to this [guide](#) to set up new API client keys. Please ensure that the scope includes read access for Event streams.



	Read	Write
Custom IOA rules	<input type="checkbox"/>	<input type="checkbox"/>
D4C registration	<input type="checkbox"/>	<input type="checkbox"/>
Event streams	<input checked="" type="checkbox"/>	—
User management	<input type="checkbox"/>	<input type="checkbox"/>

CrowdStrike API Integration Guide

Installation Steps

- Download the SIEM Connector install package (Ubuntu)
- The CrowdStrike Falcon® SIEM Connector (SIEM Connector) runs as a service on a local Linux server.
- The following links provide Installation and Configuration documentation for each CrowdStrike Cloud:
 - US1: <https://falcon.CrowdStrike.com/documentation/14/siem-connector>
 - US2: <https://falcon.us-2.CrowdStrike.com/documentation/14/siem-connector>
 - EU1: <https://falcon.eu-1.CrowdStrike.com/documentation/14/siem-connector>
 - GOV1: <https://falcon.laggar.gcw.CrowdStrike.com/documentation/14/siem-connector>

- Once logged in, navigate to:

Support and resources > Resources and tools > Tool downloads

NOTE: A comprehensive guide can be found in your console at Support and Resources > Support > Documentation

Final Steps

- Securus360 will provide you with a link to upload files to us. Please ensure the following are *both* included:
 - CrowdStrike API Key
 - Ubuntu Installation Package

Once uploaded, send an email to support@securus360.com to let us know that it has been successfully uploaded. Securus360 will confirm we have received the file as quickly as possible.