



Cisco Security Cloud App for Splunk User Guide

First Published: 2024-09-05

Last Modified: 2025-08-22

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Cisco Security Cloud App Overview 1
	Cisco Security Cloud App Overview 1
CHAPTER 2	Install and Upgrade the Cisco Security Cloud App 3
	Installation Overview 3
	Prerequisites 3
	Install Cisco Security Cloud App from a Package 4
	Install Cisco Security Cloud App from Splunkbase 5
	Upgrade Cisco Security Cloud App 7
	Upgrade from a major release to another major release 7
	Upgrade from a minor release to another minor release 8
CHAPTER 3	User Roles and Permissions in Cisco Security Cloud App 9
	User Roles and Permissions in Cisco Security Cloud App 9
	Role Assignment Best Practices 12
	Edit a User Role 12
	Known Limitations for User Role Permissions in Splunk Cloud 14
CHAPTER 4	Scale Your Deployment for Large Data Volumes 15
	Best Practices for Scaling Your Splunk Deployment 15
	Sample Cisco Security Cloud App Use Case 15
	When to Migrate from a Single Node Deployment to Distributed Deployment 16
CHAPTER 5	Configure Cisco Products in Cisco Security Cloud App 19
	Set Up an Application 19
	Configure an Application 21

Cisco Duo	22
Cisco Secure Malware Analytics	24
Cisco Secure Firewall Management Center	25
Firewall e-Streamer	25
Firewall Syslog and ASA	28
Firewall API	29
Cisco Multicloud Defense	30
Cisco XDR	31
Cisco Secure Email Threat Defense	33
Cisco Secure Network Analytics	34
Cisco Secure Endpoint	36
Cisco Vulnerability Intelligence	37
Search and Reporting Tool	39
Cisco AI Defense	42
Cisco Isovalent Runtime Security	43
Cisco Secure Client NVM	45
Cisco Identity Intelligence (CII)	45
<hr/>	
CHAPTER 6	Monitor Dashboards 53
	Data Integrity Dashboard 53
	Resource Utilization Dashboard 54
<hr/>	
CHAPTER 7	API Compatibility Matrix 57
	APIs Compatibility Matrix 58
<hr/>	
CHAPTER 8	Troubleshoot Issues in Cisco Security Cloud App 63
	Collect and Analyze Logs 63
	App Stability and Post-Upgrade Issues 64
	Failed to Create or Edit an Input 64
	Delayed Event Updates 65
	Failed to Fetch Input Data for Applications 65
	Syslog or ASA Input Deletion Issues 65
	Cisco Security Cloud App UI loads infinitely 65
	KV Store process issues 66

[Troubleshoot Splunk HEC Connectivity](#) 67

[Troubleshoot SSL Validation Errors](#) 68

[Contact Cisco Support](#) 69



CHAPTER 1

Cisco Security Cloud App Overview

- [Cisco Security Cloud App Overview, on page 1](#)

Cisco Security Cloud App Overview

Cisco Security Cloud App is a web application that offers a centralized platform to integrate Cisco security products with Splunk.

Cisco Security Cloud App Benefits

The app offers these benefits:

- A unified interface to integrate Cisco security products into Splunk.
- Built-in health checks and dashboards to monitor data ingestion and resource usage.
- Guided input configuration and validation workflows.
- Simplified upgrade and maintenance processes.
- Centralized access to dashboards, data integrity checks, and metrics across Cisco products.

List of Integrated Cisco Security Products Supported by Cisco Security Cloud App

The app supports a variety of Cisco security products, allowing ingestion and visualization of data from products such as:

- [Cisco Duo](#)
- [Cisco Secure Firewall \(Syslog, eStreamer, API\)](#)
- [Cisco Secure Malware Analytics](#)
- [Cisco Secure Endpoint](#)
- [Cisco Secure Network Analytics](#)
- [Cisco XDR](#)
- [Cisco Multicloud Defense](#)
- [Cisco Email Threat Defense](#)

- [Cisco Vulnerability Intelligence, on page 37](#)
- [Cisco AI Defense, on page 42](#)
- [Cisco Secure Client NVM, on page 45](#)
- [Cisco Isovalent Runtime Security, on page 43](#)
- [Cisco Identity Intelligence](#)

These integrations provide predefined input templates to streamline the configuration.

Architecture and Data Flow

The app supports deployment on single-instance and distributed Splunk environments. Based on your deployment scale and the volume of incoming data, you can run the app on a standalone search head or distribute it across a Splunk search head cluster.

Cisco security products send events to Splunk through APIs or syslog. The app collects these events using modular inputs, each sending data to a specific index. The built-in health checks ensure inputs work properly, and dashboards display the data for detection, correlation, and investigation.

System Requirements

Check that your Splunk Enterprise version is supported before installing or upgrading the app. Refer to the Splunkbase listing for specific version support details. View the Splunkbase listing to see which Splunk versions are supported.

Supported environments include:

- Operating Systems - Windows, macOS, and Linux.
- Supported browsers - Chrome, Microsoft Edge, and Mozilla Firefox.

Use a recent browser version and enable JavaScript for the best performance.

API Compatibility Matrix

Refer to the [API Compatibility Matrix](#) for detailed support information, which includes product versions and endpoint coverage.



CHAPTER 2

Install and Upgrade the Cisco Security Cloud App

- [Installation Overview, on page 3](#)
- [Prerequisites, on page 3](#)
- [Install Cisco Security Cloud App from a Package, on page 4](#)
- [Install Cisco Security Cloud App from Splunkbase, on page 5](#)
- [Upgrade Cisco Security Cloud App, on page 7](#)

Installation Overview

The Cisco Security Cloud App for Splunk can be deployed in either a single-instance or distributed Splunk environment:

- **Single-instance deployment:** The app runs on a single system that handles all roles—such as indexer, search head, and forwarder.
- **Distributed deployment:** Roles are distributed across multiple systems (for example, separate indexers and search heads). In this setup, you must install the app on the search heads.

You can install the app in one of the following ways:

- Install from a package
- Install from Splunkbase

Prerequisites

Ensure these prerequisites are met before installing or upgrading the app:

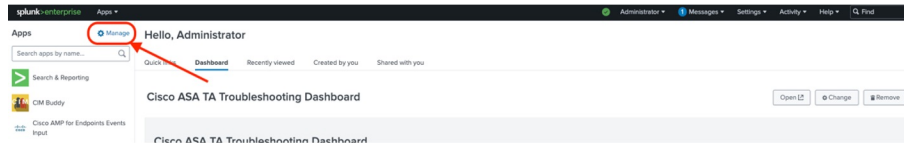
- Your system meets the required specifications. See the [System Requirements](#) section.
- You have administrator or equivalent privileges in Splunk. See [User Roles and Permissions in Cisco Security Cloud App, on page 9](#) for more information.
- Network access to Cisco Secure cloud products is available for connector configuration.

Install Cisco Security Cloud App from a Package

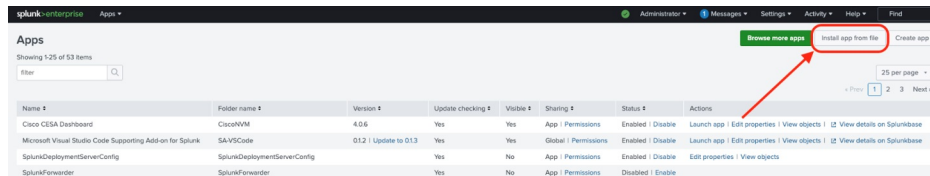
Procedure

Step 1 Download Security Cloud App from the Splunkbase: <https://splunkbase.splunk.com/app/7404>.

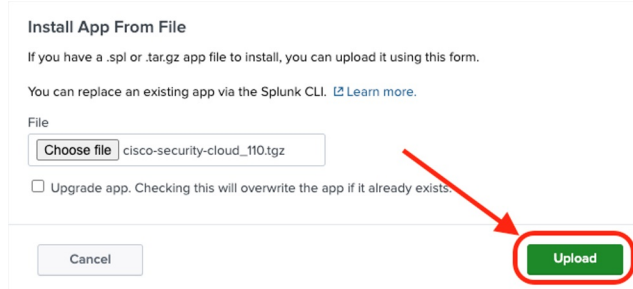
Step 2 Click **Manage** to navigate to the **Apps** page.



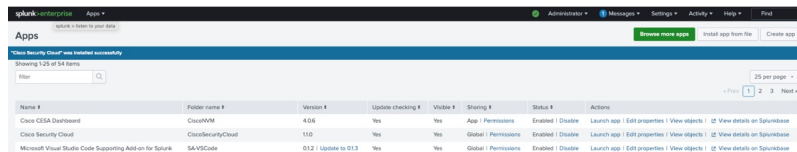
Step 3 On the **Apps** page, click **Install app from file**.

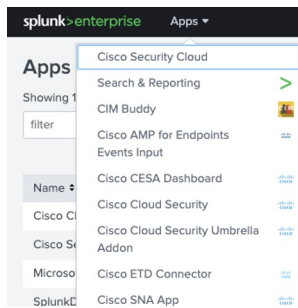


Step 4 In the **Install App From File** window, choose the file (Security Cloud App) that you downloaded and click **Upload**.



Step 5 After the installation is complete, verify that the **Cisco Security Cloud** app is listed on the **Apps** page.



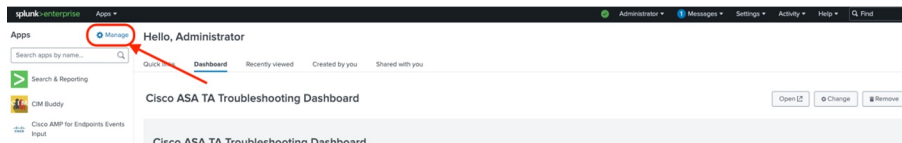


Install Cisco Security Cloud App from Splunkbase

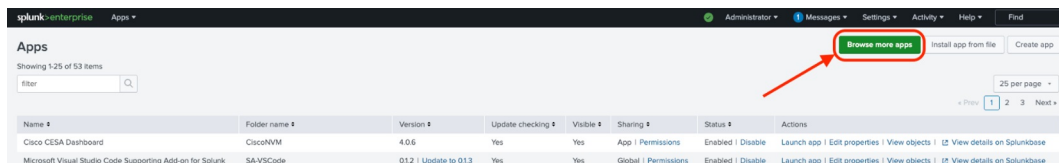
Procedure

Step 1 Log in to [Splunkbase](#) using your administrator credentials.

Step 2 Click **Manage** to navigate to the **Apps** page.

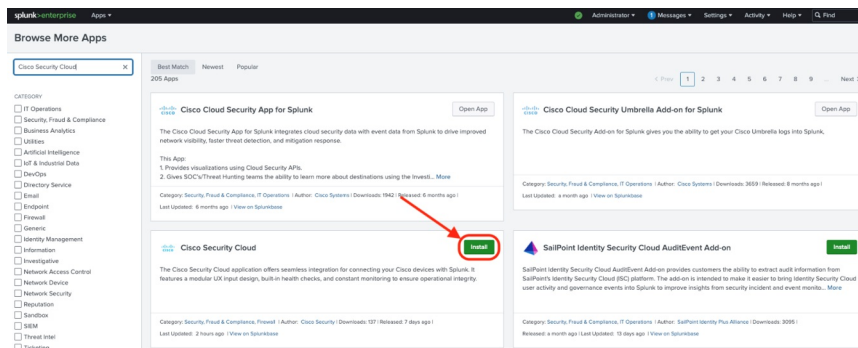


Step 3 On the **Apps** page, click **Browse more apps**.



Step 4 Search for Security Cloud App in the search bar.

Step 5 On the Security Cloud App card, click **Install**.



Install Cisco Security Cloud App from Splunkbase

Step 6 Enter your Splunk credentials in the **Login and Install** window. Review the terms and conditions and click **Agree and Install**.

Login and Install [X]

Enter your Splunk.com username and password to download the app.

Username

Password

[Forgot your password?](#)

The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app (developed by you or a third party) and does not provide any warranty or support. Installation of a third-party app can introduce security risks. By clicking "Agree" below, you acknowledge and accept such risks. If you have any questions, complaints or claims with respect to an app, please contact the applicable licensor directly whose contact information can be found on the Splunkbase download page.

Cisco Security Cloud is governed by the following license: 3rd_party_eula

I have read the terms and conditions of the license(s) and agree to be bound by them. I also agree to Splunk's Website Terms of Use.

Step 7 After the installation complete, click **Open the App**.

Complete [X]

Cisco Security Cloud was successfully installed.

Step 8 You are redirected to the **Application Setup** page of Security Cloud App.

Data Integrity Resource Utilization **Application Setup** App Analytics Cisco Security Cloud

Application Setup

My Apps

Search...

Input Name	Product	Host	Enabled	Status	Source Type	Index
Cisco Products						
Search...						

Duo
Network Security App

Zero trust is the future of information security - and Duo is your rock-solid foundation. Duo secures your workforce, taking access security beyond the corporate network perimeter to protect your data at every authentication attempt, from any device, anywhere. Confirm user identities in a snap, monitor the health of managed and unmanaged devices, set adaptive security policies tailored for your business, secure remote access without a device agent, and provide secure, user-friendly single sign-on, quickly and easily with Duo.

Secure Malware Analytics
Network Security App

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect organizations from malware. Secure Malware Analytics is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impacting the user environment.

Secure Firewall
Firewall App

The integration of Secure Firewall Threat Defense (formerly Firepower Threat Defense) provides the capability to investigate, identify, and enrich Cisco Secure Firewall intrusion events with context from integrations across the integrated products. It offers an automated triage and prioritization of intrusion events through incidents.

Multicloud Defense
Cloud Security App

Cisco Multicloud Defense protects all of your cloud environments using a single software-as-a-service (SaaS) control plane, eliminating inefficient, complex, and costly point solutions.

XDR
Threat Detection and Response

Cisco XDR changes the way security teams look at detection and response. Our cloud-based solution is designed to simplify security operations and empower security teams to detect, prioritize, and respond to the most sophisticated threats. Integrating with the broader Cisco security portfolio and select third-party offerings, Cisco XDR is one of the most comprehensive and flexible solutions on the market today.

Secure Network Analytics
Network Analytics

Analyze your existing network data to help detect threats that may have found a way to bypass your existing controls, before they can do serious damage.

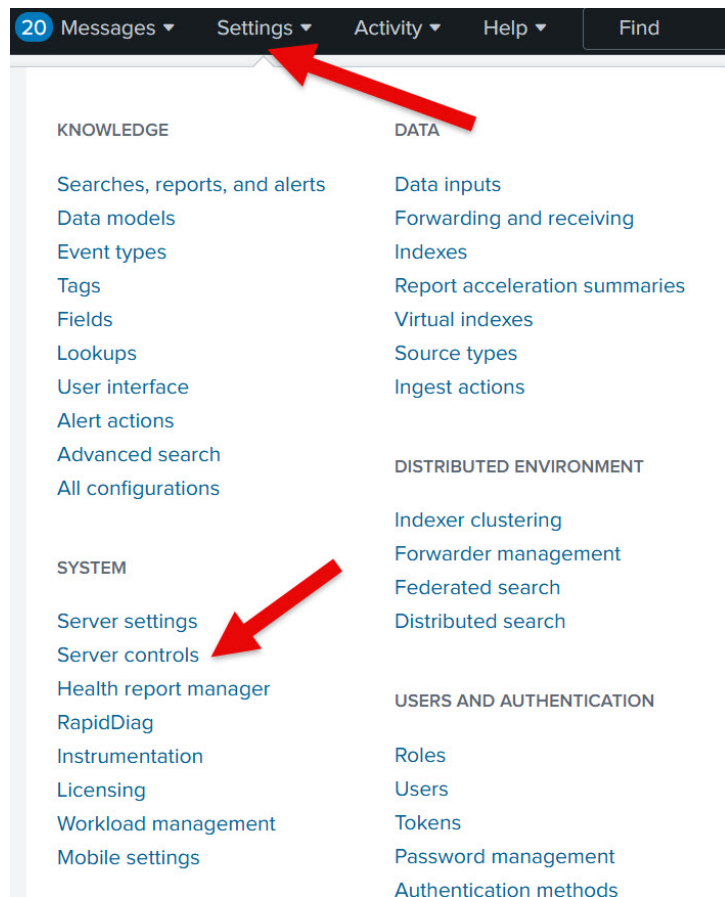
Upgrade Cisco Security Cloud App

Upgrade from a major release to another major release

Follow these steps to upgrade the Cisco Security Cloud App from a major release to another major release:

Procedure

- Step 1** Uninstall the current release of the app.
- Step 2** Clear the browser cache and cookies.
- Step 3** Install the newer release of the app using one of the two methods described earlier - [Install the app from file](#) or [Install the app from Splunkbase](#).
- Step 4** Restart Splunk by navigating to **Splunk > Settings > Server Controls > Restart Splunk**.

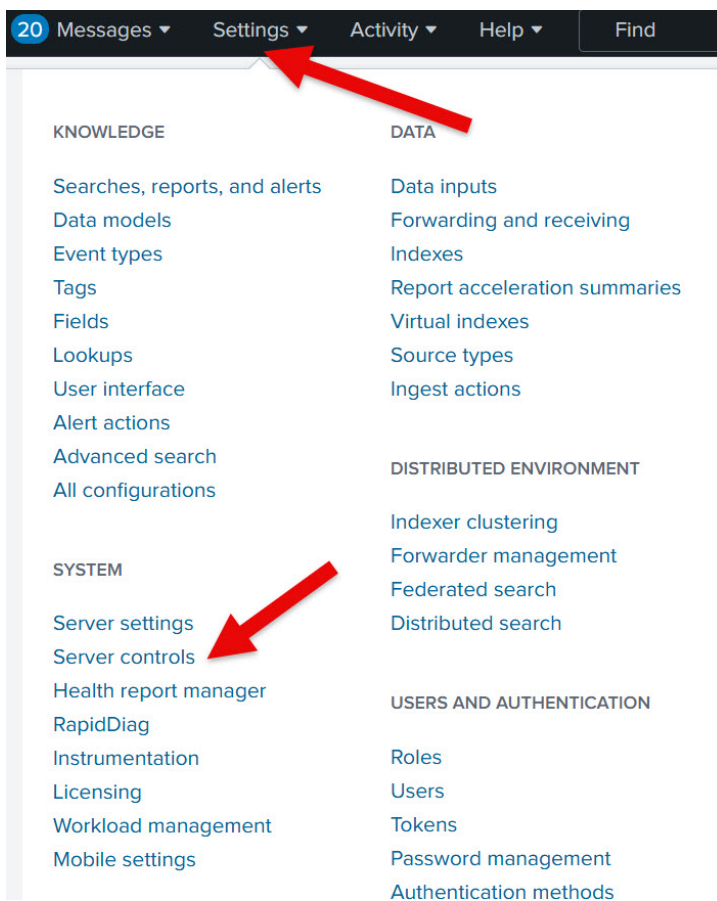


Upgrade from a minor release to another minor release

Follow these steps to upgrade the Cisco Security Cloud App from a minor release to another minor release (For example, upgrade from release x.1.x to x.2.x release)

Procedure

- Step 1** Clear the browser cache and cookies.
- Step 2** Install the newer release of the app using one of the two methods described earlier - [Install the app from file](#) or [Install the app from Splunkbase](#).
- Step 3** Restart Splunk. Navigate to **Splunk > Settings > Server Controls > Restart Splunk**.





CHAPTER 3

User Roles and Permissions in Cisco Security Cloud App

- [User Roles and Permissions in Cisco Security Cloud App, on page 9](#)
- [Role Assignment Best Practices, on page 12](#)
- [Edit a User Role, on page 12](#)
- [Known Limitations for User Role Permissions in Splunk Cloud, on page 14](#)

User Roles and Permissions in Cisco Security Cloud App

User roles help assign appropriate privileges based on each user's responsibilities. Security Cloud App provides a range of roles with varying permission levels to support different user needs. These include standard Splunk roles, aligning with Splunk's built-in role-based access control system.

The following table outlines the default roles and their associated permissions available in Security Cloud App.

Role	Purpose	Privileges
<i>Admin</i>	Role with the highest privilege in the system. It is designed for users who need complete control over system configurations, indexes, and data.	<ul style="list-style-type: none">• Full access to all functionalities, including data inputs, searches, reports, alerts, dashboards, and knowledge objects.• Ability to manage all users and roles, and access to all indexes.• Permission to configure system settings, create and manage indexes, and set up distributed environments.• Capable of modifying auth settings, system configurations, and forwarders.

Role	Purpose	Privileges
<i>Can_delete</i>	A specialized role granted to users who need the ability to delete events from indexes. Typically, it is assigned temporarily due to the risks involved.	<ul style="list-style-type: none"> • Can permanently delete events from indexes using the delete search command. • Often combined with other roles such as, Admin, for data management tasks.
<i>Power</i>	Designed for advanced users who need more capabilities than regular users but do not require full administrative access.	<ul style="list-style-type: none"> • Ability to create, edit, and share knowledge objects such as saved searches, dashboards, alerts, and reports. • Can perform real-time searches to monitor events as they occur. • Can schedule reports and alerts.
<i>Splunk-system-role</i>	Allows both administrative work and data management.	<ul style="list-style-type: none"> • Full access for managing data and performing administrative tasks. • Can configure system settings and manage users and roles, similar to the Admin role. • Can access and manage data across indexes.
<i>User</i>	The default role for most end users. It provides access to basic search and reporting functionalities.	<ul style="list-style-type: none"> • Can perform searches across the indexes to which they have access. • Can create and save personal reports, alerts, and dashboards, with limited sharing permissions. • Cannot manage users, system settings, or indexes.

In addition to the default roles, Security Cloud App provides specific roles and functionalities. The following table shows the functionalities that are allowed for each role in Security Cloud App.

Permissions	Role				
	admin	can_delete	power	splunk-system-role	user
Create inputs	✓	✗	✗	✓	✗

Permissions	Role				
	admin	can_delete	power	splunk-system-role	user
View inputs	✓	✗	✗	✓	✗
Edit inputs	✓	✗	✗	✓	✗
Delete inputs	✓	✗	✗	✓	✗
View dashboards	✓	✗	✓	✓	✓
Clone dashboards	✓	✓	✓	✓	✓
Edit dashboards	✓	✗	✗	✓	✗
Edit permissions	✓	✗	✗	✓	✗
Search events	✓	✗	✓	✓	✓
View indexes	✓	✗	✗	✓	✗
Create index	✓	✗	✗	✓	✗
Edit index	✓	✗	✗	✓	✗
Delete index	✓	✗	✗	✓	✗
View other users	✓	✗	✗	✓	✗
Edit other users	✓	✗	✗	✓	✗
Delete/Create other users	✓	✗	✗	✓	✗
Monitoring console	✓	✗	✗	✓	✗
Knowledge settings	✓	✓	✓	✓	✓
Roles settings	✓	✗	✗	✓	✗
Data settings	✓	✗	Report acceleration & Source types	✓	✗
Users and Authentication settings	✓	✗	✗	✓	Tokens
Distributed environment	✓	✗	✗	✓	✗

Role Assignment Best Practices

To maintain security and ensure appropriate access, follow these best practices when assigning user roles:

- Assign the **admin** role only to trusted administrators, as it provides full control over the system.
- Use the **can_delete** role sparingly, and only for users who need deletion rights for specific maintenance tasks.
- Grant the **power** role to security analysts and reporting staff so they can create and share searches, dashboards, and alerts.
- Use the **user** role for general access, and modify permissions only when users need to configure inputs.

Edit a User Role

By default, a user role doesn't have the required capabilities to view all apps on the **Application Setup** page.

Procedure

- Step 1** To display all the apps that are created by the Admin inputs and their status for the user, do the following:
- a) Navigate to **Settings > Roles > user**.
 - b) Add the following capabilities to the User role:
 1. list_storage_passwords
 2. dispatch_rest_to_indexers
 - c) To show the correct status of the user, check the **Included** check box for the “_* (All internal indexes)” option in the Indexes tab.

Edit Role user ×

Name ⓘ

1. Inheritance 2. Capabilities **3. Indexes** 4. Restrictions 5. Resources

Wildcards
Instead of selecting individual indexes, you can create a Wildcard Index to dynamically capture all indexes that match the Wildcard. After you add a Wildcard Index, it appears in the Indexes table. Wildcard Indexes are limited to this role.

Indexes
Enable both the "Included" and "Default" checkboxes for an index to make that index searchable by default for this role. You must save this role before you can see its inherited wildcards.

Index Name	Included ⓘ	Default ⓘ	Showing all ▼
* (All non-internal indexes)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
_* (All internal indexes)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
_audit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Step 2 To enable a user to perform the Create, Read, Update, and Delete (CRUD) operations on an input, add the following capabilities to the User role:

a) Read permissions:

- list_inputs (capability to view basic inputs)
- list_storage_passwords (capability to view inputs that have data stored to secret store)
- dispatch_rest_to_indexers (capability to get information about index)

b) Create and Update permissions:

Note

Before you enable these permissions, ensure that Read permissions are enabled.

- indexes_edit (capability to create and update index)
- edit_storage_passwords (capability to edit inputs that have data stored to secret store)
- edit_token_http (capability to create and update http tokens)
- edit_tokens_all (capability to create and update other tokens)
- edit_tcp (capability to create and update tcp hosts)
- edit_udp (capability to create and update udp hosts)
- admin_all_objects (capability to create, edit, and delete inputs)

c) Delete permissions (read permissions must be enabled):

Note

Before you enable these permissions, ensure that Read permissions are enabled.

- admin_all_objects (capability to create, edit, and delete inputs)

Known Limitations for User Role Permissions in Splunk Cloud

Splunk Cloud does not support the following capabilities:

- `dispatch_rest_to_indexers`
- `edit_tcp`
- `edit_udp`

As a result:

- You cannot create Firewall ASA or Firewall Syslog inputs.
- The **Data Integrity** and **Resource Utilization** dashboards may display incomplete data and warning messages.



CHAPTER 4

Scale Your Deployment for Large Data Volumes

To support high data volumes and many users while maintaining performance and reliability, you should plan your deployment architecture carefully. This chapter explains when a single-instance setup is sufficient and when you should move to a distributed Splunk deployment.

- [Best Practices for Scaling Your Splunk Deployment, on page 15](#)
- [Sample Cisco Security Cloud App Use Case, on page 15](#)
- [When to Migrate from a Single Node Deployment to Distributed Deployment, on page 16](#)

Best Practices for Scaling Your Splunk Deployment

Scaling is crucial for handling multiple inputs and large data volumes in your Splunk app. Ensure your deployment can scale to match your infrastructure's capabilities.

For larger data sets, add more servers or storage as needed.

Scale your indexers, search heads, and forwarders independently. Ensure that any connected APIs can handle increased load.

To enable automatic, seamless scaling based on your data volume and search needs, use Splunk Cloud.

Sample Cisco Security Cloud App Use Case

Here is a sample performance and scale data for a Security Cloud App deployment:

Load on the App

- up to 90 GB data ingested per month
- up to 15 concurrent users

Configuration of the enterprise

- one Splunk Enterprise single instance deployed on AWS.
- one EC2 c5.4xlarge (vCPUs: 16, Memory: 32 GB) with Volume 100 GiB GP2 EBS with 300 IOPS

Metrics collected

- top CPU usage: 32%
- top memory usage: 5GB

Crash issue

Disk was full.

Mitigation

Set up an alert on CloudWatch and set the retention time on Splunk. For information, refer to <https://docs.splunk.com/Documentation/Splunk/8.0.0/Indexer/Configureindexstorage>

When to Migrate from a Single Node Deployment to Distributed Deployment

We recommend that you consider the one or more of the following factors before migrating to a distributed deployment.

Data Volume

- Single Instance Data ingestion: A single instance deployment can typically handle moderate amounts of data ingestion effectively, especially on a powerful instance like c5.4xlarge.
- Threshold: A single instance can handle a data ingestion of 50-100 GB per day. Exceeding this limit may result in performance issues such as, indexing, searching, and overall system performance can degrade, particularly with complex queries or large datasets.
- Distributed Deployment: If your data ingestion often exceeds 100 GB/day, we recommend that you migrate to a distributed deployment, where indexing is not a bottleneck and search performance remains optimal.

Number of Users and Search Load

- Single Instance Deployment: A single instance setup normally supports 10-20 active users with moderate search activity (e.g., running searches every few minutes).
- Threshold: If you observe more than 20 concurrent users regularly, especially with heavy search loads or complex queries, the performance of the single-instance setup may be affected. You may notice increased search latency, slower indexing, and higher resource contention (CPU and memory).
- Distributed Deployment: If you anticipate or experience growth beyond 20 active users, or if search activity becomes increasingly complex (e.g., frequent ad-hoc searches, dashboards with real-time monitoring), we recommend that you migrate to a distributed setup with separate search heads.

Number of Inputs (Data Sources)

- Single Instance Deployment: A single instance deployment can typically handle dozens of inputs without issue, provided they're not excessively high-volume.

- **Threshold:** If the number of inputs exceeds 50-100, particularly if some inputs are high-volume (e.g., syslog, large application logs), the single instance may become overburdened, leading to dropped data, delays in indexing, or reduced search performance.
- **Distributed Deployment:** If you have varied data sources or high-volume inputs that could lead to data ingestion rates beyond what a single instance can handle, we recommend that you migrate to a distributed setup with dedicated forwarders for data collection and indexers for data storage.

Indicators for Scaling

Consider the following criteria before upgrading the system.

- **CPU and Memory Utilization:** Consistently high CPU (above 75%) and memory usage (above 80%) during peak times.
- **Disk Latency and IOPS:** If disk latency increases and IOPS approach the provisioned limit, especially during data ingestion or searches.
- **Search Performance:** Increasing search times, especially for complex or wide-ranging queries, could indicate the need for additional search heads.
- **Data Latency:** If there's a noticeable delay between data ingestion and its availability for search (data latency), indexing may be falling behind.

Recommended Distributed Architecture

We recommend the following specifications for a distributed architecture.

- **Search Head (SH):**
 - Instance Type: c5.4xlarge or c5.9xlarge for high search concurrency.
 - Handles search requests, dashboards, and user interactions.
- **Indexer (IDX)**
 - Instance Type: i3.4xlarge or r5d.4xlarge for high IOPS and storage needs.
 - Manages data indexing and storage.
- **Forwarder (HF/UF):**
 - Instance Type: t3.medium for Universal Forwarders (UF) or c5.large for Heavy Forwarders (HF).
 - Collects data from various sources and forwards it to the indexers.

Summary

- **Single instance deployment:** Can handle up to 100 GB/day of data ingestion, 20 active users, and 50-100 inputs.
- **Migrate to distributed deployment:** When data ingestion exceeds 100 GB/day, user load surpasses 20 concurrent users with heavy search activity, or when the number of inputs becomes too large or diverse.



CHAPTER 5

Configure Cisco Products in Cisco Security Cloud App

This chapter explains how to add and configure inputs for various Cisco products within Security Cloud App. Configuring inputs correctly is important because it defines the data sources that Security Cloud App uses for monitoring. Proper configuration ensures comprehensive security coverage and displays all data accurately for future tracking and monitoring.



Important

In a distributed Splunk architecture, it is critical that modular inputs are configured and executed only on the Heavy Forwarder (HF), not on Search Heads or Indexers.

- [Set Up an Application, on page 19](#)
- [Configure an Application, on page 21](#)
- [Cisco Duo, on page 22](#)
- [Cisco Secure Malware Analytics, on page 24](#)
- [Cisco Secure Firewall Management Center, on page 25](#)
- [Cisco Multicloud Defense, on page 30](#)
- [Cisco XDR, on page 31](#)
- [Cisco Secure Email Threat Defense, on page 33](#)
- [Cisco Secure Network Analytics, on page 34](#)
- [Cisco Secure Endpoint, on page 36](#)
- [Cisco Vulnerability Intelligence, on page 37](#)
- [Cisco AI Defense, on page 42](#)
- [Cisco Isovalent Runtime Security, on page 43](#)
- [Cisco Secure Client NVM, on page 45](#)
- [Cisco Identity Intelligence \(CII\), on page 45](#)

Set Up an Application

Application Setup is the first user interface for Security Cloud App. The **Application Setup** page consists of two sections:

Figure 1: My Apps

Application Setup

My Apps

Search...

Input Name	Product	Host	Enabled	Status	Source Type	Index	
duo	Duo	api-first.test.duosecurity.com		Connected	cisco:duo	tag_duo	
sma	Secure Malware Analytics	paracore.threatgrid.com		Connected	cisco:sma-submissions	tag_sma	
firewall_extremes	Secure Firewall	198.50.133.194		Not Connected	cisco:fire-extremes	cisco_fire_ext	
ftd_syslog	Secure Firewall			Not Connected	cisco:ftd-syslog	cisco_ftd_syslog	
asa_syslog	ASA Syslog			Connected	cisco:asa	cisco_asa_syslog	
mult	Multicloud Defense			Connected	cisco:multicloud-defense	cisco_multicloud_defense	
xdr	Cisco XDR			Not Connected	cisco:xdr-incidents	cisco_xdr	

- The **My Apps** section on the **Application Setup** page displays all user input configurations.
- Click a product hyperlink to go to the product dashboard.

Input Name	Product	Host
duo	Duo	api-first.test.duosecurity.com

- To edit inputs, click **Edit Configuration** under the action menu.
- To delete inputs, click **Delete** under the action menu.

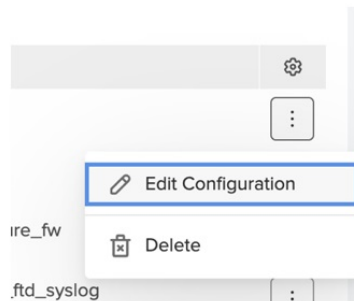


Figure 2: Cisco Products

Application Setup

My Apps

Search...

Input Name	Product	Host	Enabled	Status	Source Type	Index	
duo	Duo	api-first.test.duosecurity.com		Connected	cisco:duo	tag_duo	
sma	Secure Malware Analytics	paracore.threatgrid.com		Connected	cisco:sma-submissions	tag_sma	
firewall_extremes	Secure Firewall	198.50.133.194		Not Connected	cisco:fire-extremes	cisco_fire_ext	
ftd_syslog	Secure Firewall			Not Connected	cisco:ftd-syslog	cisco_ftd_syslog	
asa_syslog	ASA Syslog			Connected	cisco:asa	cisco_asa_syslog	
mult	Multicloud Defense			Connected	cisco:multicloud-defense	cisco_multicloud_defense	
xdr	Cisco XDR			Not Connected	cisco:xdr-incidents	cisco_xdr	

Cisco Products

Search...

Duo
Network Security App

Zero trust is the future of information security - and Duo is your rock-solid foundation. Duo secures your workforce, taking access security beyond the corporate network perimeter to protect your data at every authentication attempt, from any device, anywhere. Confirm user identities in a snap, monitor the health of managed and unmanaged devices, set adaptive security policies tailored for your business, secure remote access without a device agent, and provide secure, user-friendly single sign-on, quickly and easily with Duo.

[Learn More](#) [Configure Application](#)

Secure Malware Analytics
Network Security App

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect organizations from malware. Secure Malware Analytics is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impacting the user environment.

[Learn More](#) [Configure Application](#)

Secure Firewall
Firewall App

The integration of Secure Firewall Threat Defense (formerly Firepower Threat Defense) provides the capability to investigate, identify, and enrich Cisco Secure Firewall intrusion events with context from integrations across the integrated products. It offers an automated triage and prioritization of intrusion events through incidents.

[Learn More](#) [Configure Application](#)

Multicloud Defense
Cloud Security App

Cisco Multicloud Defense protects all of your cloud environments using a single software-as-a-service (SaaS) control plane, eliminating inefficient, complex, and costly point solutions.

[Learn More](#) [Configure Application](#)

XDR
Threat Detection and Response

Cisco XDR changes the way security teams look at detection and response. Our cloud-based solution is designed to simplify security operations and empower security teams to detect, prioritize, and respond to the most sophisticated threats. Integrating with the broader Cisco security portfolio and select third-party offerings, Cisco XDR is one of the most comprehensive and flexible solutions on the market today.

[Learn More](#) [Configure Application](#)

Secure Network Analytics
Network Analytics

Analyze your existing network data to help detect threats that may have found a way to bypass your existing controls, before they can do serious damage.

[Learn More](#) [Configure Application](#)

The **Cisco Products** page displays all available Cisco products that are integrated with Security Cloud App. You can configure inputs for each Cisco product in this section.

Configure an Application

Some configuration fields are common across all Cisco products and they are described in this section. Configuration fields that are specific to a product are described in the later sections.

Table 1: Common fields

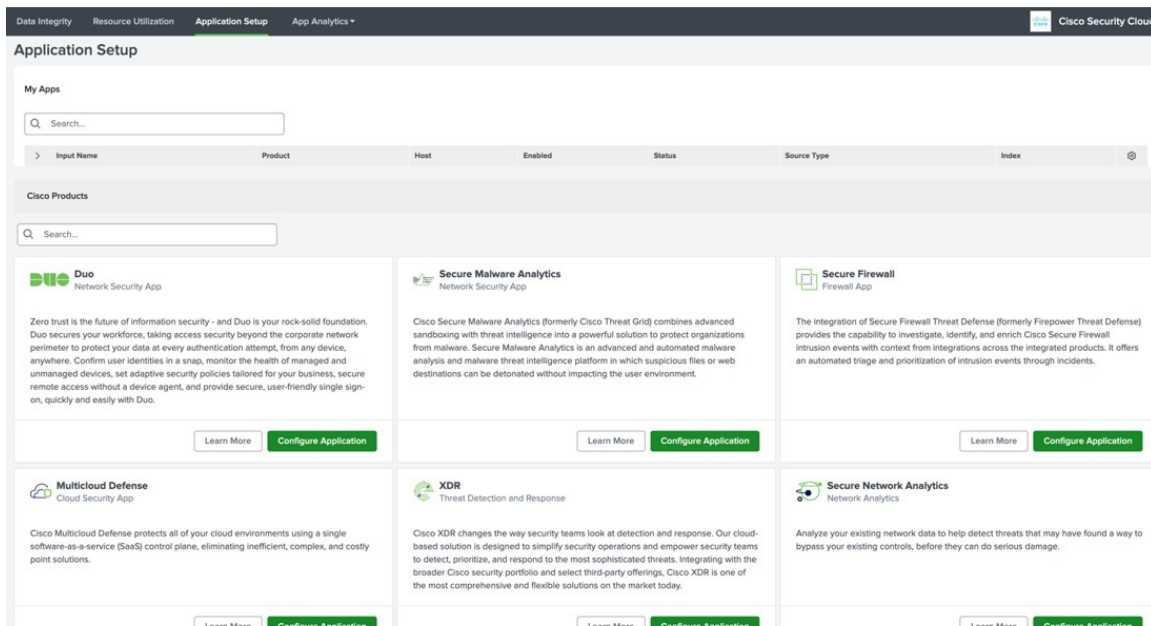
Field	Description
Input Name	(Mandatory) A unique name for inputs of the application.
Interval	(Mandatory) Time interval in seconds between API queries.
Index	(Mandatory) Destination index for application logs. It can be changed if required. Auto-complete is provided for this field.
Source Type	(Mandatory) For most apps it is a default value and is disabled. You can change its value in Advance Settings .

Procedure

Step 1 In the **Application Setup > Cisco Products** page, navigate to the required Cisco application.

Step 2 Click **Configure Application**.

The configuration page consists of three sections: Brief app description, Documentation with links to useful resources, and Configuration form.



Step 3 Fill in the configuration form. Note the following:

- Required fields are marked with asterisk *.
- There are also optional fields.
- Follow the instructions and tips described in the specific app section of the page.

Step 4 Click **Save**.

If there is an error or empty fields, the **Save** button is disabled. Correct the error and save the form.

Cisco Duo

Figure 3: Duo Configuration page

In addition of the mandatory fields described in the [Configure an Application, on page 21](#) section, the following credentials are required for authorization with Duo API:

- **ikey (Integration key)**
- **skey (Secret key)**

Authorization is handled by the Duo SDK for Python.

Table 2: Duo configuration fields

Field	Description
API Hostname	(Mandatory) All API methods use the API hostname. https://api-XXXXXXXXX.duosecurity.com . Obtain this value from the Duo Admin Panel and use it exactly as shown there.
Duo Security Logs	Optional.
Proxy Settings	Optional.
Logging Level	(Optional) Logging level for messages written to input logs in \$SPLUNK_HOME/var/log/splunk/duo_splunkapp/

Procedure

Step 1 In the Duo configuration page, enter the **Input Name**.

Step 2 Enter the Admin API credentials in the **Integration key**, **Secret key**, and the **API hostname** fields. If you do not have these credentials, [register a new account](#).

- Navigate to **Applications > Protect an Application > Admin API** to create new Admin

Dashboard > Applications > Admin API

Admin API

Setup instructions are in the [Admin API documentation](#) C7.

The Admin API allows you to programmatically create, retrieve, update, and delete users, phones, hardware tokens, admins, applications, and more.

Details

Integration key: 2IP0NABX90E032Y5C32 [Copy](#)

Secret key: *****uJcT [Copy](#)

Don't write down your secret key or share it with anyone.

API hostname: api-776c794.duosecurity.com [Copy](#)

Step 3 Define the following, if required:

- Duo Security Logs
- Proxy Settings
- Logging Level

Step 4 Click **Save**.

Cisco Secure Malware Analytics

Figure 4: Secure Malware Analytics Configuration page

Secure Malware Analytics
Network Security App

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect organizations from malware. Secure Malware Analytics is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impacting the user environment.

When integrated, Secure Malware Analytics is a reference module that provides licensed users the ability to pivot into the Secure Malware Analytics Cloud portal to gather additional intelligence about file hashes, IPs, domains, and URLs. It also provides a number of dashboard tiles for quick insight into current Secure Malware Analytics sample submission data.

Documentation

- [Free Trial](#)
- [Product Overview](#)
- [FAQ](#)
- [Support](#)
- [Privacy Policy](#)
- [Sign Up](#)

Add Secure Malware Analytics

SMA Connection

*Host Name
Enter a unique name

*Host
Enter the host for this account

*API Key
Enter the API key for this account

Proxy Settings

Logging Settings

Input Configuration

*Interval
300
Time interval in seconds between API queries

Source Type
CiscoTmccommissions

*Index
log_api
Specify the destination index for SMA Security logs

*After
10 minutes ago
The index after which and when querying the Threat Grid API. Should be 10 minutes ago

Cancel Save



Note You need an API key (**api_key**) for authorization with **Secure Malware Analytics (SMA)** API. Pass the API key as the Bearer type in the Authorization token of the request.

Secure Malware Analytics configuration data

- **Host:** (Mandatory) Specifies the name of the SMA account.
- **Proxy Settings:** (Optional) Consists of Proxy Type, Proxy URL, Port, Username, and Password.
- **Logging Settings:** (Optional) Define the settings for logging information.

Procedure

- Step 1** In the Secure Malware Analytics configuration page, enter a name in the **Input Name**.
- Step 2** Enter the **Host** and the **API Key** fields.
- Step 3** Define the following, if required:
- Proxy Settings
 - Logging Settings
- Step 4** Click **Save**.

Cisco Secure Firewall Management Center

Figure 5: Secure Firewall Management Center Configuration page


You can import data into the Secure Firewall application using any one of the two streamlined processes: **eStreamer** and **Syslog**.

The Secure Firewall configuration page provides two tabs, each corresponding to a different data import method. You can switch between these tabs to configure the respective data inputs.

Firewall e-Streamer

[eStreamer SDK](#) is used for communication with Secure Firewall Management Center.

Figure 6: Secure Firewall E-Streamer tab


Add Secure Firewall

E-Streamer
Syslog

Firewall Connection

*Input Name

Enter a unique name

*FMC Host

Enter the FMC Host for this account

*Port

Enter the Port for this account

*PKCS Certificate ⓘ

Drop your file here or [upload file...](#)
Supported types: pkcs12.

*Password

Enter the password for the PKCS certificate

*Event Types

Connection
File Events
Intrusion
Intrusion Packet

Source Type ⓘ

*Index

Specify the destination index for Firewall Security Logs

*Interval

Time Interval in seconds between API queries

Cancel
Save

Table 3: Secure Firewall configuration data

Field	Description
FMC Host	(Mandatory) Specifies the name of the management center host.
Port	(Mandatory) Specifies the port for the account.

Field	Description
PKCS Certificate	<p>(Mandatory) Certificate must be created on the Firewall Management Console - eStreamer Certificate Creation. The system supports only <code>pkcs12</code> file type.</p> <p>Note For Splunk instances with FIPS mode enabled, the PBE algorithms, that protect the <code>pkcs12</code> file must be FIPS compliant.</p> <p>To reassign certificates with the PBE algorithm, execute the following commands:</p> <pre>OpenSSL> pkcs12 -in ftdv_C_.p12 -out ftdv_C_.pem OpenSSL> pkcs12 -in ftdv_C_.p12 -out ftdv_C_.pem</pre> <p>See Troubleshoot PKCS#12 File Installation Failure with Non-FIPS Compliant PBE Algorithms for more information.</p>
Password	(Mandatory) Password for the PKCS Certificate.
Event Types	(Mandatory) Choose the type of events to ingest (All, Connection, Intrusion, File, Intrusion Packet).

Procedure

-
- Step 1** In the **E-Streamer** tab of the **Add Secure Firewall** page, in the **Input Name** field, enter a name.
- Step 2** In the **PKCS Certificate** space, upload a `.pkcs12` file to set up the PKCS certificate.
- Step 3** In the **Password** field, enter the password.
- Step 4** Choose an event under **Event Types**.
- Step 5** Define the following, If required:
- Duo Security Logs
 - Logging Level

Note

If you switch between the **E-Streamer** and **Syslog** tabs, only the active configuration tab is saved. Therefore, you can only set one data import method at a time.

- Step 6** Click **Save**.
-

Firewall Syslog and ASA

In addition to the mandatory fields that are described in the [Configure an Application, on page 21](#) section, the following are the configurations that are required on the management center side.

Table 4: Configuration fields to add a Syslog

Field	Description
TCP/UDP	(Mandatory) Specifies the type of input data.
Port	(Mandatory) Specifies a unique port for the account.

Procedure

Step 1 In the **Syslog** tab of the **Add Secure Firewall** page, set up the connection on the management center side, in the **Input Name** field, enter a name.

Figure 7: Configure Syslog

The screenshot shows the 'Add Secure Firewall' configuration page with the 'Syslog' tab selected. The form contains the following fields and options:

- Input Name:** A text field with the placeholder 'Enter a unique name'.
- Input Type:** Radio buttons for 'UDP' and 'TCP'.
- Port:** A text field with the value '514' and the placeholder 'Enter the Port for this account'.
- Source Type:** A dropdown menu with 'Select...' as the current selection.
- Index:** A text field with the value 'cisco_xfw_fld_syslog' and the placeholder 'Specify the destination index for Firewall Security Logs'.
- Interval:** A text field with the value '600' and the placeholder 'Time interval in seconds between API queries'.

At the bottom of the form, there are 'Cancel' and 'Save' buttons.

Step 2 Choose TCP or UDP for the **InputType**.

Step 3 In the **Port** field, enter the port number.

Step 4 Select a type from the **SourceType** drop-down list.

Step 5 Choose event types for the selected source type.

Note

If you switch between the **E-Streamer** and **Syslog** tabs, only the active configuration tab is saved. Therefore, you can only set one data import method at a time.

Step 6 Click **Save**.

Firewall API

Along with the required fields described in the Configure an Application, the [Secure Firewall Threat Defense REST API](#) is used.

Complete configuration procedure with the following steps:

Procedure

Step 1 In the **Secure Firewall API** tab of the **Add Secure Firewall** page, enter a unique name in the **Input Name** field.

Figure 8: Secure Firewall API

The screenshot shows the 'Add Secure Firewall' configuration page with the 'Secure Firewall API' tab selected. The page includes the following fields and options:

- Firewall Connection** (Section Header)
- *Input Name**: A text input field with a placeholder 'Enter a unique name'.
- *FMC Host**: A text input field with a placeholder 'Enter the FMC Host for this account'.
- *Username**: A text input field with a placeholder 'Enter the Username for this account'.
- *Password**: A text input field with a placeholder 'Enter the Password for this account'.
- Source Type**: A dropdown menu with a help icon, currently set to 'cisco:sfwrpolicy'.
- *Index**: A text input field with a placeholder 'Specify the destination index for Secure Firewall API', currently set to 'cisco_sfwr_api'.
- *Interval**: A text input field with a placeholder 'Time interval in seconds between API queries', currently set to '300'.
- Buttons**: 'Cancel' and 'Save' buttons at the bottom.

Step 2 In the **FMC Host** field enter the FMC host for the account.

Step 3 In the **Username** and **Password** fields, enter the username and password for the account.

Step 4 Click **Save**.

If you switch between the tabs on the **Add Secure Firewall** page, only the active configuration tab is saved. Therefore, you can only set one data import method at a time.

Step 5 Click **Save**.

Cisco Multicloud Defense

Figure 9: Secure Malware Analytics Configuration page

Multicloud Defense

Set Up Guide

1. Go to **Data Inputs Console** in Splunk Settings
Settings -> Data Inputs -> HTTP Event Collector
2. Copy the Token Value for the collector with the name you specified during the input creation.
3. On the Multicloud Defense instance go to **Log Forwarding tab**
Manage -> Profiles -> Log Forwarding
4. Create a Log Forwarding Profile:
 - a. Click Create
 - b. Enter unique name for the profile
 - c. Choose **"Standalone"** from the Type dropdown.
 - d. Choose **"Splunk"** from the Destination dropdown.
5. Enter the link to the Http Event Collectors with port on your Splunk instance
e.g. `https://<your_splunk_host>:<hec_port>/services/collector`
6. Enter the token you copied in Data Inputs Console in the Token field.
7. Enter the index you specified in the created input in the Index field.

Documentation

[About Multicloud Defense](#)

Go to Cisco Defense Orchestrator and follow the steps in the Set Up Guide to the left to install Multicloud Defense instance.

[Go to CDO](#)

Add Cisco Multicloud Defense

Multicloud Defense Connection

*Input Name
Enter a unique name

*Interval
300
Time interval in seconds between API queries

Source Type
cisco-multicloud-defense

*Index
cisco_multicloud_defense
Specify the destination index for MCD Security Logs

Port
8088
Enter the Port for this account

[Cancel](#) [Save](#)

Multicloud Defense (MCD) leverages the HTTP Event Collector functionality of Splunk instead of communicating through an API.

Create an instance in Cisco Defense Orchestrator (CDO), by following the steps that are defined in the **Set Up Guide** section of the **Multicloud Defense** configuration page.

Set Up Guide

1. Go to **Data Inputs Console** in Splunk Settings
Settings -> Data Inputs -> HTTP Event Collector
2. Copy the Token Value for the collector with the name you specified during the input creation.
3. On the Multicloud Defense instance go to **Log Forwarding tab**
Manage -> Profiles -> Log Forwarding
4. Create a Log Forwarding Profile:
 - a. Click Create
 - b. Enter unique name for the profile
 - c. Choose **"Standalone"** from the Type dropdown.
 - d. Choose **"Splunk"** from the Destination dropdown.
5. Enter the link to the Http Event Collectors with port on your Splunk instance
e.g. `https://<your_splunk_host>:<hec_port>/services/collector`
6. Enter the token you copied in Data Inputs Console in the Token field.
7. Enter the index you specified in the created input in the Index field.

Only the mandatory fields defined in the [Configure an Application, on page 21](#) section are required for authorization with Multicloud Defense.

Procedure

- Step 1** Install a Multicloud Defense instance in CDO by following the **Set Up Guide** on the configuration page.
- Step 2** Enter a name in the **Input Name** field.
- Step 3** Click **Save**.

Cisco XDR

Figure 10: XDR Configuration page

Cisco XDR

XDR
Threat Detection and Response

Cisco XDR changes the way security teams look at detection and response. Our cloud-based solution is designed to simplify security operations and empower security teams to detect, prioritize, and respond to the most sophisticated threats. Integrating with the broader Cisco security portfolio and select third-party offerings, Cisco XDR is one of the most comprehensive and flexible solutions on the market today.

Designed by security practitioners for security practitioners, Cisco XDR helps analysts aggregate and correlate data from multiple sources into a unified view to streamline investigations, reduce false positives, prioritize alerts, and achieve the shortest path from detection to response. Built-in automation, orchestration, and guided remediation recommendations help analysts automate repetitive tasks and mitigate threats more effectively, freeing up time and resources to focus on other critical security tasks.

The data-driven Cisco XDR approach allows SOC teams to define the most impactful events and focus remediation strategies there first, strengthening the organization's overall security posture and increasing resilience.

Documentation

[About XDR](#)

[Data Sheet](#)

[Privacy Policy](#)

[Get started](#)

Add XDR

XDR Connection

*Input Name
Enter a unique name

*Region
Select...
Enter the Region for this account

*Authentication Method ⓘ
Select...

*Import Time Range ⓘ
Select...

Promote XDR Incidents to ES Notables? ⓘ
All Critical Medium Low Info Unknown None

*Interval
300
Time interval in seconds between API queries

Source Type ⓘ
cisco_xdr_incidents

*Index
cisco_xdr
Specify the destination index for XDR Security Logs

Cancel Save

The following credentials are required for authorization with Private Intel API:

- **client_id**
- **client_secret**

Every input run results in a call to GET /iroh/oauth2/token endpoint to obtain a token that is valid for 600 seconds.

Table 5: Cisco XDR configuration data

Field	Description
Region	(Mandatory) Select a region before selecting an Authentication Method.
Authentication Method	(Mandatory) Two authentication methods are available: Using Client ID and OAuth.

Field	Description
Import Time Range	(Mandatory) Three import options are available: Import All Incident data, Import from created date-time, and Import from defined date-time.
Promote XDR Incidents to ES Notables?	<p>(Optional) Splunk Enterprise Security (ES) promotes Notables.</p> <p>If you have not enabled Enterprise Security, you can still choose to promote to notables, but events do not appear in that index or notable macros.</p> <p>After you enable Enterprise Security, events are present in the index.</p> <p>You can choose the type of incidents to ingest (All, Critical, Medium, Low, Info, Unknown, None).</p>

Procedure

-
- Step 1** In the Cisco XDR configuration page, enter a name in the **Input Name** field.
- Step 2** Select a method from the **Authentication Method** drop-down list.
- Client ID:
 - a. Click the **Go to XDR** button to create a client for your account in XDR.
 - b. Copy and paste the Client ID
 - c. Set a password (Client_secret)
 - OAuth:
 - a. Follow the generated link and authenticate. You need to have an XDR account.
 - b. If the first link with the code didn't work, in the second link, copy the User code and paste it manually.
- Step 3** Define an import time in the **Import Time Range** field.
- Step 4** If required, select a value in the **Promote XDR Incidents to ES Notables?** field.
- Step 5** Click **Save**.
-

Cisco Secure Email Threat Defense

Figure 11: Secure Email Threat Defense Configuration page

Cisco Secure Email Threat Defense

Cisco Secure Email Threat Defense (formerly Secure Email Cloud Mailbox) provides the most comprehensive protection against damaging and costly threats that compromise your organization's brand and operations.

AI-driven threat detection uses multiple detection engines to simultaneously evaluate different portions of an incoming email. These verdict details help ensure accurate threat classification, identify business risk, and promote an appropriate response action.

Using rapid message remediation directly in Email Threat Defense or through Cisco XDR empowers your team to act quickly and easily to help ensure maximum threat protection.

Identify the malicious techniques used in attacks targeting your organization. Understand the specific business risks and categorize threats to gain insight into the parts of your organization that are most vulnerable to attack.

Documentation

[At-A-Glance](#)

[Q+A](#)

[Data Sheet](#)

Add Cisco Secure Email Threat Defense

ETD Connection

*Input Name
Enter a unique name

*API Key
Enter the API Key for this account

*Client ID
Enter the Client ID for this account

*Secret Key
Enter the Secret Key for this account

*Region
Select...
Enter the Region for this account

*Import Time Range ⓘ
Select...

Input Configuration

*Interval
300
Time interval in seconds between API queries

Source Type ⓘ
cisco_etd

*Index
cisco_etd
Specify the destination index for ETD Security Logs

Cancel Save

The following credentials required for authorization of Secure Email Threat Defense APIs:

- api_key
- client_id
- client_secret

Table 6: Secure Email Threat Defense configuration data

Field	Description
Region	(Mandatory) You can edit this field to change the region.
Import Time Range	(Mandatory) Three options are available: Import All message data, Import from created date-time, Import from defined date-time.

Procedure

- Step 1** In the Secure Email Threat Defense configuration page, enter a name in the **Input Name** field.
- Step 2** Enter the **API Key**, **Client ID**, **Client Secret Key**.

- Step 3** Select a region from the **Region** drop-down list.
- Step 4** Set an import time under **Import Time Range**.
- Step 5** Click **Save**.

Cisco Secure Network Analytics

Secure Network Analytics (SNA), formerly known as **Stealthwatch**, analyzes the existing network data to help identify threats that may have found a way to bypass the existing controls.

Figure 12: Secure Network Analytics Configuration page

Secure Network Analytics
Network Analytics

Analyze your existing network data to help detect threats that may have found a way to bypass your existing controls, before they can do serious damage.

Detect attacks in real time across the dynamic network with high-fidelity alerts enriched with context, including user, device, location, timestamp, and application.

Validate the efficacy of policies, adopt the right ones based on your environment's needs, and streamline policy violation investigations.

Use advanced analytics to quickly detect unknown malware, insider threats like data exfiltration and policy violations, and other sophisticated attacks.

Identify and isolate threats in encrypted traffic without compromising privacy and data integrity.

Documentation

- [Free Trial](#)
- [FAQ](#)
- [Support](#)
- [Sign Up](#)

Add Secure Network Analytics

SNA Connection

*Input Name
Enter a unique name

*SMC Address (IP Address or Hostname)

*SMC Domain ID

*SMC Username

*SMC Password

> Proxy Settings

> Logging Settings

Input Configuration

*Interval
300
Time interval in seconds between API queries

Source Type [?](#)
cisco:sna

*Index
cisco_sna
Specify the destination index for SNA Security Logs

Cancel Save

Credentials required for authorization:

- `smc_host`: (IP address or hostname of the Stealthwatch Management Console)
- `tenant_id` (Stealthwatch Management Console domain ID for this account)
- `username` (Stealthwatch Management Console username)
- `password` (Stealthwatch Management Console password for this account)

Table 7: Secure Network Analytics configuration data

Field	Description
Proxy type	choose a value from the drop-down list: <ul style="list-style-type: none"> • Host • Port • Username • Password
Interval	(Mandatory) Time interval in seconds between API queries. By default, 300 secs.
Source type	(Mandatory)
Index	(Mandatory) Specifies the destination index for SNA Security Logs. By default, state: <i>cisco_sna</i> .
After	(Mandatory) The initial after value used when querying the Stealthwatch API. By default, the value is <i>10 minutes ago</i> .
Logging Settings	(Optional)
Promote SNA Alarms to ES Notables?	<p>(Optional)</p> <p>After ES is enabled, events are available in the index. You can choose the incident level that must be ingested (All, Critical, Major, Minor, Trivial, or Info)</p> <p>Note Splunk Enterprise Security is required to promote Notables. In case you do not have it, you can still enable this option, but events will not appear in the index or by notable macros.</p>

Procedure

-
- Step 1** In the Secure Network Analytics configuration page, enter a name in the **Input Name** field.
- Step 2** Enter **Manager Address (IP or Host)**, **Domain ID**, **Username**, and **Password**.
- Step 3** If required, set the following under **Proxy settings**:
- Choose a proxy from the **Proxy type** drop-down list.
 - Enter the host, port, username, and password in the respective fields.
- Step 4** Define the Input configurations:
- Set a time under **Interval**. By default, the interval is set to 300 seconds (5 minutes).

- You can change the **Source type** under **Advanced Settings**, if required. Default value is *cisco:sna*.
- Enter the destination index for the Security logs in the **Index** field.

Step 5 Click **Save**.

Cisco Secure Endpoint

Cisco Secure Endpoint (SE) is a single-agent solution that provides comprehensive protection, detection, response, and user access coverage to defend against threats to your endpoints.

Configure the following in the **Add Cisco Secure Endpoint** page:

Add Cisco Secure Endpoint

Secure Endpoint Connection

* Input Name
Enter a unique name

* Host
Enter the Host for this account

* API Key
Enter the API Key for this account

* Client ID
Enter client ID for this account

* Import Time Range ⓘ
Select...

* Event Types
Select...

Input Configuration

* Interval
300
Time interval in seconds between API queries

* Source Type ⓘ
cisco:se

* Index
cisco_se
Specify the destination index for SE Security Logs

Before you begin

Credentials are required for authorization:

- **api_host:** host for SE

- **api_key:** API key (password) for the account SE
- **client_id:** client id (username) for the account SE

Procedure

Step 1 Enter the values for all the fields as described in the following table:

Field	Description
Input Name	(Mandatory) Unique name for the input
Import Time Range	(Mandatory) Choose a date to import data
Event type	(Mandatory) You can select more than one event types.
Interval	(Mandatory) Time interval between API queries. By default, the interval is 300 secs. Range is 1 to 900.
Source Type	By default, the source type is cisco:se . This field is disabled by default. To enable and change the source type, go to Advance Settings .
Index	Specifies the destination index for SE Security Logs. By default, the value is cisco:se .
Groups	This field is displayed only you enter the correct credentials (api_host , api_key , and client_id)

After you enter the input name, host id, API key, and client ID, the **Groups** field is enabled.

- Step 2** In the **Groups** drop-down list, select the required groups. You can select more than one group.
- Step 3** From the **Import Time Range** drop-down list, choose a timeline to import the data.
- Step 4** From the **Event Types** drop-down list, choose one or more events.
- Step 5** In the **Interval** field, set the interval between API queries.
- Step 6** To submit the form, click **Save**.

Cisco Vulnerability Intelligence

Cisco Vulnerability Intelligence (CVI) gives access to a collection of vulnerability information that includes Common Vulnerabilities and Exposures (CVE) data, through an API. You can access CVI through the Cisco Vulnerability Management platform.

Here is a description of the mandatory configuration input fields in the **Add Cisco Vulnerability Intelligence** page.

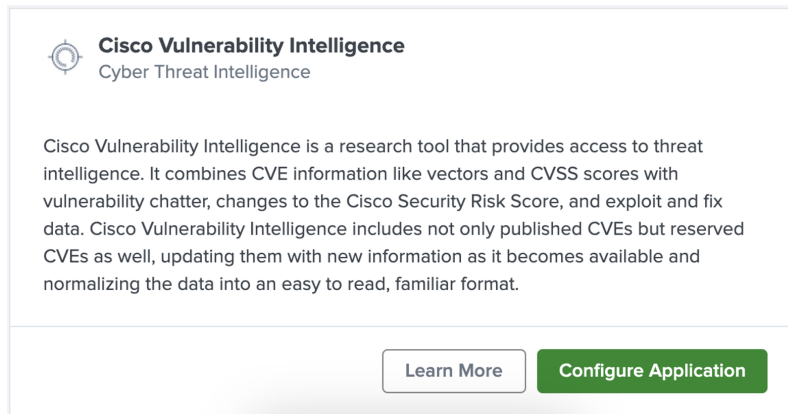


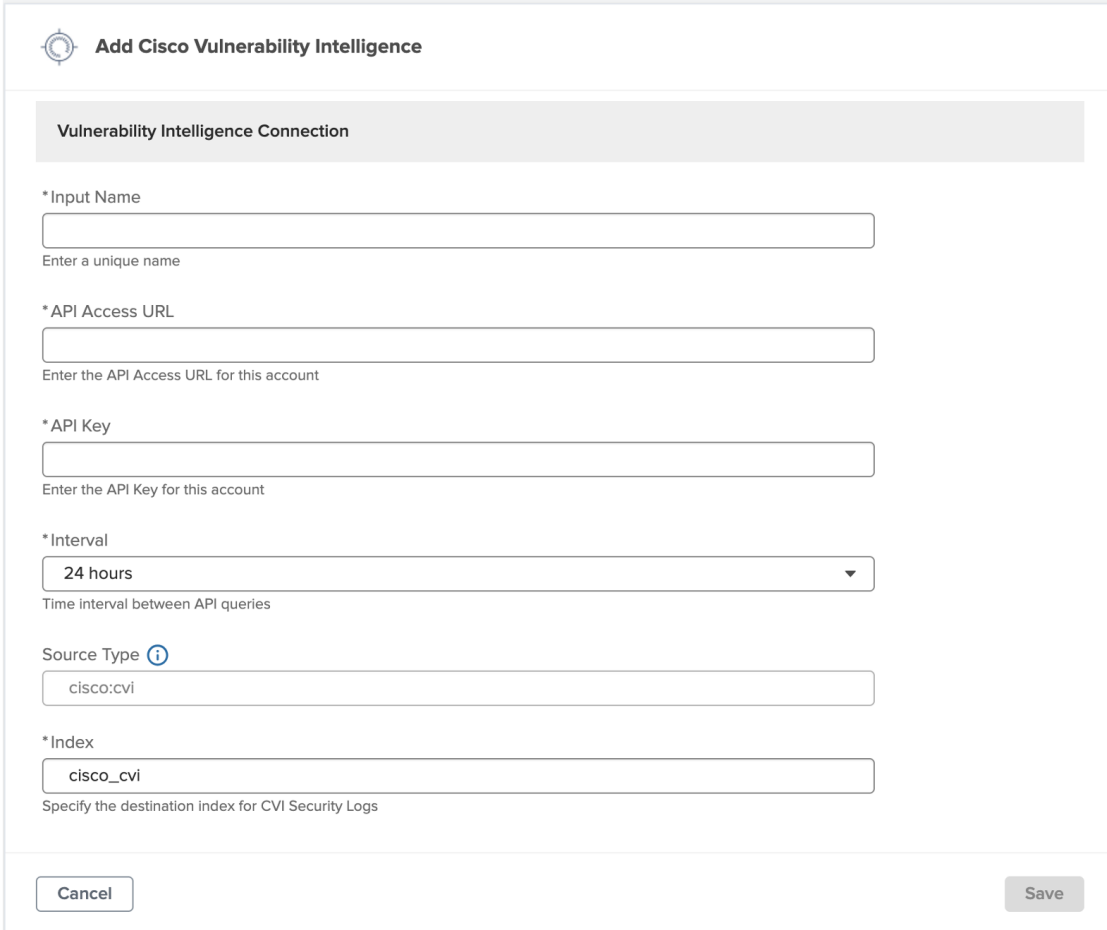
Table 8: CVI configuration data

Field	Description
Input Name	A name for this connection.
API Access URL	The endpoint for your instance of CVM. This URL can be found on the Settings > API Keys > API Key Access & Generation page in CVM. Enter only the domain name and include a front slash at the end. For example, api.kennasecurity.com/
API Key	The API Key generated from the Settings > API Keys page in CVM.
Interval	Time interval between the API queries. By default, it is 24 hours.
The fields Source Type and Index have a default value, which you can retain.	

Use the following procedure to configure Cisco Vulnerability Intelligence.

Procedure

- Step 1** In the **Application Setup** page of Security Cloud App, go to the **Cisco Products** section and search for **Cisco Vulnerability Intelligence**.
- Step 2** In the Cisco Vulnerability Intelligence card, click **Configure Application**.
- Step 3** In the **Add Cisco Vulnerability Intelligence** page, enter the specific connection details based on your CVM settings.

Figure 13: Configure CVI

The screenshot shows a web form titled "Add Cisco Vulnerability Intelligence". It contains several input fields and a dropdown menu. The fields are labeled with asterisks to indicate they are required. The "Source Type" field has an information icon (i) next to it. The "Index" field has a description below it. At the bottom, there are "Cancel" and "Save" buttons.

Add Cisco Vulnerability Intelligence

Vulnerability Intelligence Connection

*Input Name

Enter a unique name

*API Access URL

Enter the API Access URL for this account

*API Key

Enter the API Key for this account

*Interval
24 hours
Time interval between API queries

Source Type ⓘ

*Index

Specify the destination index for CVI Security Logs

Cancel Save

Step 4 Click **Save**.

This establishes a connection to CVM. CVI data is loaded into the `cisco_cvi` index of your Splunk instance.

Search and Reporting Tool

The `cisco_cvi` index stores all vulnerability data by default. You can reference the `cisco_cvi` index through the Search and Reporting tool of Splunk. In the tool, you can generate reports and filter data based on the different fields.

CIM Mapping to Vulnerability Model

Along with vulnerability data in the `cisco_cvi` index, many fields are mapped to the CIM Vulnerability model. You can reference this mapping manually or in other tools that reference the Vulnerability model.

Splunk CIM Model	Splunk Field Name	Splunk Data Type	CVM VI + Data snapshot Field Name
Cisco Security.CVM VI Dataset	exploits	Array of structured types	exploits
Cisco Security.CVM VI Dataset	fixes	Array of structured types	fixes
Cisco Security.CVM VI Dataset	threat_actors	Array of structured types	threat_actors
Cisco Security.CVM VI Dataset	created_at	time	created_at
Cisco Security.CVM VI Dataset	daily_trend	string	daily_trend
Cisco Security.CVM VI Dataset	predicted_exploitable	boolean	predicted_exploitable
Cisco Security.CVM VI Dataset	predicted_exploitable_confidence	float	predicted_exploitable_confidence
Cisco Security.CVM VI Dataset	successful_exploitations	number	successful_exploitations
Cisco Security.CVM VI Dataset	velocity_day	number	velocity_day
Cisco Security.CVM VI Dataset	velocity_month	number	velocity_month
Cisco Security.CVM VI Dataset	velocity_week	number	velocity_week
Cisco Security.CVM VI Dataset	cve_id	string	cve_id
Cisco Security.CVM VI Dataset	cvss_score	float	cvss_score
Cisco Security.CVM VI Dataset	cvss_exploit_subscore	float	cvss_exploit_subscore
Cisco Security.CVM VI Dataset	cvss_impact_subscore	float	cvss_impact_subscore
Cisco Security.CVM VI Dataset	cvss_vector	float	cvss_vector
Cisco Security.CVM VI Dataset	cvss_temporal_score	float	cvss_temporal_score
Cisco Security.CVM VI Dataset	cvss_v3_score	float	cvss_v3_score
Cisco Security.CVM VI Dataset	cvss_v3_exploit_subscore	float	cvss_v3_exploit_subscore
Cisco Security.CVM VI Dataset	last_modified_on	_time	last_modified_on
Cisco Security.CVM VI Dataset	published_on	_time	published_on
Cisco Security.CVM VI Dataset	vulnerable_products	string	vulnerable_products
Cisco Security.CVM VI Dataset	vuln_state	string	state

Splunk CIM Model	Splunk Field Name	Splunk Data Type	CVM VI + Data snapshot Field Name
Cisco Security.CVM VI Dataset	id	number	id
Cisco Security.CVM VI Dataset	cve_description	string	cve_description
Cisco Security.CVM VI Dataset	cvss_access_complexity	string	cvss_access_complexity
Cisco Security.CVM VI Dataset	cvss_access_vector	string	cvss_access_vector
Cisco Security.CVM VI Dataset	cvss_authentication	string	cvss_authentication
Cisco Security.CVM VI Dataset	description	string	description
Cisco Security.CVM VI Dataset	cisco_security_risk_score	float	risk_meter_score
Cisco Security.CVM VI Dataset	cvss_availability_impact	string	cvss_availability_impact
Cisco Security.CVM VI Dataset	cvss_confidentiality_impact	string	cvss_confidentiality_impact
Cisco Security.CVM VI Dataset	cvss_integrity_impact	string	cvss_integrity_impact
Cisco Security.CVM VI Dataset	easily_exploitable	boolean	easily_exploitable
Cisco Security.CVM VI Dataset	malware_exploitable	boolean	malware_exploitable
Cisco Security.CVM VI Dataset	active_internet_breach	boolean	active_internet_breach
Cisco Security.CVM VI Dataset	malware_count	number	malware_count
Cisco Security.CVM VI Dataset	chatter_count	boolean	chatter_count
Cisco Security.CVM VI Dataset	popular_target	boolean	popular_target
Cisco Security.CVM VI Dataset	remote_code_execution	boolean	remote_code_execution
Cisco Security.CVM VI Dataset	pre_nvd_chatter	boolean	pre_nvd_chatter
Cisco Security.CVM VI Dataset	stride_threat	Array of strings	stride_threat
Cisco Security.CVM VI Dataset	vulnerability_type	Array of strings	vulnerability_type
Cisco Security.CVM VI Dataset	exploitation_methodology	Array of strings	exploitation_methodology
Cisco Security.CVM VI Dataset	affected_source_file_module	Array of strings	affected_source_file_module
Cisco Security.CVM VI Dataset	mitre_techniques	Array of strings	mitre_techniques

Cisco AI Defense

Figure 14: AI Defense Configuration on Security Cloud Control app for Splunk

Cisco AI Defense

Cisco AI Defense
AI Security

AI Defense safeguards production applications from attacks and undesired responses in real time with guardrails that can be automatically configured to the specific vulnerabilities of each model identified with our AI Validation offering. Using AI Defense your organization will be able to block malicious inputs by inspecting every input and automatically blocking malicious payloads such as prompt injection, prompt extraction, and PII detection. Ensure safe outputs by scanning model outputs to ensure they are absent of sensitive information, hallucinations, and otherwise harmful content. Get started with one of hundreds of out-of-the-box protections which can be custom fit to each model and further tailored to your organizations standards.

Deploy AI applications with the confidence of unmatched visibility and enforcement, model and application agnostic security, and lightning fast protection for your critical applications.

Documentation

[About Cisco AI Defense](#)

Add Cisco AI Defense

AI Defense Connection

*Input Name
Enter a unique name

*Interval
Time interval in seconds between API queries
300

Source Type ⓘ
cisco:ai:defense

*Index
cisco_ai_defense
Specify the destination index for AI Defense Security Logs

Port
8088
Enter the Port for this account

Cancel Save

Follow these steps to complete the configuration on the Splunk Cisco Security Cloud app.

Before you begin

In order to forward AI Defense events to Splunk, you must have the following in place:

- [An index in Splunk](#) to store data sent by AI Defense
- [HTTP Event Collector enabled](#) in Splunk
- [An Event Collector token](#) in Splunk for AI Defense

Follow these steps to connect AI Defense to Splunk:

1. From your Splunk instance, gather the following values:
 - **Splunk Collector URL**, including the HTTP Port Number: The URL used to access the Splunk HTTP Event Collector (HEC).
This URL has the format, `https://<splunk-server>:<hec_port>/services/collector`. For example, `https://mysplunkserver.example.com:8088/services/collector`.
 - **HTTP Event Collector Token**: The Splunk Token to allow AI Defense to communicate with Splunk.
 - **Index Name**: The name of the Splunk index that you will use for storing AI Defense events.
2. In AI Defense, open the **Administration: Integrations** tab and find the card for **Splunk**.
3. Click the **Connect** button and enter the Splunk HEC details (Splunk Collector URL, HTTP Event Collector Token, and Index Name).
4. Once you fill in the details, click the **Connect** button and the Splunk card status will show as connected.

Only the mandatory fields defined in the [Configure an Application](#) section are required for authorization with AI Defense.

Procedure

- Step 1** Open the **Application Setup** tab and find the card for **AI Defense**.
- Step 2** Click **Configure Application**.
- Step 3** In the **Cisco AI Defense** panel, set up the **AI Defense Connection**. Most fields here are preconfigured and can be left as-is.
- In the **Input Name** field, specify the name to be used in this connection to refer to the AI Defense data input.
 - Optionally, you can edit the **Index name** where the events will be stored in Splunk.
- Step 4** Click **Save**.
- The connection appears in the **My Apps** list of the **Application Setup** panel.
-

What to do next

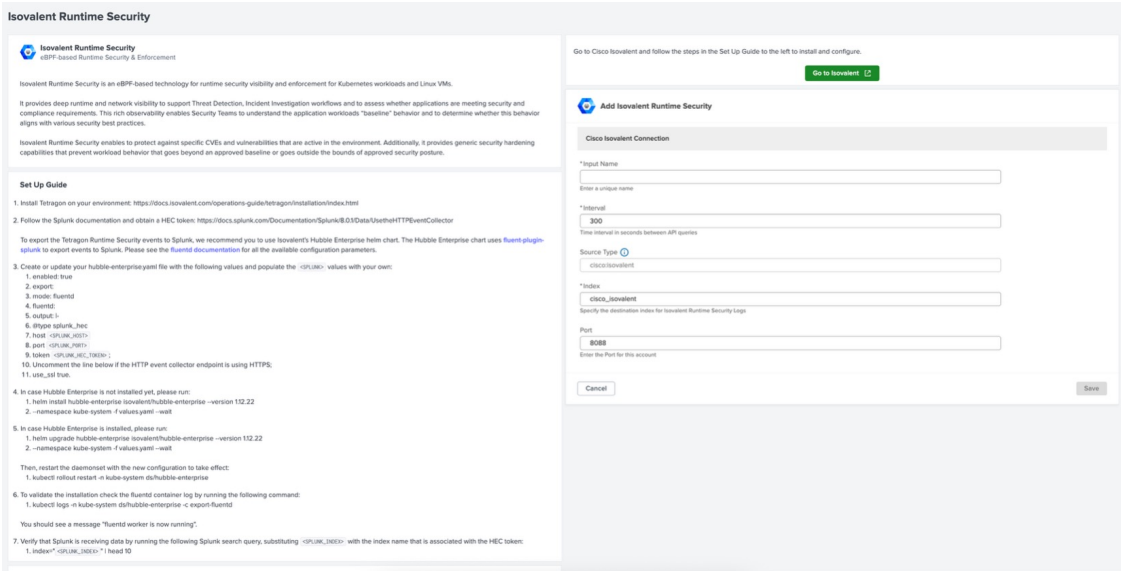
Once you have added the AI Defense connection:

- The **Data Integrity** tab shows the health of the connection.
- The **Resource Utilization** tab shows the system resources being consumed by AI Defense.
- The **Cisco AI Defense Dashboard** is available in Splunk.

Cisco Isovalent Runtime Security

Cisco Isovalent Runtime Security configuration page looks like this:

Figure 15: Cisco Isovalent Runtime Security Configuration



Procedure

- Step 1** Set up a connection on Isovalent using Setup guide in the configuration page.
- Step 2** Enter a name in the **Input name** field.
- Step 3** Click **Save**.

Cisco Secure Client NVM

Figure 16: Cisco Secure Client NVM Configuration

Cisco Secure Client NVM
Secure Client Network Visibility Module

The Network Visibility Module (NVM) of Cisco Secure Client collects rich flow context from an endpoint on or off premise and provides visibility into network connected devices and user behaviors when coupled with a Cisco solution such as Splunk.

The Network Visibility Module collects the endpoint telemetry for better visibility into the following:

- The device — the endpoint, irrespective of its location
- The user — the one logged into the endpoint
- The application — what generates the traffic
- The location — the network location the traffic was generated on
- The destination — the actual FQDN to which the traffic was intended

Set Up Guide

1. Complete the configuration mentioned in the "Secure Client NVM Collector HEC Connection" panel in this page.
2. Navigate to **Settings > Data Inputs > HTTP Event Collector** and gather the following details:
 - a. Select the HEC input configured during the setup process and copy the corresponding HEC token.
 - b. Click on **Global Settings** to retrieve the `HEC_PORT`.
 - c. Ensure that the token is enabled under the HEC Global Settings.
3. In the collector instance(s), do the following:
 - a. Install Fluent Bit using the following link.
 - b. Download the Fluent Bit and Parser configuration files by clicking on the "Download File" button in this page and place them in the path `/usr/fluent-bit`.
* Ensure the browser does not block the download.
 - c. In the path `/usr/fluent-bit`, create a file named `fluent-bit` with the following contents:


```
HEC_TOKEN=HEC_TOKEN
HEC_PORT=HEC_PORT
SPUNK_HOST=SPUNK_HOST_IPFQDN
COLLECTOR_IPFQDN=COLLECTOR_IPFQDN
COLLECTOR_IPFQDN=COLLECTOR_IPFQDN
TLS_ENABLED=1 # Set to 0 if HEC Global Settings require TLS, otherwise OFF.
TLS_VERIFY=ON/OFF? Set to 0 to enable TLS certificate verification, or OFF to disable it.
CA_PATH=/usr/share/ca-certificates # e.g., /usr/share/ca-certificates.pem
* Make sure that the COLLECTOR_IPFQDN is the same as syslog_server.ip in the /usr/share/ciscoconf/conf file configured in the collector instance.
```
 - d. Once everything is in place, run the following commands:
 - `service fluent-bit stop`
 - `service fluent-bit start`

Documentation

[About NVM](#)

Use the button below to download the most recent Fluent Bit and Parser configuration files for the NVM Collector instance.

[Download File](#)

Add Cisco Secure Client NVM

Secure Client NVM Collector HEC Connection

*Input Name
Enter a unique name

*Interval
300
Time interval in seconds between API queries

Source Type
ciscoconn

*Default Index
main

Cancel Save

The **Cisco Secure Client NVM** integrates with Splunk through its **HTTP Event Collector (HEC)**, not via a direct API connection.

Before you begin

Download the Fluent Bit configuration file from the configuration page using the provided **Download** button.

Procedure

Step 1 Create an NVM Collector instance by following the steps that are defined in the **Set Up Guide** section of the **Cisco Secure Client NVM** configuration page.

Note

While following the setup, note the critical configuration parameters—such as the **Token**, **Port**, and **Host IP**—as these values are required when updating the Fluent Bit configuration for NVM.

Step 2 Enter a name in the **Input Name** field.

Step 3 Click **Save**.

Cisco Identity Intelligence (CII)

There are two primary methods to forward data from Cisco Identity Intelligence to Splunk. Choose the method that best fits your operational needs and infrastructure.

1. [Method 1: Webhooks \(Recommended for Real-Time Events\)](#)

2. [Method 2: AWS S3 Bucket \(Recommended for Batch Data\)](#)

Test the connectivity between Splunk and Cisco Identity Intelligence with the following steps:

Before you begin

Ensure that you meet the following prerequisites before starting the integration.

- Administrative access to **Cisco Identity Intelligence**
- Administrative access to **Splunk Enterprise** or **Splunk Cloud**
- **Cisco Security Cloud** app installed from Splunkbase
- **Splunk Add-on for AWS** installed from Splunkbase
- Appropriate permissions to configure a Splunk HTTP Event Collector (HEC) or manage AWS S3 buckets and Splunk data inputs

Procedure

Step 1 In Splunk

Verify test application in Splunk

- a) Navigate to Splunk and ensure the test application (test_splunk_demo) is listed in the **My Apps** table.
- b) Go to **App Analytics** and select the **Cisco Identity Intelligence Dashboard** from the list of available dashboards.

[Data Integrity](#) [Resource Utilization](#) [Alerts & Detection](#) [Application Setup](#) [App](#)

Application Setup


My Apps

Q Search...

>	Input Name	Product
>	test_splunk_demo	Cisco Ide

Cisco Products

Q Search...

 **Duo**
Network Security App

Zero trust is the future of information security - and Duo is your rock-solid foundation. Duo secures your workforce, taking access security beyond the corporate network perimeter to protect your data at every authentication attempt, from any device, anywhere. Confirm user identities in a snap, monitor the health of managed and unmanaged devices, set adaptive security policies tailored for your business, secure remote access without a device agent, and provide secure, user-friendly single sign-on, quickly and easily with Duo.

[Learn More](#) [Configure Application](#)

[Secure Malware](#)
[Duo Dashboard](#)
[Cisco Multicloud](#)
[Secure Firewall](#)
[XDR Dashboard](#)
[Cisco Secure Em](#)
[Dashboard](#)
[Secure Network](#)
[Cisco Secure En](#)
[ASA Dashboard](#)
[Cisco Identity Int](#)
[Cisco Vulnerabili](#)
[Cisco AI Defense](#)

- c) Check the dashboard data. Filter the data by index if you used a unique index during the setup process.

Note

If this is your first time using the dashboard, it is expected that no data will be displayed.

Cisco Identity Intelligence ▾

Overview

Time Range

Last 24 hours ▾

Index

All

(1) ▾

Severity ⚠

All ▾

Users with most amount of failed checks

Events logging

Step 2 In Cisco Identity Intelligence (CII)

- a) Navigate to **Cisco Identity Intelligence** and navigate to the **Integrations** section.
- b) Under **Notifications Targets** table locate the integration entry:
 1. If you are using **Webhook**, search for the input named test_splunk_demo
 2. If you are using **AWS S3**, search for the input name s3-splunk-cii-demo-set-up (or s3-<name of your AWS bucket>)
- c) Click on the three dots (menu icon) next to the integration entry.
- d) Select **Test Connectivity** from the menu options.

A popup appears indicating the status **Success**

What to do next

1. Navigate to the **Cisco Identity Intelligence Dashboard** in Splunk.
2. Confirm that the test event triggered during connectivity testing is visible in the dashboard.



CHAPTER 6

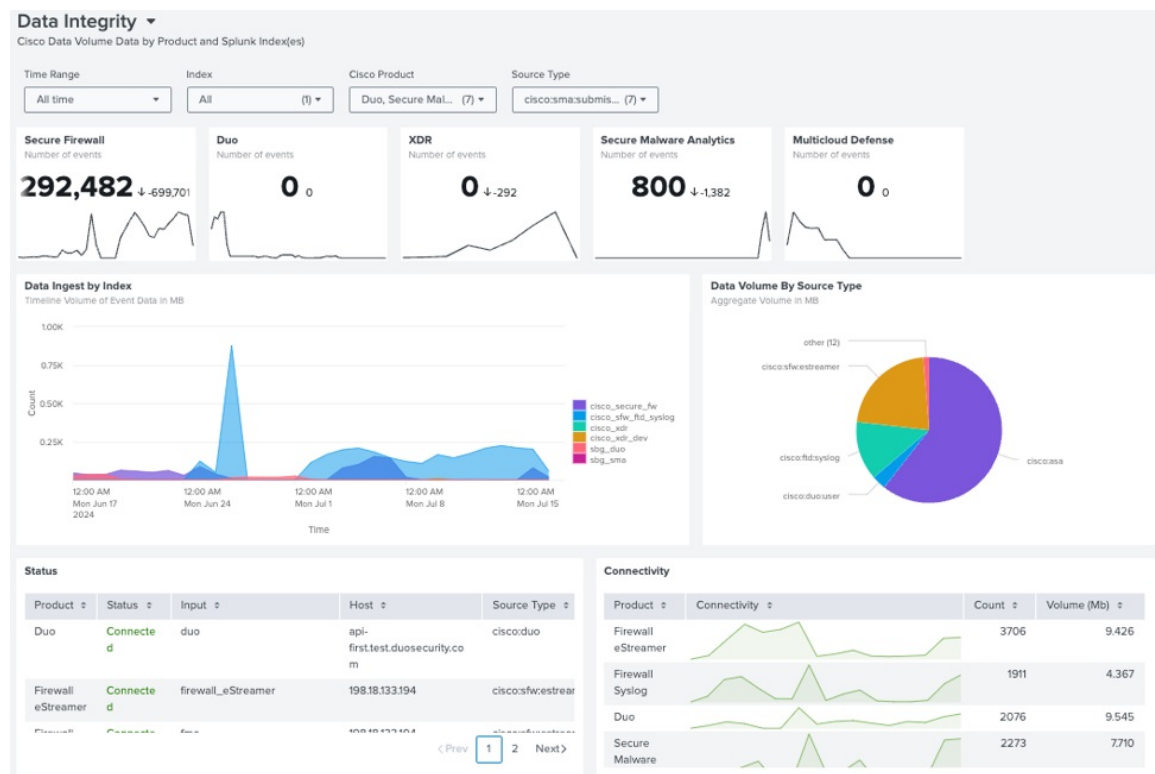
Monitor Dashboards

- [Data Integrity Dashboard, on page 53](#)
- [Resource Utilization Dashboard, on page 54](#)

Data Integrity Dashboard

The Data Integrity dashboard serves as a centralized hub for monitoring the health and flow of data from the inputs that you have created. The dashboard provides you with a comprehensive view of the statistics and status of each application's data, ensuring that you have the insights that are needed to maintain the integrity and reliability of your security environment.

Figure 17: Data Integrity Dashboard



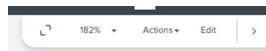
Data Integrity Dashboard Specifics

- You can filter data using the **Time Range**, **Index**, **Cisco Product**, or **Source Type** filters:
 1. **Time Range**: defines the time for which you would like to see data. Works with all tiles on the dashboard.
 2. **Index**: indexes that you've used while creating inputs on the Configuration Application pages. The filter works only with the Event count cards located at the top of the page. It shows "0" on all other cards.
 3. **Cisco Product**: allows to filter data by Product Name. Works with all tiles on the dashboard, except Event count cards.
 4. **Source Type**: source types that were used while creating inputs on the Configuration Application pages. Works with all tiles on the dashboard, except Event count cards.
- The **Data Integrity** dashboard is XML-based.

To edit the dashboard, click the **Edit** button.



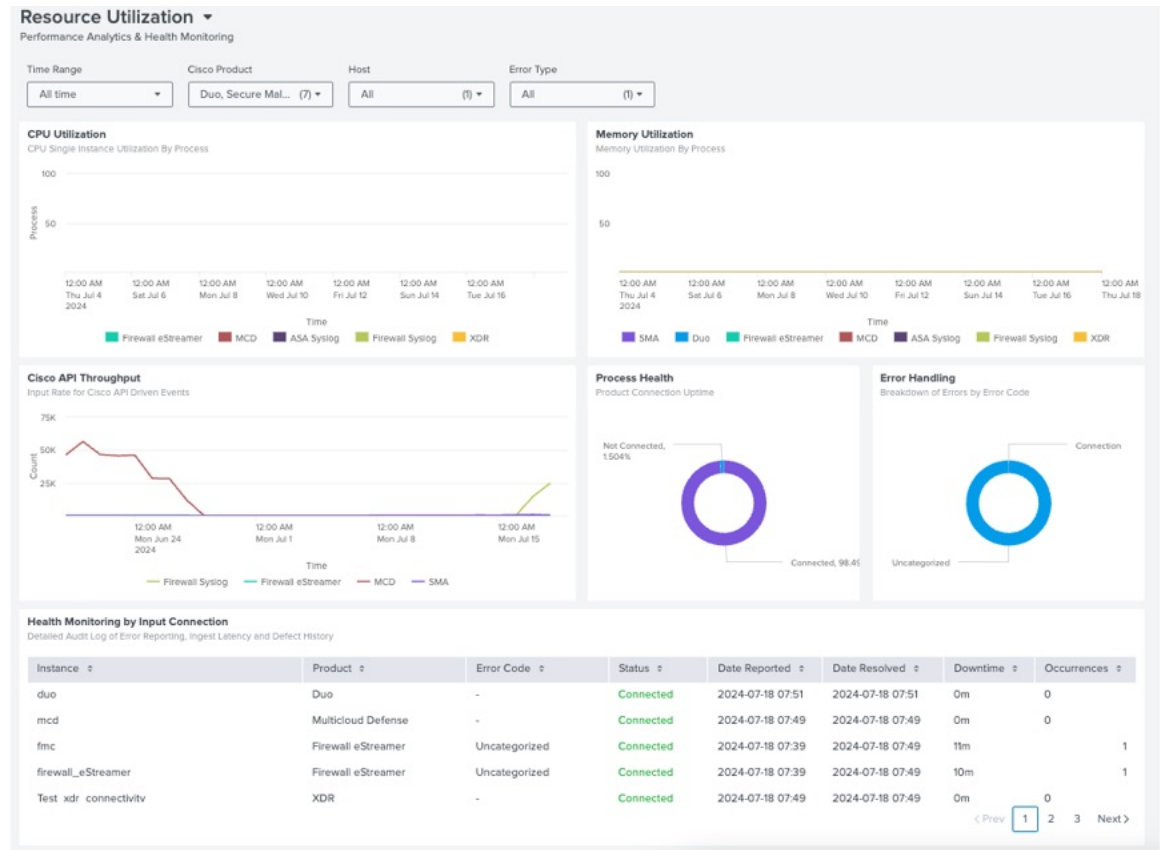
Note This action will only affect the existing user.



Resource Utilization Dashboard

The **Resource Utilization** dashboard is a vital component of Security Cloud App. It provides a detailed account of the performance and monitors the health of the inputs that you have created. **Resource Utilization** dashboard is instrumental in ensuring that your security infrastructure is running optimally and that resources are being used effectively.

Figure 18: Resource Utilization Dashboard



Resource Utilization dashboard Specifics

- You can filter data using the **Time Range**, **Index**, **Cisco Product**, or **Source Type** filters:
 - Time Range:** defines the time for which you would like to see data.
 - Cisco Product:** allows to filter data by Product Name.
 - Host:** allows to filter data by Host.
 - Error type:** allows to filter data by the type of error.
- The **Resource Utilization** dashboard is XML-based.

To edit the dashboard, click the **Edit** button.



Note This action will only affect the existing user.





CHAPTER 7

API Compatibility Matrix

- [APIs Compatibility Matrix](#), on page 58

APIs Compatibility Matrix

Application	Service Version	Data Type	API	API Version
Duo	-	Account Log	Method/Endpoint: GET /admin/v1/info/summary	v1
		Activity Log	Method/Endpoint: GET /admin/v2/logs/activity	v2
		Administrator Log	Method/Endpoint: GET /admin/v1/logs/administrator	v1
		Authentication Log	Method/Endpoint: GET /admin/v2/logs/authentication	v2
		Authentication Log (Legacy v1)]	Method/Endpoint: GET /admin/v1/logs/authentication	v1
		Endpoint Log	Method/Endpoint: GET /admin/v1/endpoints	v1
		Telephony Log	Method/Endpoint: GET /admin/v2/logs/telephony	v2
		Telephony Log (Legacy v1)	Method/Endpoint: GET /admin/v1/logs/telephony	v1
		Trust Monitor	Method/Endpoint: GET /admin/v1/trust_monitor/events	v1
		Users list	Method/Endpoint: GET /admin/v1/users	v1
Secure Firewall (eStreamer)	7.4.1	-	eStreamer SDK	7.4.0
Secure Firewall (Syslog)	7.4.1	-	TCP/UDP inputs used	No API
Secure Firewall (ASA)	-	-	TCP/UDP inputs used	No API

Application	Service Version	Data Type	API	API Version
Secure Firewall (API)	7.4.1	-	Management Center REST API	7.4.1
SMA	Versions: 3.5.160 - 171	Submissions	Method/Endpoint: GET /api/v2/search/submissions	v2
XDR Incidents	1.0.107	Incidents Summary	Method/Endpoint: GET /api/v2/incidents/summary	No API version
		Incidents	Method/Endpoint: GET /api/v2/incidents	No API version
		User details (whoami)	Method/Endpoint: GET /iroh/profile/whoami	No API version
Cisco Multi-Cloud Defense	24.06	-	HTTP Event Collector is used	No API version
Secure Email Threat Defense	Works with any version of Email Threat Defense	Email Metadata	Method/Endpoint: POST /messages/search	v1 v2
	-	Download links	Method/Endpoint: POST /v1/logs/downloadLinks	

Application	Service Version	Data Type	API	API Version
Secure Network Analytics	7.5.1	Authentication	Method/Endpoint: POST /token/v2/authenticate	v2
		Traffic queries	Method/Endpoint: POST /swg/tan/v1/queries	v1
		Traffic queries search results	Method/Endpoint: GET /swg/tan/v1/queries	v1
		Traffic results	Method/Endpoint: GET /swg/tan/v1/results	v1
		Filtered traffic	Method/Endpoint: GET /swg/tan/v1/filtered	v1
		Alarm Report	Method/Endpoint: POST /api/v1/alerts	v1
		Network Performance Report	Method/Endpoint: POST /api/v1/performance	v1
		Flow Collection Trend by FC	Method/Endpoint: POST /api/v1/flowcollectionbyfc	v1
		SAL Collection Trend	Method/Endpoint: POST /api/v1/salcollection	v1
		NVM Collection Trend	Method/Endpoint: POST /api/v1/nvmcollection	v1
		Todays Summary	Method/Endpoint: POST /api/v2/todaysummary	v2
		Top Ports queries	Method/Endpoint: POST /swg/tan/v1/topports	v1
		Top Ports search results	Method/Endpoint: GET /swg/tan/v1/topports	v1

Application	Service Version	Data Type	API	API Version
		Top Ports results	Method/Endpoint: GET /api/v1/top-ports	v1
		Top Hosts queries	Method/Endpoint: POST /api/v1/top-hosts	v1
		Top Hosts search results	Method/Endpoint: GET /api/v1/top-hosts	v1
		Top Hosts results	Method/Endpoint: GET /api/v1/top-hosts	v1
		Top Conversations queries	Method/Endpoint: POST /api/v1/top-conversations	v1
		Top Conversations search results	Method/Endpoint: GET /api/v1/top-conversations	
		Top Conversations results	Method/Endpoint: GET /api/v1/top-conversations	

Application	Service Version	Data Type	API	API Version
Secure Endpoint	5.4.20241024	Fetch list of events	Method/Endpoint: GET /v1/events	v1
		Fetch list of event types	Method/Endpoint: GET /v1/event_types	v1
		Fetch list of groups filtered by name	Method/Endpoint: GET /v1/groups	v1
		Fetch list of compromises	Method/Endpoint: GET /v1/compromises	v1
		Fetch list of vulnerabilities filtered by group guid	Method/Endpoint: GET /v1/vulnerabilities	v1
		Fetch list of computers filtered by group guid	Method/Endpoint: GET /v1/computers	v1
		Fetch malware threats metric dashboard details	Method/Endpoint: GET /v1/malware_threats	v1
CII	-	Exchange the client credentials for an access token	OORT Public API Method/Endpoint: POST / .../api	No API version
		Register webhook	OORT Public API Method/Endpoint: mutation / registerWebhookWithApiKey	No API version
		Delete webhook	OORT Public API Method/Endpoint: mutation / unregisterWebhook	No API version
CVI	-	GZIP File with list of vulnerabilities	Method/Endpoint: GET /v1/defense_dashboard	v1
AI Defense	-	-	HTTP Event Collector is used	No API version



CHAPTER 8

Troubleshoot Issues in Cisco Security Cloud App

If you encounter issues with the Cisco Security Cloud App, follow these steps to identify and address the problem:

1. **Check logs** – Review system and app-specific logs for error patterns related to configuration, API connectivity, data ingestion, or access control.
2. **Apply fixes** – Use the guidance in this section to resolve any identified issues.
3. **Seek further assistance** – Gather diagnostic details and contact Cisco TAC for additional support.
 - [Collect and Analyze Logs, on page 63](#)
 - [App Stability and Post-Upgrade Issues, on page 64](#)
 - [Failed to Create or Edit an Input, on page 64](#)
 - [Delayed Event Updates, on page 65](#)
 - [Failed to Fetch Input Data for Applications, on page 65](#)
 - [Syslog or ASA Input Deletion Issues, on page 65](#)
 - [Cisco Security Cloud App UI loads infinitely , on page 65](#)
 - [KV Store process issues, on page 66](#)
 - [Troubleshoot Splunk HEC Connectivity, on page 67](#)
 - [Troubleshoot SSL Validation Errors, on page 68](#)
 - [Contact Cisco Support, on page 69](#)

Collect and Analyze Logs

Analyzing logs is essential for identifying root causes and resolving issues quickly. When troubleshooting, check for the following indicators:

- Review system and app-specific logs for error messages related to configuration, API connectivity, data ingestion, or access control. Check the logs for entries marked with `ERROR`, `WARN`, or `FATAL`.
- Input-specific issues such as *“Failed to fetch inputs,” “Invalid credentials,”* or *“Timeout”*.
- Timestamp bookmarks where data ingestion pauses or stops.

The following log files are particularly useful during diagnostics:

- **Main Splunk Log**

Contains general system errors, including indexing issues, ingestion failures, and Splunk service restarts.

```
$SPLUNK_HOME/var/log/splunk/splunkd.log
```

- **Cisco App-Specific Log**

Tracks input creation, connectivity to Cisco APIs, and error responses from connectors.

```
$SPLUNK_HOME/var/log/splunk/CiscoSecurityCloud/CiscoSecurityCloud.log
```

- **Performance Metrics Log**

Provides metrics on data throughput, CPU usage, memory, and indexing delays.

```
$SPLUNK_HOME/var/log/splunk/metrics.log
```

App Stability and Post-Upgrade Issues

If you encounter instability, crashes, or no visible changes after an upgrade, use the following steps to resolve the issue:

- Check the health indicator at the top right side of your navigation tab.
- **Avoid multiple sessions:** Do not run the app in multiple Splunk browser sessions simultaneously.
- **Restart Splunk from CLI:** Restart Splunk using the command line (`$SPLUNK_HOME/bin/splunk restart`) instead of the user interface (UI).
- **Use a fresh session:** Open Splunk in a new incognito window.
- **Clear cache and cookies:** Flush your browser's cache and cookies, then test again in another supported browser (latest versions of Chrome, Firefox, Edge, or Safari).

Failed to Create or Edit an Input

The system displays an error message when it fails to create or edit an SNA, ETD, or XDR input. This failure occurs under the following conditions:

Type	Issue	Workaround
Environment-related issue	The system triggers the error if you open two Splunk windows in parallel and create inputs simultaneously, or if the environment runs slowly.	Use a single Splunk window when creating inputs and avoid simultaneous input creation in multiple sessions.
Configuration error	During input creation, the CII application checks the provided credentials and HEC URL. If either value is invalid, the system fails to create the input.	Verify the credentials and HEC URL, and enter valid data.

Delayed Event Updates

In high-volume environments or on slower systems, performance lag during input creation can cause delayed updates. To address this issue:

- Verify that the input was not created multiple times in parallel from different browser windows.
- Use the **Resource Utilization** dashboard to review input lag and monitor system metrics.

Failed to Fetch Input Data for Applications

If dashboards or indexes show no data after you create an input or perform an upgrade:

- Check if the input is configured correctly.
- Check the status of your input on the Error Handling, Cisco API ThroughPut widgets of the **Resource Utilization** dashboard.
- Verify that the user role has the required permissions. See [User Roles and Permissions in Cisco Security Cloud App](#), on page 9.

For eStreamer inputs, you will not see an immediate status display after creation. The high volume of initial data and the short query interval (3 seconds) prevent the system from capturing ingestion status on the first run.

Syslog or ASA Input Deletion Issues

You cannot delete the Syslog or ASA input with the following details:

- Input Type: TCP, any available port
- Multiple host values separated by commas (for example: "host1, host2, host3")

As a workaround, delete or edit the restricted host for the input in
`/opt/splunk/etc/apps/CiscoSecurityCloud/local/inputs.conf.`

Cisco Security Cloud App UI loads infinitely

When the UI fails to load or becomes unresponsive:

- Use an incognito browser window.
- Clear your browser cache and perform a hard reload.
- Try another supported browser.
- If you're upgrading, always clear the cache after the upgrade.

KV Store process issues

Error message

The KV Store process terminated abnormally (exit code 6, status exited with code 6.)

Possible Cause

This error message is observed only in Single Node configurations with an excessive data volume.

Recommended Action

- Ensure that the Mongo key has the correct permissions or run the following command:

```
chmod 400
$SPLUNKHOME/var/lib/splunk/kvstore/mongo/splunk.key
```

- Consider raising the maximum allowed memory for the KV Store cache.

Add the following configuration to the **server.conf** file in your **\$SPLUNKHOME/etc/system/local** directory:

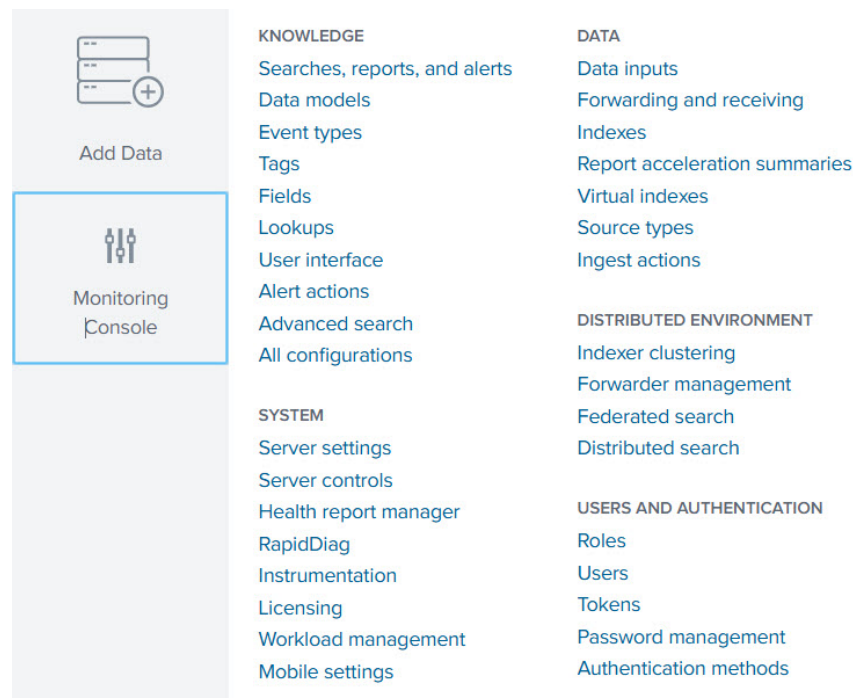
```
[kvstore]
percRAMForCache = 15
```

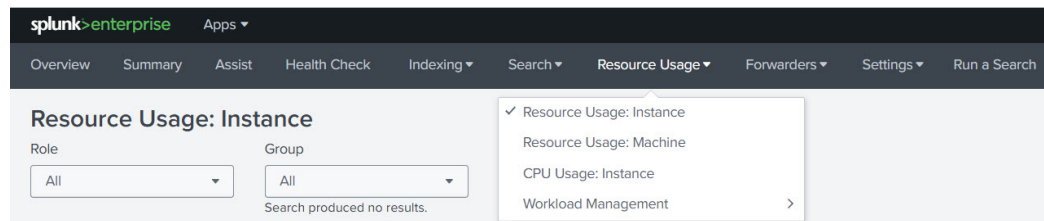


Note 15% is the default value. Increase the percentage based on the current memory consumption of the instance.

You can check your current configuration in the **\$SPLUNKHOME/etc/system/default** in **server.conf** file.

To check the current instance memory consumption, go to **Resource Usage** under **Monitoring Console**.





Troubleshoot Splunk HEC Connectivity

This section describes how to verify the Splunk HTTP Event Collector (HEC) setup and troubleshoot common issues such as connectivity failures or missing data ingestion from Cisco Identity Intelligence (CII).

Prerequisites

Ensure you have `sc_admin` or equivalent permissions in Splunk.

Verify HEC configuration in Splunk

1. Go to **Settings > Data Inputs > HTTP Event Collector**.
2. If HEC is disabled:
 - Select **Global Settings**.
 - Enable **All Tokens**, then click **Save**.
3. Click **New Token**, provide a name (for example, `test_token`), and select **Submit**.
4. Copy the **Token Value** displayed. This will be referred to as `{Token Value}`.

Identify the HEC URL

Identify the correct HEC endpoint based on your Splunk deployment type.

• Splunk Enterprise

```
https://<your-splunk-host>:8088/services/collector/raw
```

• Splunk Cloud Platform

```
https://http-inputs-<splunk-stack>.splunkcloud.com:443/services/collector/raw
```

Replace `<your-splunk-host>` with the Splunk server's IP address or hostname. This will be referred to as `{HEC URL}`.

Send a Test Event

Use `curl` to send a sample event to Splunk and confirm that HEC is receiving data correctly.

1. Open a terminal.
2. Run the following command (replace placeholders with your values):

```
curl -k -H "Authorization: Splunk {Token Value}" \
-d '{"event": "Hello, Splunk HEC Test!"}' {HEC URL}
```

3. Verify the result. A successful response returns:

```
{"text": "Success", "code": 0}
```

4. In Splunk, search for the event to confirm ingestion:

```
index=<your_index> "Hello, Splunk HEC Test!"
```

For more details, see the [Cisco webhook integration documentation](#).

Troubleshoot external system integration

If the Splunk input and the Cisco Identity Intelligence (CII) webhook are both configured successfully, perform the following checks:

1. **Run a connectivity test**

- Verify whether data is being sent from CII to Splunk.

2. **Check IP allowlisting**

- If no data appears in Splunk after the test, confirm that the CII IP address is included in the Splunk allowlist.



Note For testing purposes, you may temporarily add a broad range (for example, 0.0.0.0/0) to confirm connectivity.

This configuration should **never** be used in production, as it introduces security risks.

3. **Apply a secure configuration**

- Obtain the specific CII cloud IP addresses or ranges from Cisco.
- Add only those addresses to the Splunk allowlist to enable secure and reliable data ingestion.

Troubleshoot SSL Validation Errors

If you repeatedly encounter the following error while creating a new input in the Cisco Security Cloud add-on:

```
The provided API credentials cannot get the necessary logs.
Please verify that the API settings are correctly configured
Argument validation for scheme=sbg_fw_estreamer_input: killing process, because executing
it took too long (over 30000 msecs).
[sbg_fw_estreamer_input] stream_events():292 instance=New_Input, error_type=Connection,
error_code=SSLError, error_detail=Unable to process sbg_fw_estreamer_input://New_Input due
to SSLError, traceback=[SSL: TLSV1_ALERT_UNKNOWN_CA] tlsv1 alert unknown ca (_ssl.c:1143),
filter_value=sbg_fw_estreamer_input.py
```

This error indicates that the connection failed due to an SSL certificate trust issue.

TLSV1_ALERT_UNKNOWN_CA means the SSL handshake failed because the Certificate Authority (CA) that issued the FMC certificate is not trusted.

To resolve this issue:

1. Create a PEM file from the existing PKCS file.

```
openssl pkcs12 -in certificate.pkcs12 -info -nodes  
openssl pkcs12 -in 10.x.x.x.pkcs12 -cacerts -nokeys -out ca_certs.pem
```

2. Add the PEM file to the trusted store on the Heavy Forwarder (HF) instance by placing it in:

```
/etc/pki/ca-trust/source/anchors/
```

3. Refresh the CA trust on the HF instance:

```
sudo update-ca-trust
```

4. Restart the Splunk service.

Contact Cisco Support

If your issue remains unresolved after troubleshooting, contact Cisco Support in any of the following ways:

- Cisco TAC (Technical Assistance Center)
- Cisco Community: <https://community.splunk.com>

Ensure you include relevant logs and screenshots when opening a case.

Info to collect before opening a case

- OS and platform (for example, Red Hat 8.10, Splunk Cloud, or Enterprise)
- Deployment type (Single-instance, Distributed, or Clustered)
- Connector or Cisco product that is impacted
- Configuration details used during input creation
- Region or tenant (US, EU, Asia)
- Relevant log files:
 - `splunkd.log`
 - `CiscoSecurityCloud.log`
 - `metrics.log`

See [Collect and Analyze Logs, on page 63](#) for more information.

- Console browser errors (attach screenshots)
- API call details (if applicable)

