

Integrate SNA to Splunk Using Security Cloud Application

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[FAQs](#)

Introduction

This document describes the smooth SNA integration with Splunk using Cisco Security Cloud for faster incident response for the threats identified.

Prerequisites

Basic knowledge of Splunk and Cisco Devices.

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these hardware and software versions:

Splunk Enterprise

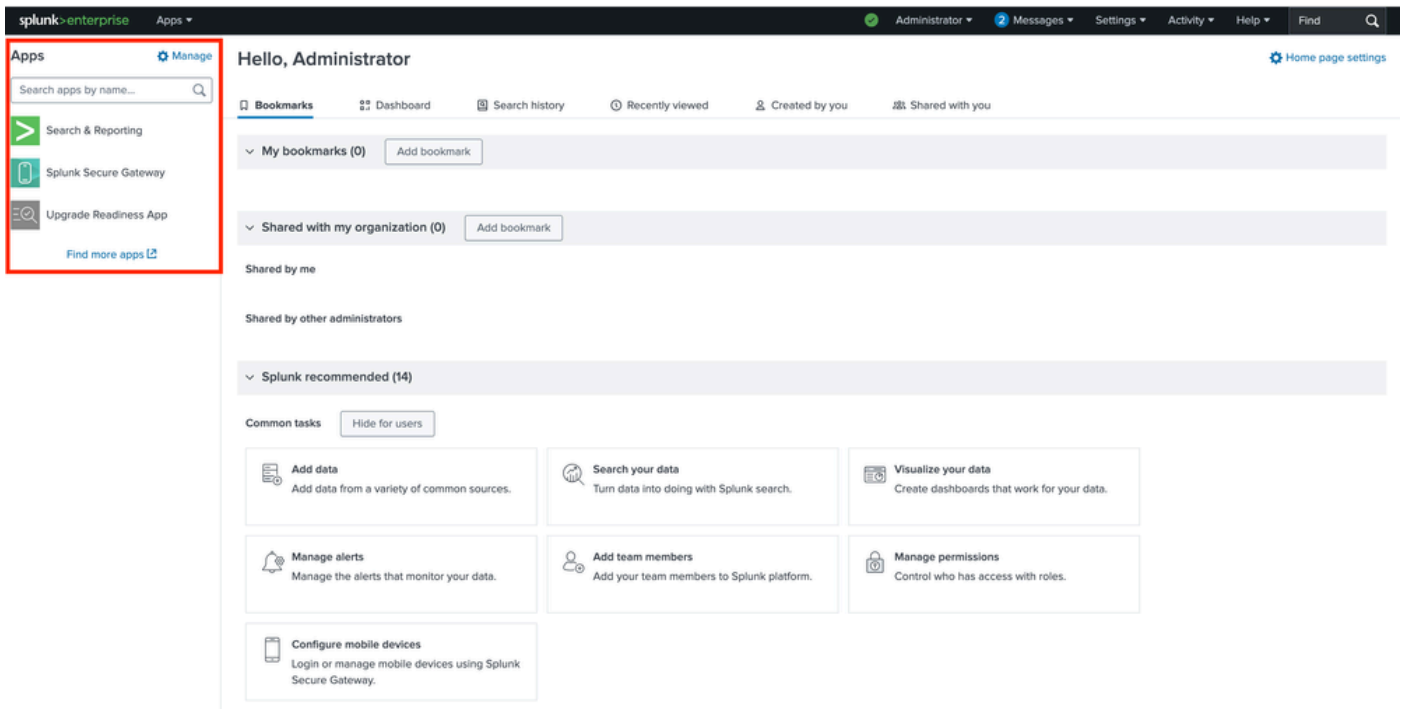
Secure Network Analytics v7.5.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

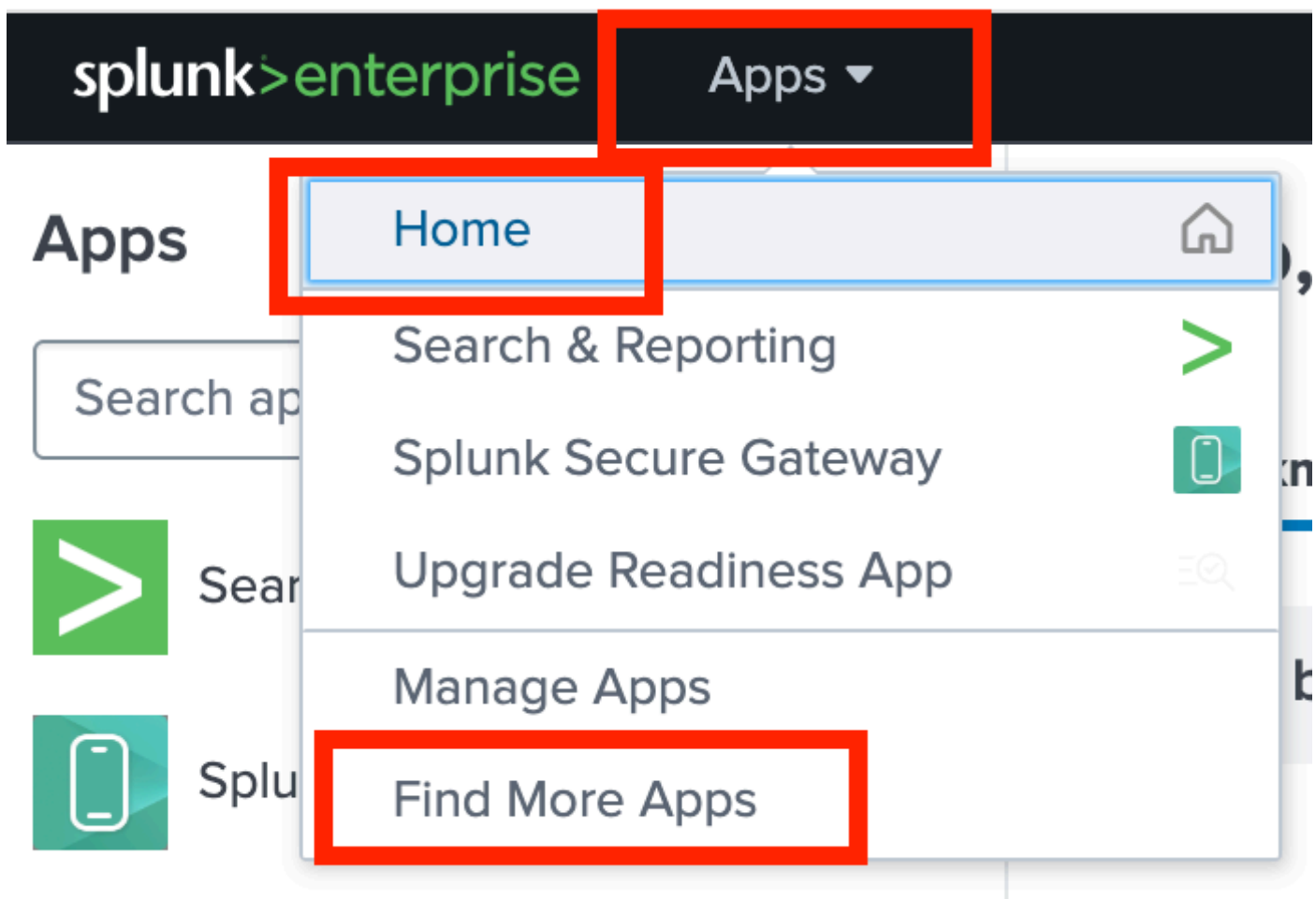
Step1: Access the **Splunk** Application and Install the **Cisco Security Cloud** Application.

i. Log in to the **Splunk web portal** with the admin credentials and on successful log in, the home page can be seen with the list of installed applications on the left side under the App section:

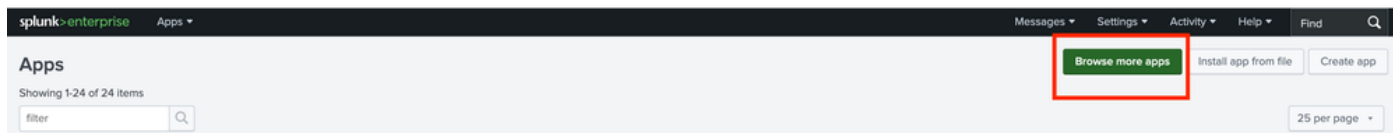


ii. For integrating the SNA with Splunk, it is required to install the Cisco Security Cloud Application which can be achieved in either of the mentioned methods:

1. Select **Find More Apps** from the drop down.

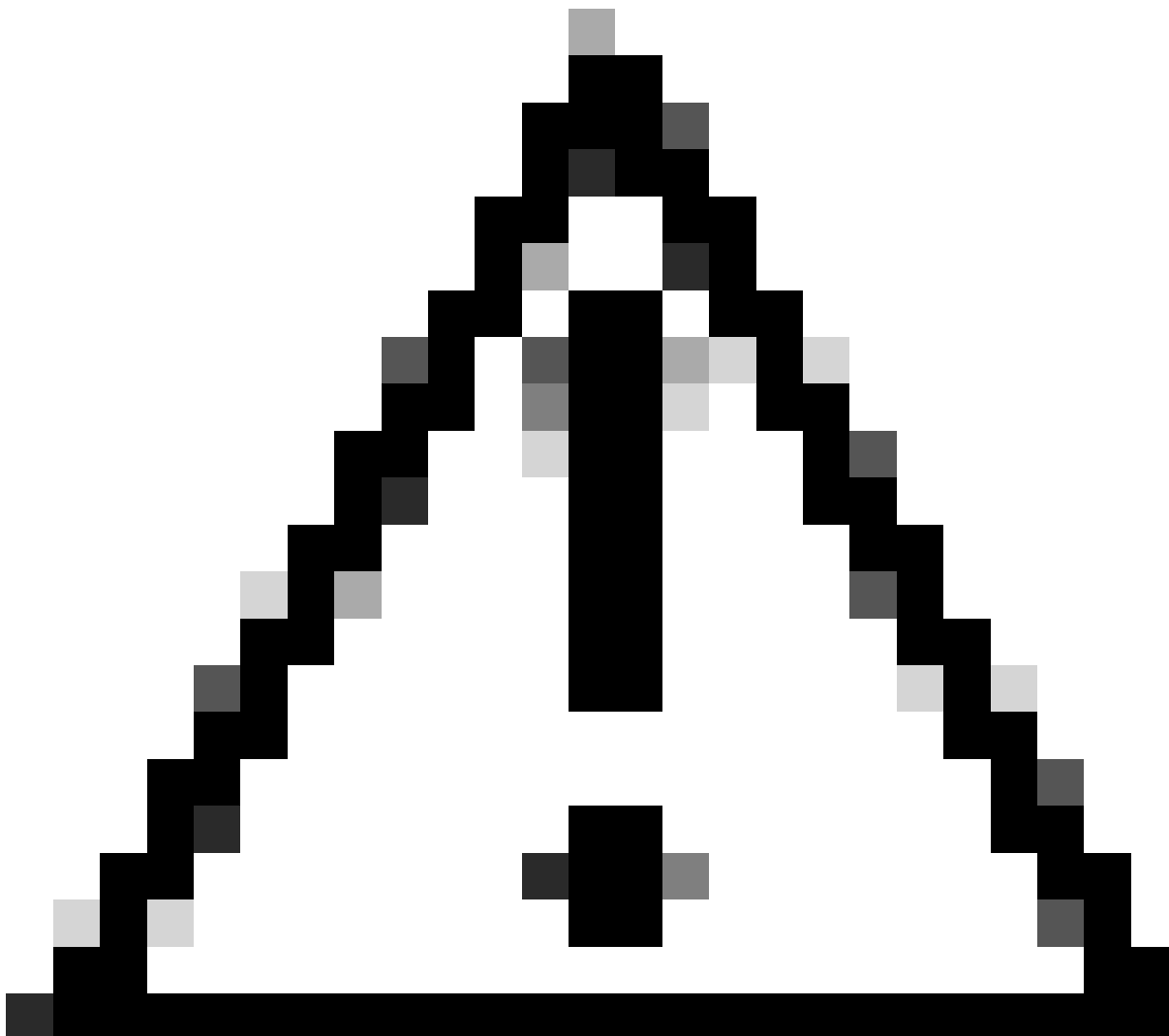


- b. Browse more apps under the **Manager gear icon**.

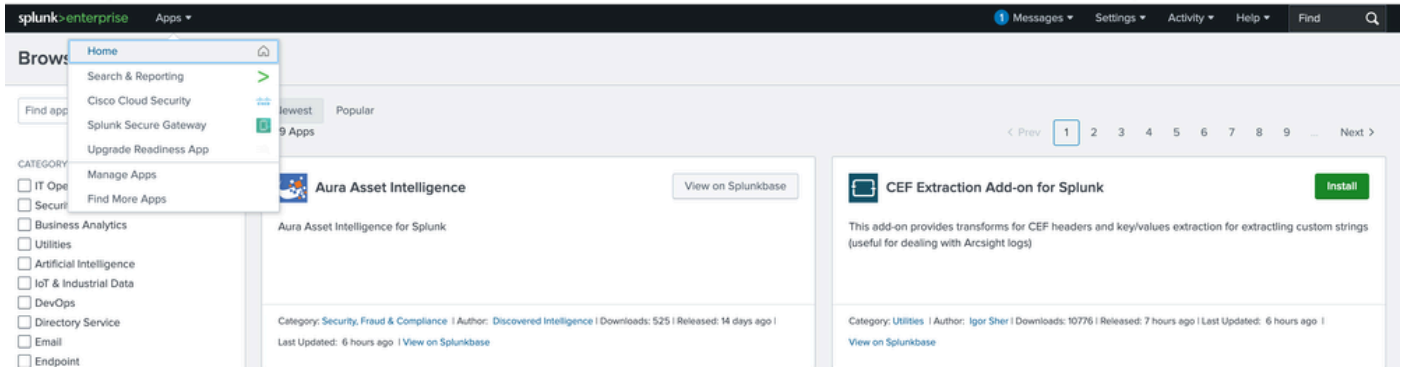


Step 2: Installation of the Cisco Security Cloud Application.

i. Look for the **Cisco Security Cloud Application**. Now, either scroll down till you find the app or search for **Cisco security cloud**.



Caution: Do not get confused with Cisco Cloud Security App.



ii. Install the application by clicking the **Install** button.

Cisco Security Cloud

Install

The **Author** Cisco Security Cloud application offers seamless integration for connecting your Cisco devices with Splunk. It features a modular UX input design, built-in health checks, and constant monitoring to ensure operational integrity.

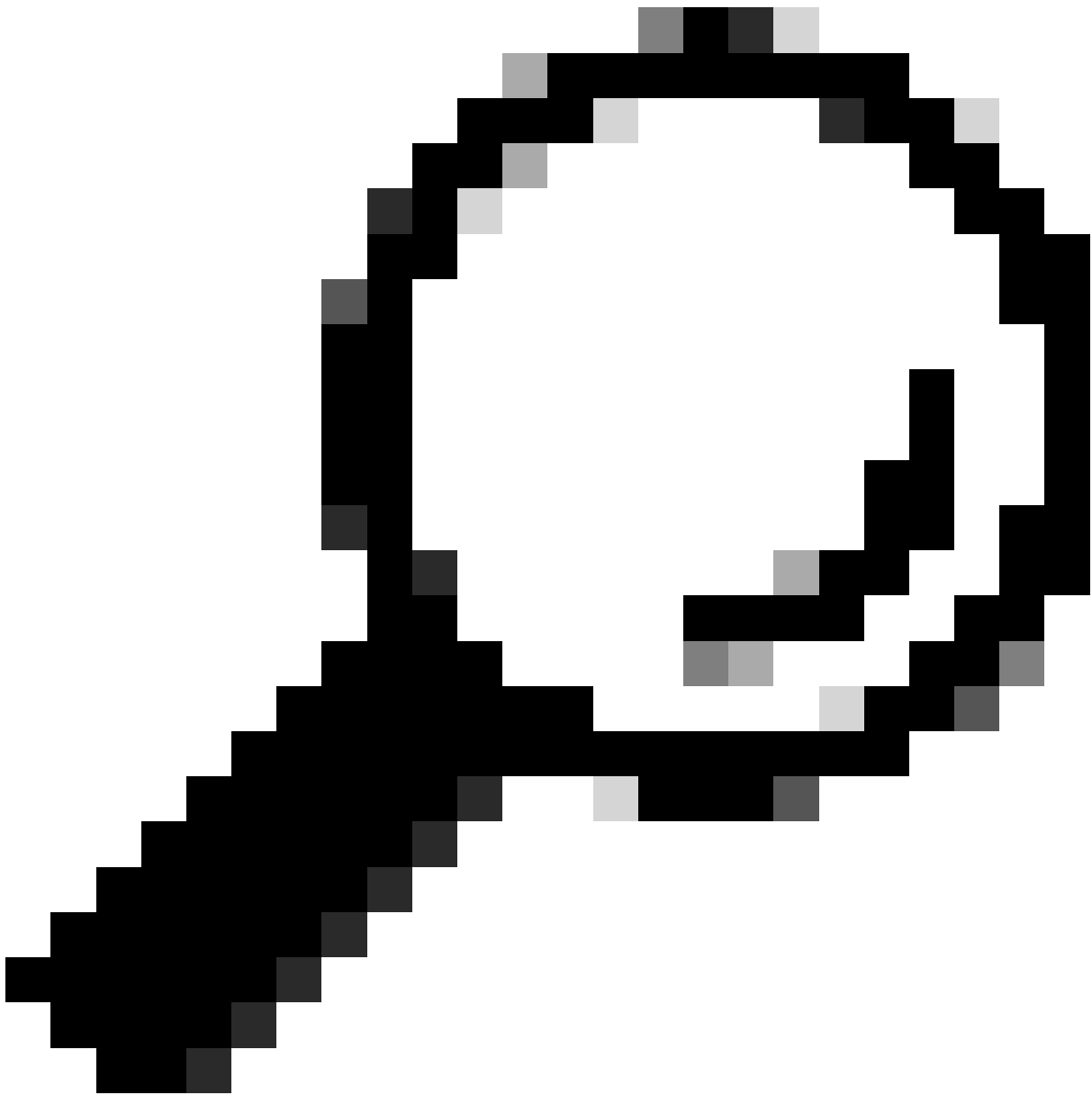
Product(s) Enabled:

- Cisco AI Defense
- Cisco Duo
- Cisco Email Threat Defense (ETD)
- Cisco Identity Intell... [More](#)

Category: [Firewall](#), [Security](#), [Fraud & Compliance](#) | Author: [Cisco Systems, Inc.](#) | Downloads: 17522 |

Released: a month ago | Last Updated: a month ago | [View on Splunkbase](#)

iii. The moment you click the install button a window pops up asking for the credentials of the Splunk account before installing the application. Provide the **credentials** and click **Agree and Install** to proceed further.



Tip: Provide the credentials which are used to access the Splunk portal, not the admin credentials used for Splunk enterprise application while logging in.

Login and Install



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

[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_custom](#)

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](#).

Cancel

Agree and Install

iv. A message pops up on successful installation of the application as depicted. Click **Done**.

Complete



Cisco Security Cloud was successfully installed.

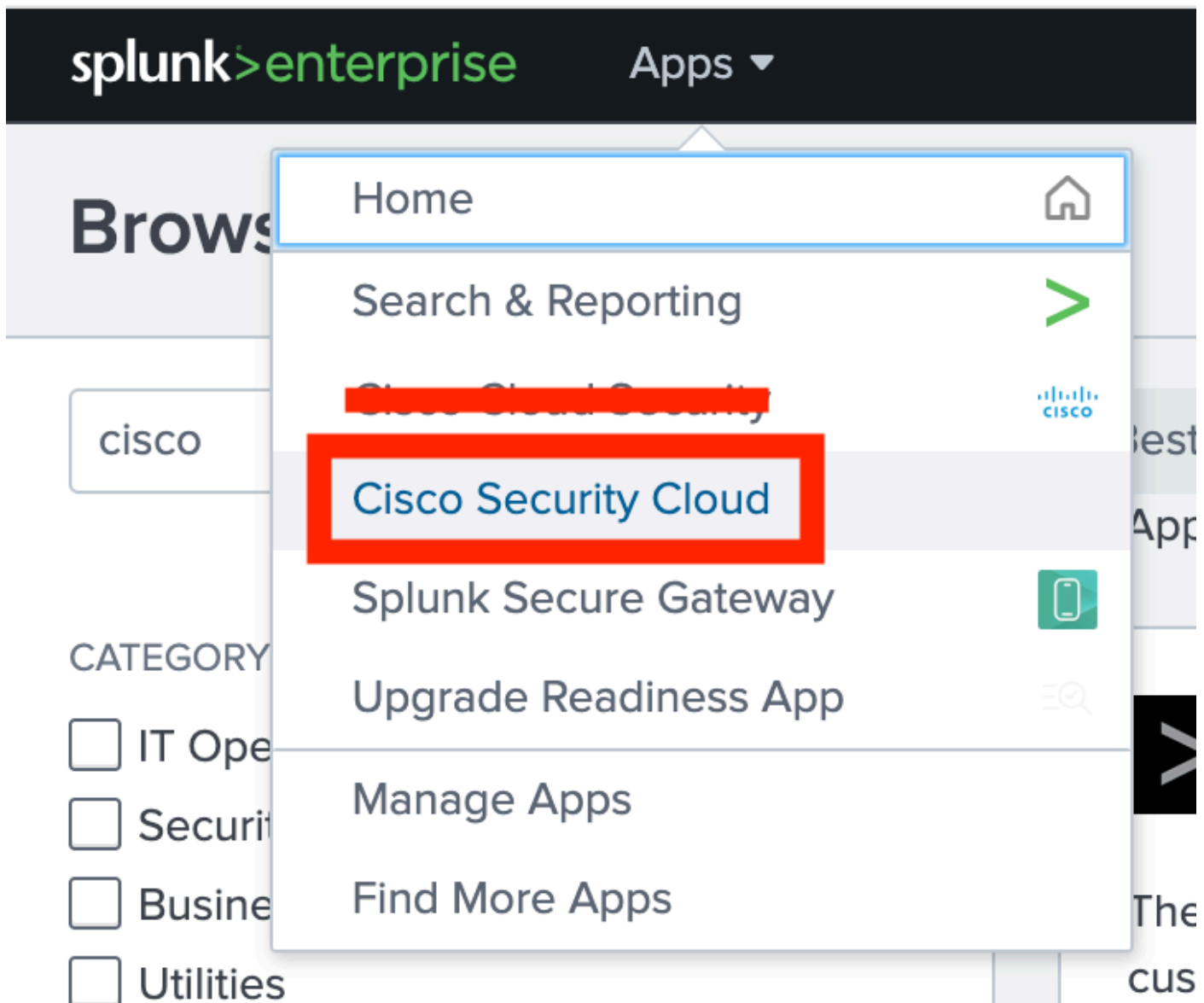
Open the App

Go Home

Done

Step 3: Verification of the Installation of the Cisco Security Cloud Application.

i. Click the **Apps** drop down option, and now the app can be seen in the list after the successful installation:



ii. Select **Cisco Security Cloud** by clicking it. You get redirected to the **Application Setup** page where all the available Cisco Cloud security products can be found.

splunk>enterprise Apps ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Data Integrity Resource Utilization Alerts & Detection **Application Setup** App Analytics ▾

Application Setup

My Apps

Q Search...

>	Input Name	Product	Host	Enabled	Status	Source Type	Index
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 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](#)

Cisco Identity Intelligence
Identity Security

As organizations face growing complexity in identity management, Cisco Identity Intelligence focuses on detecting, monitoring, and responding to identity-based threats. By centralizing and correlating identity data, it provides visibility into user behaviors and risks. With its ITDR and identity posture management capabilities, security teams can proactively detect and mitigate threats in real-time, using AI-powered insights to uncover anomalies and malicious activities, ensuring a robust identity security posture.

[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](#)

Step 4: Integration with Secure Network Analytics (SNA).

The objective of this document is to highlight the installation steps of the Splunk with Secure Network Analytics (SNA) mentioned further.

i. Search for the **Secure Network Analytics** and when it appears, please select **Configure Application**:

Q secure network analytics ✕

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](#)

ii. When selecting the configure option, the configuration page for the detail to add pops up.

Data IntegrityResource UtilizationAlerts & DetectionApplication SetupApp Analytics

Application Setup / Secure Network Analytics

Secure Network Analytics

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](#)

[Privacy Policy](#)

[Sign Up](#)

Add Secure Network Analytics

SNA Connection

*Input Name

Enter a unique name

Input Name is a required field

*Manager Address (IPv4 or IPv6 Address or Hostname)

Enter the Manager Address (IPv4 or IPv6 Address or Hostname) for this account

*Domain ID

Enter the Domain ID for this account

*Username (Role of Primary Admin or Power Analyst)

Enter the Username (Role of Primary Admin or Power Analyst) for this account

*Password

Enter the Password for this account

> Logging Settings

Input Configuration

iii. Fill in all the mandatory details as mentioned for the SNA Connection Details:

1. **Input Name:** any unique name for SNA
2. **Manager Address** (IPv4 or IPv6 Address or Hostname): Management IP of the Primary SNA Manager
3. **Domain ID:** Enter the Value against domain_ID (for example 301)
4. **Username:** The username of the primary manager (for example admin)
5. **Password:** Password of the primary manager user

SNA Connection

*Input Name

SNA_Manager

Enter a unique name

*Manager Address (IPv4 or IPv6 Address or Hostname)

192.168.1.1

Enter the Manager Address (IPv4 or IPv6 Address or Hostname) for this account

*Domain ID

301

Enter the Domain ID for this account

*Username (Role of Primary Admin or Power Analyst)

admin

Enter the Username (Role of Primary Admin or Power Analyst) for this account

*Password

Enter the Password for this account

iv. Leave the remaining settings at their default values or modify them as needed, then click **Save**. A successful message pops up on the screen after the completion.

Logging Settings

Log level

INFO

Input Configuration

Promote SNA Alarms to ES Notables? ⓘ

All Critical Major Minor Trivial Info

☒ Include SNA Alarms as Risk Events ⓘ

*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

Step 5: Verification of Integration.

This is an important step where you need to verify whether the integration executed in the previous step is successfully done, or not.

i. The connection status for the input has to be **Connected** in the **Application Setup** tab with default as **Enabled** for the right name in **Input** field.

Input Name	Product	Host	Enabled	Status	Source Type	Index
SNA_Manager	Secure Network Analytics	Splunk-Server	<input checked="" type="checkbox"/>	Connected	cisco:sna	cisco_sna

ii. Select the **Secure Network Analytics Dashboard** from the drop down, and the stats eventually start reflecting on the dashboard.

splunk>enterprise Apps ▾

Data Integrity Resource Utilization Alerts & Detection Application Setup **App Analytics ▾**

Application Setup

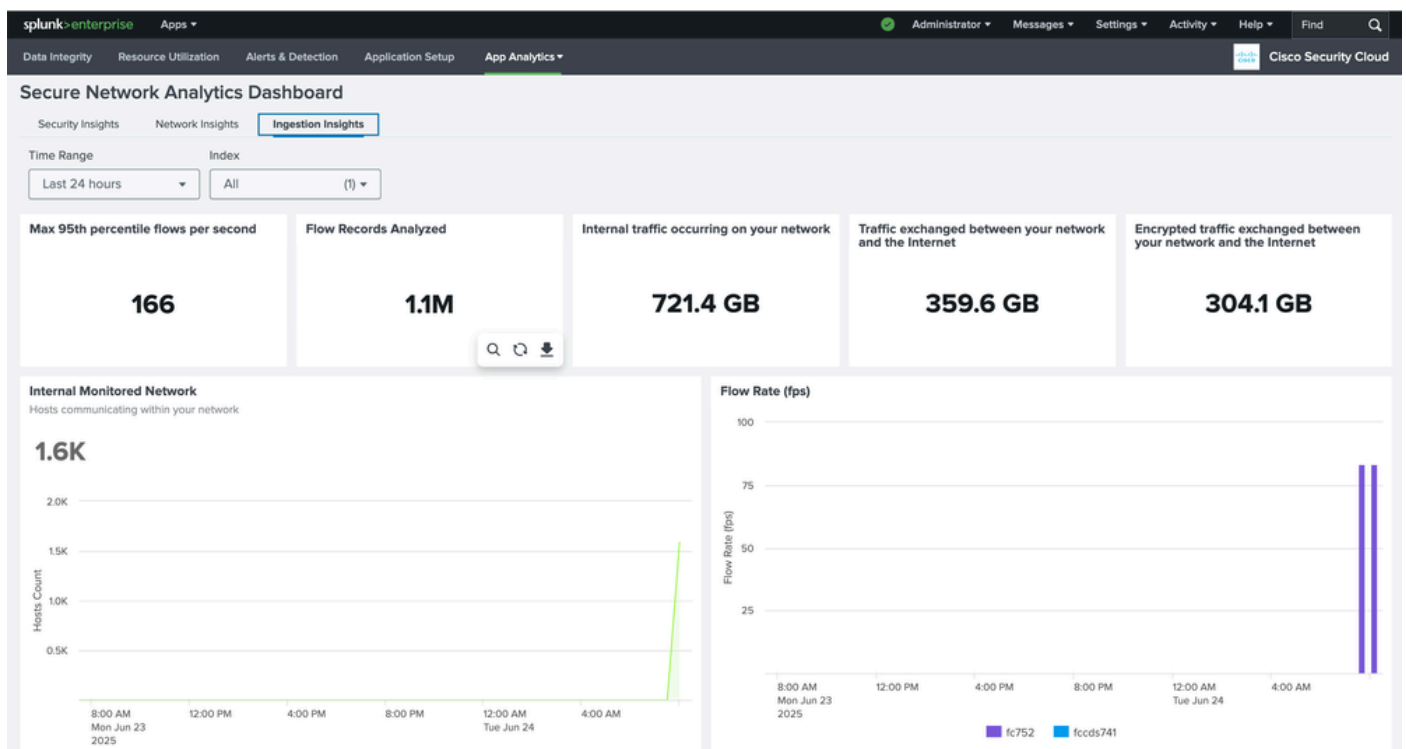
My Apps

Q Search...

>	Input Name	Product
>	SNA_Manager	Secure Network Analytics
>	fmc_syslog_117	Secure Firewall
>	dv_firewall	Secure Firewall
>	Edge_Fw_BB	Secure Firewall

Cisco Products

- Secure Malware Analytics Dashboard
- Duo Dashboard
- Cisco Multicloud Defense Dashboard
- Secure Firewall Dashboard
- XDR Dashboard
- Cisco Secure Email Threat Defense Dashboard
- Secure Network Analytics Dashboard**
- Cisco Secure Endpoint Dashboard
- ASA Dashboard
- Cisco Identity Intelligence Dashboard
- Cisco Vulnerability Intelligence Dashboard
- Cisco AI Defense Dashboard



FAQs

Where to find the domain Id for the SNA manager?

Answer:

i. Log in to the **SNA primary manager** and redirect to the **Appliance administer page** or access [Manager IP Index](#) URL.

ii. Browse the **smc** folder under the **Support** section.

← → ↻ Not Secure https://manager.ift/smc/files/

Manager VE

- Home
- Configuration
- Support**
 - Backup/Restore Database
 - Browse Files
 - Packet Capture
 - Diagnostics Pack
- Operations
- Logout
- Help

Browse Files

Name	Size	Last Modified
admin	-	19-May-2025, 2:13:03 am UTC
apps	-	06-Jun-2025, 9:26:56 am UTC
database	-	06-Jun-2025, 9:26:56 am UTC
etc	-	06-Jun-2025, 9:26:56 am UTC
fedlet	-	15-May-2025, 3:01:03 pm UTC
fedlet-manager	-	15-May-2025, 3:01:03 pm UTC
logs	-	24-Jun-2025, 1:01:05 am UTC
manual-set-time	-	06-Jun-2025, 9:26:54 am UTC
nginx	-	06-Jun-2025, 9:26:56 am UTC
security	-	06-Jun-2025, 9:26:56 am UTC
services	-	06-Jun-2025, 9:26:56 am UTC
smc	-	09-May-2025, 10:59:39 pm UTC
tcpdump	-	29-Apr-2025, 8:57:16 pm UTC
tomcat	-	26-May-2025, 2:27:00 pm UTC

iii. Open **domain.xml** file available in **domain_XXX** folder under the **config** folder.



Home

Configuration

Support

Operations

Logout

Help

Browse Files (/smc/config/domain_301)

/smc/config/domain_301

Parent Directory

	Name	Size	Last Modified
	alarm_configuration.xml	63	15-May-2025, 5:57:26 pm UTC
	application_definitions.xml	93	15-May-2025, 5:57:26 pm UTC
	custom_security_events.json	8.48k	15-May-2025, 5:57:27 pm UTC
	domain.xml	155	15-May-2025, 5:57:26 pm UTC
	exporter_301_10.106.127.73.xml	252	06-Jun-2025, 8:59:01 am UTC
	exporter_301_10.106.127.74.xml	300	19-May-2025, 2:26:58 am UTC
	exporter_301_10.122.147.1.xml	14.2k	14-Jun-2025, 6:31:00 pm UTC
	exporter_301_10.197.163.45.xml	587	19-May-2025, 2:30:00 am UTC
	exporter_snmp.xml	344	15-May-2025, 5:57:26 pm UTC
	host_group_pairs.xml	60.22k	06-Jun-2025, 9:32:36 am UTC
	host_groups.xml	56.99k	06-Jun-2025, 9:33:58 am UTC
	host_policy.xml	113.32k	15-May-2025, 5:57:27 pm UTC
	map_0.xml	25.2k	06-Jun-2025, 9:31:15 am UTC
	map_1.xml	629.25k	06-Jun-2025, 9:31:16 am UTC
	map_2.xml	436.26k	06-Jun-2025, 9:31:16 am UTC
	service_definitions.xml	140.09k	15-May-2025, 5:57:26 pm UTC
	swa_301.xml	2.19k	06-Jun-2025, 8:57:50 am UTC