

# 使用安全雲應用將SNA整合到Splunk

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[常見問題](#)

---

## 簡介

本文檔介紹使用Cisco安全雲與Splunk順利整合SNA，以便更快地對已確定的威脅作出事件響應。

## 必要條件

Splunk和思科裝置的基本知識。

### 需求

本文件沒有特定需求。

### 採用元件

本文件中的資訊是以下列硬體與軟體版本為依據：

Splunk企業版

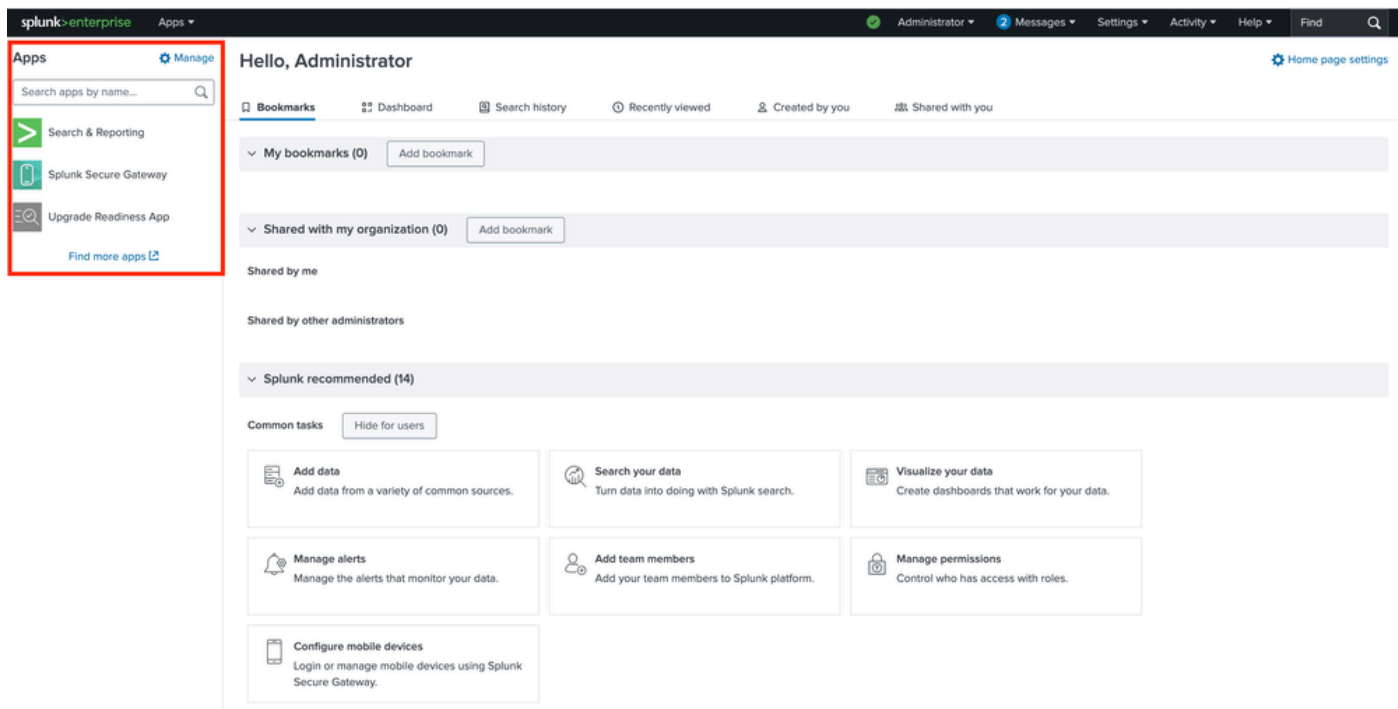
安全網路分析v7.5.2.

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 設定

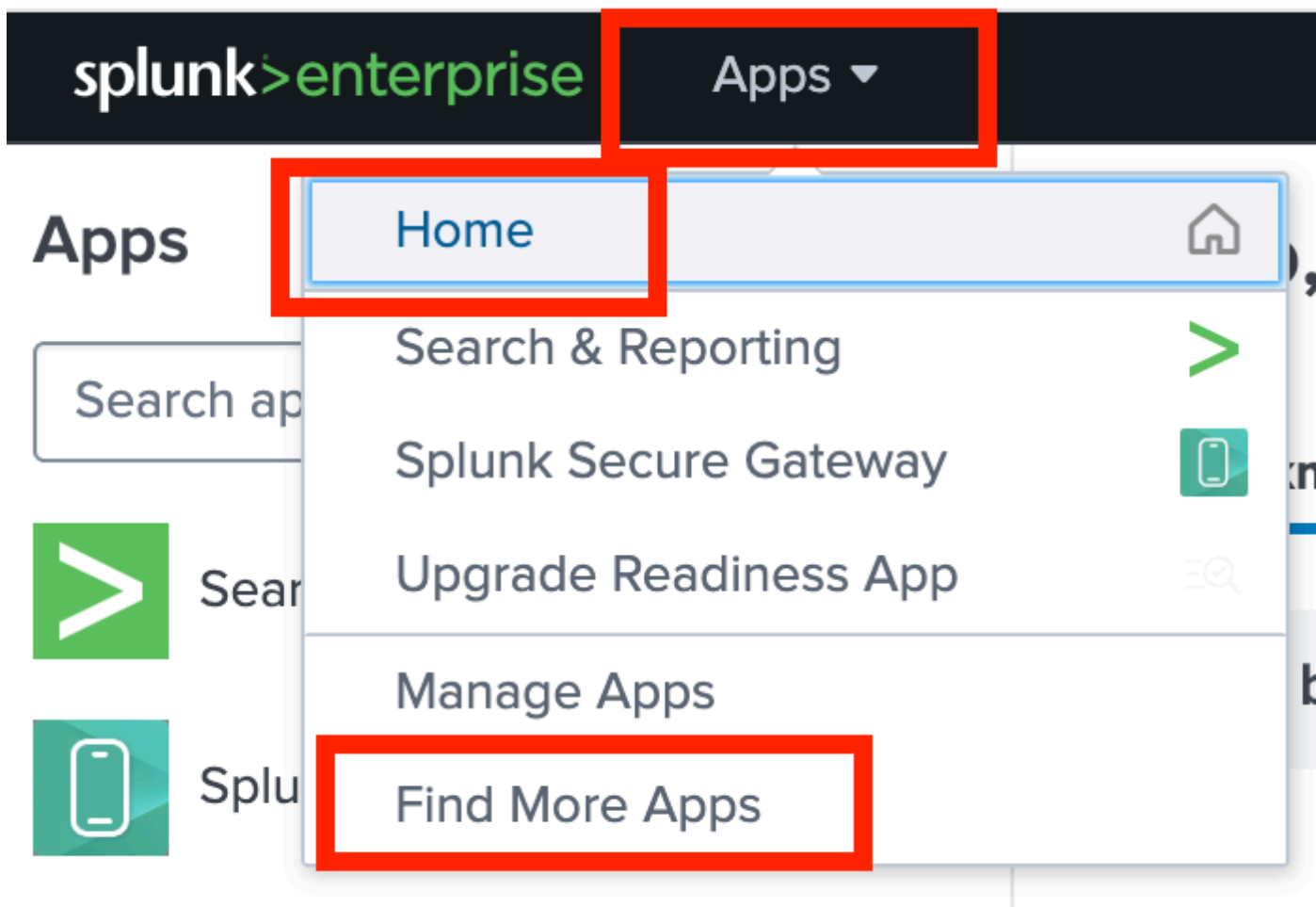
第1步：存取Splunk應用程式，並安裝思科安全雲應用程式。

i.使用管理員憑據登入到Splunk Web門戶，成功登入後，可以看到「應用」部分左側已安裝應用程式清單的首頁：

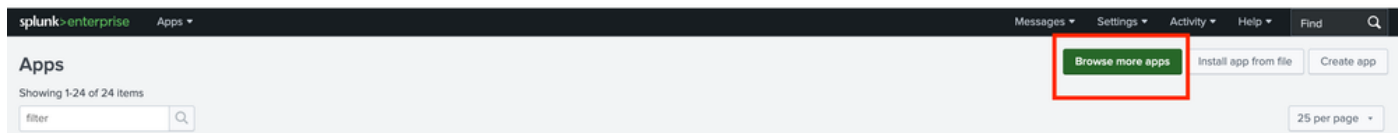


二。為了將SNA與Splunk整合，需要安裝思科安全雲應用，可通過以下任一方法實現：

1. 從下拉選單中選擇查詢更多應用。



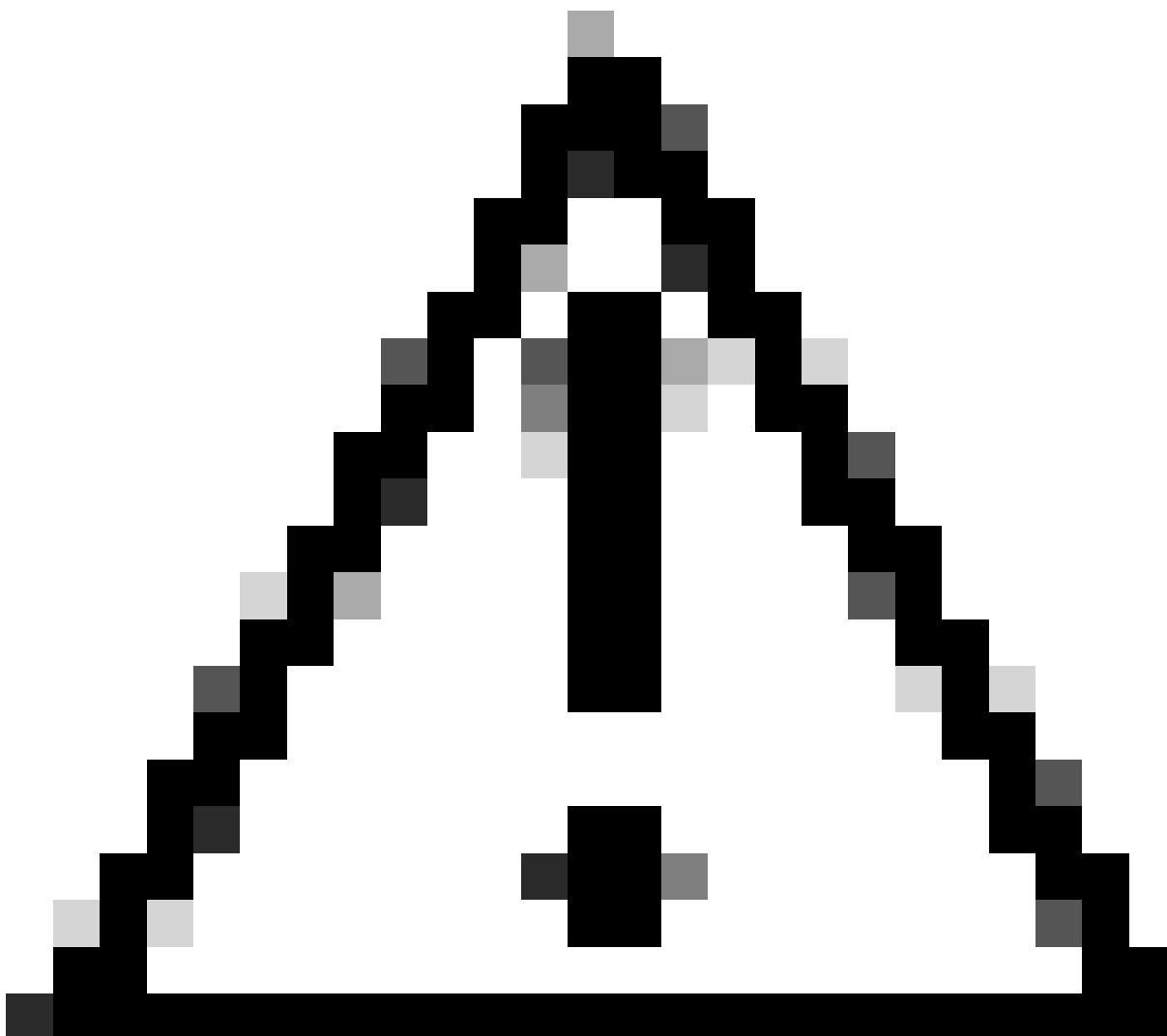
b.在Manager gear icon下瀏覽更多應用程式。



步驟 2:安裝思科安全雲應用。

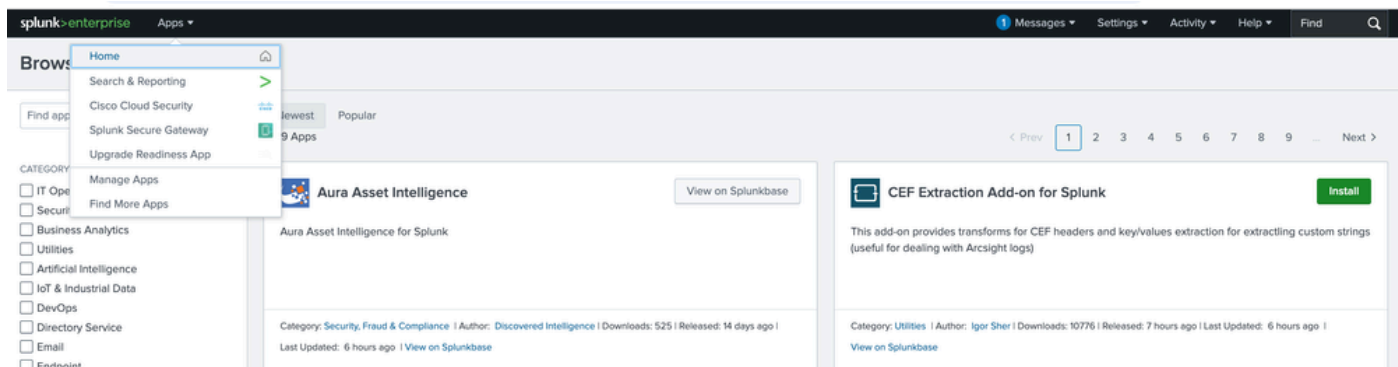
i.尋找思科安全雲應用。現在，向下滾動至找到應用或搜尋思科安全雲。

---

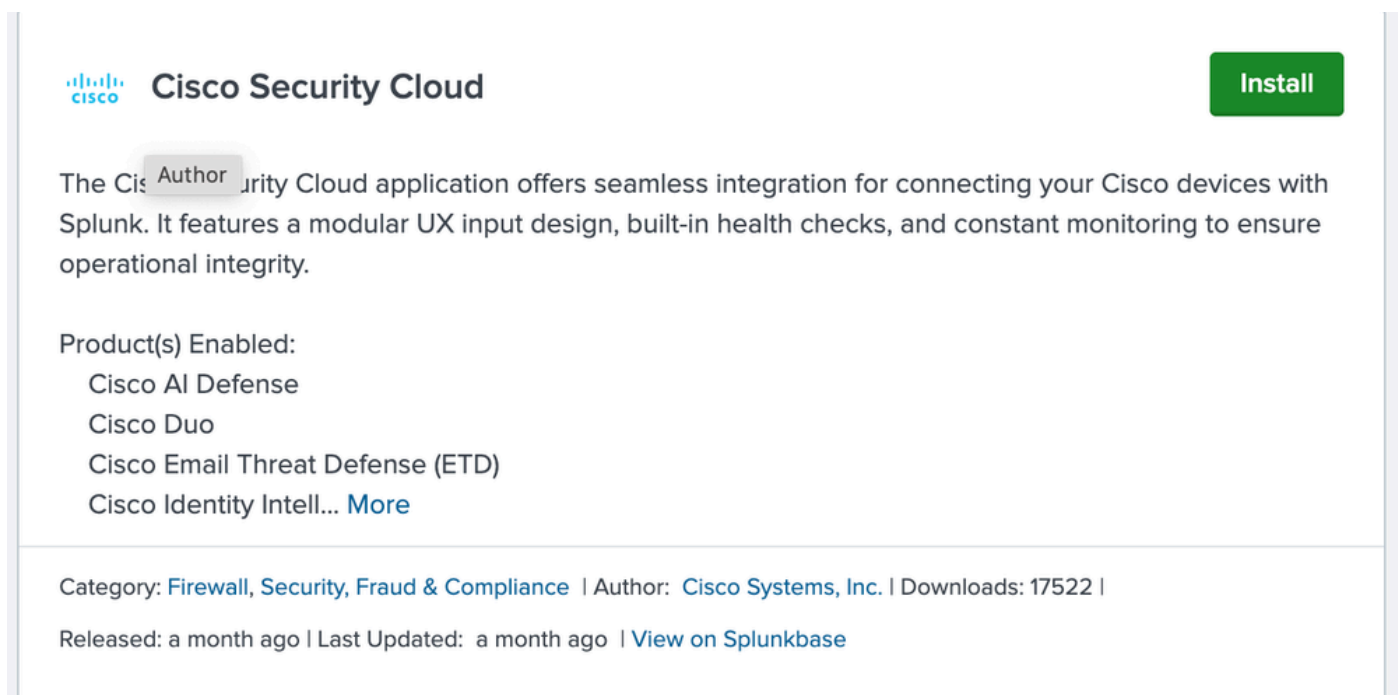


注意：請勿與思科雲端安全應用相混淆。

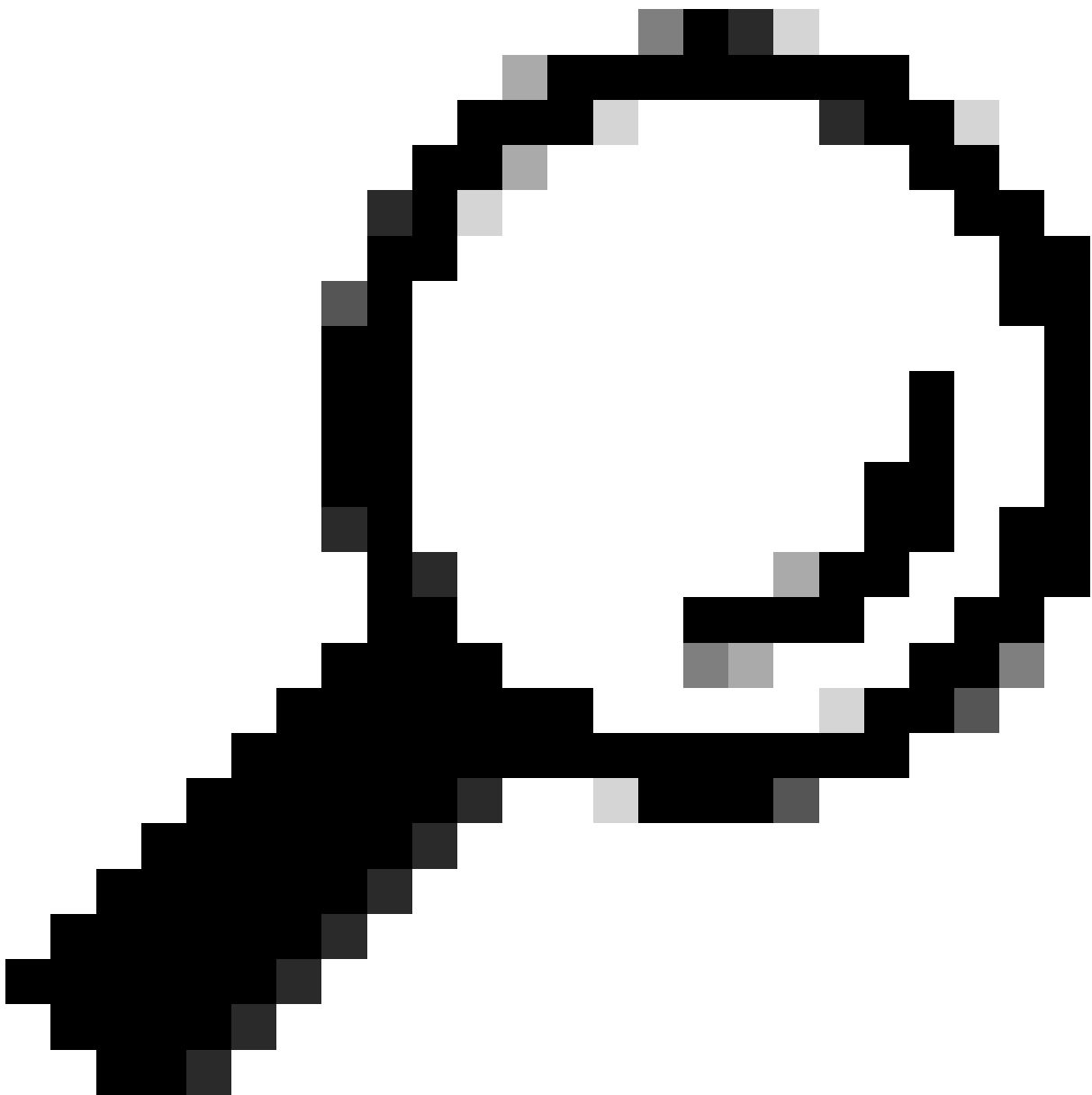
---



二。按一下Install按鈕安裝應用程式。



三。當您按一下「安裝」按鈕時，會彈出一個視窗，要求您提供Splunk帳戶的憑據，然後再安裝應用程式。提供憑據，然後按一下Agree and Install以繼續操作。



提示：提供用於訪問Splunk門戶的憑據，而不是登入時用於Splunk企業應用程式的管理員憑據。

---

## 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

四。成功安裝應用程式時會顯示一條消息，如圖所示。按一下「完成」。

## Complete



Cisco Security Cloud was successfully installed.

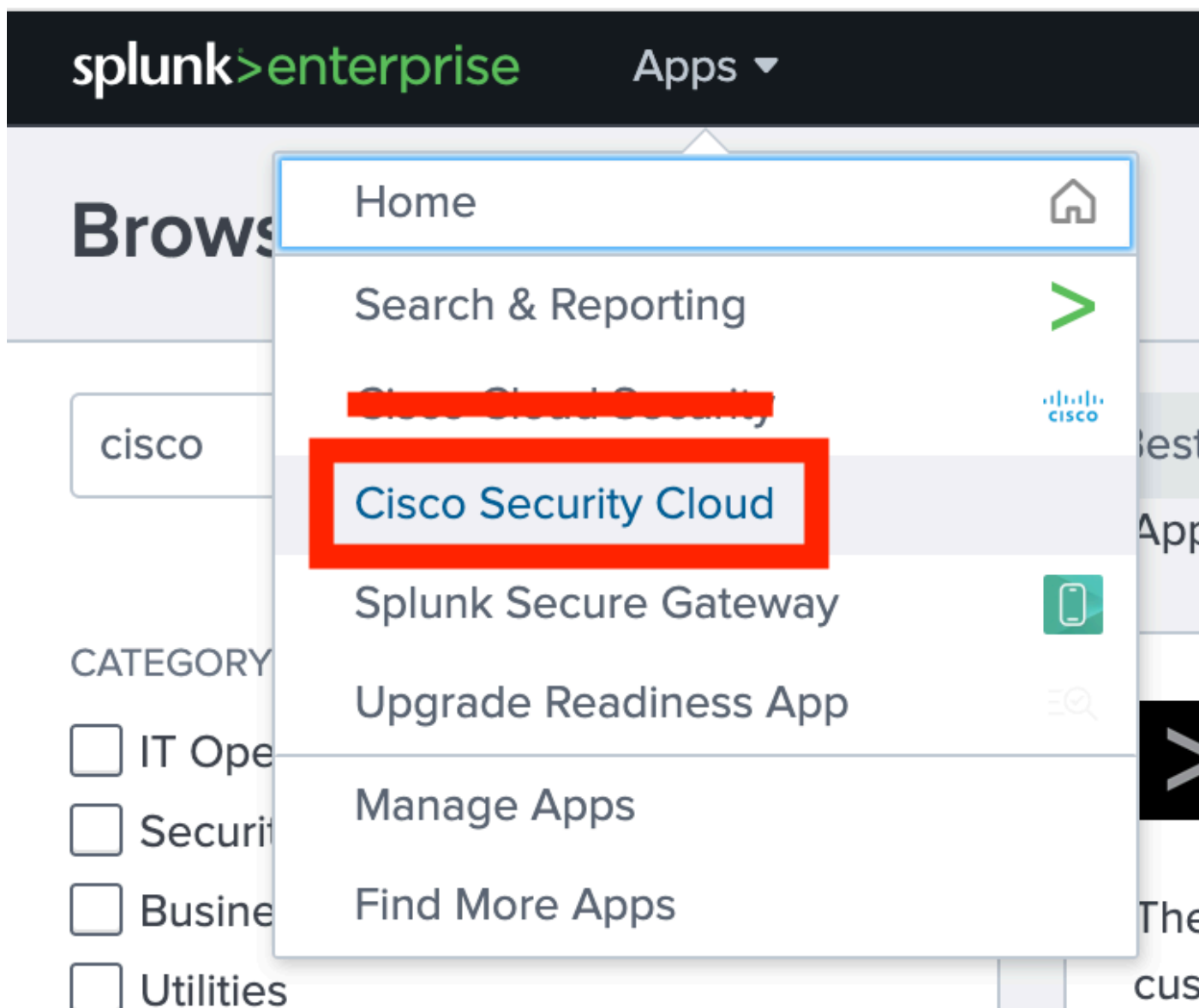
Open the App

Go Home

Done

步驟 3:驗證思科安全雲應用的安裝。

i.按一下Apps下拉選項，成功安裝後，即可從清單中看到該應用：



ii. 按一下Cisco Security Cloud將其選中。系統會將您重新導向至應用程式設定頁面，您可以在此頁面找到所有可用的思科雲端安全產品。



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

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

### 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.


[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](#)

步驟 4:與安全網路分析(SNA)整合。

本文的目標為著重說明進一步提到的使用安全網路分析(SNA)的Splunk的安裝步驟。

i. 搜尋Secure Network Analytics，並在出現時選擇Configure Application:

Search 🔍 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](#)

二。選擇配置選項時，將彈出要新增詳細資訊的配置頁面。

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

### 三。填寫SNA連線詳細資訊中提到的所有必填詳細資訊：

- 輸入名稱:SNA的任何唯一名稱
- Manager地址（IPv4或IPv6地址或主機名）：主SNA管理器的管理IP
- 域ID：根據domain\_ID輸入值（例如301）
- 使用者名稱:主管理器的使用者名稱（例如admin）
- 密碼:主管理員使用者的密碼

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

四。將其餘設定保留為預設值，或根據需要對其進行修改，然後按一下Save。完成後，螢幕上會彈出一條成功消息。

Logging Settings

Log level

INFO

Input Configuration

Promote SNA Alarms to ES Notables?

AllCriticalMajorMinorTrivialInfo

☒ 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

步驟 5:驗證整合。

這是一個重要的步驟，您需要確認上一步執行的整合是否成功完成。

i.在Application Setup頁籤中，輸入的連線狀態必須是Connected，對於Input欄位中的正確名稱，其預設值為Enabled。

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Data IntegrityResource UtilizationAlerts & DetectionApplication SetupApp Analytics

Application Setup

My Apps

Search...

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.從下拉選單中選擇Secure Network Analytics Dashboard，統計資料最終開始在控制面板上反映。

splunk>enterprise Apps ▾

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

## Application Setup

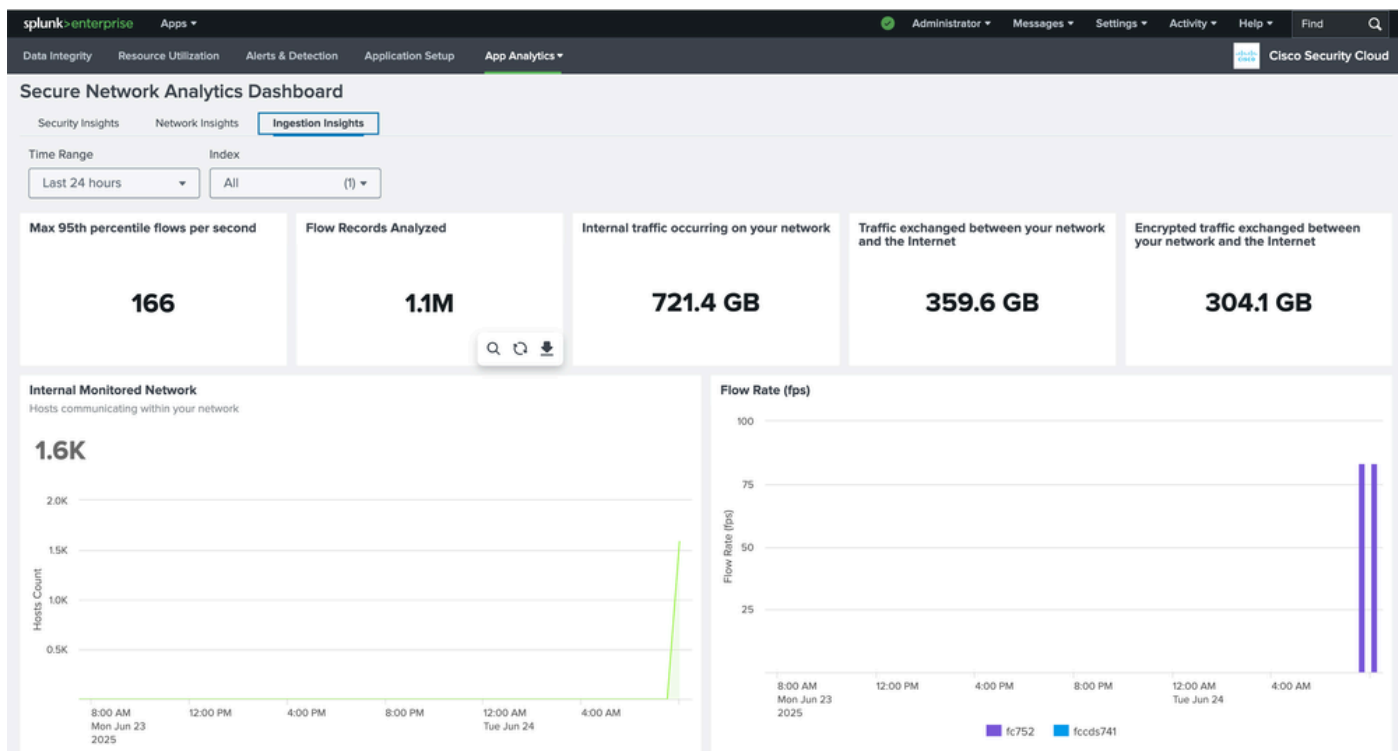
My Apps

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



## 常見問題

在哪裡查詢SNA管理器的域ID？

答案：

i. 登入到SNA主管理器，並重定向到裝置管理頁面或訪問[Manager IP索引](#)URL。

二。瀏覽支援部分下的smc資料夾。

← → ↻ 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
<b>smc</b>	-	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

三。開啟config 資料夾下的domain\_XXX資料夾中可用的domain.xml檔案。



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

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。