

# 使用安全云应用将SNA集成到Splunk

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[常见问题解答](#)

---

## 简介

本文档介绍使用思科安全云与Splunk进行顺畅的SNA集成，以便更快地响应已发现的威胁。

## 先决条件

Splunk和思科设备的基本知识。

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于下列硬件和软件版本：

Splunk企业

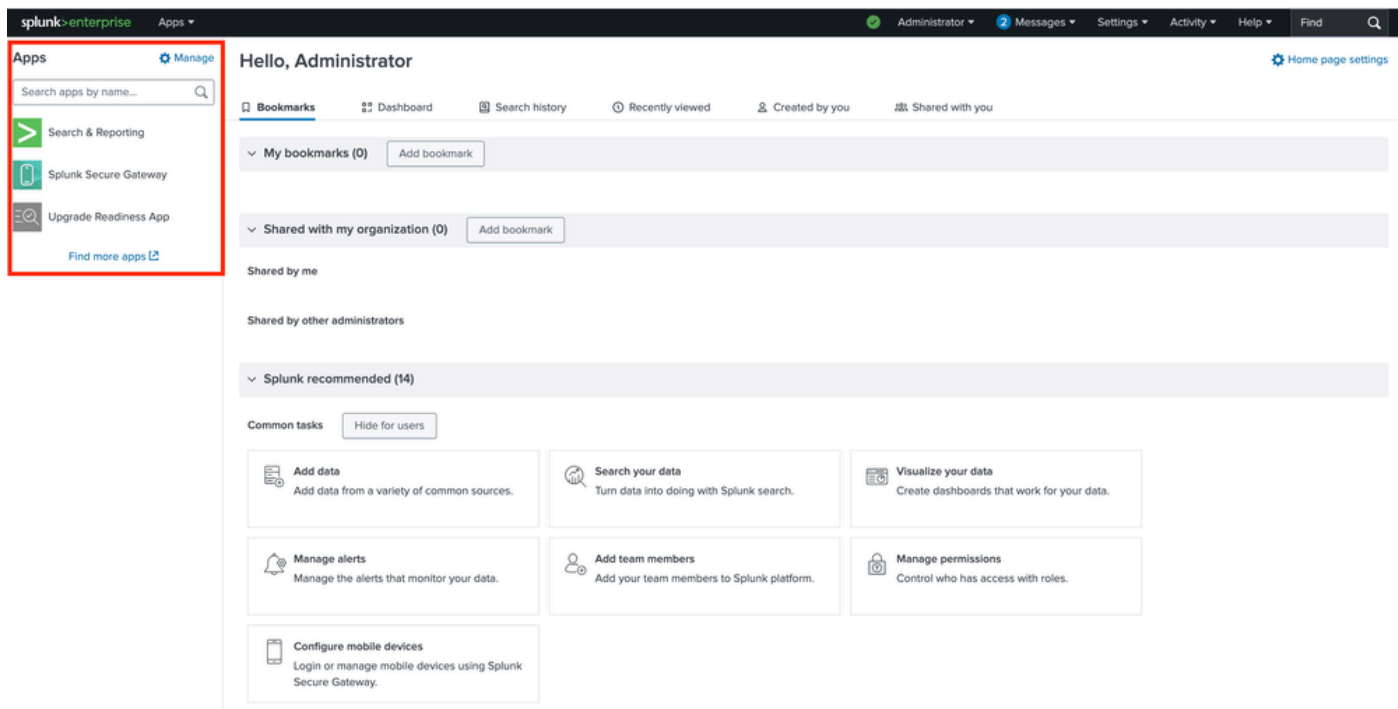
安全网络分析v7.5.2。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

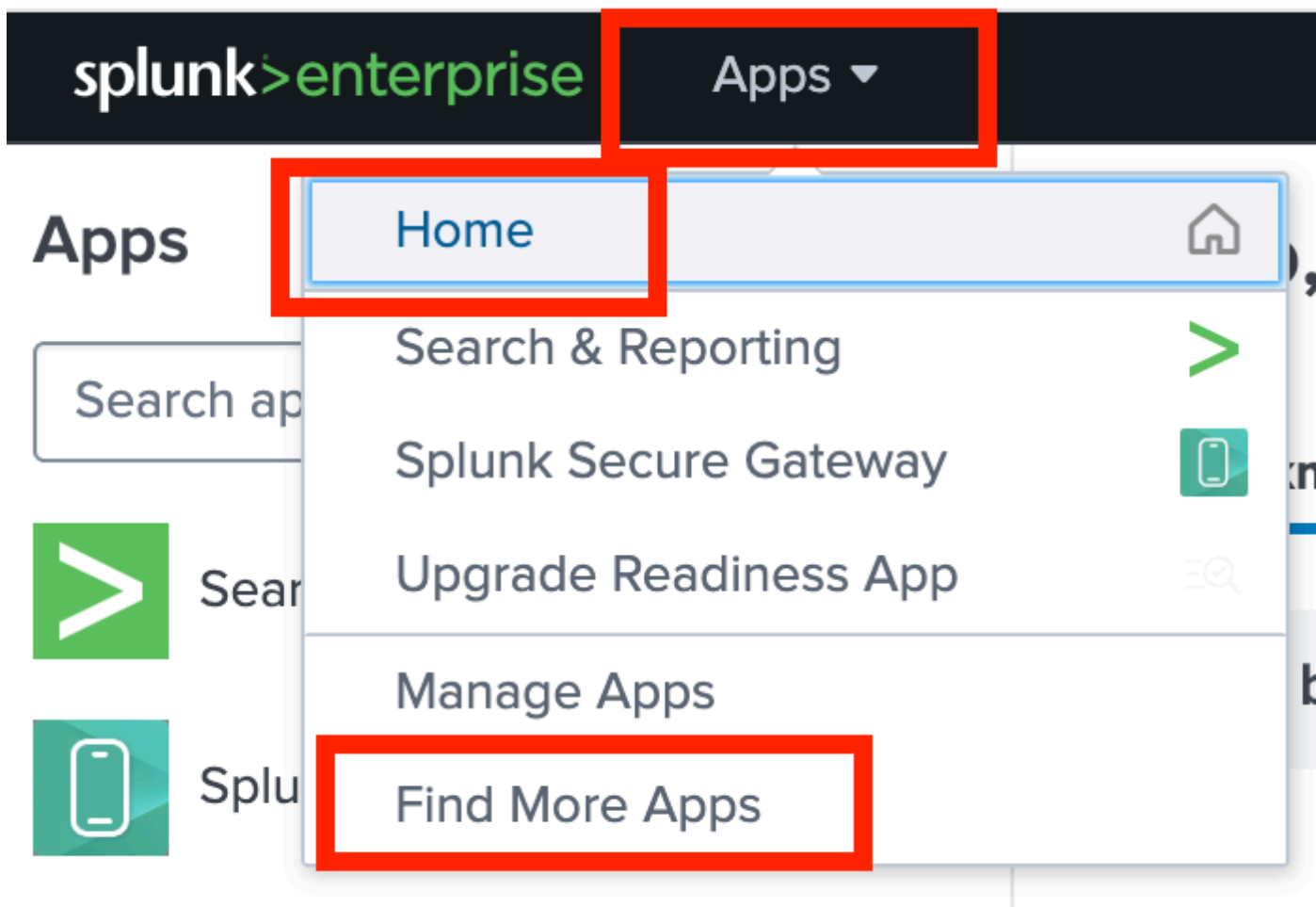
步骤1:访问Splunk应用并安装思科安全云应用。

i.使用管理员凭证登录Splunk Web门户，成功登录时，主页左侧的“应用”(App)部分下会显示已安装应用的列表：

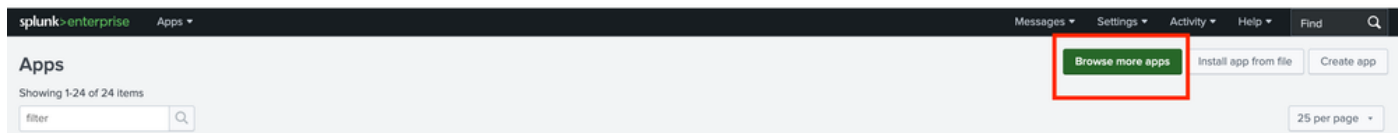


二、要将SNA与Splunk集成，需要安装思科安全云应用，可通过以下任一方法实现：

1. 从下拉菜单中选择Find More Apps。



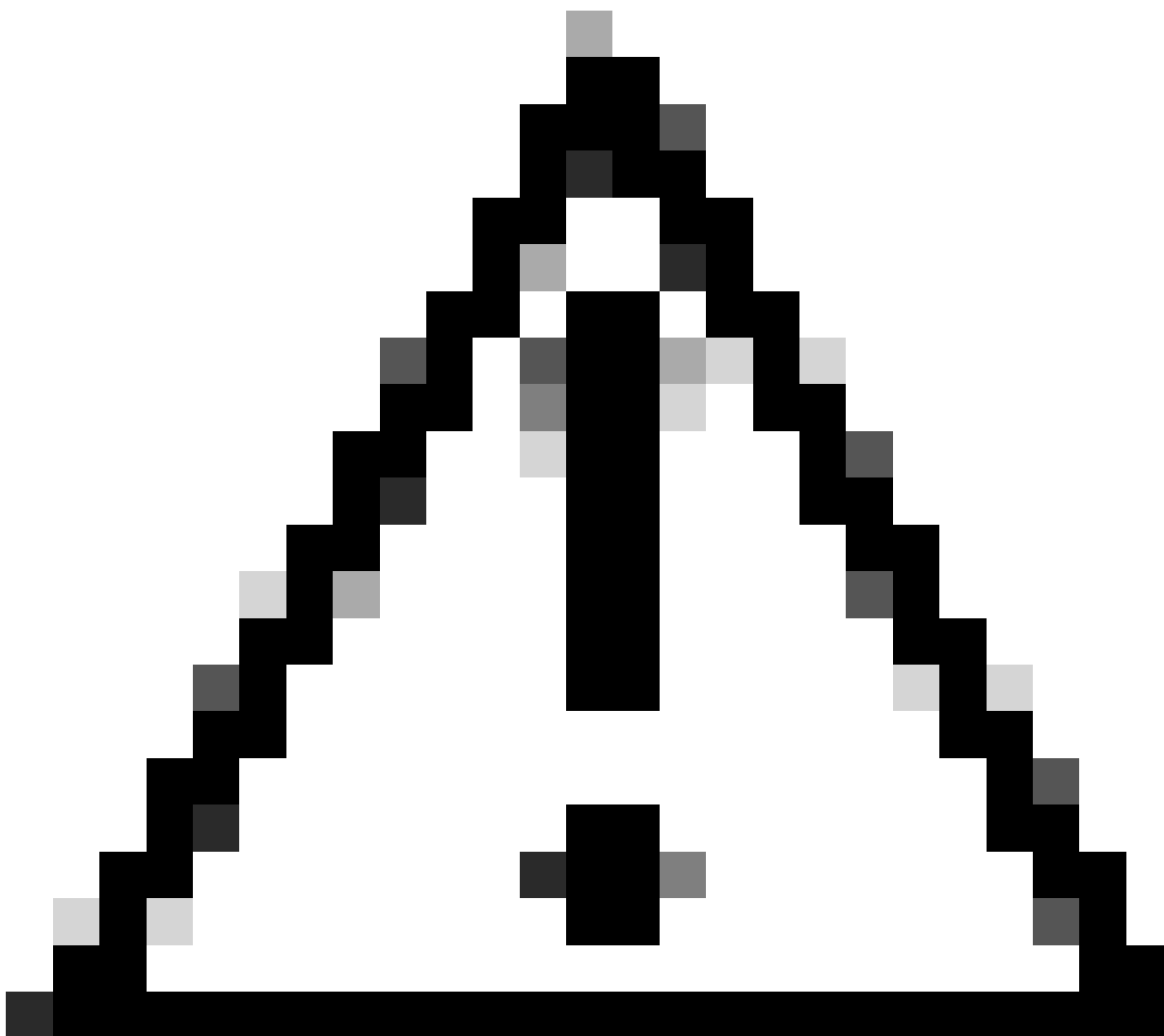
b.在Manager gear图标下浏览更多应用。



步骤 2：思科安全云应用的安装。

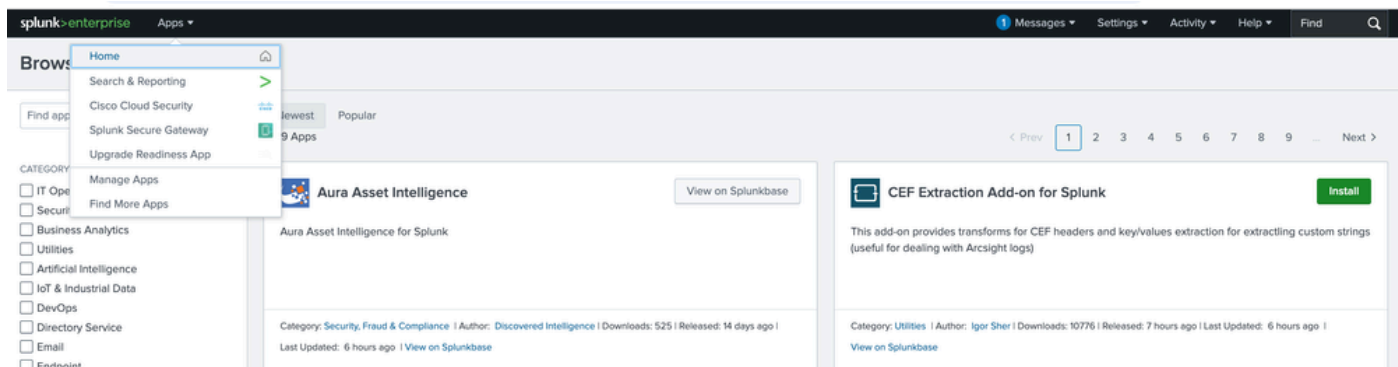
i. 寻找思科安全云应用。现在，向下滚动至找到应用或搜索思科安全云。

---

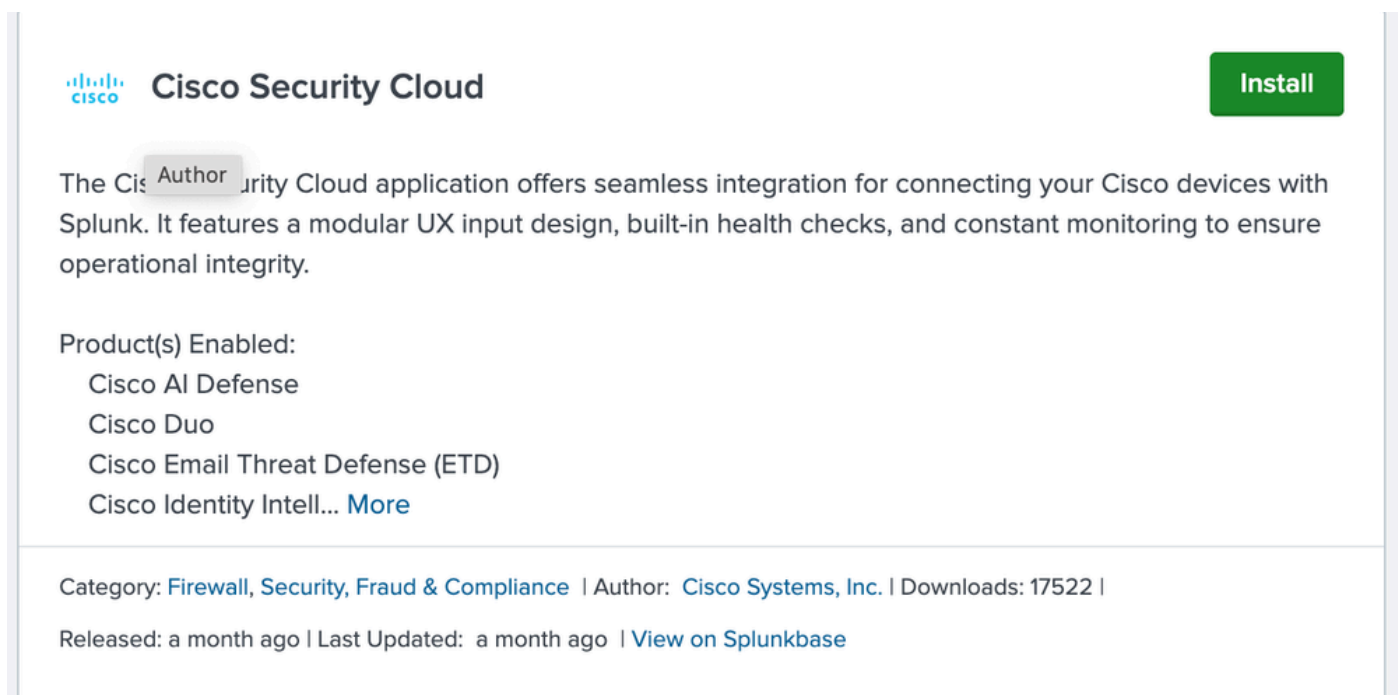


警告：不要与思科云安全应用相混淆。

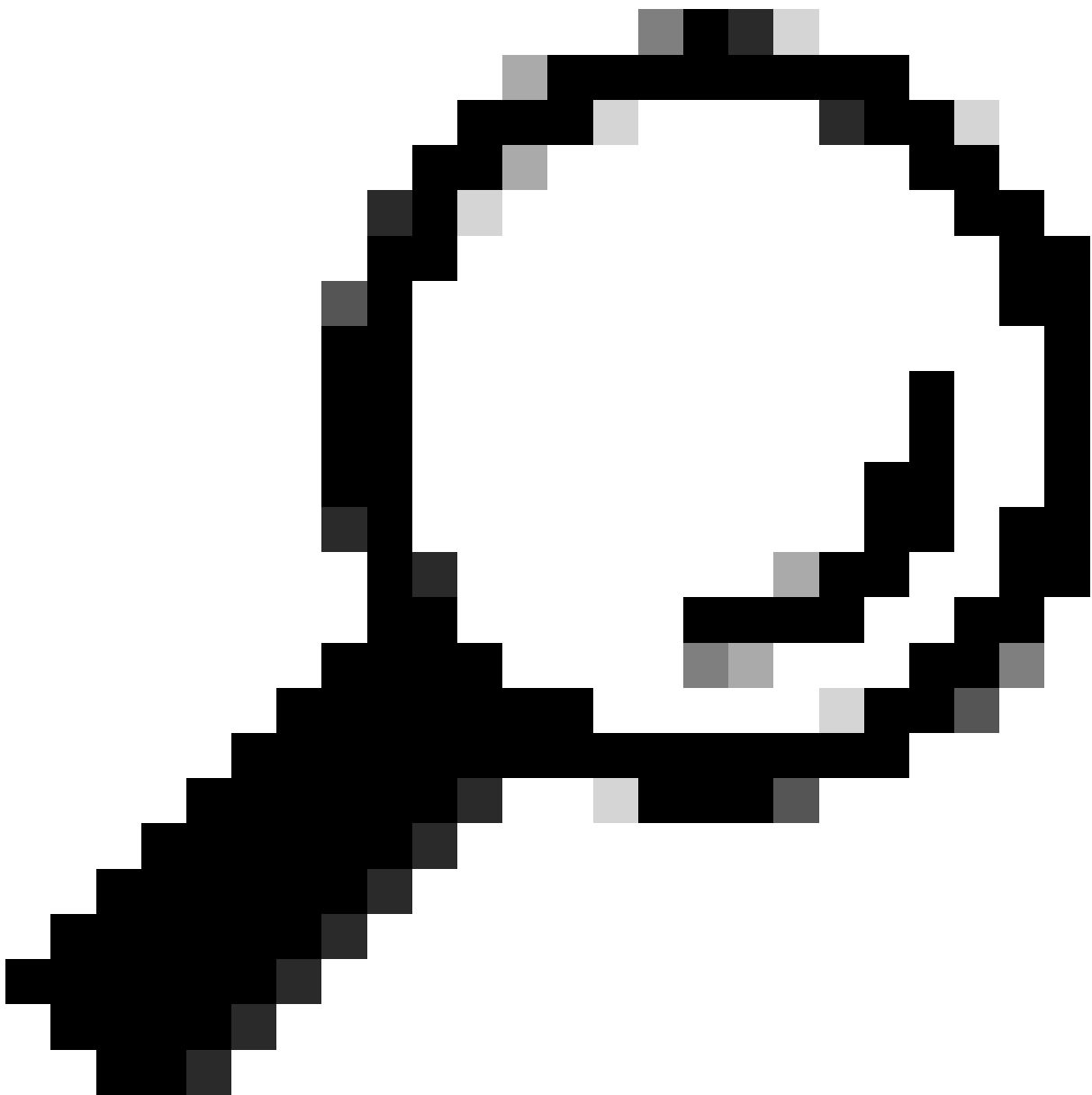
---



## 二、单击Install按钮安装应用。



三。一旦您单击安装按钮，就会弹出一个窗口，要求您提供Splunk帐户的凭证，然后再安装应用。提供凭证，然后单击Agree and Install继续操作。



提示：提供用于访问Splunk门户的凭据，而不是登录时用于Splunk企业应用的管理员凭据。

---

## 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。如图所示，成功安装应用后会弹出一条消息。单击Done。

## Complete



Cisco Security Cloud was successfully installed.

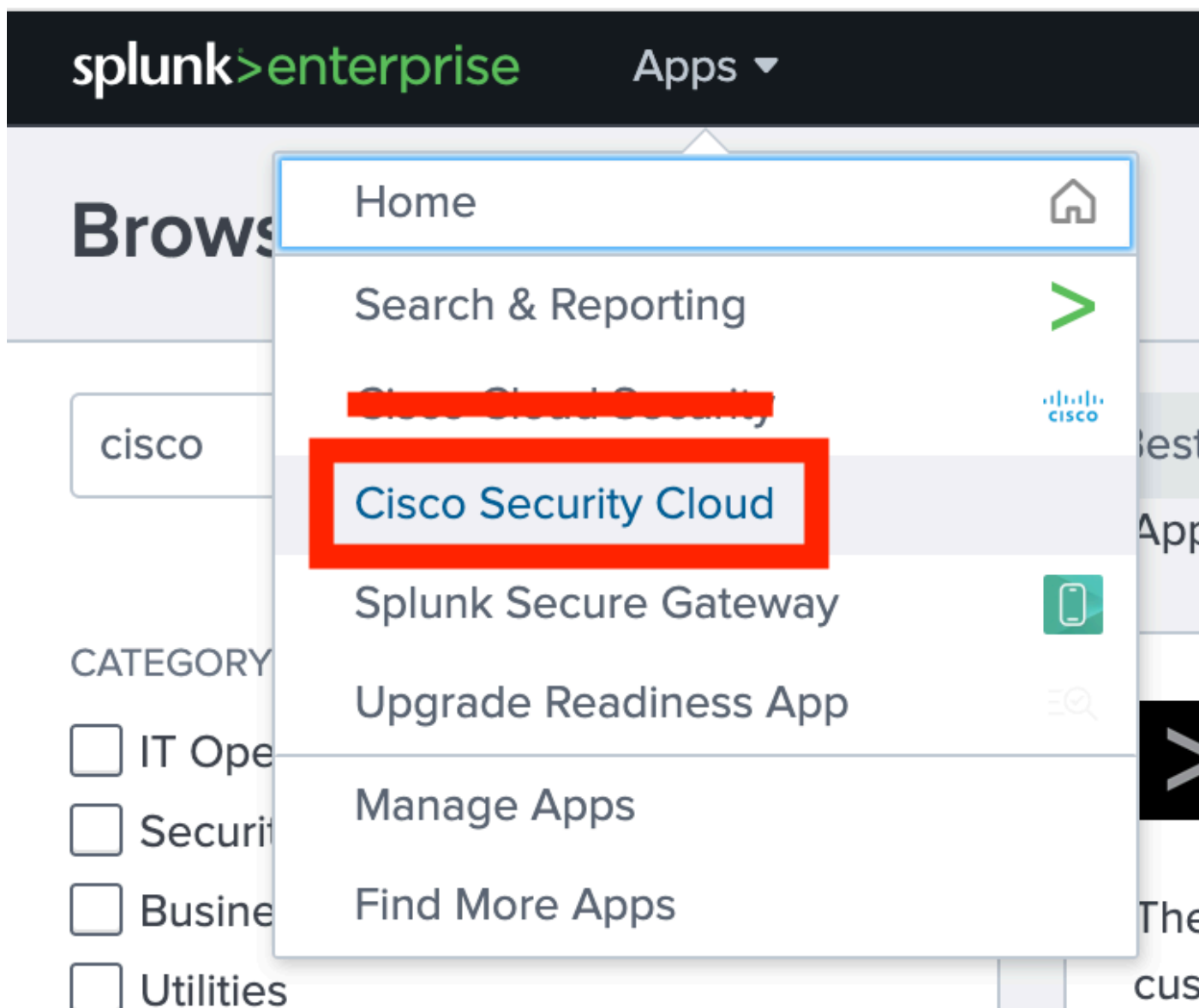
Open the App

Go Home

Done

步骤 3：验证思科安全云应用的安装。

i.单击Apps下拉选项，现在安装成功后即可从列表中看到该应用：



ii.单击Cisco Security Cloud以将其选中。您将重定向到应用设置页面，您可以在该页面找到所有可用的思科云安全产品。



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](#)

步骤 4：与安全网络分析(SNA)集成。

本文档旨在重点介绍进一步提到的具有安全网络分析(SNA)的Splunk的安装步骤。

i.搜索Secure Network Analytics，出现时，请选择配置应用：

Q secure network analytics X



**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、选择配置选项时，将弹出要添加详细信息的配置页面。

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。填写SNA连接详细信息中提及的所有必填详细信息：

1. 输入名称:SNA的任何唯一名称
2. Manager地址（IPv4或IPv6地址或主机名）：主SNA管理器的管理IP
3. 域ID：根据domain\_ID输入值（例如301）
4. username：主管理器的用户名（例如admin）
5. 密码：主要管理员用户的密码

SNA Connection

\*Input Name

SNA\_Manager

Enter a unique name

\*Manager Address (IPv4 or IPv6 Address or Hostname)

10.10.10.10

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。将剩余设置保留为默认值，或根据需要对其进行修改，然后单击Save。完成后，屏幕上会弹出一条成功的消息。

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

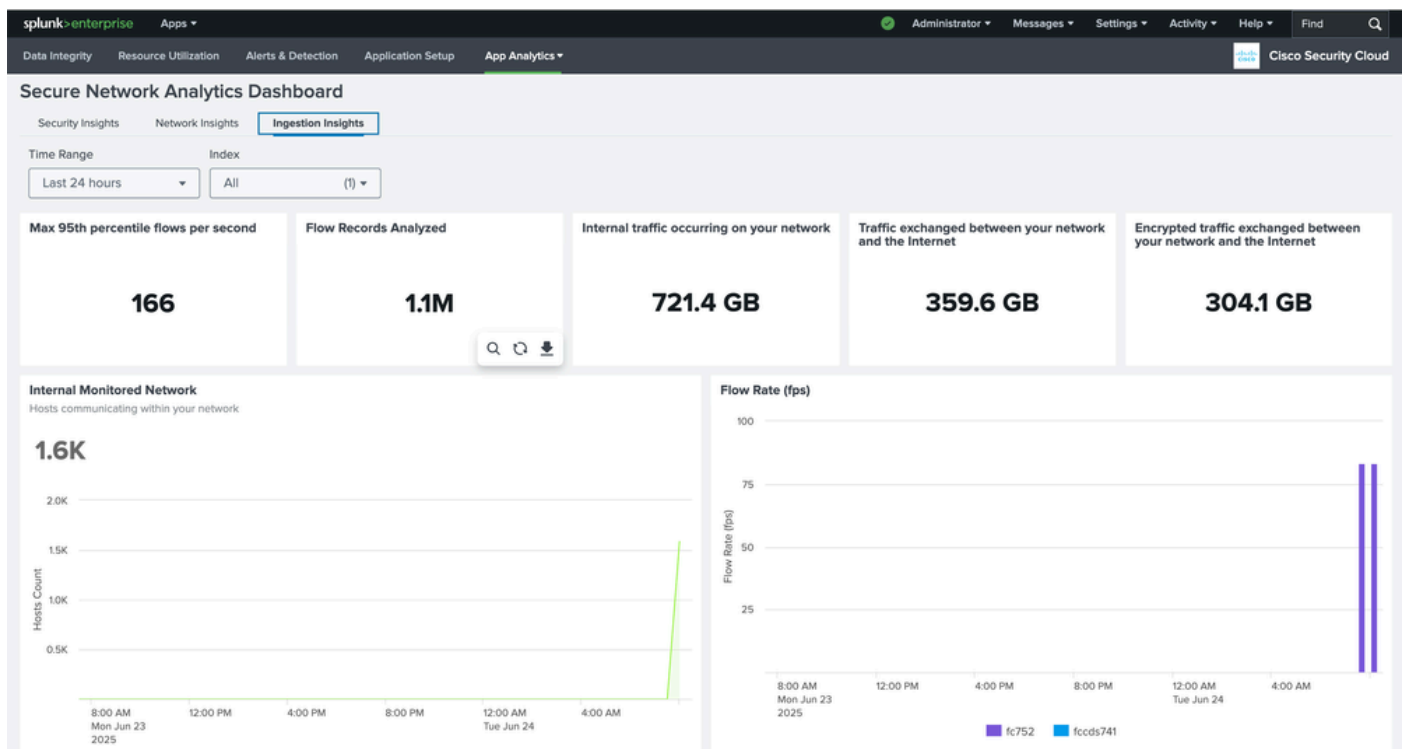
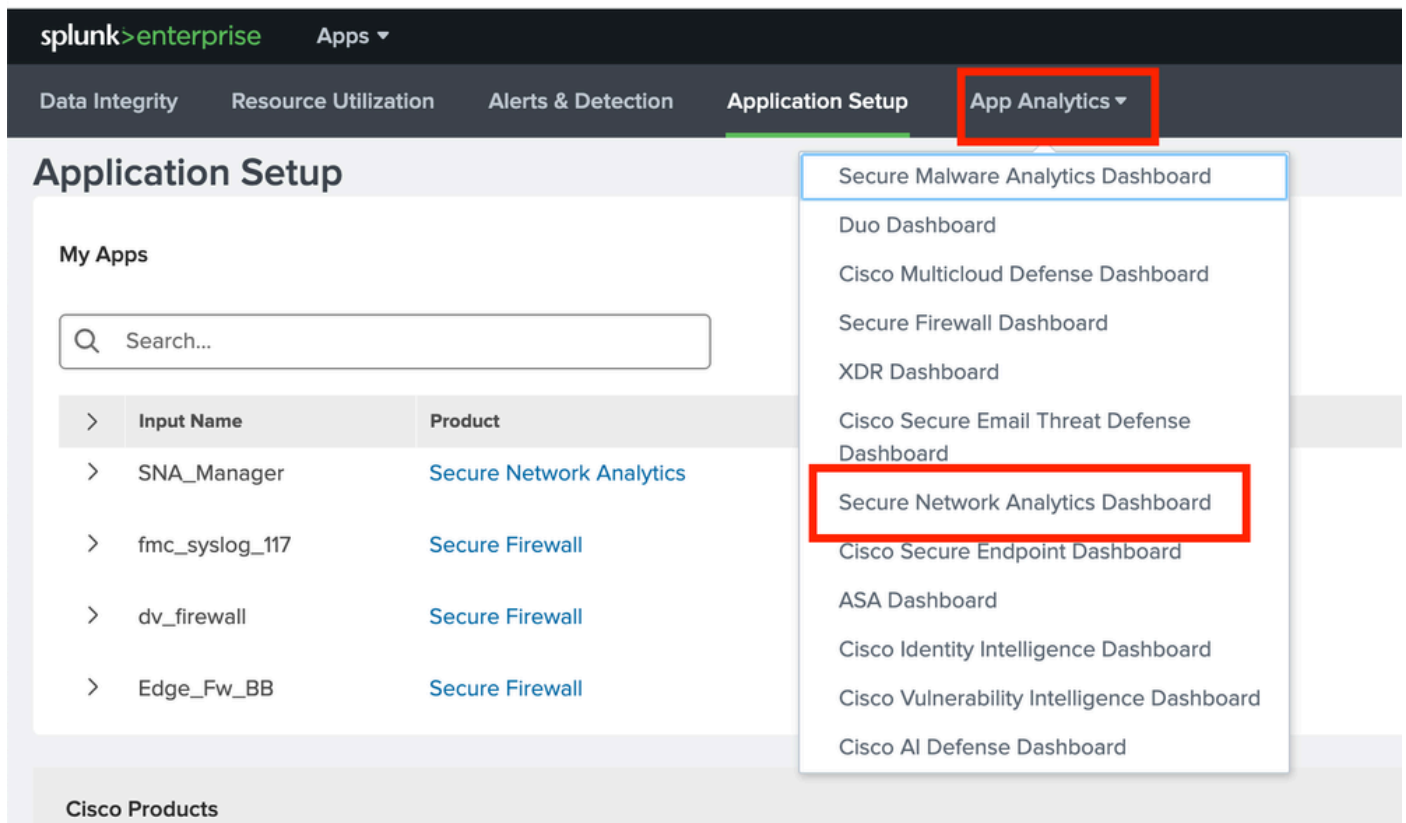
步骤 5：集成验证。

这是一个重要步骤，您需要验证上一步执行的集成是否成功完成。

i.在Application Setup选项卡中，输入的连接状态必须是Connected，对于Input字段中的正确名称，默认值为Enabled。

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.从下拉菜单中选择Secure Network Analytics Dashboard，统计数据最终开始在控制面板上反映。



## 常见问题解答

在哪里可以找到SNA管理器的域ID?

回答：

i. 登录到SNA主管理器并重定向到设备管理页面或访问[管理器IP](#) Index URL。

二、浏览支持部分下的smc文件夹。

← → ↻

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

三。在config文件夹下的domain\_XXX文件夹中打开domain.xml文件。



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

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。