

Integración de SNA para desplegarse mediante la aplicación de nube de seguridad

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Preguntas más Frecuentes](#)

Introducción

Este documento describe la integración de SNA sin problemas con Splunk mediante Cisco Security Cloud para una respuesta más rápida ante incidentes de las amenazas identificadas.

Prerequisites

Conocimientos básicos de Splunk y dispositivos Cisco.

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

Splunk Enterprise

Secure Network Analytics v7.5.2.

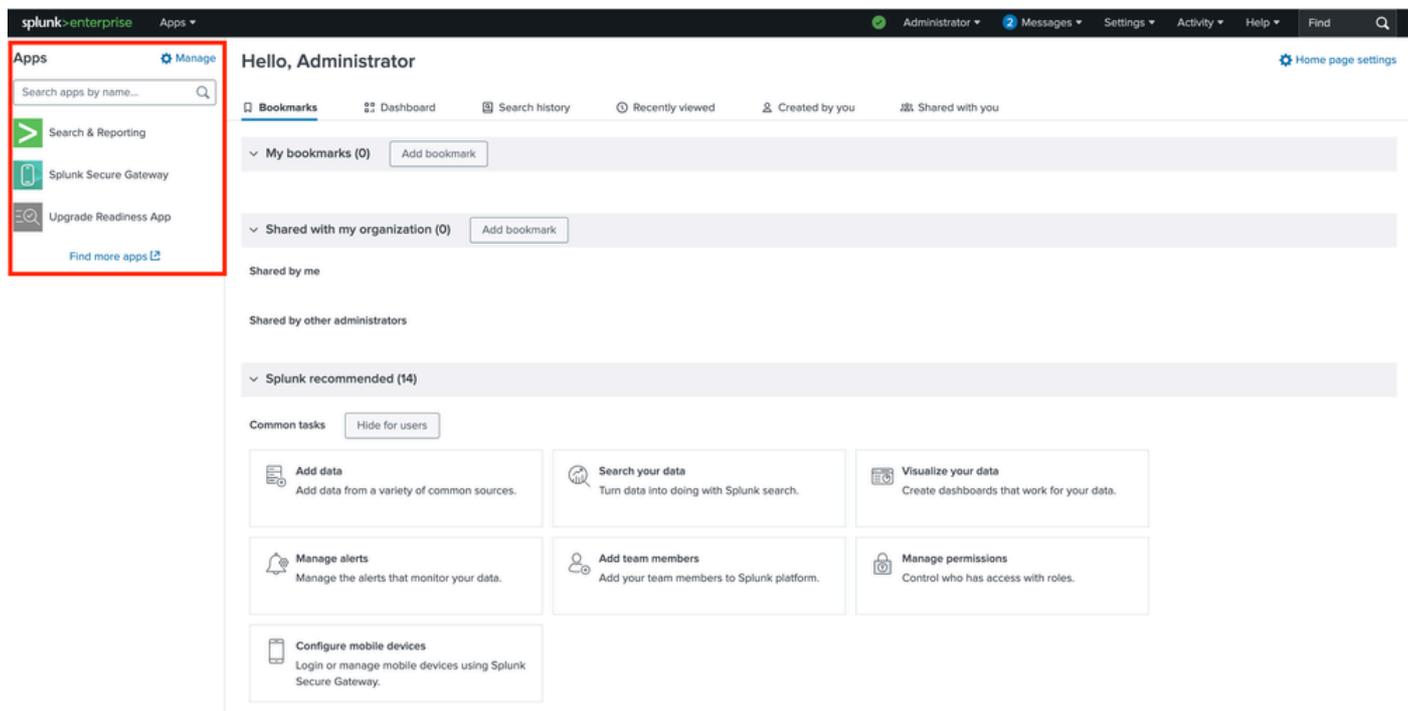
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso 1: Acceda a la aplicación Splunk e instale la aplicación Cisco Security Cloud.

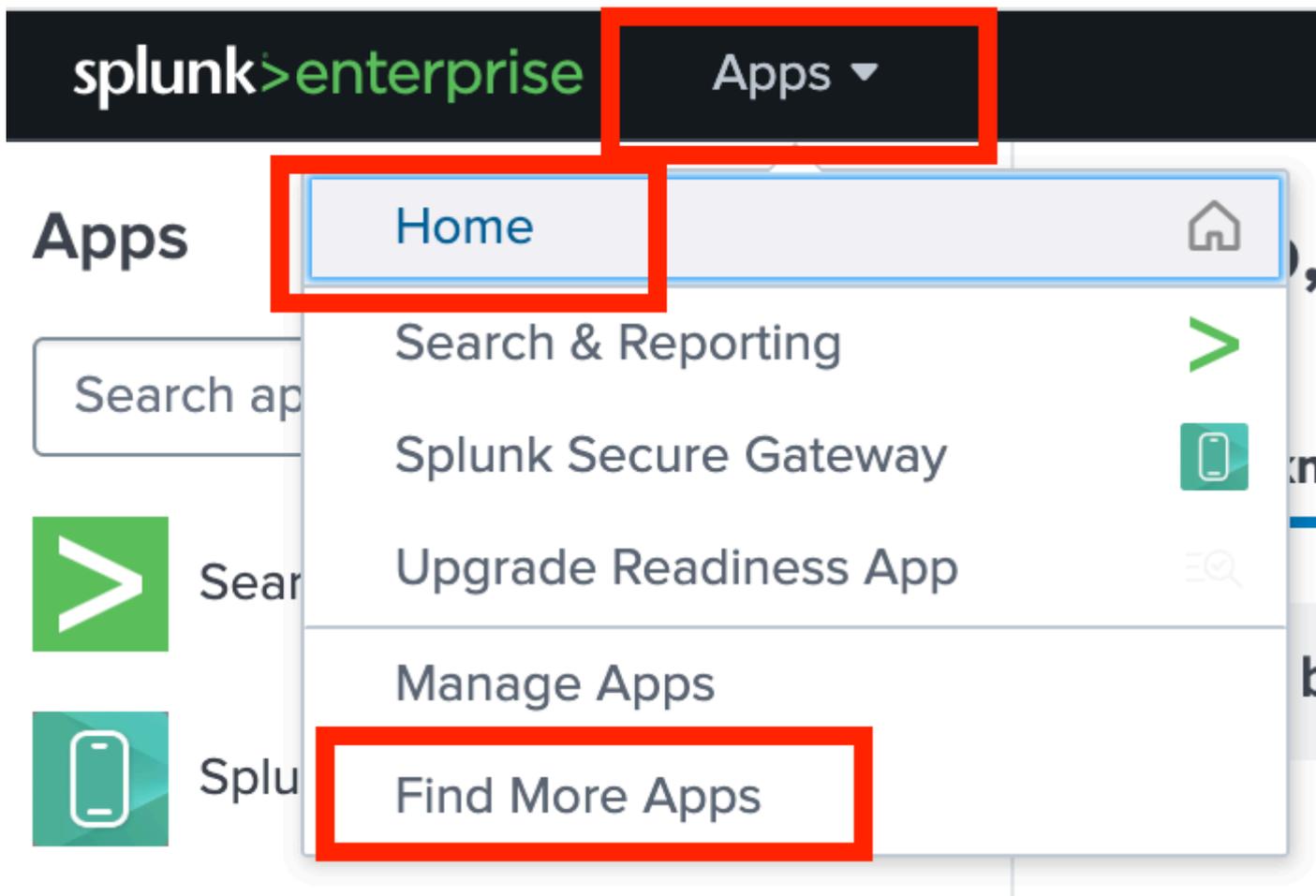
i. Inicie sesión en el portal web de Splunk con las credenciales de administrador y, si inicia sesión

correctamente, la página de inicio se puede ver con la lista de aplicaciones instaladas en el lado izquierdo en la sección Aplicación:

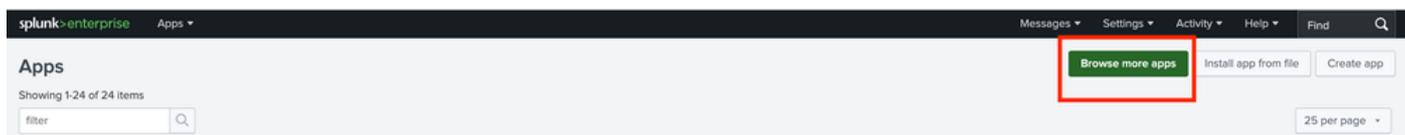


ii. Para integrar el SNA con Splunk, es necesario instalar la aplicación Cisco Security Cloud Application, lo que se puede lograr con cualquiera de los métodos mencionados:

1. Seleccione Find More Apps en el menú desplegable.

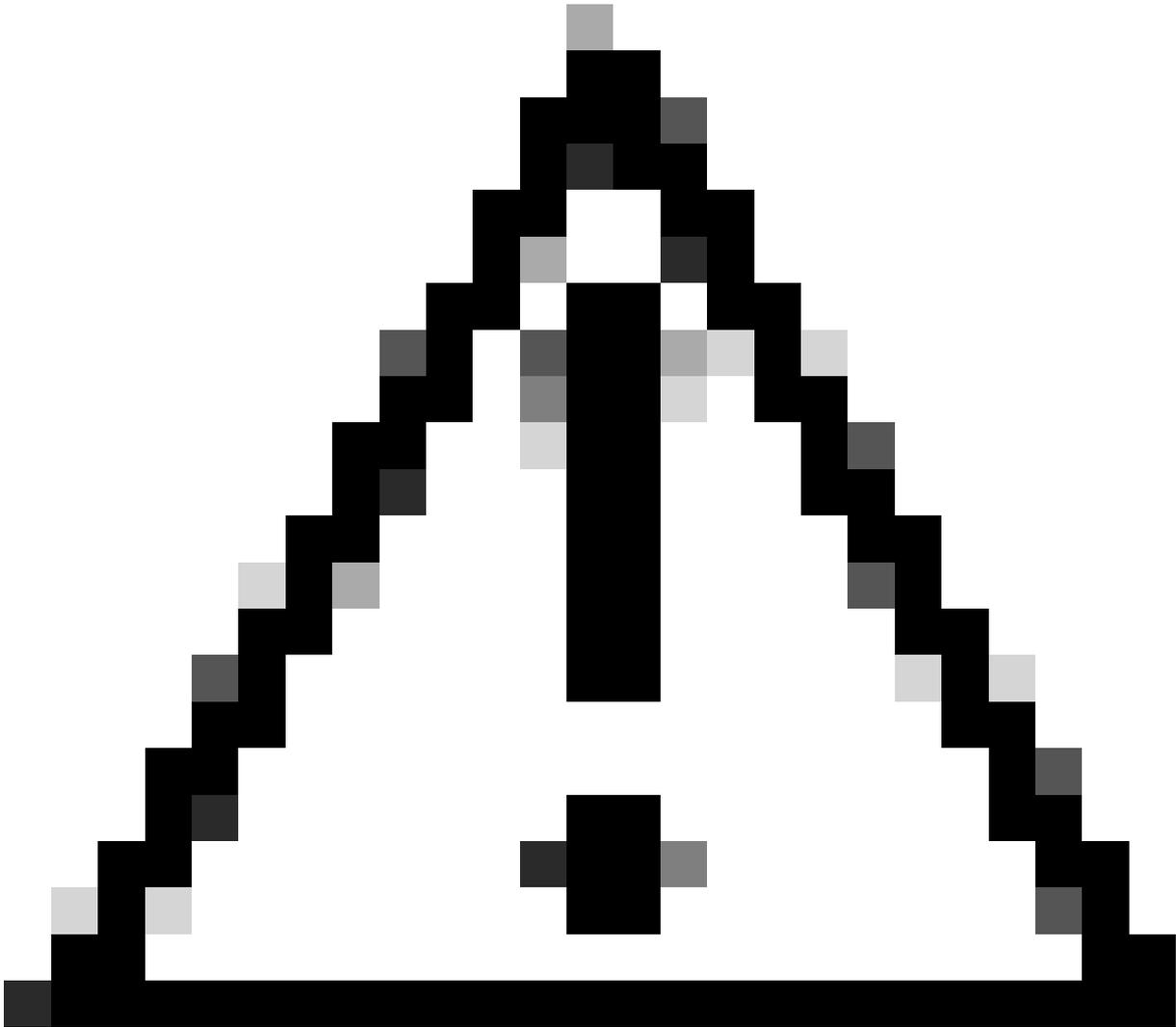


b. Navega por más aplicaciones bajo el icono de equipo de Manager.

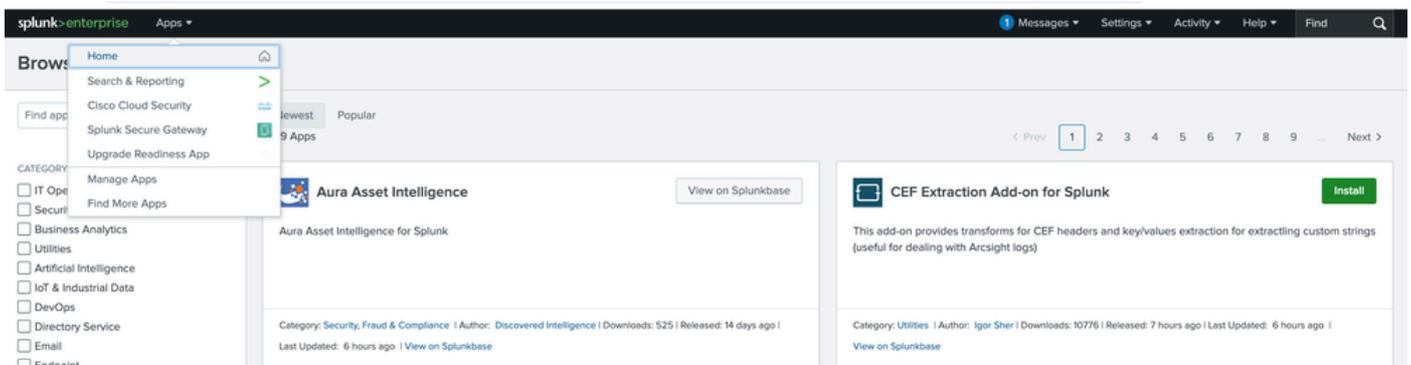


Paso 2: Instalación de la aplicación Cisco Security Cloud.

i. Busque la aplicación Cisco Security Cloud. Ahora, desplácese hacia abajo hasta encontrar la aplicación o busque Cisco security cloud.



Precaución: No se confunda con la aplicación Cisco Cloud Security.



ii. Instale la aplicación haciendo clic en el botón Install.



Cisco Security Cloud

Install

The 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

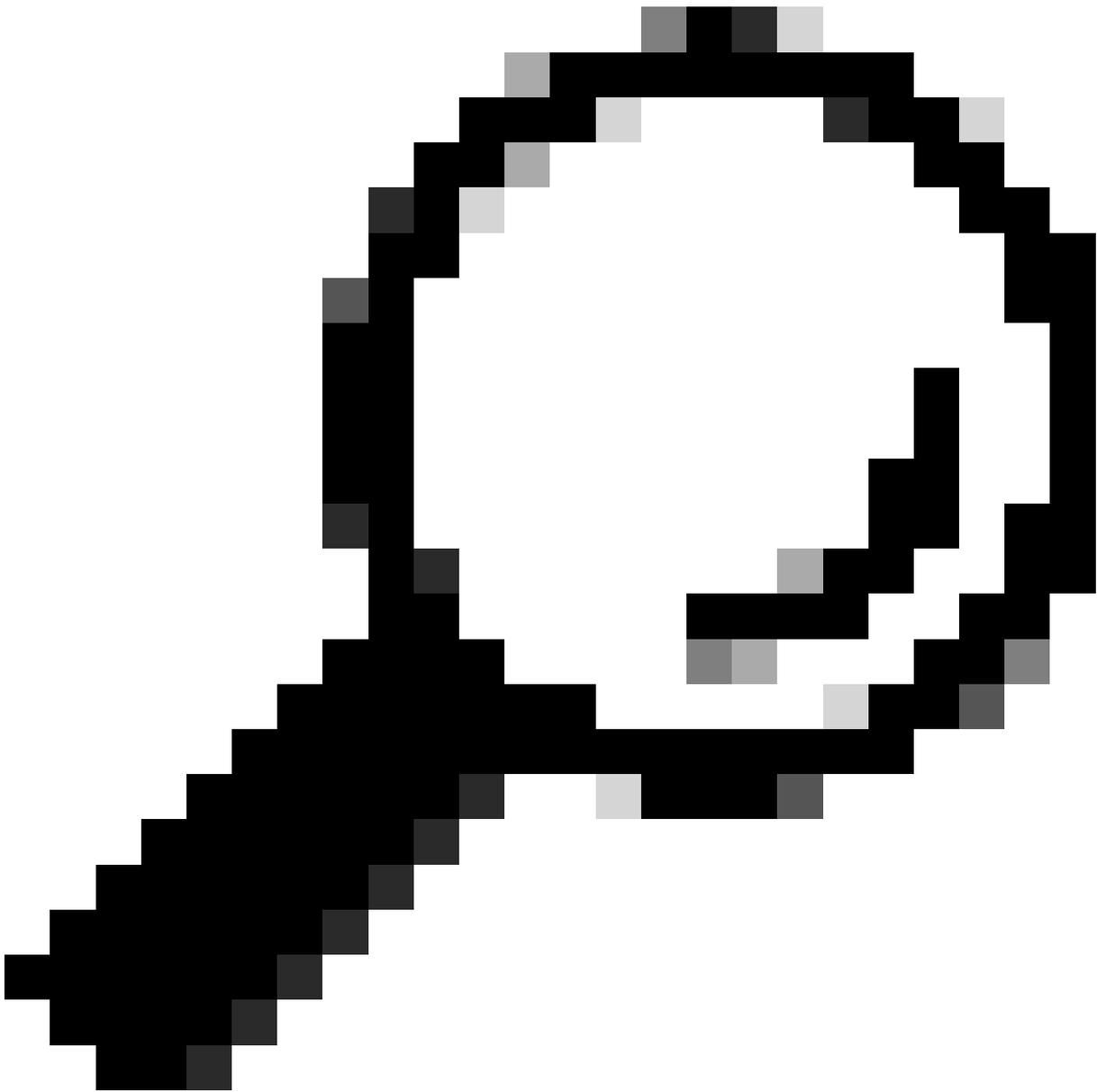
Cisco Email Threat Defense (ETD)

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. Al hacer clic en el botón de instalación, aparece una ventana que le solicita las credenciales de la cuenta Splunk antes de instalar la aplicación. Proporcione las credenciales y haga clic en Aceptar e instalar para continuar.



Consejo: Proporcione las credenciales que se utilizan para acceder al portal Splunk, no las credenciales de administrador que se utilizan para la aplicación empresarial Splunk al iniciar sesión.

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](#).

iv. Aparece un mensaje cuando la instalación de la aplicación se realiza correctamente, como se muestra en la imagen. Haga clic en Done (Listo).

Complete



Cisco Security Cloud was successfully installed.

Open the App

Go Home

Done

Paso 3: Verificación de la instalación de la aplicación Cisco Security Cloud.

i. Haga clic en la opción desplegable Apps, y ahora la aplicación se puede ver en la lista después de la instalación exitosa:

Browse

cisco

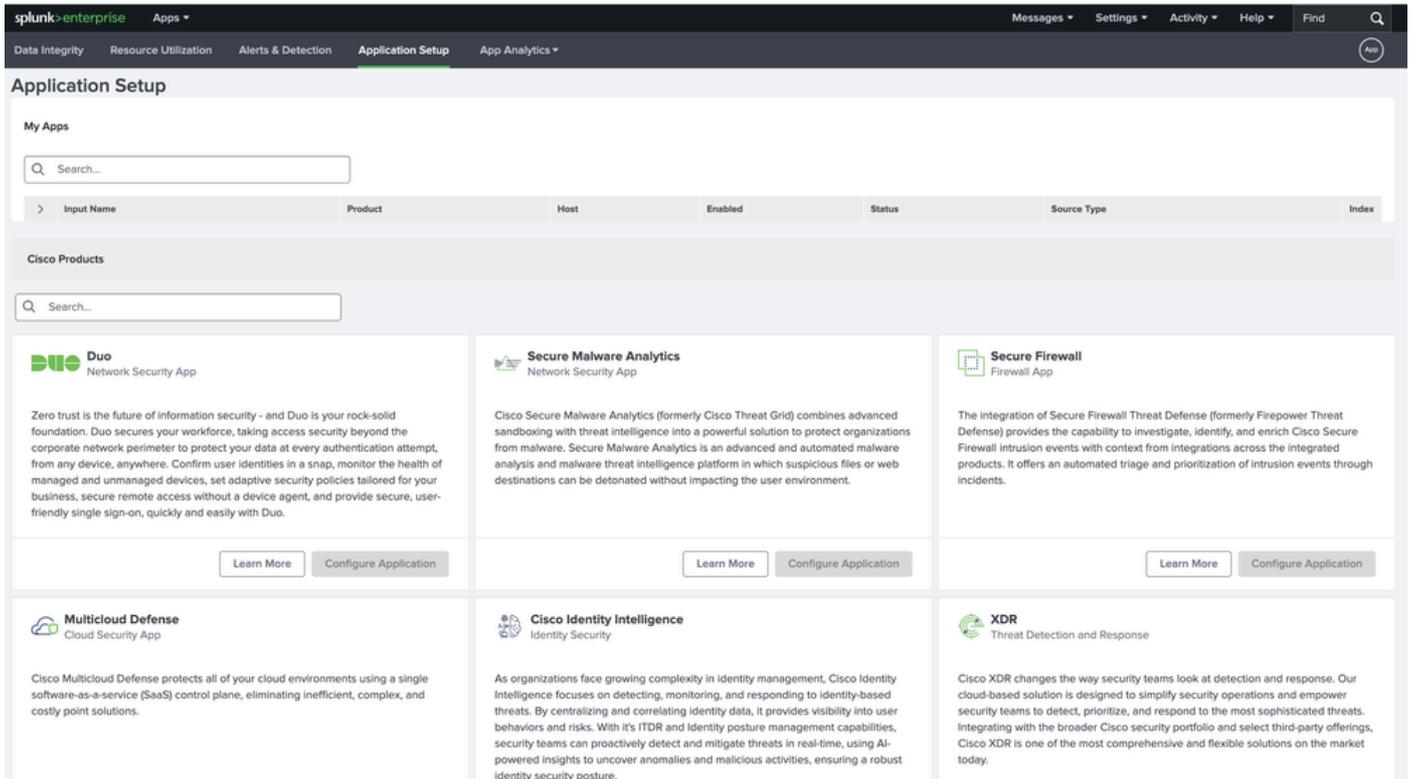
CATEGORY

 IT Oper Securiti Busine UtilitiesHome Search & Reporting ~~Cisco Cloud Security~~ Cisco Security Cloud Splunk Secure Gateway Upgrade Readiness App 

Manage Apps

Find More Apps

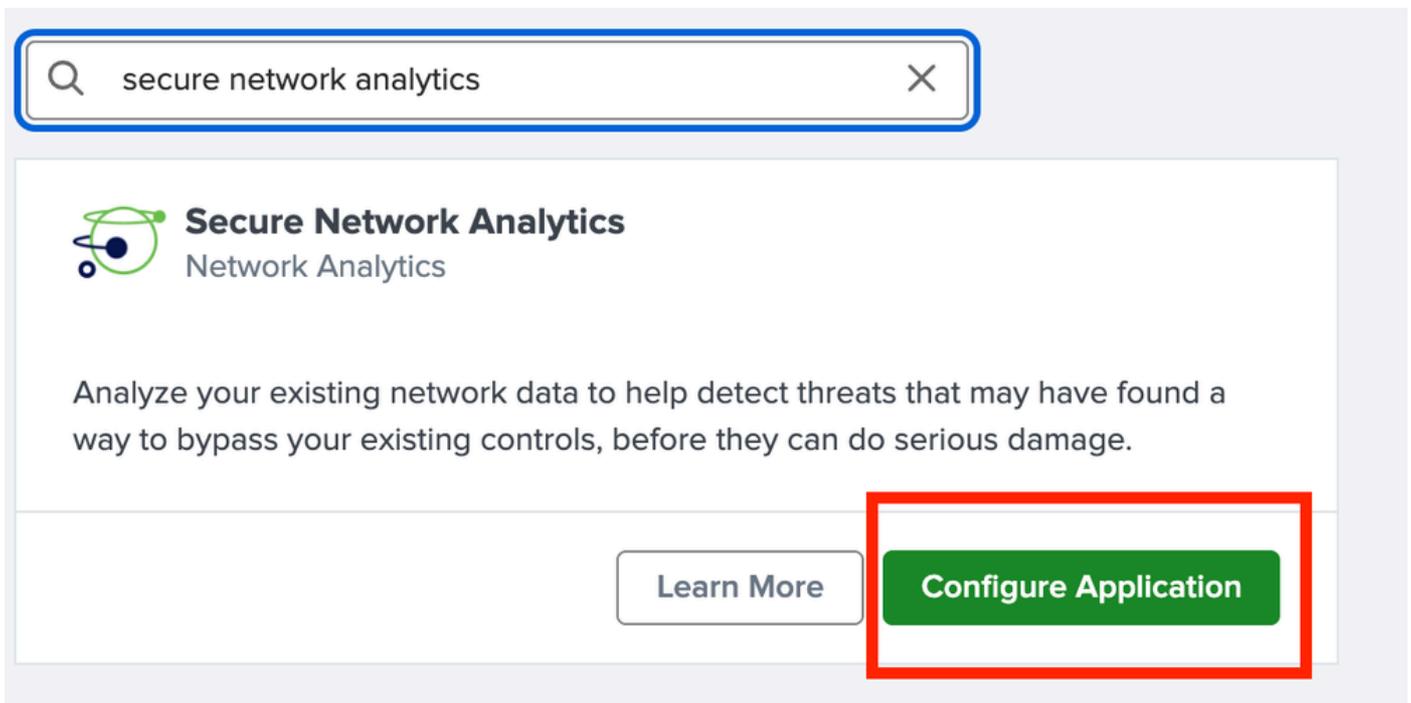
ii. Haga clic en Cisco Security Cloud para seleccionarla. Se le redirige a la página Application Setup, donde se pueden encontrar todos los productos de seguridad para la nube de Cisco disponibles.



Paso 4: Integración con Secure Network Analytics (SNA).

El objetivo de este documento es destacar los pasos de instalación de Splunk con Secure Network Analytics (SNA) que se mencionan más adelante.

i. Busque Secure Network Analytics y cuando aparezca, seleccione Configure Application:



ii. Al seleccionar la opción de configuración, aparece la página de configuración para que los detalles se agreguen.

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

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. Rellene todos los detalles obligatorios mencionados para los detalles de conexión SNA:

1. Nombre de entrada: cualquier nombre único para SNA
2. Dirección del jefe (dirección IPv4 o IPv6 o nombre de host): IP de administración del administrador SNA principal
3. ID de dominio: introduzca el valor correspondiente a domain_ID (por ejemplo, 301).
4. Nombre de usuario: El nombre de usuario del administrador principal (por ejemplo, admin)
5. Contraseña Contraseña del usuario del jefe principal

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. Deje los valores predeterminados del resto de la configuración o modifíquelos según sea necesario y, a continuación, haga clic en Save. Aparece un mensaje de éxito en la pantalla después de la finalización.

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

Paso 5: Verificación de la integración.

Se trata de un paso importante en el que debe comprobar si la integración ejecutada en el paso anterior se ha realizado correctamente o no.

i. El estado de conexión de la entrada debe ser Connected en la ficha Application Setup con el valor predeterminado Enabled para el nombre correcto en el campo Input.

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. Seleccione el panel Secure Network Analytics del menú desplegable y las estadísticas comenzarán a reflejarse en el panel.

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

splunk>enterprise Apps ▾ Administrator Messages Settings Activity Help Find

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

Secure Network Analytics Dashboard

Security Insights Network Insights **Ingestion Insights**

Time Range: Last 24 hours Index: All (1)

Max 95th percentile flows per second	Flow Records Analyzed	Internal traffic occurring on your network	Traffic exchanged between your network and the Internet	Encrypted traffic exchanged between your network and the Internet
166	1.1M	721.4 GB	359.6 GB	304.1 GB

Internal Monitored Network
Hosts communicating within your network

1.6K

Hosts Count

Flow Rate (fps)

Flow Rate (fps)

8:00 AM Mon Jun 23 2025 12:00 PM 4:00 PM 8:00 PM 12:00 AM Tue Jun 24 4:00 AM

fc752 fccds741

Preguntas más Frecuentes

¿Dónde se encuentra el ID de dominio para el administrador SNA?

Respuesta:

i. Inicie sesión en el administrador principal SNA y redirija a la página de administración del

dispositivo o acceda a la URL [Índice IP del administrador](#).

ii. Busque la carpeta smc en la sección Soporte.

The screenshot shows the Manager VE interface with a 'Browse Files' section. The left sidebar contains a 'Support' menu item, which is highlighted with a red box. The main content area displays a table of files and folders. The 'smc' folder is highlighted with a red box in the table.

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. Abra el archivo domain.xml disponible en la carpeta domain_XXX en la carpeta config.

- 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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).