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

Contenido

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.

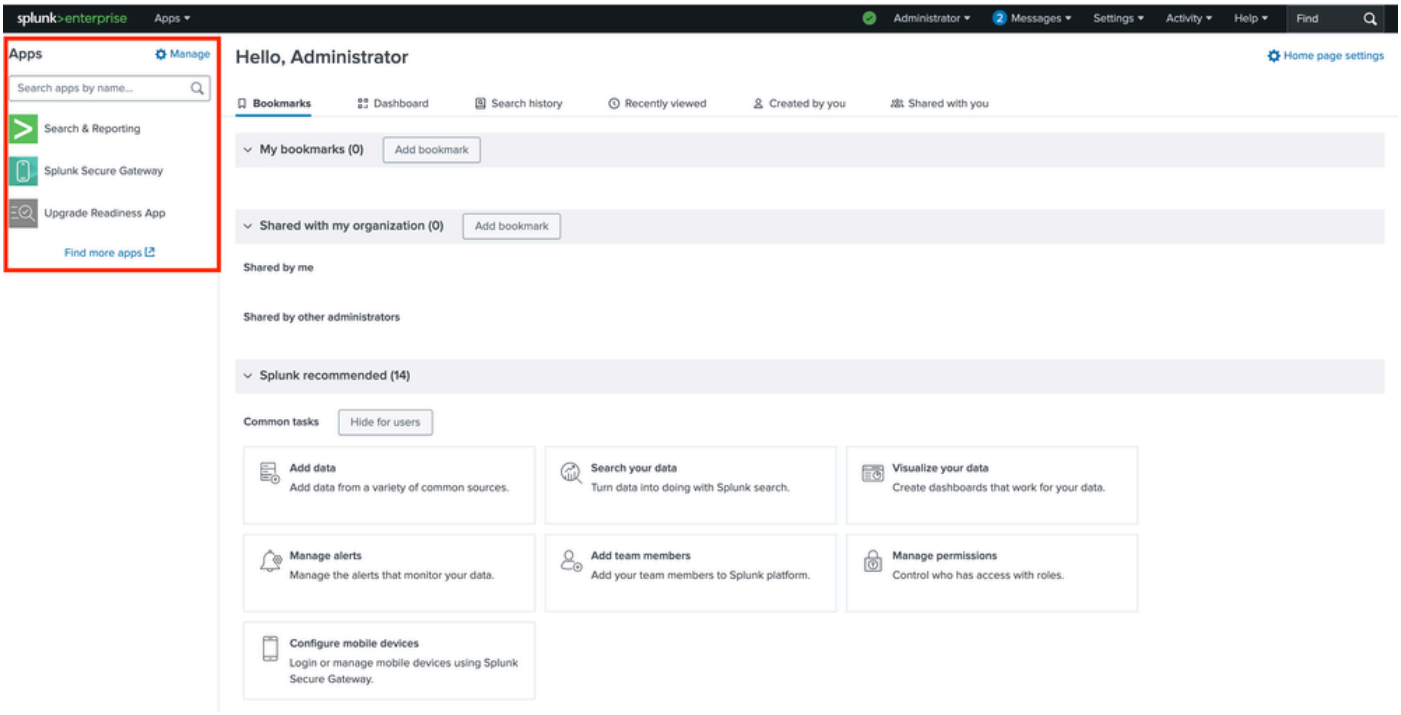
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Configurar

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

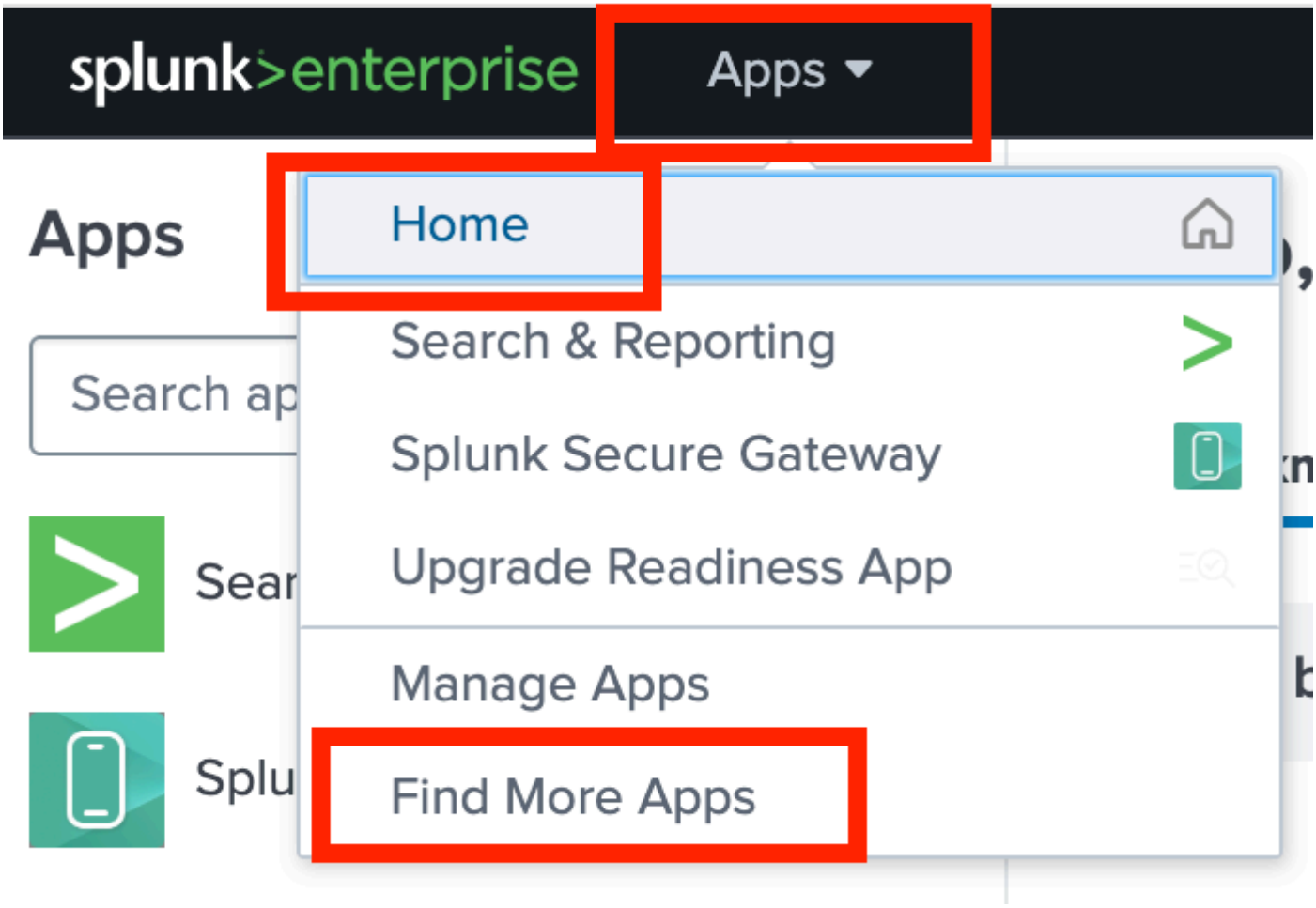
i. Inicie sesión en el portal web de Splunk con las credenciales de administrador y, si inicia sesión

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

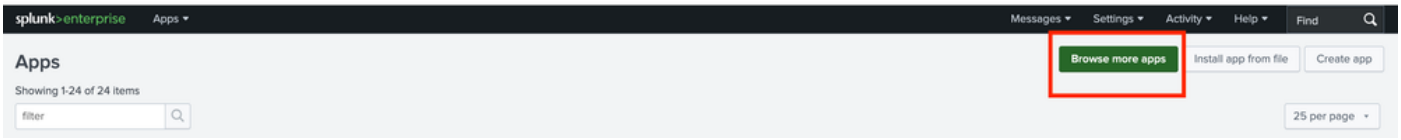


ii. Para integrar el SNA con Splunk, es necesario instalar la aplicación Cisco Security Cloud Application, lo que se puede lograr con cualquiera de los métodos mencionados:

1. Seleccione Find More Apps en el menú desplegable.



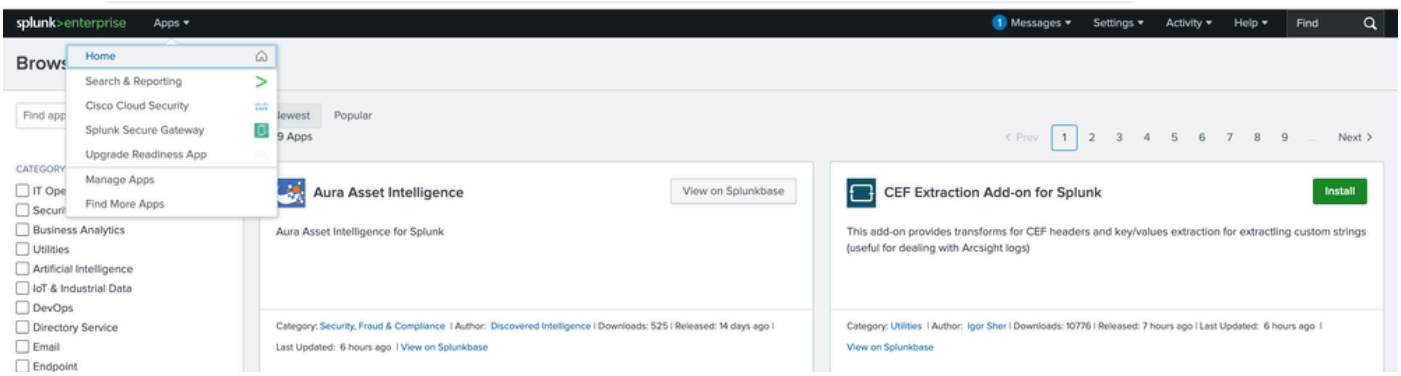
b. Navega por más aplicaciones bajo el icono de equipo de Manager.



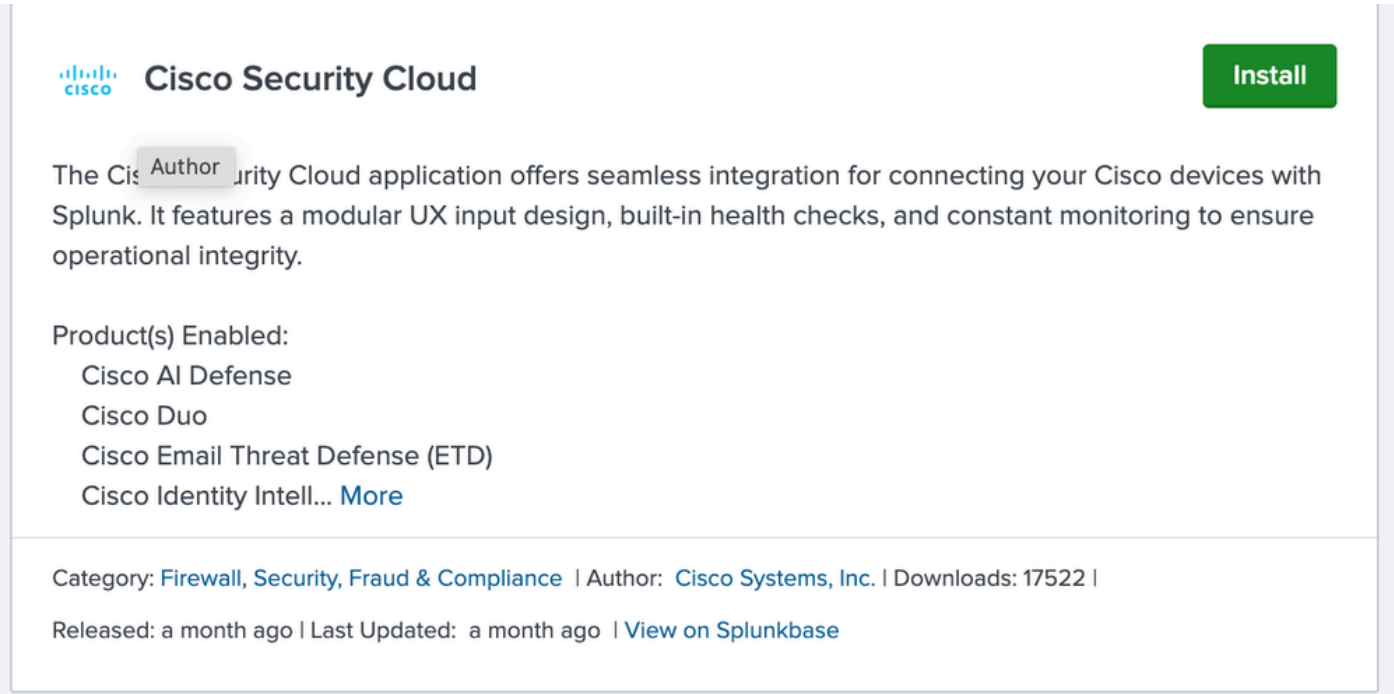
Paso 2: Instalación de la aplicación Cisco Security Cloud.

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

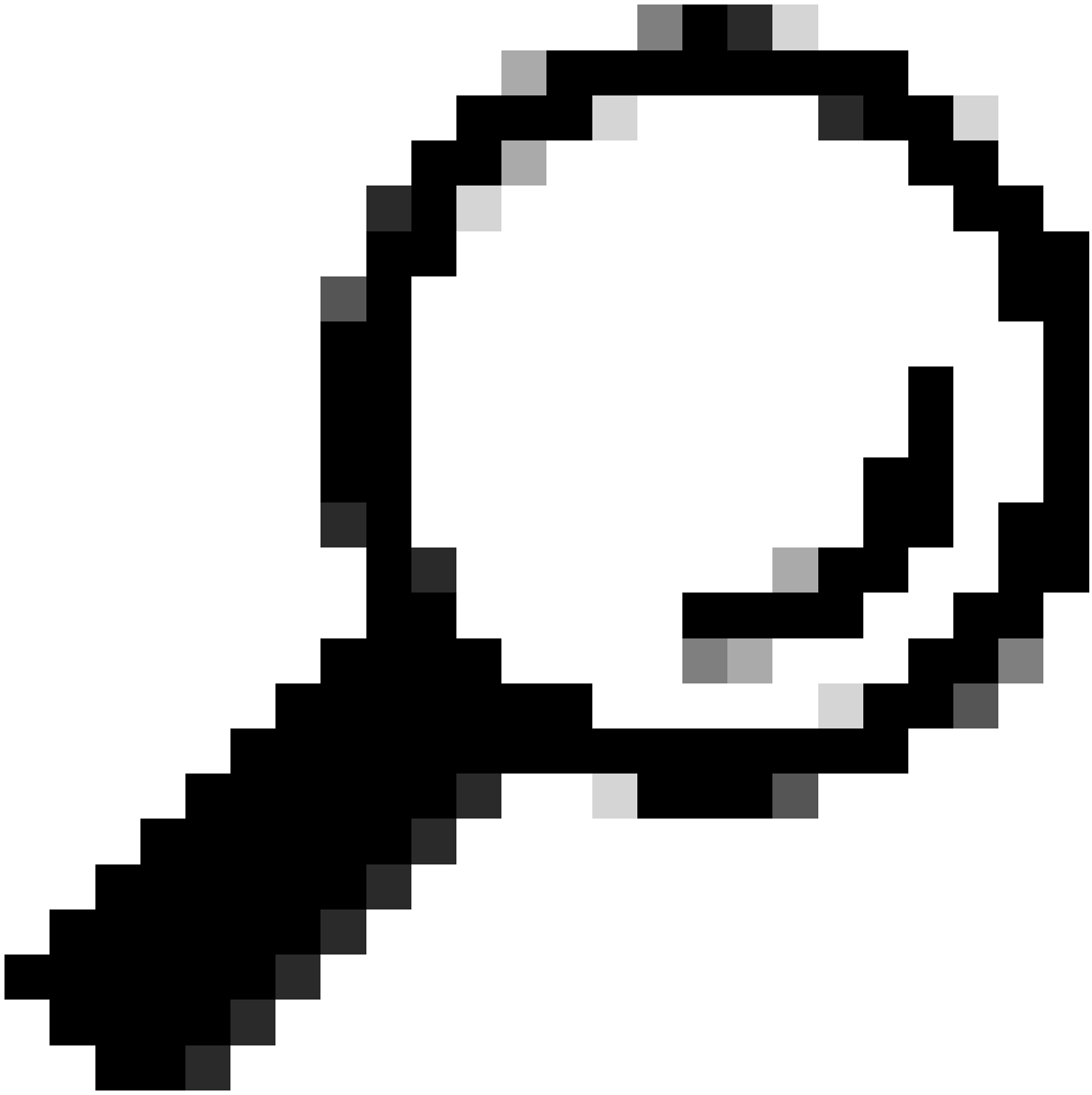
Precaución: No se confunda con la aplicación Cisco Cloud Security.



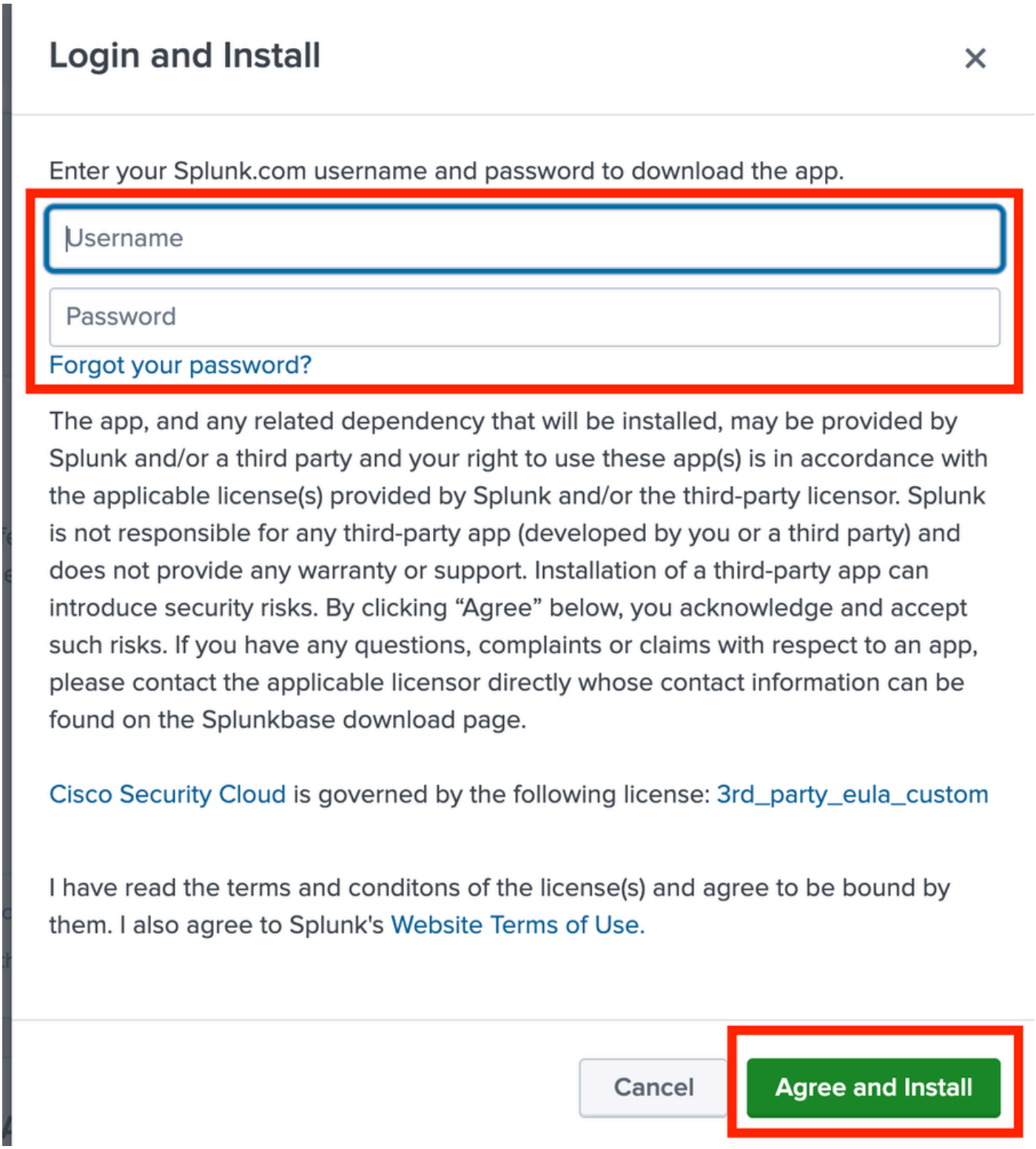
ii. Instale la aplicación haciendo clic en el botón Install.



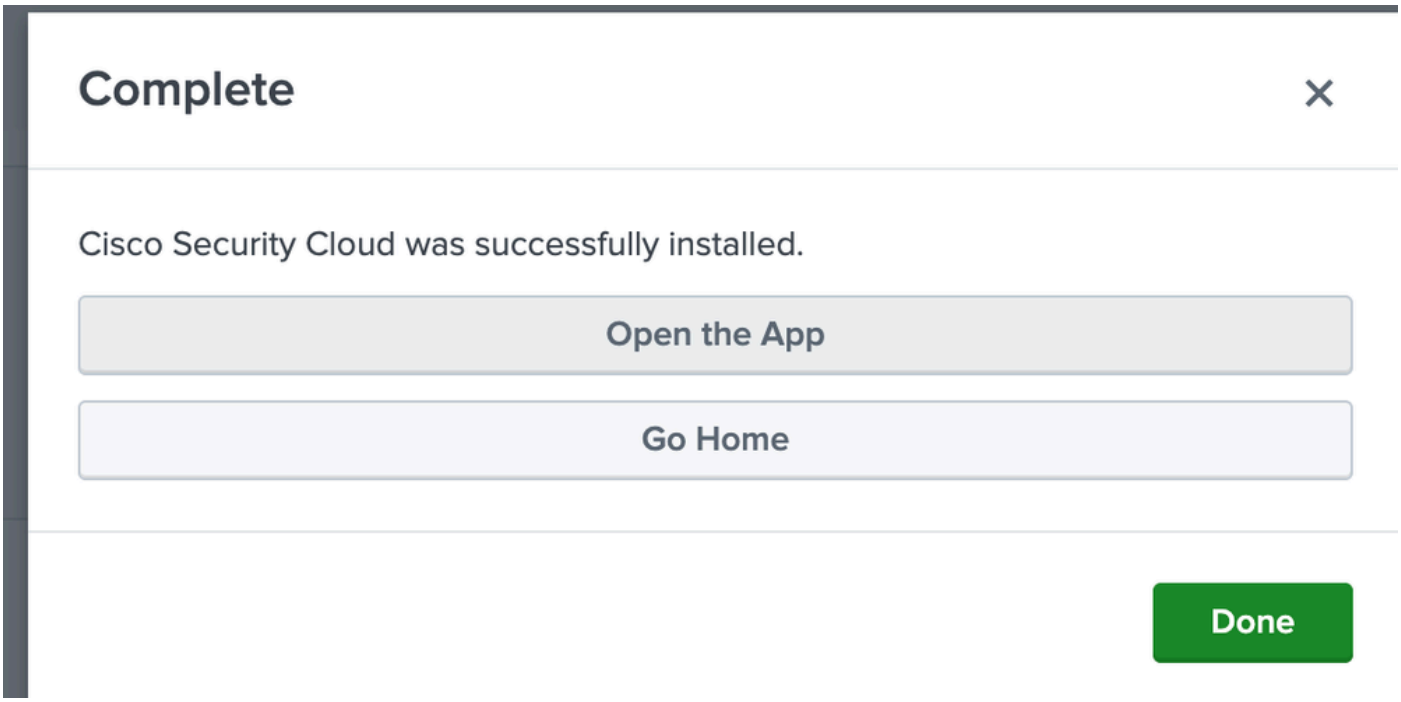
iii. Al hacer clic en el botón de instalación, aparece una ventana que le solicita las credenciales de la cuenta Splunk antes de instalar la aplicación. Proporcione las credenciales y haga clic en Aceptar e instalar para continuar.



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.

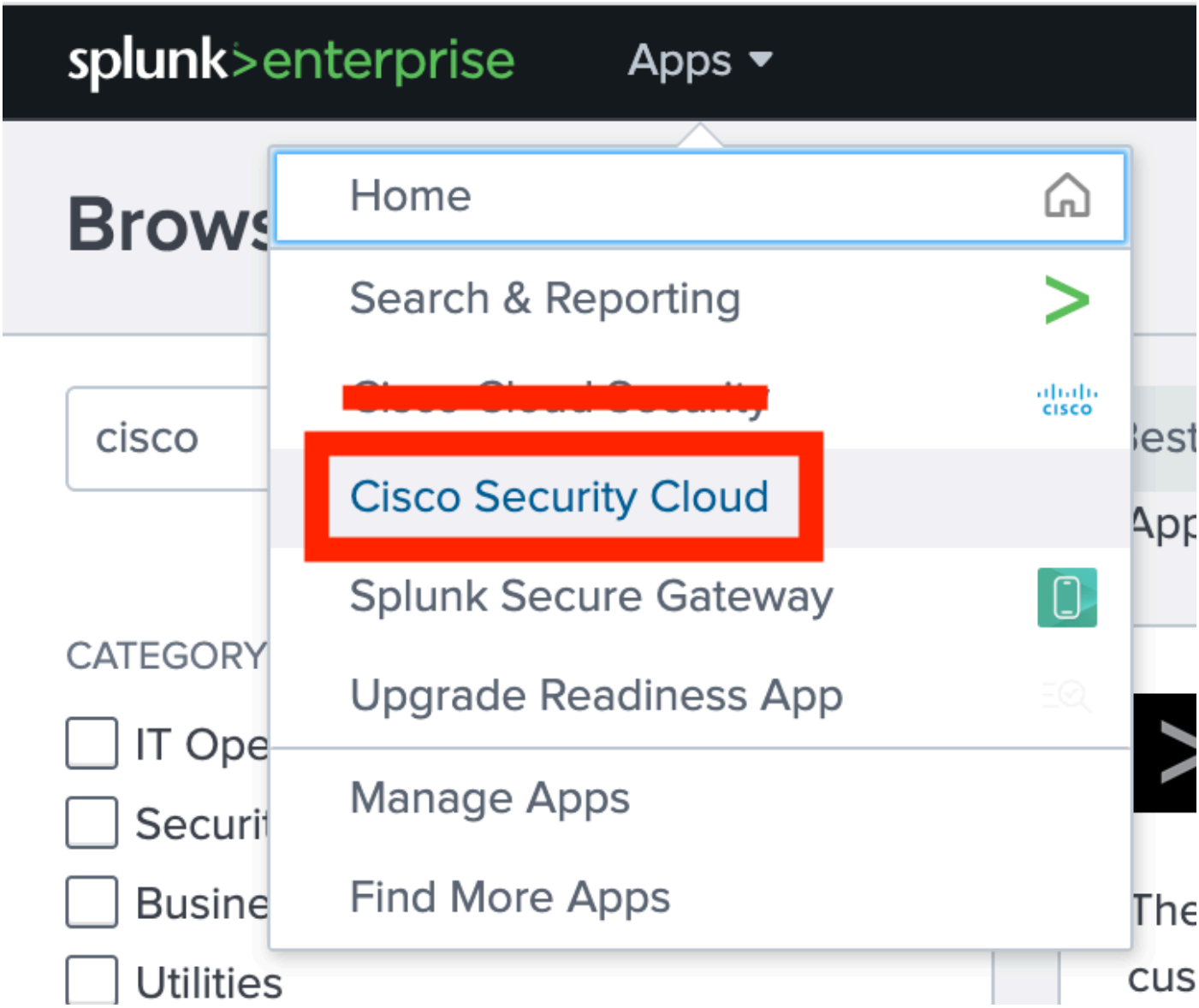


iv. Aparece un mensaje cuando la instalación de la aplicación se realiza correctamente, como se muestra en la imagen. Haga clic en Done (Listo).

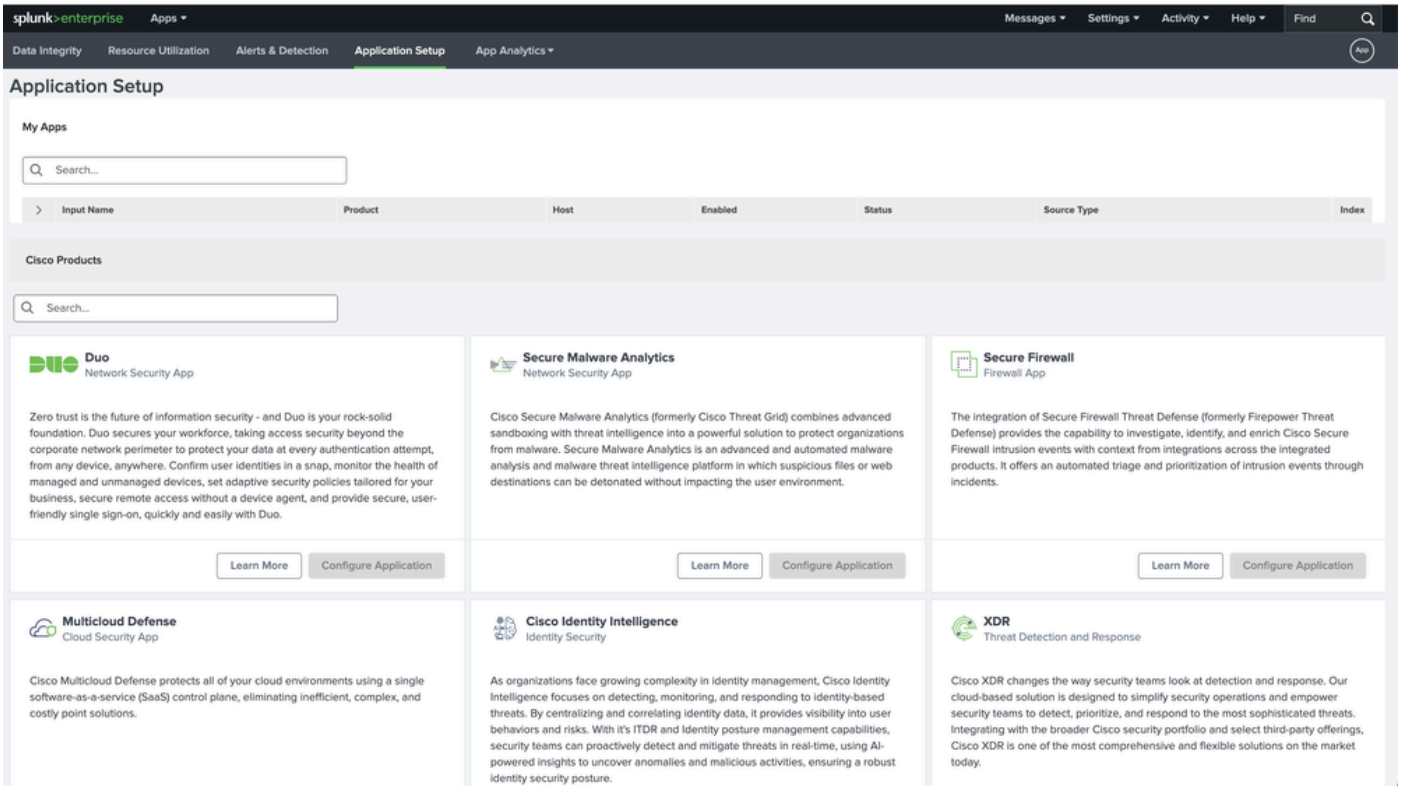


Paso 3: Verificación de la instalación de la aplicación Cisco Security Cloud.

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



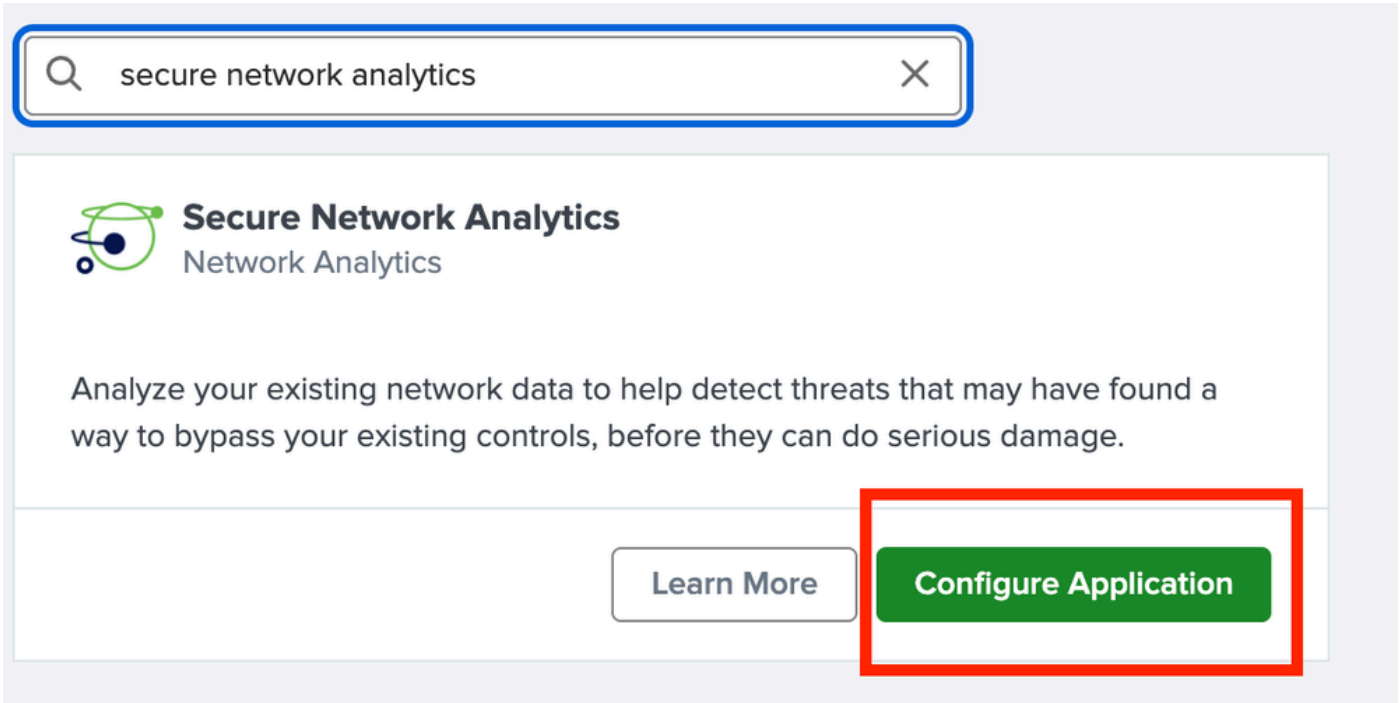
ii. Haga clic en Cisco Security Cloud para seleccionarla. Se le redirige a la página Application Setup, donde se pueden encontrar todos los productos de seguridad para la nube de Cisco disponibles.



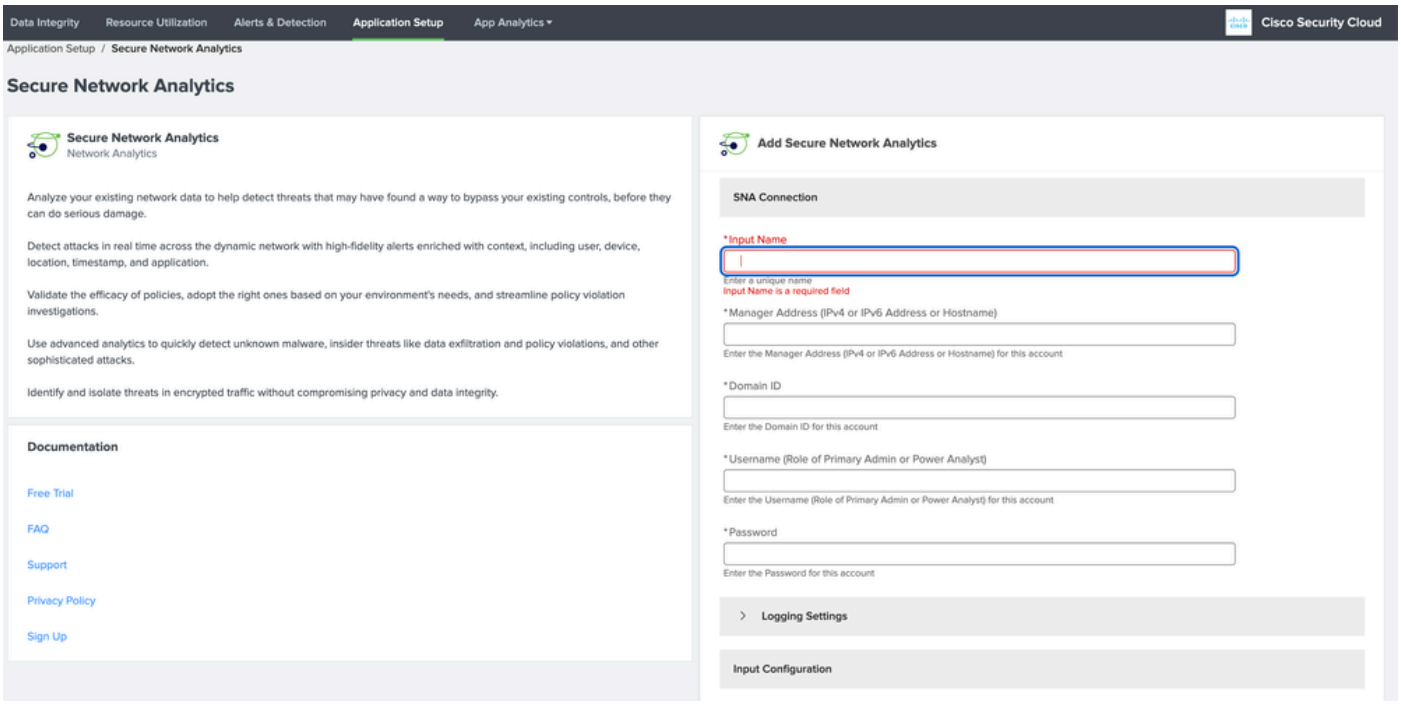
Paso 4: Integración con Secure Network Analytics (SNA).

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:

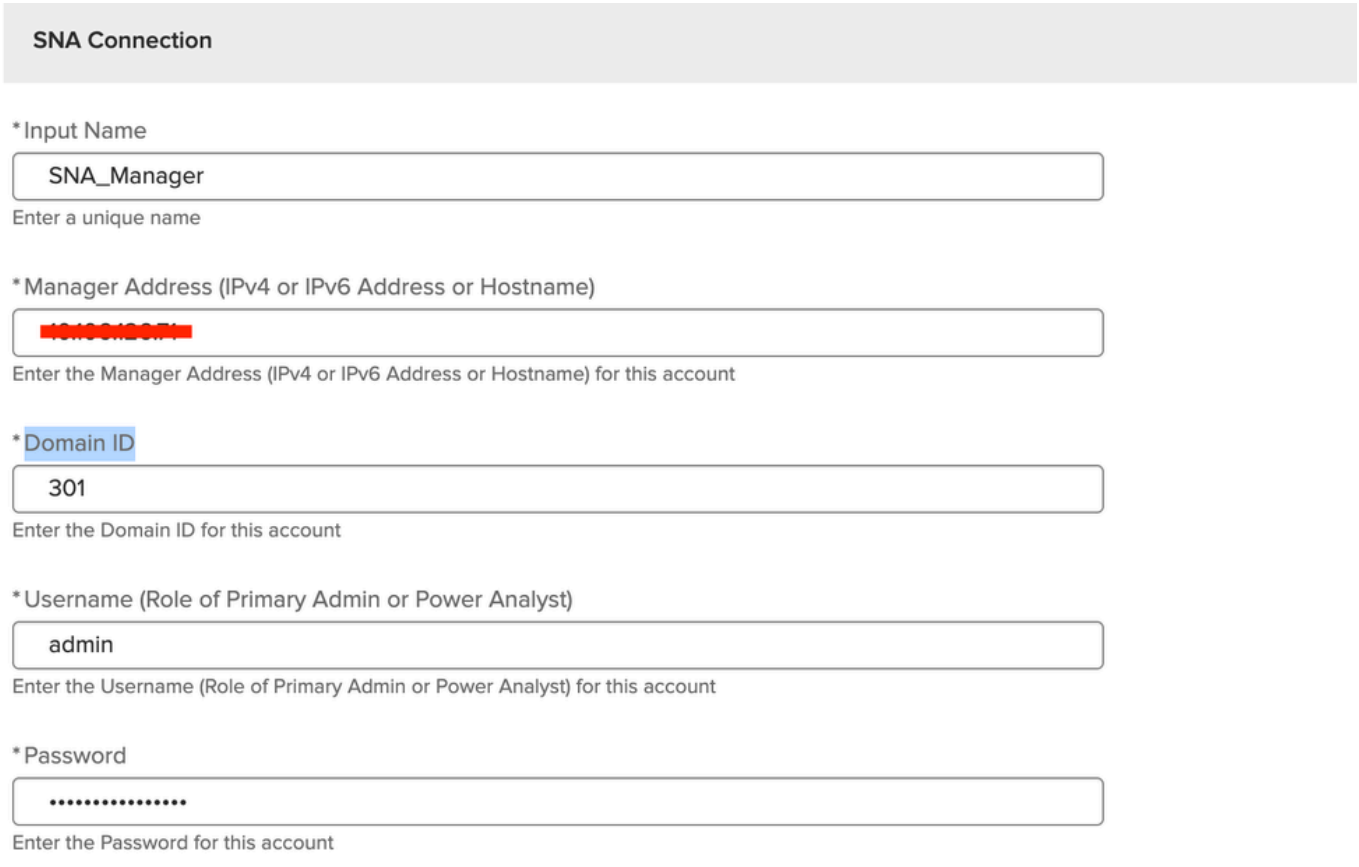


ii. Al seleccionar la opción de configuración, aparece la página de configuración para que los detalles se agreguen.

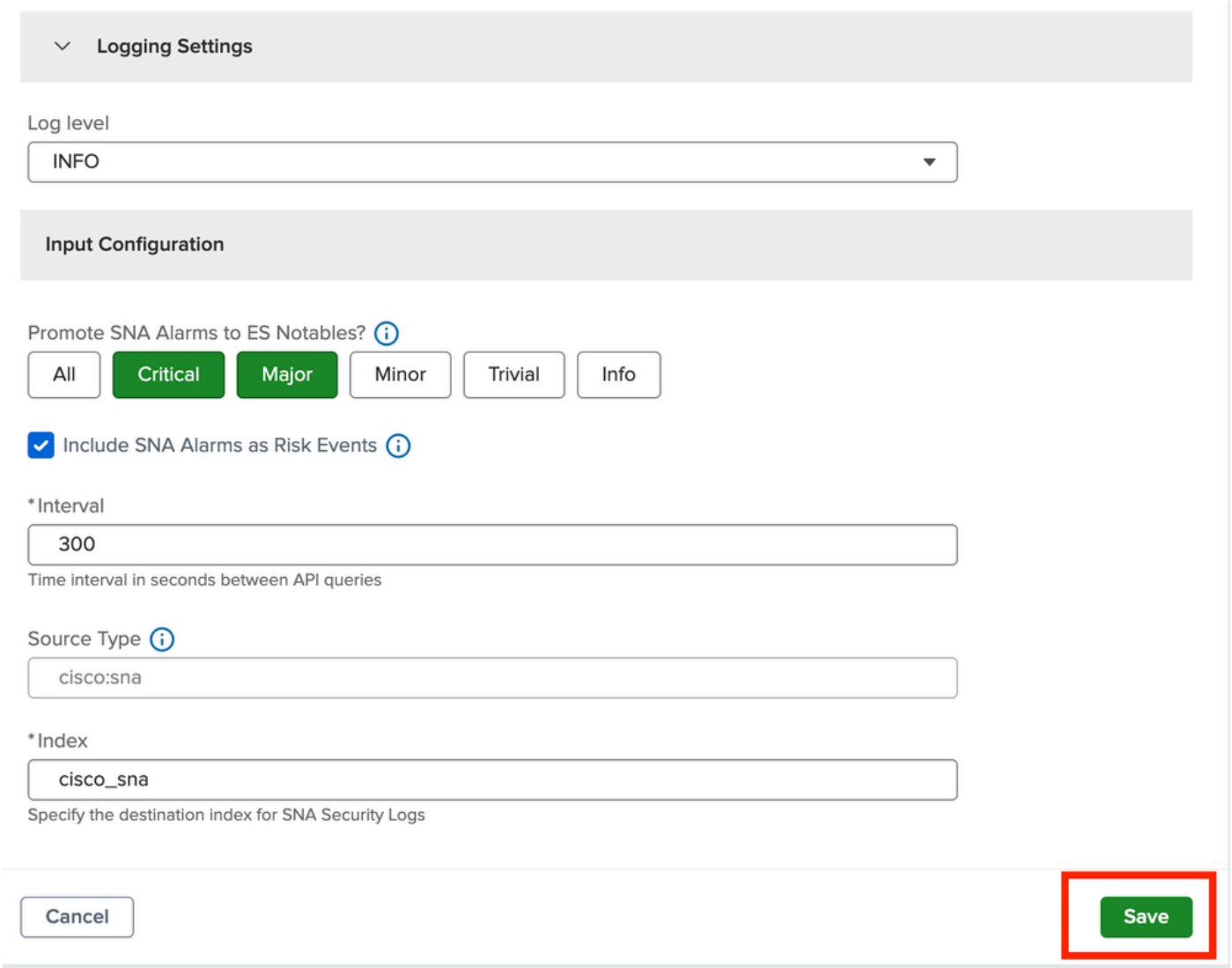


iii. Rellene todos los detalles obligatorios mencionados para los detalles de conexión SNA:

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



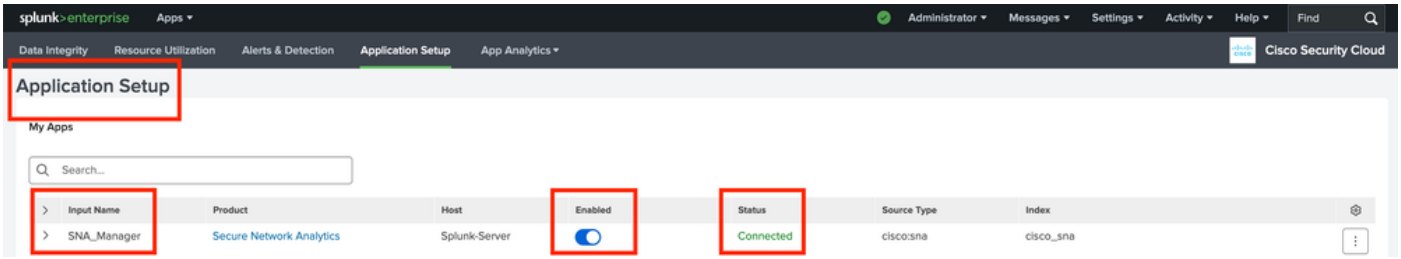
iv. Deje los valores predeterminados del resto de la configuración o modifíquelos según sea necesario y, a continuación, haga clic en Save. Aparece un mensaje de éxito en la pantalla después de la finalización.



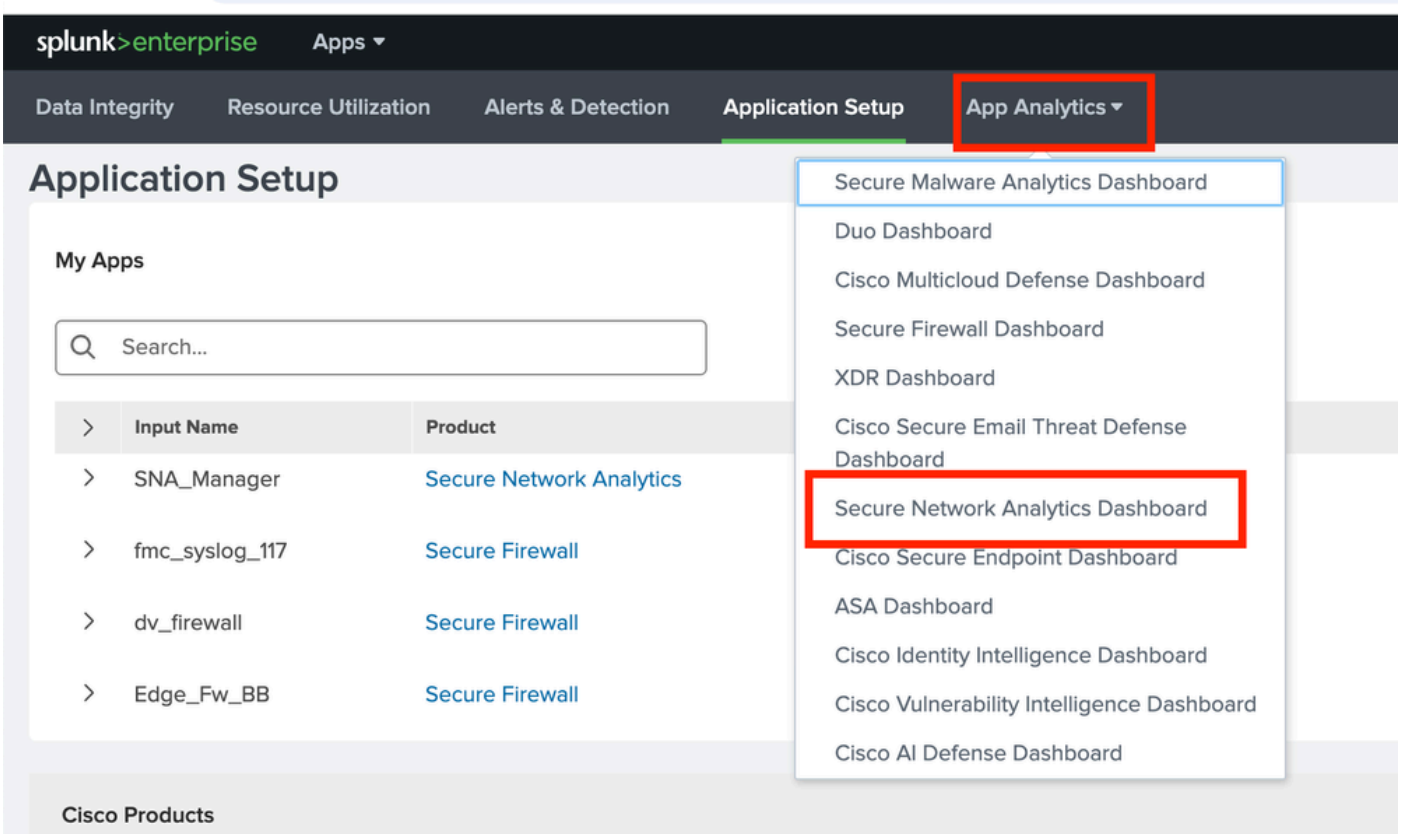
Paso 5: Verificación de la integración.

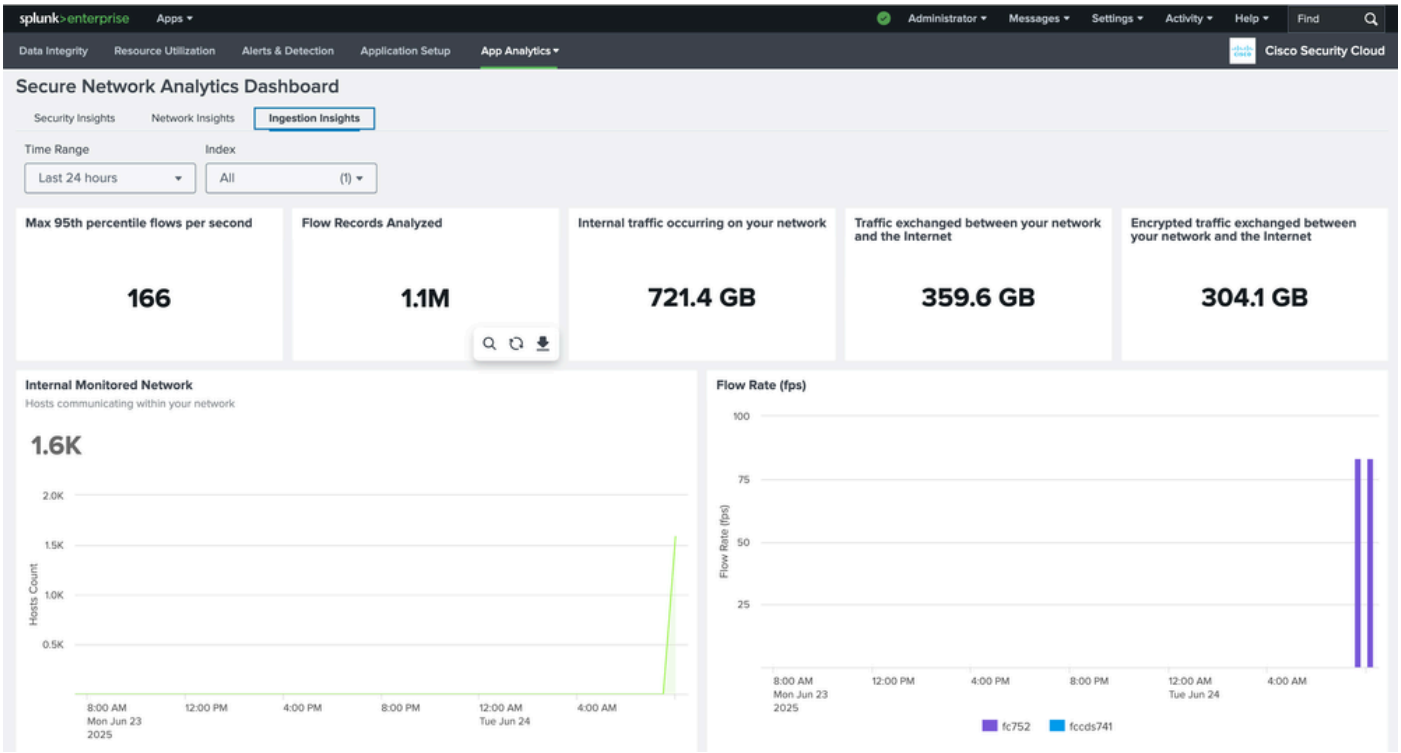
Se trata de un paso importante en el que debe comprobar si la integración ejecutada en el paso anterior se ha realizado correctamente o no.

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.



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





Preguntas más Frecuentes

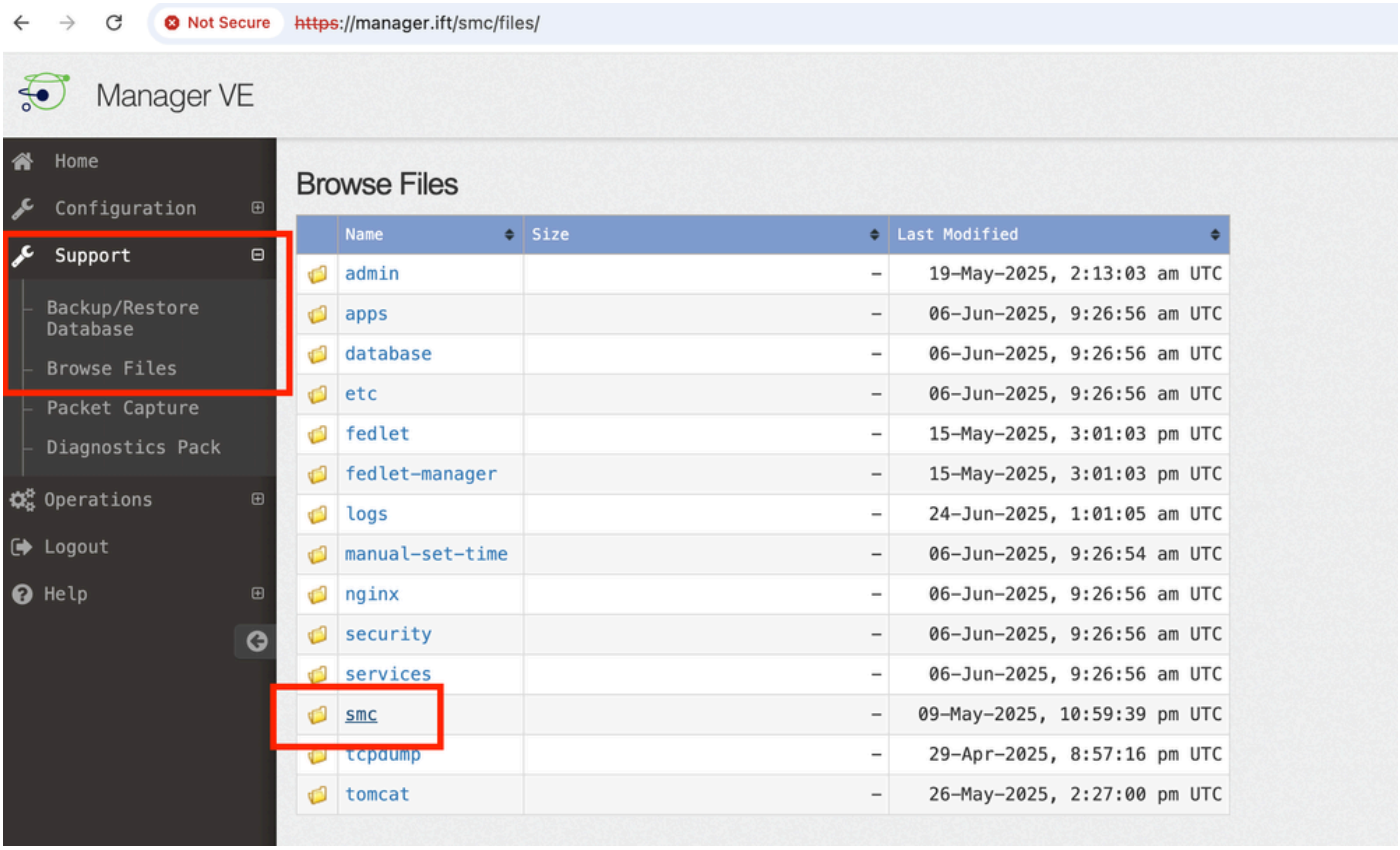
¿Dónde se encuentra el ID de dominio para el administrador SNA?

Respuesta:

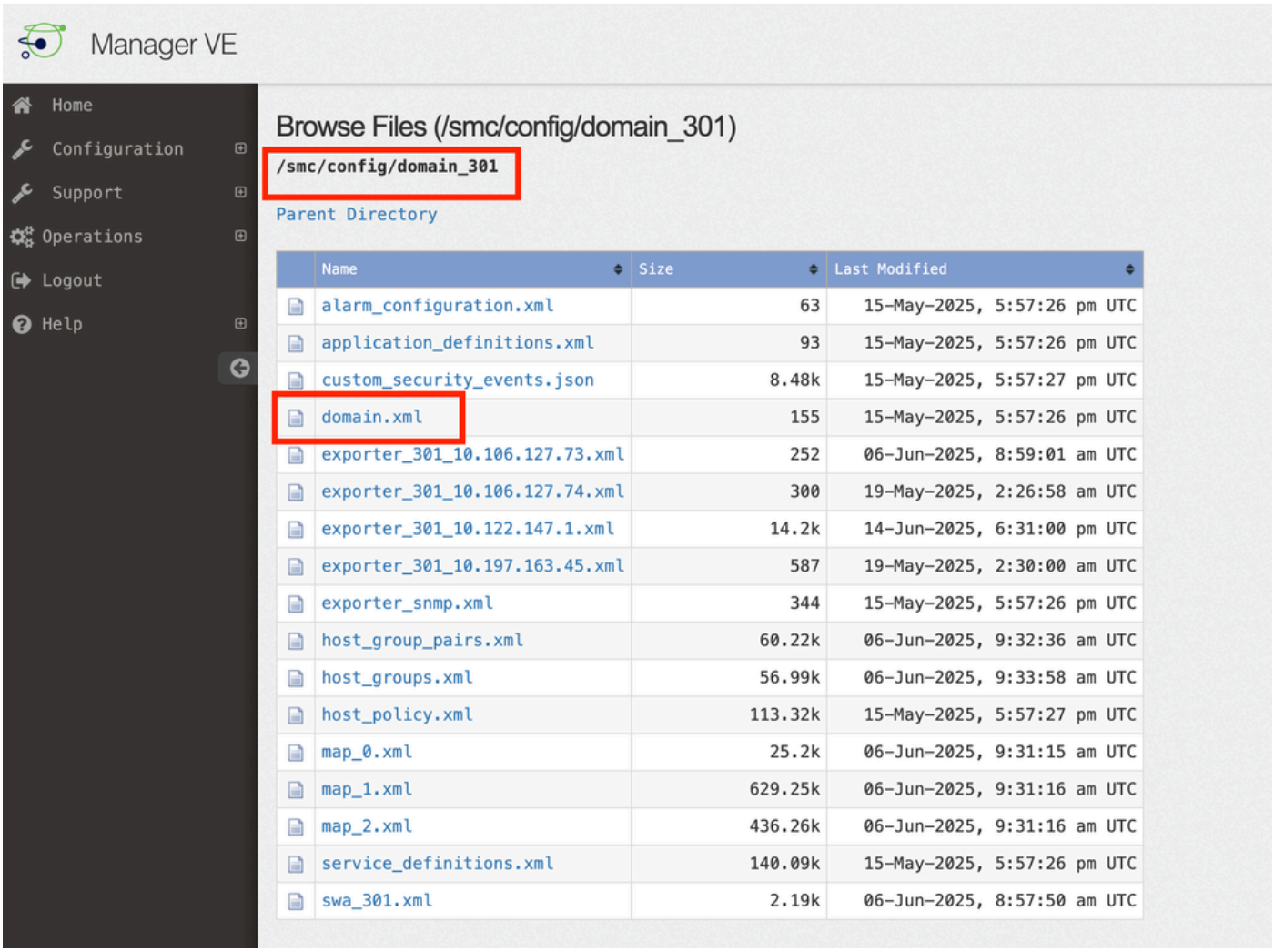
i. Inicie sesión en el administrador principal SNA y redirija a la página de administración del

dispositivo o acceda a la URL Índice IP del administrador.

ii. Busque la carpeta smc en la sección Soporte.



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


Manager VE
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).