Integrate SNA to Splunk Using Security Cloud Application

Contents

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

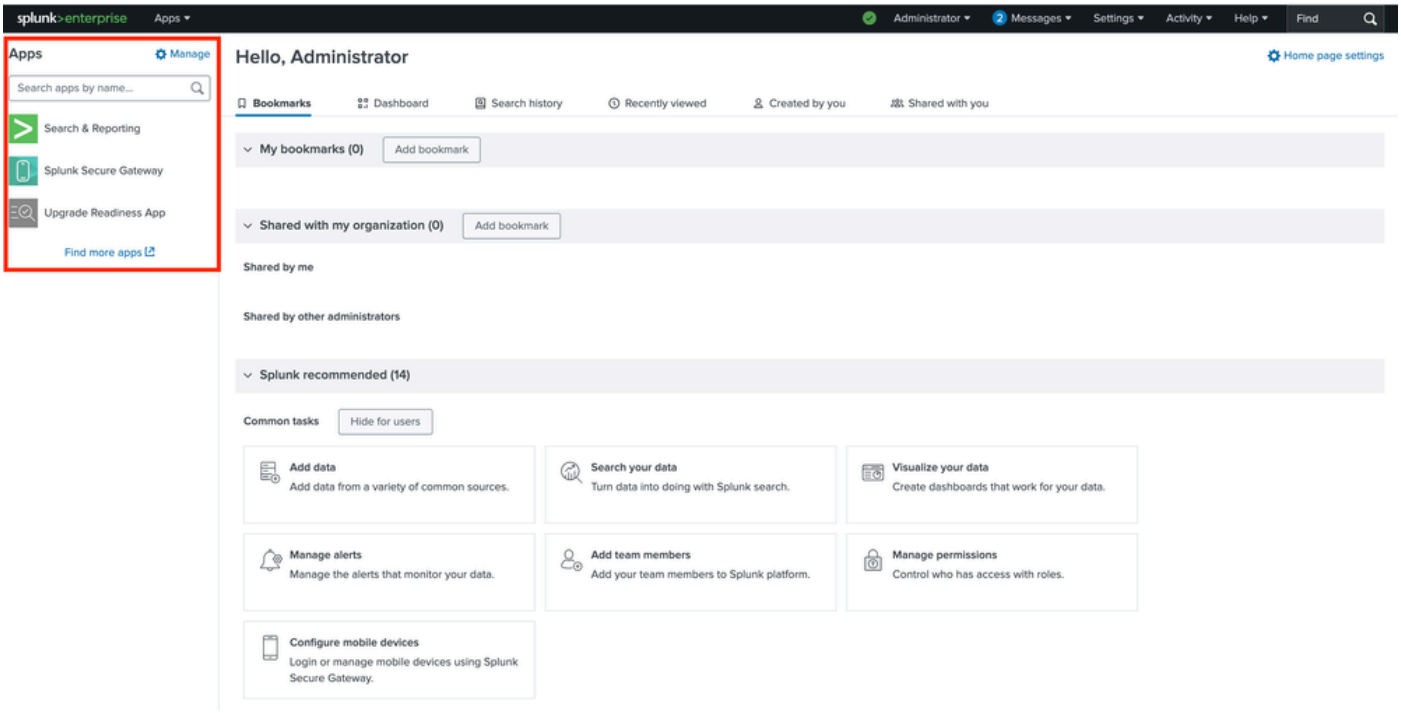
Secure Network Analytics v7.5.2.

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

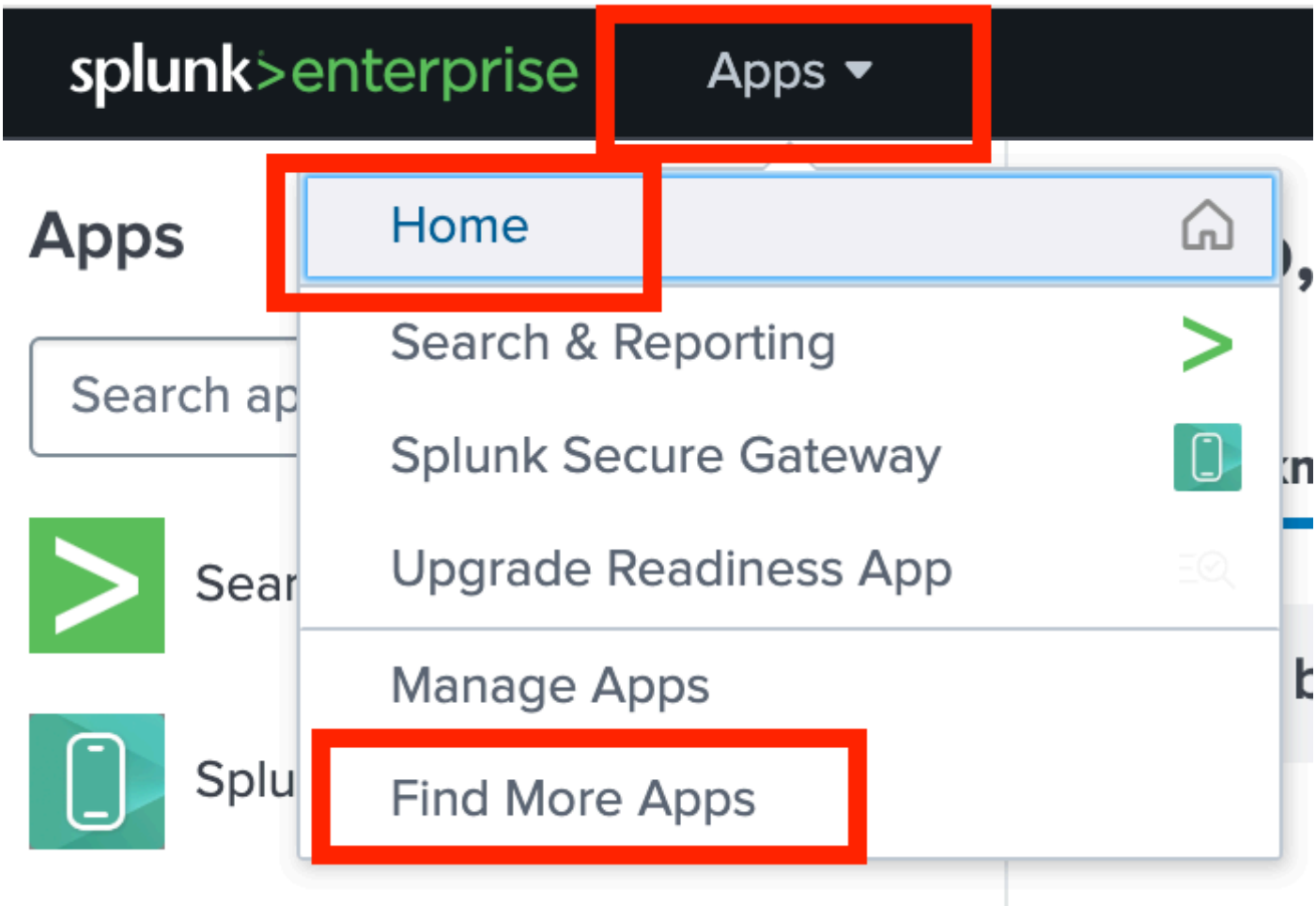
Step1: Access the **Splunk** Application and Install the **Cisco Security Cloud** Application.

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:

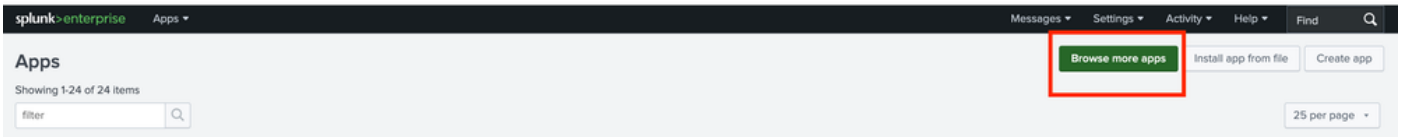


ii. For integrating the SNA with Splunk, it is required to install the Cisco Security Cloud Application which can be achieved in either of the mentioned methods:

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

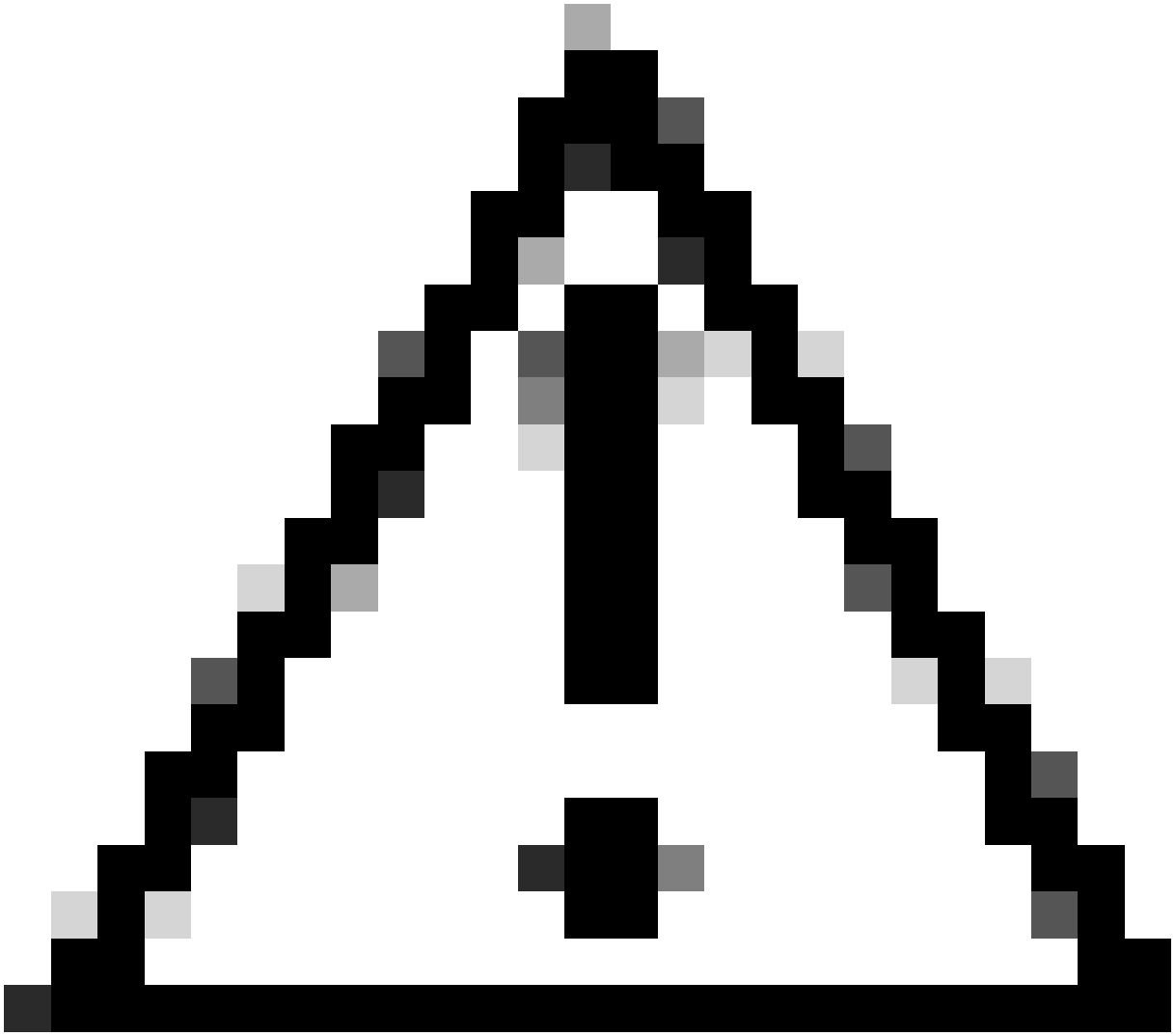


b. Browse more apps under the **Manager gear icon**.

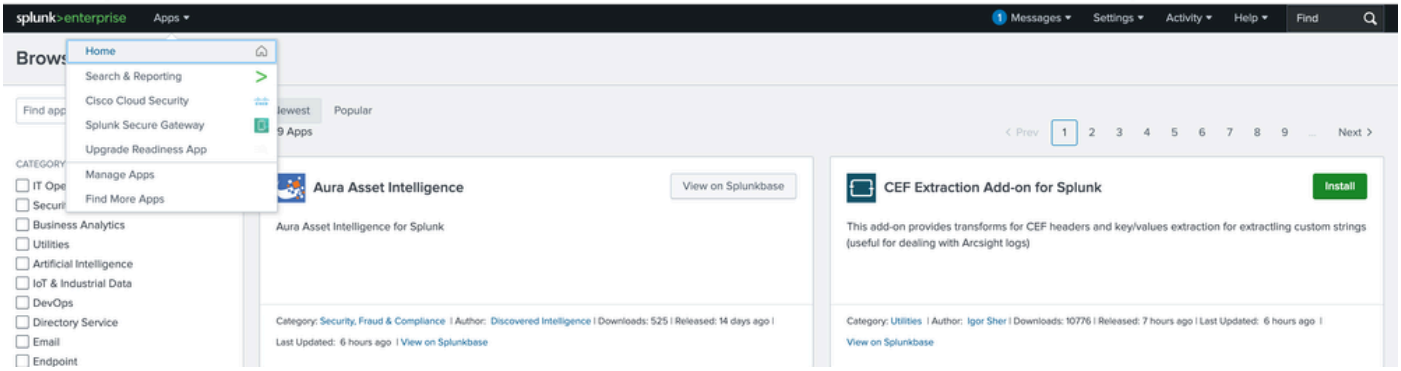


Step 2: Installation of the Cisco Security Cloud Application.

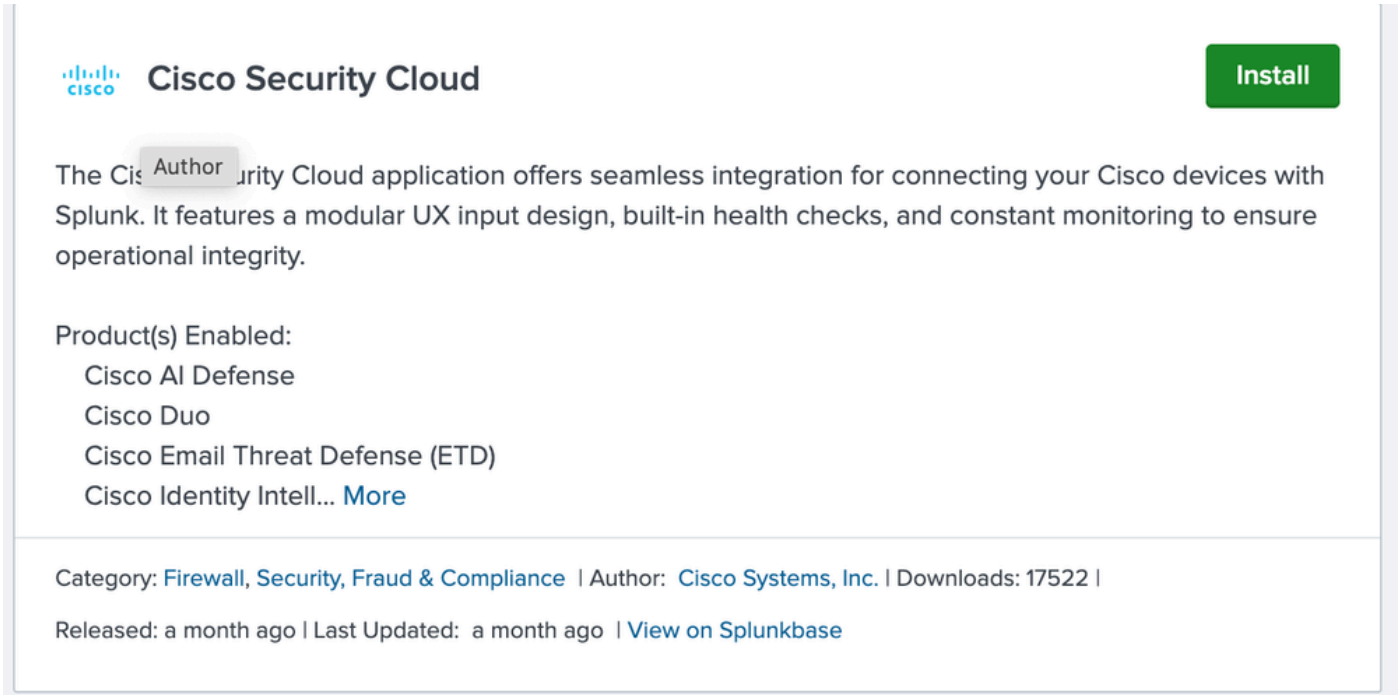
i. Look for the **Cisco Security Cloud Application**. Now, either scroll down till you find the app or search for **Cisco security cloud**.



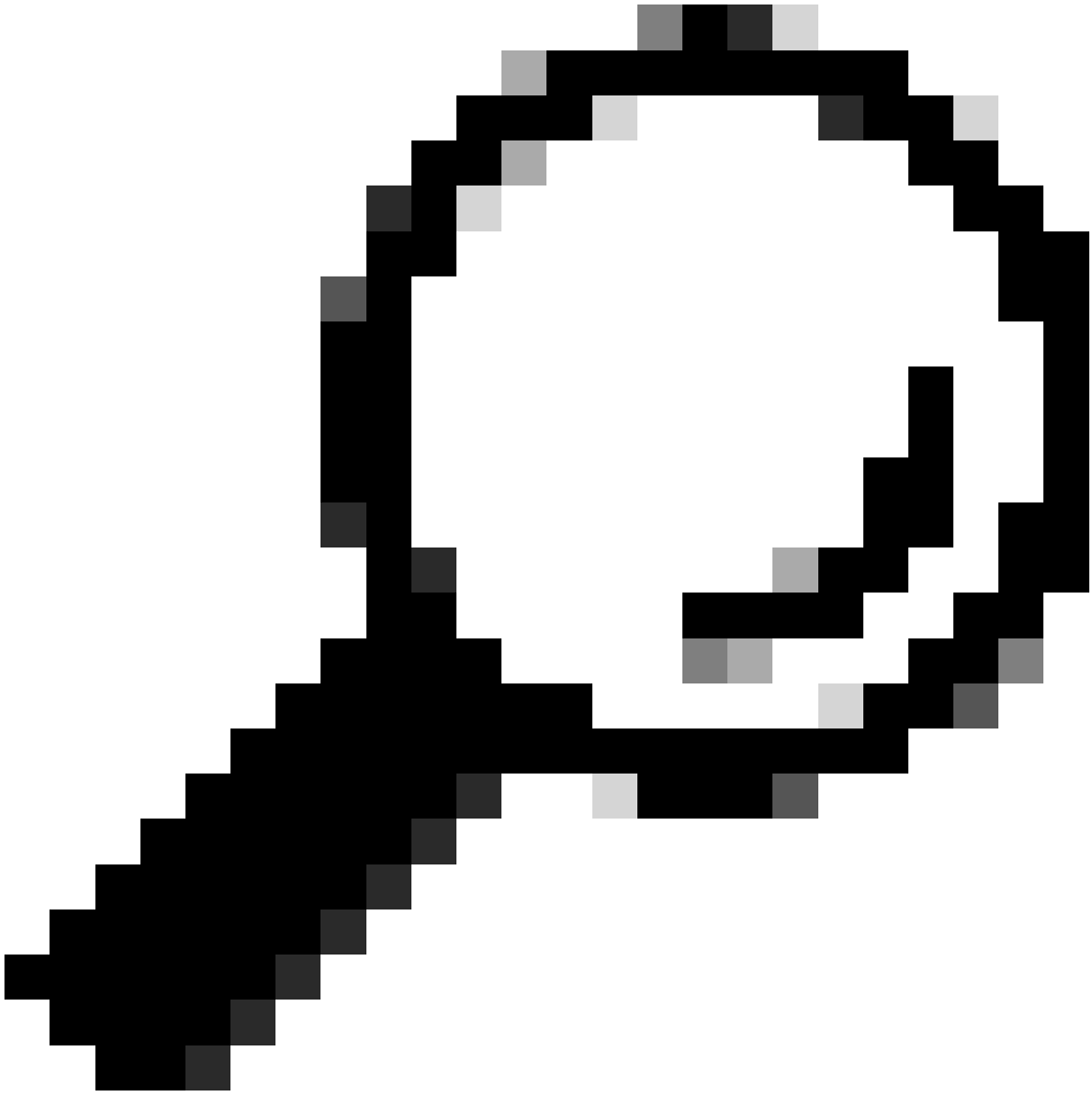
Caution: Do not get confused with Cisco Cloud Security App.



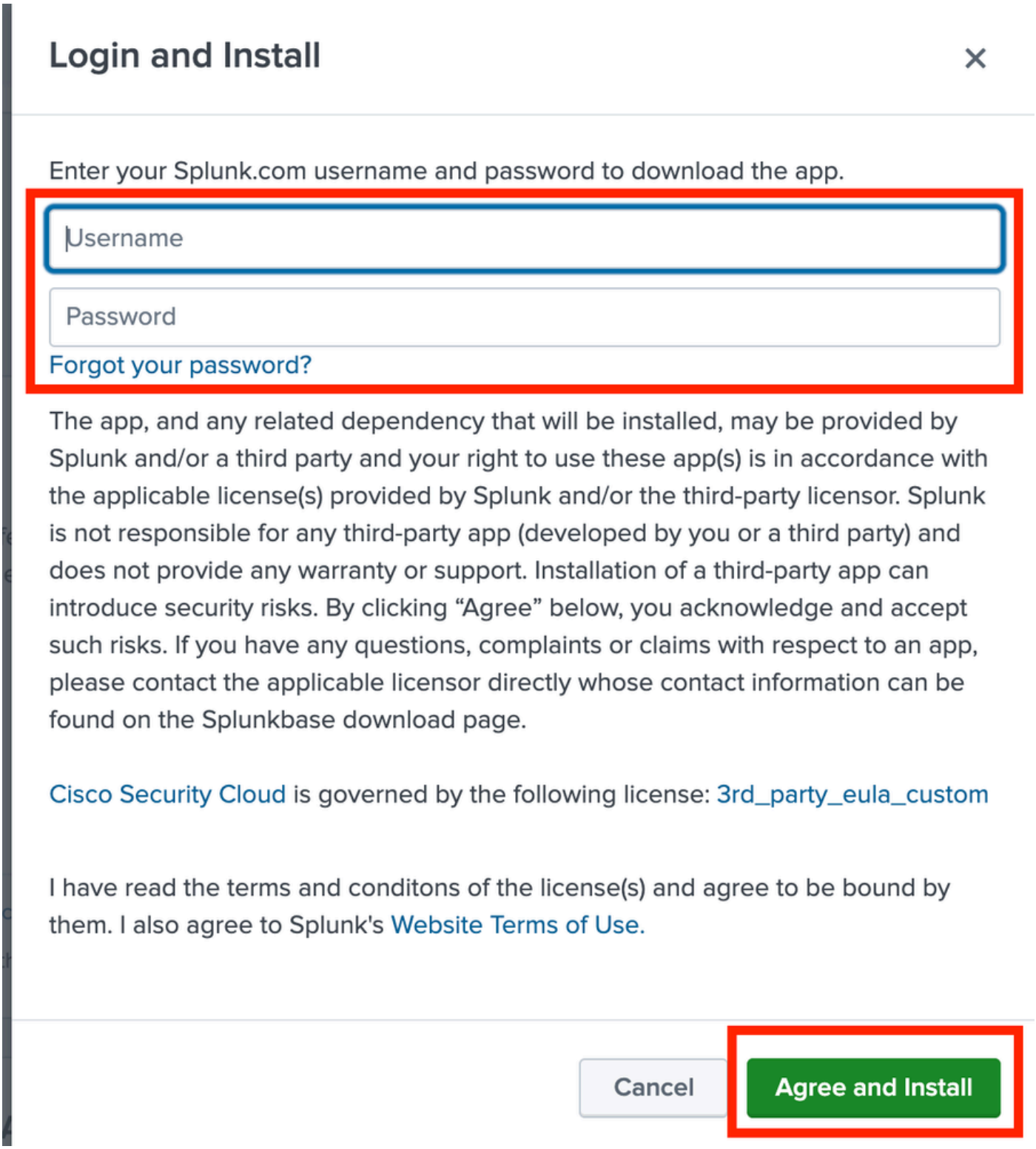
ii. Install the application by clicking the **Install** button.



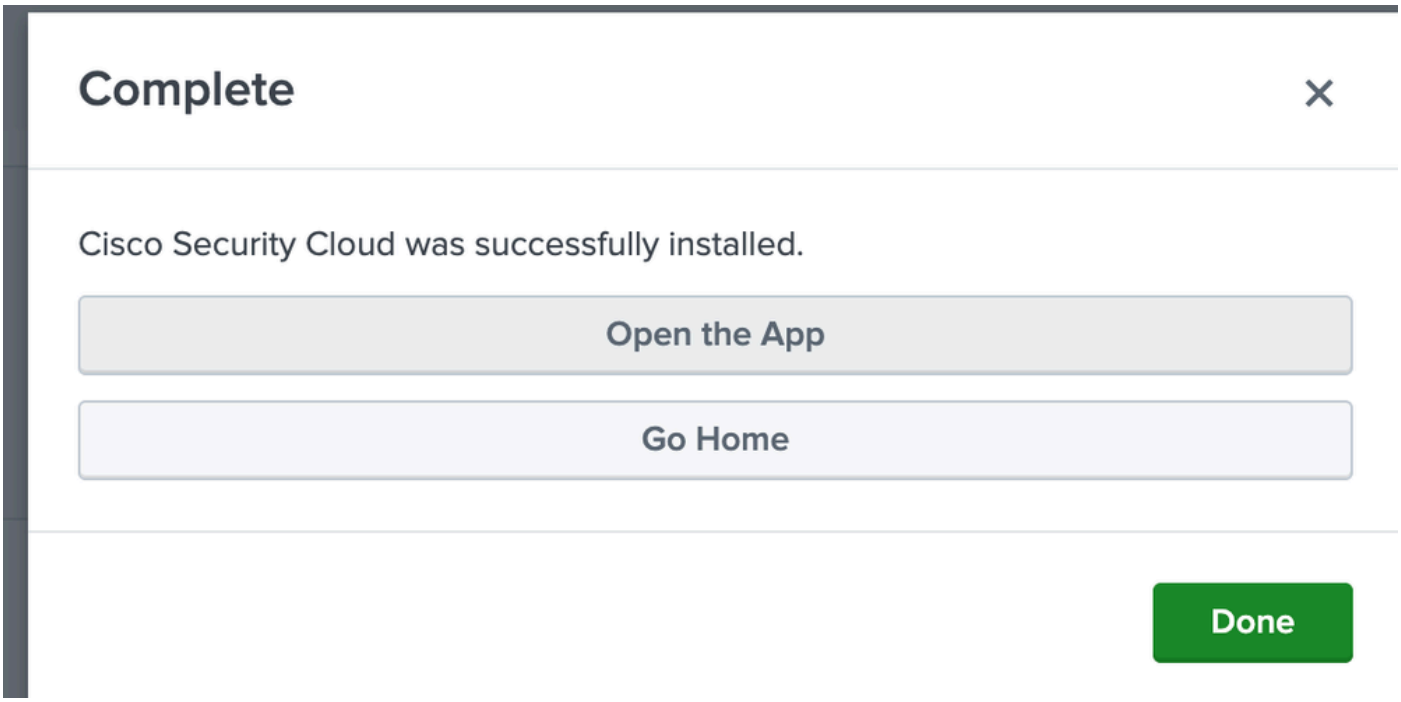
iii. The moment you click the install button a window pops up asking for the credentials of the Splunk account before installing the application. Provide the **credentials** and click **Agree and Install** to proceed further.



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

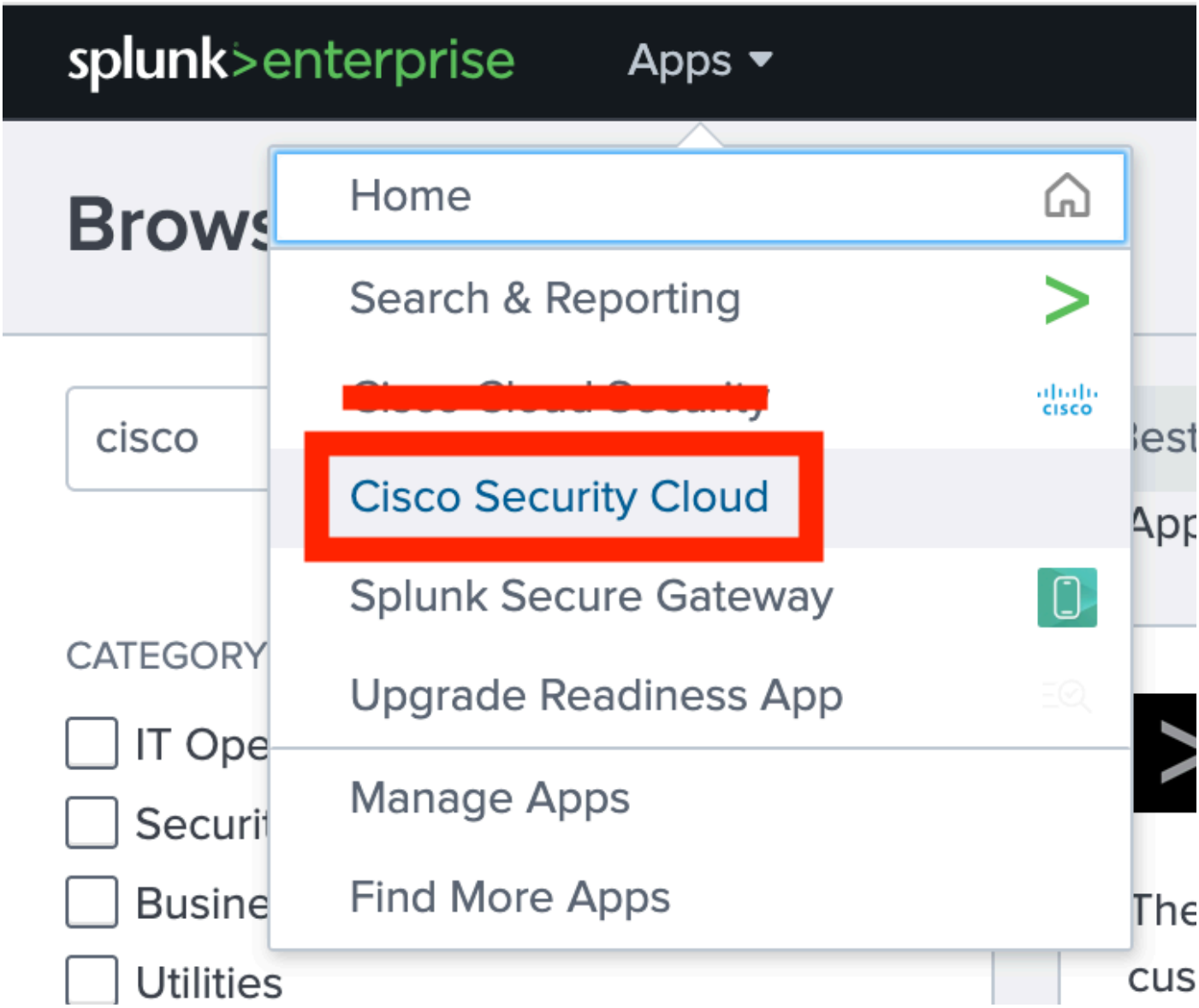


iv. A message pops up on successful installation of the application as depicted. Click **Done**.

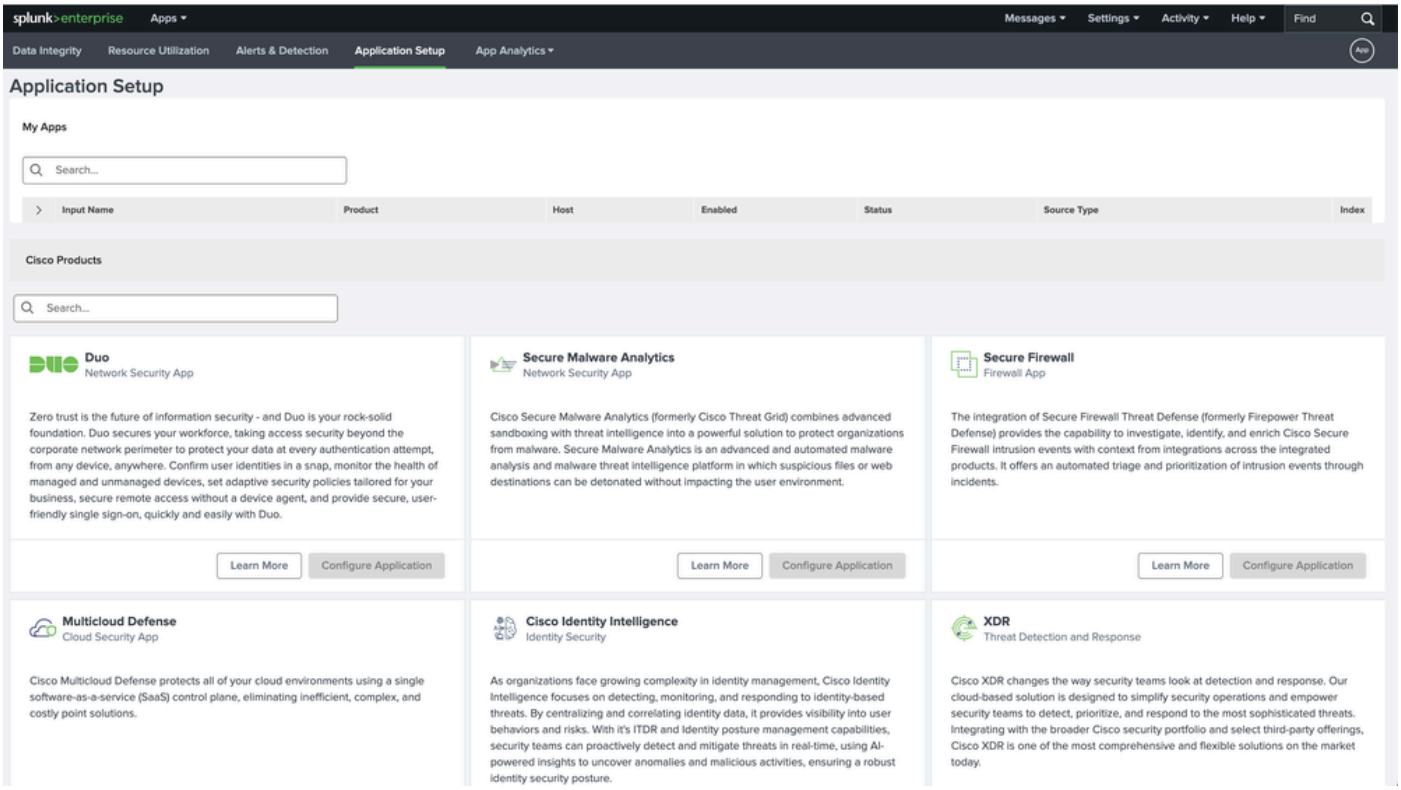


Step 3: Verification of the Installation of the Cisco Security Cloud Application.

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



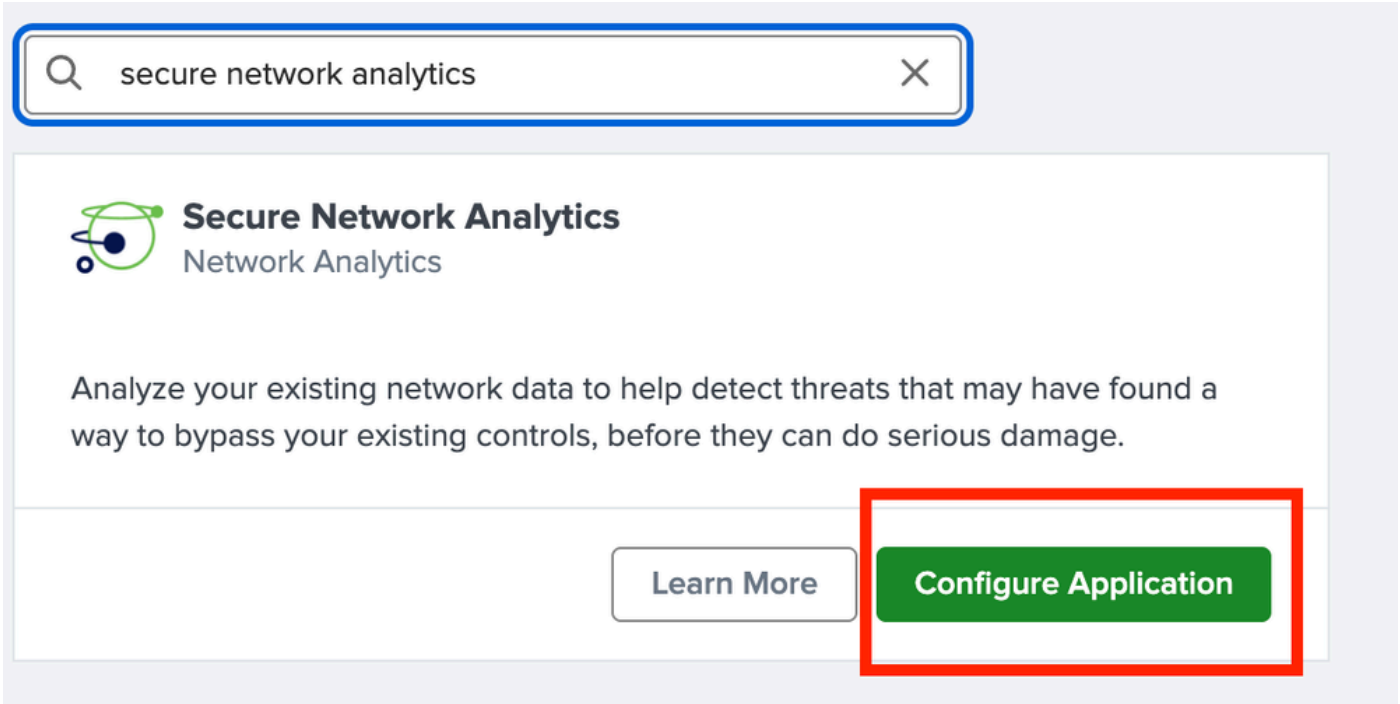
ii. Select **Cisco Security Cloud** by clicking it. You get redirected to the **Application Setup** page where all the available Cisco Cloud security products can be found.



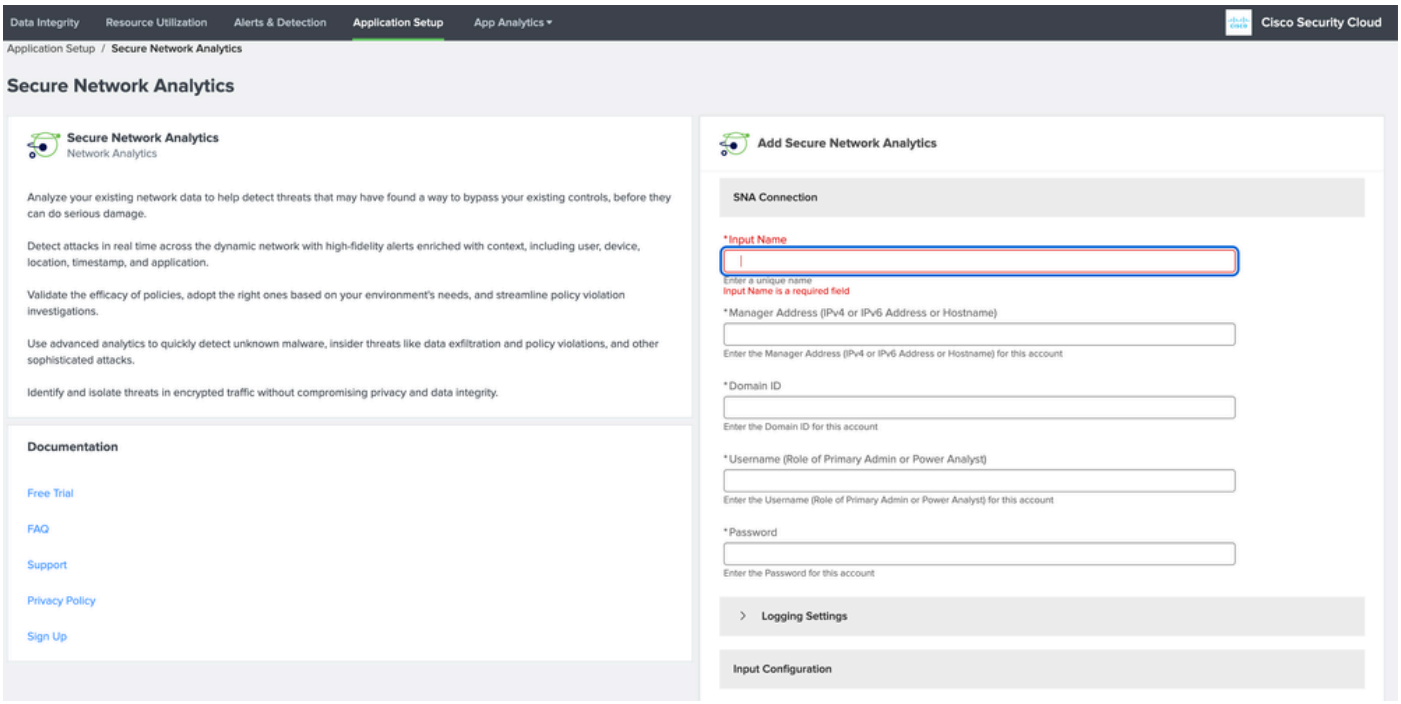
Step 4: Integration with Secure Network Analytics (SNA).

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**:

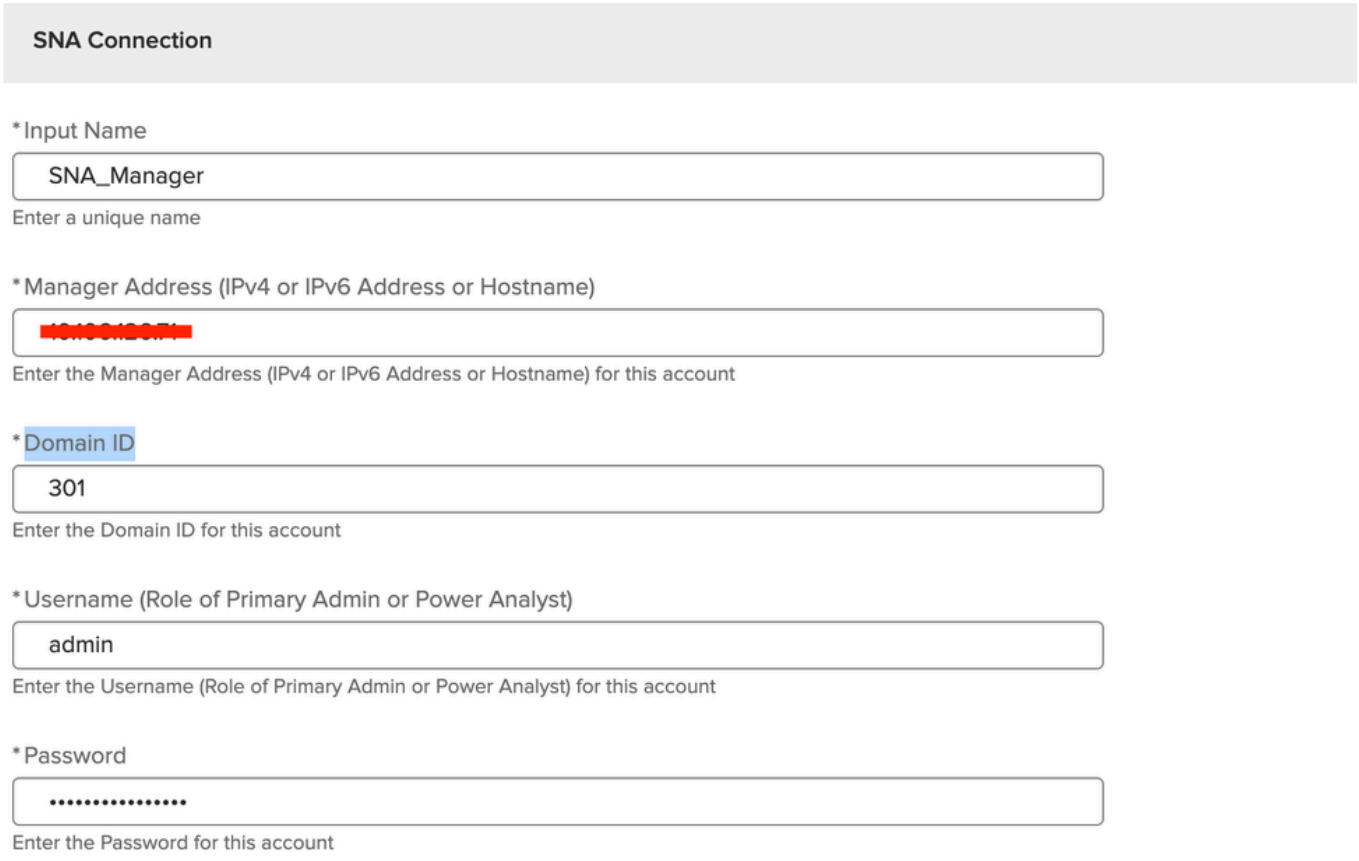


ii. When selecting the configure option, the configuration page for the detail to add pops up.

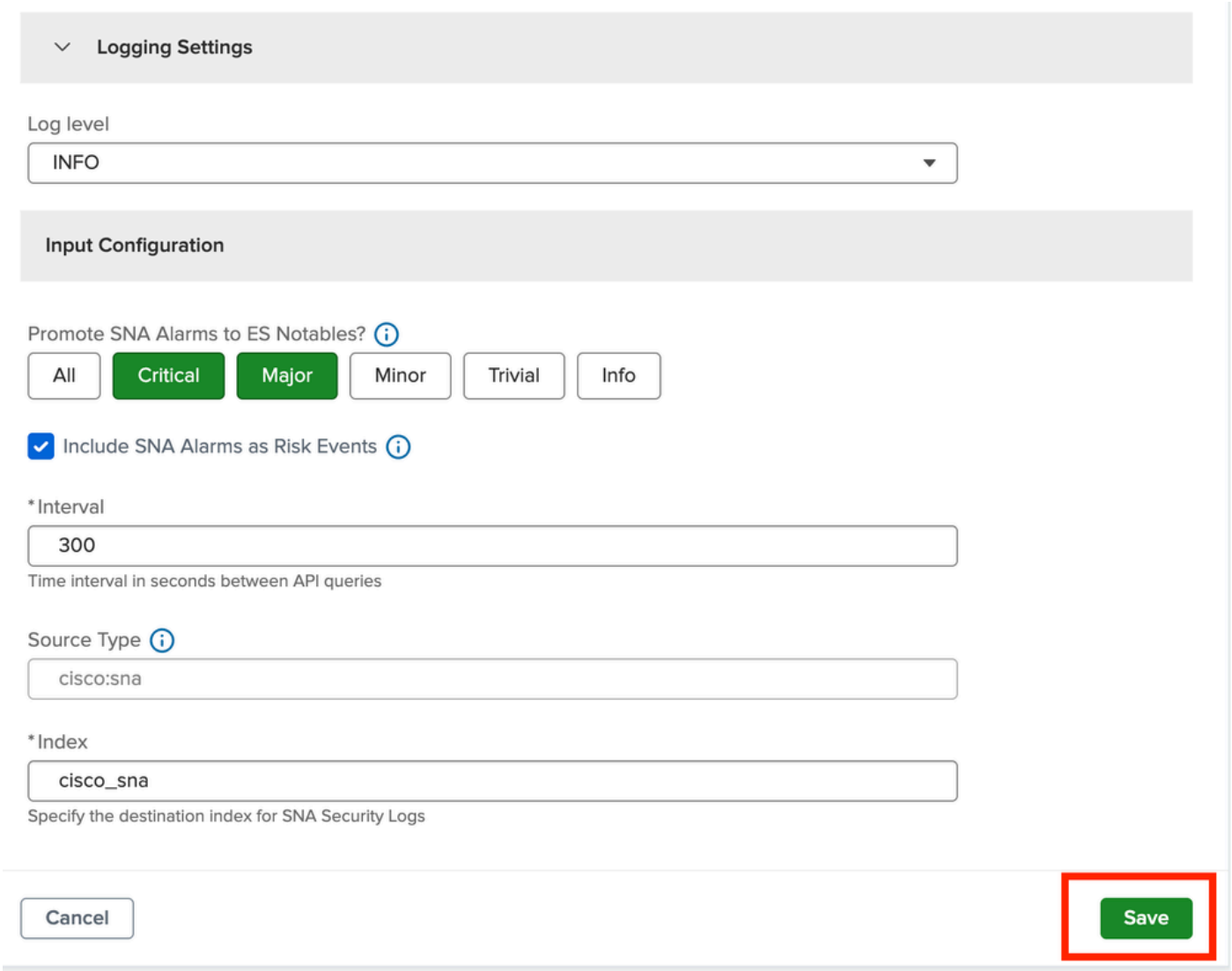


iii. Fill in all the mandatory details as mentioned for the SNA Connection Details:

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



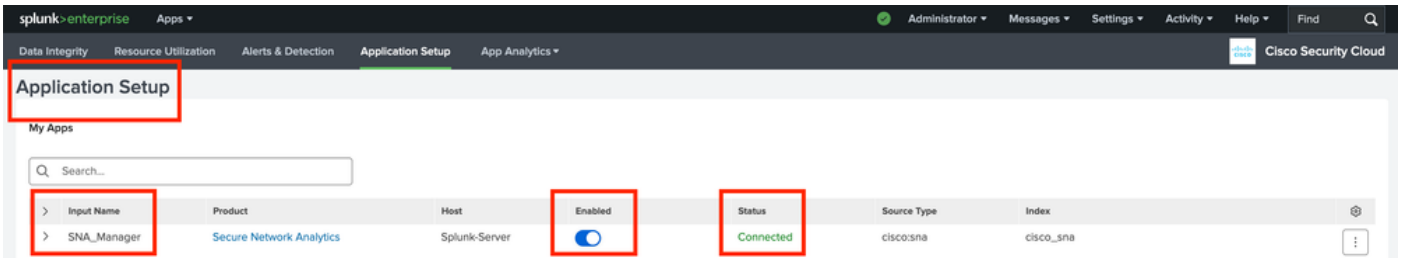
iv. Leave the remaining settings at their default values or modify them as needed, then click **Save**. A successful message pops up on the screen after the completion.



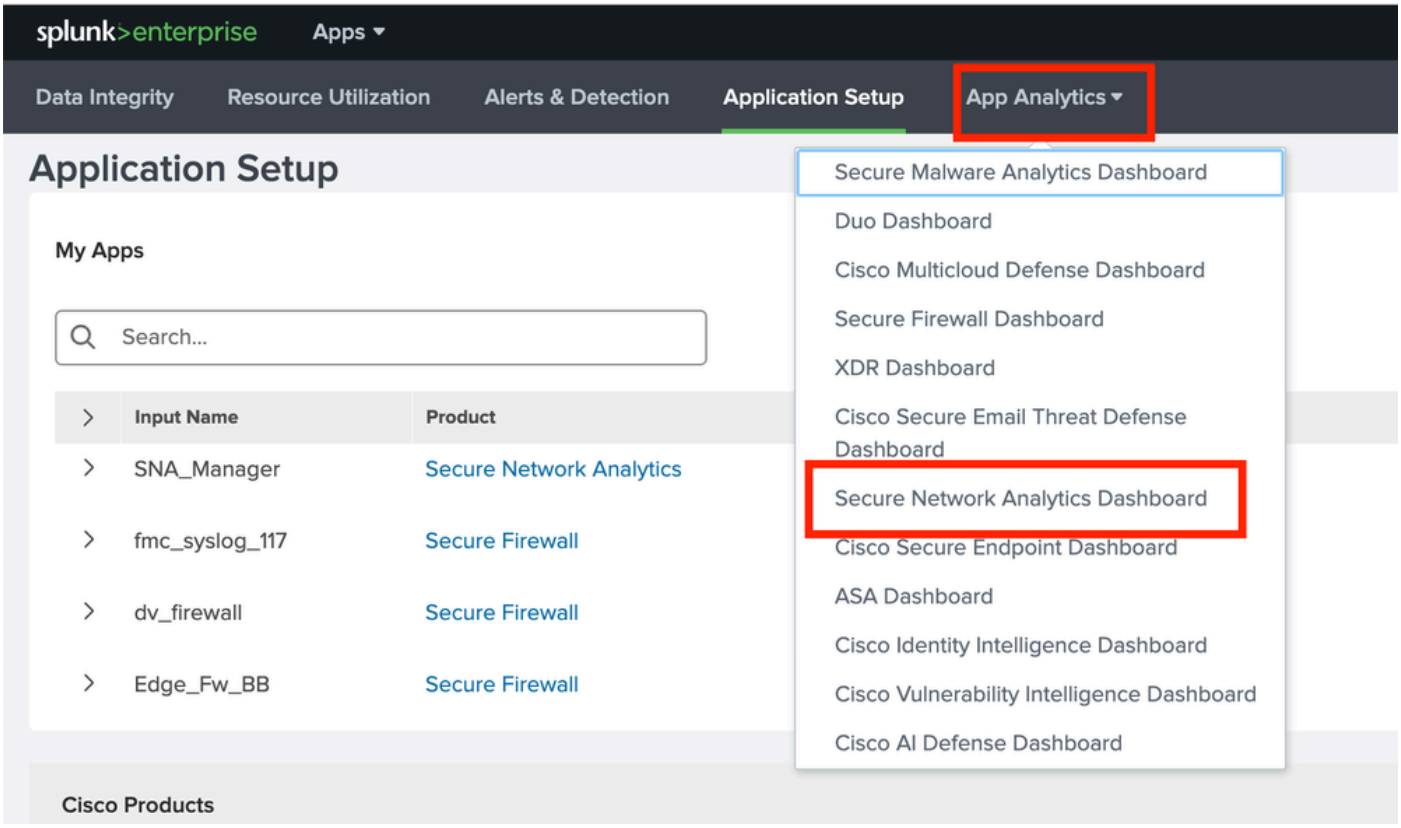
Step 5: Verification of Integration.

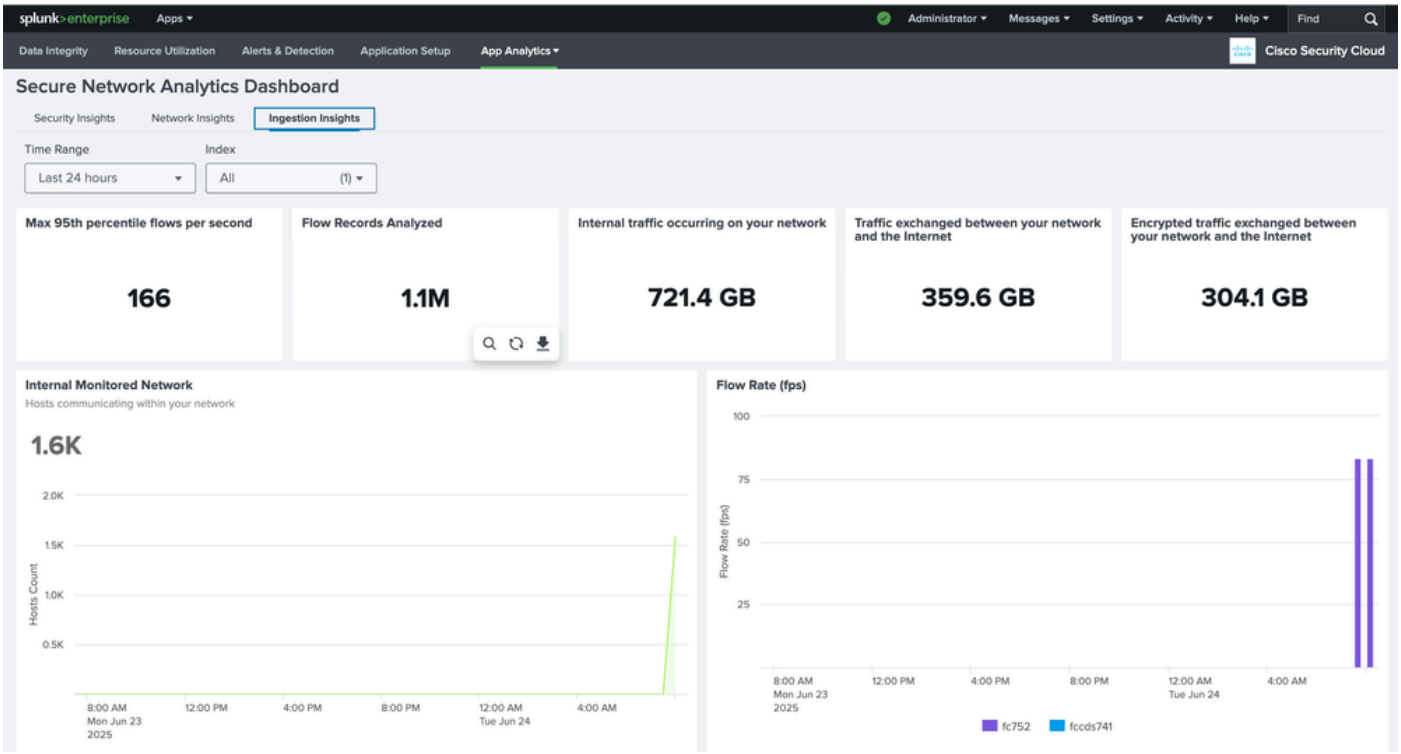
This is an important step where you need to verify whether the integration executed in the previous step is successfully done, or not.

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.



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





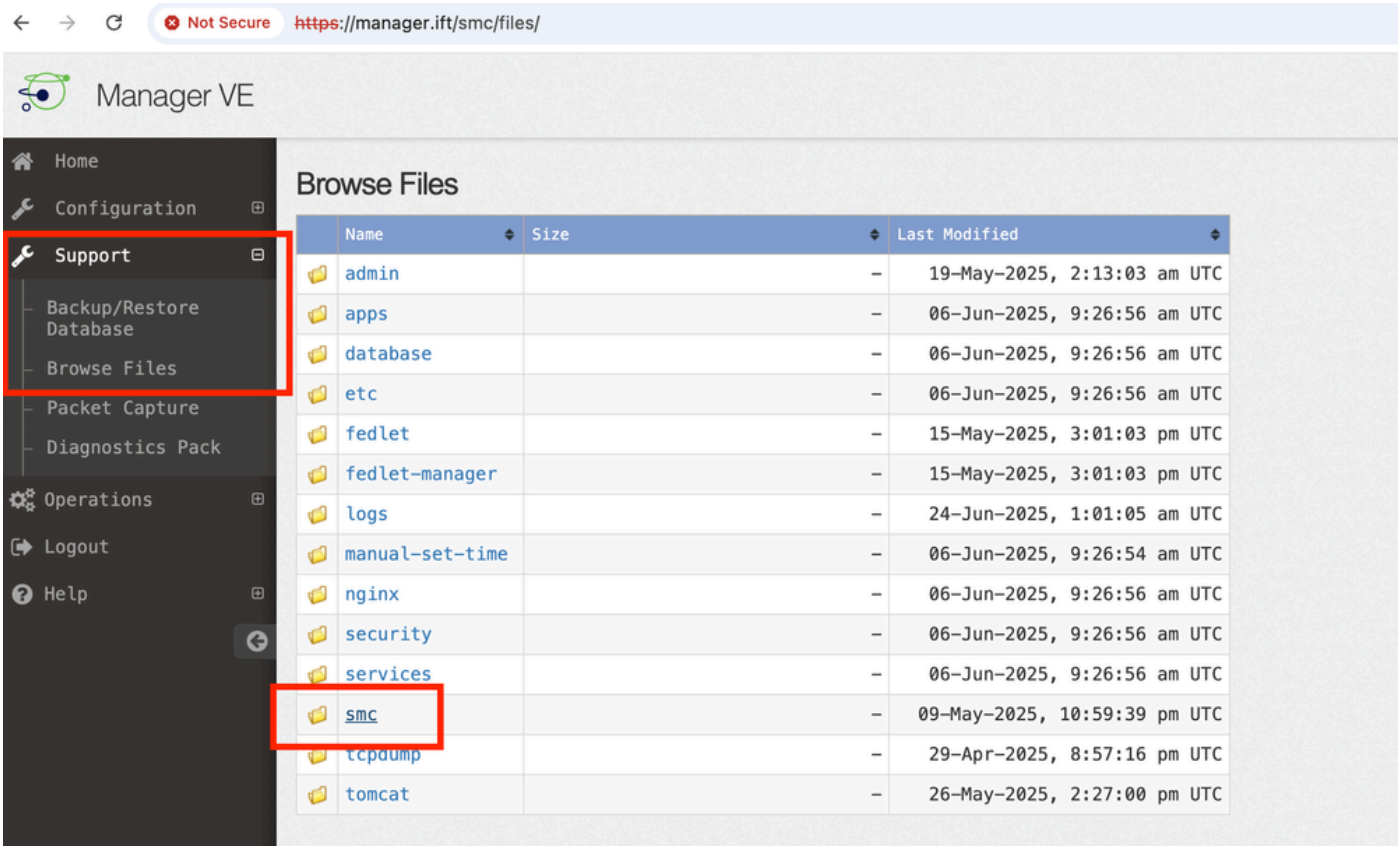
FAQs

Where to find the domain Id for the SNA manager?

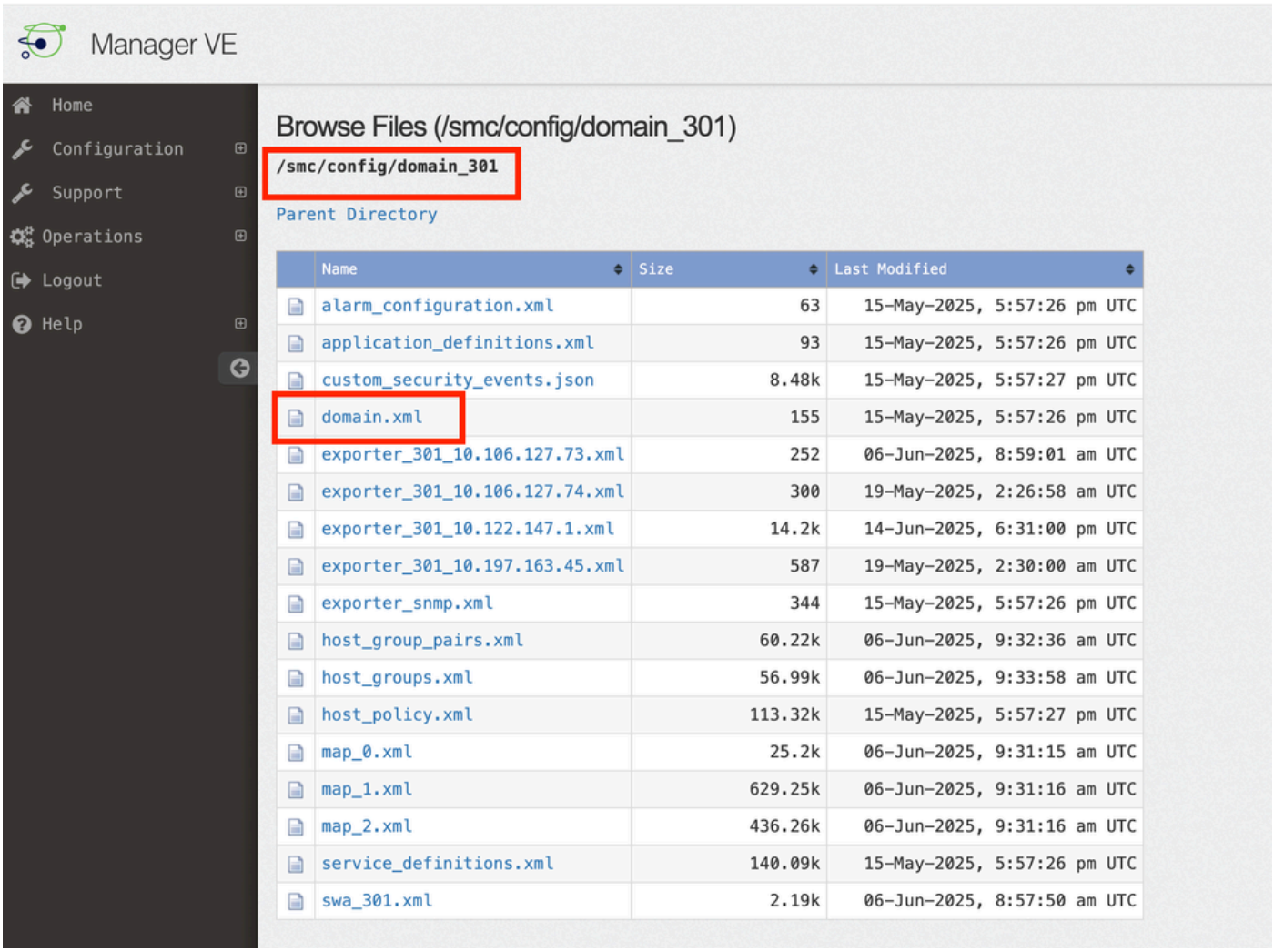
Answer:

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.



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


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