セキュリティクラウドアプリケーションを使用したSNAのSplunkへの統合

内容

はじめに

このドキュメントでは、特定された脅威に対する迅速なインシデント対応を実現するCisco Security Cloudを使用した、Splunkとの円滑なSNA統合について説明します。

前提条件

Splunkおよびシスコデバイスに関する基礎知識

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

Splunkエンタープライズ

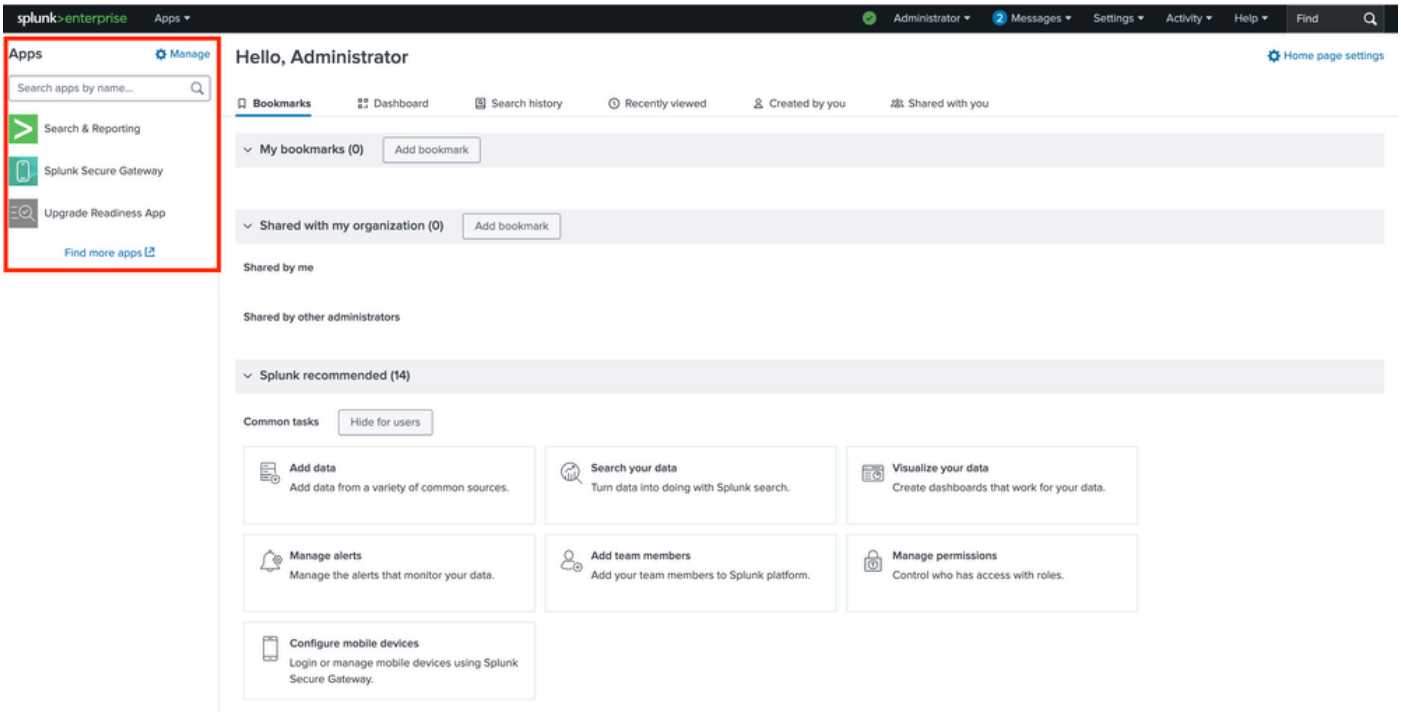
Secure Network Analytics v7.5.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

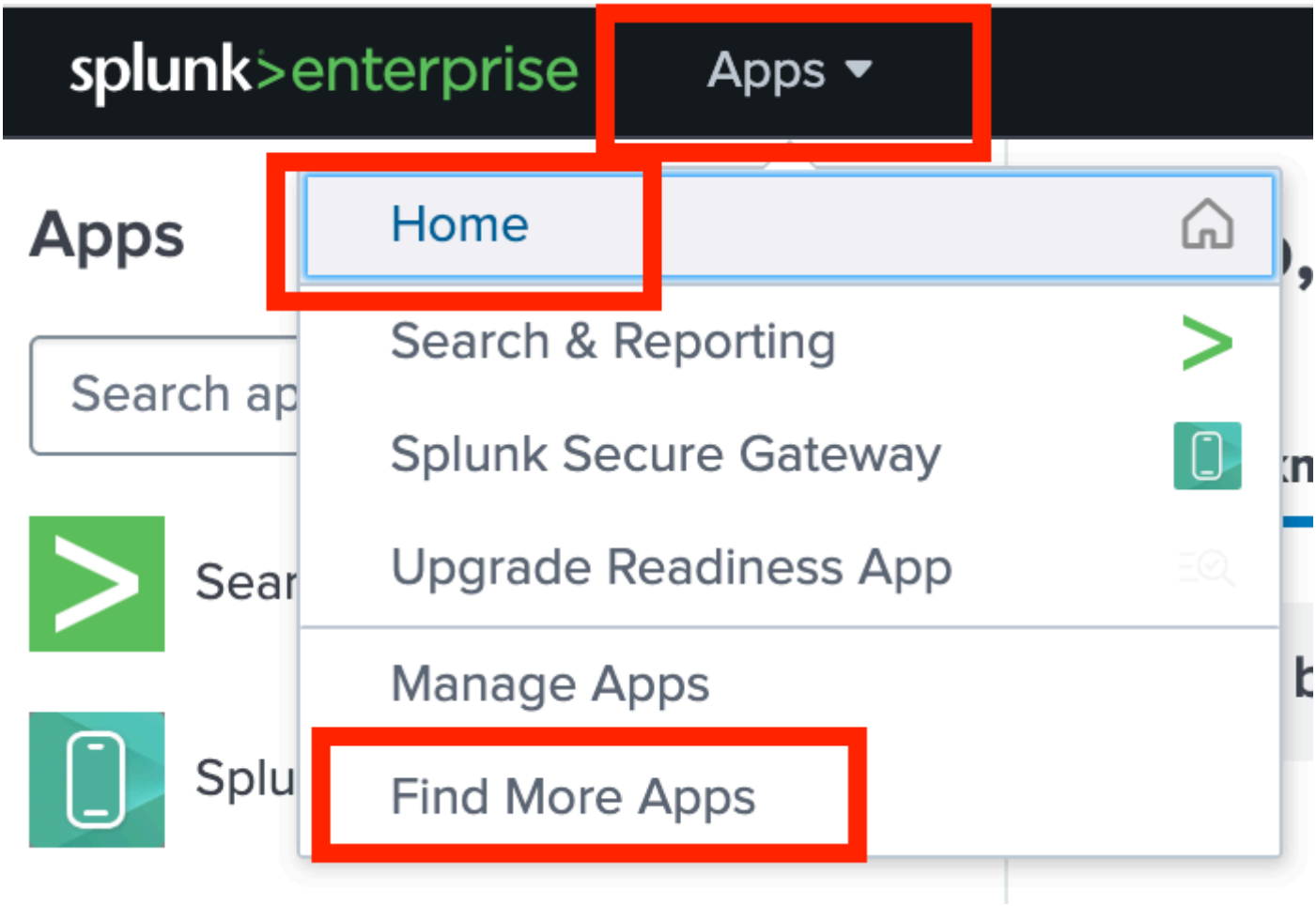
ステップ1:Splunkアプリケーションにアクセスし、Cisco Security Cloudアプリケーションをインストールします。

i.管理者クレデンシャルを使用してSplunk Webポータルにログインします。正常にログインすると、ホームページの左側のアプリケーションセクションにインストールされたアプリケーションのリストが表示されます。

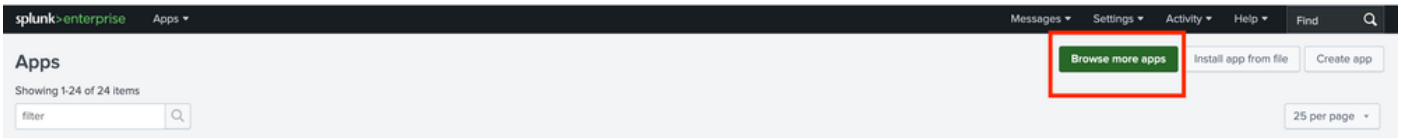


ii. SNAをSplunkと統合するには、Cisco Security Cloud Applicationをインストールする必要があります。このアプリケーションは、次のいずれかの方法で実行できます。

1. ドロップダウンからFind More Appsを選択します。



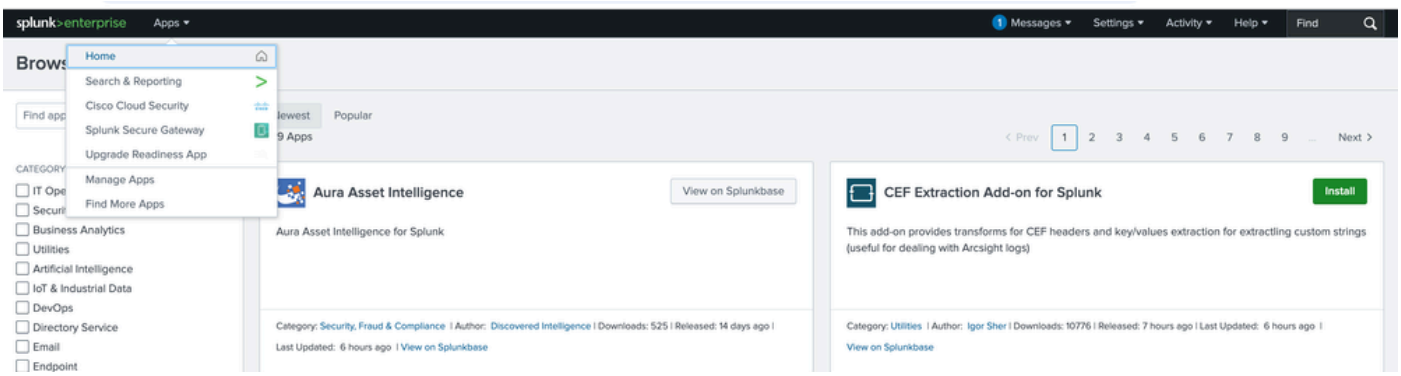
b. マネージャの歯車アイコンの下で、他のアプリケーションを参照します。



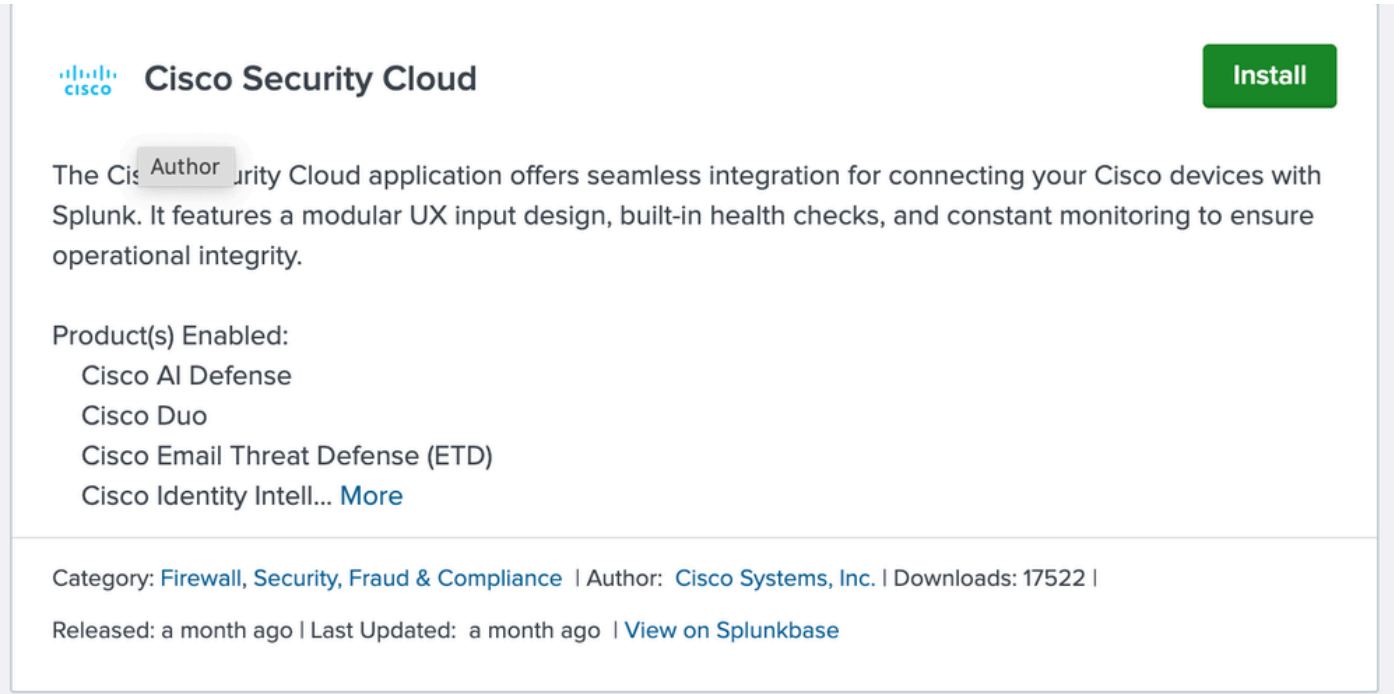
ステップ2:Cisco Security Cloud Applicationのインストール。

i. Cisco Security Cloud Applicationを探します。アプリが見つかるまで下にスクロールするか、Cisco Security Cloudを検索します。

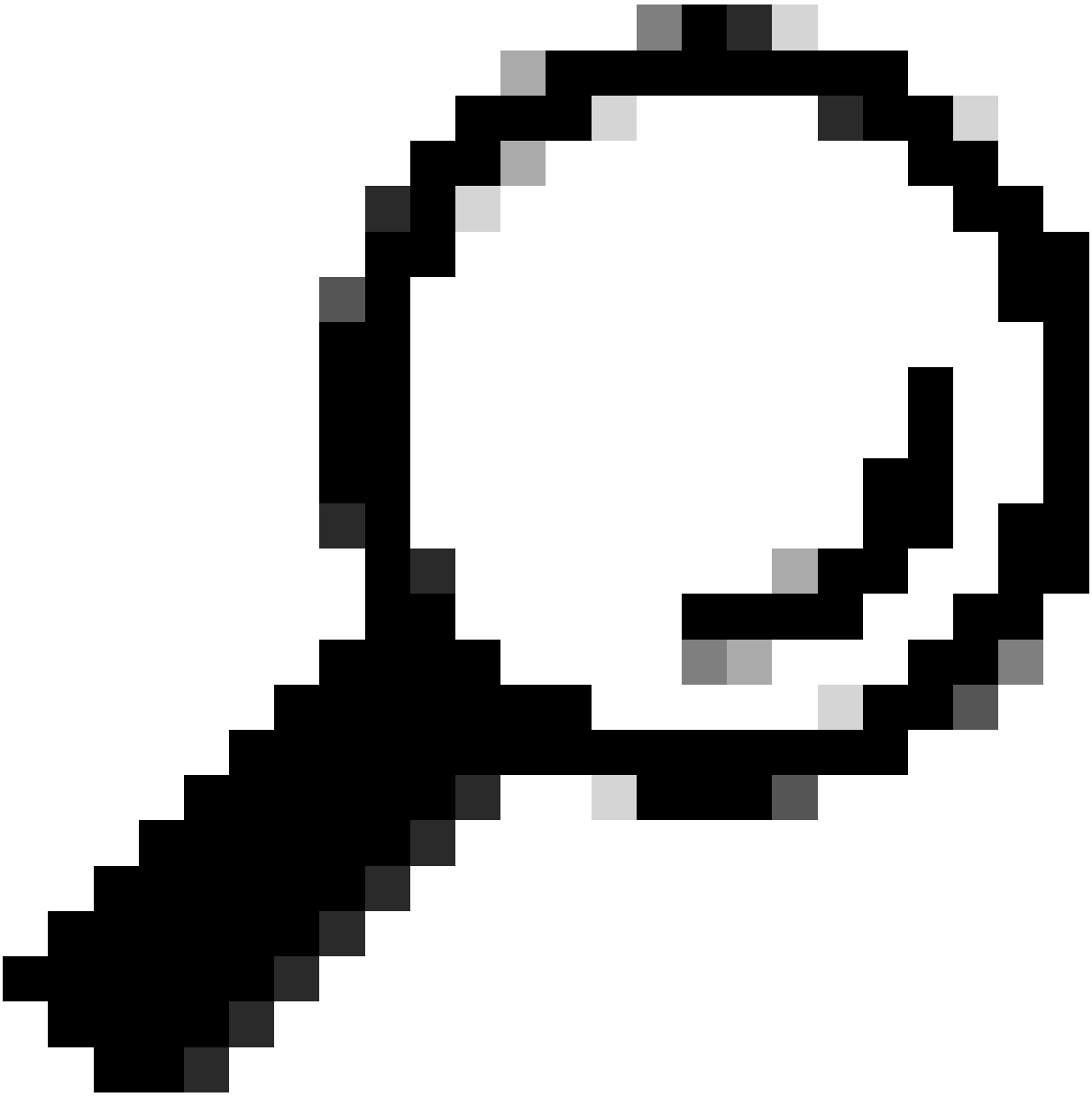
注意:Cisco Cloud Securityアプリケーションと混同しないでください。



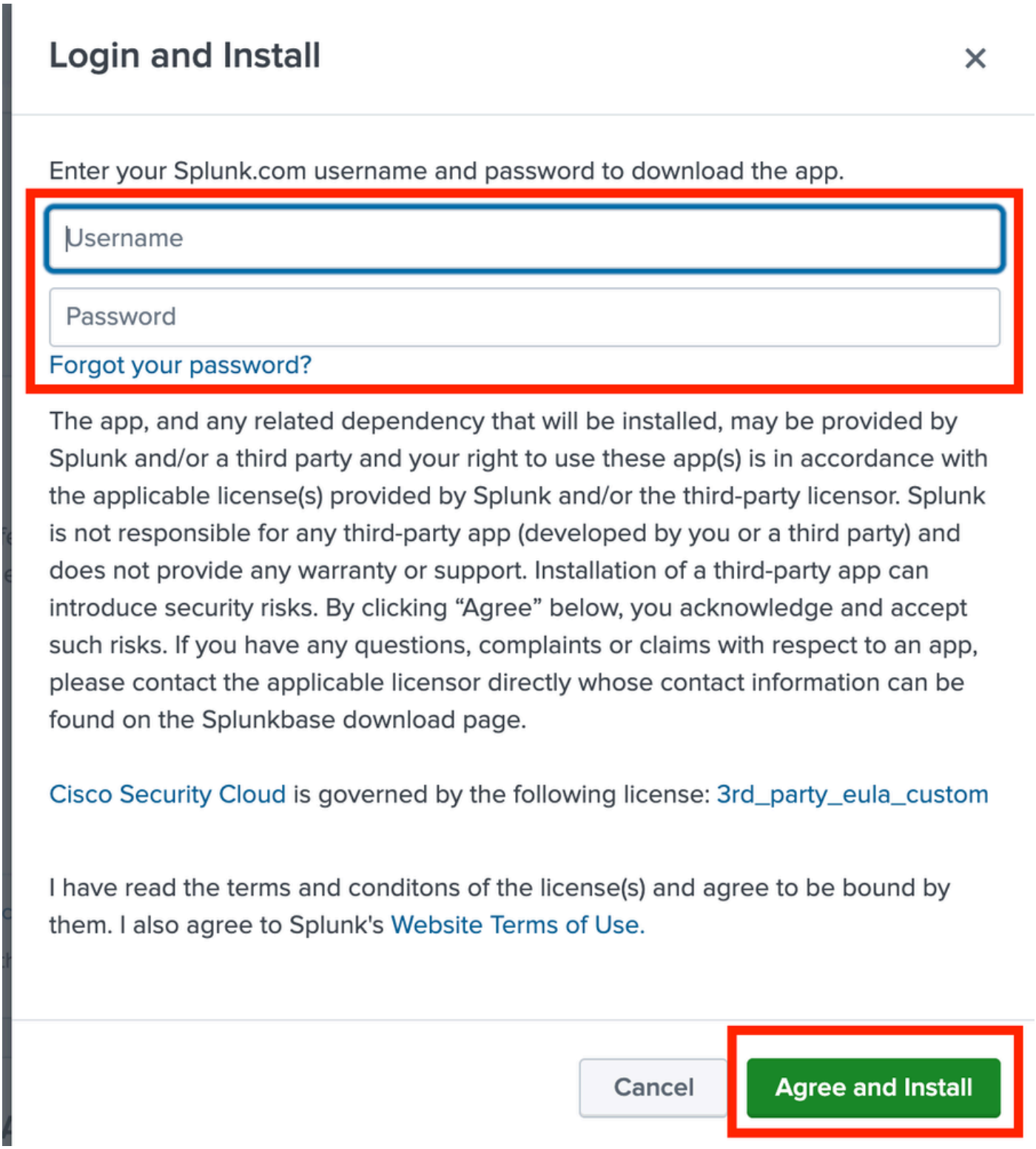
ii. Installボタンをクリックして、アプリケーションをインストールします。



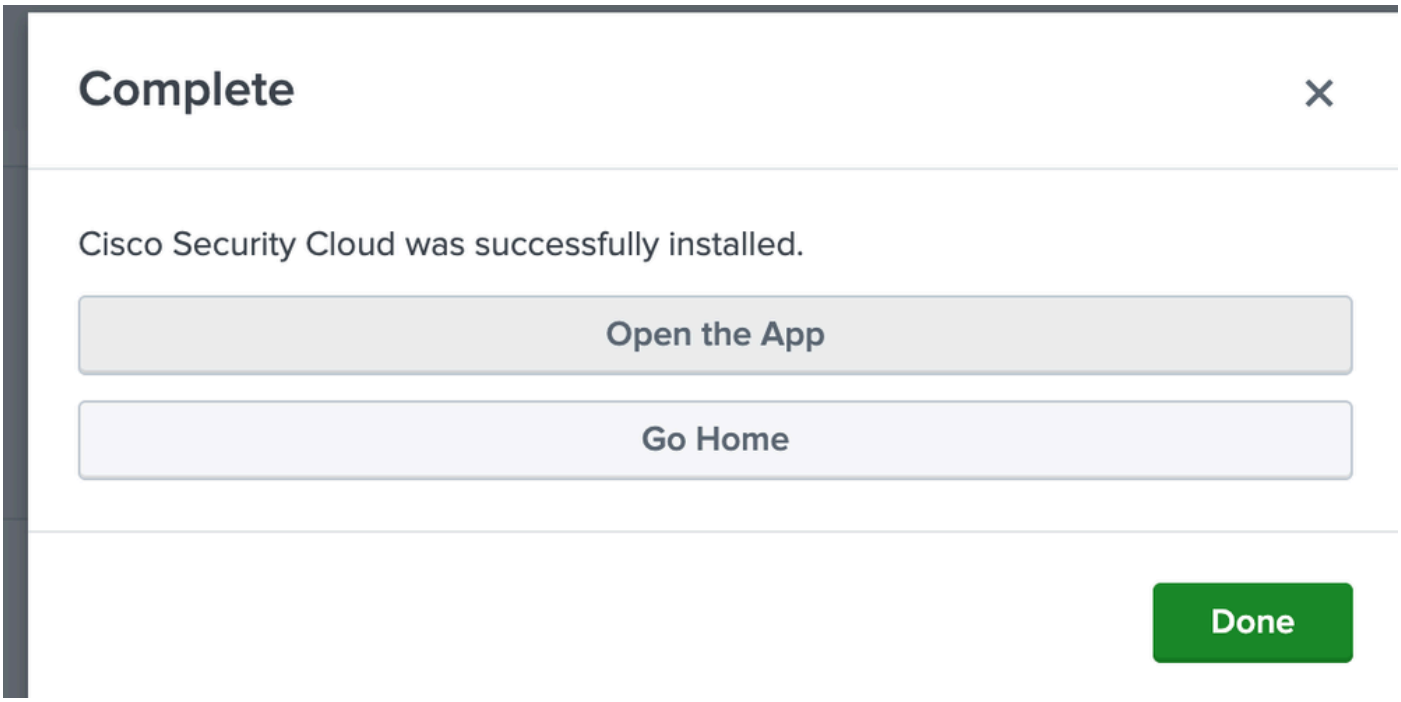
iii.インストールボタンをクリックすると、アプリケーションをインストールする前に、Splunkアカウントのクレデンシャルを求めるウィンドウがポップアップ表示されます。クレデンシャルを入力し、Agree and Installをクリックしてさらに先に進みます。



ヒント：ログイン時にSplunk Enterpriseアプリケーションに使用される管理者クレデンシャルではなく、Splunkポータルへのアクセスに使用されるクレデンシャルを指定します。

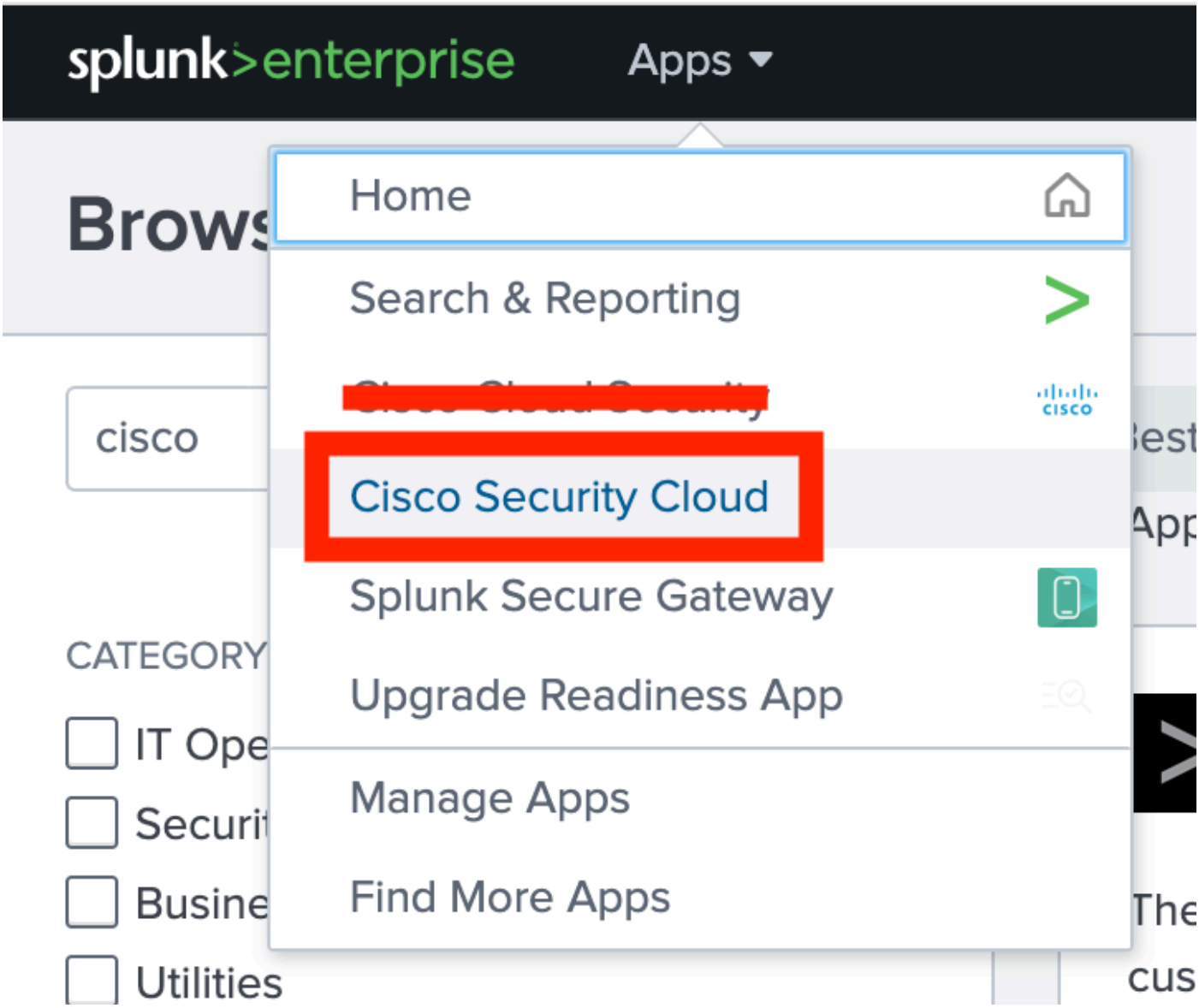


iv.アプリケーションのインストールが正常に完了すると、次に示すメッセージが表示されます。[Done] をクリックします。

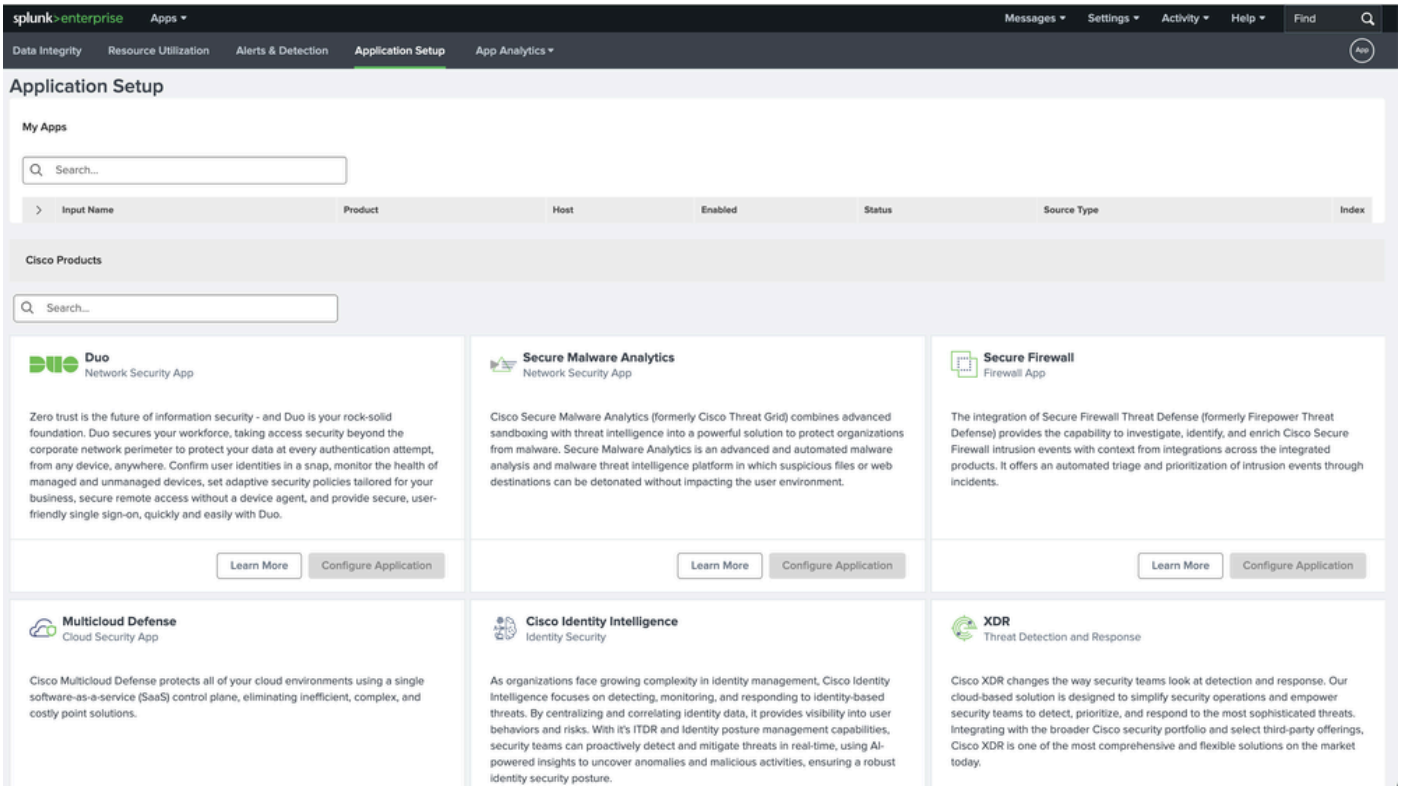


ステップ3:Cisco Security Cloud Applicationのインストールの検証。

i. Appsドロップダウンオプションをクリックすると、インストールが成功した後、アプリがリストに表示されます。



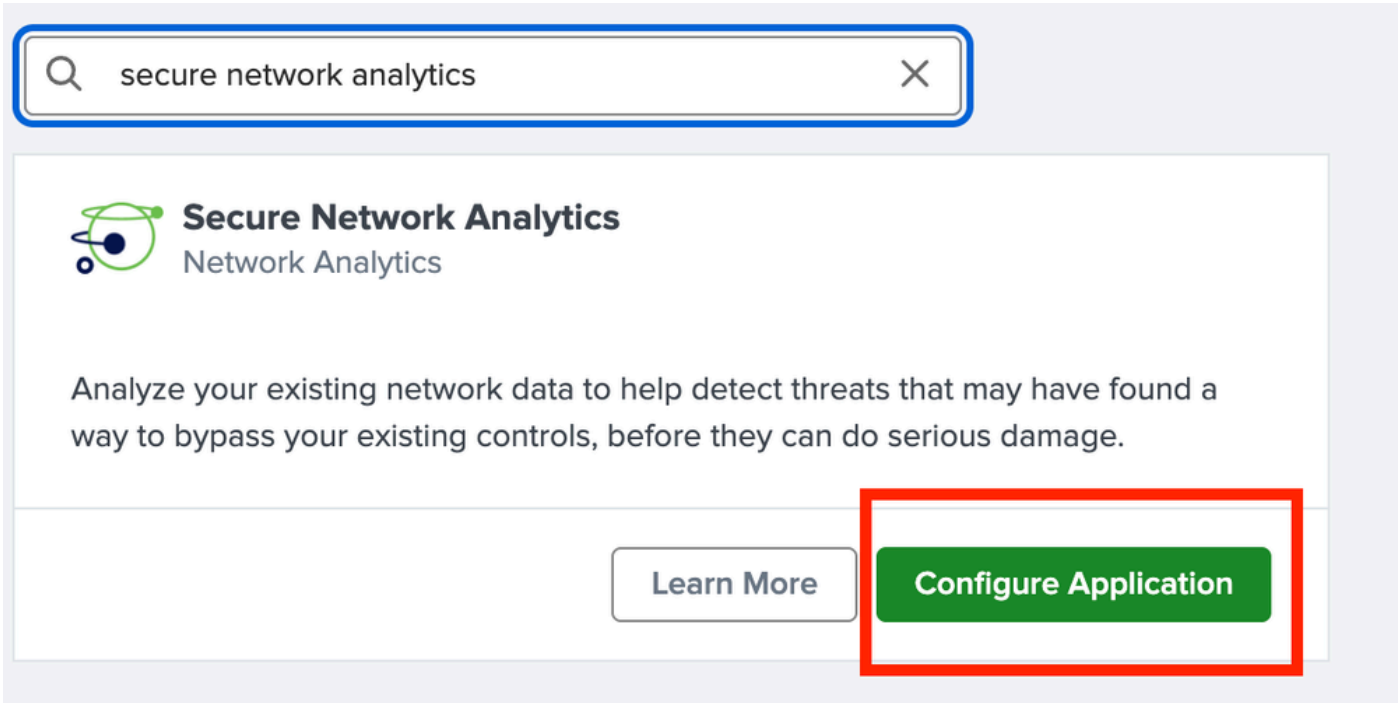
ii. Cisco Security Cloudをクリックして選択します。アプリケーションセットアップページにリダイレクトされます。このページには、利用可能なすべてのCisco Cloud Security製品が表示されます。



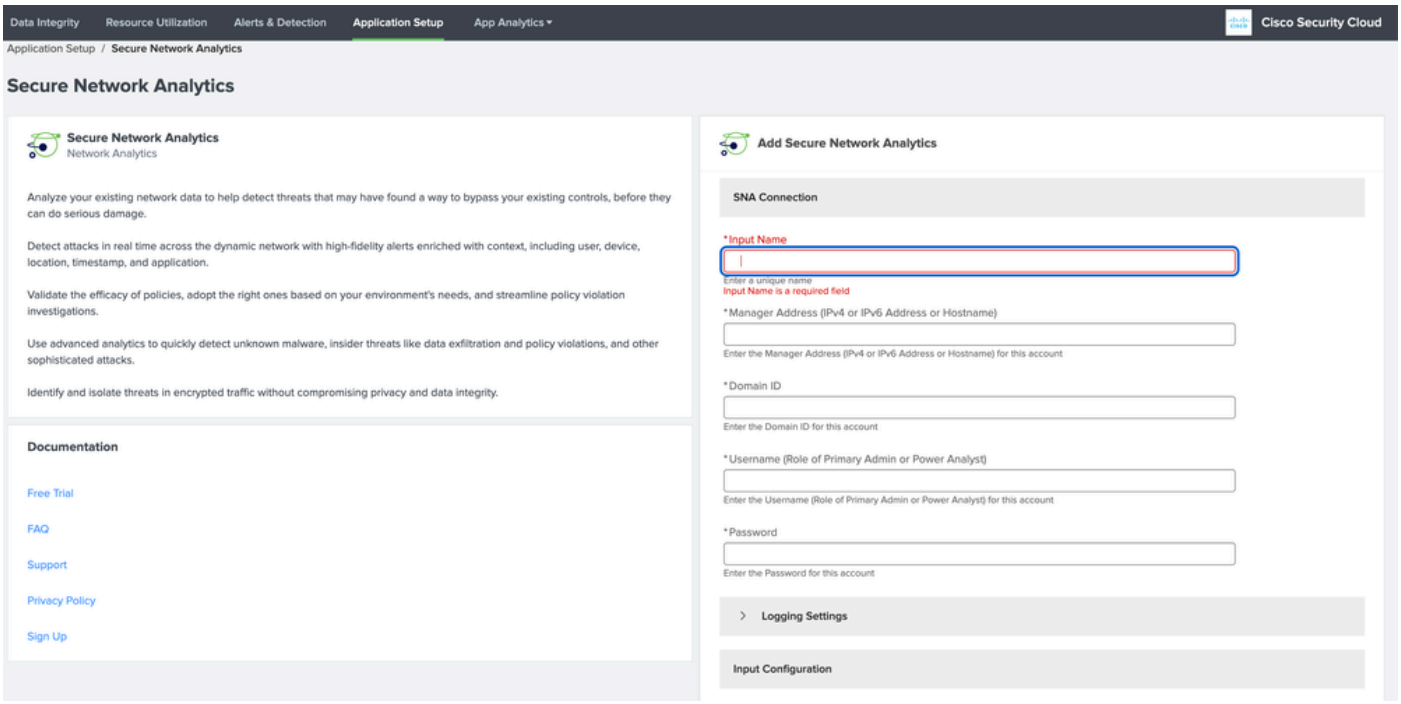
ステップ4:Secure Network Analytics(SNA)との統合

このドキュメントの目的は、前述のSecure Network Analytics(SNA)を使用したSplunkのインストール手順に焦点を当てることです。

i. Secure Network Analyticsを検索し、表示されたら、Configure Applicationを選択します。

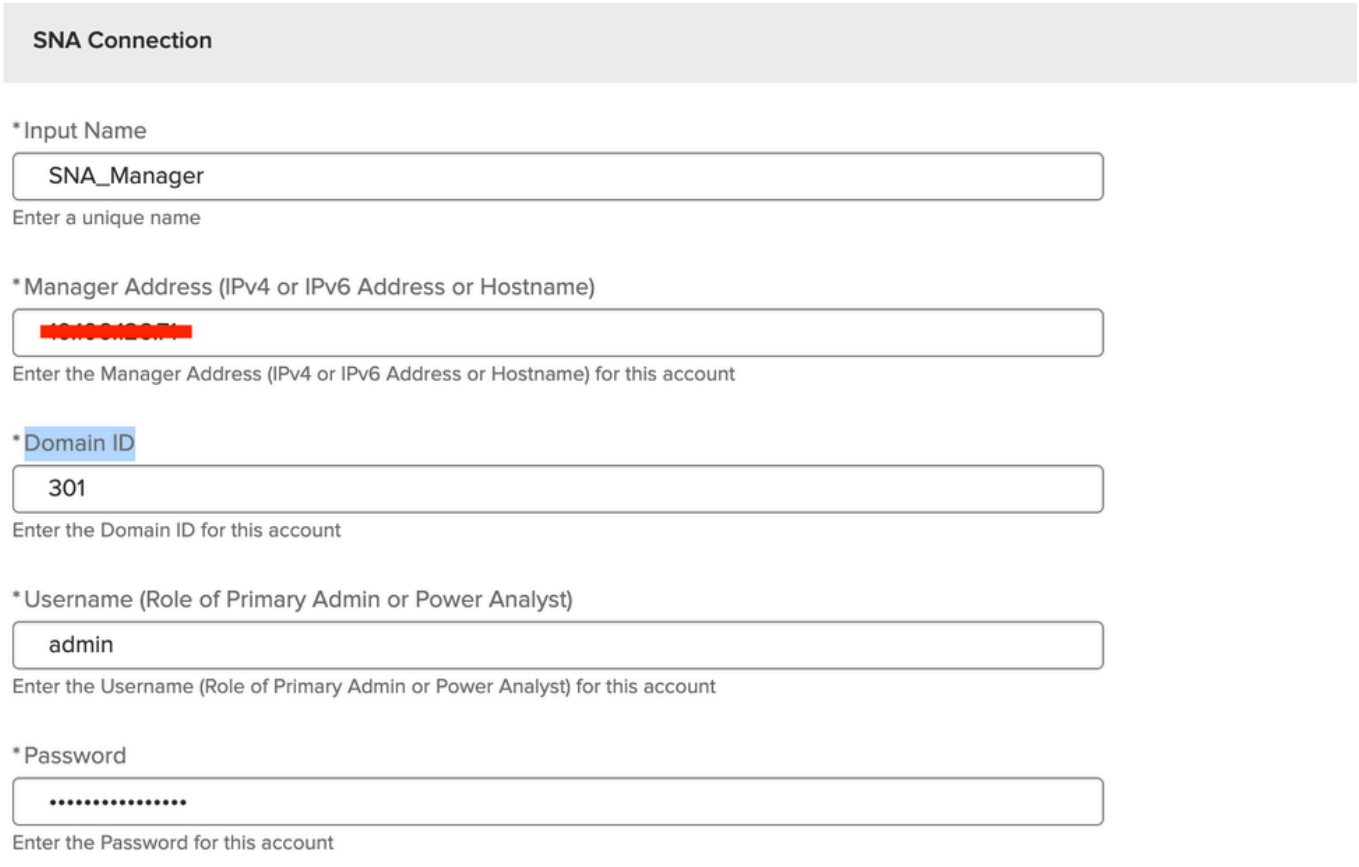


ii.構成オプションを選択すると、追加する詳細の構成ページがポップアップ表示されます。

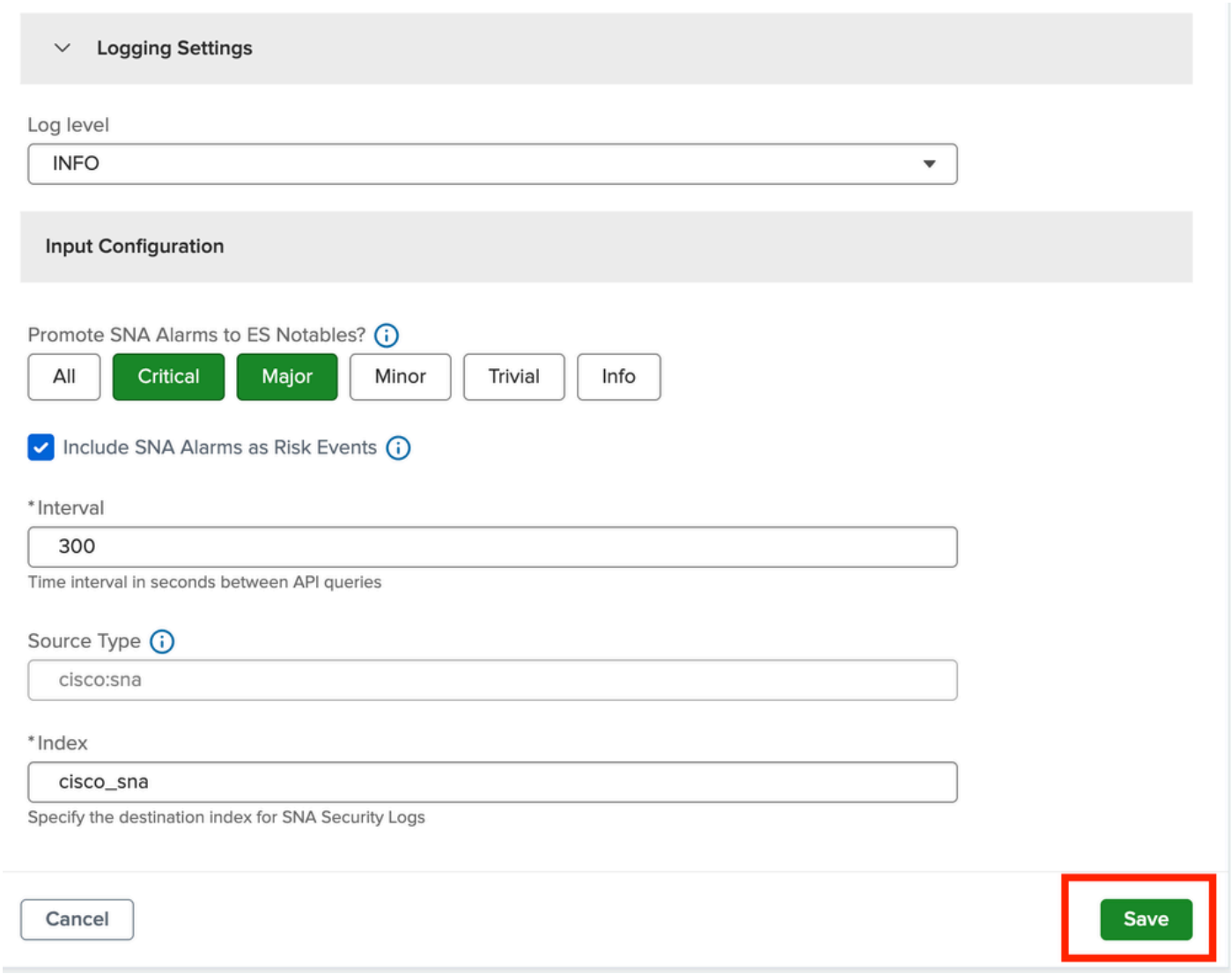


iii. SNA接続の詳細に関して説明した必須の詳細をすべて入力します。

1. Input Name:SNAの一意の名前
2. マネージャアドレス（IPv4またはIPv6アドレスまたはホスト名）：プライマリSNAマネージャの管理IP
3. ドメインID:domain_IDに対する値を入力します（例：301）。
4. ユーザ名：プライマリマネージャのユーザ名（adminなど）。
5. Password：プライマリマネージャユーザのパスワード



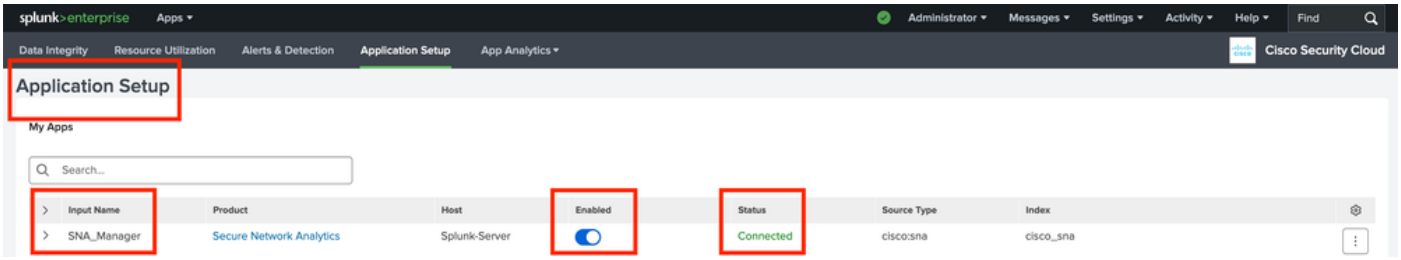
iv.残りの設定をデフォルト値のままにするか、必要に応じて変更してから、Saveをクリックします。完了すると、画面に正常なメッセージがポップアップ表示されます。



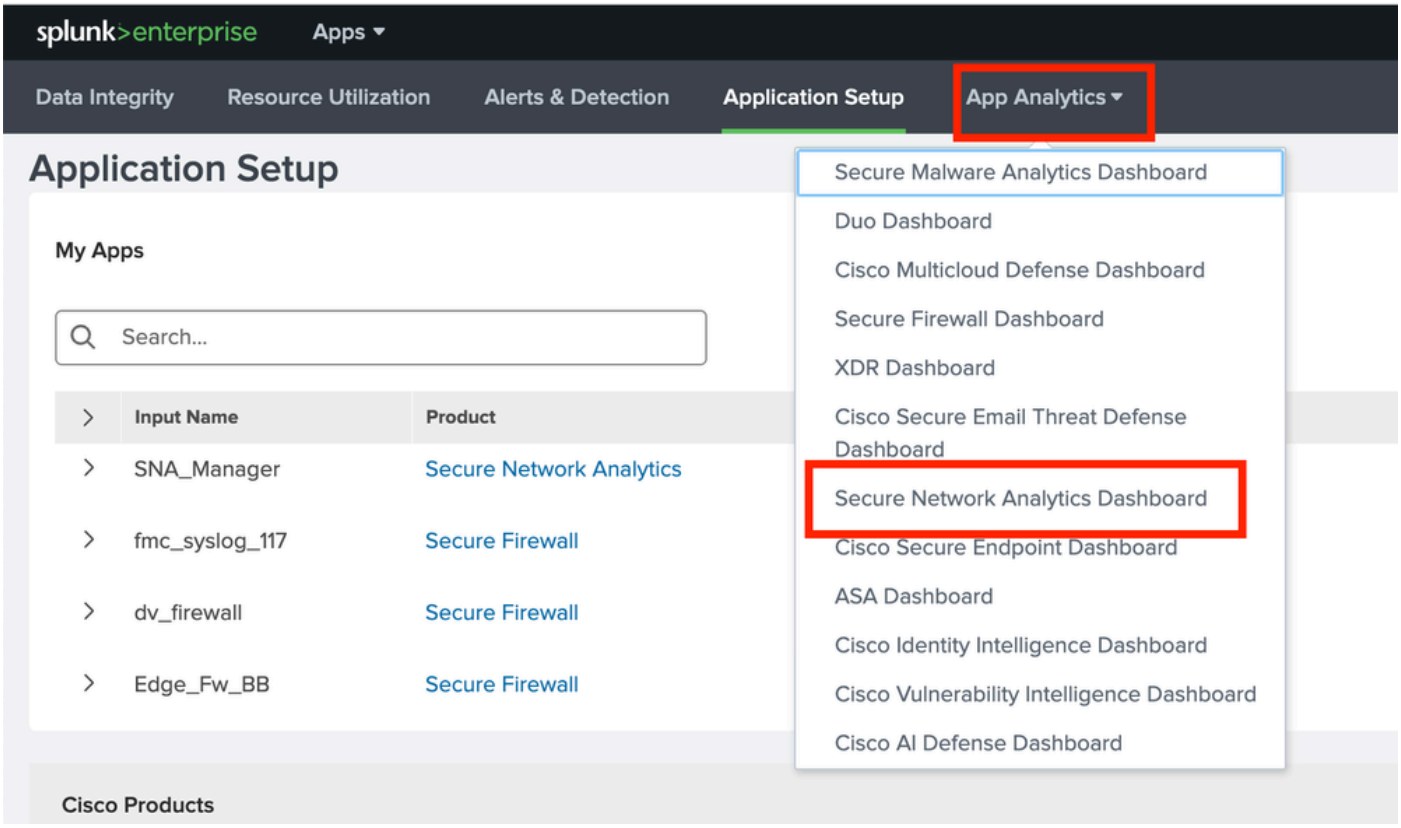
ステップ5：統合の検証。

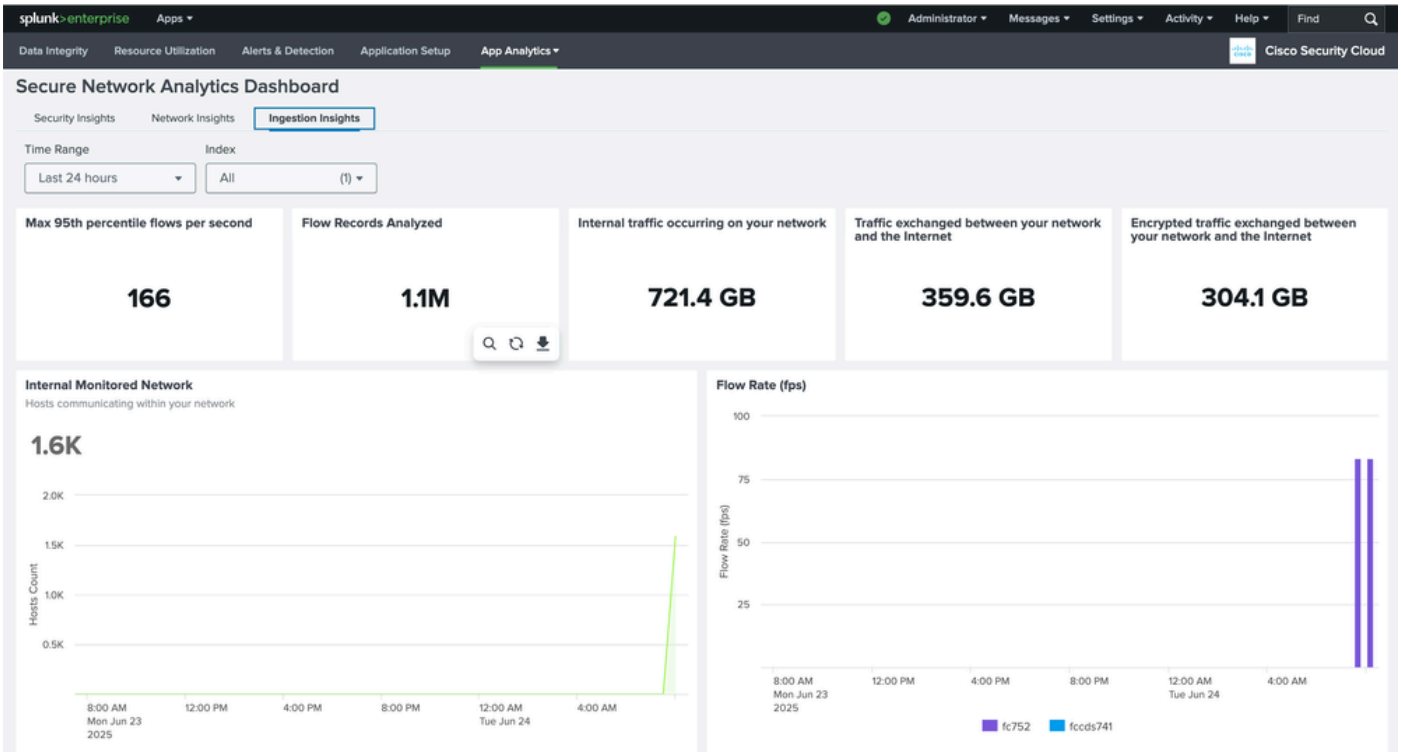
これは、前の手順で実行した統合が正常に実行されたかどうかを確認する必要がある重要な手順です。

i.入力の接続ステータスは、Application SetupタブでConnectedになっている必要があります。Inputフィールドの右側の名前は、デフォルトでEnabledになっています。



ii.ドロップダウンからSecure Network Analytics Dashboardを選択すると、最終的に統計がダッシュボードに反映され始めます。





FAQ

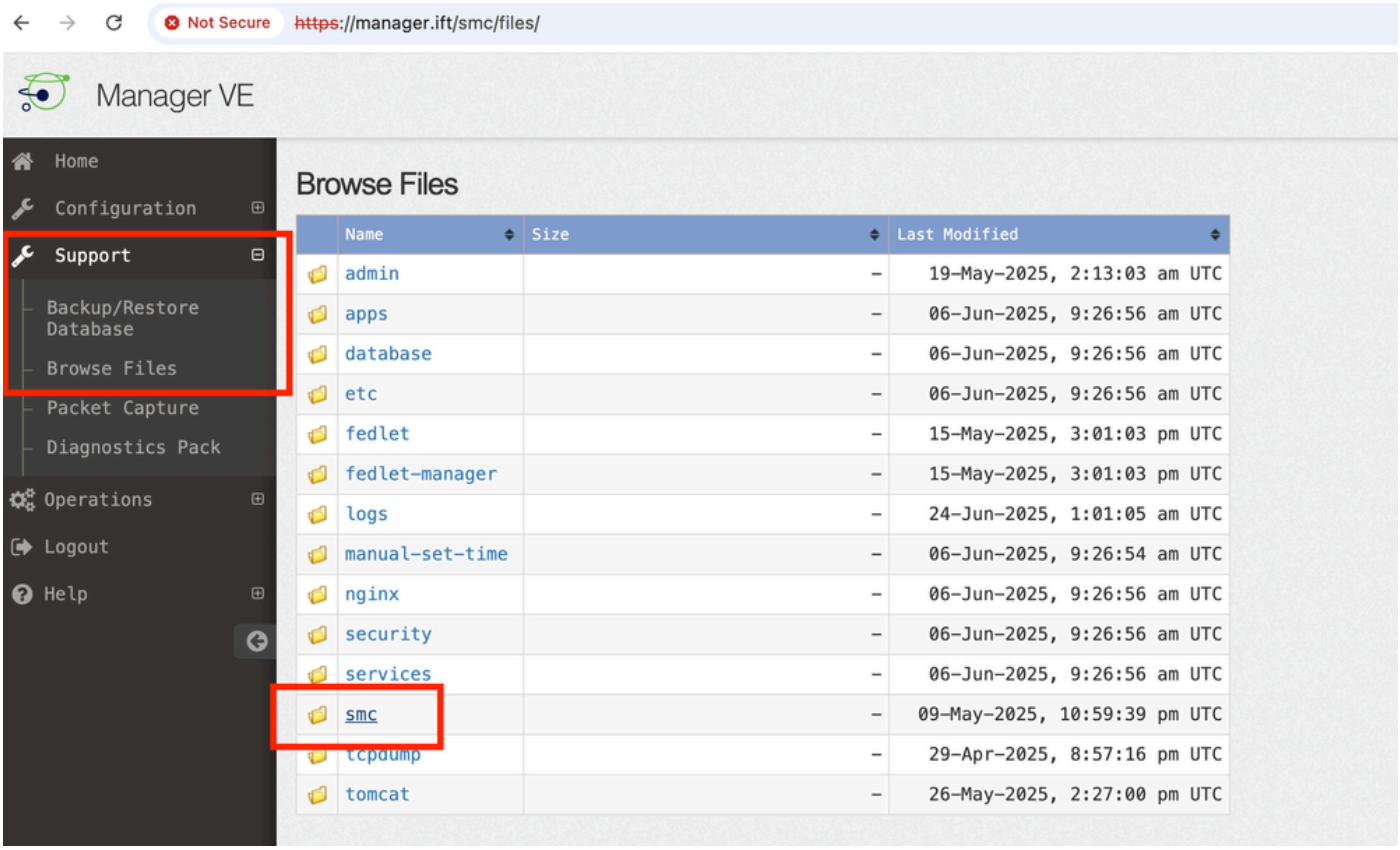
SNAマネージャのドメインIDの参照先

回答：

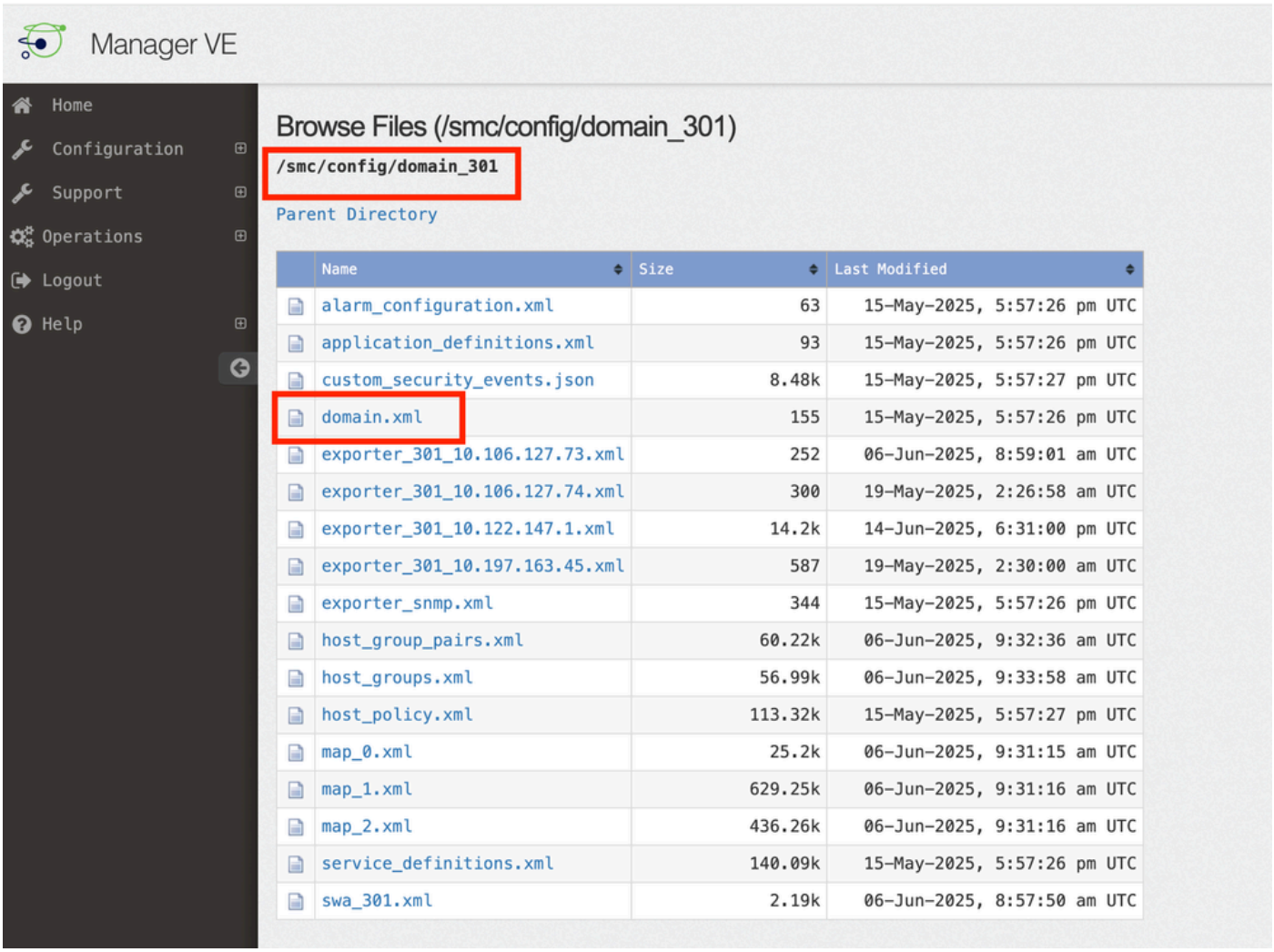
i. SNAプライマリマネージャにログインして、アプライアンス管理ページにリダイレクトするか

、マネージャIPインデックス URLにアクセスします。

ii. Supportセクションの下にあるsmcフォルダをブラウズします。



iii. configフォルダの下のdomain_XXXフォルダにあるdomain.xmlファイルを開きます。


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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。