

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[FAQ](#)

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

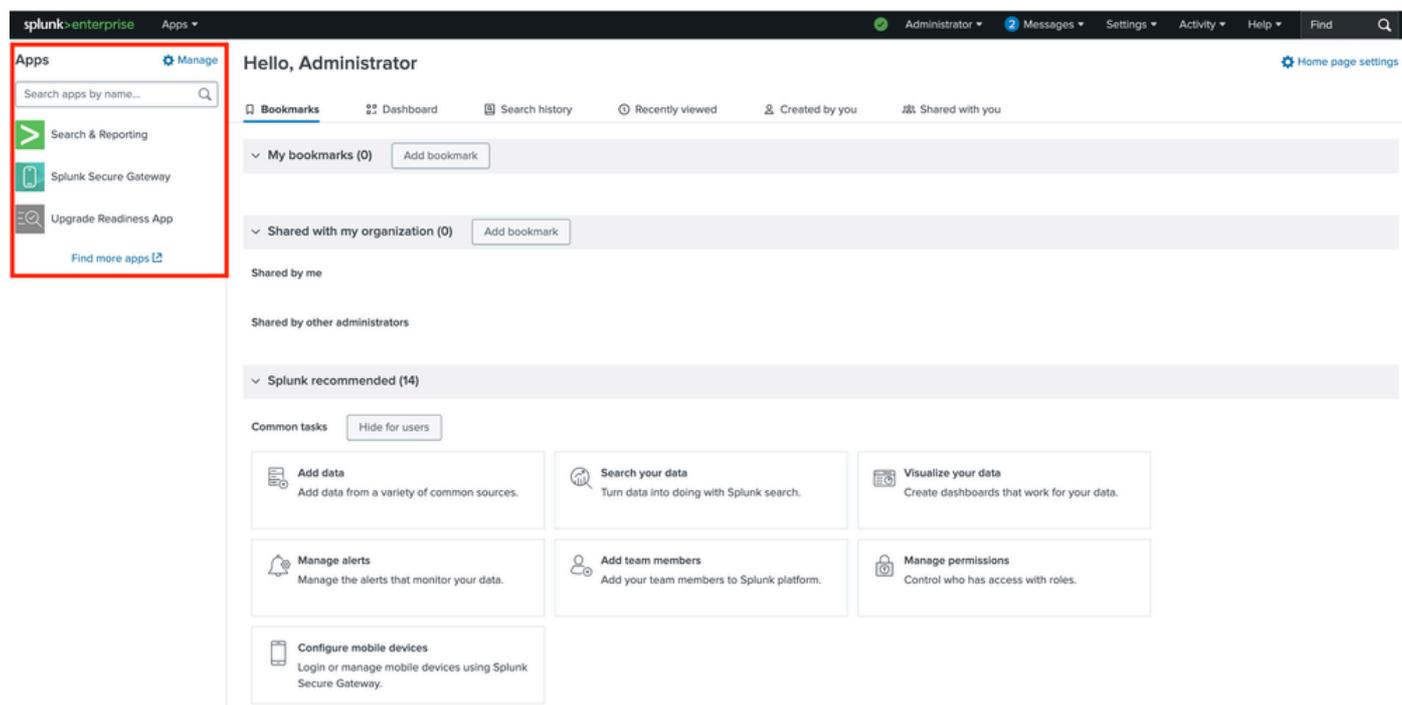
Secure Network Analytics v7.5.2

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

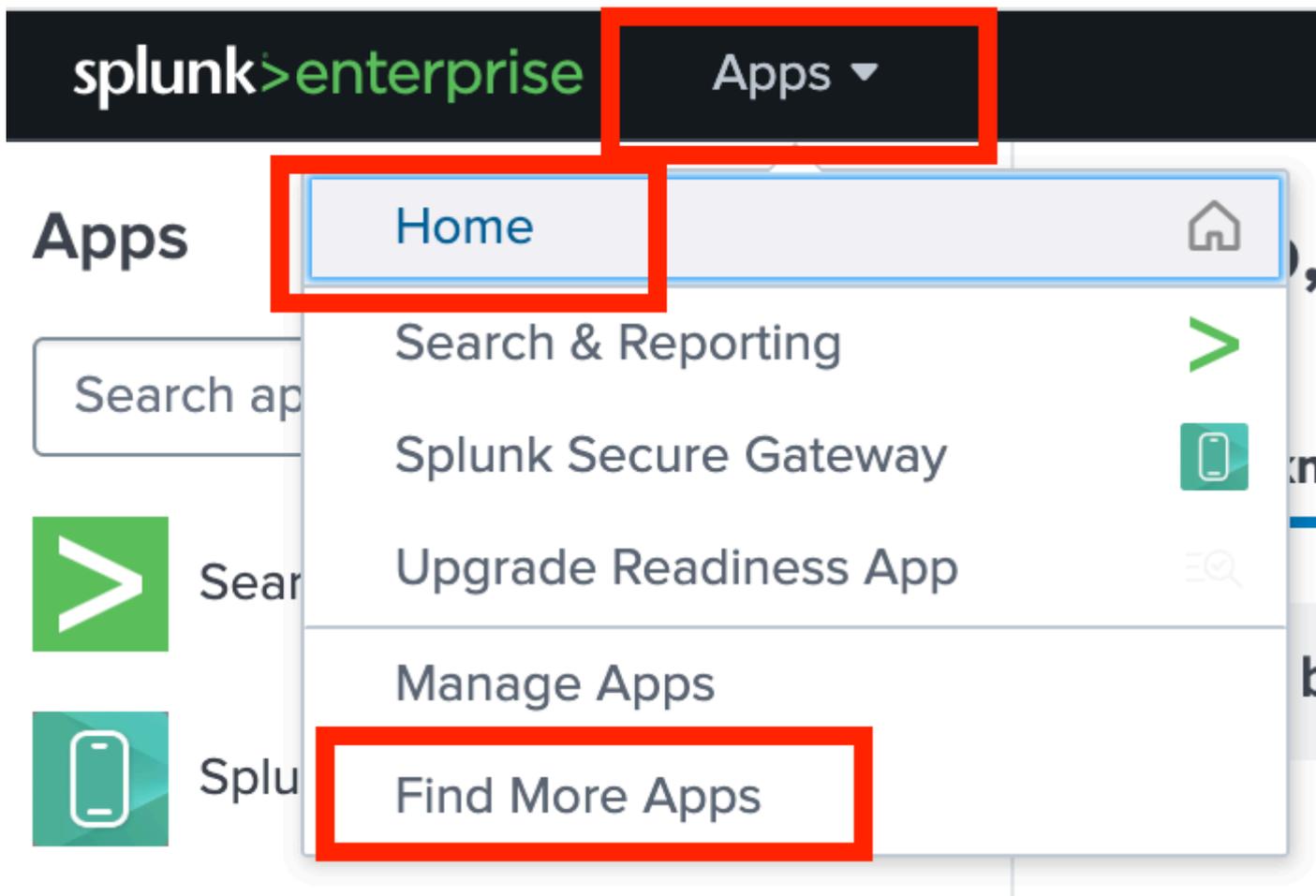
ステップ1: Splunkアプリケーションにアクセスし、Cisco Security Cloudアプリケーションをインストールします。

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。

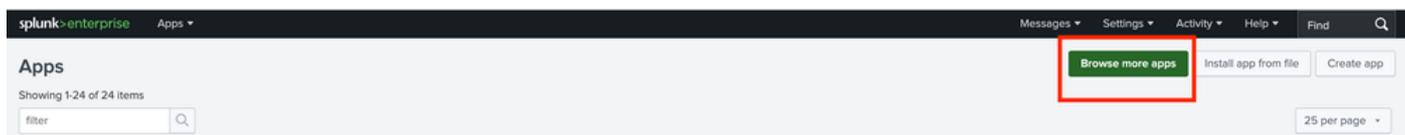


ii. SNAをSplunkと統合するには、Cisco Security Cloud Applicationをインストールする必要があります。このアプリケーションは、次のいずれかの方法で実行できます。

1. ドロップダウンからFind More Appsを選択します。

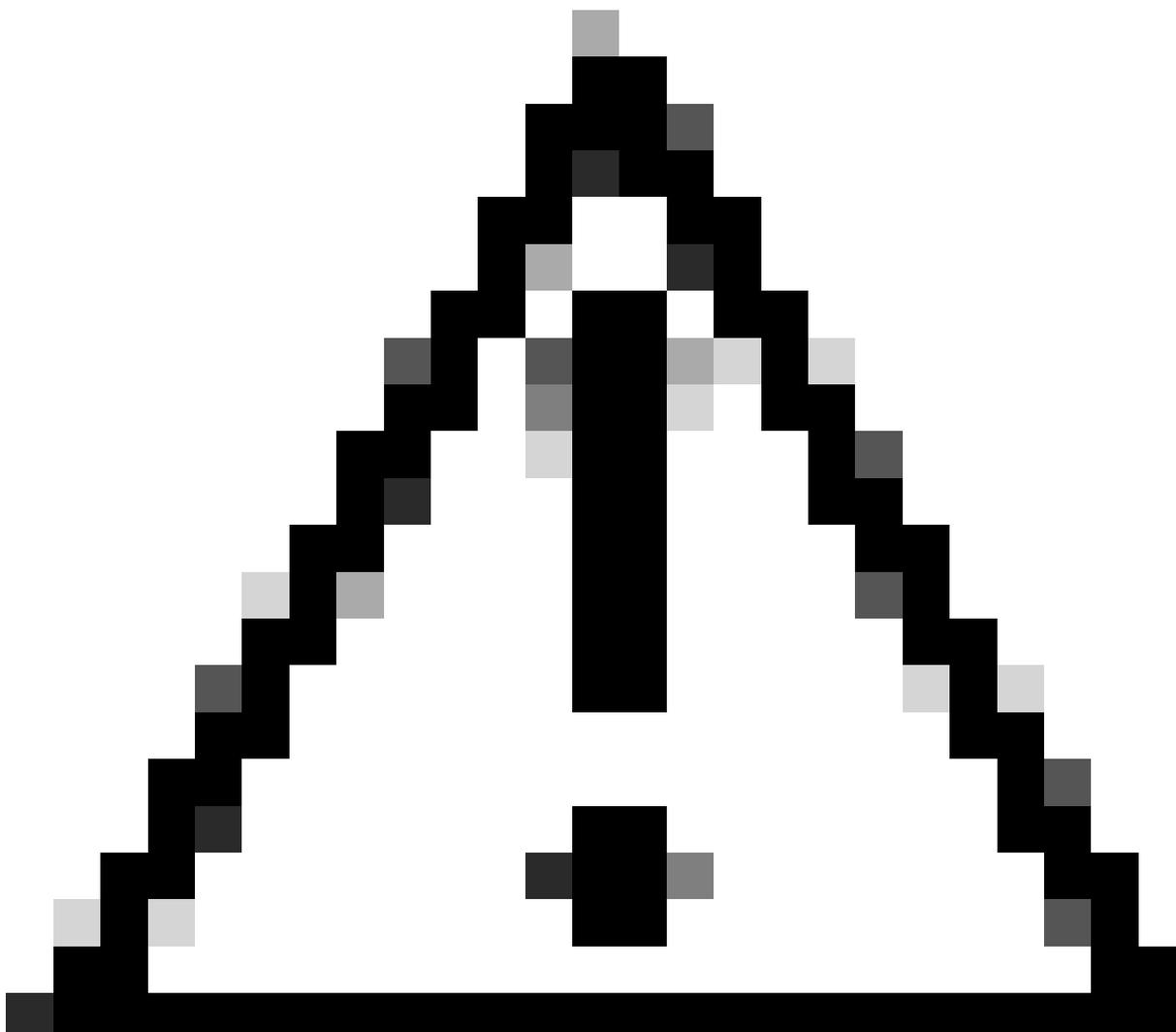


b. マネージャの歯車アイコンの下で、他のアプリケーションを参照します。

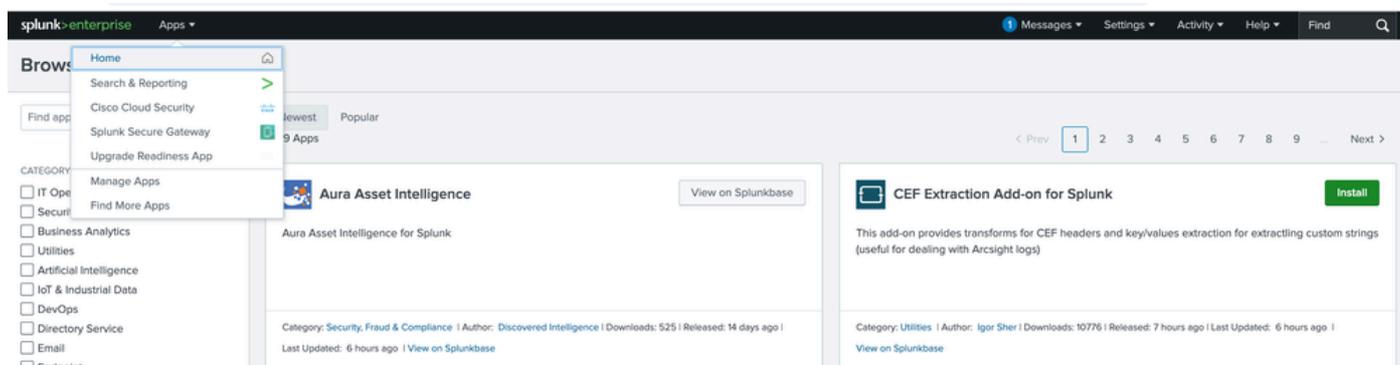


ステップ2: Cisco Security Cloud Applicationのインストール。

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。



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

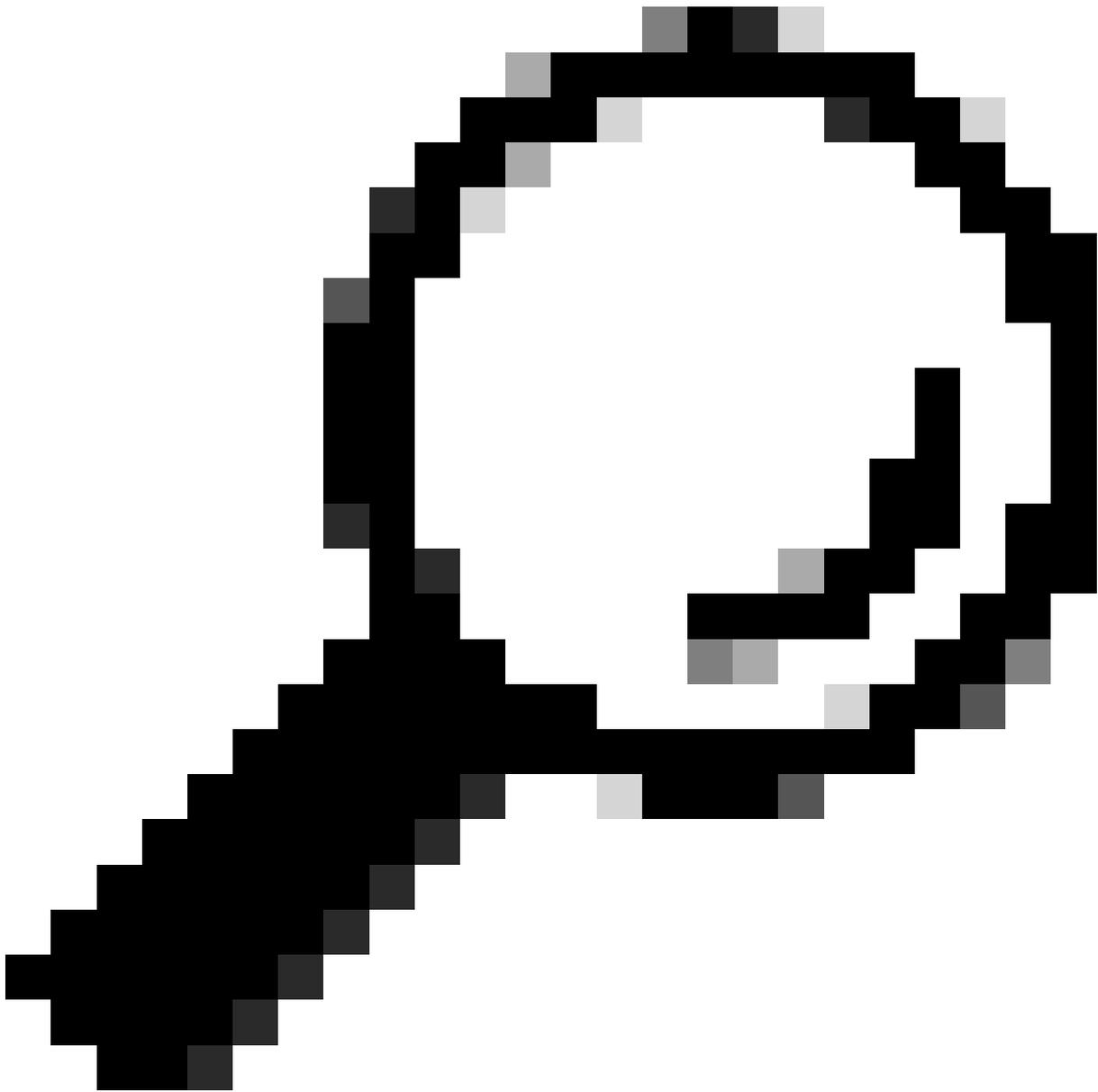
Cisco Email Threat Defense (ETD)

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. 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ヤルではなく、Splunkポータルへのアクセスに使用されるクレデンシヤルを指定します。

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. 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。

Complete



Cisco Security Cloud was successfully installed.

Open the App

Go Home

Done

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。

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. 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。

The screenshot shows the 'Application Setup' page in Splunk Enterprise. At the top, there are navigation tabs: Data Integrity, Resource Utilization, Alerts & Detection, Application Setup (selected), and App Analytics. Below the tabs, there are two search bars: 'My Apps' and 'Cisco Products'. The main content area displays six application cards, each with a logo, name, and a brief description. The cards are: Duo Network Security App, Secure Malware Analytics Network Security App, Secure Firewall Firewall App, Multicloud Defense Cloud Security App, Cisco Identity Intelligence Identity Security, and XDR Threat Detection and Response. Each card has a 'Learn More' button and a 'Configure Application' button.

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。

The screenshot shows the search results for 'secure network analytics'. The search bar at the top contains the text 'secure network analytics'. Below the search bar, the results for 'Secure Network Analytics Network Analytics' are displayed. The description reads: '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.' At the bottom of the result card, there are two buttons: 'Learn More' and 'Configure Application'. The 'Configure Application' button is highlighted with a red box.

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。

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. 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

SNA Connection

*Input Name

Enter a unique name

*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

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。

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

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。

| Input Name | Product | Host | Enabled | Status | Source Type | Index |
|-------------|--------------------------|---------------|---------|-----------|-------------|-----------|
| SNA_Manager | Secure Network Analytics | Splunk-Server | Enabled | Connected | cisco:sna | cisco_sna |

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。

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

Hours Count

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

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

FAQ

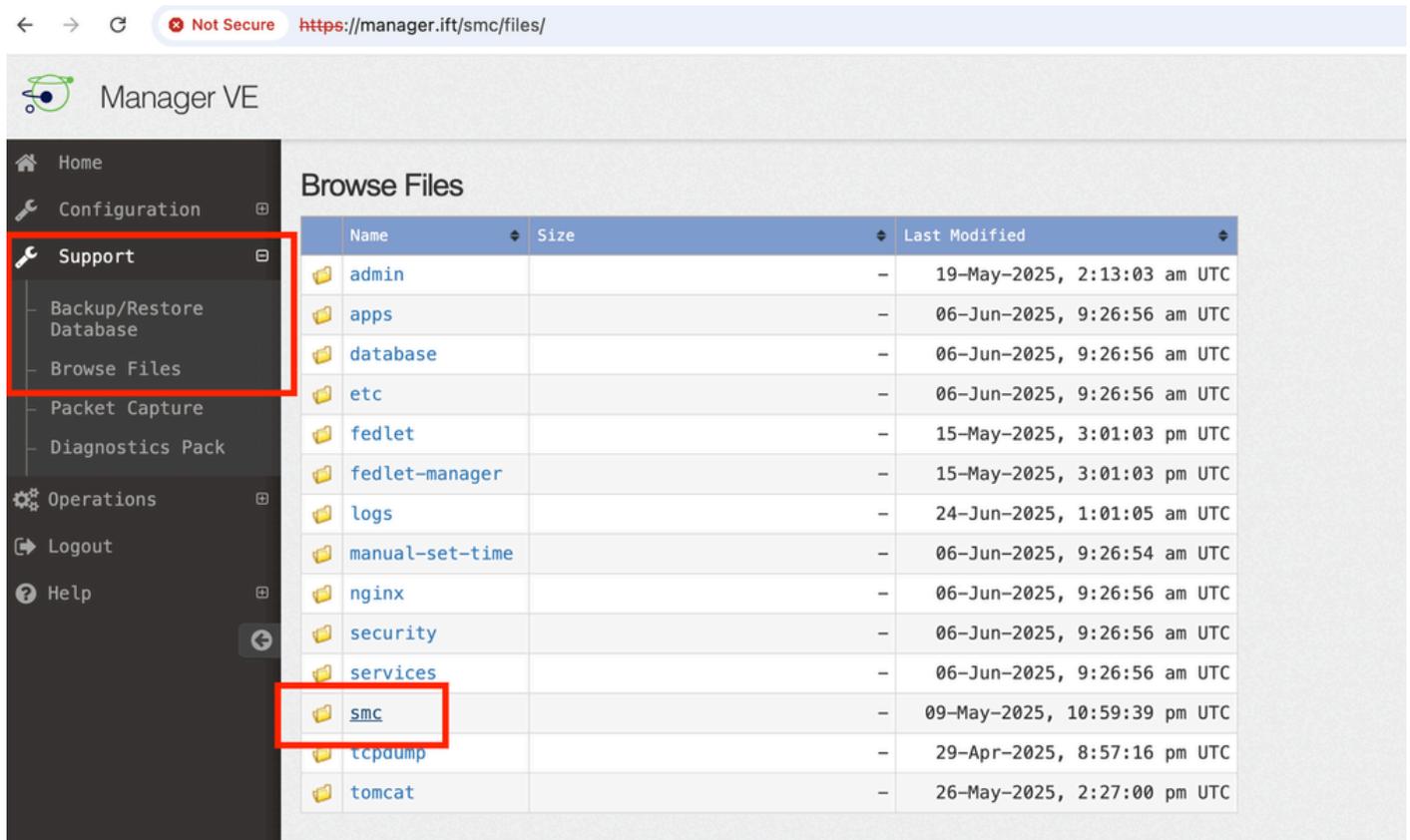
SNAマネージャのドメインIDの参照先

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。



The screenshot shows the Manager VE web interface. The browser address bar displays "Not Secure https://manager.ift/smc/files/". The interface includes a navigation sidebar on the left with the following items: Home, Configuration, Support (highlighted with a red box), Backup/Restore Database, Browse Files, Packet Capture, Diagnostics Pack, Operations, Logout, and Help. The main content area is titled "Browse Files" and contains a table with the following data:

| 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. 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。

- 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。