

# SNA integreren in Splunk met behulp van Security Cloud-applicatie

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Veelgestelde vragen](#)

---

## Inleiding

Dit document beschrijft de soepele SNA-integratie met Splunk met behulp van Cisco Security Cloud voor snellere incidentrespons voor de geïdentificeerde bedreigingen.

## Voorwaarden

Basiskennis van Splunk en Cisco Devices.

## Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende hardware- en softwareversies:

Splunk Enterprise

Secure Network ANalytics v7.5.2.

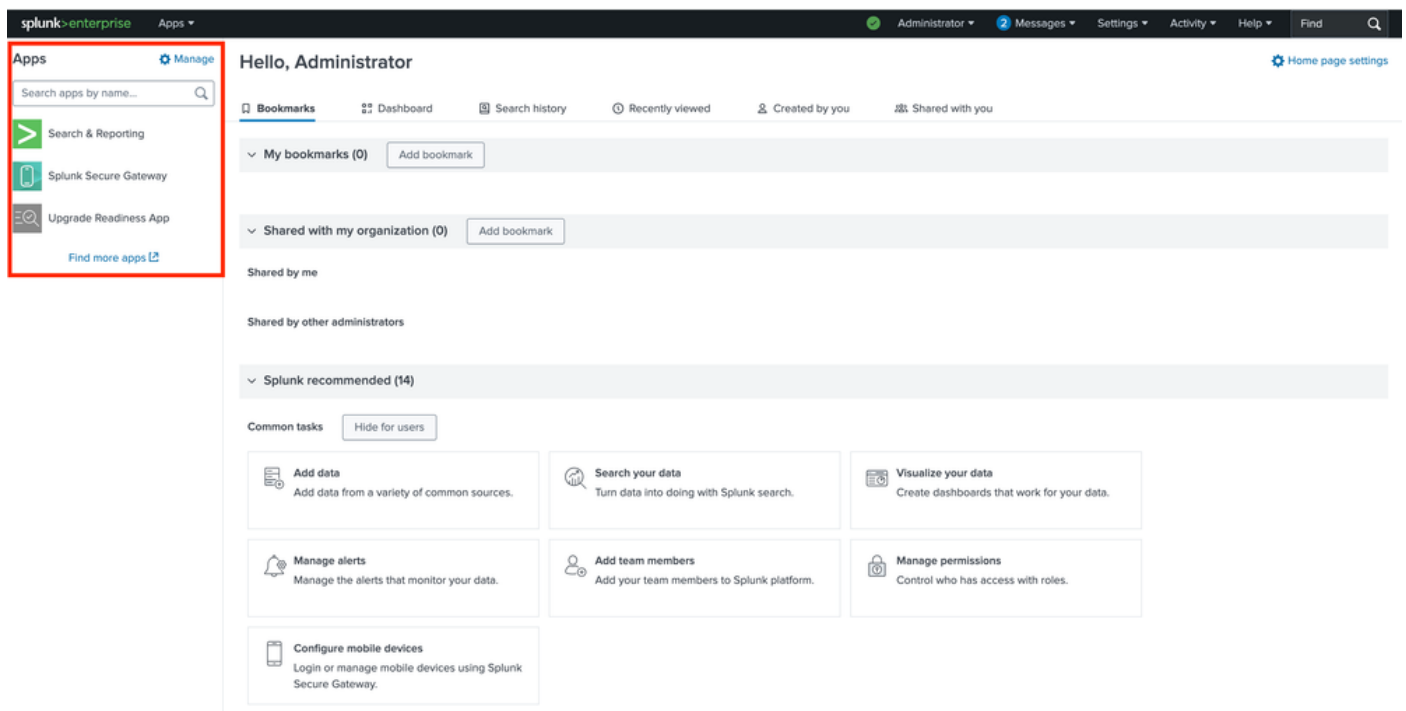
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Configureren

Stap 1: Toegang krijgen tot de Splunk-applicatie en de Cisco Security Cloud-applicatie installeren.

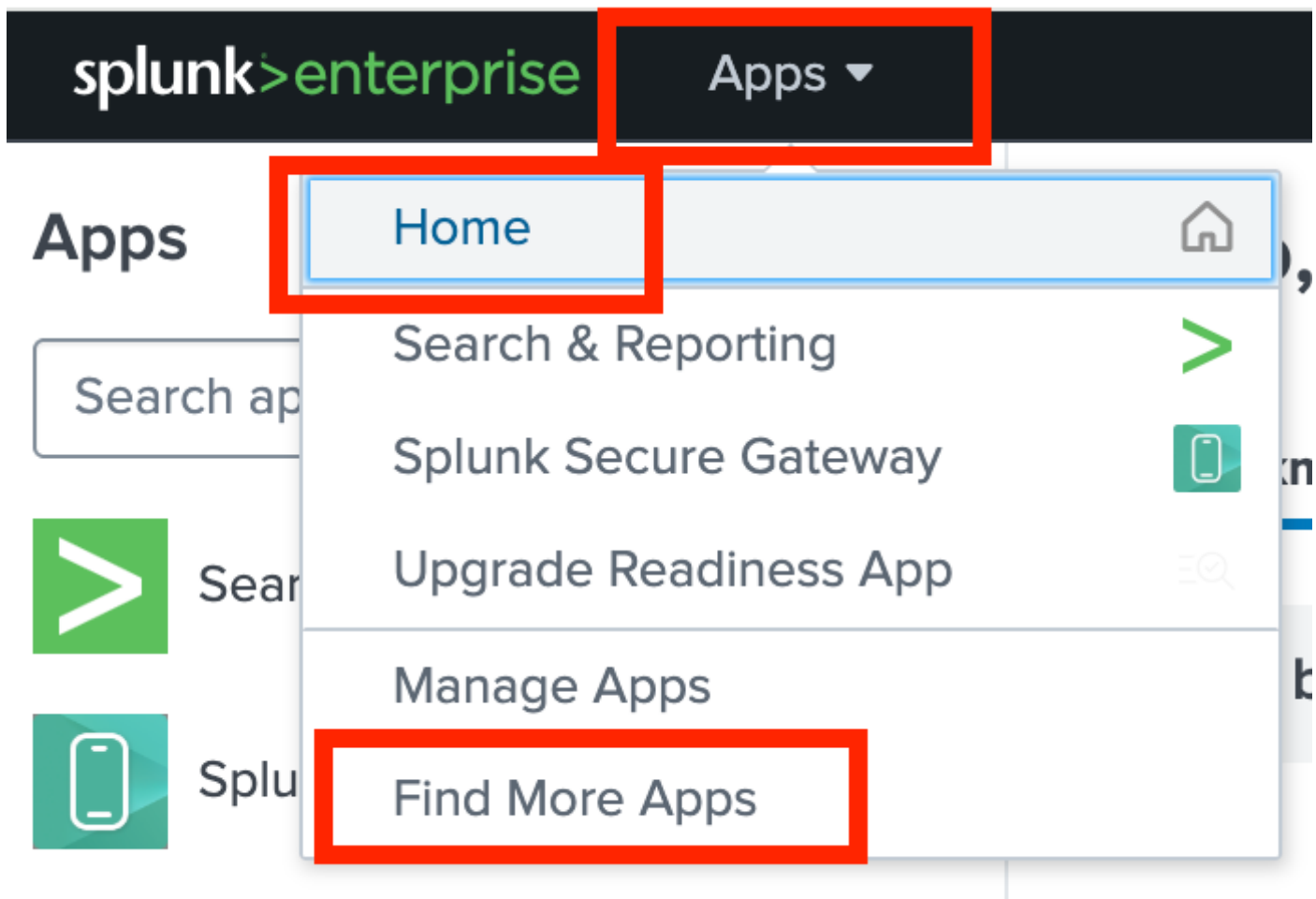
1. Meld u aan bij het Splunk-webportaal met de beheerdersreferenties en bij succesvol

inloggen, is de startpagina te zien met de lijst met geïnstalleerde toepassingen aan de linkerkant onder het gedeelte App:

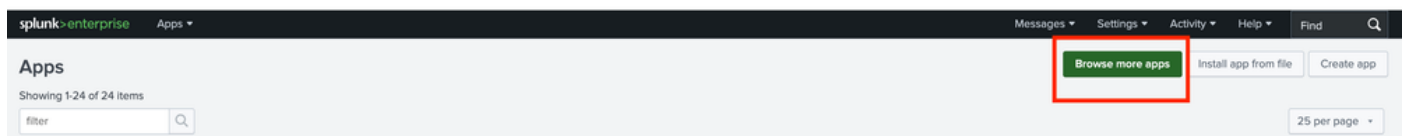


2. Voor de integratie van het SNA met Splunk moet de Cisco Security Cloud Application worden geïnstalleerd die kan worden bereikt met een van de genoemde methoden:

1. Selecteer Meer apps zoeken in de vervolgkeuzelijst.

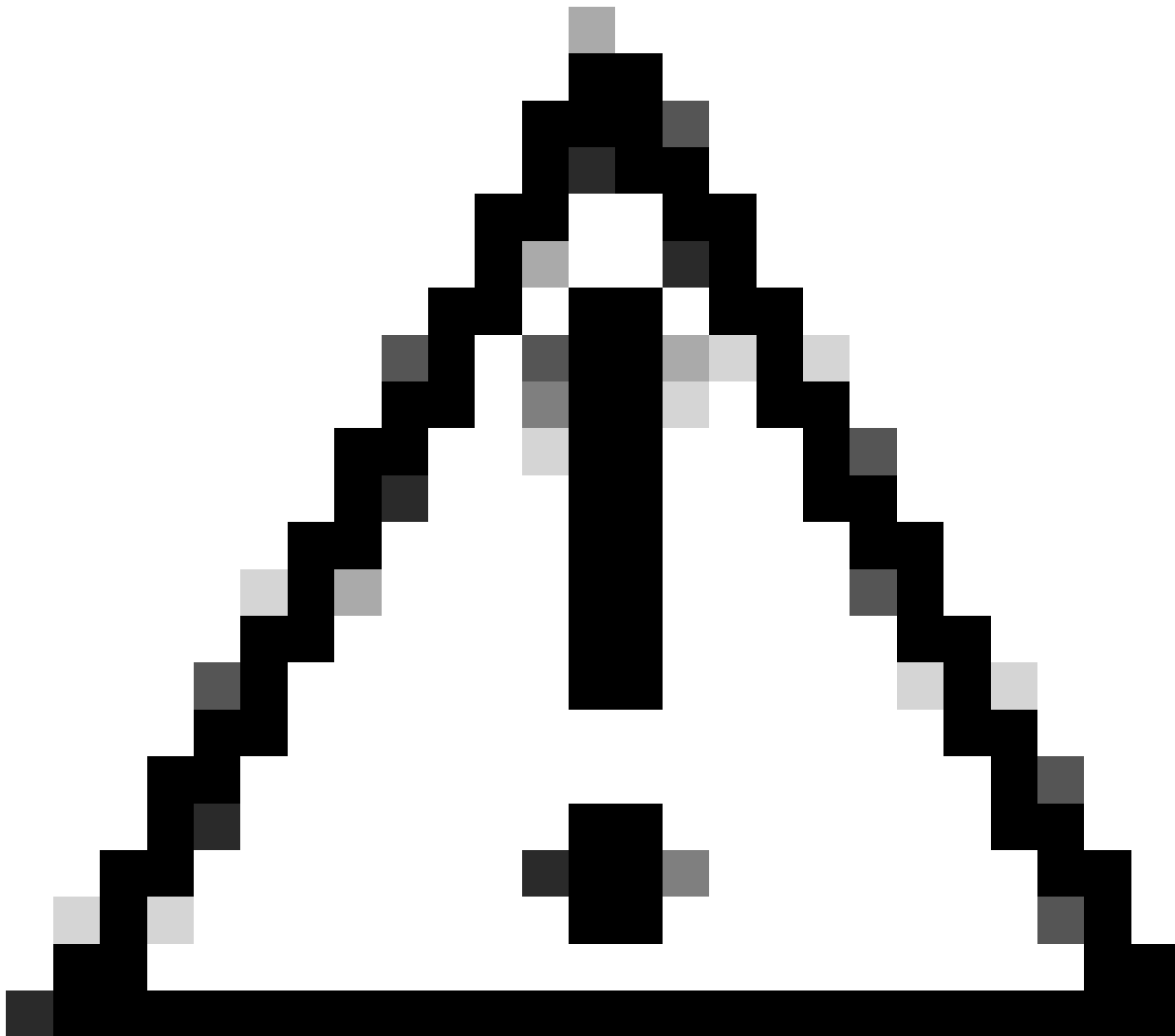


b. Blader door meer apps onder het tandwielpictogram Manager.

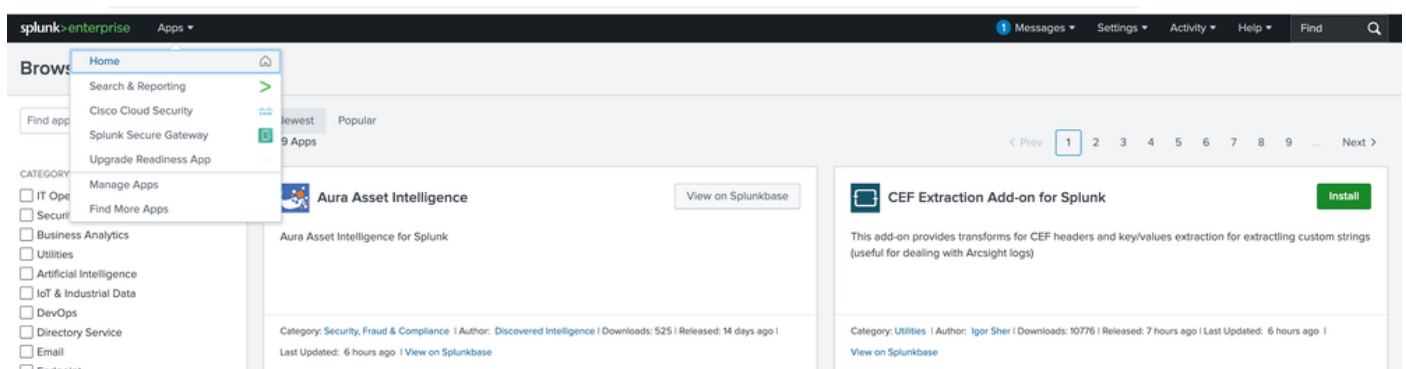


Stap 2: Installatie van de Cisco Security Cloud-applicatie.

i. Zoek naar de Cisco Security Cloud-toepassing. Blader nu naar beneden totdat u de app hebt gevonden of zoek naar Cisco Security Cloud.



Let op: raak niet in de war met de Cisco Cloud Security App.



i. Installeer de toepassing door op de knop Installeren te klikken.



## Cisco Security Cloud

[Install](#)

The Cisco **Author** 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

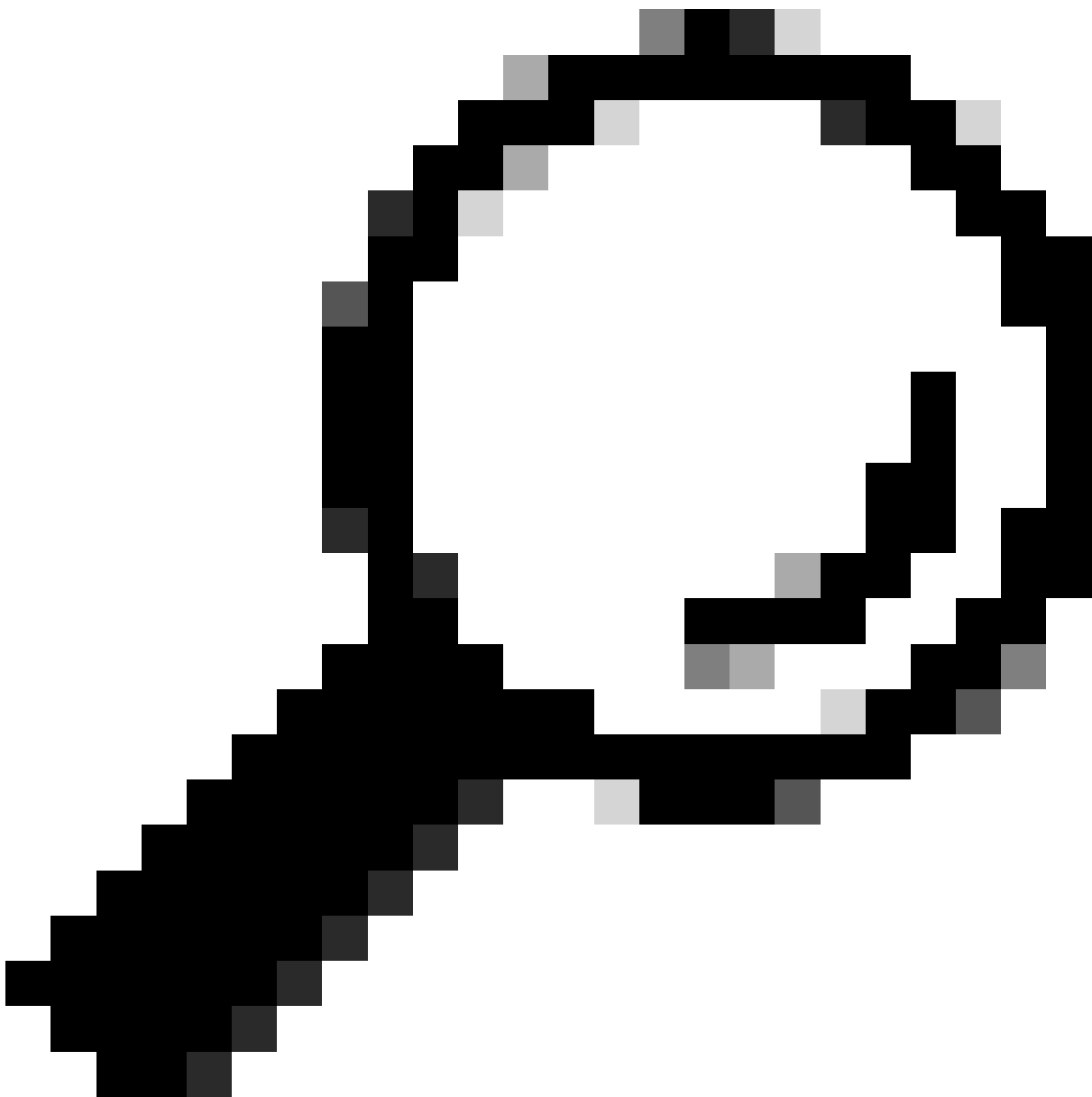
Cisco Email Threat Defense (ETD)

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](#)

- ii. Op het moment dat u op de installatieknop klikt, verschijnt een venster waarin u wordt gevraagd naar de referenties van de Splunk-account voordat u de toepassing installeert. Geef de referenties op en klik op Akkoord en Installeren om verder te gaan.



Tip: Geef de referenties op die worden gebruikt om toegang te krijgen tot het Splunk-portaal, niet de beheerdersreferenties die worden gebruikt voor Splunk-bedrijfstoeppingen tijdens het inloggen.

---

## 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](#).

Cancel

Agree and Install

iii. Er verschijnt een bericht over de geslaagde installatie van de toepassing zoals afgebeeld. Klik op Gereed.

## Complete



Cisco Security Cloud was successfully installed.

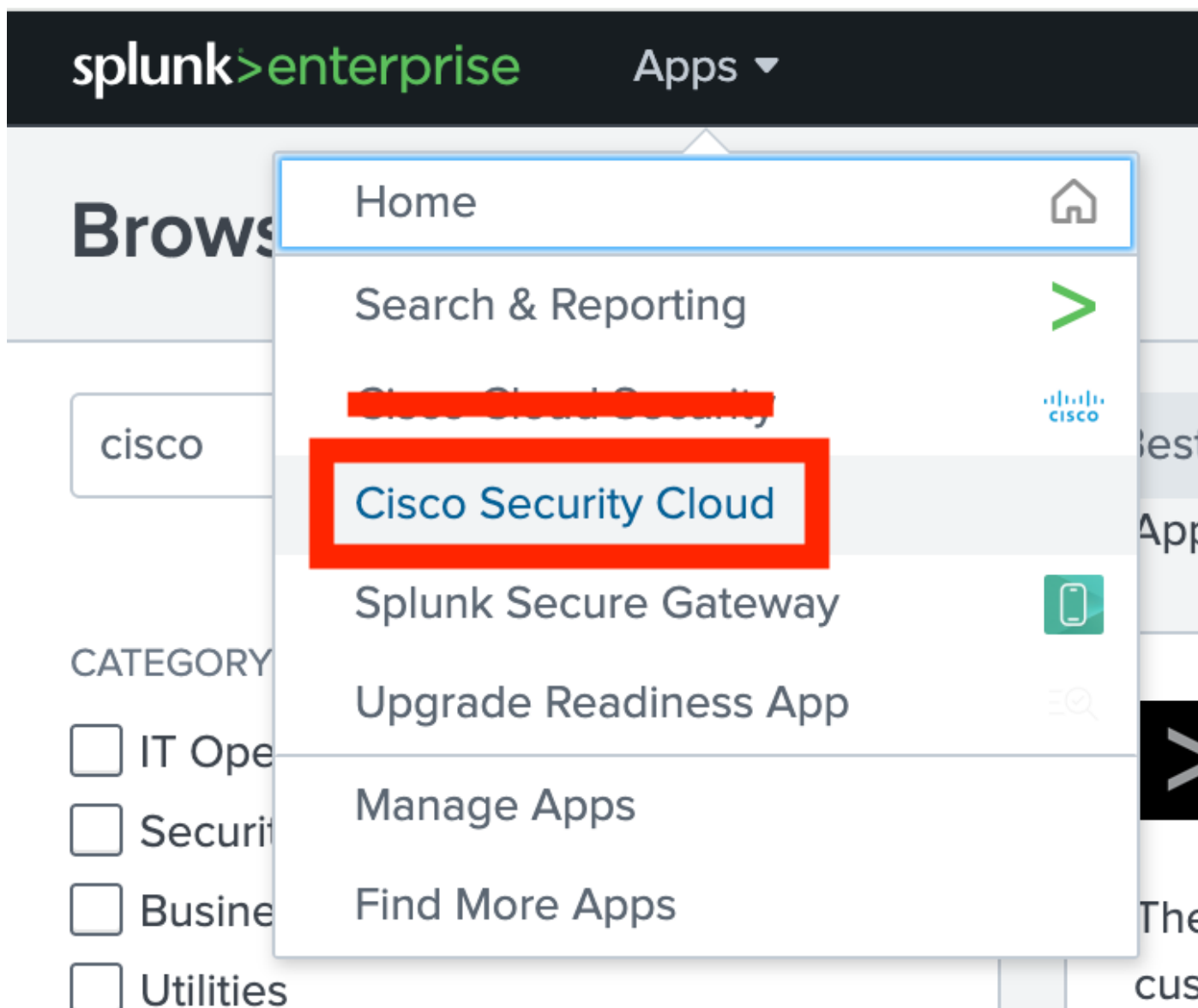
Open the App

Go Home

Done

Stap 3: Verificatie van de installatie van de Cisco Security Cloud-applicatie.

i. Klik op de vervolgkeuzelijst Apps en nu is de app te zien in de lijst na de succesvolle installatie:



- ii. Selecteer Cisco Security Cloud door erop te klikken. U wordt doorgestuurd naar de pagina Toepassingsinstellingen waar alle beschikbare Cisco Cloud-beveiligingsproducten te vinden zijn.

**splunk>enterprise** Apps ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

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

### Application Setup

My Apps

Q Search...

| >              | Input Name | Product | Host | Enabled | Status | Source Type | Index |
|----------------|------------|---------|------|---------|--------|-------------|-------|
| Cisco Products |            |         |      |         |        |             |       |
| Q Search...    |            |         |      |         |        |             |       |

**Duo**  
Network Security App

Zero trust is the future of information security - and Duo is your rock-solid foundation. Duo secures your workforce, taking access security beyond the corporate network perimeter to protect your data at every authentication attempt, from any device, anywhere. Confirm user identities in a snap, monitor the health of managed and unmanaged devices, set adaptive security policies tailored for your business, secure remote access without a device agent, and provide secure, user-friendly single sign-on, quickly and easily with Duo.

[Learn More](#) [Configure Application](#)

**Secure Malware Analytics**  
Network Security App

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect organizations from malware. Secure Malware Analytics is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impacting the user environment.

[Learn More](#) [Configure Application](#)

**Secure Firewall**  
Firewall App

The integration of Secure Firewall Threat Defense (formerly Firepower Threat Defense) provides the capability to investigate, identify, and enrich Cisco Secure Firewall intrusion events with context from integrations across the integrated products. It offers an automated triage and prioritization of intrusion events through incidents.

[Learn More](#) [Configure Application](#)

**Multicloud Defense**  
Cloud Security App

Cisco Multicloud Defense protects all of your cloud environments using a single software-as-a-service (SaaS) control plane, eliminating inefficient, complex, and costly point solutions.

[Learn More](#) [Configure Application](#)

**Cisco Identity Intelligence**  
Identity Security

As organizations face growing complexity in identity management, Cisco Identity Intelligence focuses on detecting, monitoring, and responding to identity-based threats. By centralizing and correlating identity data, it provides visibility into user behaviors and risks. With its ITDR and identity posture management capabilities, security teams can proactively detect and mitigate threats in real-time, using AI-powered insights to uncover anomalies and malicious activities, ensuring a robust identity security posture.

[Learn More](#) [Configure Application](#)

**XDR**  
Threat Detection and Response

Cisco XDR changes the way security teams look at detection and response. Our cloud-based solution is designed to simplify security operations and empower security teams to detect, prioritize, and respond to the most sophisticated threats. Integrating with the broader Cisco security portfolio and select third-party offerings, Cisco XDR is one of the most comprehensive and flexible solutions on the market today.

[Learn More](#) [Configure Application](#)

#### Stap 4: Integratie met Secure Network Analytics (SNA).

Het doel van dit document is om de installatiestappen van de Splunk met Secure Network Analytics (SNA) nader te belichten.

i. Zoek naar de Secure Network Analytics en selecteer Toepassing configureren wanneer deze wordt weergegeven:

Q secure network analytics X

**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.

[Learn More](#) [Configure Application](#)

ii. Wanneer u de configuratieoptie selecteert, verschijnt de configuratiepagina voor de details die u wilt toevoegen.

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. Vul alle verplichte gegevens in zoals vermeld voor de SNA Connection Details:

1. Invoernaam: elke unieke naam voor SNA
2. Adres Manager (IPv4- of IPv6-adres of hostnaam): IP-beheer van de primaire SNA-manager
3. Domein-ID: Voer de waarde in tegen domein\_ID (bijvoorbeeld 301)
4. Gebruikersnaam: De gebruikersnaam van de primaire beheerder (bijvoorbeeld admin)
5. Wachtwoord: Wachtwoord van de primaire beheerder gebruiker

### 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. Laat de overige instellingen op hun standaardwaarden staan of wijzig ze indien nodig en klik op Opslaan. Een succesvol bericht verschijnt op het scherm na de voltooiing.

Logging Settings

Log level

INFO

Input Configuration

Promote SNA Alarms to ES Notables?

AllCriticalMajorMinorTrivialInfo

☒ 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

CancelSave

Stap 5: Verificatie van de integratie.

Dit is een belangrijke stap waarbij u moet controleren of de integratie die in de vorige stap is uitgevoerd, al dan niet succesvol is uitgevoerd.

i. De verbindingstatus voor de invoer moet worden verbonden op het tabblad Toepassingsinstellingen met standaard als Ingeschakeld voor de juiste naam in het Input-veld.

| Application Setup |                          |               |                                     |           |             |           |
|-------------------|--------------------------|---------------|-------------------------------------|-----------|-------------|-----------|
| 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. Selecteer het Secure Network Analytics Dashboard in de vervolgkeuzelijst en de statistieken beginnen uiteindelijk te reflecteren op het dashboard.

splunk>enterprise Apps ▾

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

## Application Setup

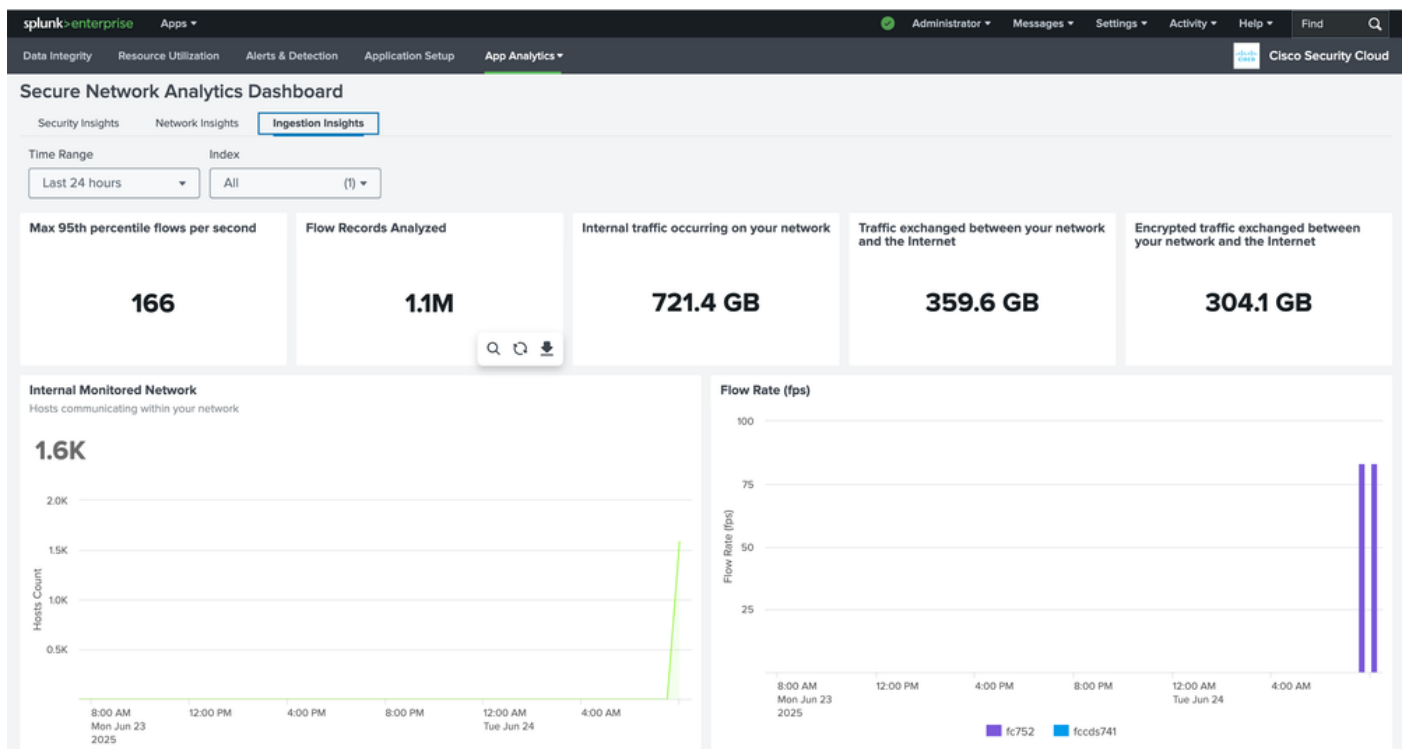
My Apps

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



## Veelgestelde vragen

Waar vind je de domein-id voor de SNA-manager?

Antwoord:

i. Meld u aan bij het primaire SNA-beheer en verwijst naar de pagina Toestelbeheer of de [IP Index-](#)

URL van [Access Manager](#).

ii. Blader door de map smc onder de sectie Ondersteuning.

← → ↻ Not Secure https://manager.ift/smc/files/

Manager VE

- Home
- Configuration
- Support**
  - Backup/Restore Database
  - Browse Files
  - Packet Capture
  - Diagnostics Pack
- Operations
- Logout
- Help

### Browse Files

| 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  |
| <b>smc</b>      |      | 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. Open het bestand domain.xml dat beschikbaar is in de map domain\_XXX onder de map 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 |

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.