

Integration von SNA in Splunk mithilfe der Security Cloud-Anwendung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Häufig gestellte Fragen](#)

Einleitung

In diesem Dokument wird die reibungslose SNA-Integration mit Splunk unter Verwendung der Cisco Security Cloud für eine schnellere Reaktion auf Vorfälle bei den erkannten Bedrohungen beschrieben.

Voraussetzungen

Grundkenntnisse von Splunk und Cisco Devices

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Software-Versionen:

Splunk Enterprise

Secure Network Analytics v7.5.2

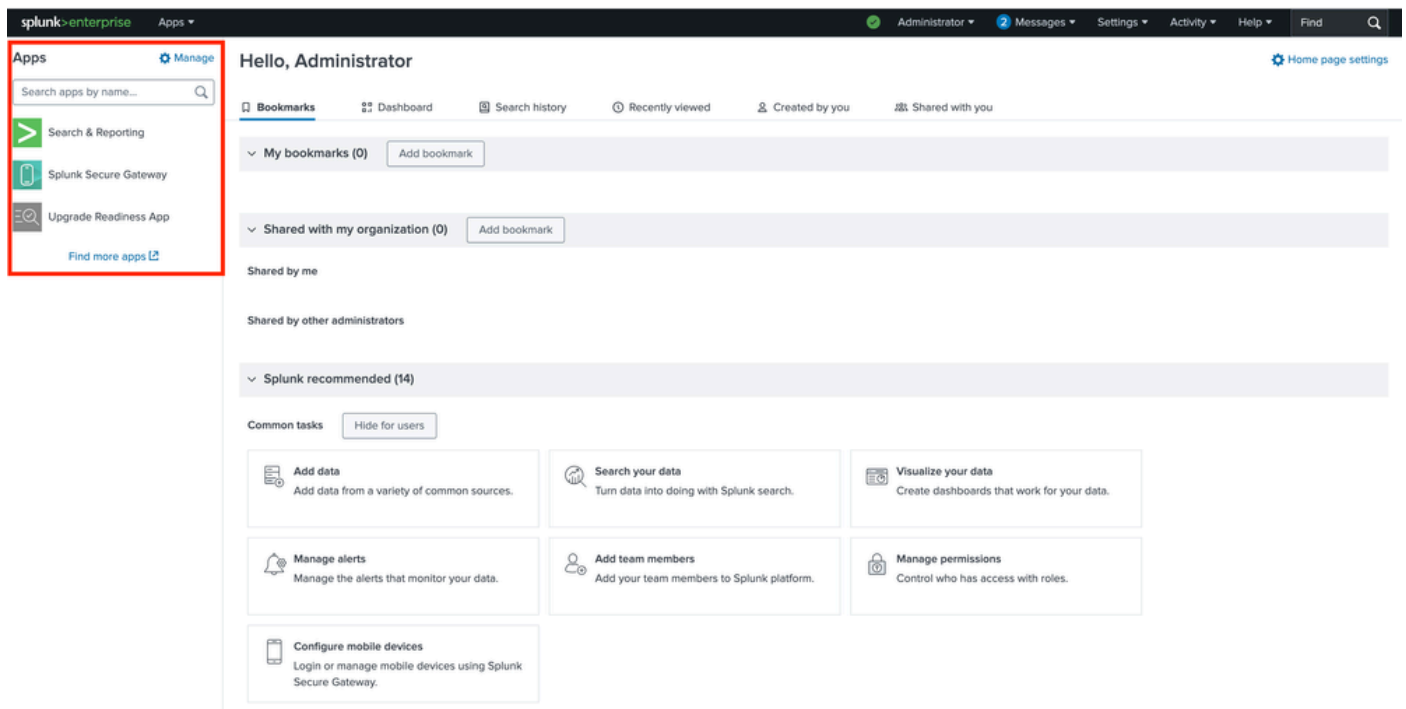
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Schritt 1: Greifen Sie auf die Splunk-Anwendung zu, und installieren Sie die Cisco Security Cloud-

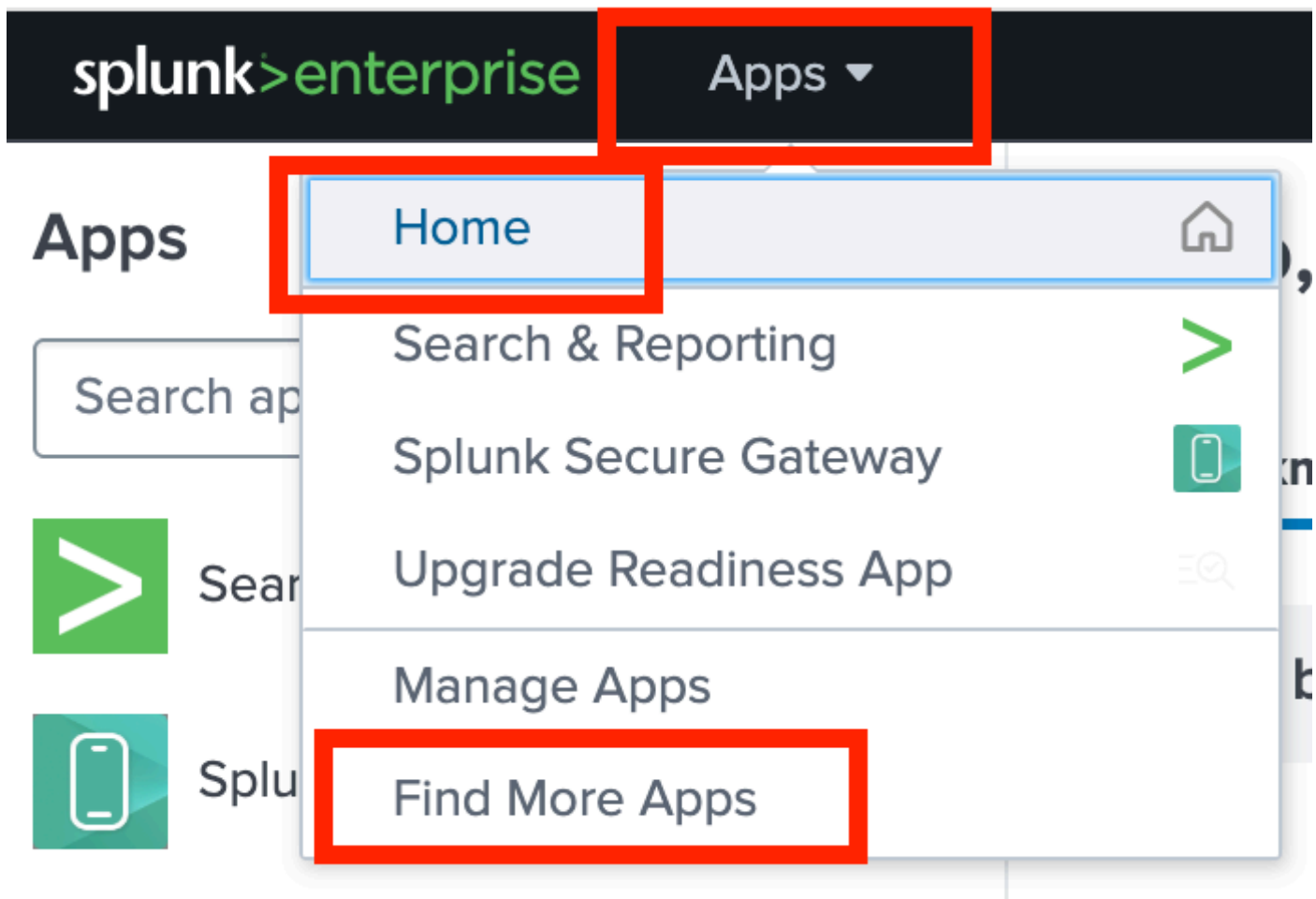
Anwendung.

1. Melden Sie sich mit den Administratorrechten beim Splunk-Webportal an, und nach erfolgreicher Anmeldung wird die Startseite mit der Liste der installierten Anwendungen auf der linken Seite unter dem App-Abschnitt angezeigt:

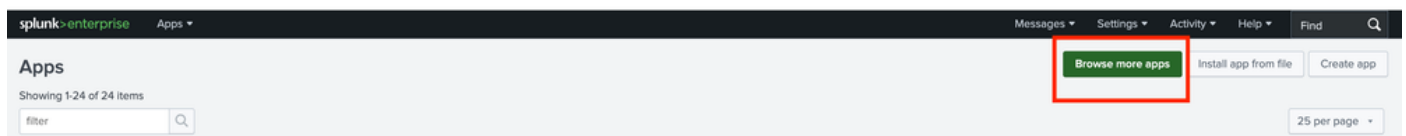


2. Für die Integration der SNA mit Splunk muss die Cisco Security Cloud-Anwendung installiert werden, die mit einer der folgenden Methoden erreicht werden kann:

1. Wählen Sie im Dropdown-Menü die Option Weitere Apps suchen aus.

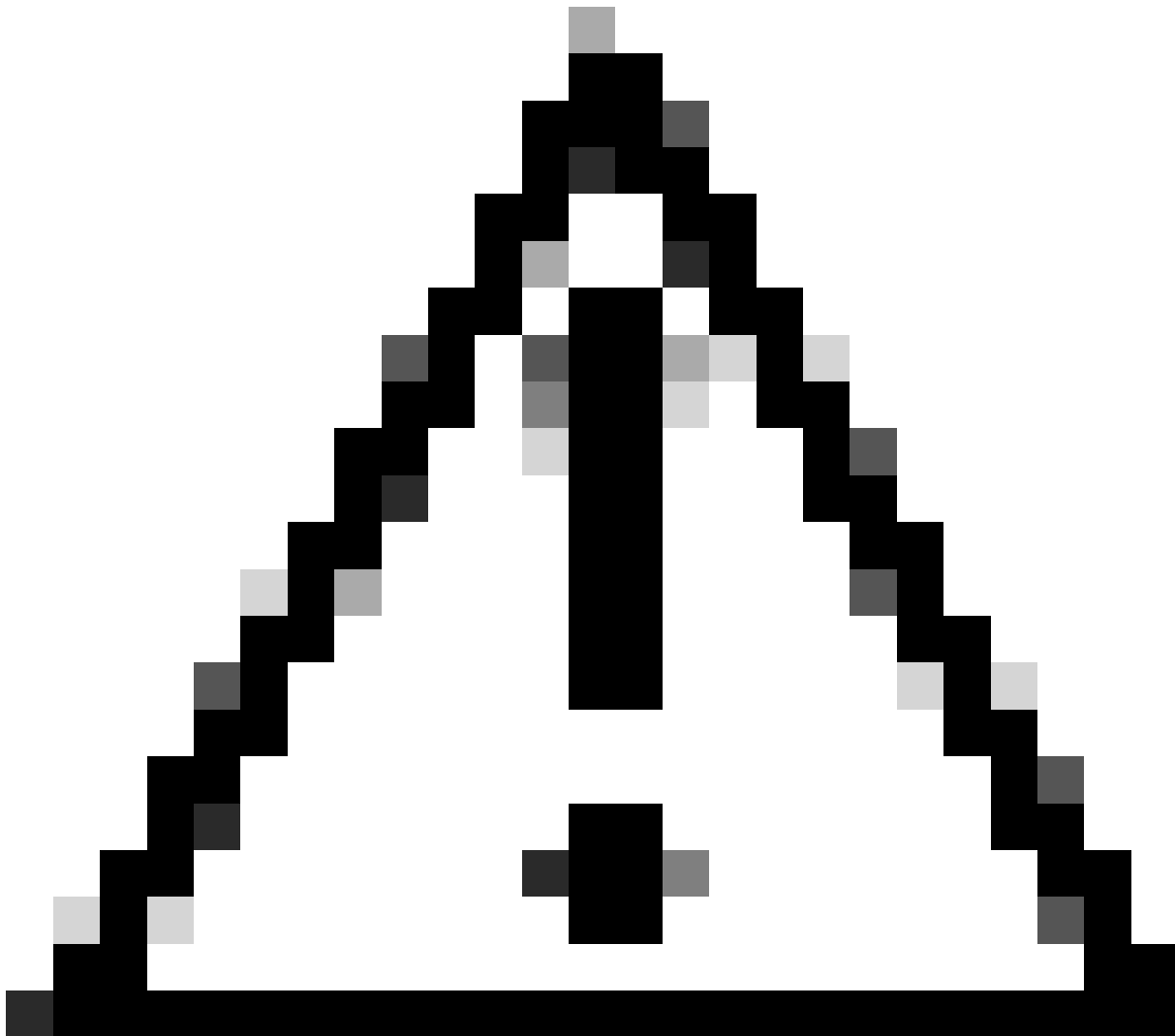


b. Über das Manager-Symbol können Sie weitere Apps durchsuchen.

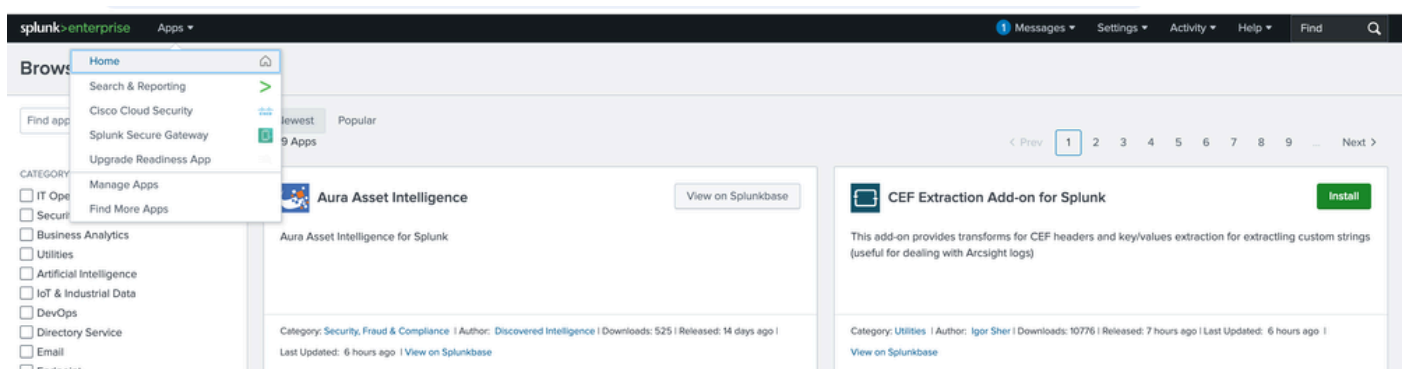


Phase 2: Installation der Cisco Security Cloud-Anwendung

i. Suchen Sie nach der Cisco Security Cloud-Anwendung. Scrollen Sie jetzt nach unten, bis Sie die App gefunden haben, oder suchen Sie nach der Cisco Security Cloud.



Vorsicht: Lassen Sie sich nicht mit der Cisco Cloud Security App verwechseln.



i. Installieren Sie die Anwendung, indem Sie auf die Schaltfläche Installieren klicken.



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

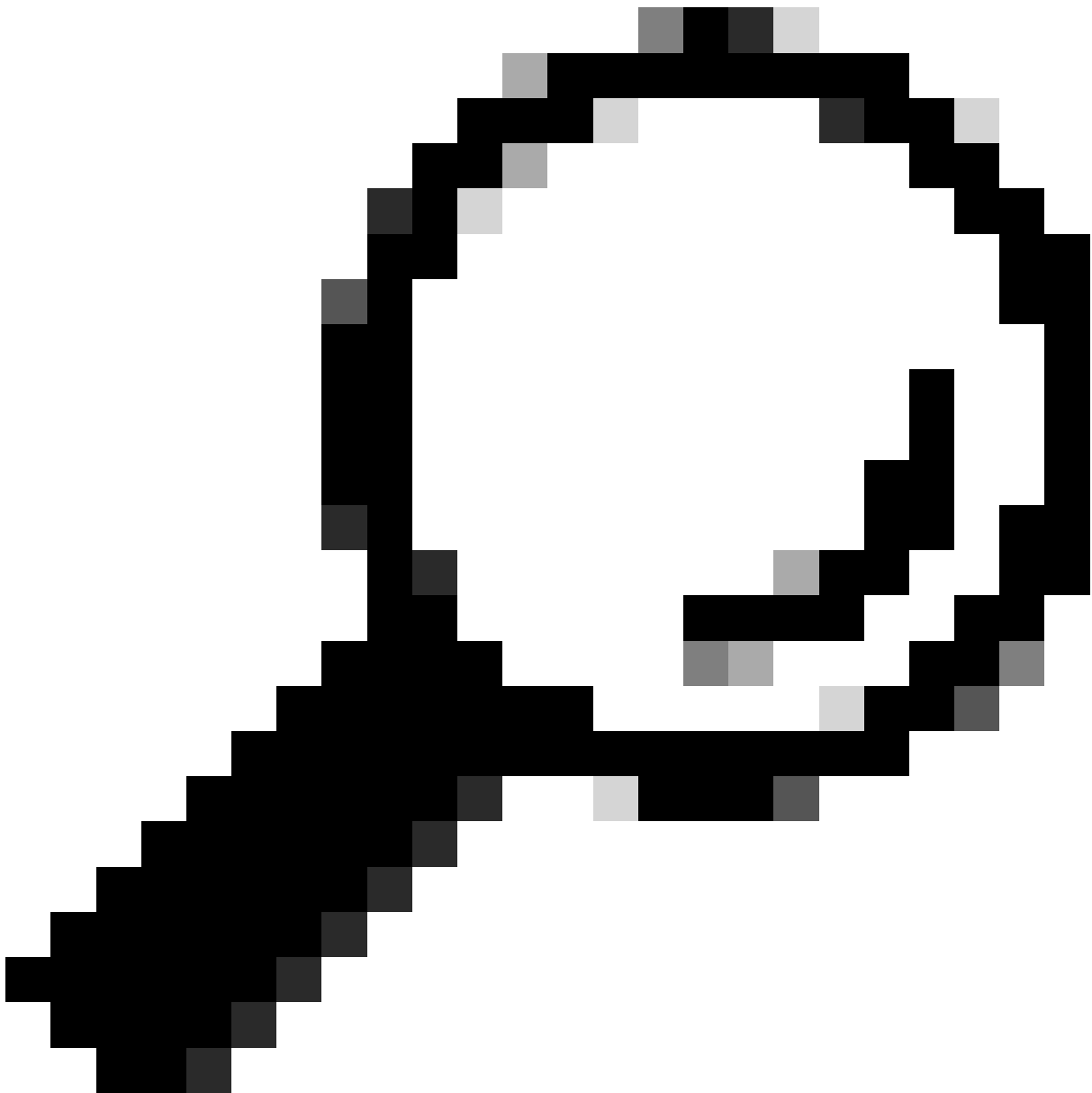
Cisco Email Threat Defense (ETD)

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](#)

ii) Sobald Sie auf die Schaltfläche "Installieren" klicken, wird ein Fenster angezeigt, in dem Sie vor der Installation der Anwendung nach den Anmeldeinformationen des Splunk-Kontos gefragt werden. Geben Sie Ihre Anmeldeinformationen an, und klicken Sie auf Agree and Install, um fortzufahren.



Tipp: Geben Sie die Anmeldeinformationen an, die für den Zugriff auf das Splunk-Portal verwendet werden, nicht die Admin-Anmeldeinformationen, die für die Splunk-Unternehmensanwendung bei der Anmeldung verwendet werden.

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. Bei erfolgreicher Installation der Anwendung wird eine Meldung angezeigt, wie dargestellt. Klicken Sie auf Done (Fertig).

Complete



Cisco Security Cloud was successfully installed.

Open the App

Go Home

Done

Schritt 3: Verifizierung der Installation der Cisco Security Cloud-Anwendung

i. Klicken Sie auf die Dropdown-Option Apps, und nun wird die App in der Liste nach der erfolgreichen Installation angezeigt:

Browse

cisco

CATEGORY

☐ IT Operations☐ Security☐ Business☐ Utilities

Home



Search & Reporting

~~Cisco Cloud Security~~

Cisco Security Cloud

Splunk Secure Gateway



Upgrade Readiness App



Manage Apps

Find More Apps

ii. Wählen Sie Cisco Security Cloud aus, indem Sie darauf klicken. Sie werden zur Seite Application Setup (Anwendungseinrichtung) weitergeleitet, auf der Sie alle verfügbaren Cisco Cloud Security-Produkte finden.

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

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

Application Setup

My Apps

🔍 Search...

>	Input Name	Product	Host	Enabled	Status	Source Type	Index
Cisco Products							
🔍 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](#)

Schritt 4: Integration mit Secure Network Analytics (SNA)

In diesem Dokument werden die Installationsschritte für Splunk mit Secure Network Analytics (SNA) erläutert.

i. Suchen Sie nach sicheren Netzwerkanalysen, und wählen Sie, wenn diese angezeigt wird, **Configure Application** (Anwendung konfigurieren):

🔍 **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.

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

ii) Wenn Sie die Konfigurationsoption auswählen, wird die Konfigurationsseite angezeigt, auf der die hinzuzufügenden Details angezeigt werden.

Data IntegrityResource UtilizationAlerts & DetectionApplication SetupApp Analytics

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. Füllen Sie alle obligatorischen Angaben aus, die für die SNA-Verbindungsdetails angegeben sind:

1. Eingabename: ein eindeutiger Name für SNA
2. Manager-Adresse (IPv4- oder IPv6-Adresse oder Hostname): Management-IP des primären SNA-Managers
3. Domänen-ID: Geben Sie den Wert für domain_ID ein (z. B. 301).
4. Benutzername: Der Benutzername des primären Managers (z. B. admin)
5. Kennwort: Passwort des primären Managers

SNA Connection

*Input Name

SNA_Manager

Enter a unique name

*Manager Address (IPv4 or IPv6 Address or Hostname)

192.168.1.1

Enter the Manager Address (IPv4 or IPv6 Address or Hostname) for this account

*Domain ID

301

Enter the Domain ID for this account

*Username (Role of Primary Admin or Power Analyst)

admin

Enter the Username (Role of Primary Admin or Power Analyst) for this account

*Password

.....

Enter the Password for this account

iv. Lassen Sie die übrigen Einstellungen auf ihren Standardwerten, oder ändern Sie sie nach Bedarf, und klicken Sie dann auf Speichern. Nach Abschluss des Vorgangs wird eine Meldung angezeigt.

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

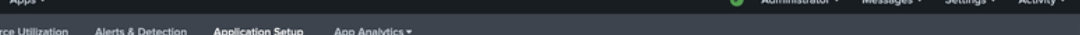
Cancel

Save

Schritt 5: Überprüfung der Integration.

Dies ist ein wichtiger Schritt, bei dem Sie überprüfen müssen, ob die im vorherigen Schritt durchgeführte Integration erfolgreich abgeschlossen wurde.

i. Der Verbindungsstatus für den Eingang muss auf der Registerkarte Application Setup (Anwendungseinrichtung) standardmäßig für den richtigen Namen im Eingabefeld Enabled (Aktiviert) angegeben werden.



The screenshot shows the Splunk Enterprise interface. The top navigation bar includes links for Data Integrity, Resource Utilization, Alerts & Detection, Application Setup (selected), and App Analytics. Below this, the 'Application Setup' section is highlighted with a red box. Under 'My Apps', there is a search bar and a table of installed apps. The table has columns: Input Name, Product, Host, Enabled, Status, Source Type, and Index. The first row shows 'SNA_Manager' with 'Secure Network Analytics' as the product, 'Splunk-Server' as the host, 'Enabled' (checked), 'Connected' status, 'cisco:sna' as the source type, and 'cisco_sna' as the index. The 'Enabled' and 'Status' columns are highlighted with red boxes.

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

ii. Wählen Sie das Secure Network Analytics-Dashboard aus dem Dropdown-Menü aus, und die Statistiken werden schließlich auf dem Dashboard angezeigt.

splunk>enterprise Apps ▾

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

Application Setup

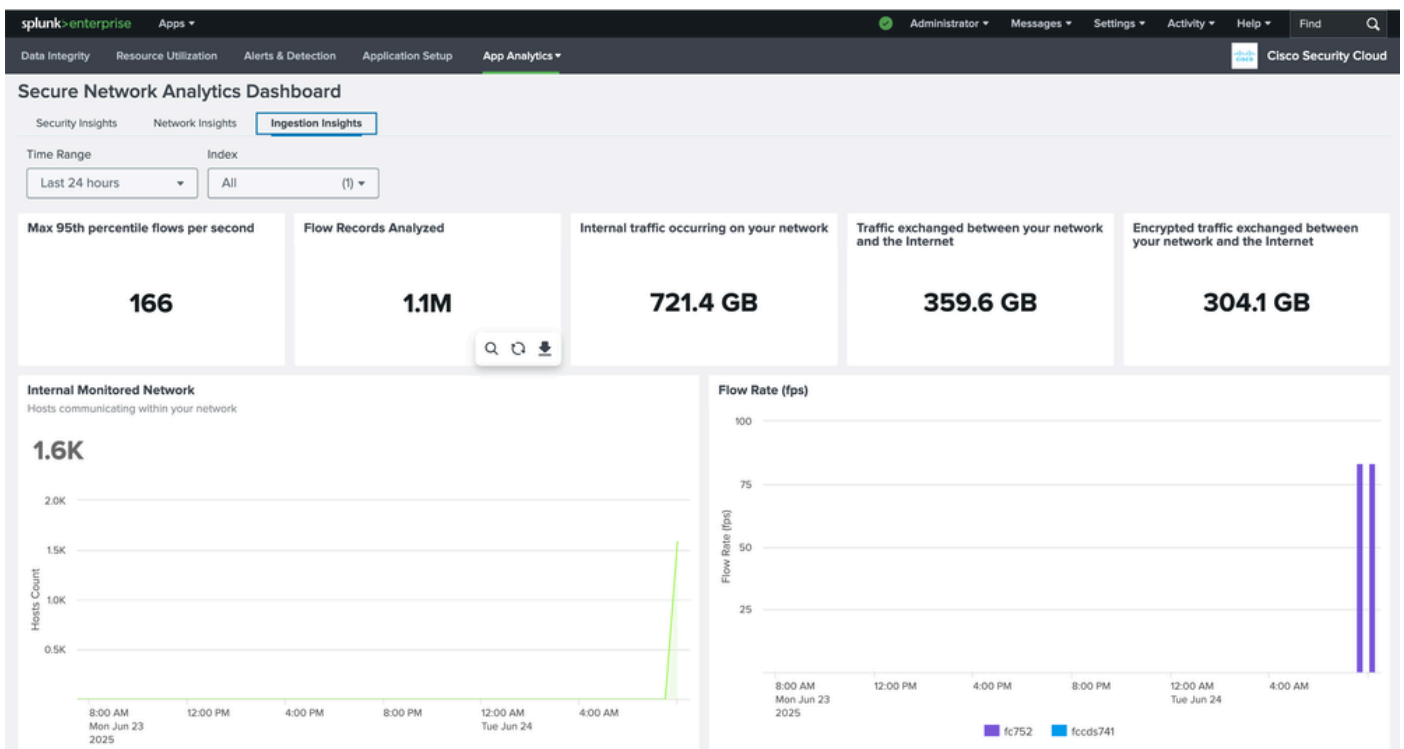
My Apps

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



Häufig gestellte Fragen

Wo finde ich die Domänen-ID für den SNA-Manager?

Antwort:

i. Melden Sie sich beim primären SNA-Manager an, und leiten Sie zur Verwaltungsseite der

Appliance um. Alternativ können Sie auf die [IP Index](#)-URL des [Managers](#) zugreifen.

ii) Durchsuchen Sie den Ordner smc im Abschnitt Support.

← → ↻ 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
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. Öffnen Sie die Datei domain.xml im Ordner domain_XXX unter dem Ordner 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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.