

Integrare SNA in Splunk utilizzando l'applicazione Security Cloud

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Wireless LAN Controller serie 9800](#)

Introduzione

Questo documento descrive l'integrazione perfetta tra SNA e Splunk con Cisco Security Cloud per una risposta più rapida agli incidenti per le minacce identificate.

Prerequisiti

Conoscenze base di Splunk e dispositivi Cisco.

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

Splunk Enterprise

Secure Network Analytics v7.5.2.

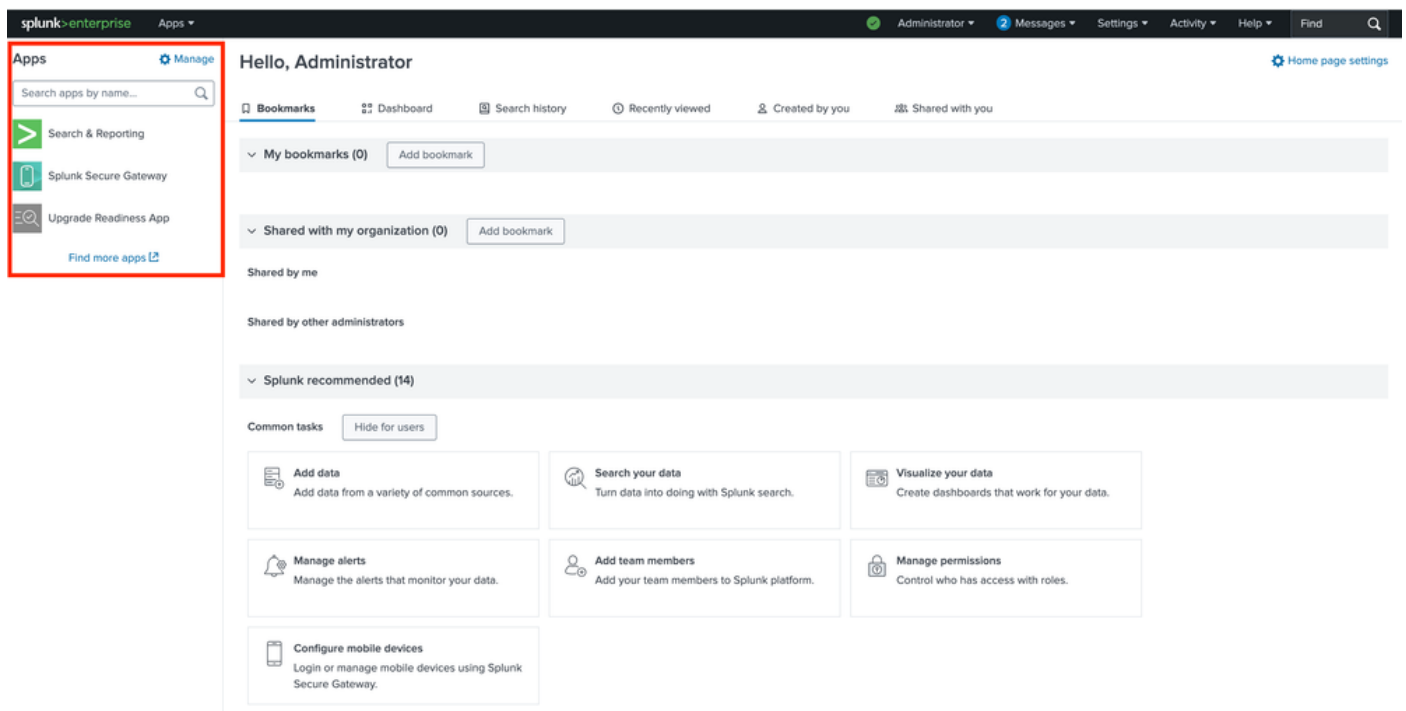
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Fase 1: Accedere all'applicazione Splunk e installare l'applicazione Cisco Security Cloud.

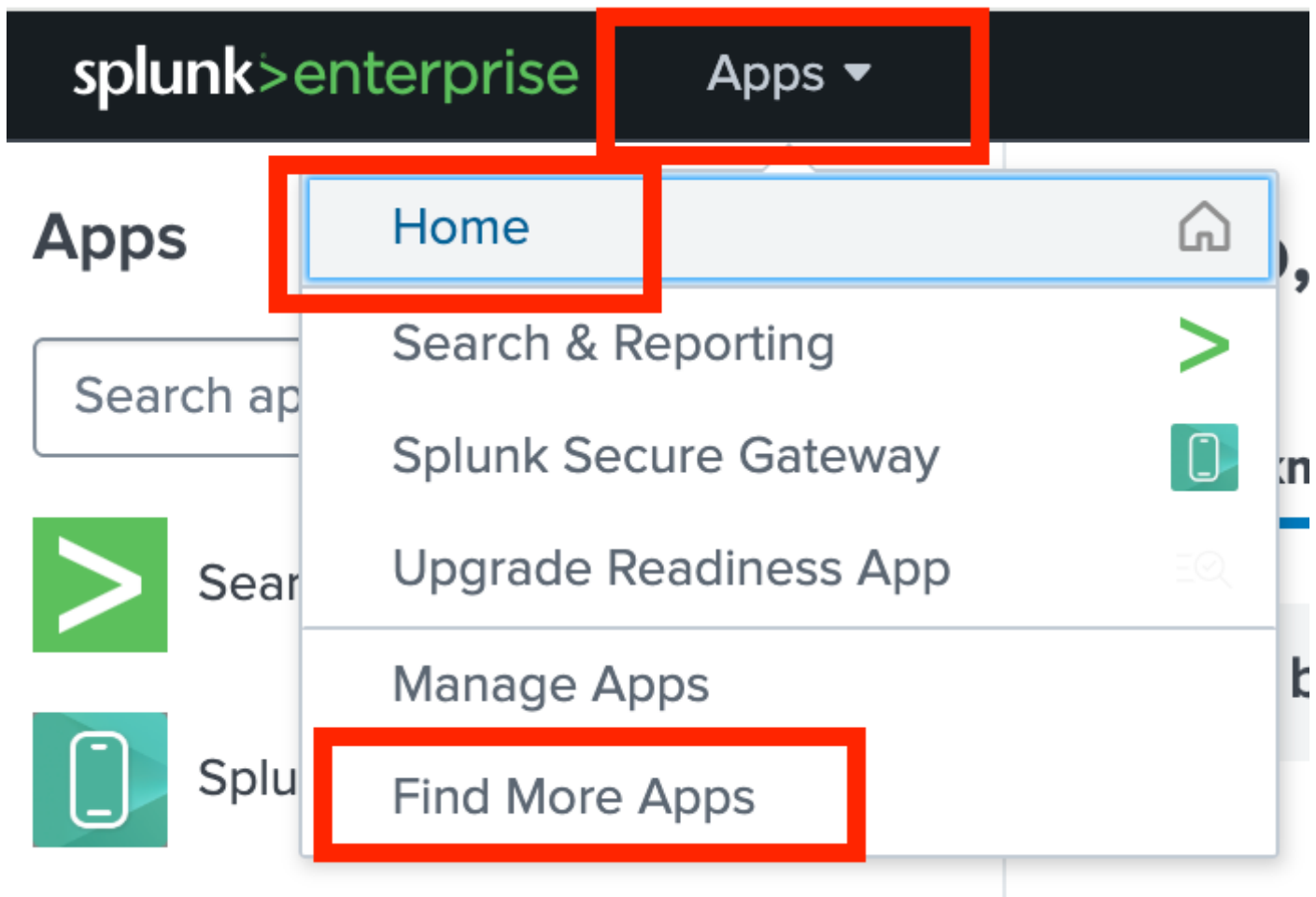
i. Accedere al portale Web Splunk con le credenziali di amministratore e, al termine dell'accesso,

la home page può essere visualizzata con l'elenco delle applicazioni installate sul lato sinistro sotto la sezione App:

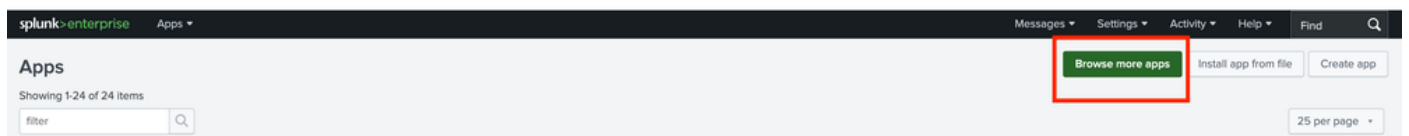


ii. Per integrare la SNA con Splunk, è necessario installare l'applicazione Cisco Security Cloud, che può essere ottenuta in uno dei metodi descritti:

1. Selezionare Trova altre app dall'elenco a discesa.

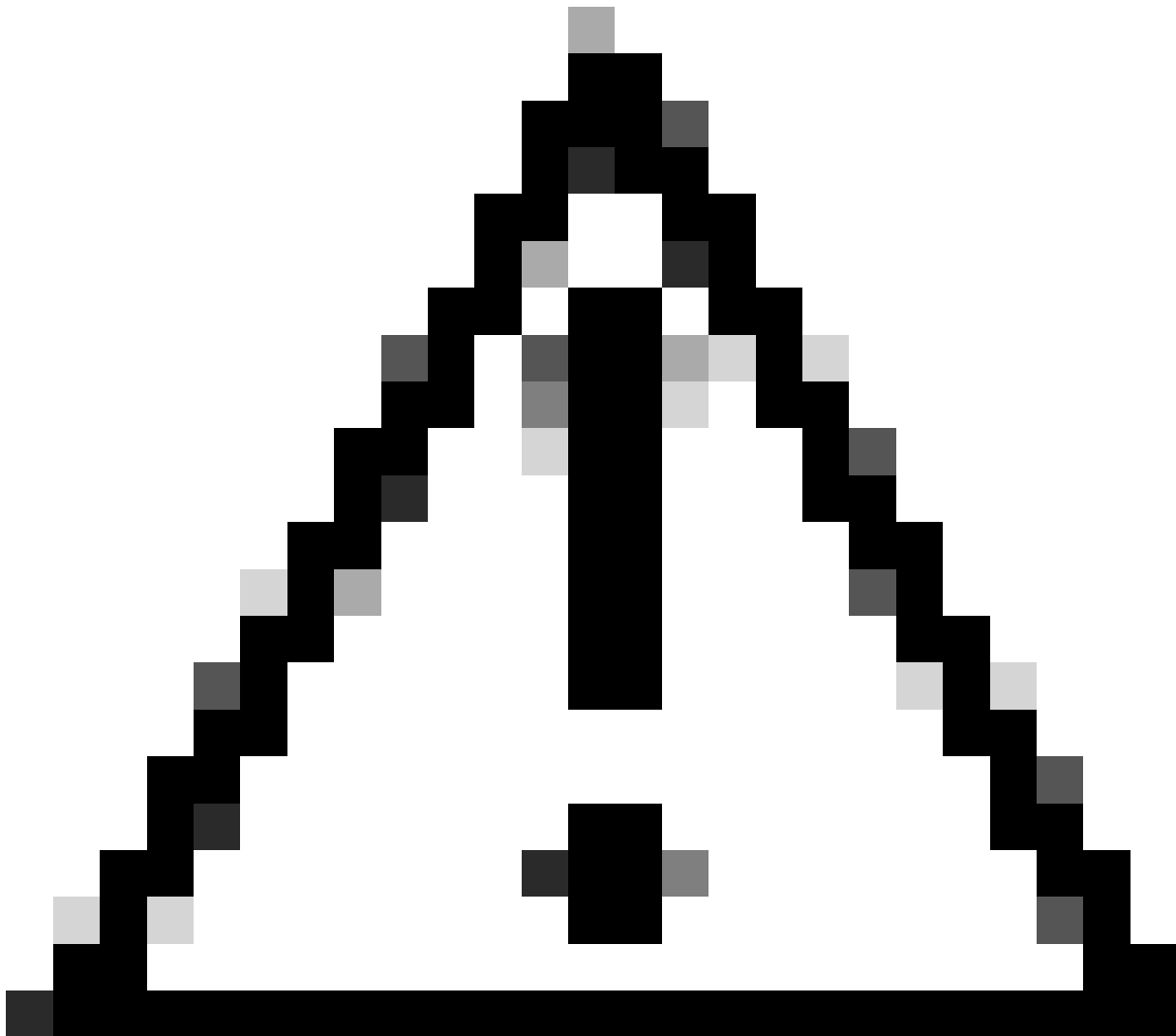


b. Sfoglia altre app sotto l'icona di Manager gear.

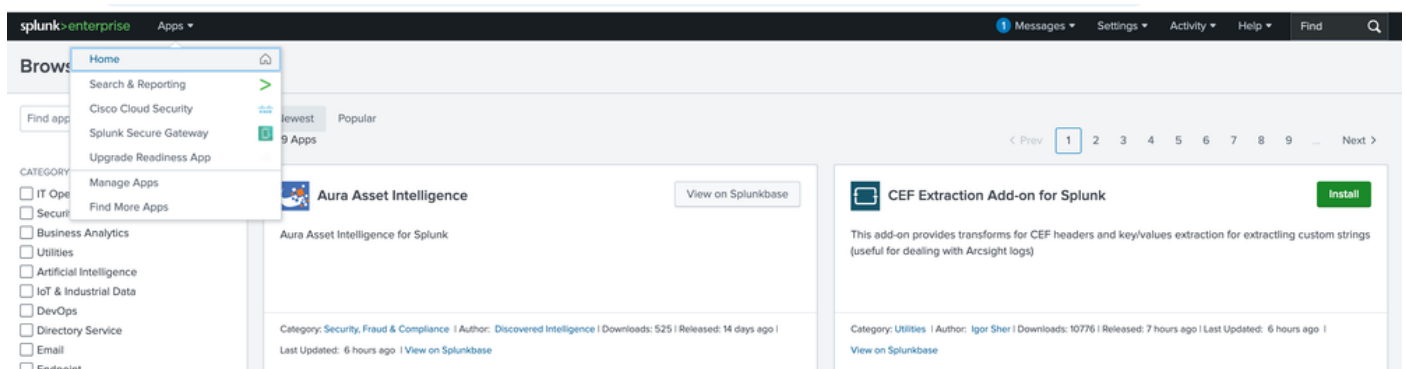


Passaggio 2: Installazione dell'applicazione Cisco Security Cloud.

i. Cercare l'applicazione Cisco Security Cloud. Ora, scorri verso il basso fino a trovare l'app o cerca Cisco Security Cloud.



Attenzione: Non confonderti con Cisco Cloud Security App.



ii. Installare l'applicazione facendo clic sul pulsante Installa.



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

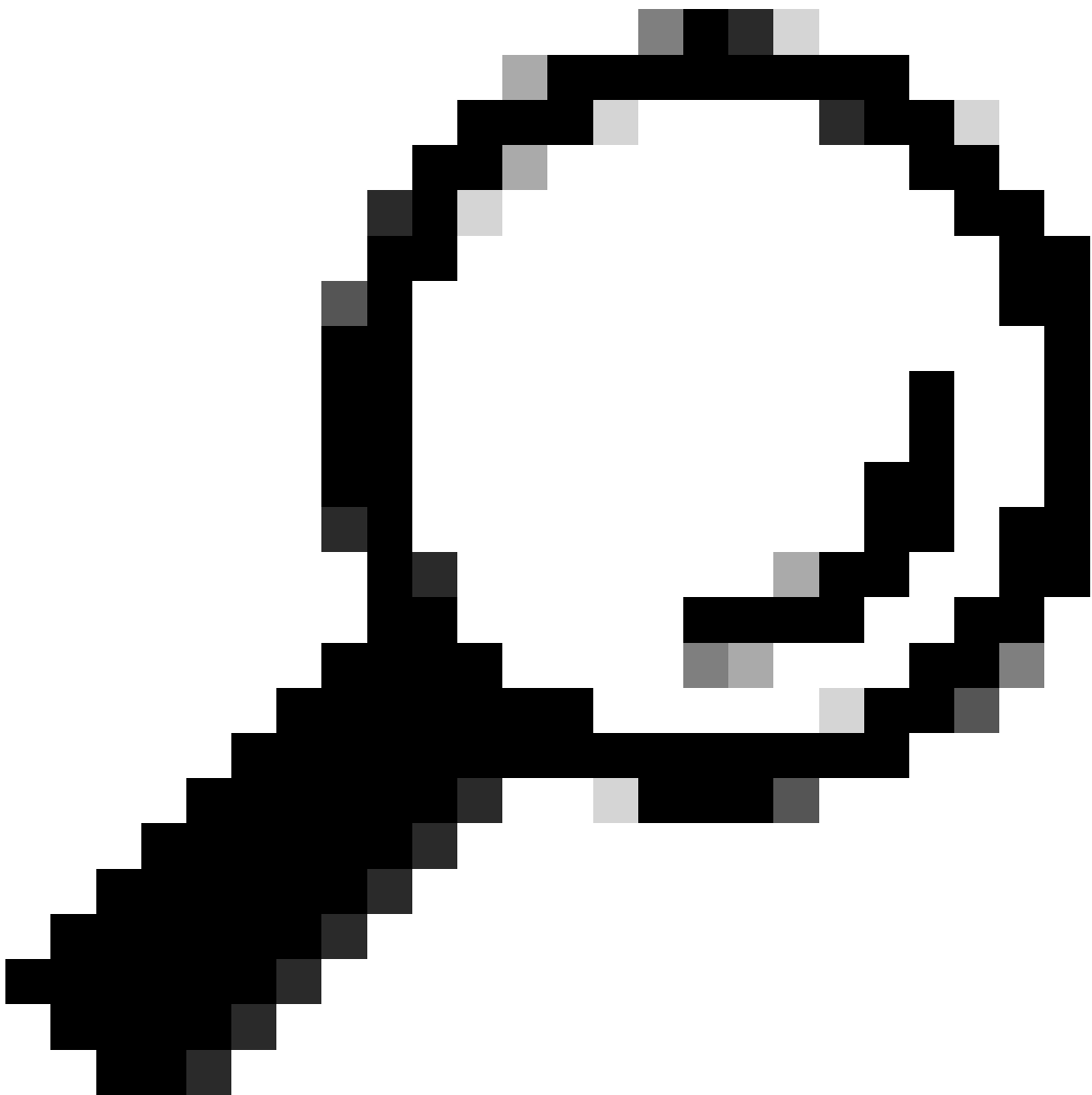
Cisco Email Threat Defense (ETD)

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](#)

iii. Quando si fa clic sul pulsante di installazione, viene visualizzata una finestra che richiede le credenziali dell'account Splunk prima di installare l'applicazione. Specificare le credenziali e fare clic su Accetto e installa per continuare.



Suggerimento: Specificare le credenziali utilizzate per accedere al portale Splunk, non le credenziali amministrative utilizzate per l'applicazione Splunk enterprise durante l'accesso.

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 conditons 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

iv. Quando l'installazione dell'applicazione viene completata correttamente, viene visualizzato un messaggio come illustrato. Selezionate Fatto (Done).

Complete



Cisco Security Cloud was successfully installed.

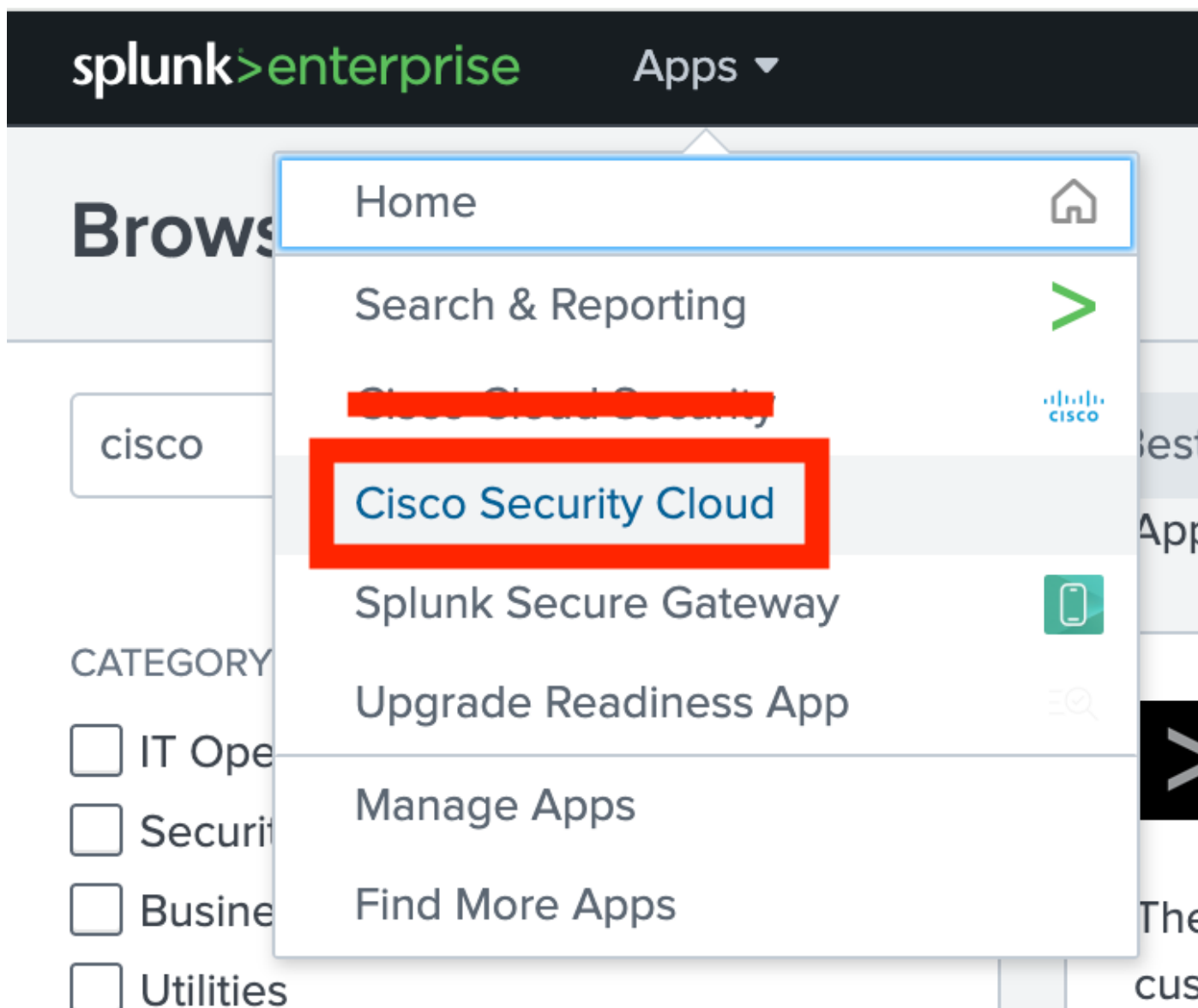
Open the App

Go Home

Done

Passaggio 3: Verifica dell'installazione dell'applicazione Cisco Security Cloud.

i. Fare clic sull'opzione a discesa Apps, e ora l'app può essere visualizzata nell'elenco dopo la corretta installazione:



ii. Selezionare Cisco Security Cloud facendo clic su di esso. Viene visualizzata la pagina Configurazione applicazione, in cui è possibile trovare tutti i prodotti di sicurezza Cisco Cloud disponibili.

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](#)

Passaggio 4: Integrazione con Secure Network Analytics (SNA).

L'obiettivo di questo documento è evidenziare le fasi di installazione di Splunk con Secure Network Analytics (SNA) menzionate più avanti.

i. Cercare Secure Network Analytics e, quando viene visualizzato, selezionare Configure Application (Configura applicazione):

🔍 **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. Quando si seleziona l'opzione Configura, viene visualizzata la pagina di configurazione per i dettagli da aggiungere.

Data Integrity

Resource Utilization

Alerts & Detection

Application Setup

App Analytics

Application Setup / Secure Network Analytics

Cisco Security Cloud

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. Completare tutti i dettagli obbligatori come indicato per i dettagli della connessione SNA:

1. Nome input: qualsiasi nome univoco per SNA
2. Indirizzo manager (indirizzo IPv4 o IPv6 o nome host): IP di gestione di SNA Manager principale
3. ID dominio: immettere il valore per domain_ID (ad esempio 301)
4. Username: Il nome utente del responsabile principale (ad esempio admin)
5. Password: Password dell'utente responsabile primario

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. Mantenere i valori predefiniti delle restanti impostazioni o modificarli in base alle esigenze, quindi fare clic su Salva. Dopo il completamento, sullo schermo viene visualizzato un messaggio che indica la riuscita dell'operazione.

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

CancelSave

Passaggio 5: Verifica dell'integrazione.

Si tratta di un passaggio importante in cui è necessario verificare se l'integrazione eseguita nel passaggio precedente è stata eseguita correttamente o meno.

i. Lo stato della connessione per l'input deve essere Connesso nella scheda Impostazione applicazione con l'impostazione predefinita Abilitato per il nome del diritto nel campo Input.

Application Setup							
My Apps							
Search...							
Input Name	Product	Host	Enabled	Status	Source Type	Index	
SNA_Manager	Secure Network Analytics	Splunk-Server	Enabled	Connected	cisco:sna	cisco_sna	

ii. Selezionare Secure Network Analytics Dashboard dall'elenco a discesa e gli stati iniziano a riflettere sul dashboard.

splunk>enterprise Apps ▾

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

Application Setup

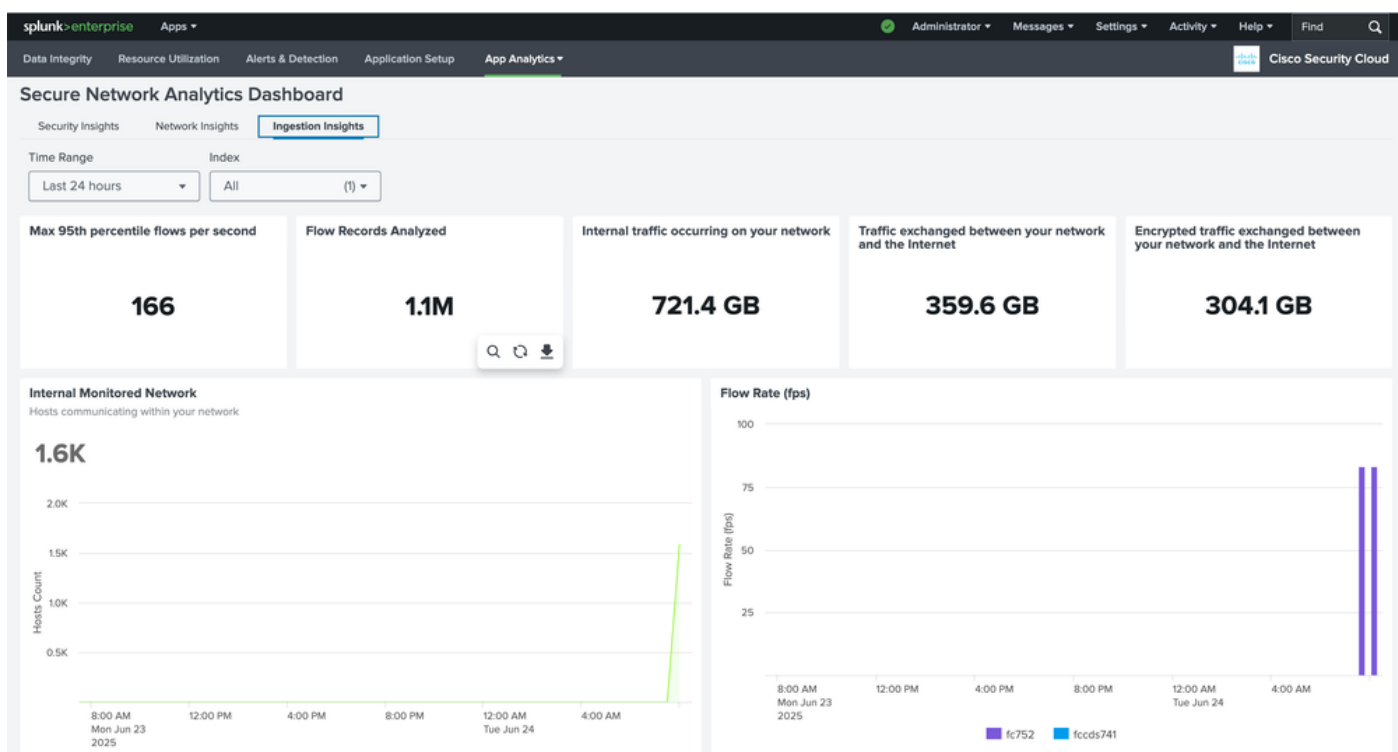
My Apps

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



Wireless LAN Controller serie 9800

Dove trovare l'ID di dominio per il gestore SNA?

Risposta.

i. Accedere al gestore primario della SNA e reindirizzare alla pagina di amministrazione

dell'accessorio o all'URL dell'[indice IP di access_manager](#).

ii. Sfogliare la cartella smc nella sezione Supporto.

← → ↻ 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. Aprire il file domain.xml disponibile nella cartella domain_XXX all'interno della cartella 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).