Integrare SNA in Splunk utilizzando l'applicazione Security Cloud

Sommario

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.

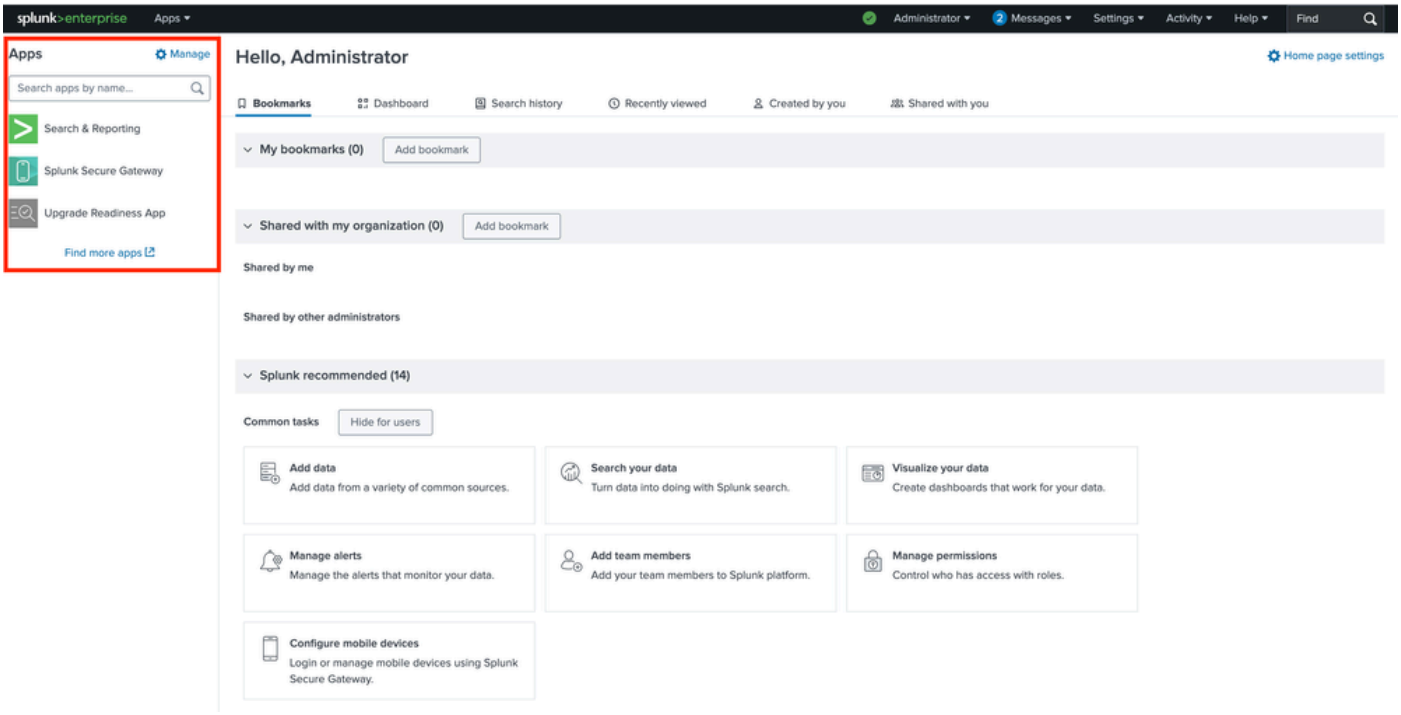
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

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

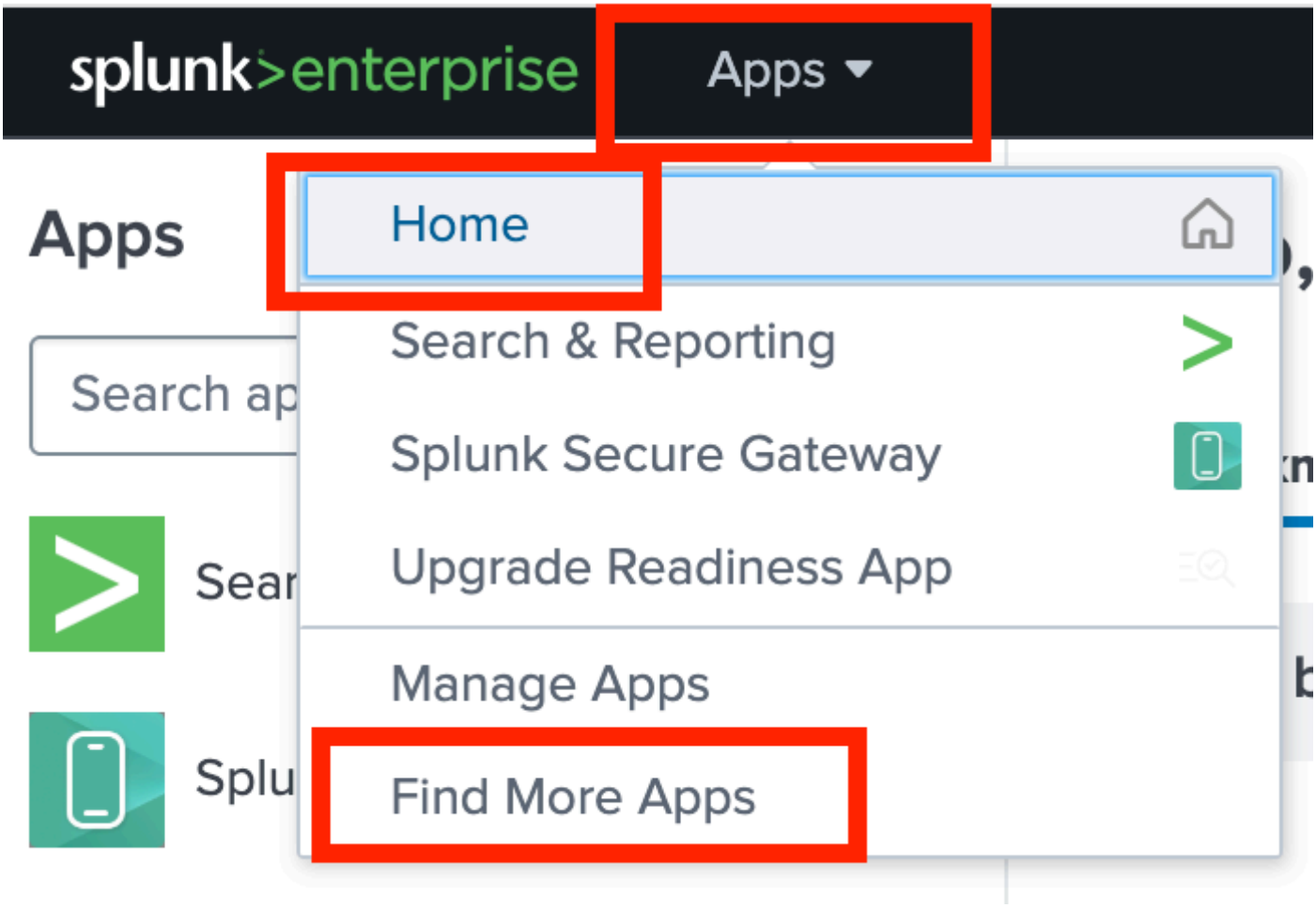
i. Accedere al portale Web Splunk con le credenziali di amministratore e, al termine dell'accesso,

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

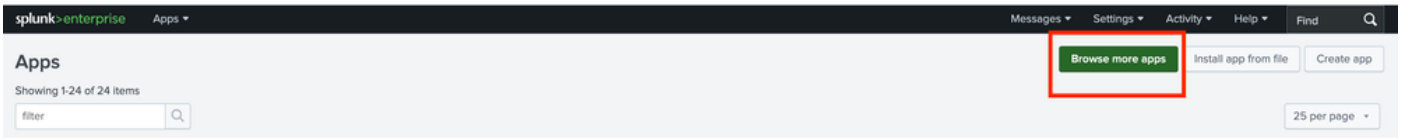


ii. Per integrare la SNA con Splunk, è necessario installare l'applicazione Cisco Security Cloud, che può essere ottenuta in uno dei metodi descritti:

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



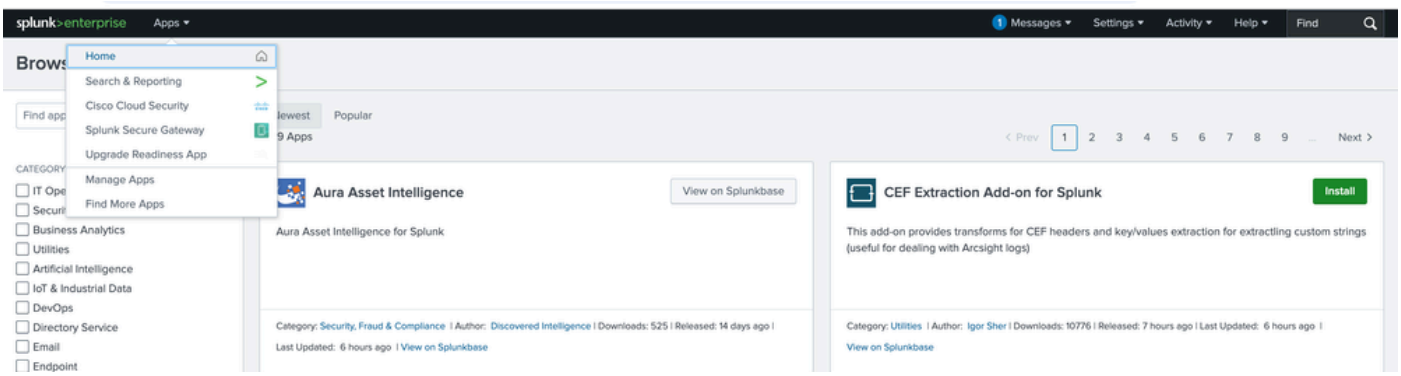
b. Sfoglia altre app sotto l'icona di Manager gear.



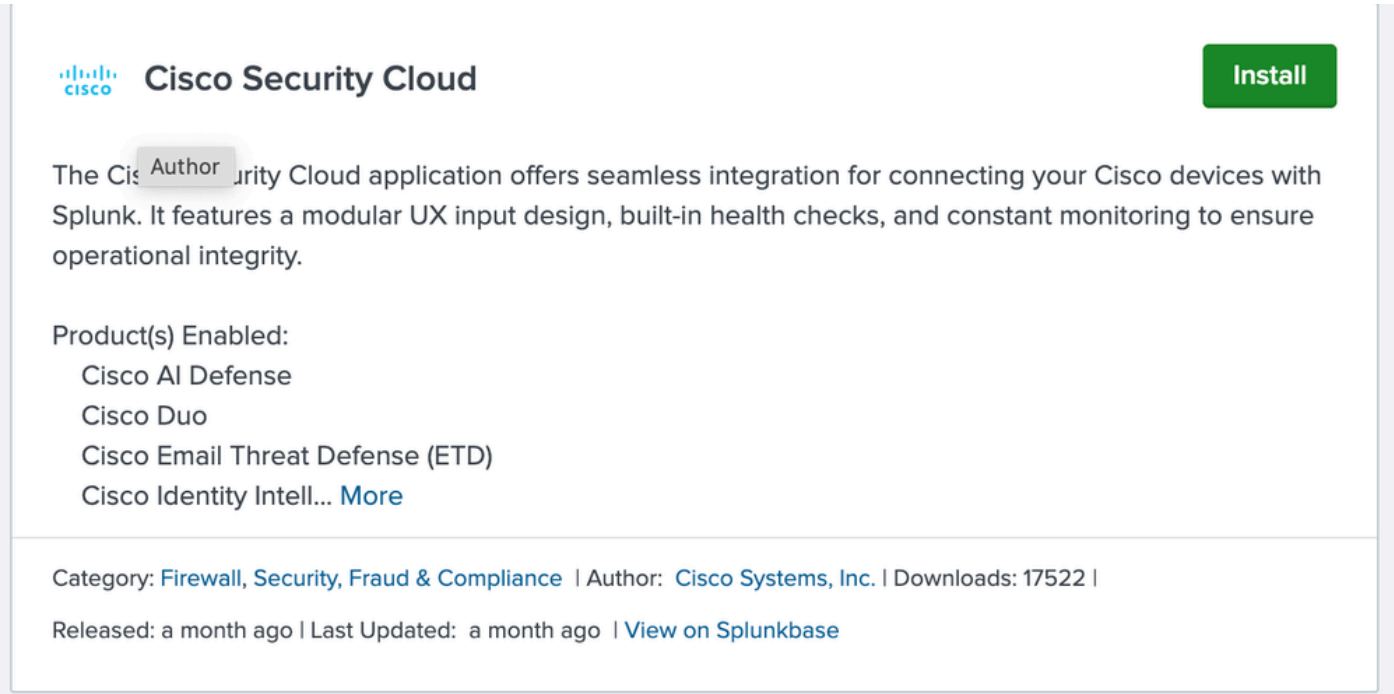
Passaggio 2: Installazione dell'applicazione Cisco Security Cloud.

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

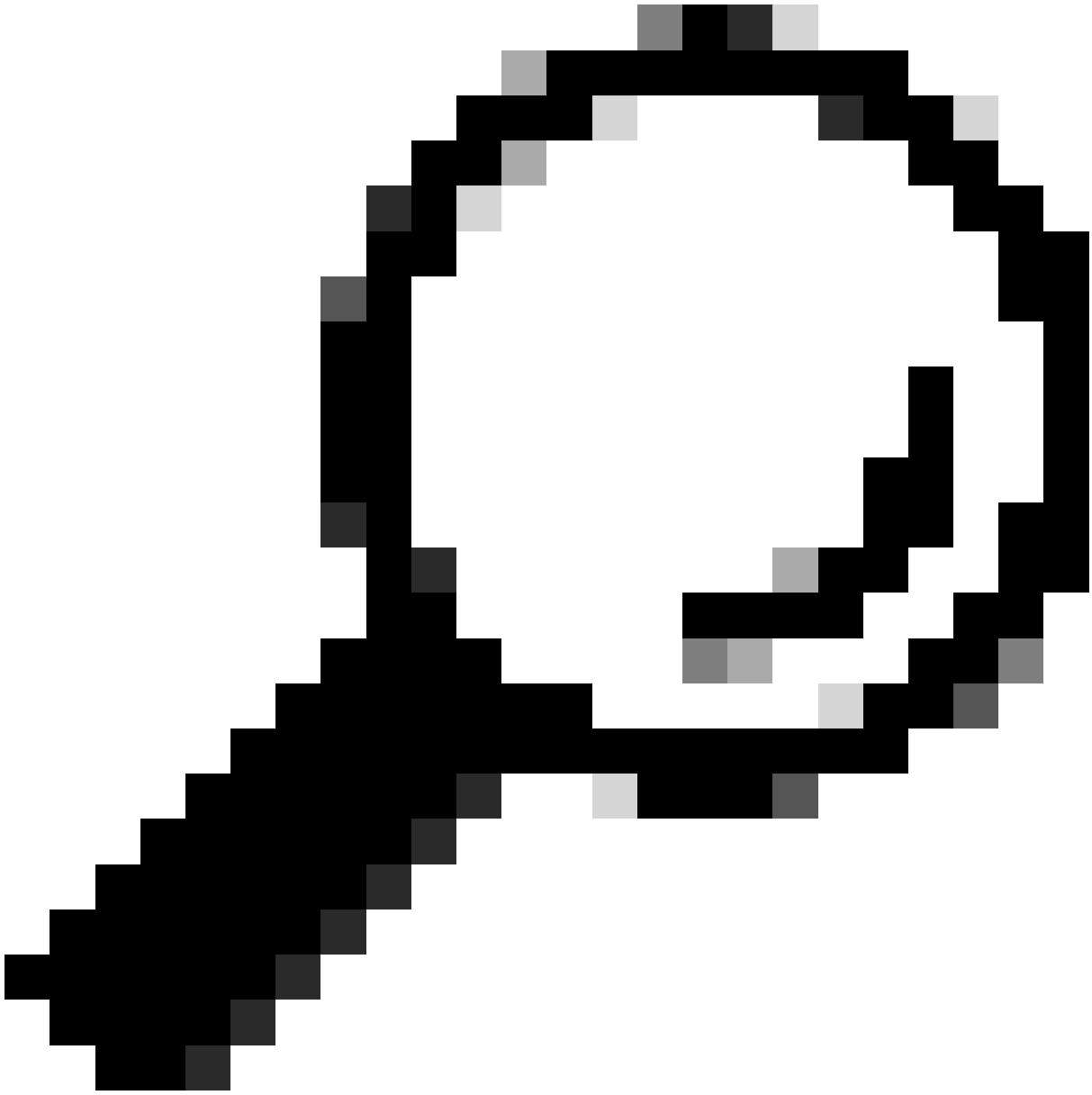
Attenzione: Non confonderti con Cisco Cloud Security App.



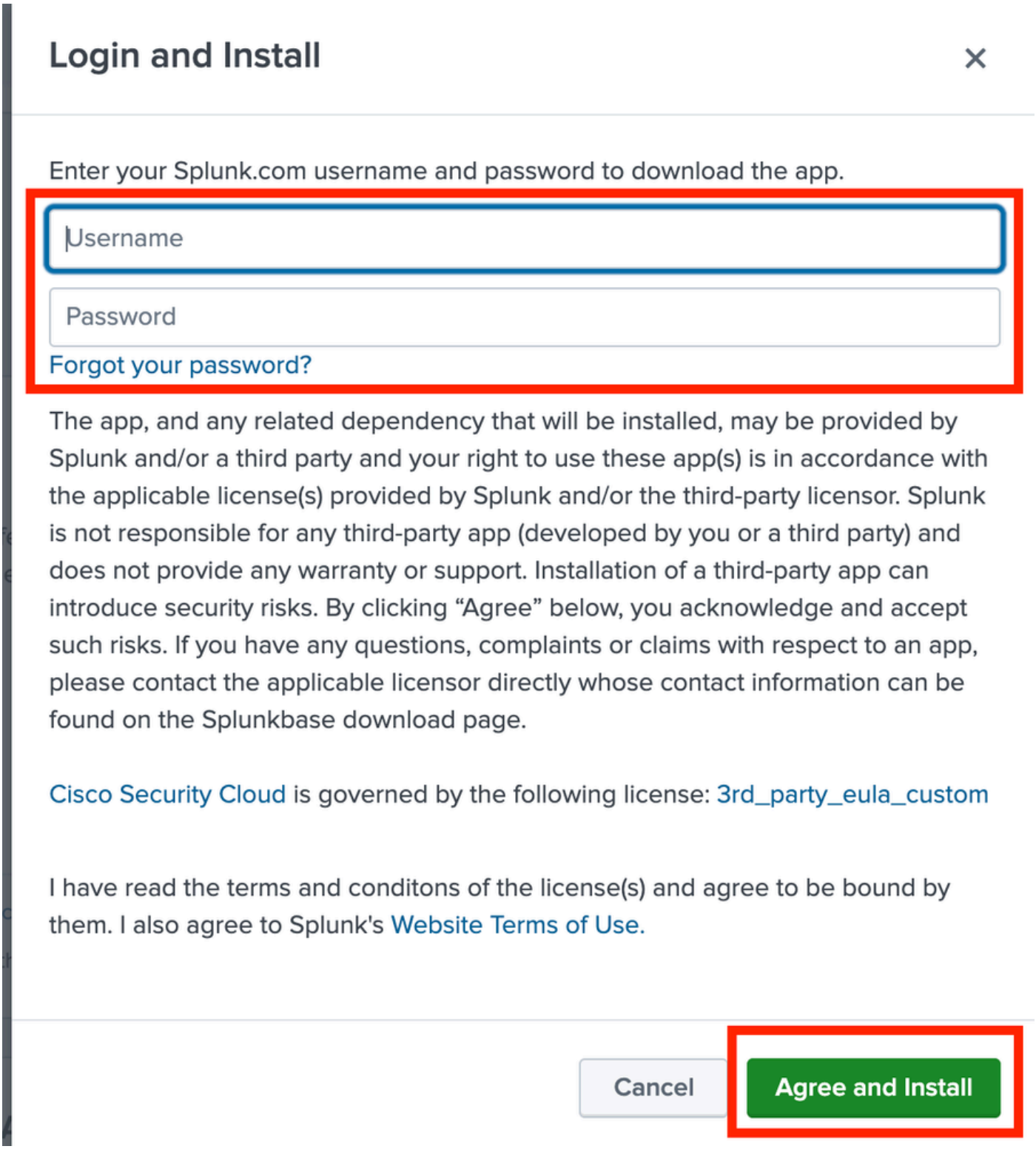
ii. Installare l'applicazione facendo clic sul pulsante Installa.



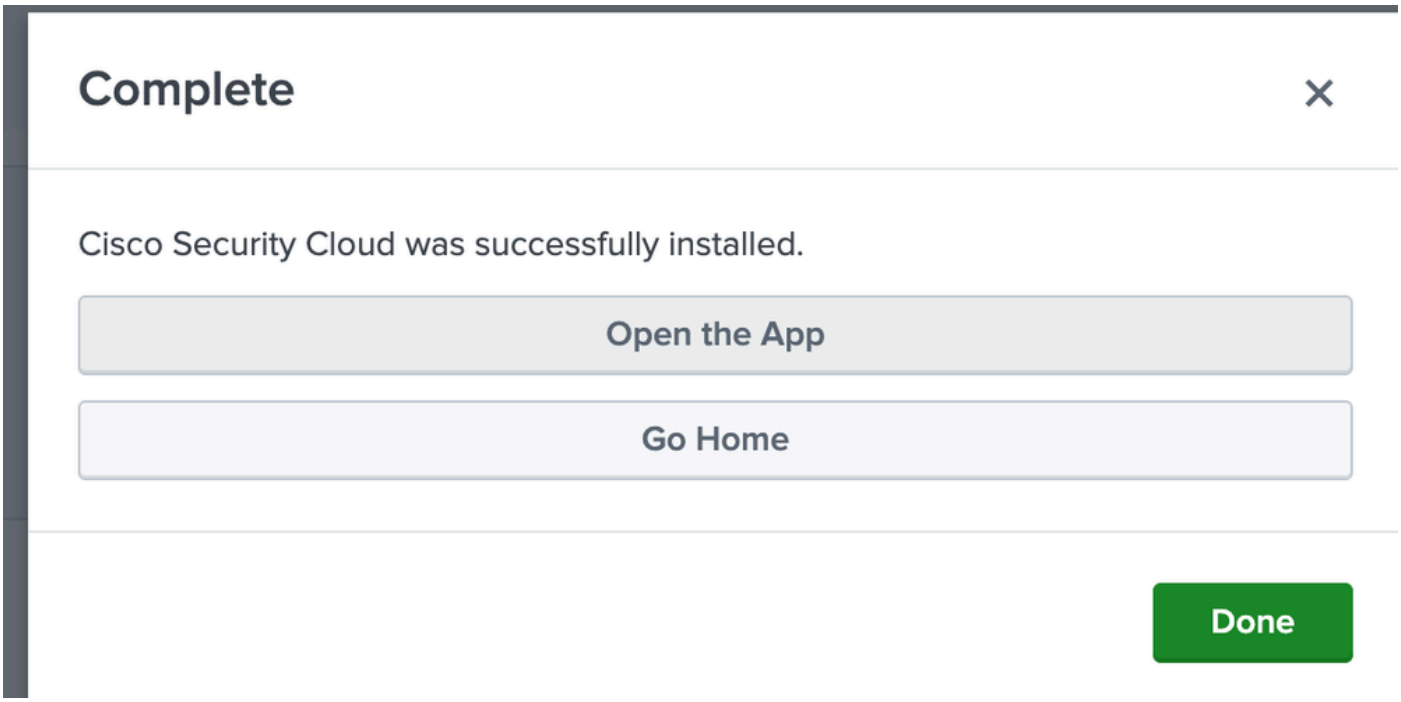
iii. Quando si fa clic sul pulsante di installazione, viene visualizzata una finestra che richiede le credenziali dell'account Splunk prima di installare l'applicazione. Specificare le credenziali e fare clic su Accetto e installa per continuare.



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

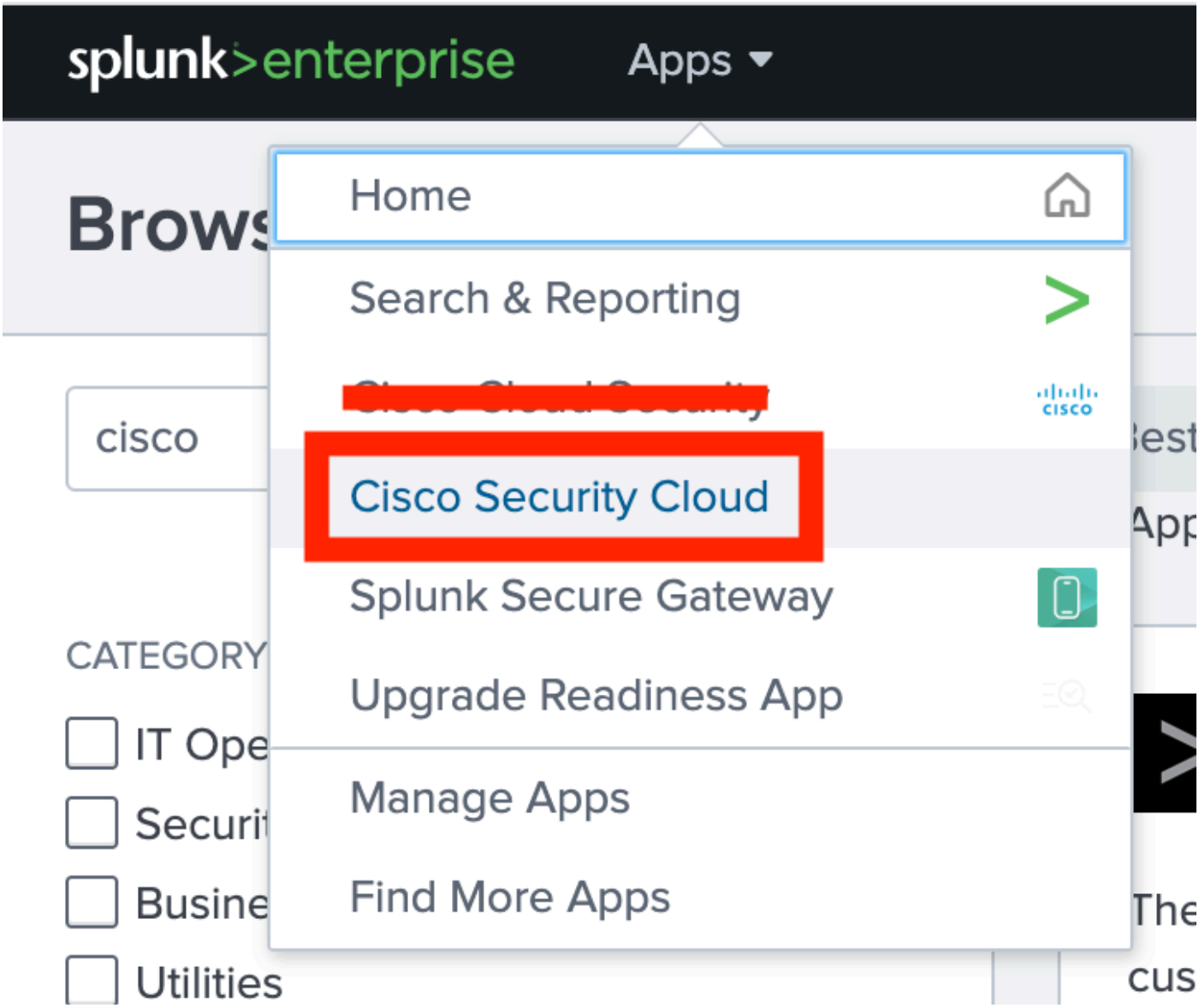


iv. Quando l'installazione dell'applicazione viene completata correttamente, viene visualizzato un messaggio come illustrato. Selezionate Fatto (Done).

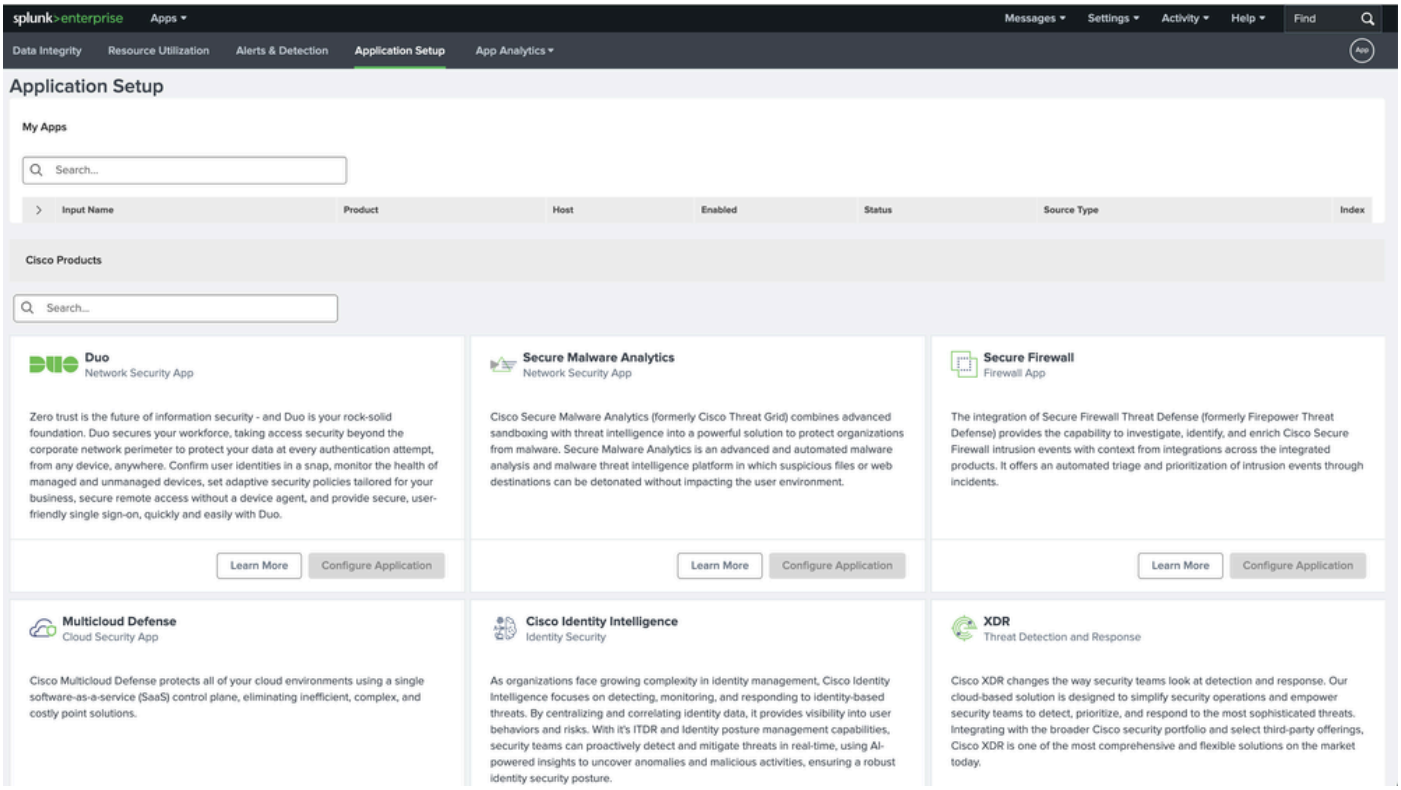


Passaggio 3: Verifica dell'installazione dell'applicazione Cisco Security Cloud.

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



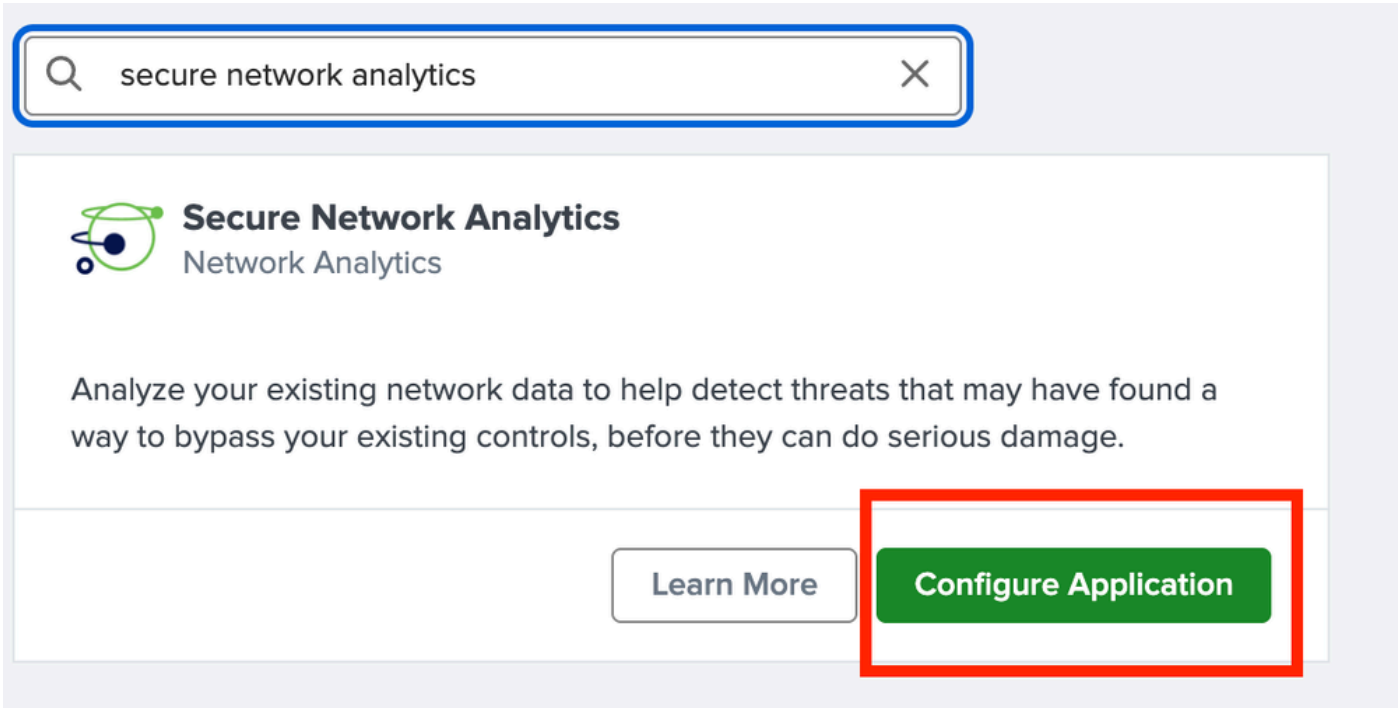
ii. Selezionare Cisco Security Cloud facendo clic su di esso. Viene visualizzata la pagina Configurazione applicazione, in cui è possibile trovare tutti i prodotti di sicurezza Cisco Cloud disponibili.



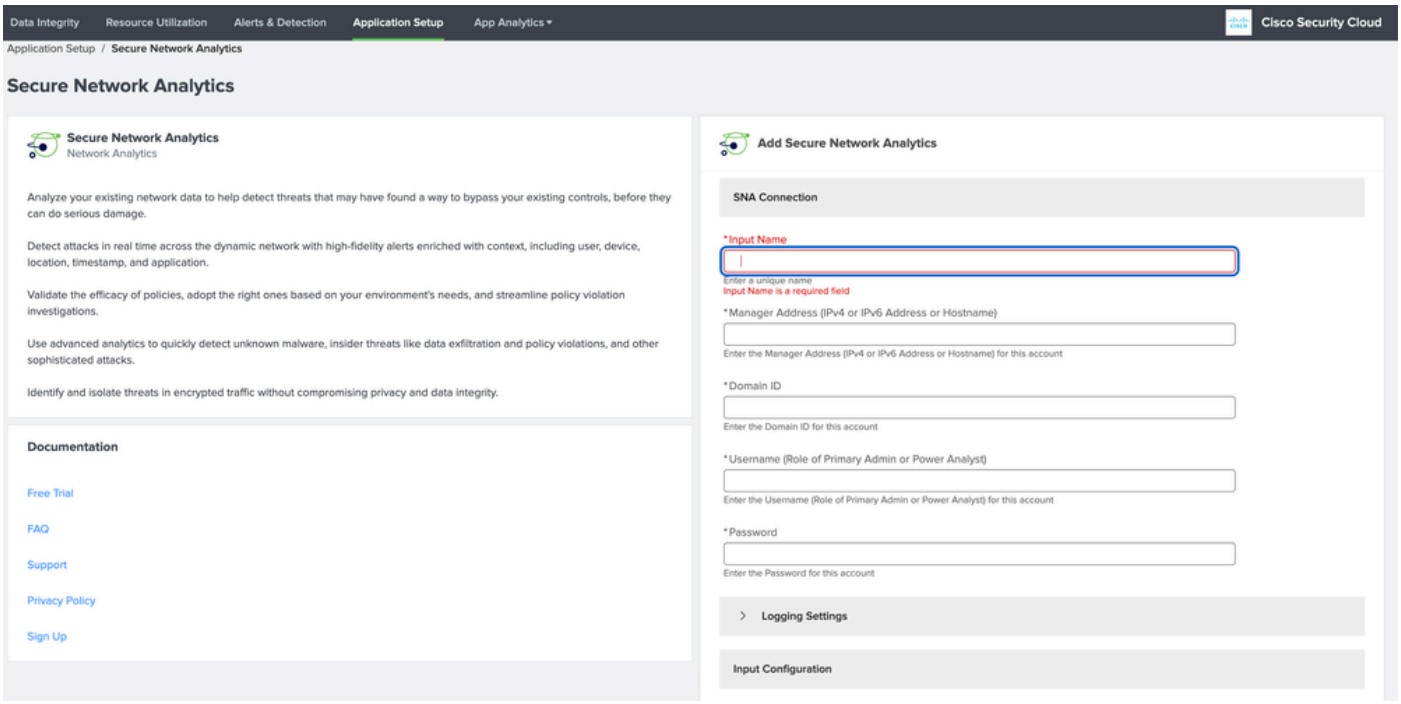
Passaggio 4: Integrazione con Secure Network Analytics (SNA).

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):

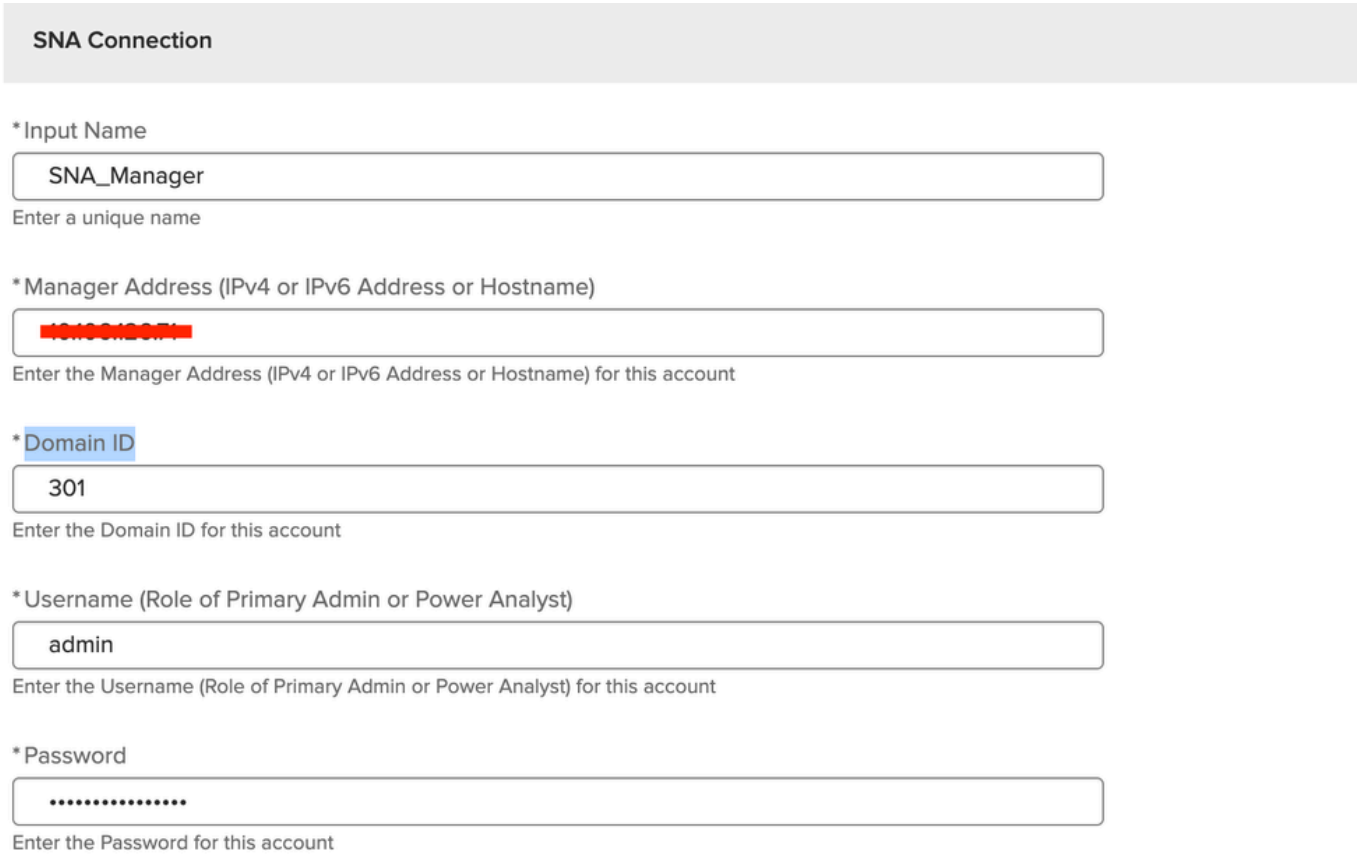


ii. Quando si seleziona l'opzione Configura, viene visualizzata la pagina di configurazione per i dettagli da aggiungere.

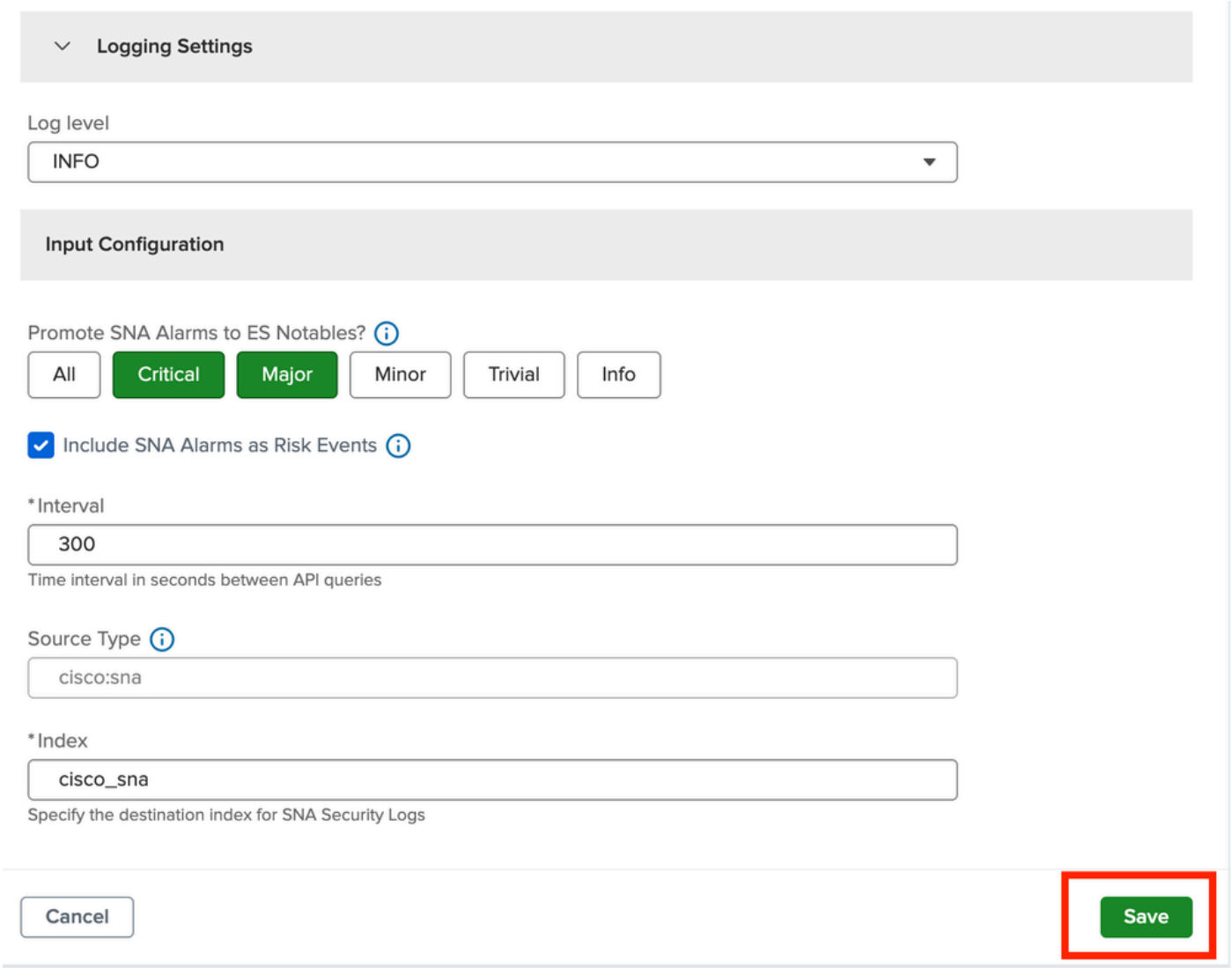


iii. Completare tutti i dettagli obbligatori come indicato per i dettagli della connessione SNA:

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



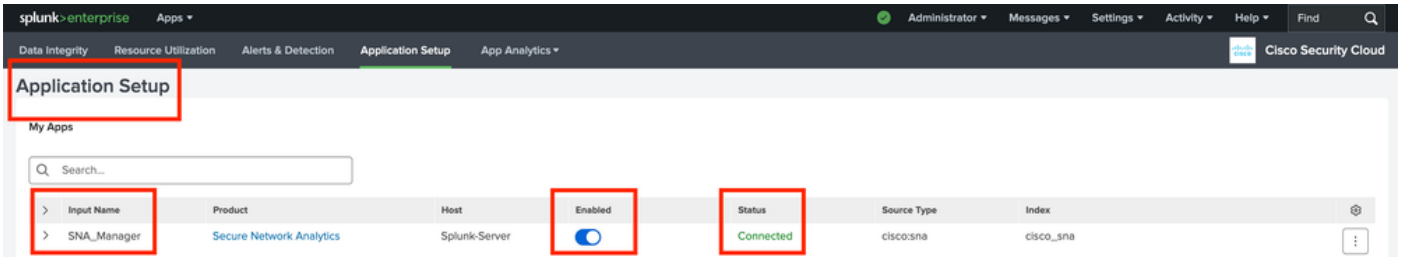
iv. Mantenere i valori predefiniti delle restanti impostazioni o modificarli in base alle esigenze, quindi fare clic su Salva. Dopo il completamento, sullo schermo viene visualizzato un messaggio che indica la riuscita dell'operazione.



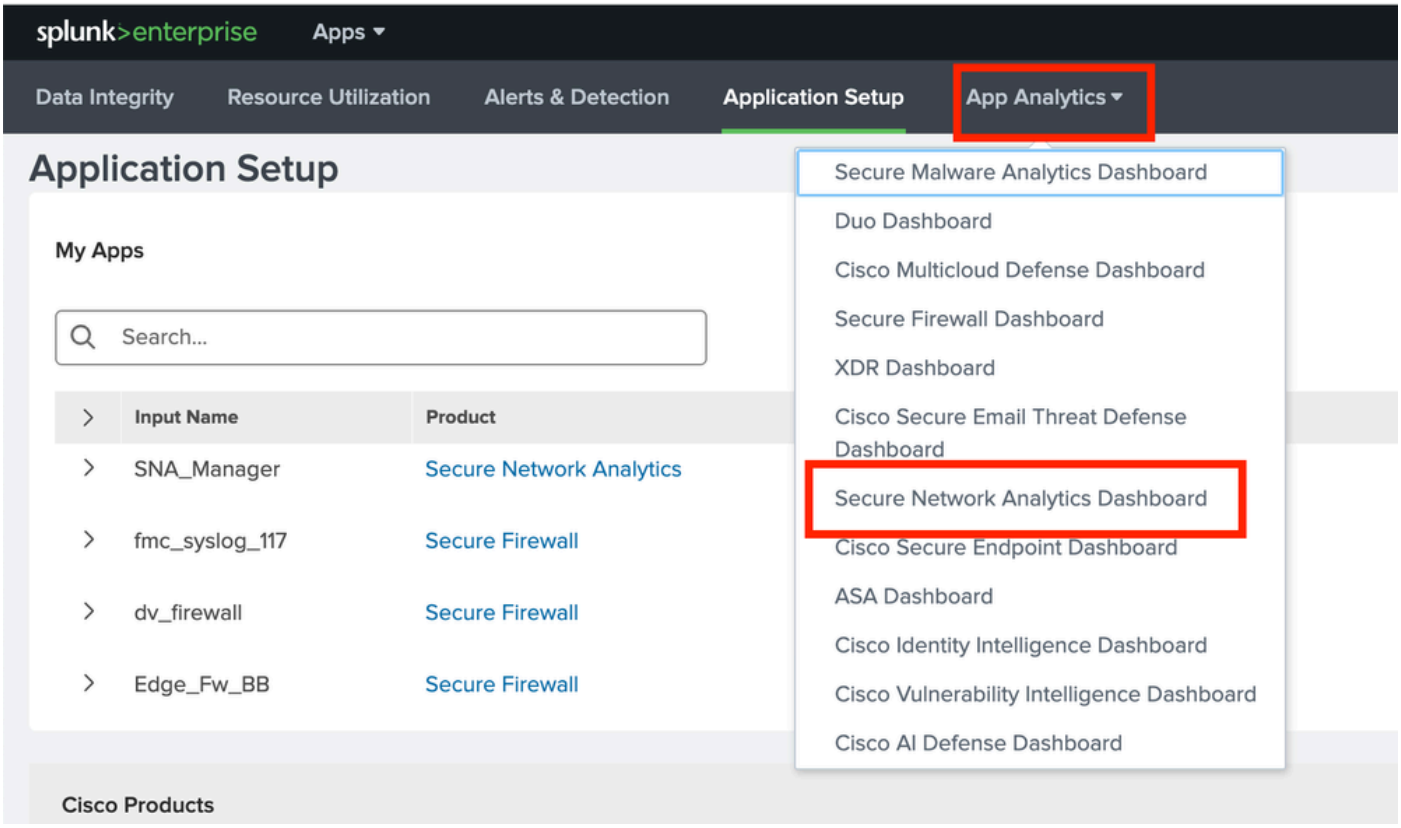
Passaggio 5: Verifica dell'integrazione.

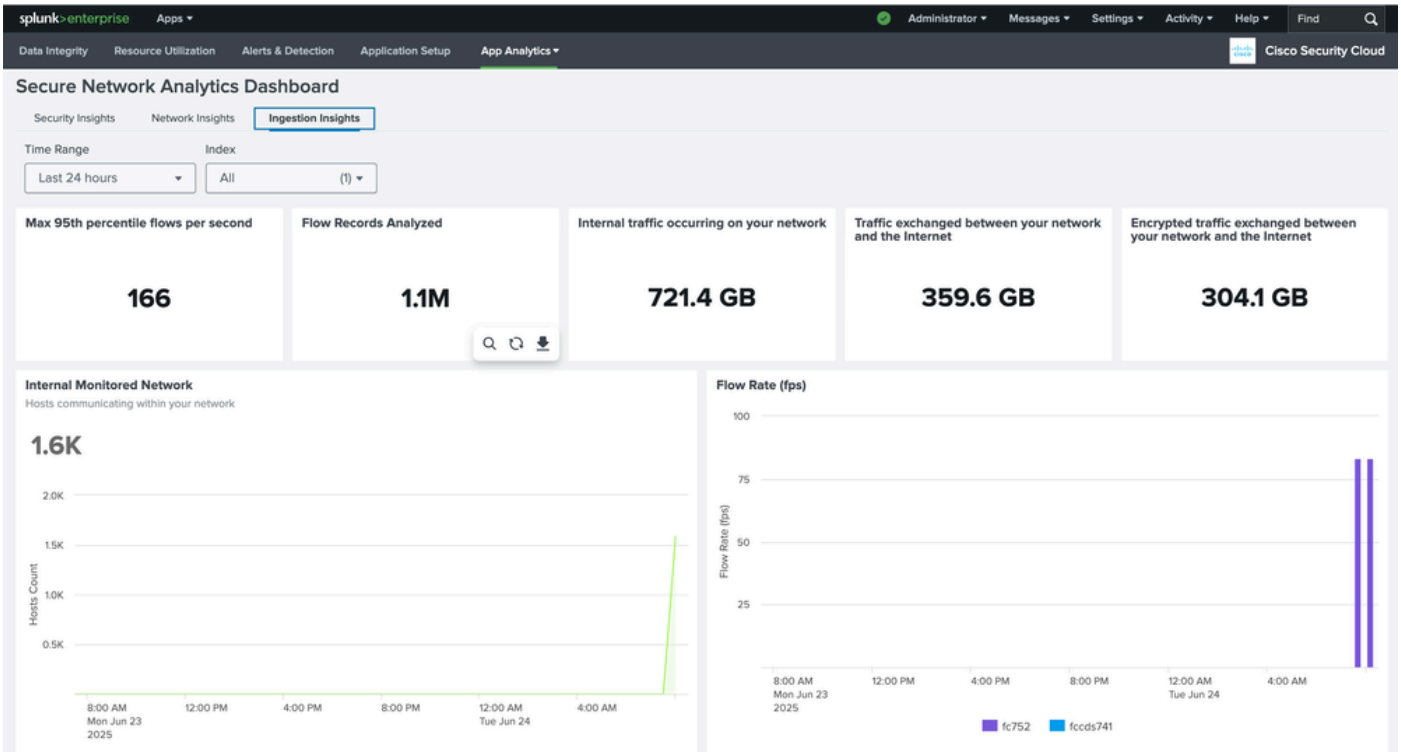
Si tratta di un passaggio importante in cui è necessario verificare se l'integrazione eseguita nel passaggio precedente è stata eseguita correttamente o meno.

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.



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





Wireless LAN Controller serie 9800

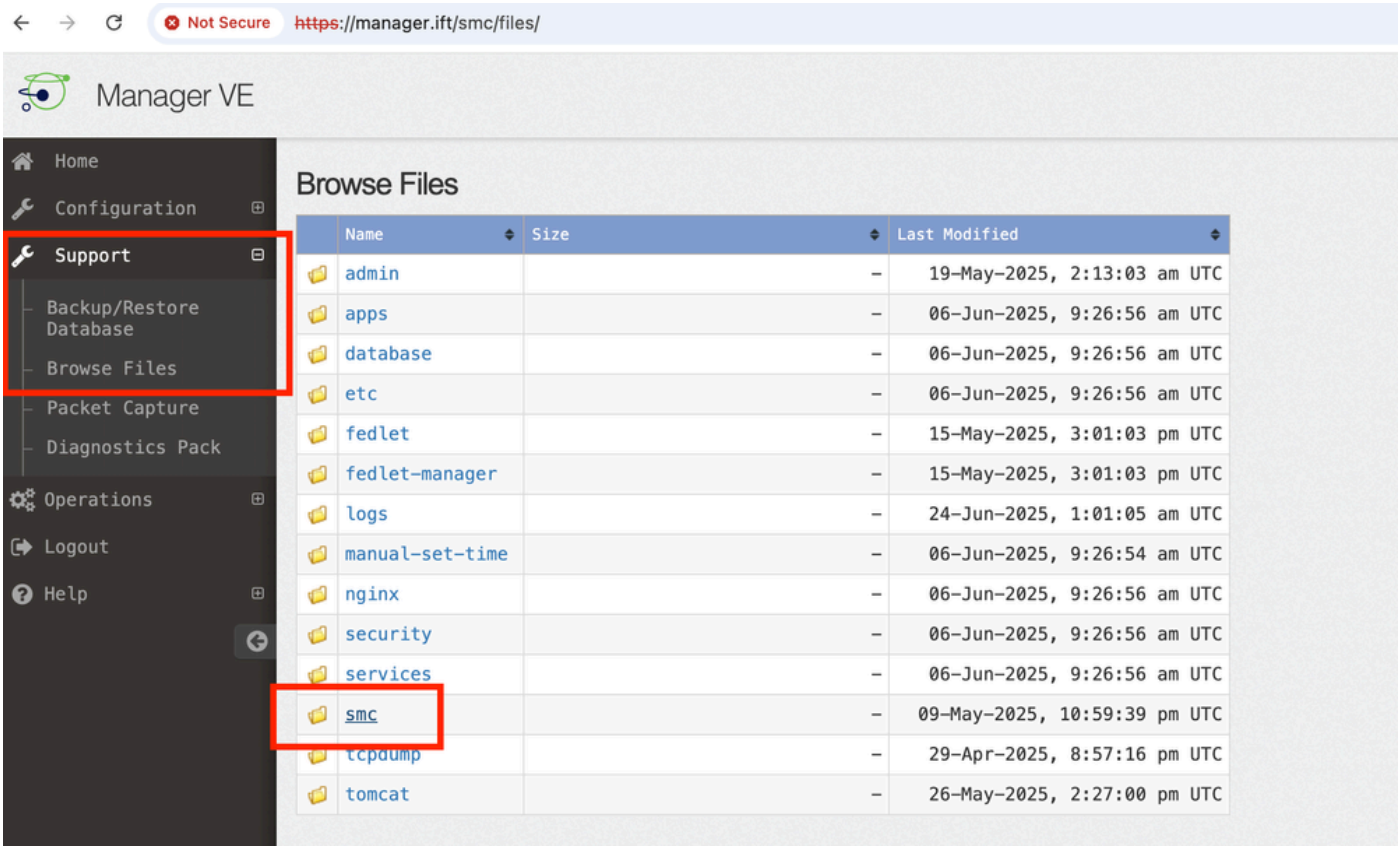
Dove trovare l'ID di dominio per il gestore SNA?

Risposta.

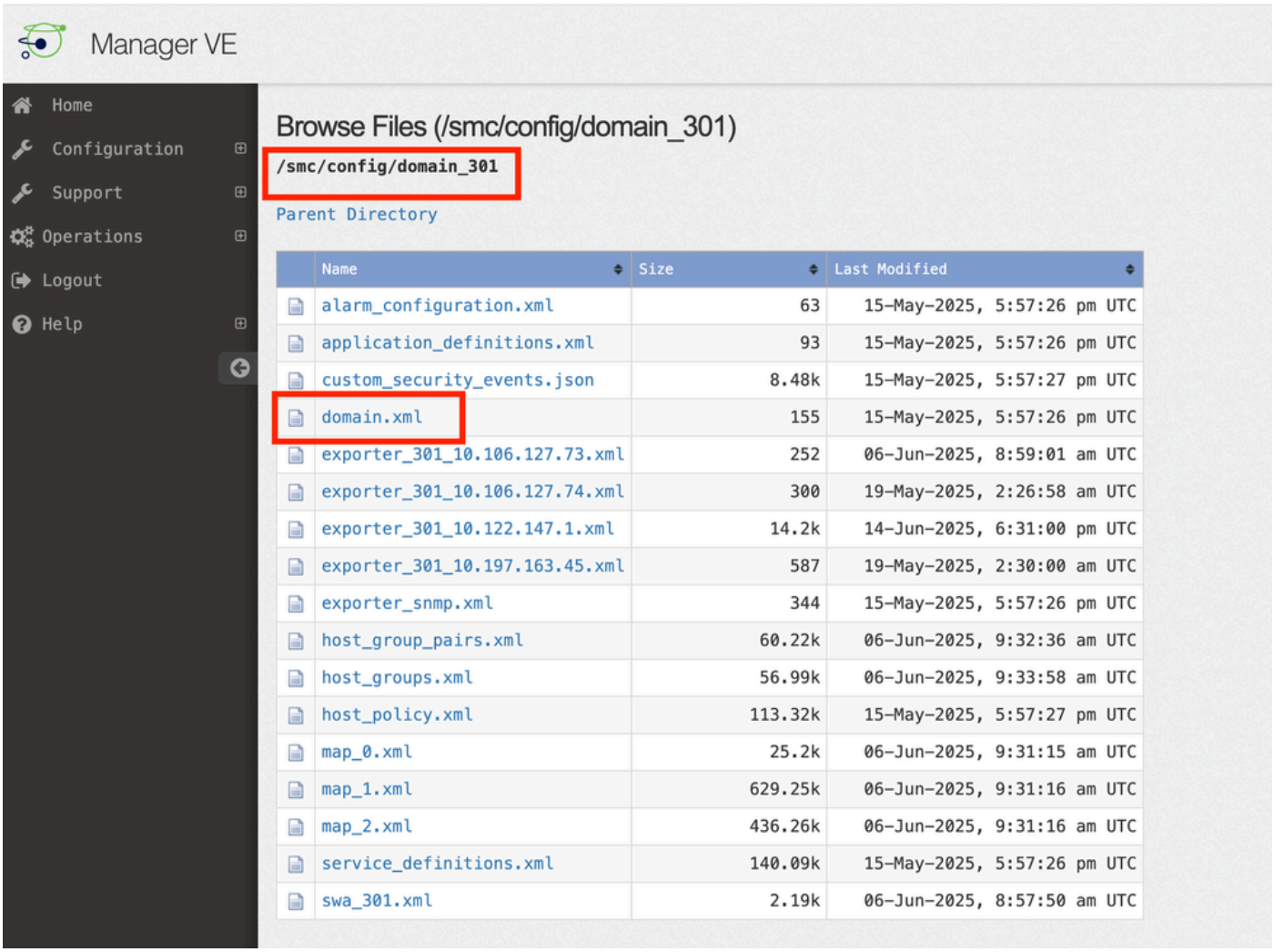
i. Accedere al gestore primario della SNA e reindirizzare alla pagina di amministrazione

dell'accessorio o all'URL dell'indice IP di access manager.

ii. Sfogliare la cartella smc nella sezione Supporto.



iii. Aprire il file domain.xml disponibile nella cartella domain_XXX all'interno della cartella config.


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

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).