Integration von SNA in Splunk mithilfe der Security Cloud-Anwendung

Inhalt

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

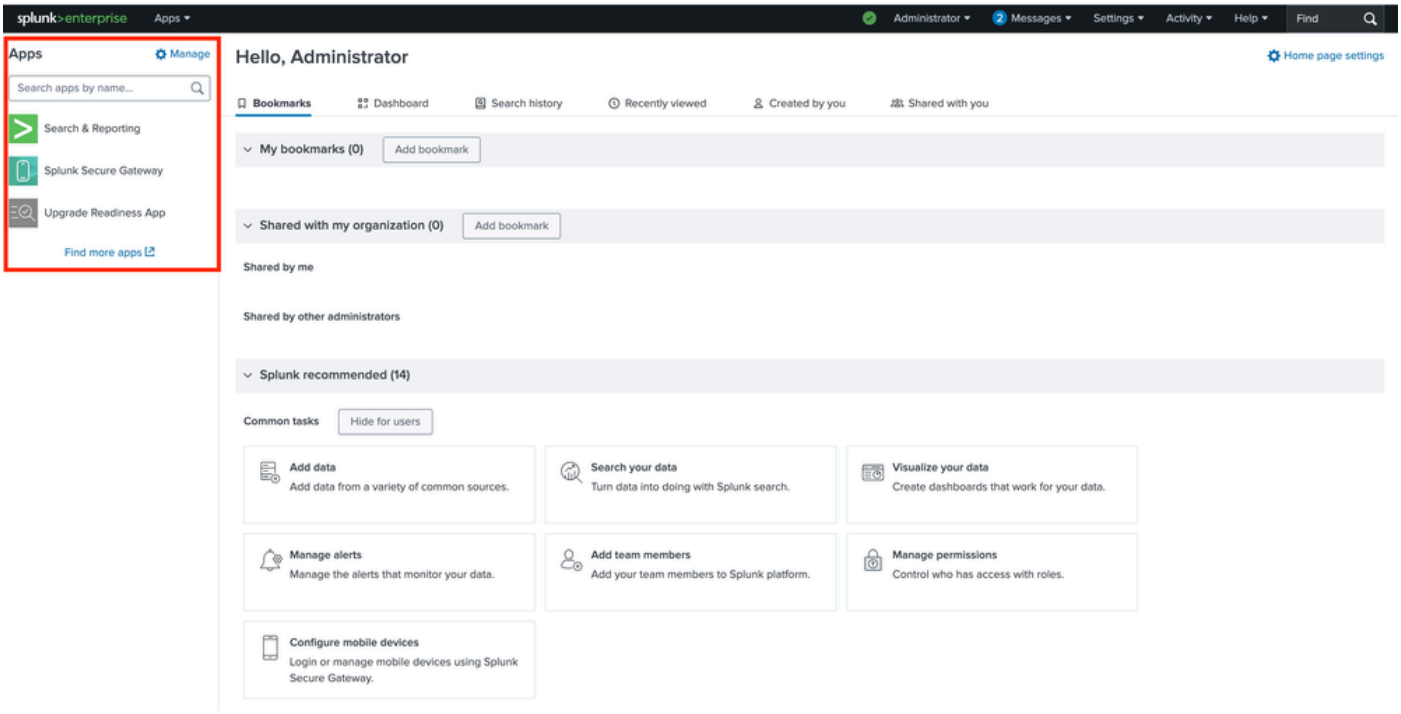
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Konfigurieren

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

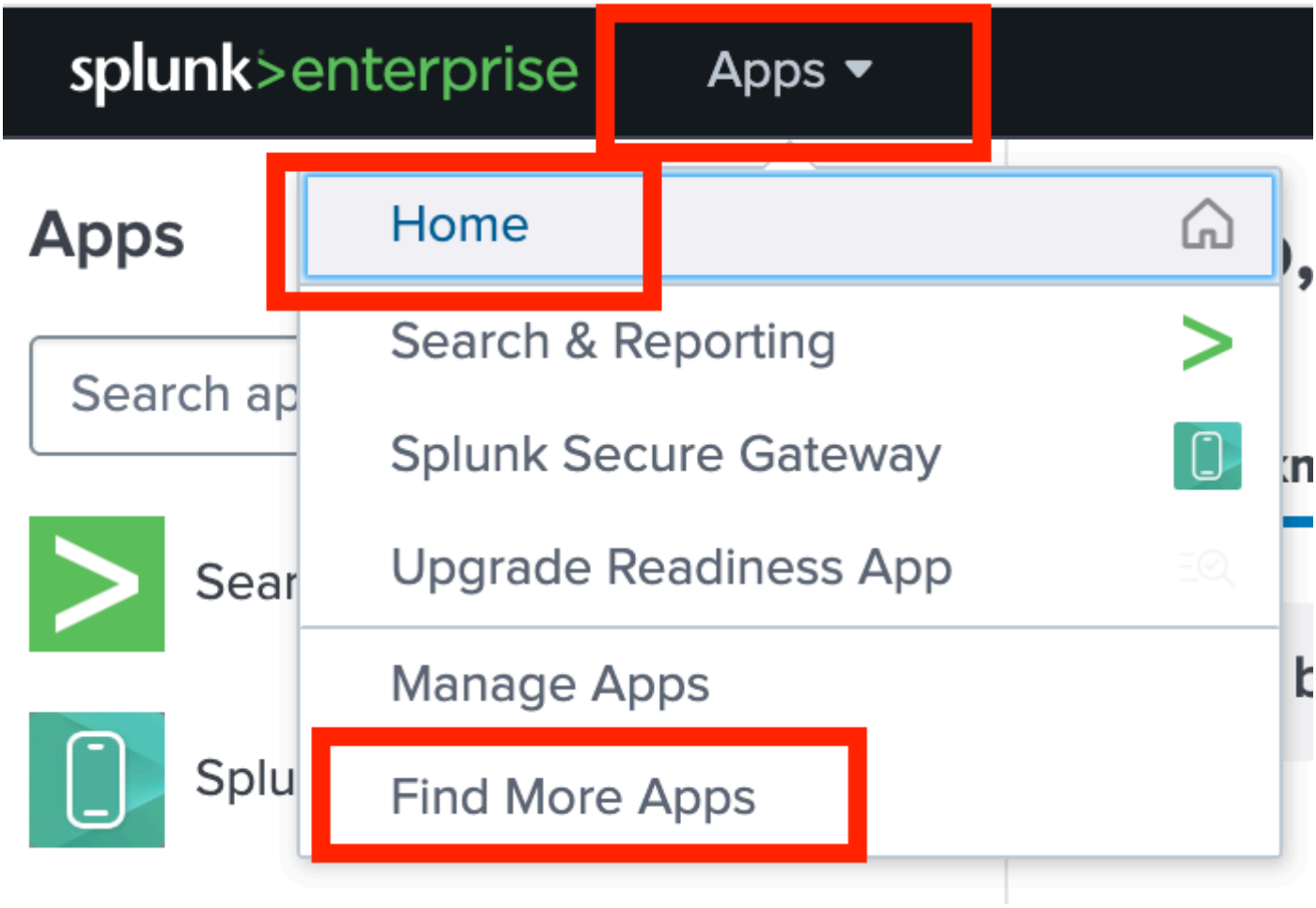
Anwendung.

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:

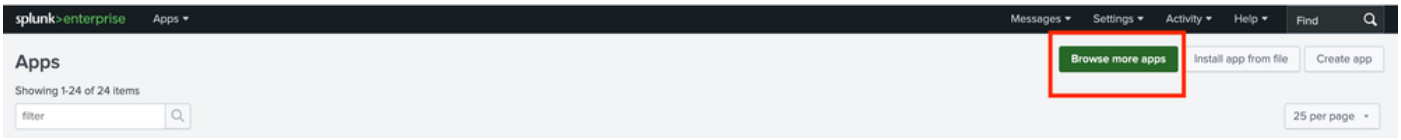


2. Für die Integration der SNA mit Splunk muss die Cisco Security Cloud-Anwendung installiert werden, die mit einer der folgenden Methoden erreicht werden kann:

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



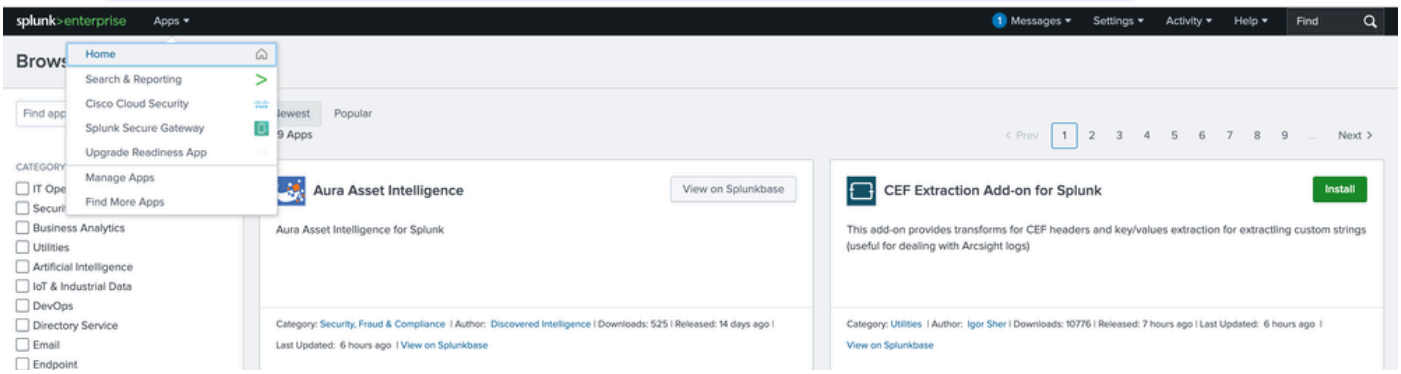
b. Über das Manager-Symbol können Sie weitere Apps durchsuchen.



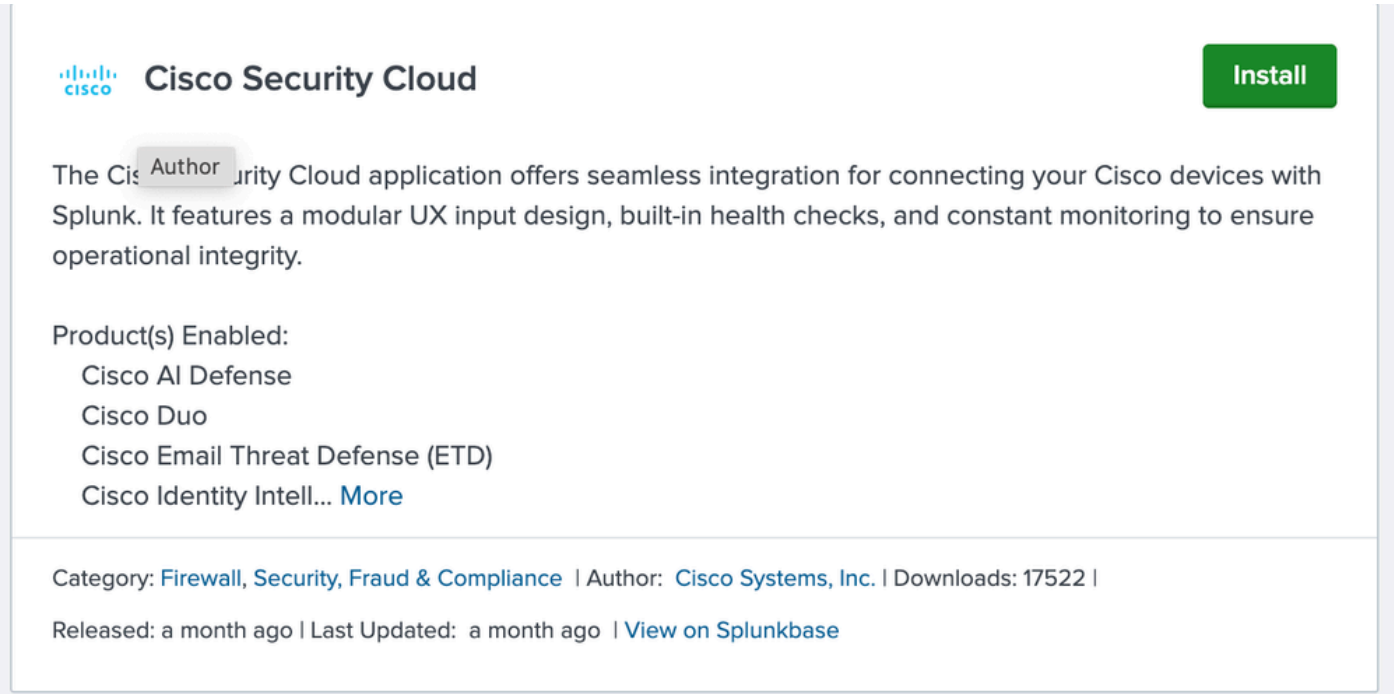
Phase 2: Installation der Cisco Security Cloud-Anwendung

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.

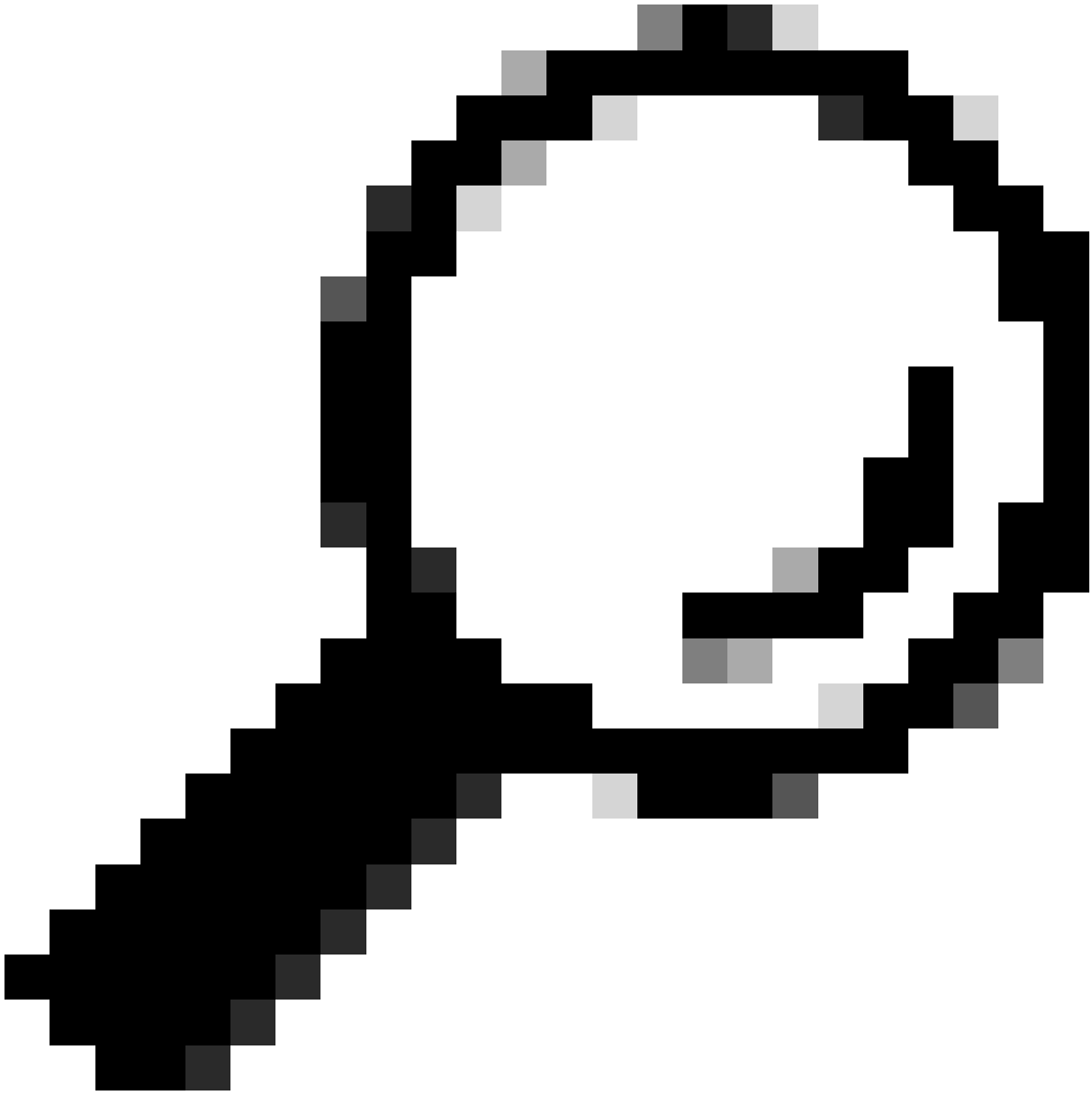
Vorsicht: Lassen Sie sich nicht mit der Cisco Cloud Security App verwechseln.



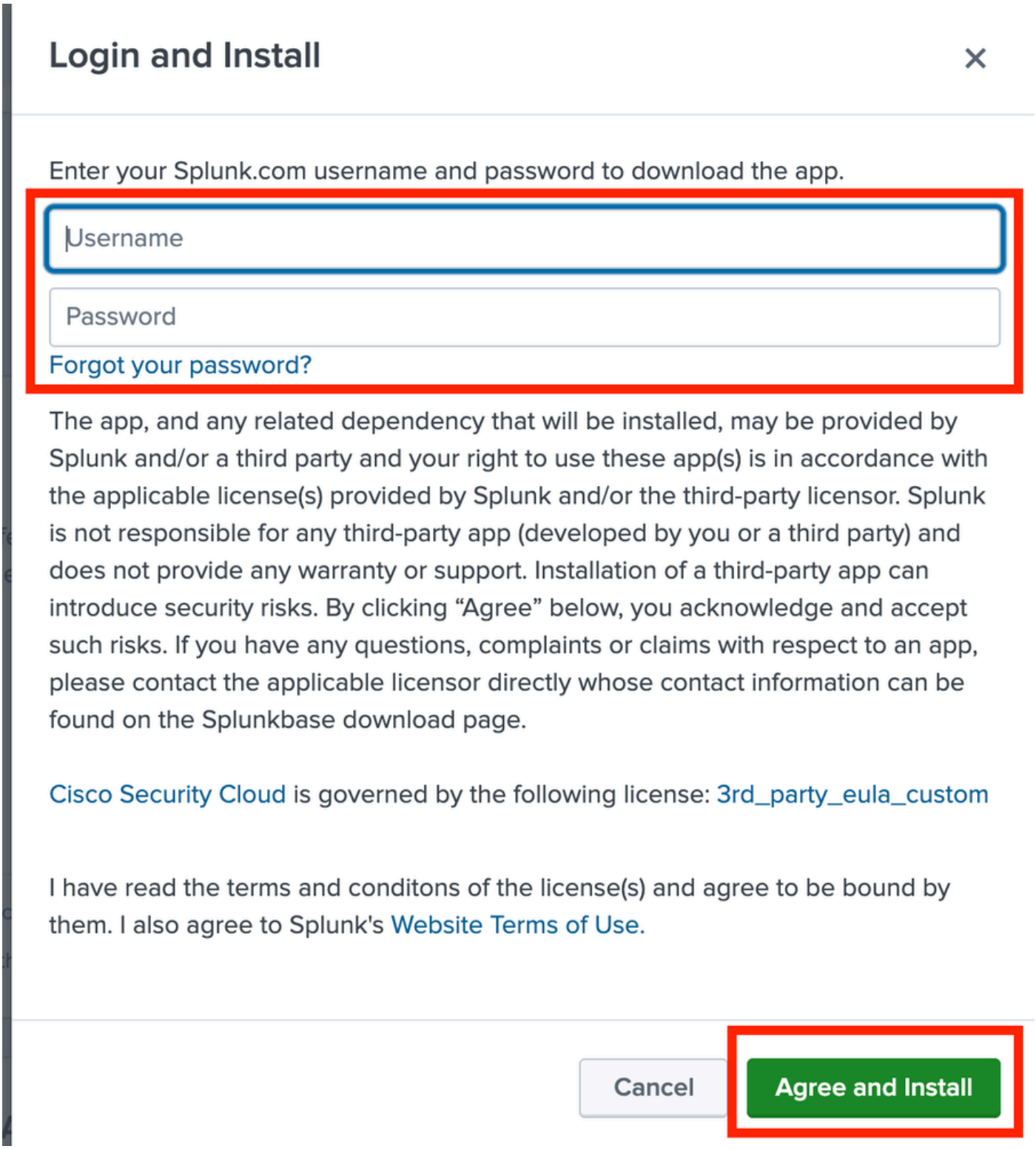
i. Installieren Sie die Anwendung, indem Sie auf die Schaltfläche Installieren klicken.



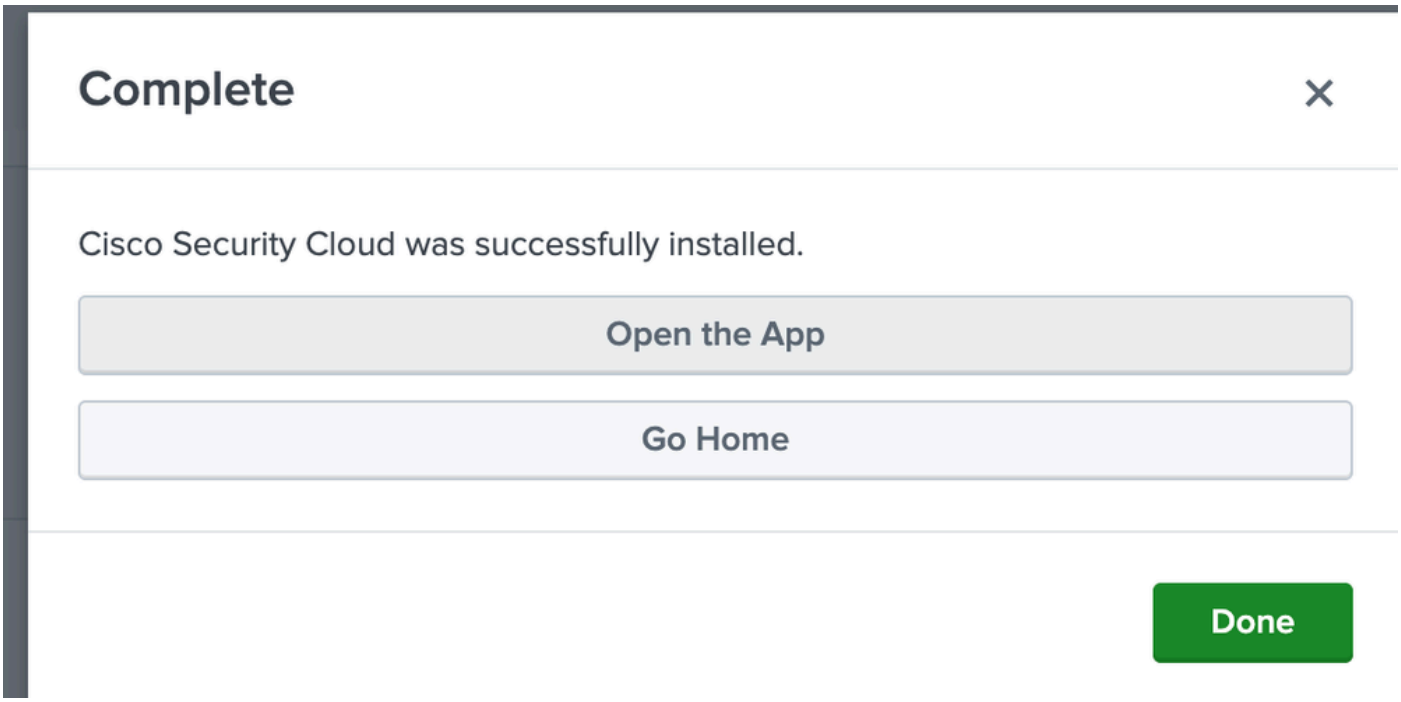
ii) Sobald Sie auf die Schaltfläche "Installieren" klicken, wird ein Fenster angezeigt, in dem Sie vor der Installation der Anwendung nach den Anmeldeinformationen des Splunk-Kontos gefragt werden. Geben Sie Ihre Anmeldeinformationen an, und klicken Sie auf Agree and Install, um fortzufahren.



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.

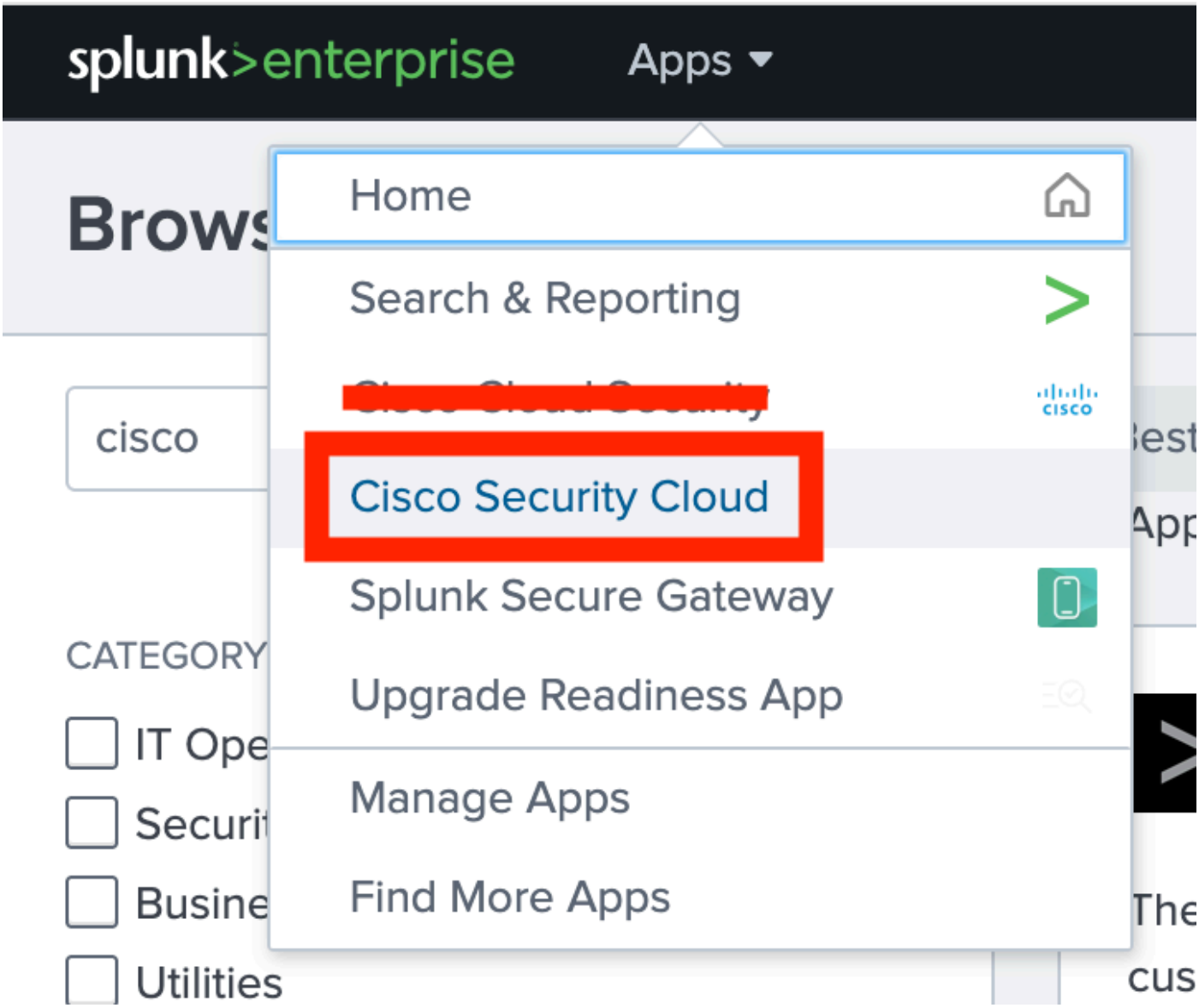


iii. Bei erfolgreicher Installation der Anwendung wird eine Meldung angezeigt, wie dargestellt. Klicken Sie auf Done (Fertig).

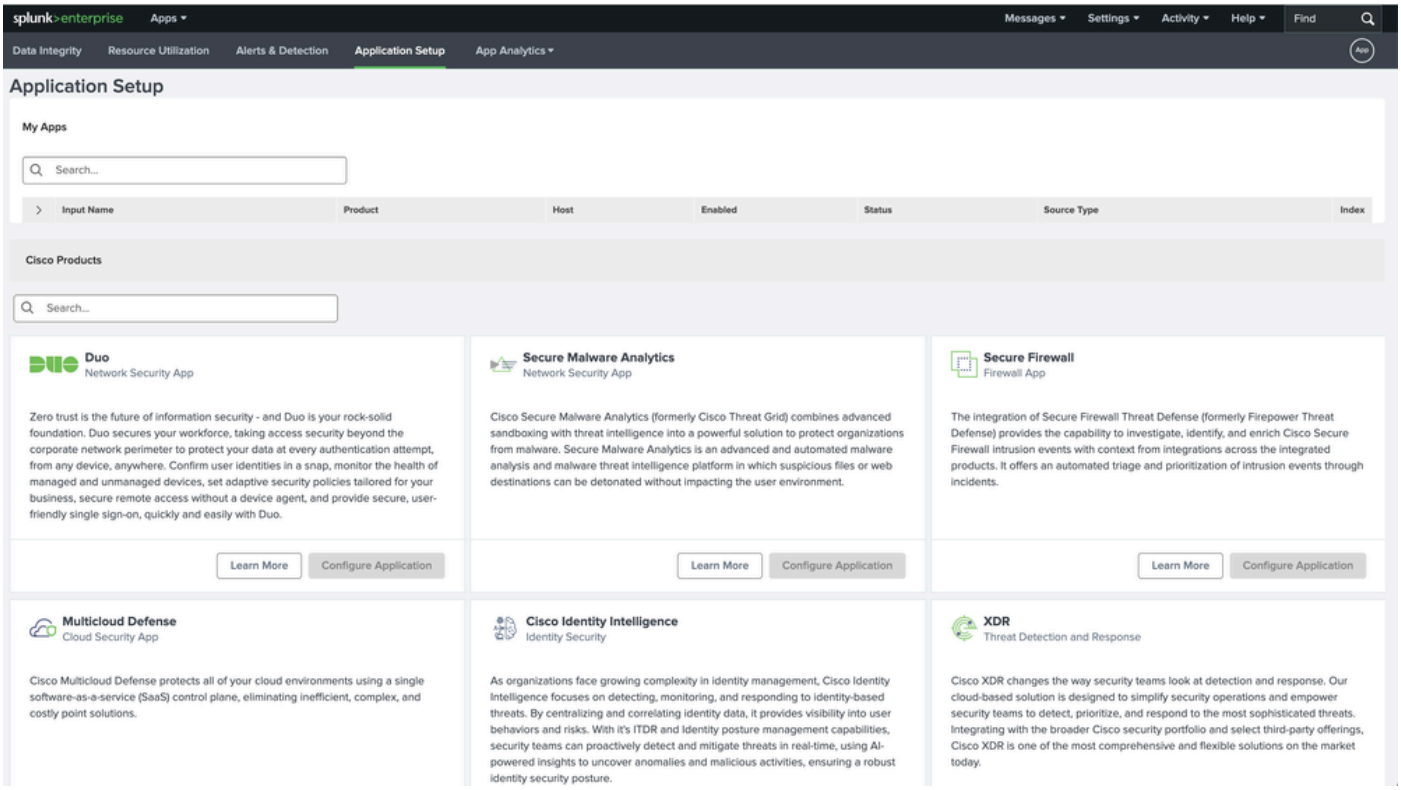


Schritt 3: Verifizierung der Installation der Cisco Security Cloud-Anwendung

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



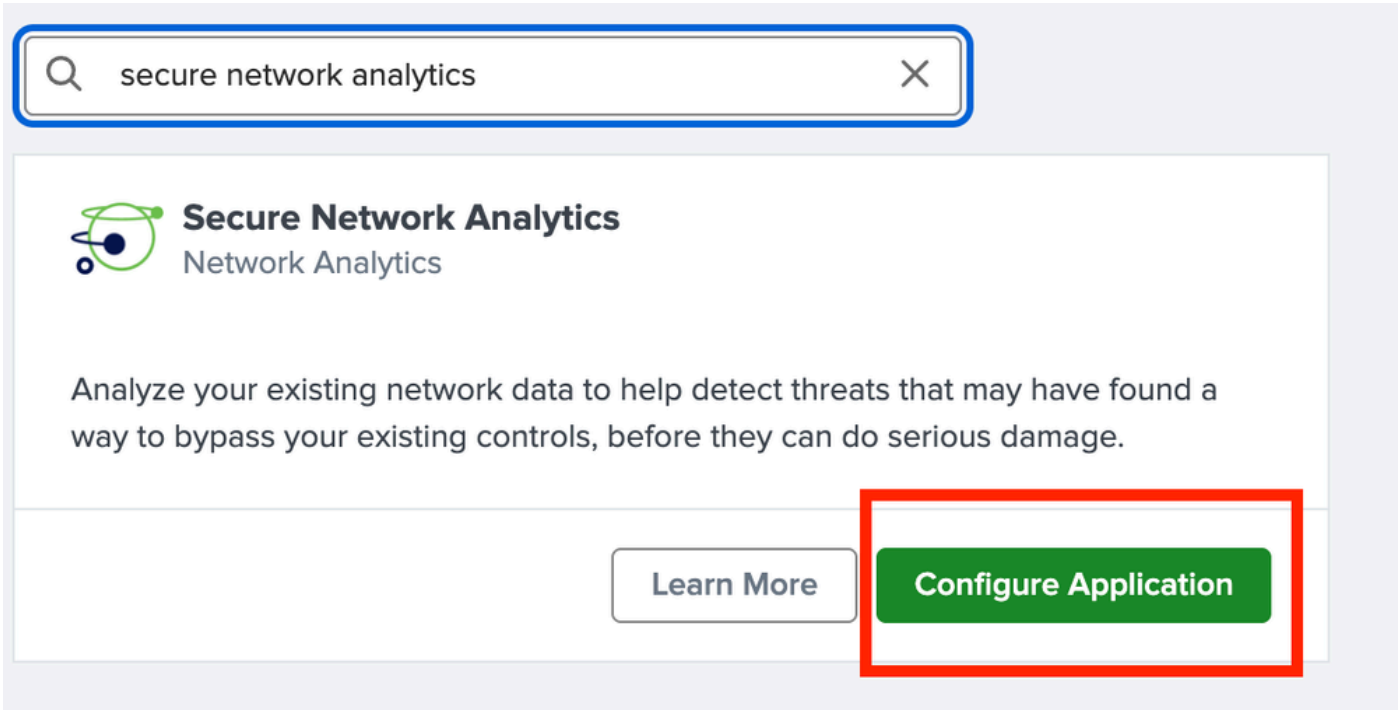
ii. Wählen Sie Cisco Security Cloud aus, indem Sie darauf klicken. Sie werden zur Seite Application Setup (Anwendungseinrichtung) weitergeleitet, auf der Sie alle verfügbaren Cisco Cloud Security-Produkte finden.



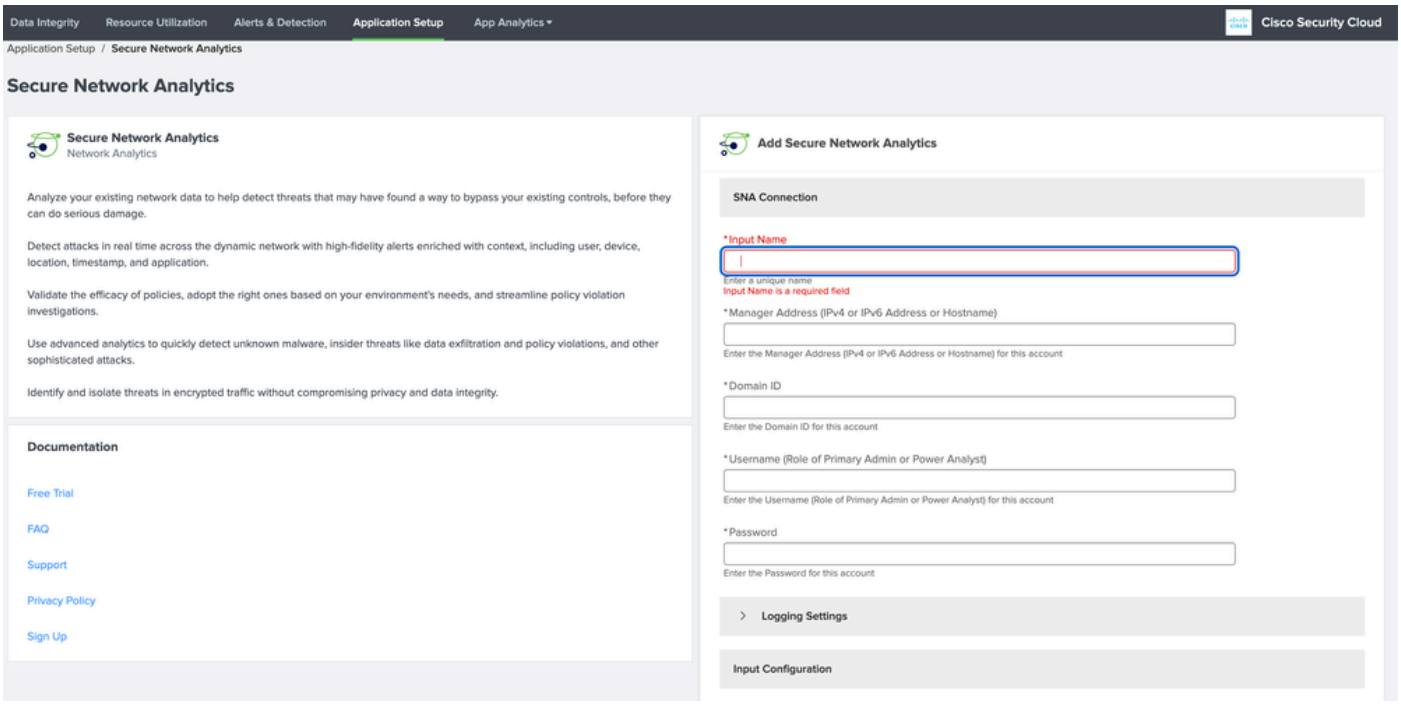
Schritt 4: Integration mit Secure Network Analytics (SNA)

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):

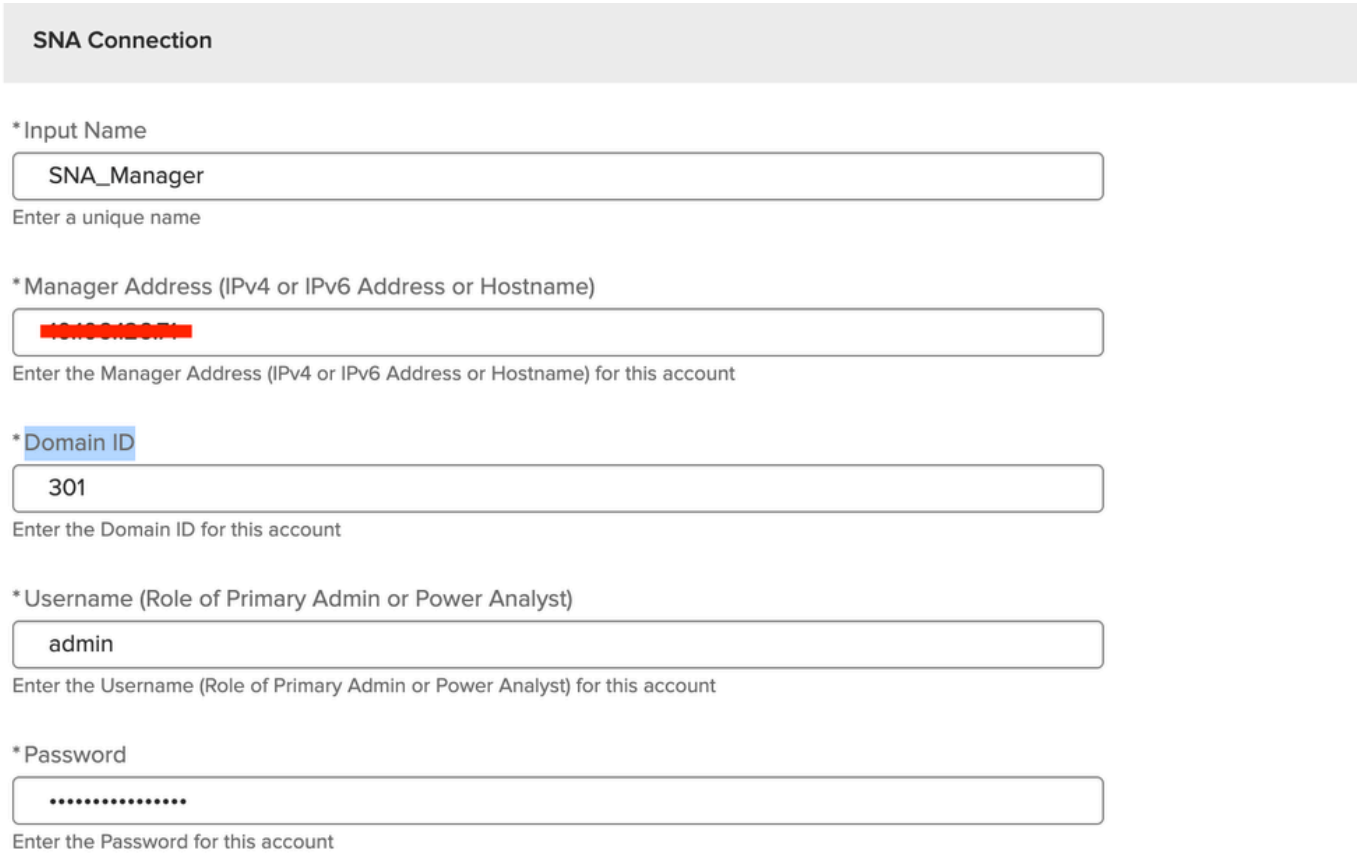


ii) Wenn Sie die Konfigurationsoption auswählen, wird die Konfigurationsseite angezeigt, auf der die hinzuzufügenden Details angezeigt werden.

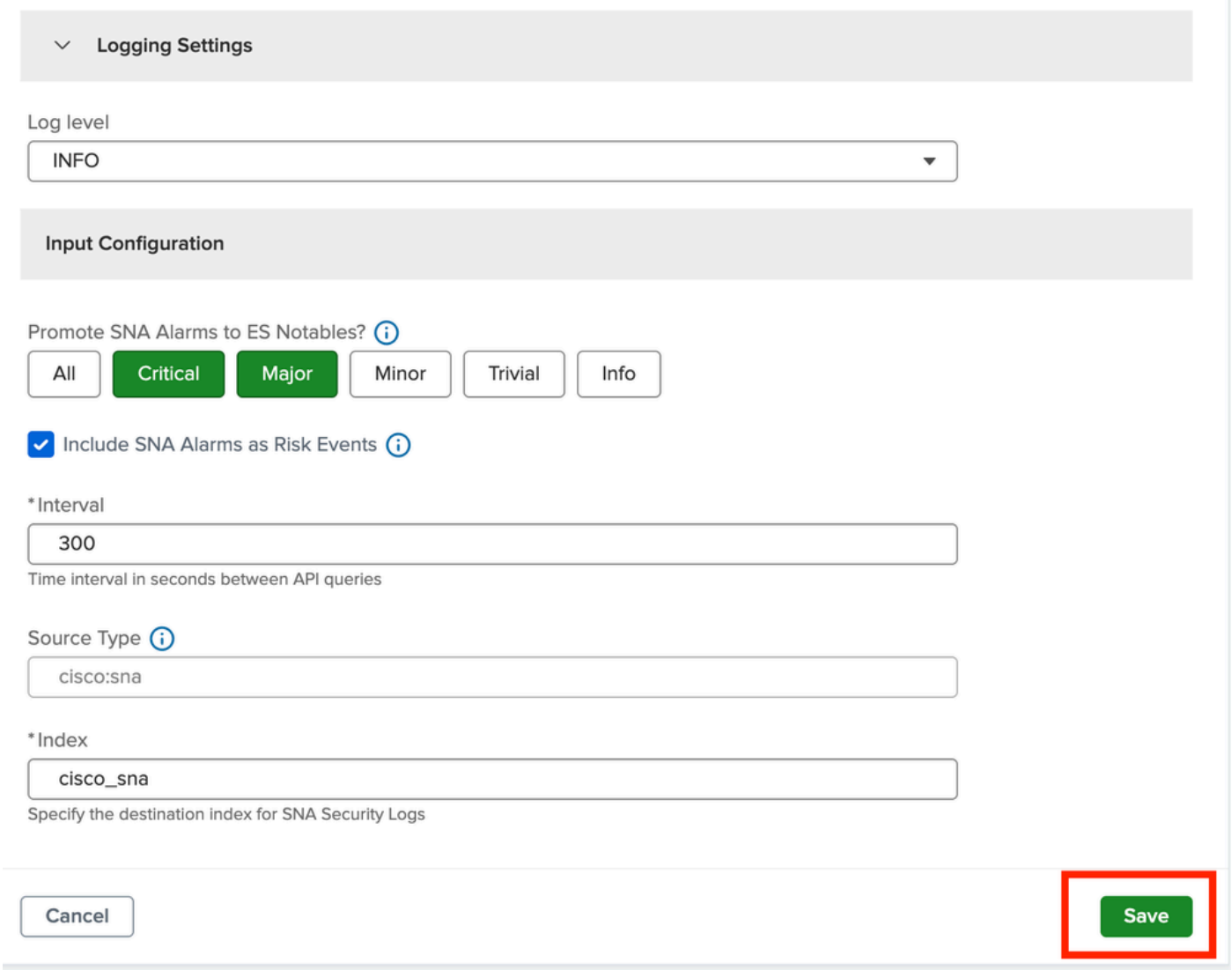


iii. Füllen Sie alle obligatorischen Angaben aus, die für die SNA-Verbindungsdetails angegeben sind:

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



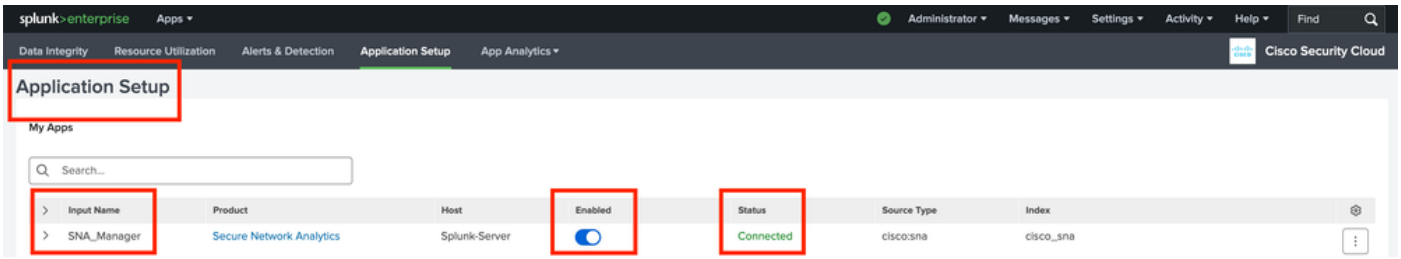
iv. Lassen Sie die übrigen Einstellungen auf ihren Standardwerten, oder ändern Sie sie nach Bedarf, und klicken Sie dann auf Speichern. Nach Abschluss des Vorgangs wird eine Meldung angezeigt.



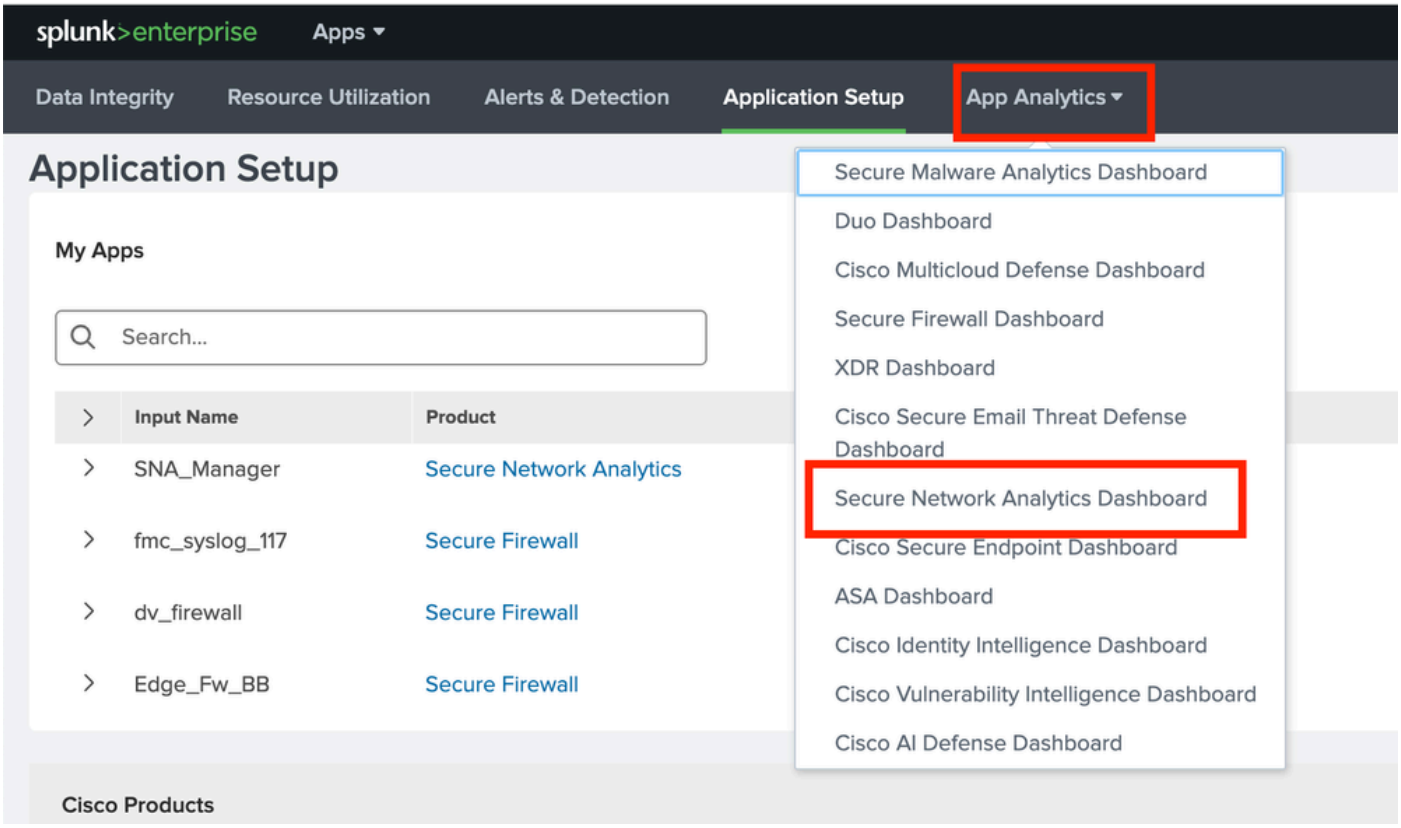
Schritt 5: Überprüfung der Integration.

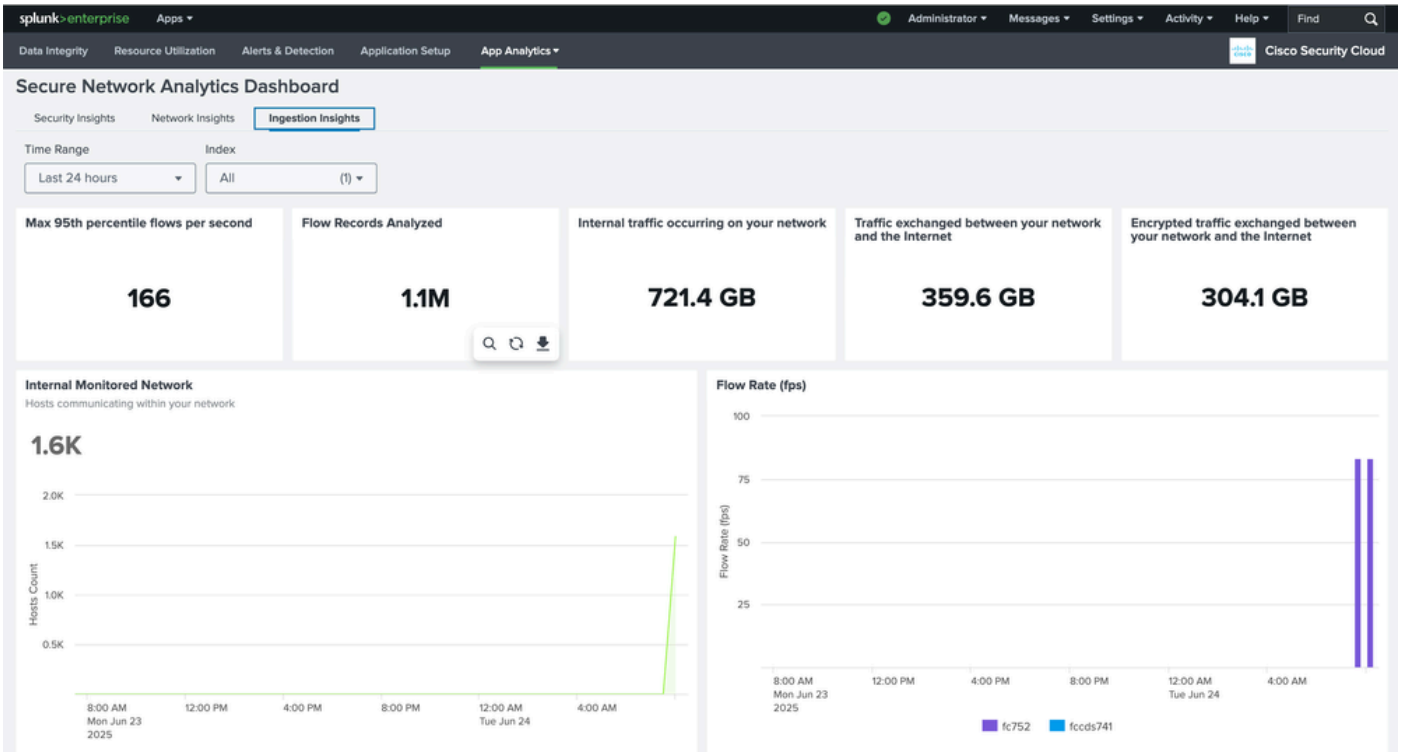
Dies ist ein wichtiger Schritt, bei dem Sie überprüfen müssen, ob die im vorherigen Schritt durchgeführte Integration erfolgreich abgeschlossen wurde.

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



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





Häufig gestellte Fragen

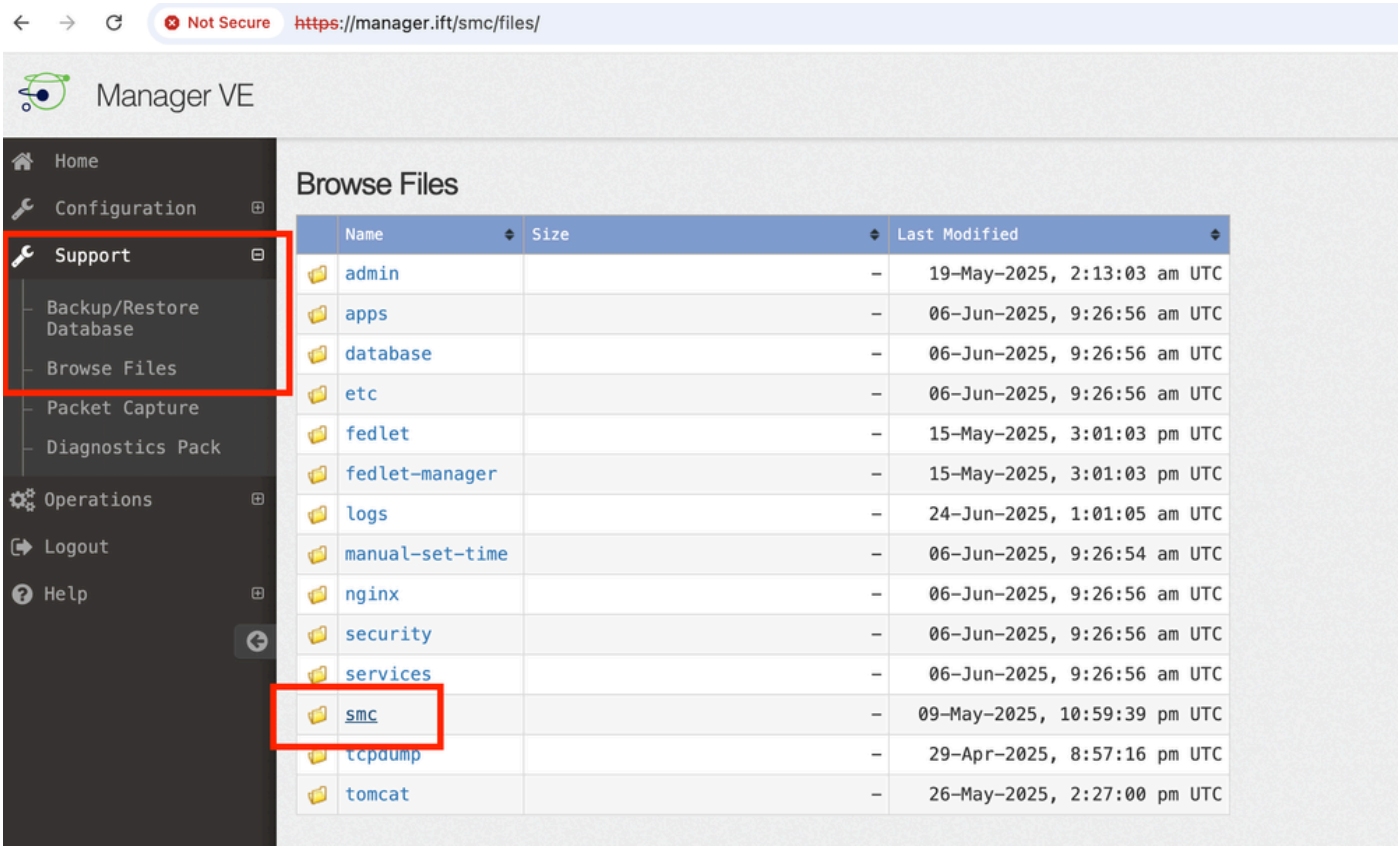
Wo finde ich die Domänen-ID für den SNA-Manager?

Antwort:

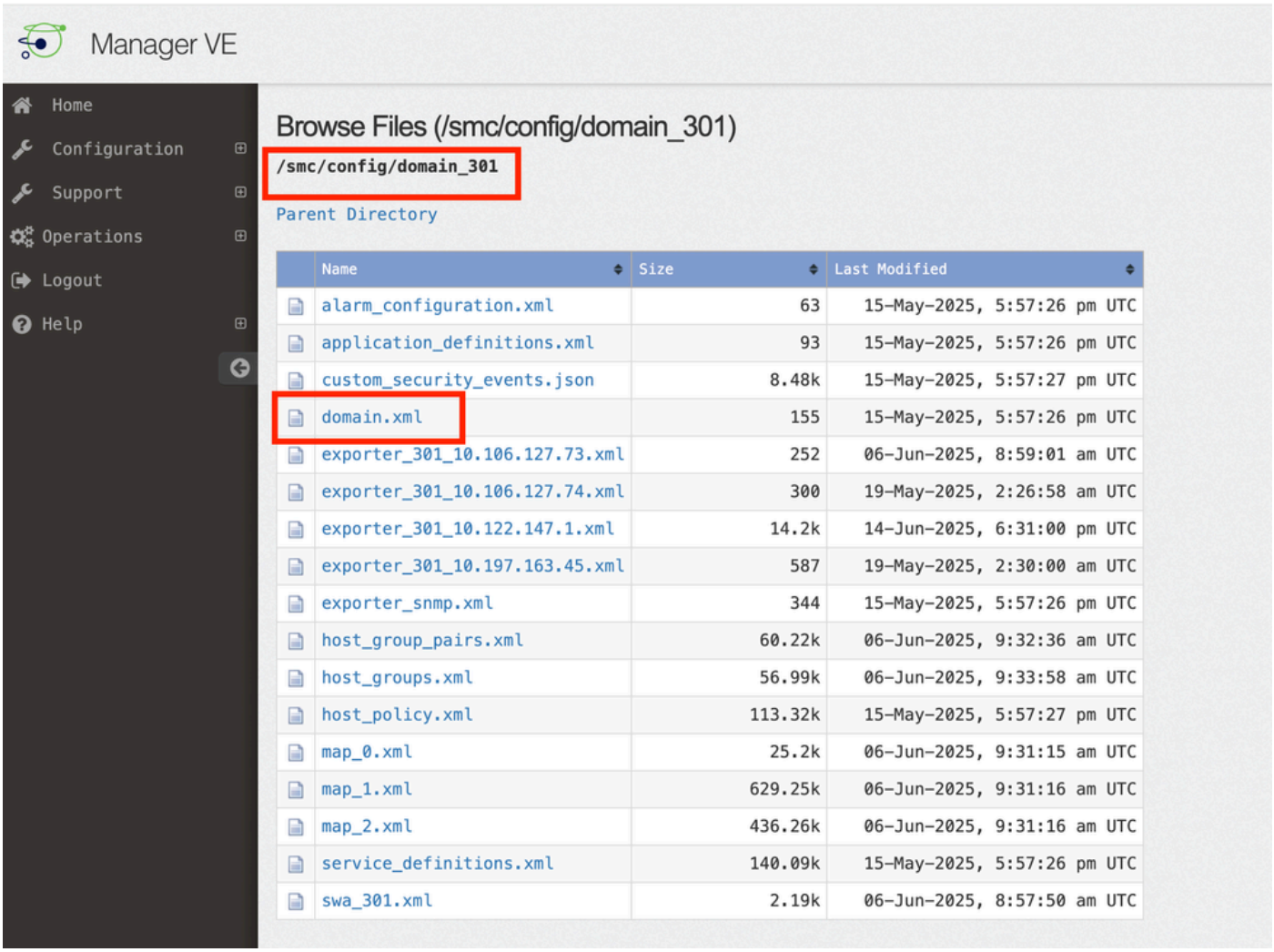
i. Melden Sie sich beim primären SNA-Manager an, und leiten Sie zur Verwaltungsseite der

Appliance um. Alternativ können Sie auf die IP Index-URL des Managers zugreifen.

ii) Durchsuchen Sie den Ordner smc im Abschnitt Support.



iii. Öffnen Sie die Datei domain.xml im Ordner domain_XXX unter dem Ordner 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

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.