SNA integreren in Splunk met behulp van Security Cloud-applicatie

Inhoud

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.

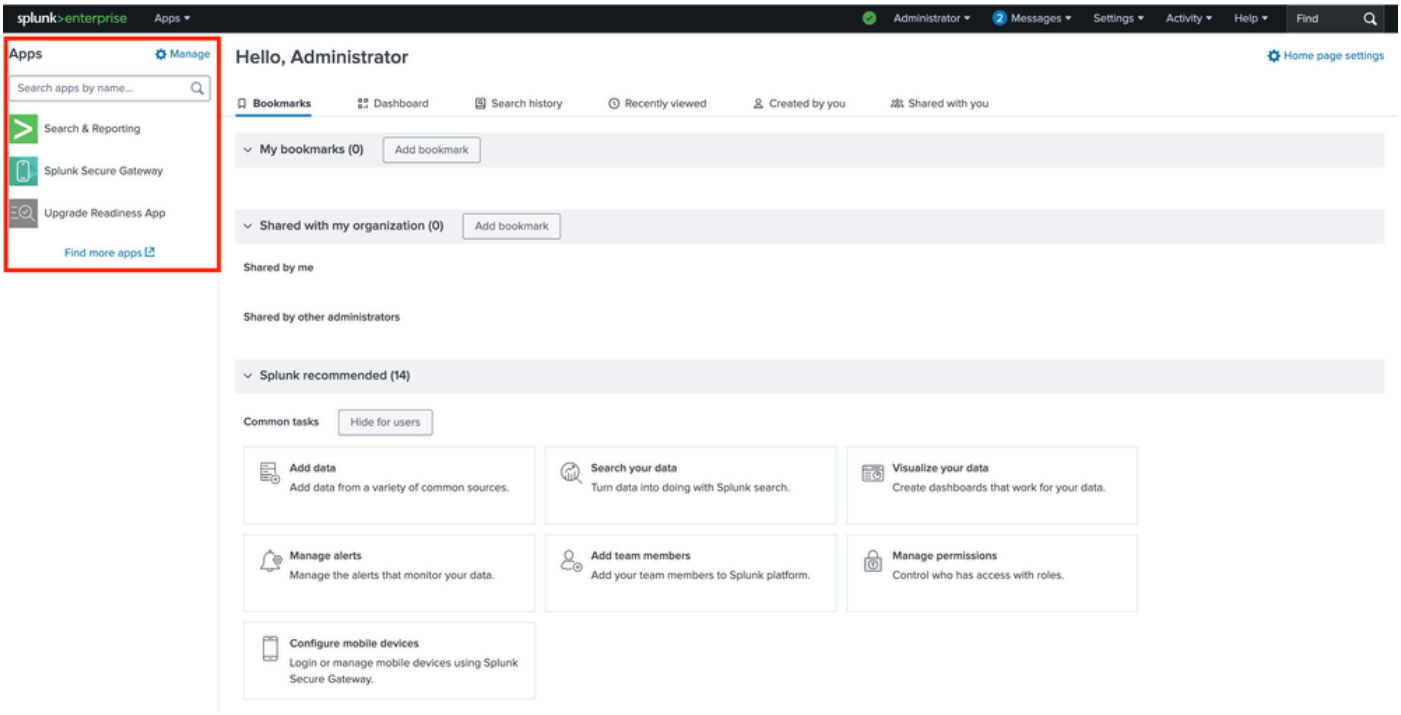
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

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

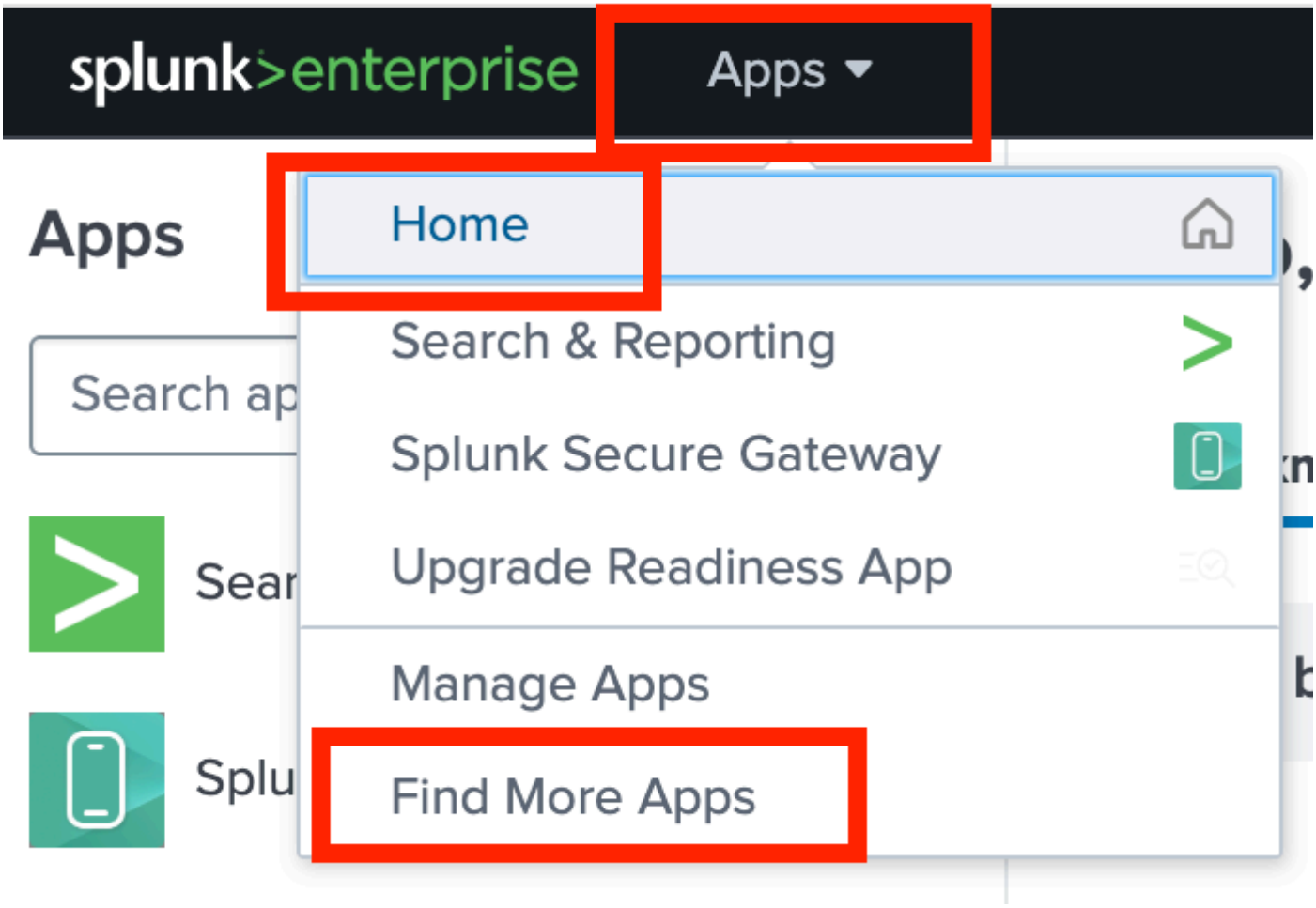
1. Meld u aan bij het Splunk-webportaal met de beheerdersreferenties en bij succesvol

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

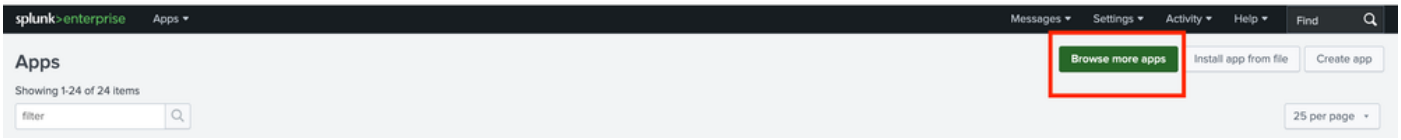


2. Voor de integratie van het SNA met Splunk moet de Cisco Security Cloud Application worden geïnstalleerd die kan worden bereikt met een van de genoemde methoden:

1. Selecteer Meer apps zoeken in de vervolgkeuzelijst.

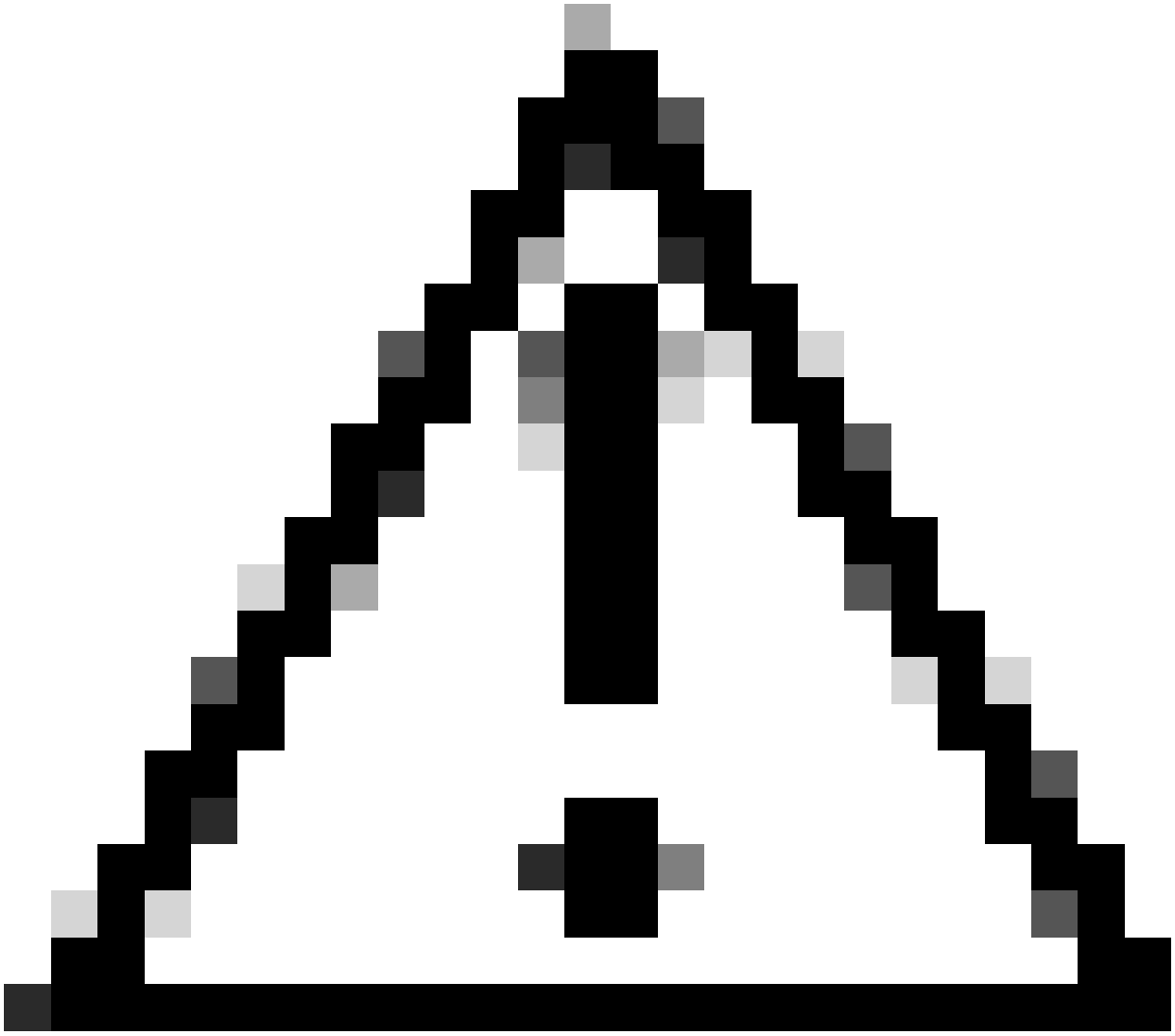


b. Blader door meer apps onder het tandwielpictogram Manager.

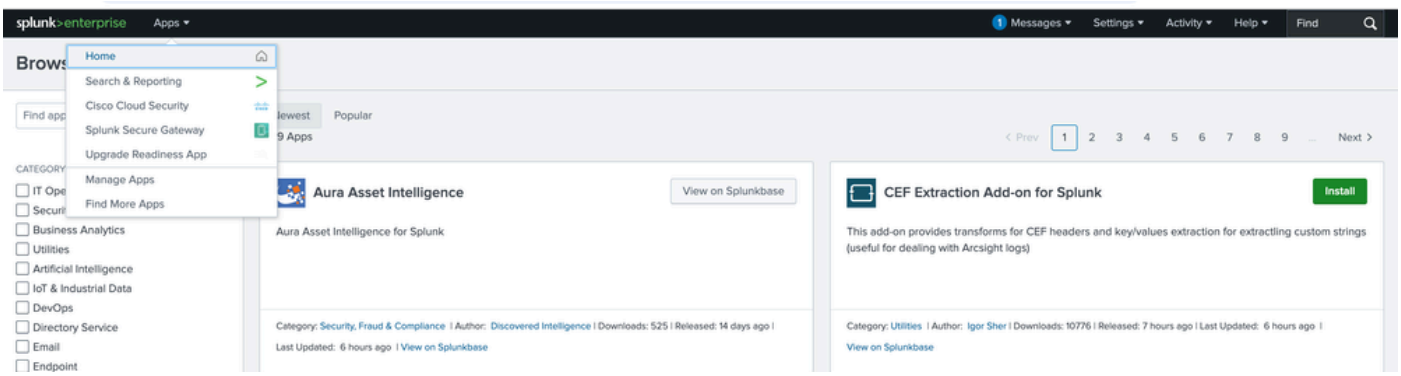


Stap 2: Installatie van de Cisco Security Cloud-applicatie.

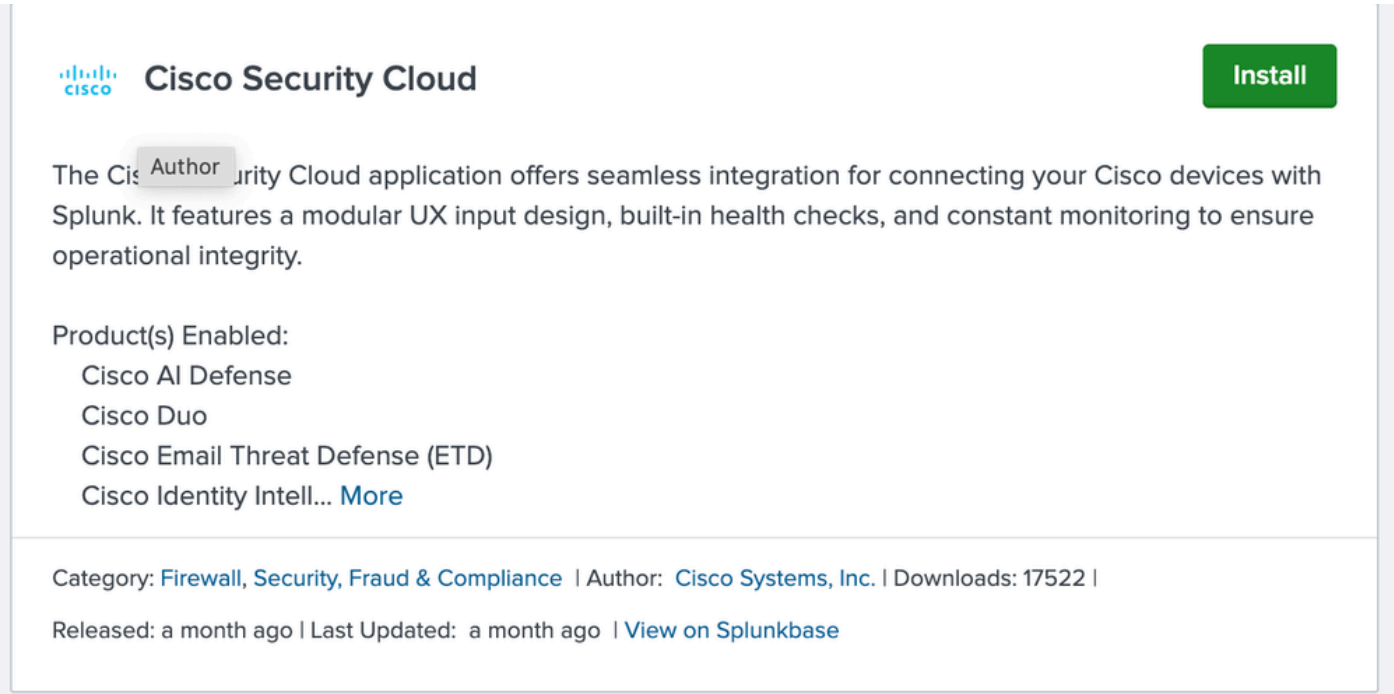
i. Zoek naar de Cisco Security Cloud-toepassing. Blader nu naar beneden totdat u de app hebt gevonden of zoek naar Cisco Security Cloud.



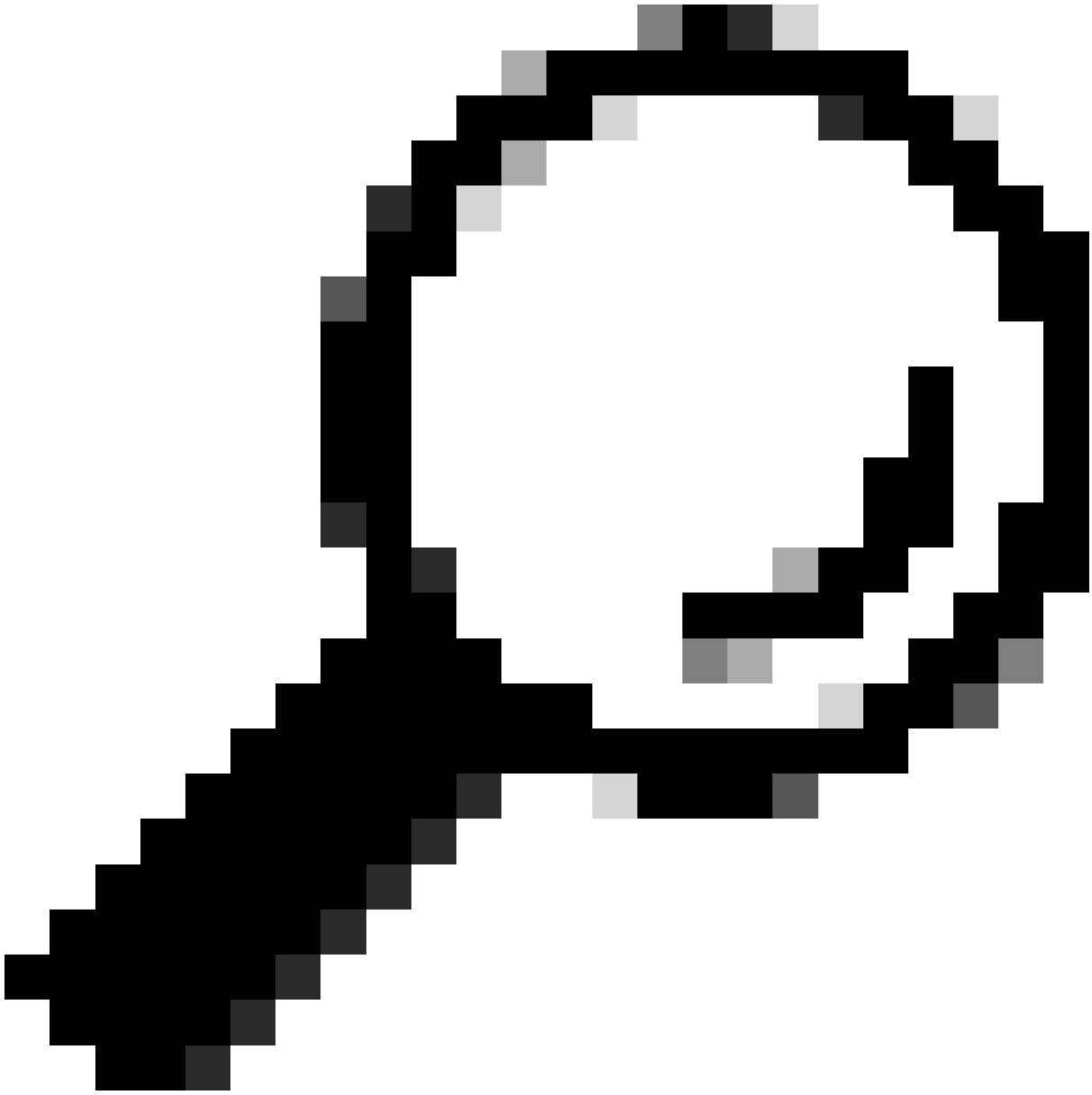
Let op: raak niet in de war met de Cisco Cloud Security App.



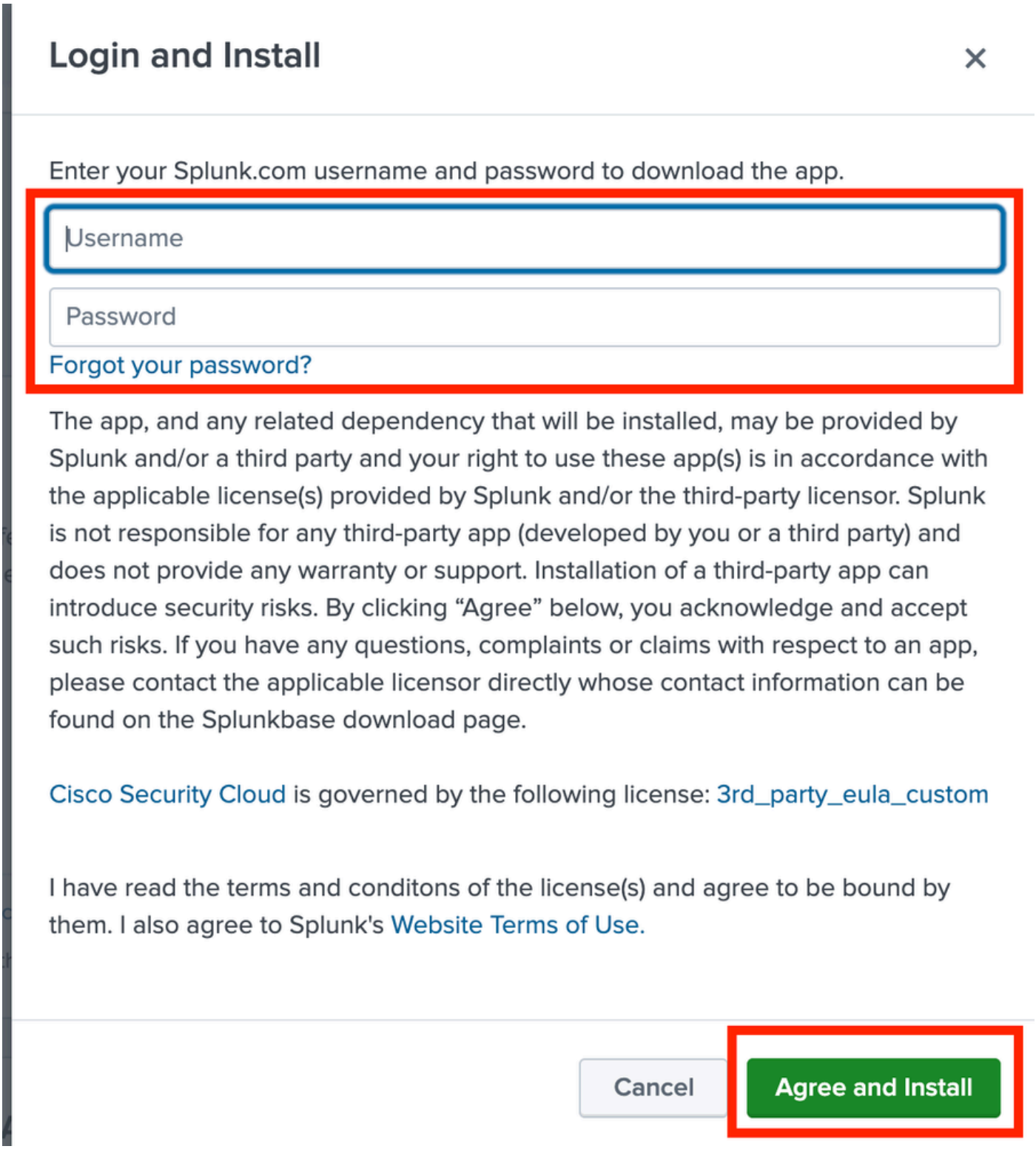
i. Installeer de toepassing door op de knop Installeren te klikken.



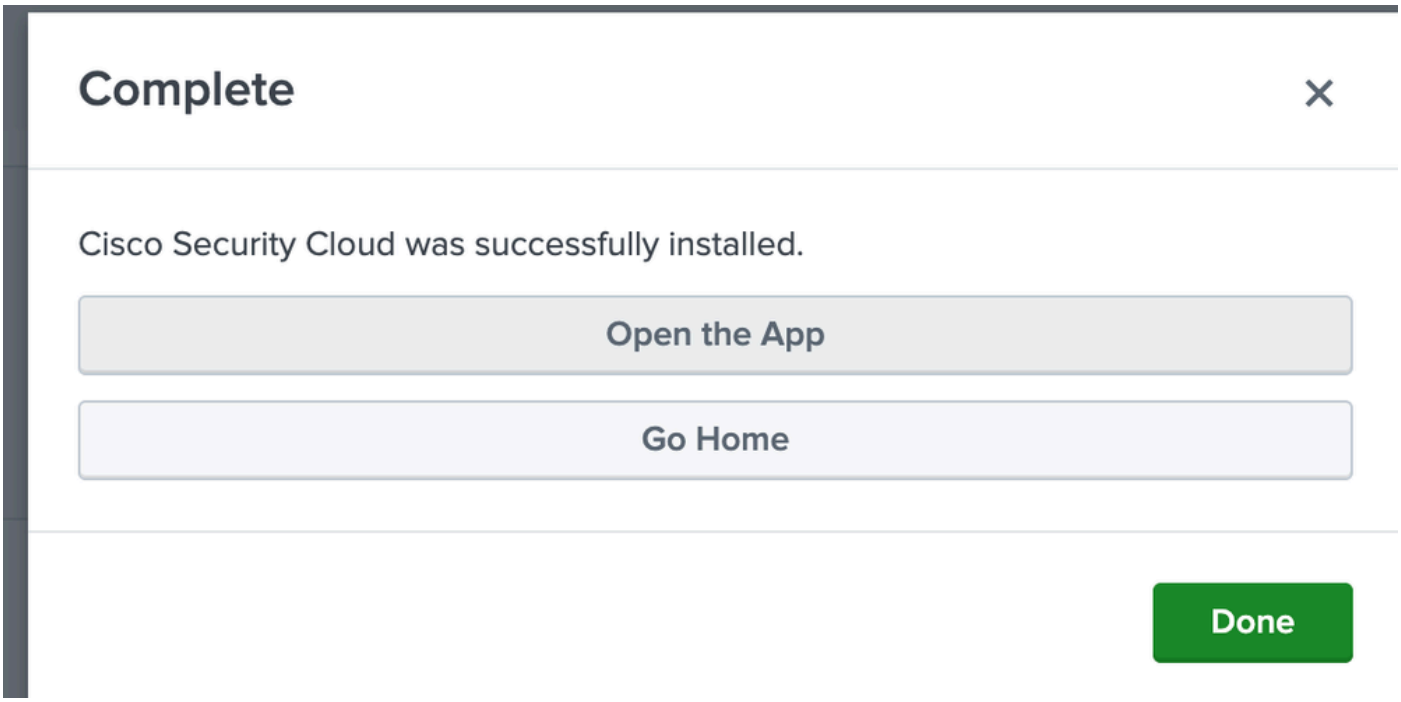
ii. Op het moment dat u op de installatieknop klikt, verschijnt een venster waarin u wordt gevraagd naar de referenties van de Splunk-account voordat u de toepassing installeert. Geef de referenties op en klik op Akkoord en Installeren om verder te gaan.



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

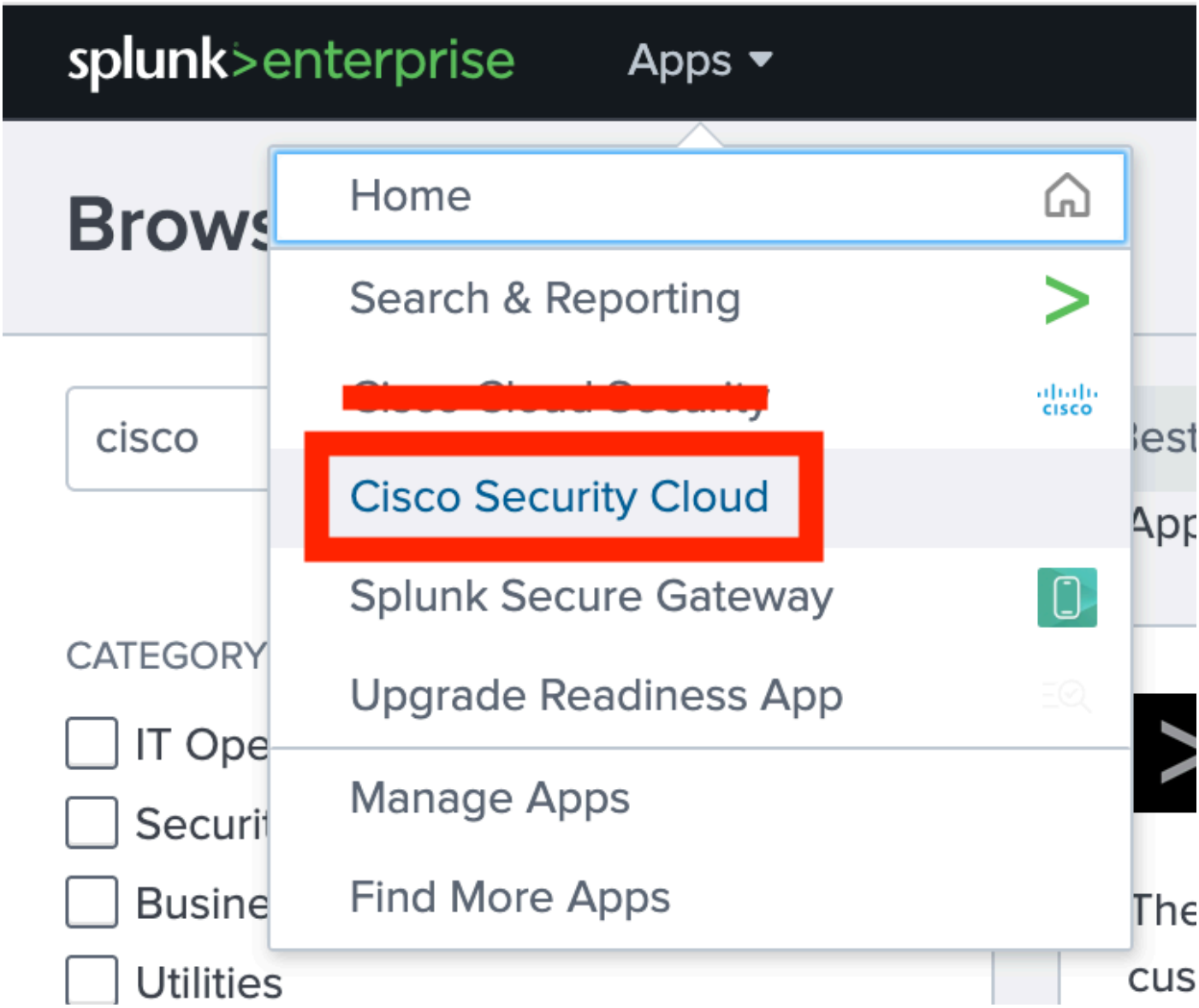


iii. Er verschijnt een bericht over de geslaagde installatie van de toepassing zoals afgebeeld. Klik op Gereed.

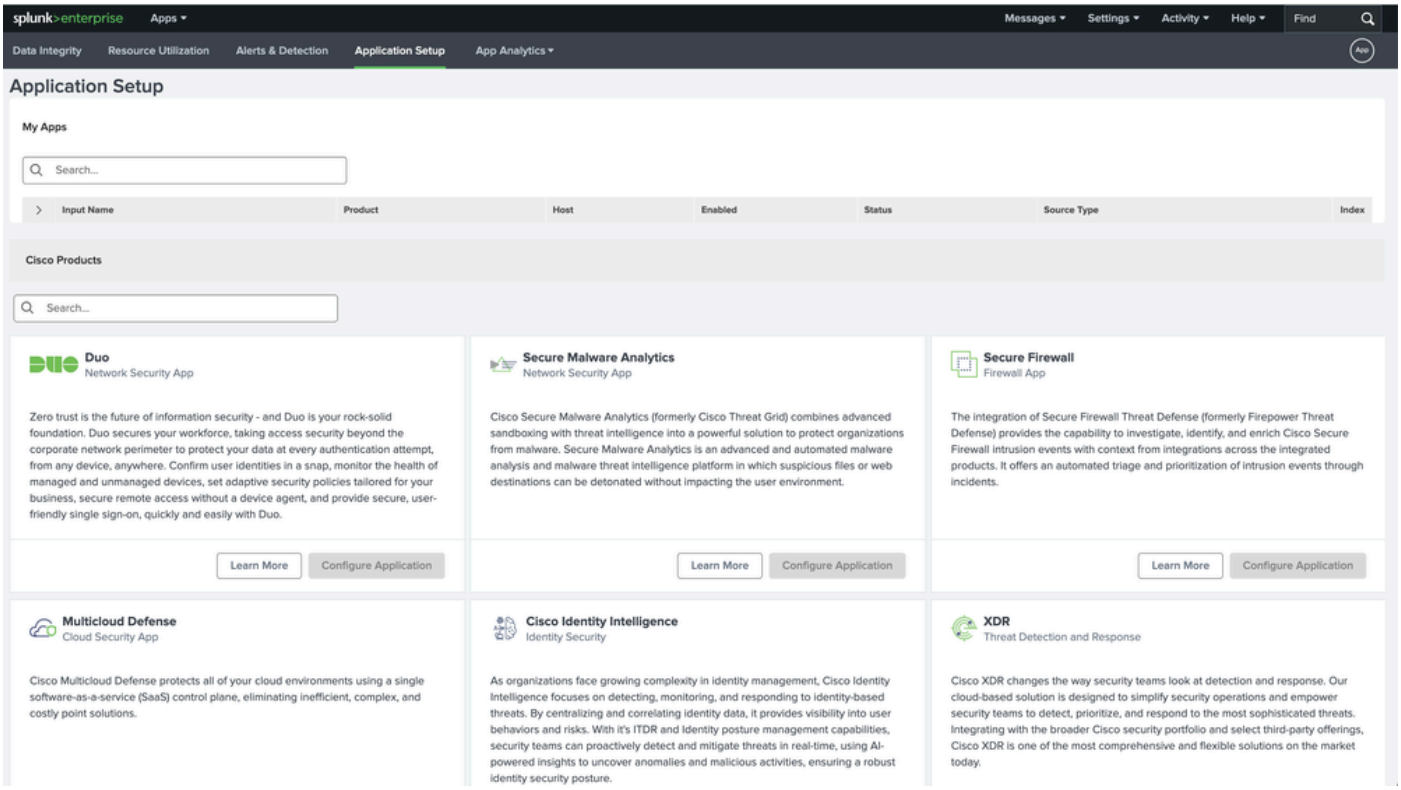


Stap 3: Verificatie van de installatie van de Cisco Security Cloud-applicatie.

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



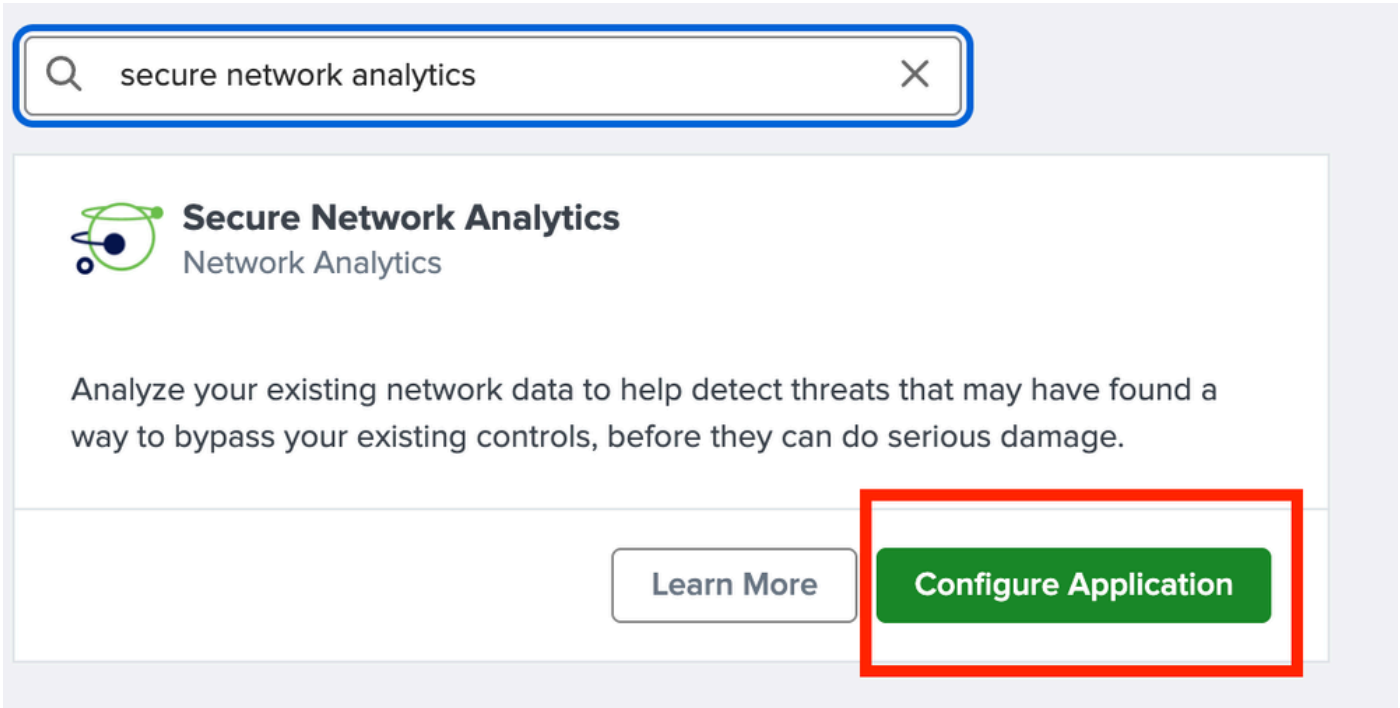
ii. Selecteer Cisco Security Cloud door erop te klikken. U wordt doorgestuurd naar de pagina Toepassingsinstellingen waar alle beschikbare Cisco Cloud-beveiligingsproducten te vinden zijn.



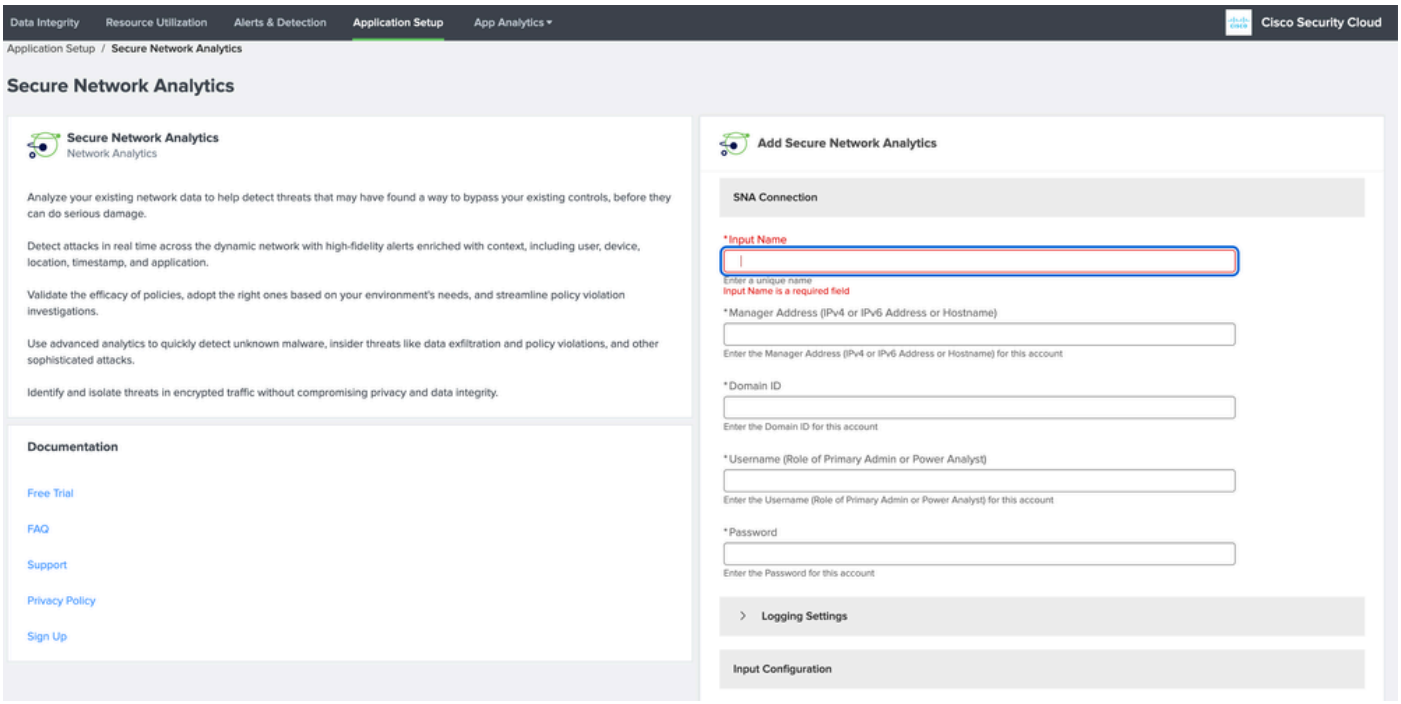
Stap 4: Integratie met Secure Network Analytics (SNA).

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:

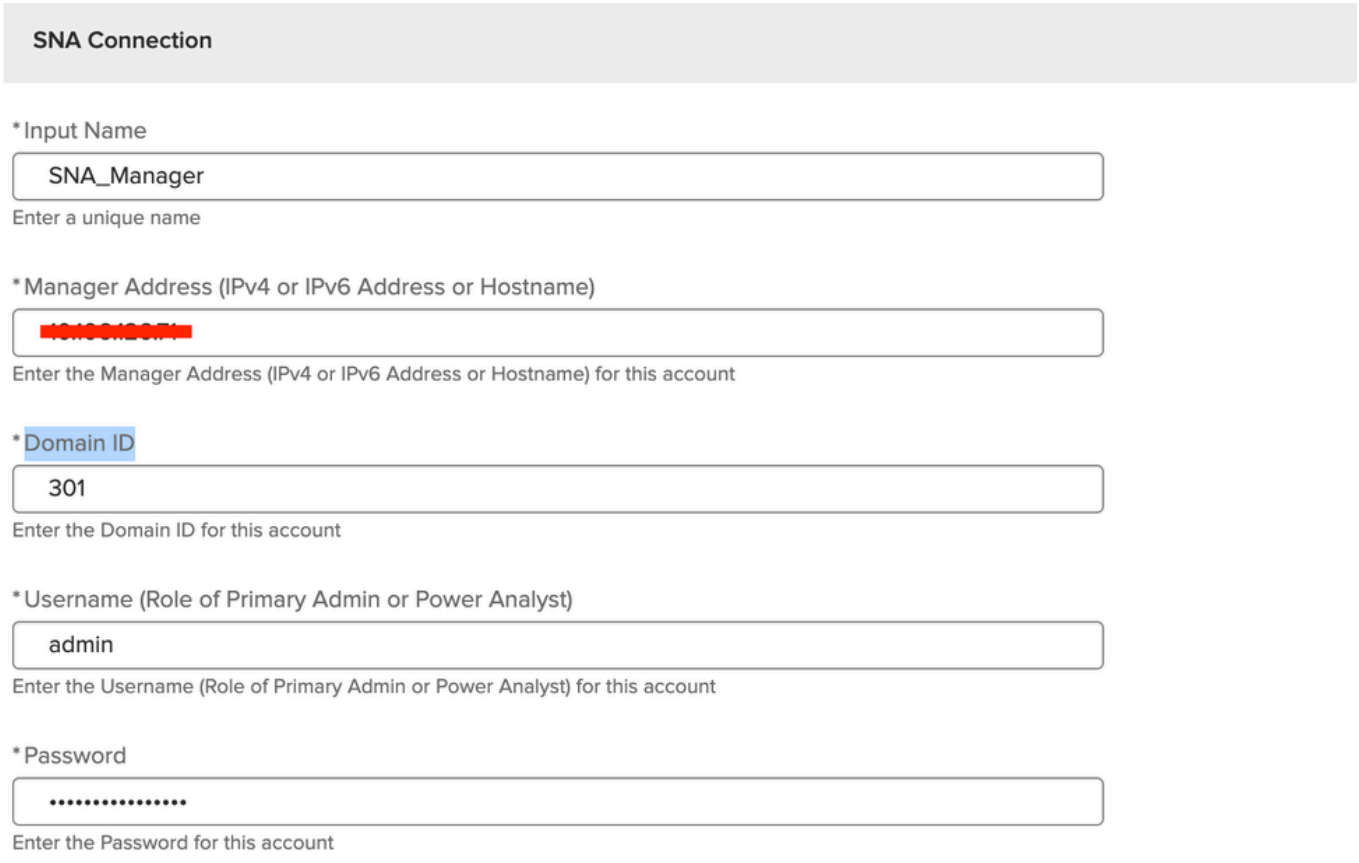


ii. Wanneer u de configuratieoptie selecteert, verschijnt de configuratiepagina voor de details die u wilt toevoegen.

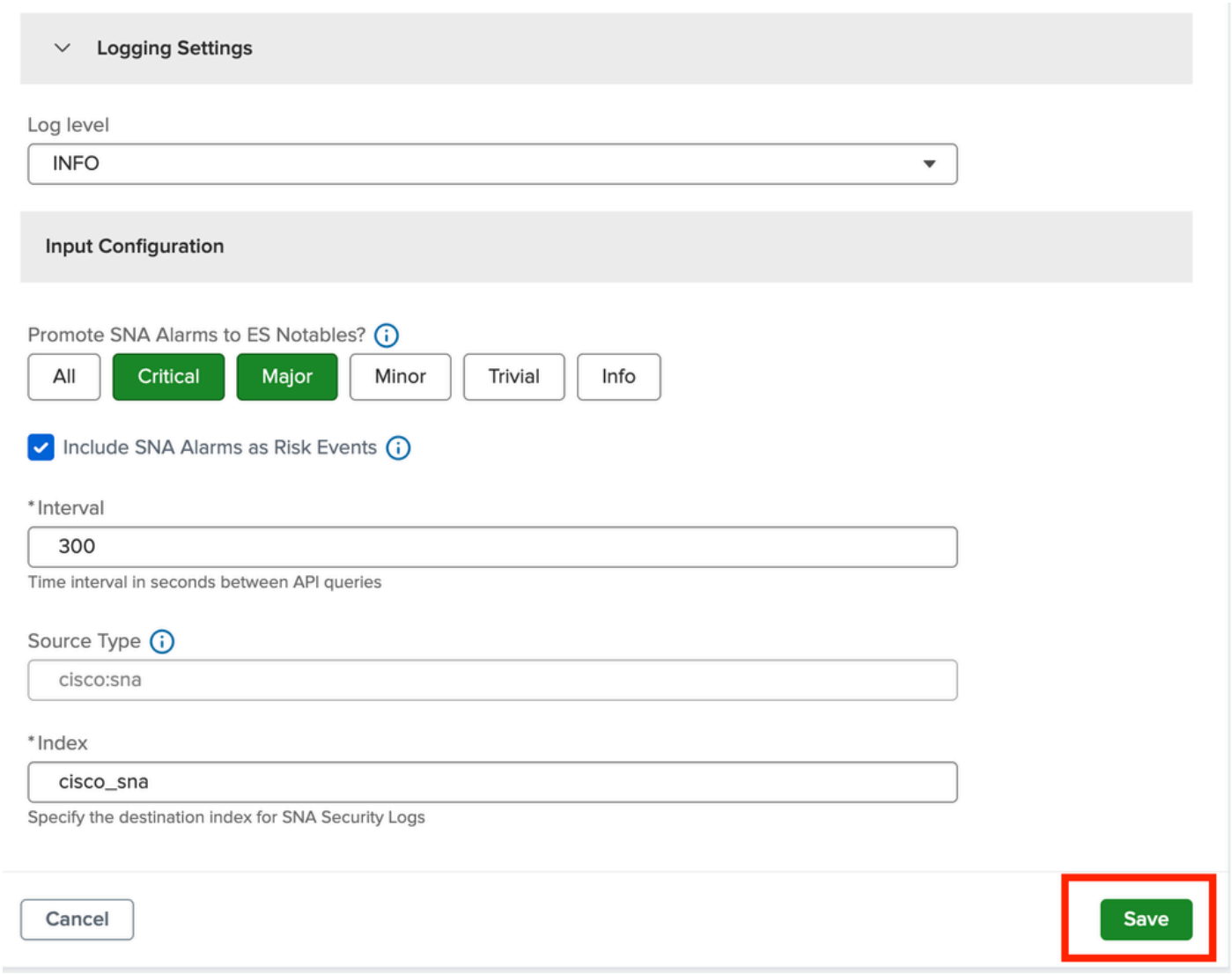


iii. Vul alle verplichte gegevens in zoals vermeld voor de SNA Connection Details:

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



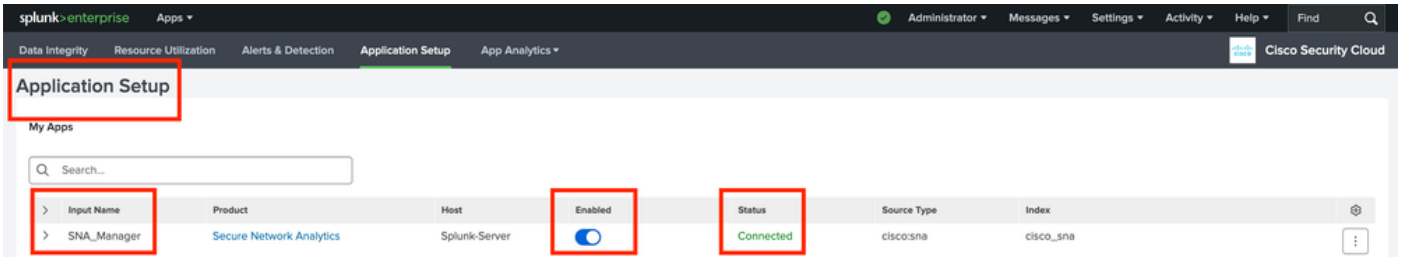
iv. Laat de overige instellingen op hun standaardwaarden staan of wijzig ze indien nodig en klik op Opslaan. Een succesvol bericht verschijnt op het scherm na de voltooiing.



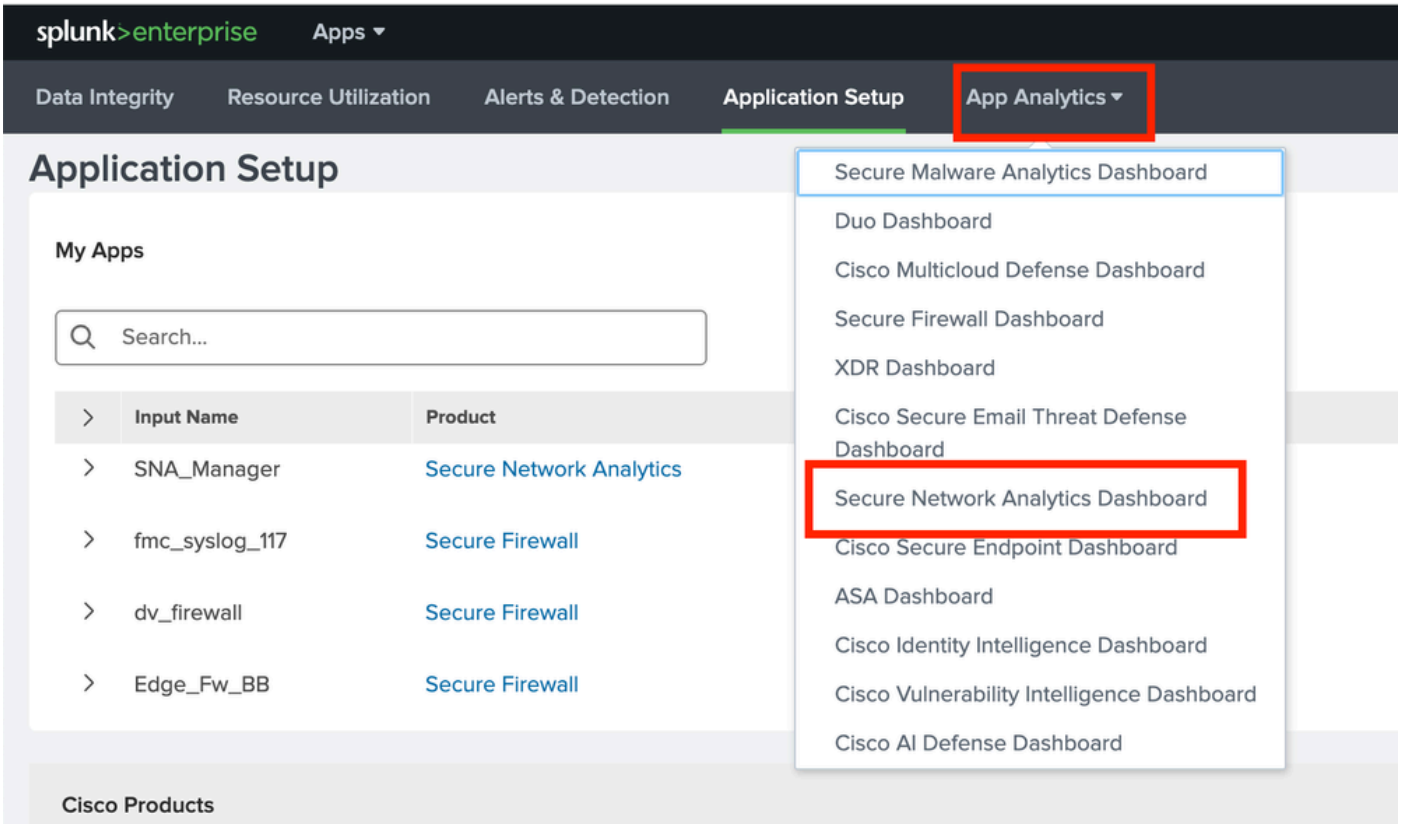
Stap 5: Verificatie van de integratie.

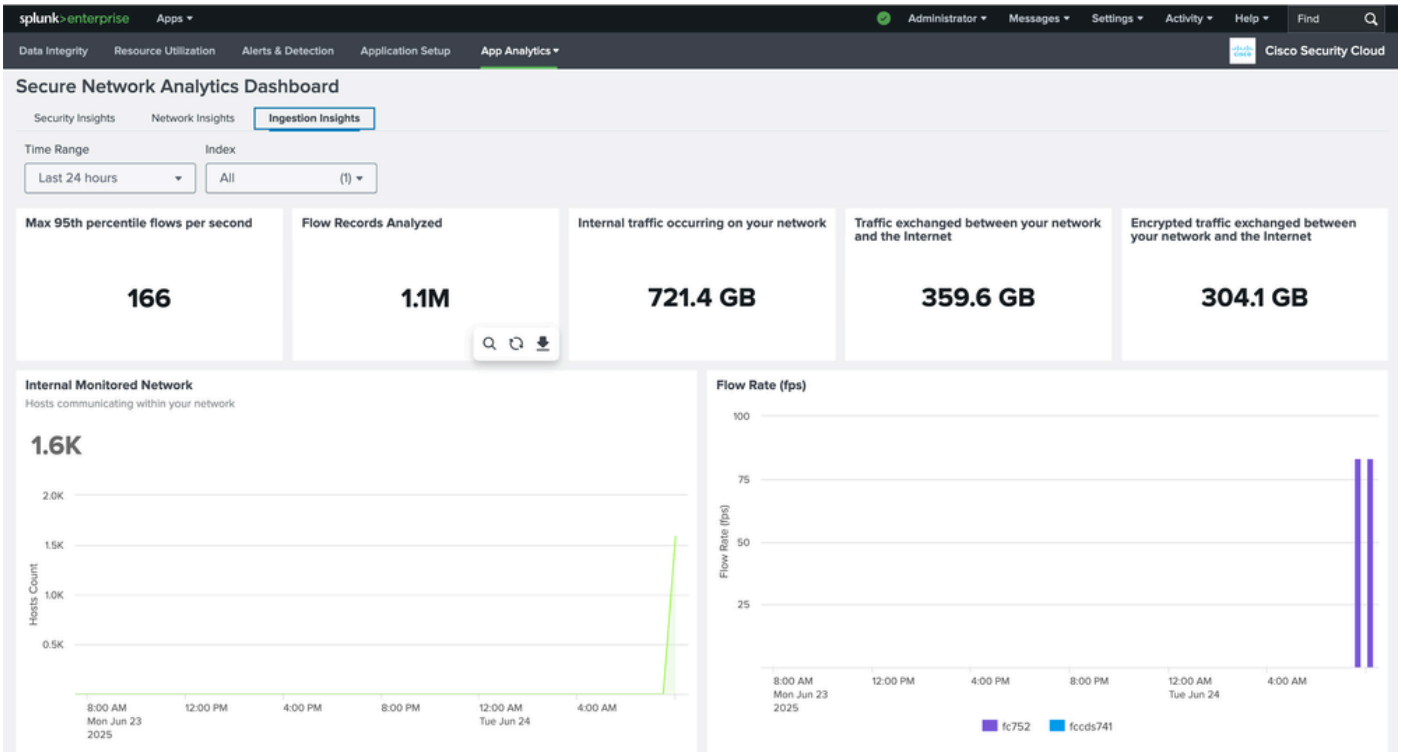
Dit is een belangrijke stap waarbij u moet controleren of de integratie die in de vorige stap is uitgevoerd, al dan niet succesvol is uitgevoerd.

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



ii. Selecteer het Secure Network Analytics Dashboard in de vervolgkeuzelijst en de statistieken beginnen uiteindelijk te reflecteren op het dashboard.





Veelgestelde vragen

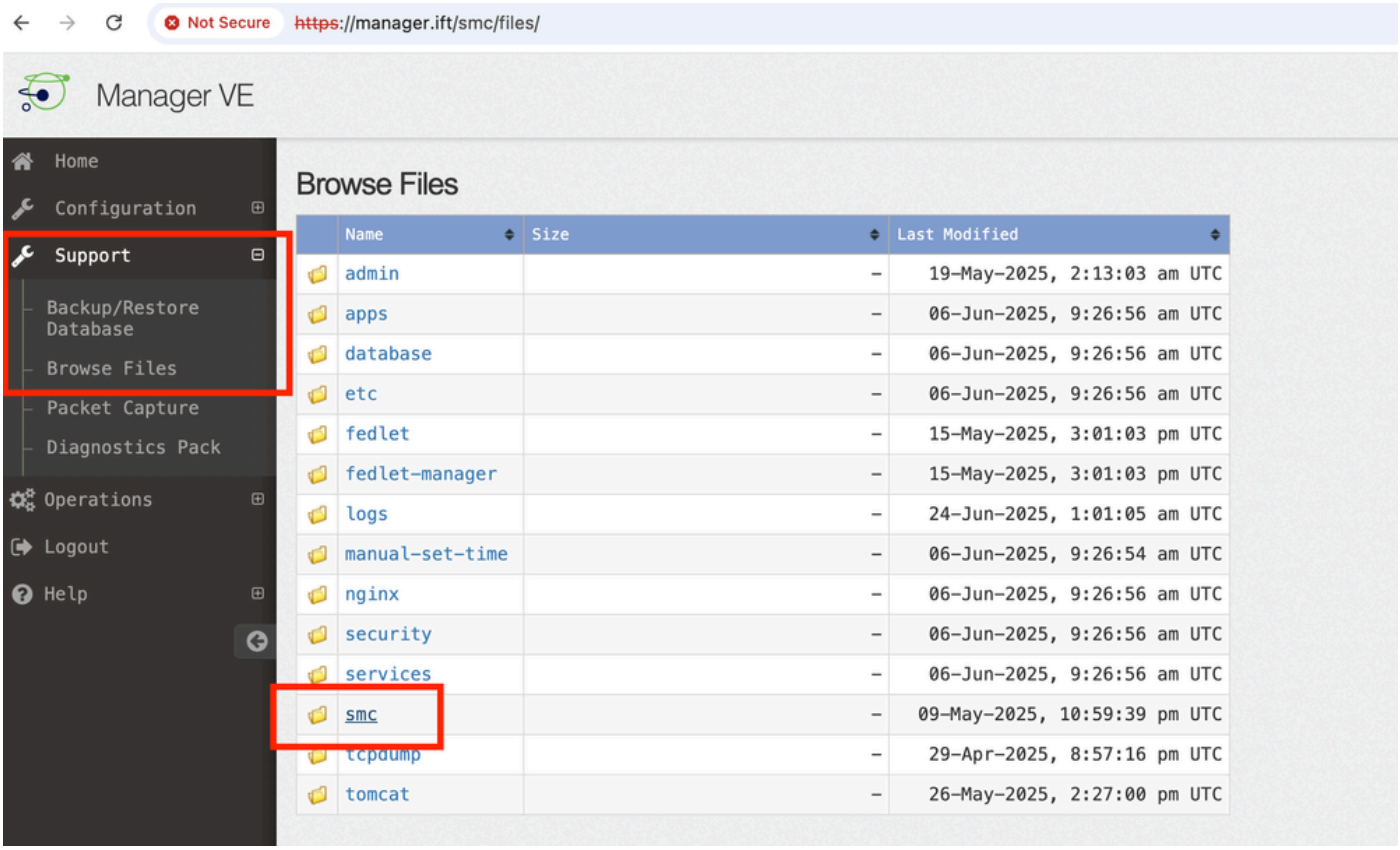
Waar vind je de domein-id voor de SNA-manager?

Antwoord:

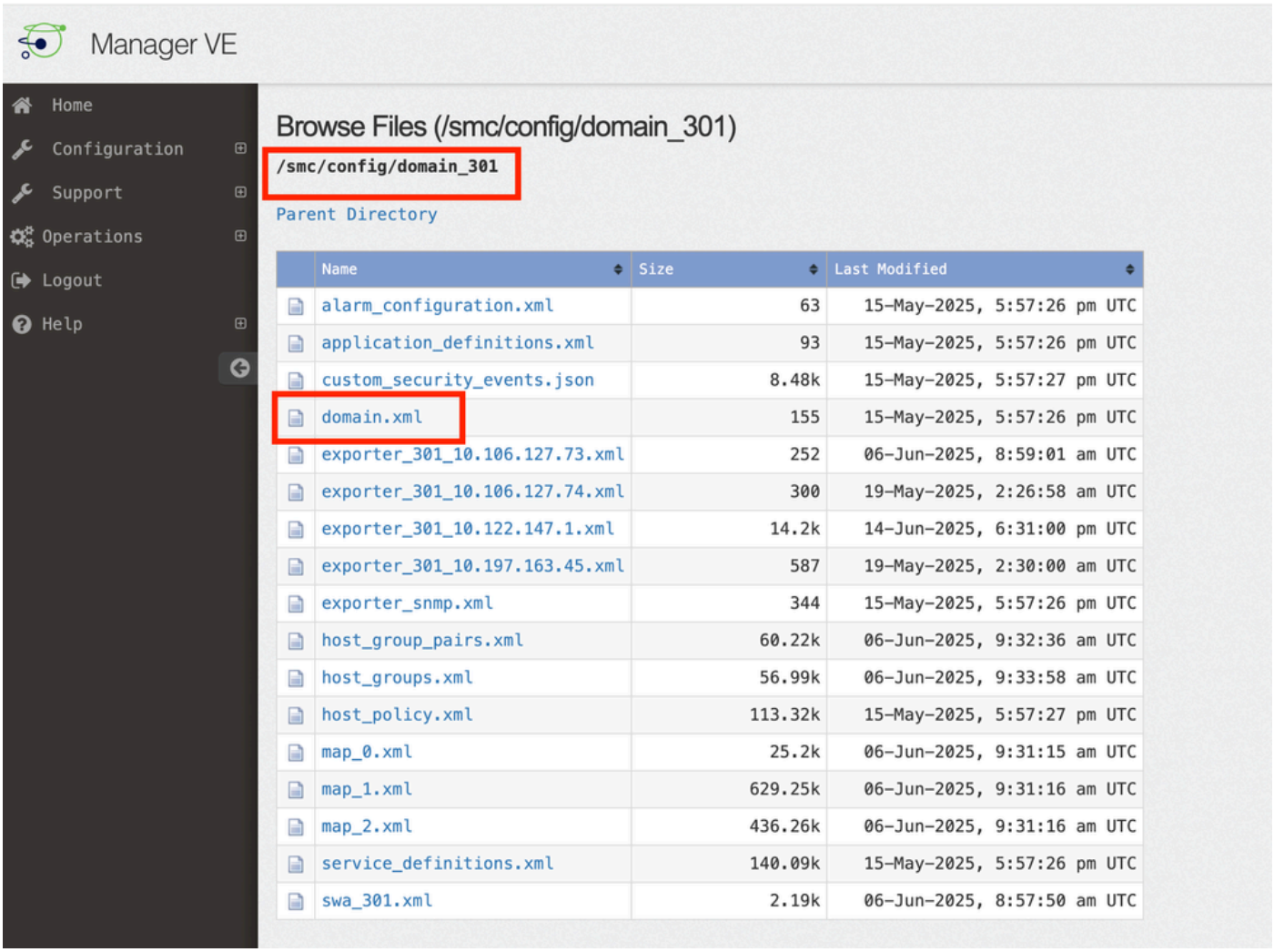
i. Meld u aan bij het primaire SNA-beheer en verwijs naar de pagina Toestelbeheer of de IP Index-

URL van Access Manager.

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



iii. Open het bestand domain.xml dat beschikbaar is in de map domain_XXX onder de map 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

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.