Intégration de SNA à Splunk via une application cloud de sécurité

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

FAQ

Introduction

Ce document décrit l'intégration SNA fluide avec Splunk à l'aide de Cisco Security Cloud pour une réponse plus rapide aux incidents pour les menaces identifiées.

Conditions préalables

Connaissances de base sur les périphériques Splunk et Cisco.

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Splunk Enterprise

Secure Network Analytics v7.5.2.

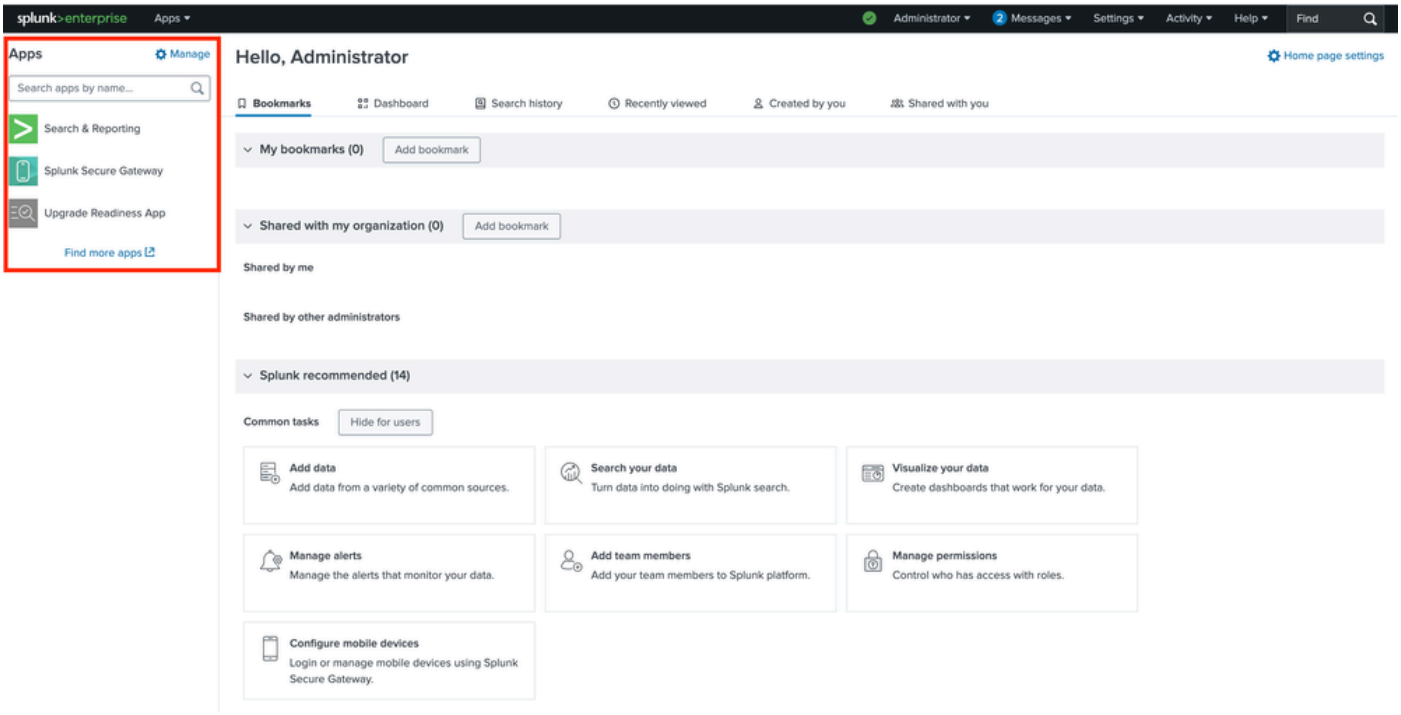
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Étape 1 : Accédez à l'application Splunk et installez l'application Cisco Security Cloud.

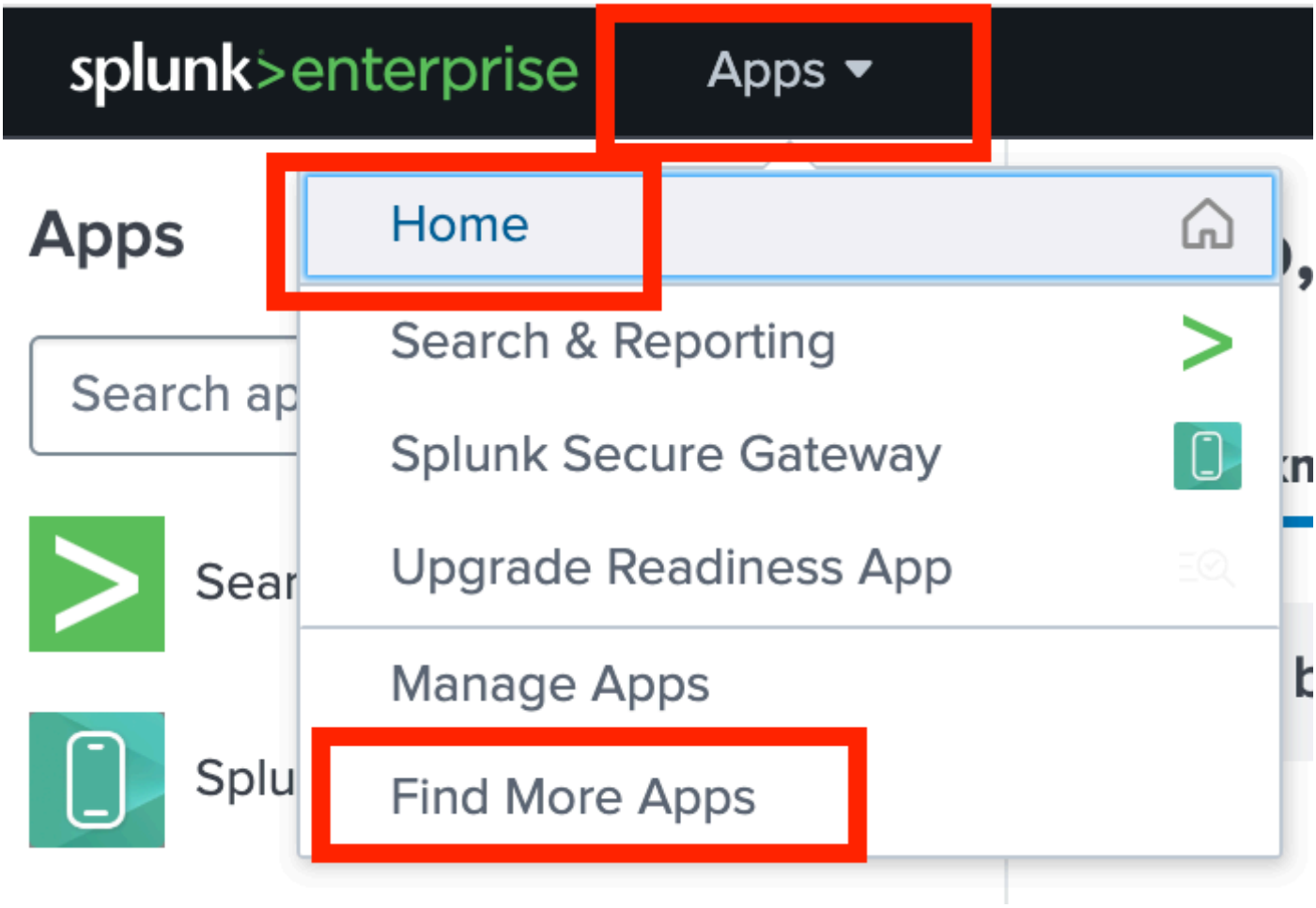
i. Connectez-vous au portail Web Splunk avec les identifiants d'administrateur et, une fois

connecté, la page d'accueil s'affiche avec la liste des applications installées sur le côté gauche sous la section App :

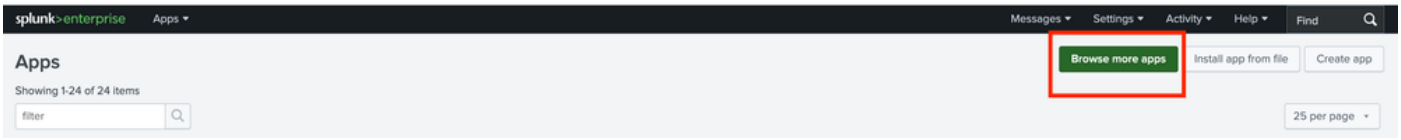


ii. Pour intégrer l'architecture SNA avec Splunk, il est nécessaire d'installer l'application cloud de sécurité Cisco, qui peut être réalisée selon l'une des méthodes mentionnées :

1. Sélectionnez Find More Apps dans la liste déroulante.

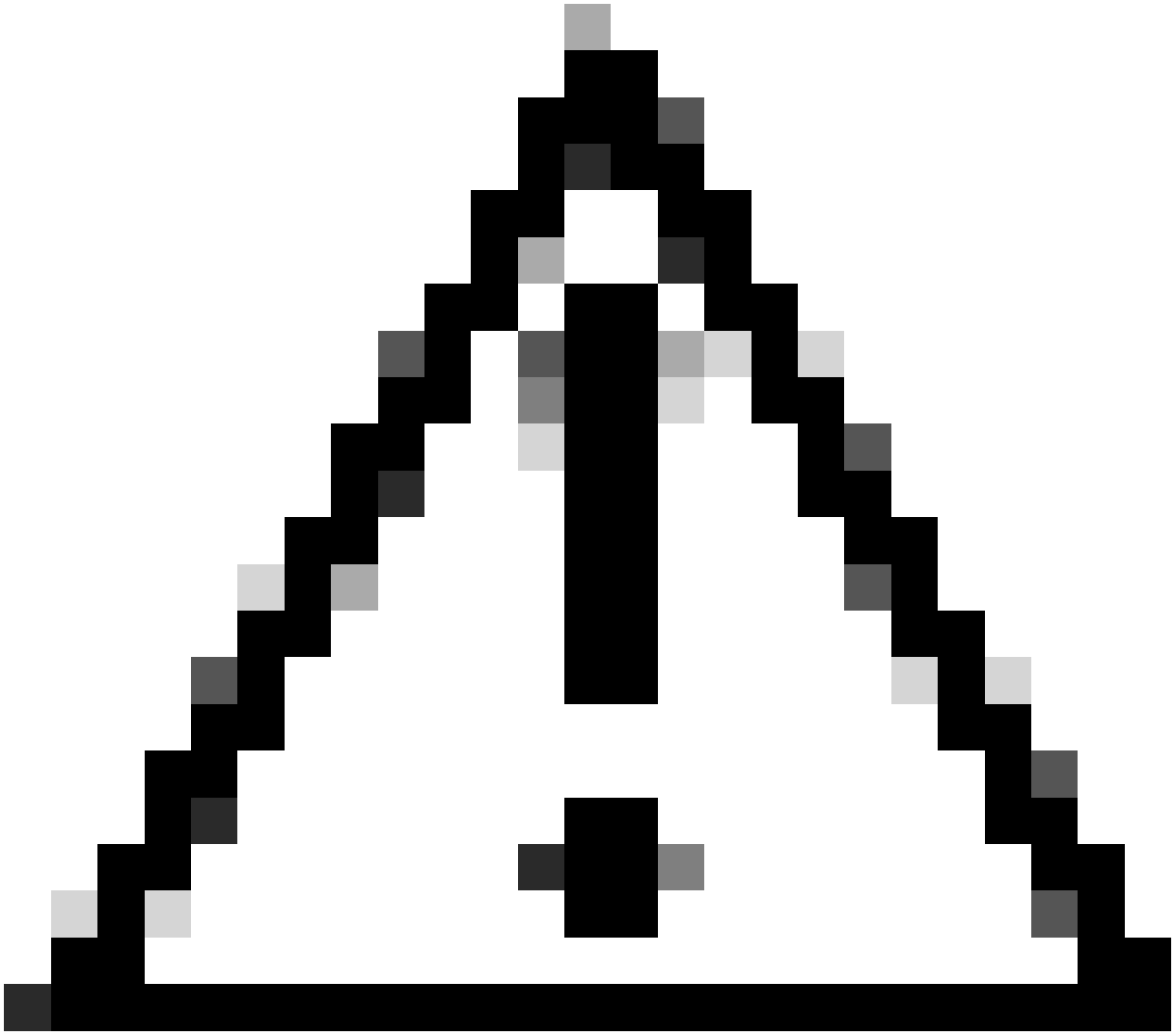


b. Parcourez d'autres applications sous l'icône du pignon Manager.

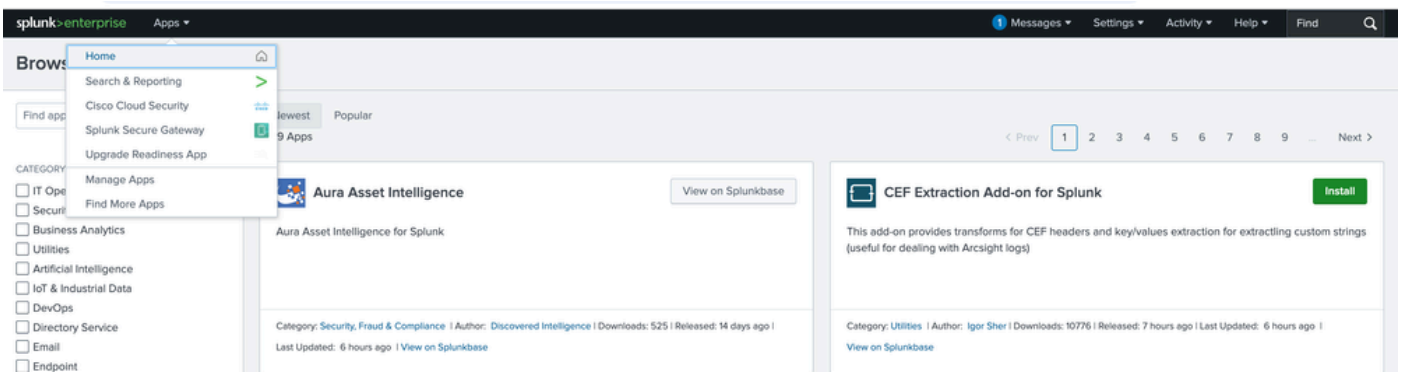


Étape 2 : Installation de l'application cloud de sécurité Cisco.

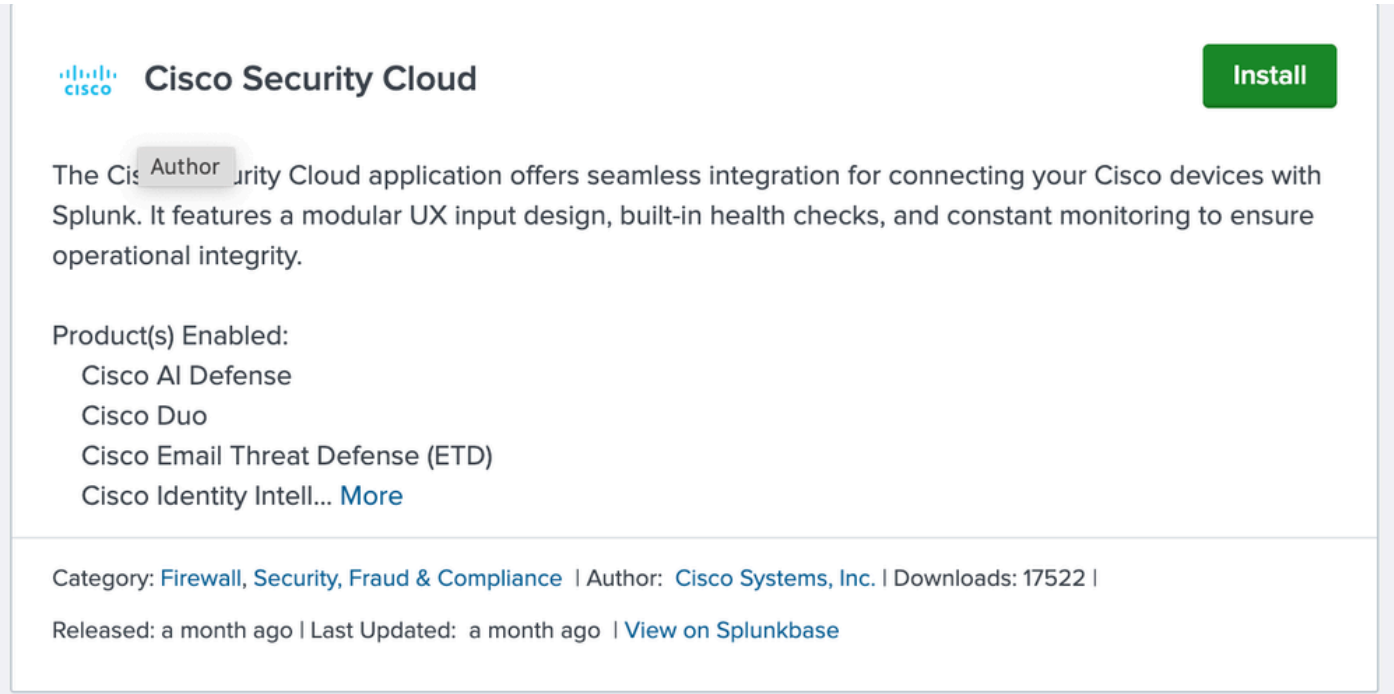
i. Recherchez l'application Cisco Security Cloud. Faites défiler la liste jusqu'à ce que vous trouviez l'application ou recherchez le cloud de sécurité Cisco.



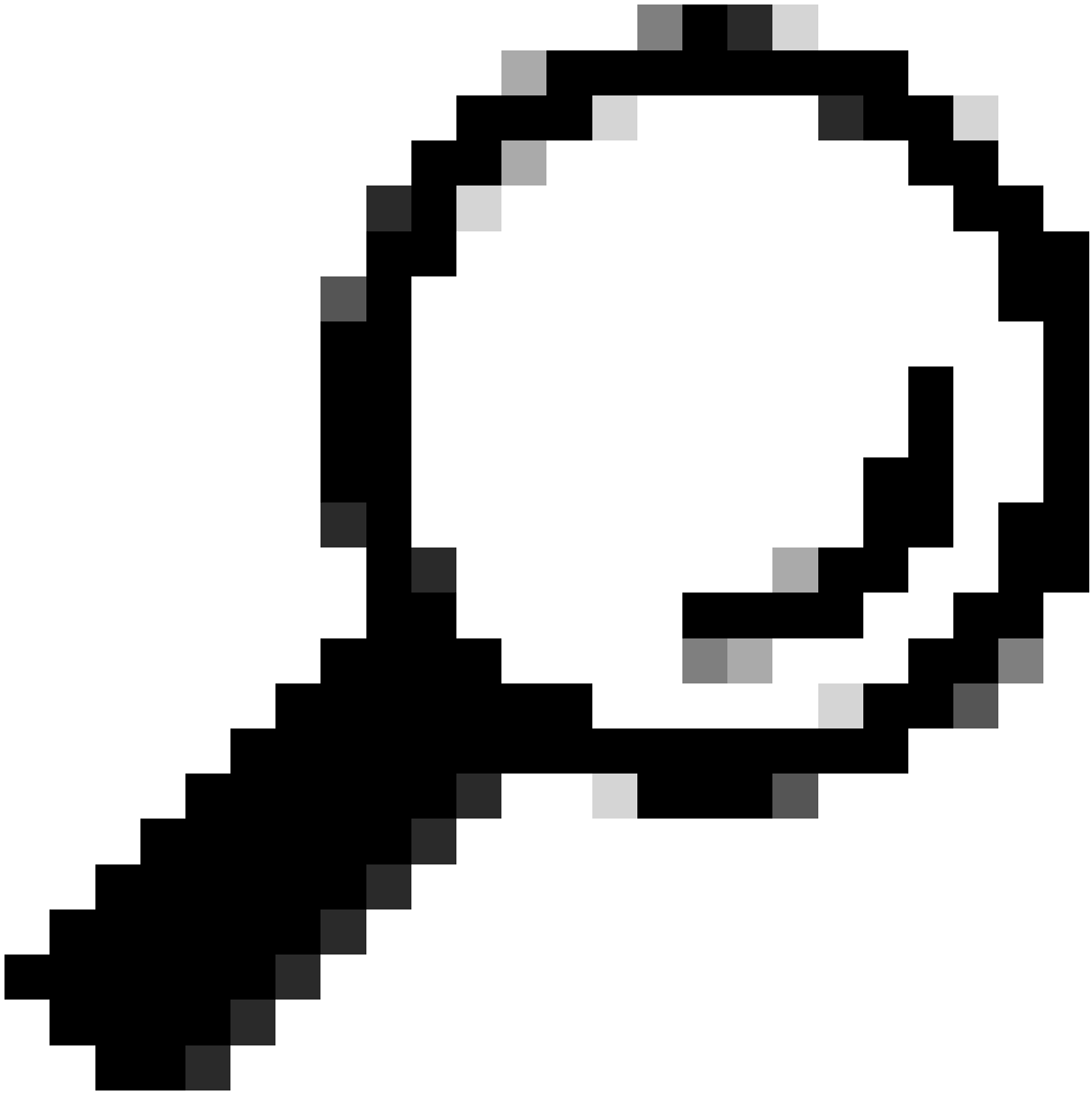
Mise en garde : Ne vous confondez pas avec l'application Cisco Cloud Security.



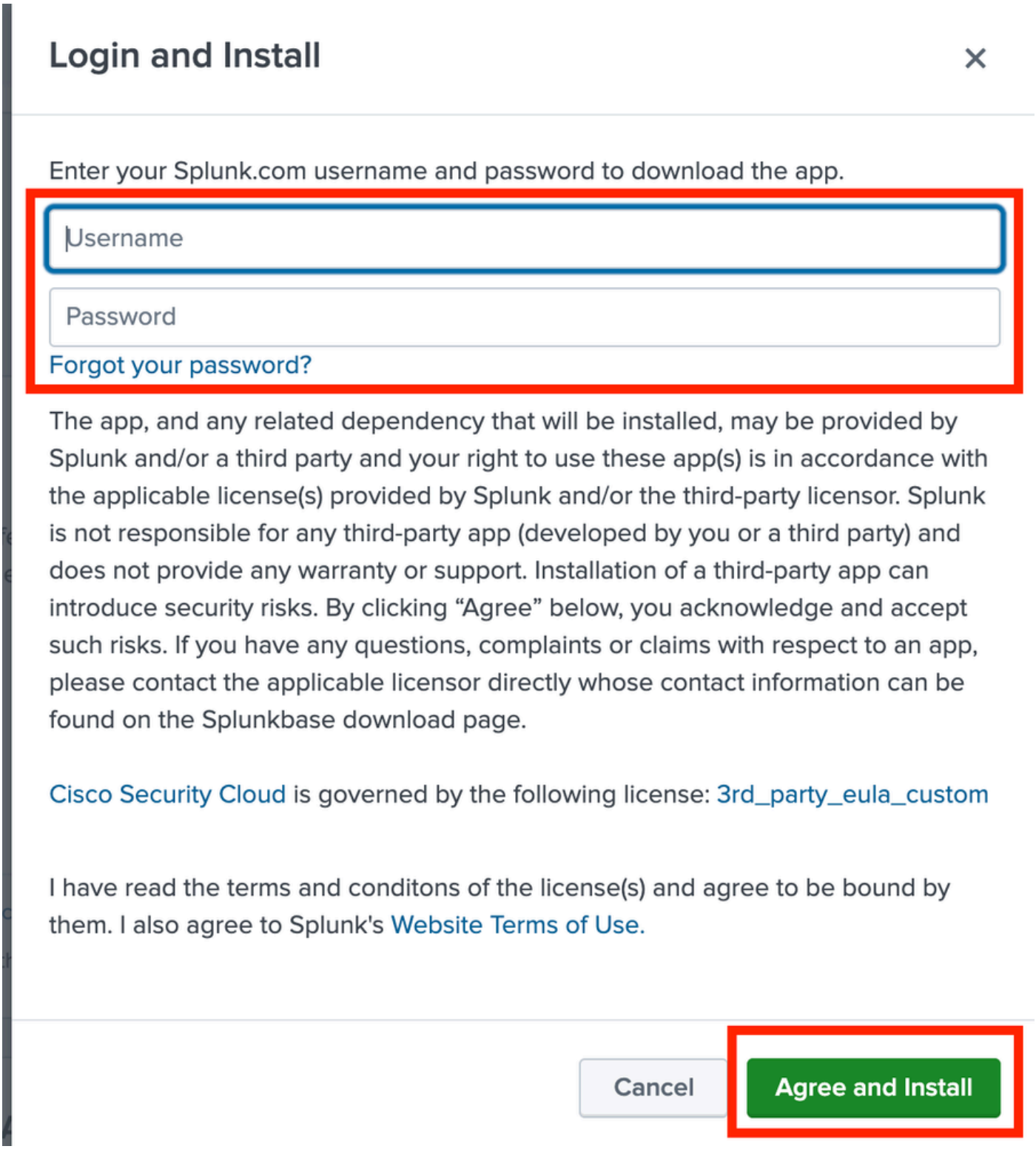
ii. Installez l'application en cliquant sur le bouton Installer.



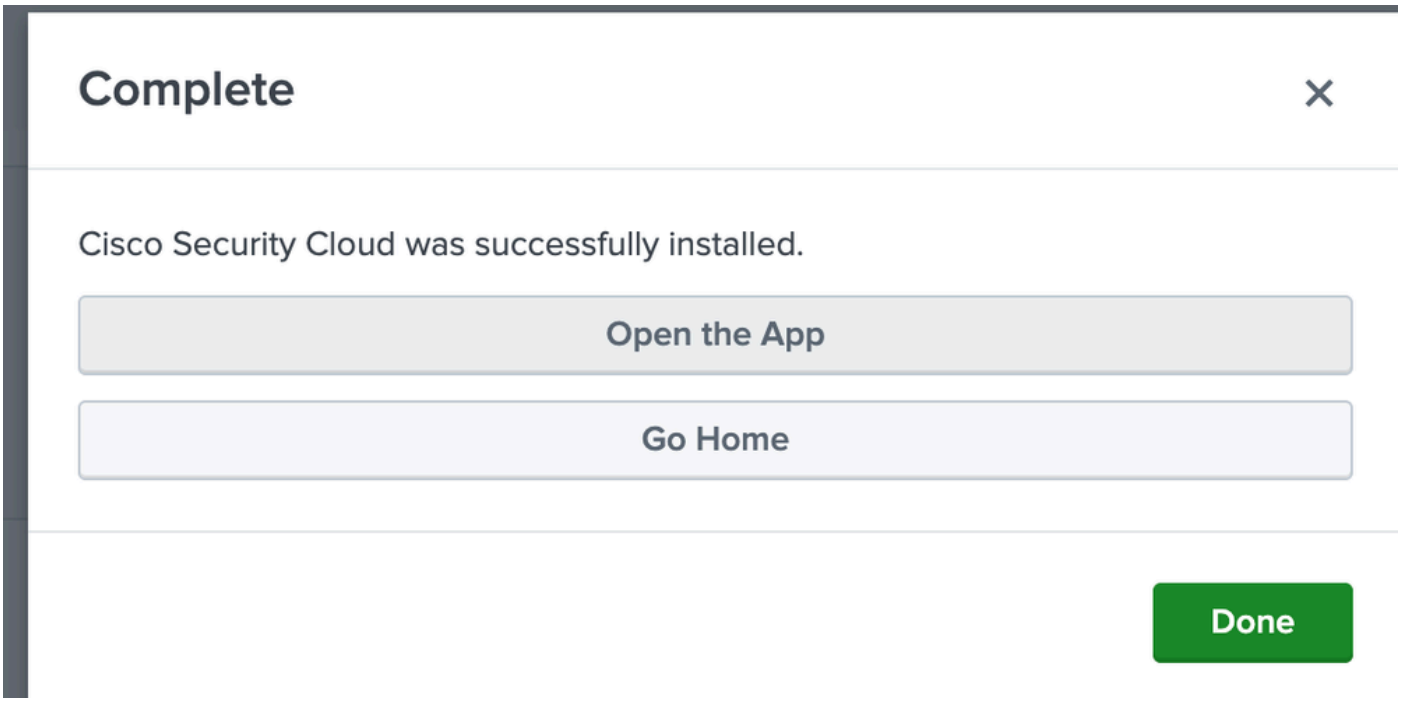
iii. Dès que vous cliquez sur le bouton d'installation, une fenêtre s'affiche pour vous demander les informations d'identification du compte Splunk avant d'installer l'application. Fournissez les informations d'identification et cliquez sur Agree and Install pour continuer.



Conseil : Fournissez les informations d'identification utilisées pour accéder au portail Splunk, et non les informations d'identification d'administrateur utilisées pour l'application d'entreprise Splunk lors de la connexion.

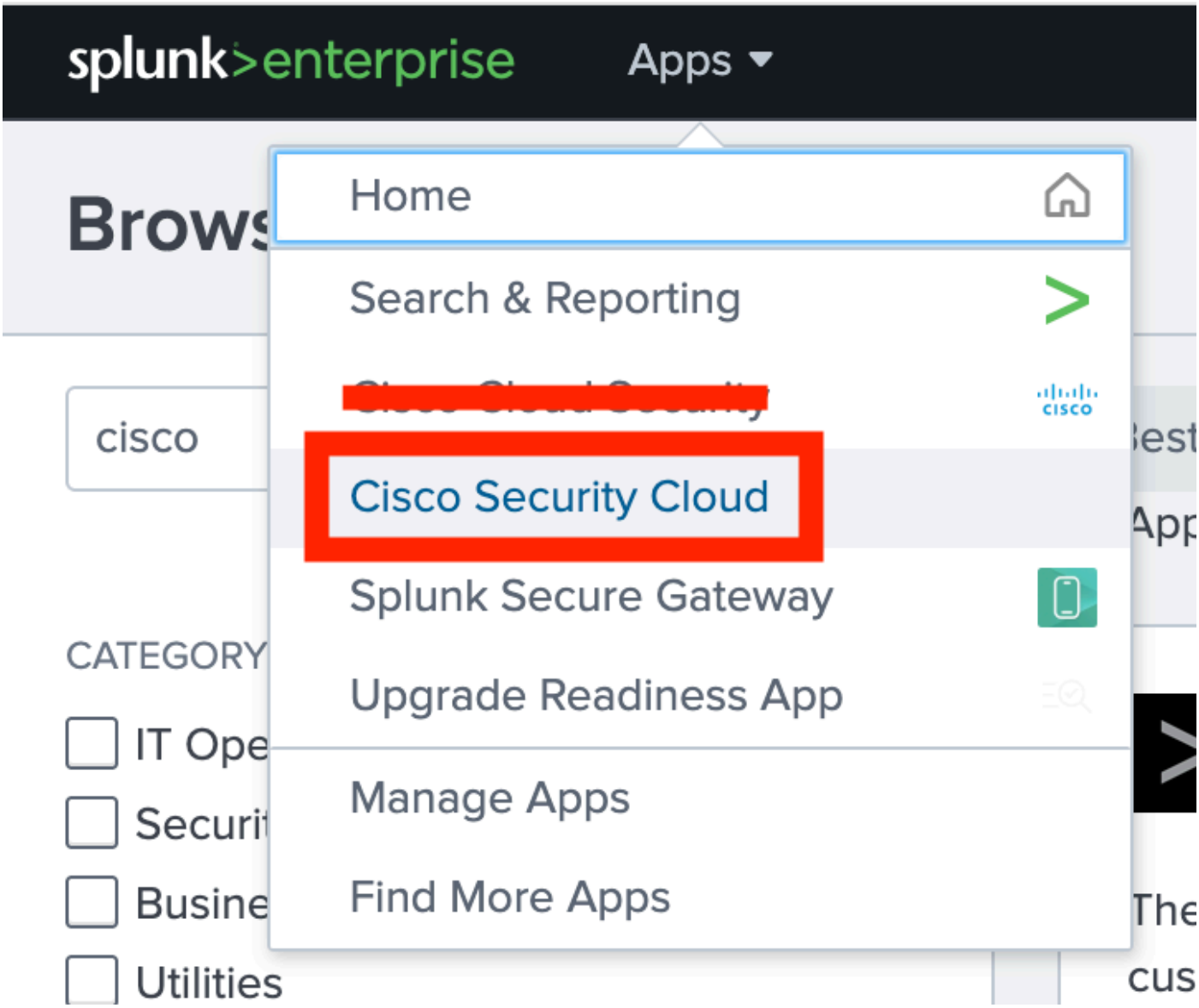


iv. Un message s'affiche lorsque l'installation de l'application a réussi, comme illustré. Cliquez sur Done.

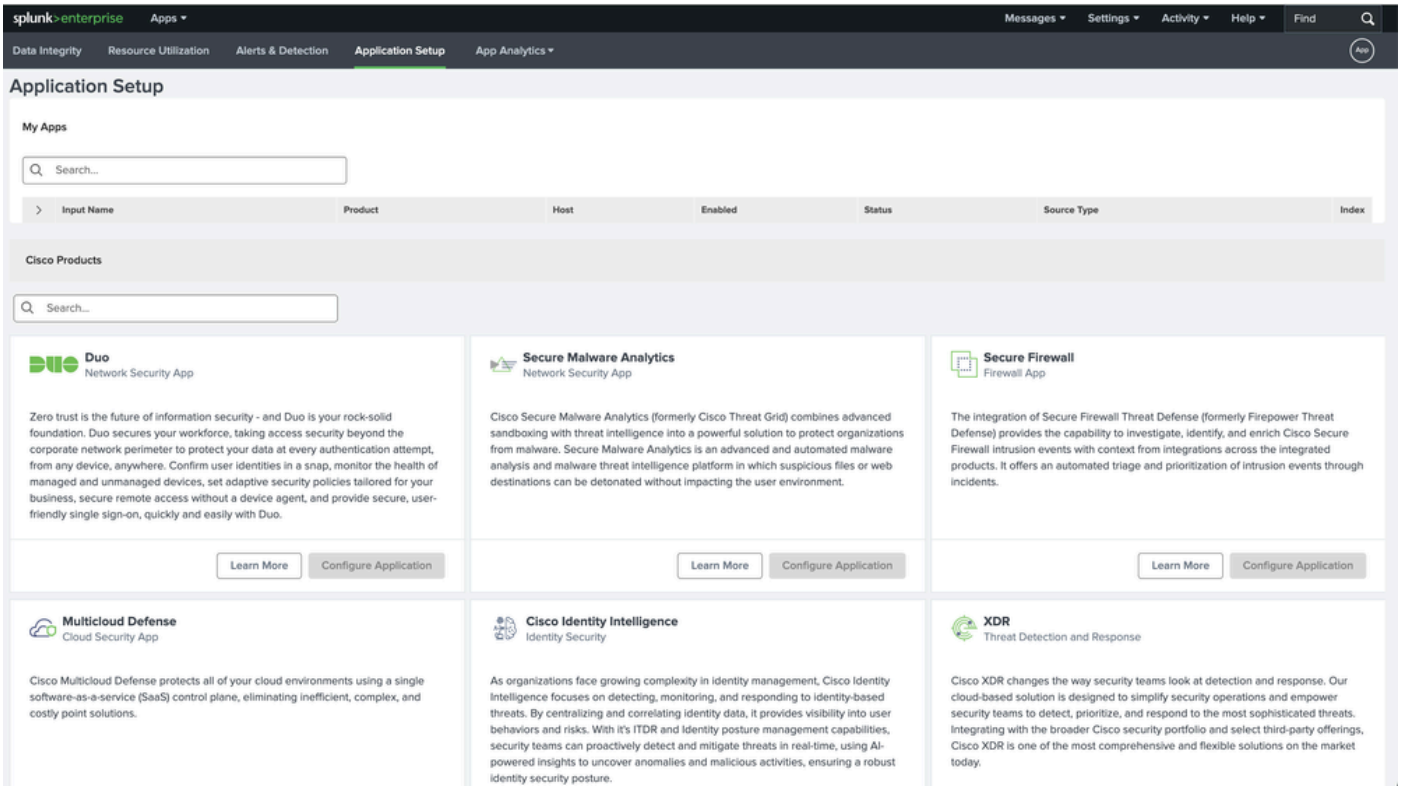


Étape 3 : Vérification de l'installation de l'application cloud de sécurité Cisco.

i. Cliquez sur l'option Apps déroulante, et maintenant l'application peut être vu dans la liste après l'installation réussie :



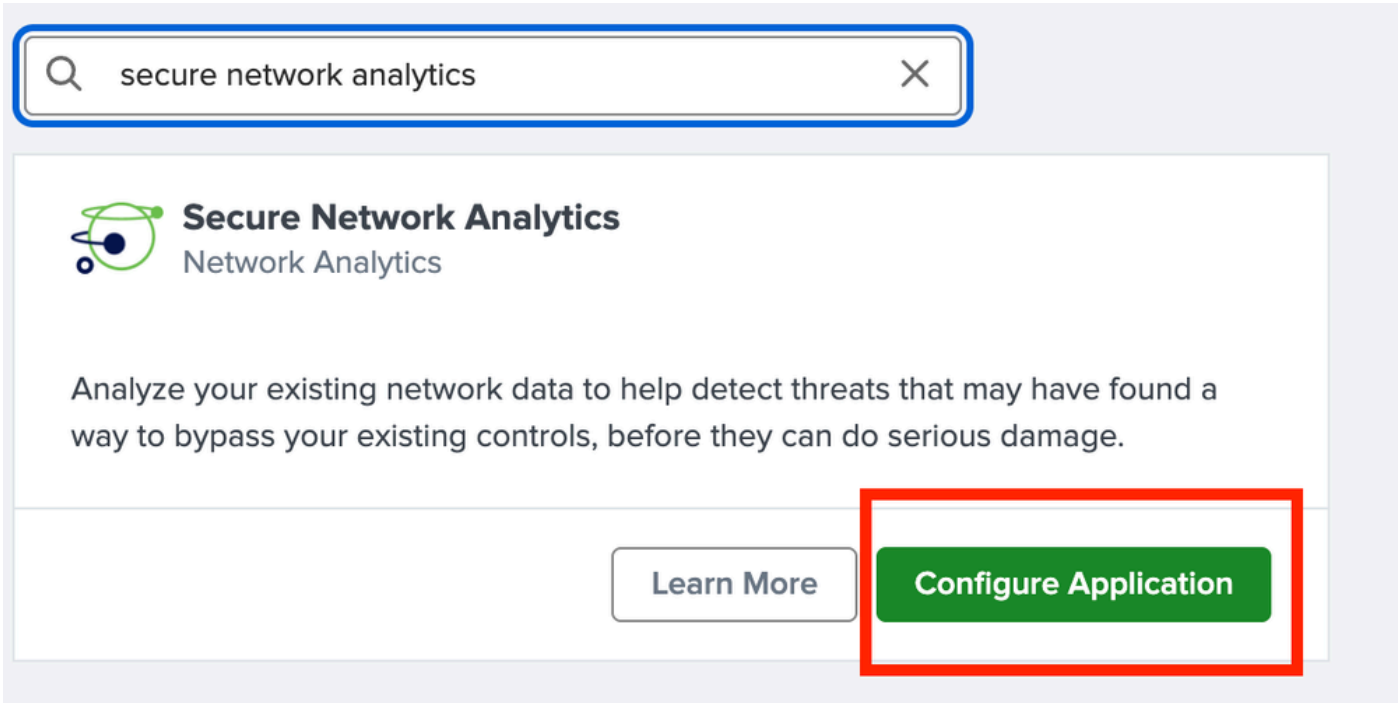
ii. Sélectionnez Cisco Security Cloud en cliquant dessus. Vous êtes redirigé vers la page Application Setup où tous les produits de sécurité Cisco Cloud disponibles peuvent être trouvés.



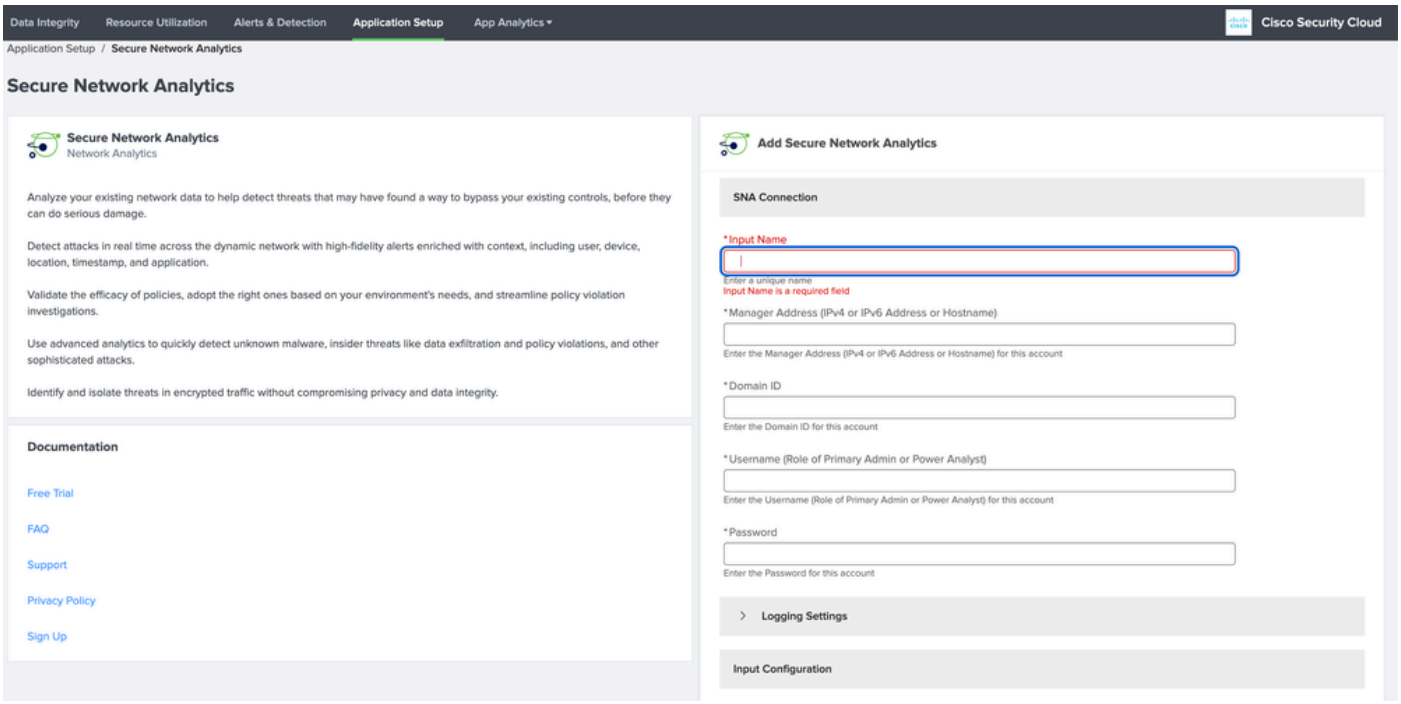
Étape 4 : Intégration à Secure Network Analytics (SNA).

L'objectif de ce document est de mettre en évidence les étapes d'installation du Splunk avec Secure Network Analytics (SNA) mentionnées plus loin.

i. Recherchez Secure Network Analytics et, lorsqu'il apparaît, sélectionnez Configure Application:

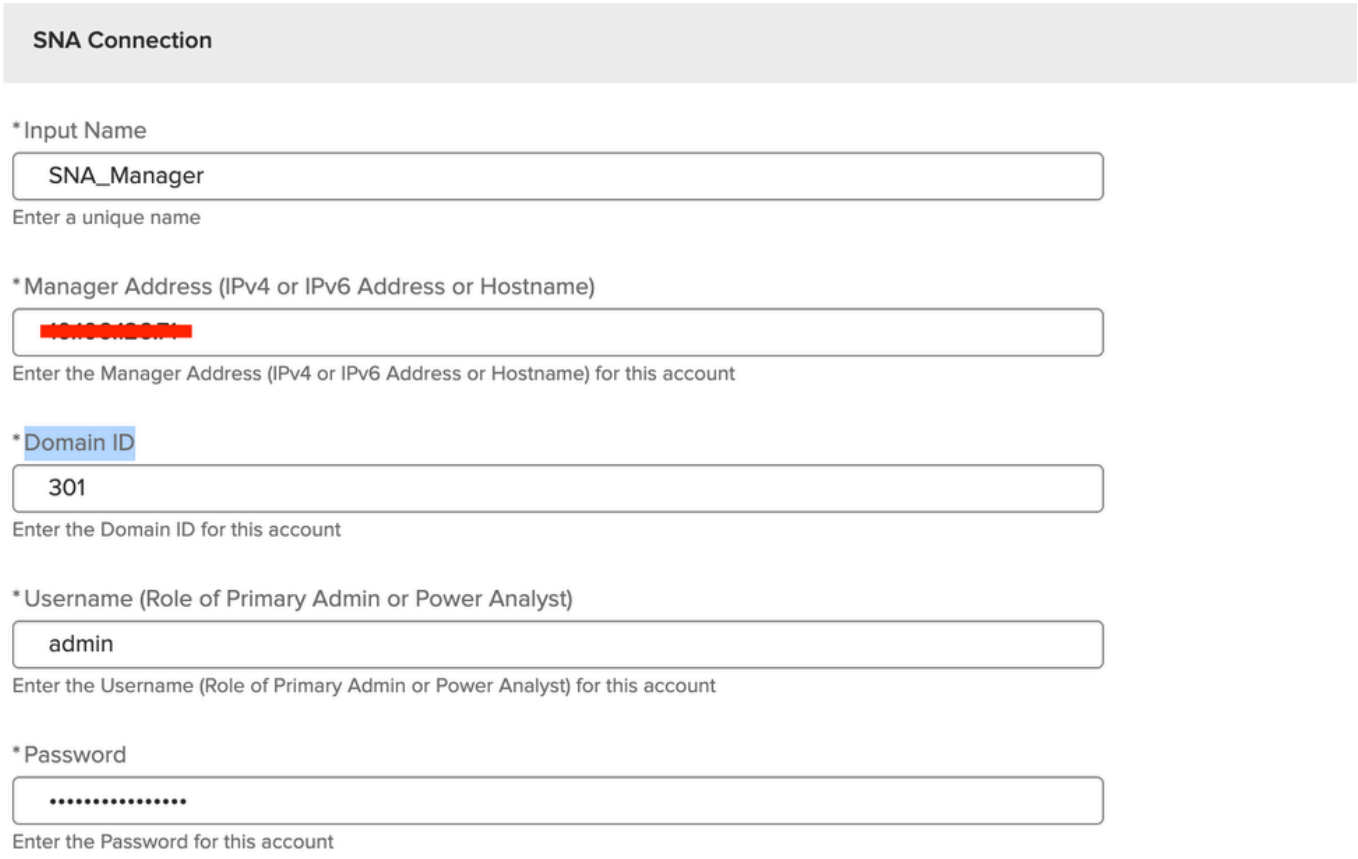


ii. Lorsque vous sélectionnez l'option configure, la page de configuration des détails à ajouter apparaît.

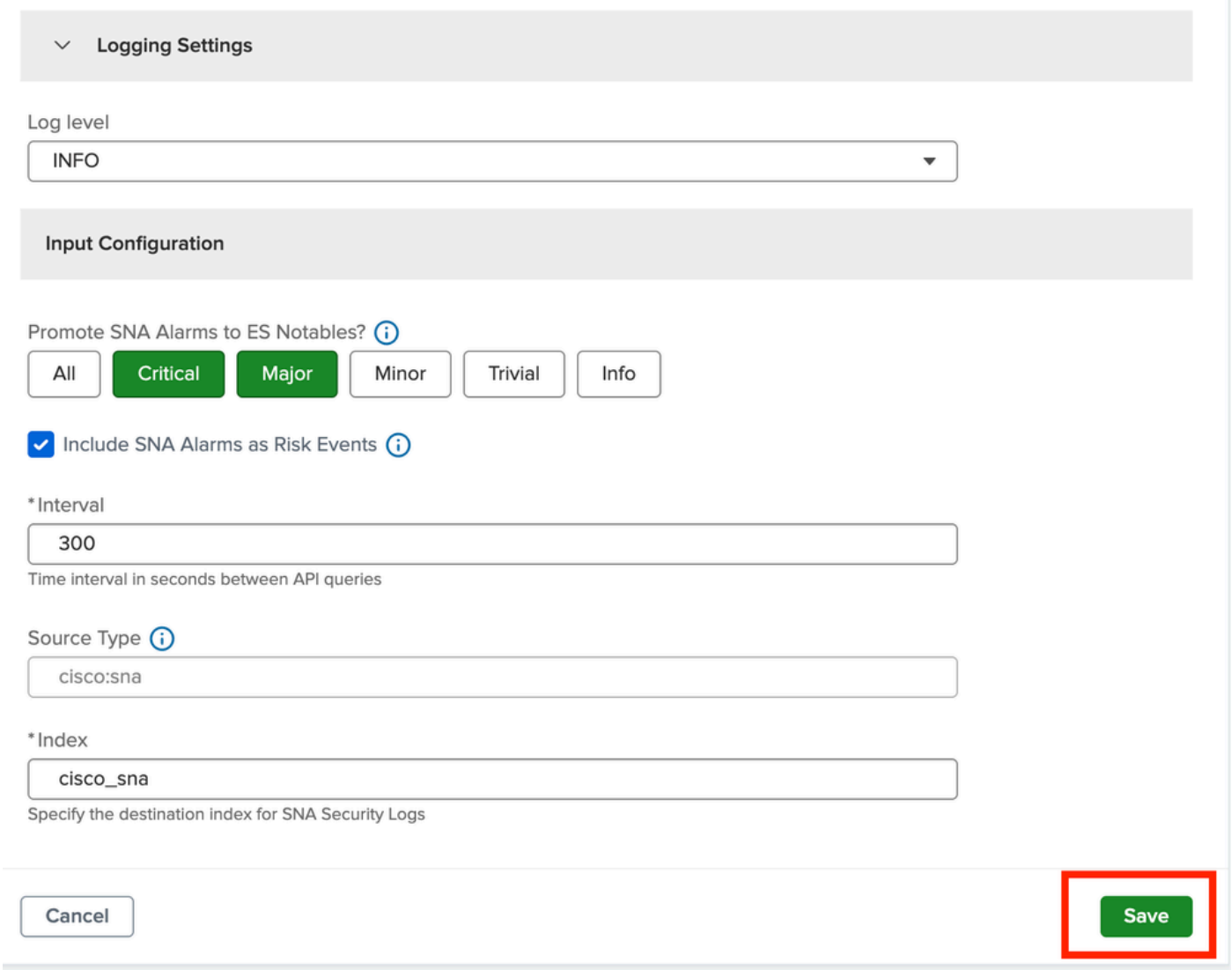


iii. Renseignez tous les détails obligatoires mentionnés pour les détails de la connexion SNA :

1. Nom d'entrée : tout nom unique pour SNA
2. Adresse du responsable (adresse IPv4 ou IPv6 ou nom d'hôte) : IP de gestion du SNA Manager principal
3. Domain ID : saisissez la valeur par rapport à domain_ID (par exemple 301)
4. username (nom d'utilisateur) : Le nom d'utilisateur du gestionnaire principal (par exemple admin)
5. Mot de passe : Mot de passe de l'utilisateur du gestionnaire principal



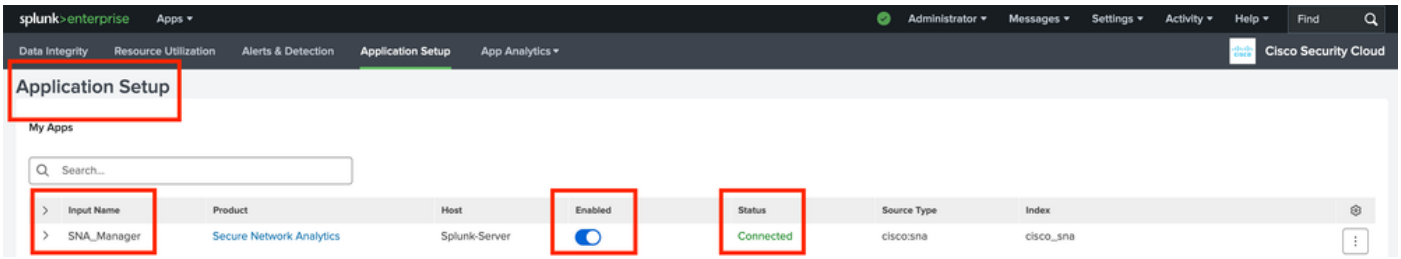
iv. Conservez les valeurs par défaut des paramètres restants ou modifiez-les si nécessaire, puis cliquez sur Enregistrer. Un message de réussite s'affiche à l'écran une fois l'opération terminée.



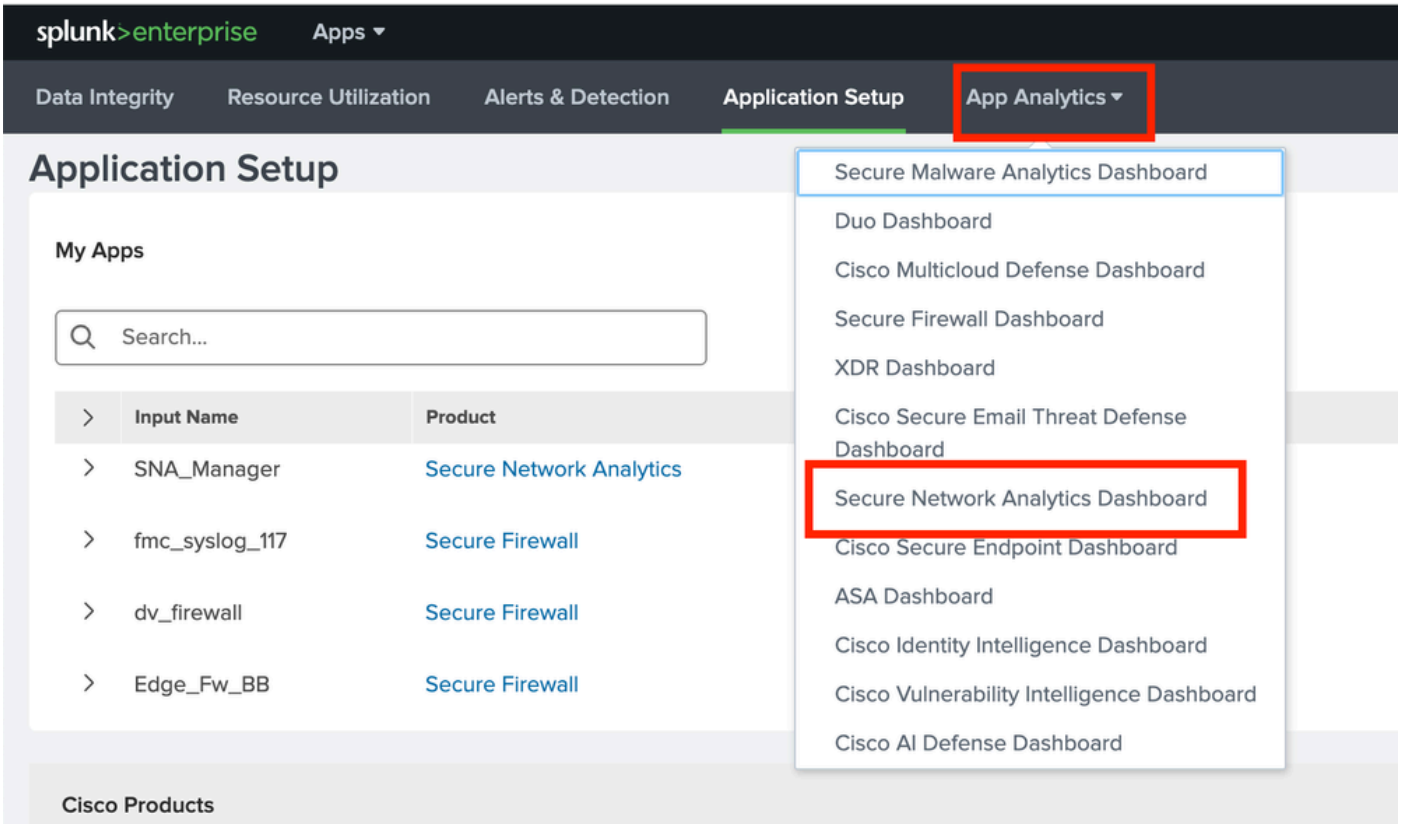
Étape 5 : Vérification de l'intégration.

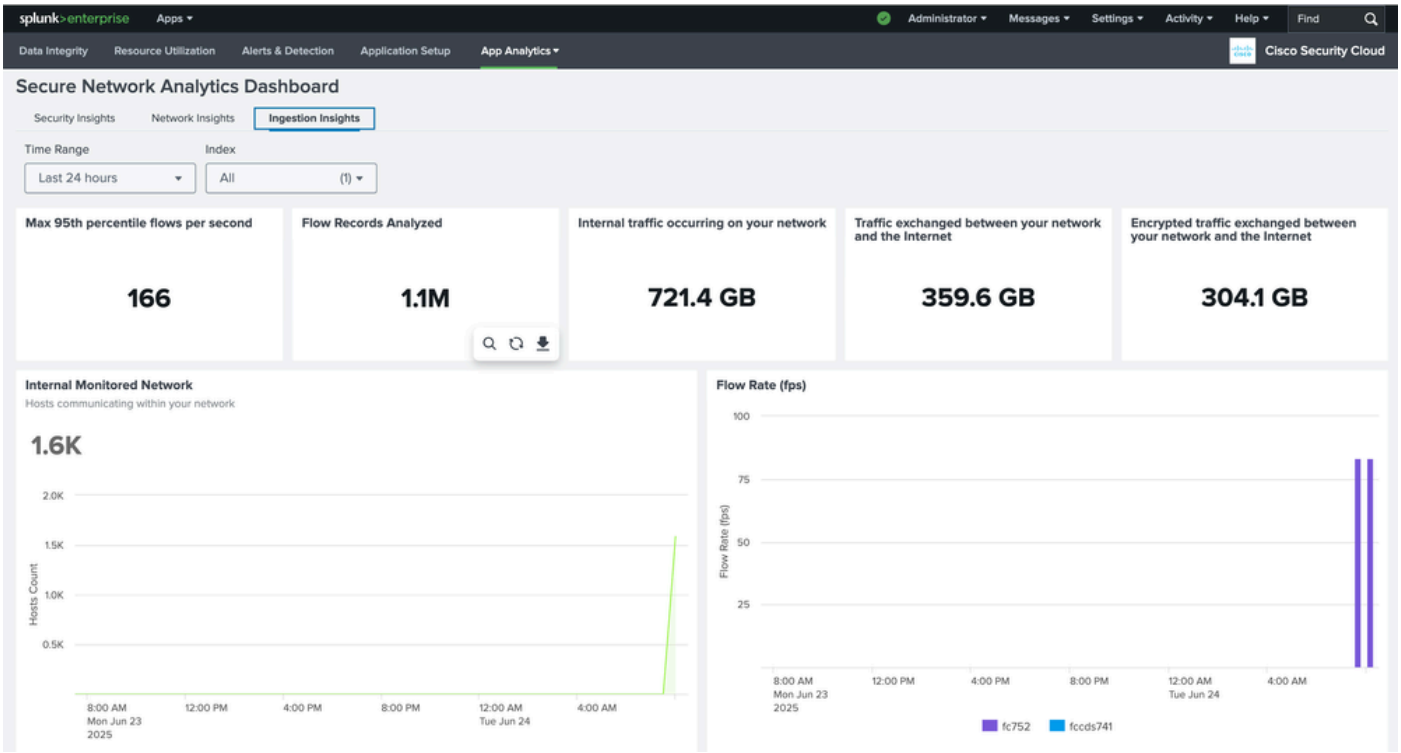
Il s'agit d'une étape importante au cours de laquelle vous devez vérifier si l'intégration exécutée à l'étape précédente s'est déroulée correctement ou non.

i. L'état de connexion pour l'entrée doit être Connected dans l'onglet Application Setup avec la valeur par défaut Enabled pour le nom correct dans le champ Input.



ii. Sélectionnez le tableau de bord Secure Network Analytics dans la liste déroulante, et les statistiques commencent éventuellement à réfléchir sur le tableau de bord.





FAQ

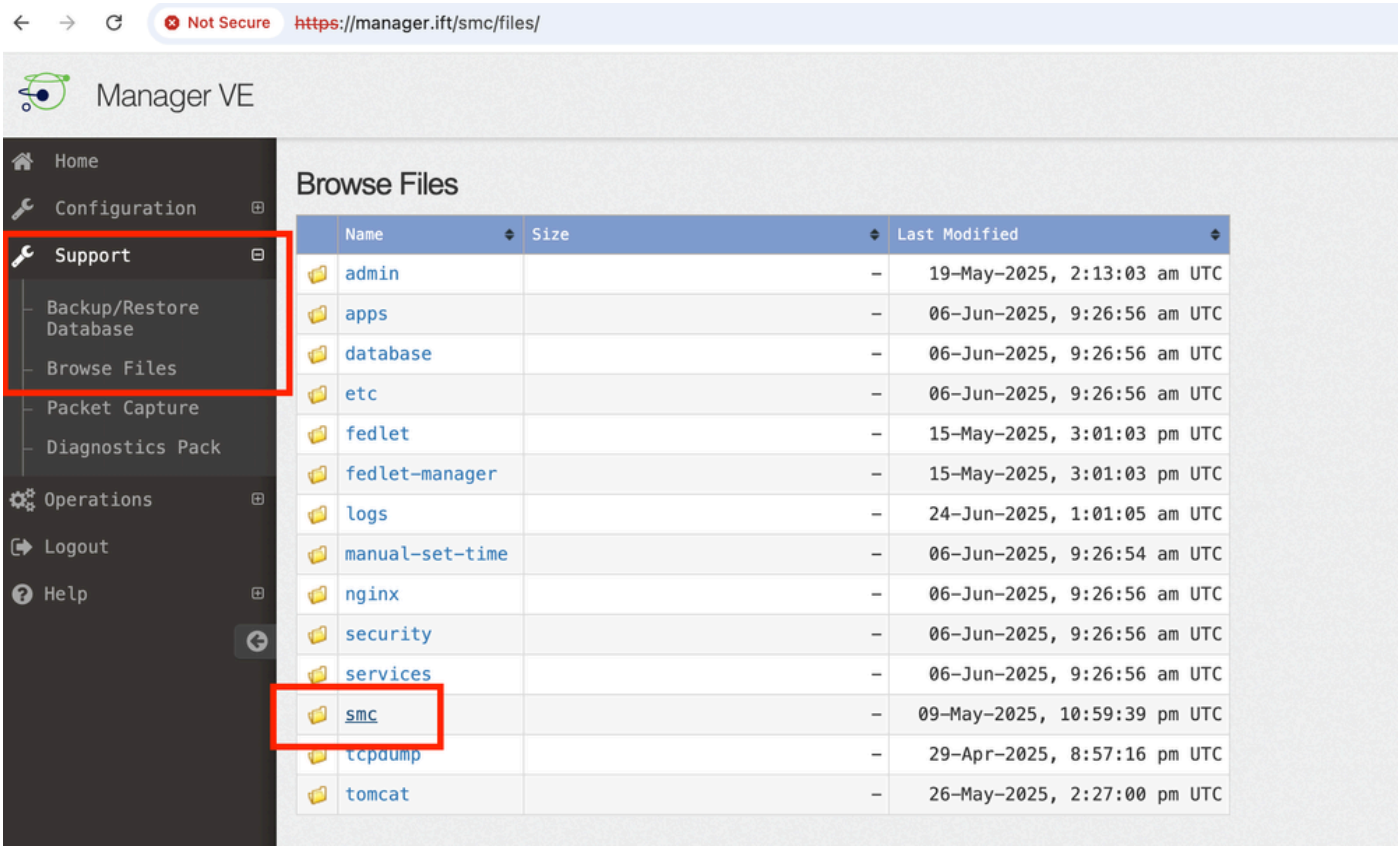
Où trouver l'ID de domaine du gestionnaire SNA ?

Réponse :

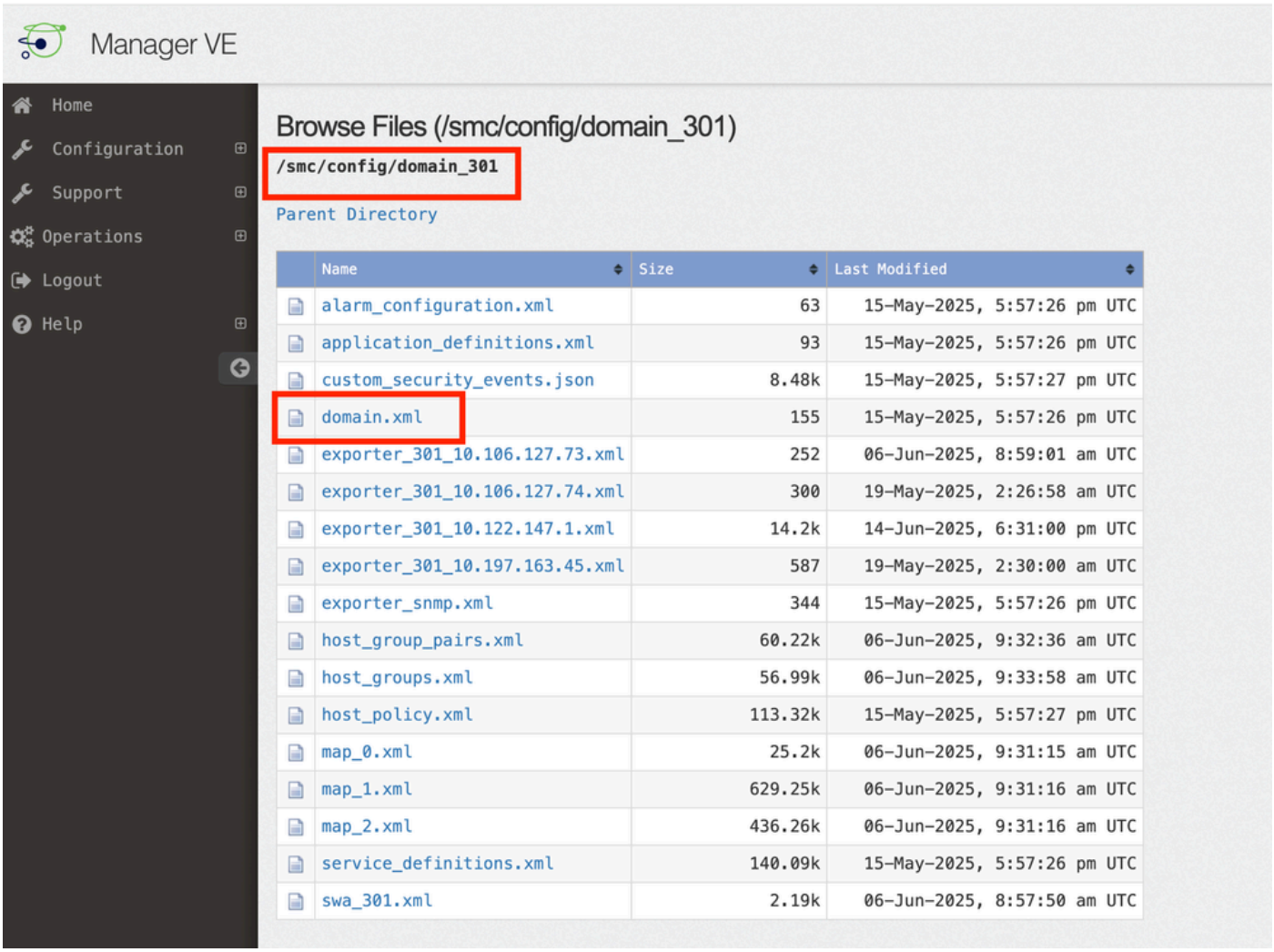
i. Connectez-vous au gestionnaire principal SNA et redirigez-vous vers la page Appliance

administrator ou accédez à l'URL IP Index du gestionnaire.

ii. Parcourez le dossier smc sous la section Support.



iii. Ouvrez le fichier domain.xml disponible dans le dossier domain_XXX sous le dossier 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.