

Integre a SNA ao Splunk usando o aplicativo de nuvem de segurança

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Perguntas freqüentes](#)

Introdução

Este documento descreve a integração perfeita do SNA com o Splunk usando o Cisco Security Cloud para uma resposta mais rápida a incidentes para as ameaças identificadas.

Pré-requisitos

Conhecimento básico do Splunk e dos dispositivos da Cisco.

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

Empresa Splunk

Análise de rede segura v7.5.2.

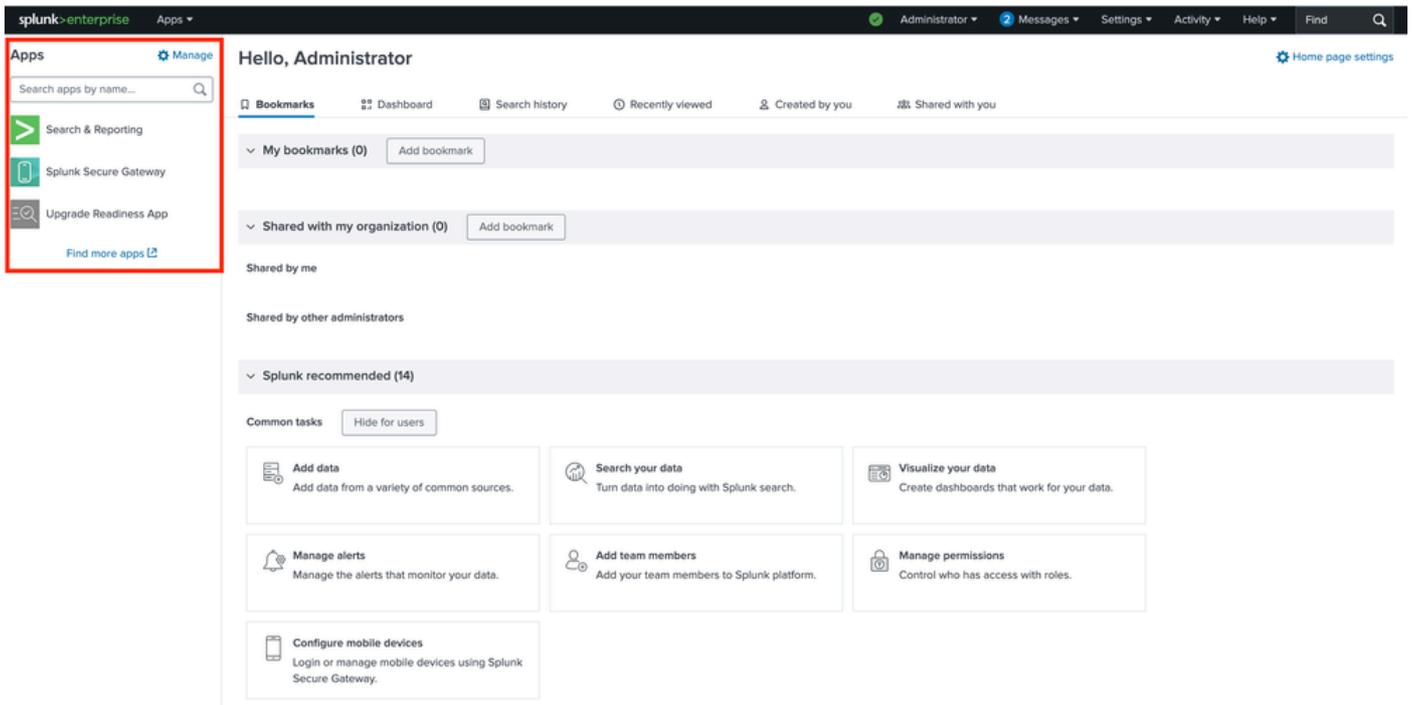
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa1: Acesse o aplicativo Splunk e instale o aplicativo Cisco Security Cloud.

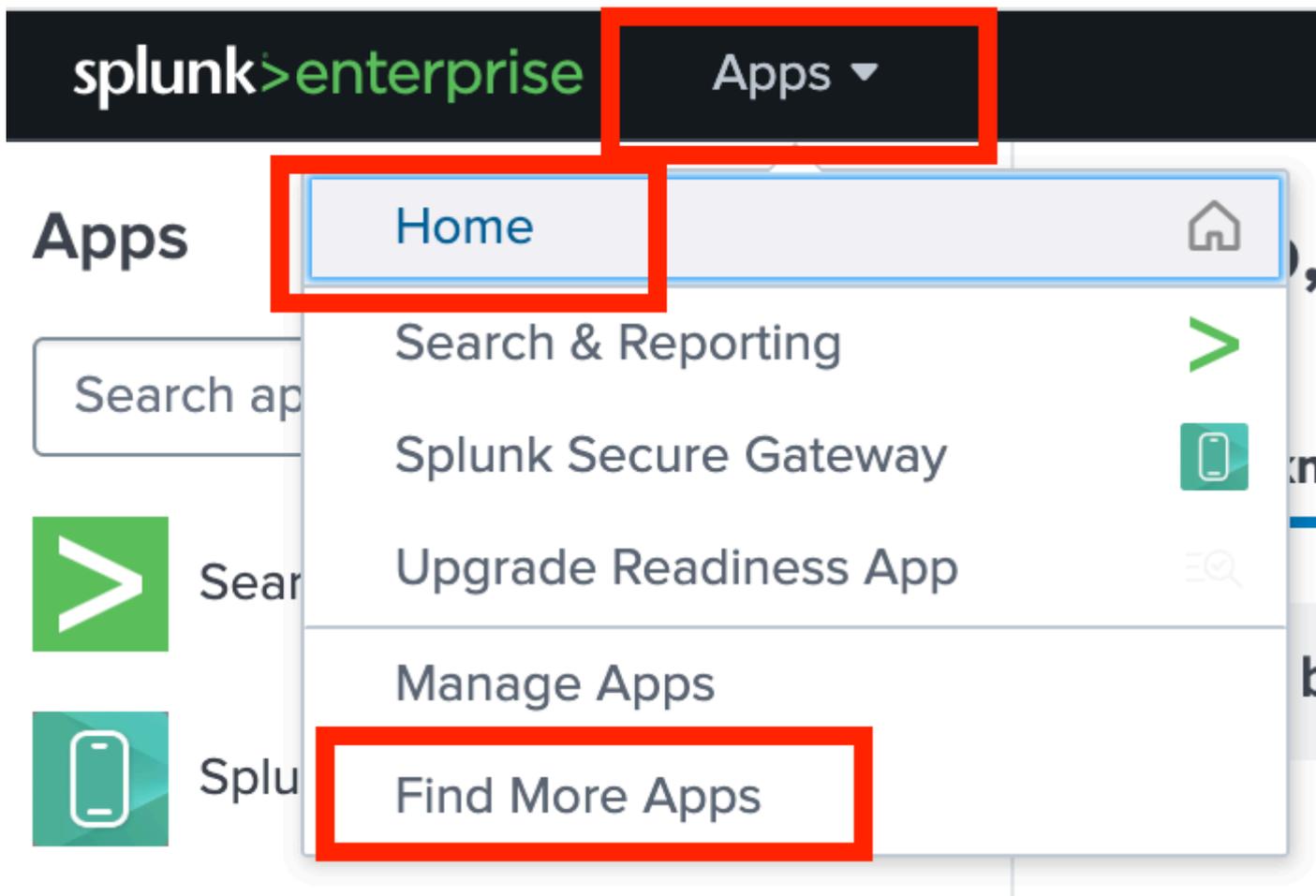
i. Faça login no portal da Web Splunk com as credenciais de administrador e, em um login bem-

sucedido, a página inicial pode ser vista com a lista de aplicativos instalados no lado esquerdo na seção App:

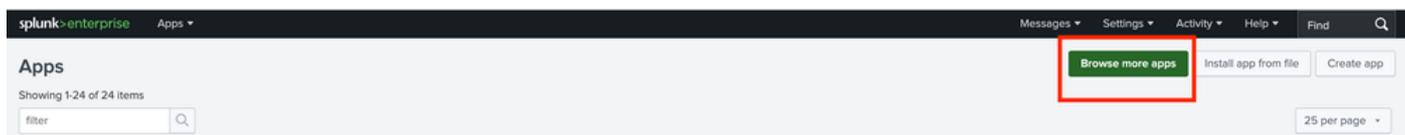


ii) Para integrar o SNA com o Splunk, é necessário instalar o Cisco Security Cloud Application, que pode ser obtido em qualquer um dos métodos mencionados:

1. Selecione Find More Apps no menu suspenso.

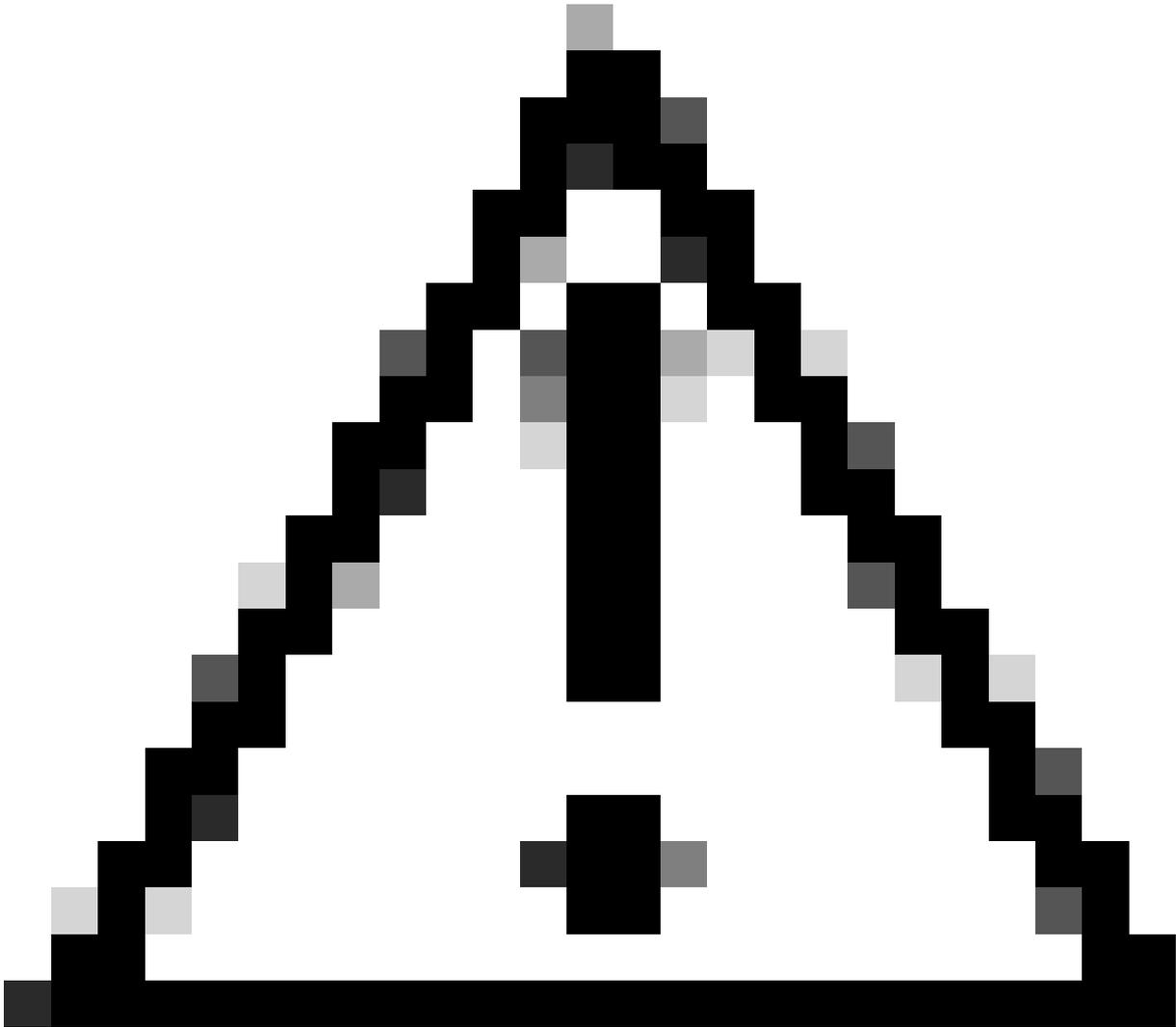


b. Procure mais aplicativos sob o ícone de equipamento Gerenciador.

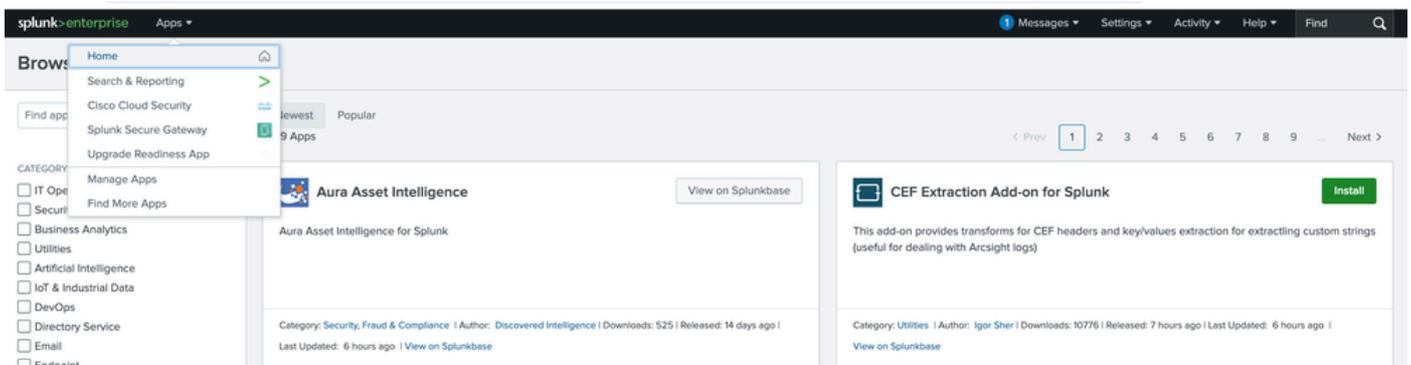


Passo 2: Instalação do Cisco Security Cloud Application.

i. Procure o Cisco Security Cloud Application. Agora, role para baixo até encontrar o aplicativo ou pesquise a nuvem de segurança da Cisco.



Caution: Não se confunda com o Cisco Cloud Security App.



ii) Instale o aplicativo clicando no botão Instalar.



Cisco Security Cloud

[Install](#)

The Cisco 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) No momento em que você clica no botão de instalação, uma janela aparece solicitando as credenciais da conta Splunk antes de instalar o aplicativo. Forneça as credenciais e clique em Concordo e instalar para continuar.



Tip: Forneça as credenciais usadas para acessar o portal Splunk, não as credenciais de administrador usadas para o aplicativo empresarial Splunk durante o logon.

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 conditions of the license(s) and agree to be bound by them. I also agree to Splunk's [Website Terms of Use](#).

iv) Uma mensagem é exibida sobre a instalação bem-sucedida do aplicativo conforme descrito. Clique em Concluído.

Complete



Cisco Security Cloud was successfully installed.

Open the App

Go Home

Done

Passo 3: Verificação da instalação do aplicativo de nuvem de segurança da Cisco.

i. Clique na opção suspensa Apps e agora o aplicativo poderá ser visto na lista após a instalação bem-sucedida:

Browse

cisco

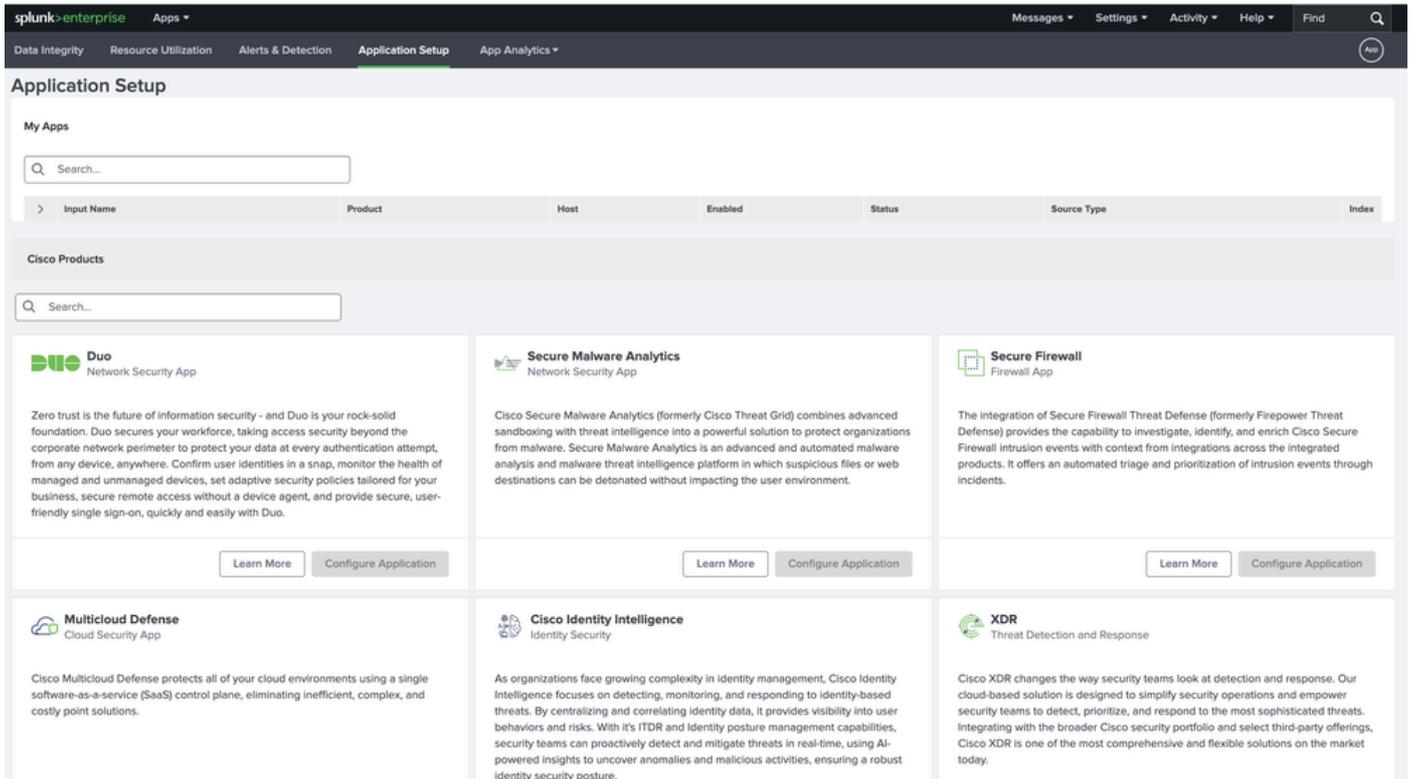
CATEGORY

 IT Oper Securit Busine UtilitiesHome Search & Reporting ~~Cisco Cloud Security~~ Cisco Security Cloud Splunk Secure Gateway Upgrade Readiness App 

Manage Apps

Find More Apps

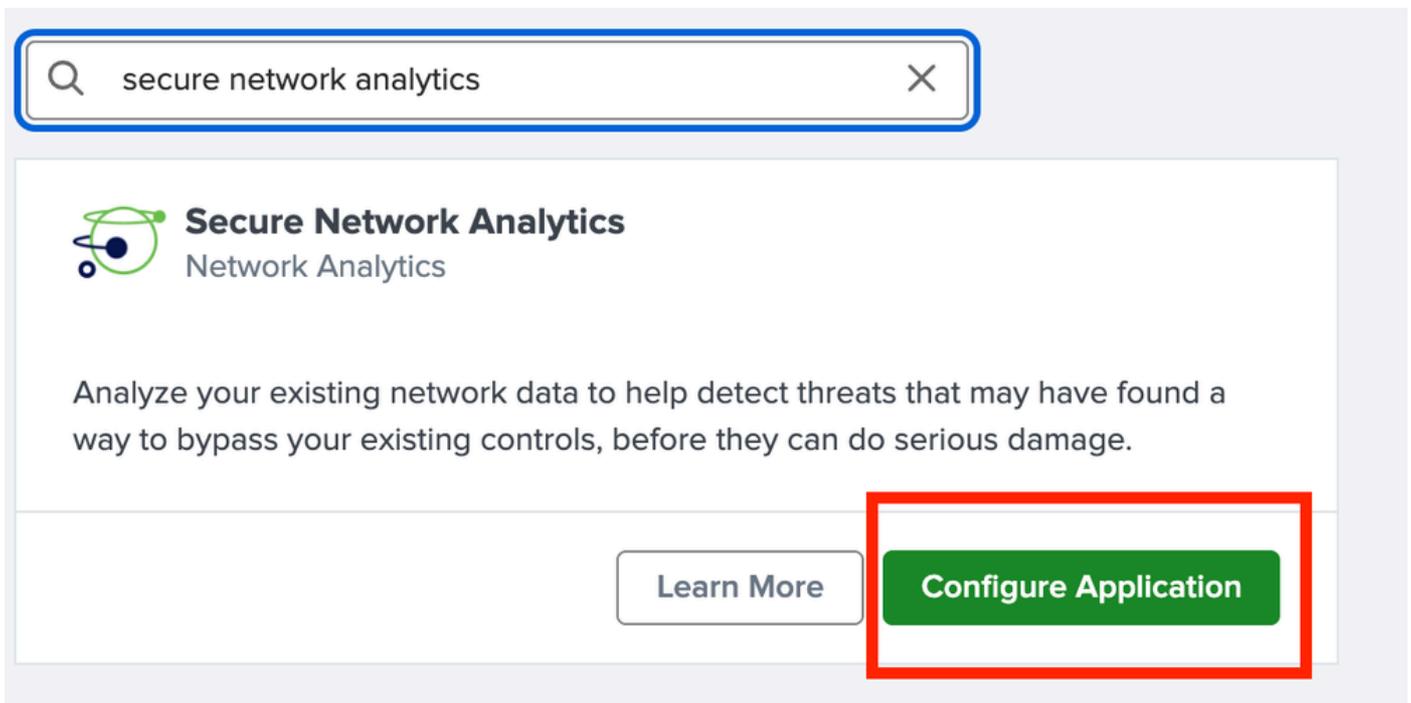
ii. Selecione Cisco Security Cloud clicando nele. Você será redirecionado para a página Configuração de aplicativos, onde todos os produtos de segurança de nuvem da Cisco disponíveis poderão ser encontrados.



Passo 4: Integração com Secure Network Analytics (SNA).

O objetivo deste documento é destacar as etapas de instalação do Splunk com Secure Network Analytics (SNA) mencionadas mais adiante.

i. Procure o Secure Network Analytics e, quando ele aparecer, selecione Configure Application:



ii) Ao selecionar a opção de configuração, a página de configuração do detalhe a ser adicionado é exibida.

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) Preencha todos os detalhes obrigatórios como mencionado para os Detalhes da conexão SNA:

1. Nome de entrada: qualquer nome exclusivo para SNA
2. Endereço do gerenciador (endereço IPv4 ou IPv6 ou nome de host): IP de gerenciamento do SNA Manager principal
3. ID do Domínio: Informe o Valor em relação ao domain_ID (por exemplo, 301)
4. Nome de usuário: O nome de usuário do gerenciador principal (por exemplo, admin)
5. Senha: Senha do usuário gerente principal

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) Deixe as configurações restantes com seus valores padrão ou modifique-as conforme necessário e clique em Salvar. Uma mensagem bem-sucedida é exibida na tela após a conclusão.

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

Cancel Save

Passo 5: Verificação da integração.

Esta é uma etapa importante na qual você precisa verificar se a integração executada na etapa anterior foi realizada com êxito ou não.

i. O status da conexão para a entrada deve ser Connected na guia Application Setup com o padrão como Enabled para o nome direito no campo Input.

splunk-enterprise Apps

Administrator 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
SNA_Manager	Secure Network Analytics	Splunk-Server	<input checked="" type="checkbox"/>	Connected	cisco:sna	cisco_sna

ii. Selecione o Secure Network Analytics Dashboard na lista suspensa e as estatísticas começarão a refletir no painel.

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

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

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

Secure Network Analytics Dashboard

Security Insights Network Insights **Ingestion Insights**

Time Range: Last 24 hours Index: All (1)

Max 95th percentile flows per second	Flow Records Analyzed	Internal traffic occurring on your network	Traffic exchanged between your network and the Internet	Encrypted traffic exchanged between your network and the Internet
166	1.1M	721.4 GB	359.6 GB	304.1 GB

Internal Monitored Network
Hosts communicating within your network

1.6K

Flow Rate (fps)

fc752 fccds741

Perguntas freqüentes

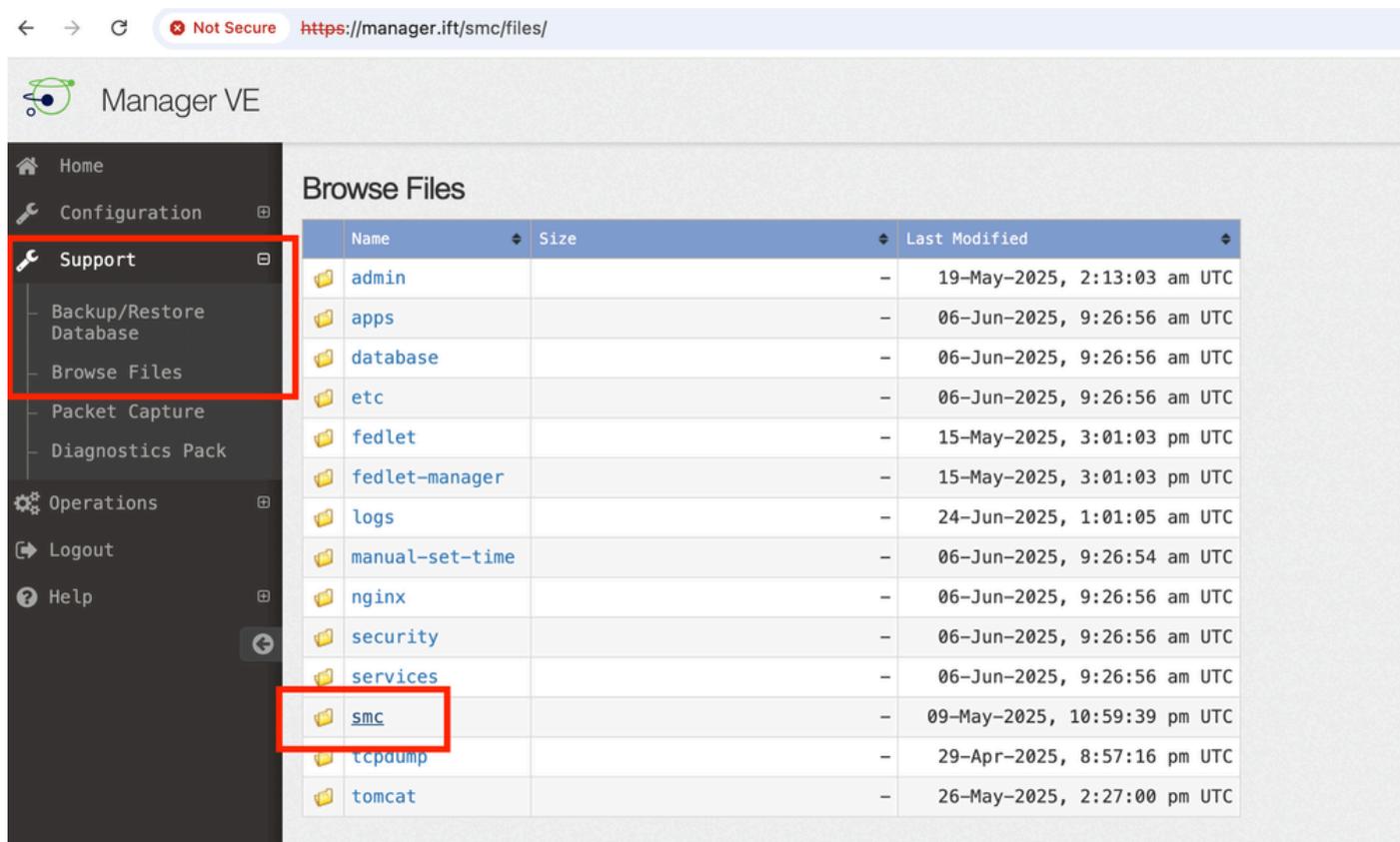
Onde encontrar a ID de domínio do gerenciador SNA?

Resposta:

i. Faça login no gerenciador principal do SNA e redirecione para a URL da página de

administração do dispositivo ou do [Índice IP do gerenciador](#).

ii) Procure a pasta smc na seção Suporte.



The screenshot shows the Manager VE web interface. The browser address bar displays 'https://manager.ift/smc/files/'. The left sidebar contains a navigation menu with the following items: Home, Configuration, Support, Backup/Restore Database, Browse Files, Packet Capture, Diagnostics Pack, Operations, Logout, and Help. The 'Support' menu item is highlighted with a red box. The main content area is titled 'Browse Files' and displays a table of files and folders. The 'smc' folder is highlighted with a red box in the table.

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) Abra o arquivo domain.xml disponível na pasta domain_XXX na pasta 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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.