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.

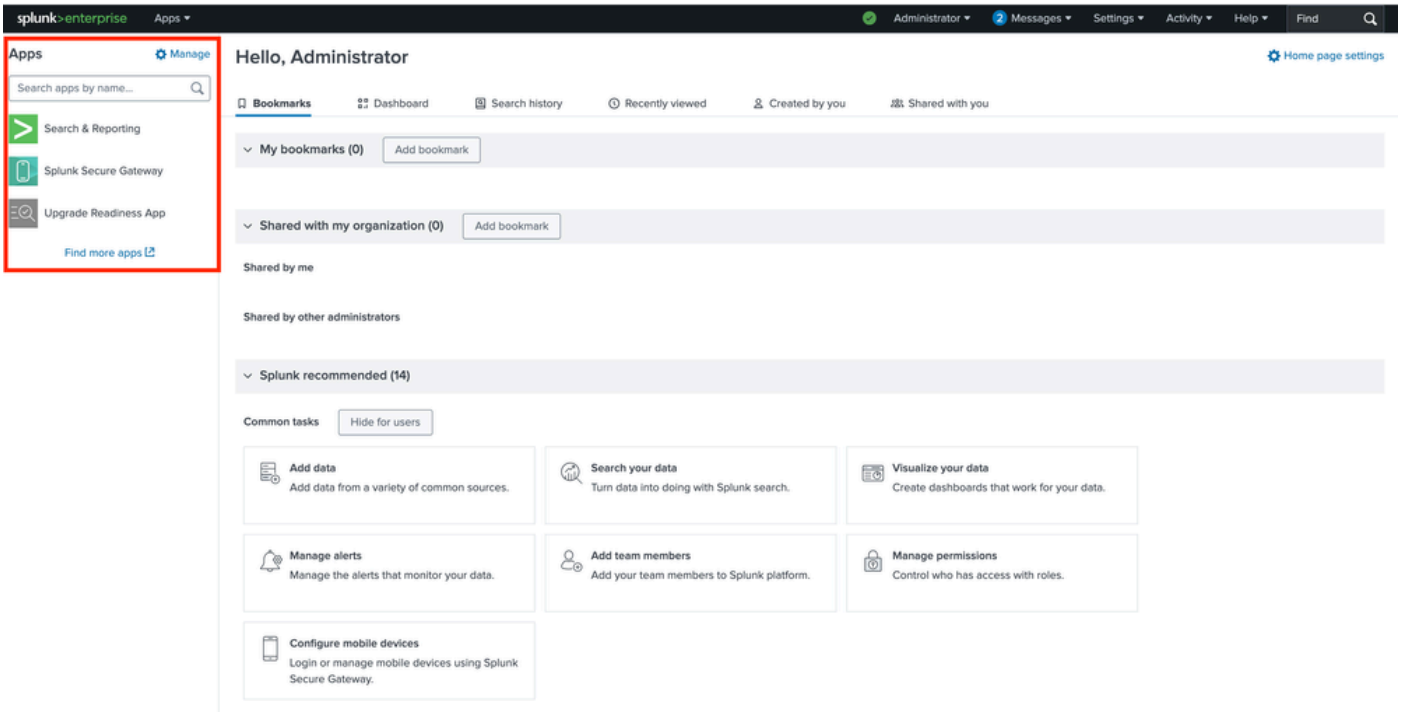
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Configurar

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

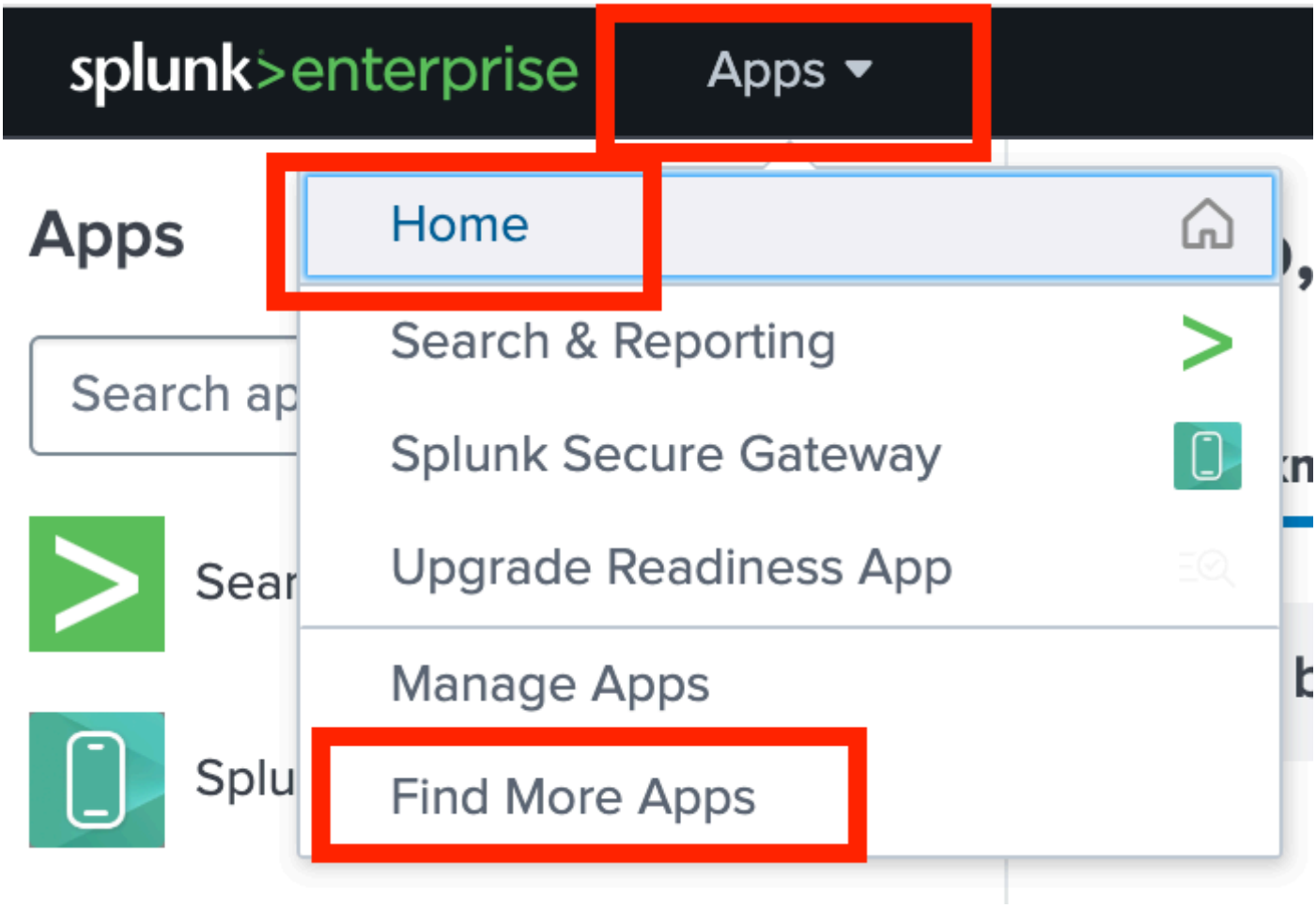
i. Faça login no portal da Web Splunk com as credenciais de administrador e, em um login bem-

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

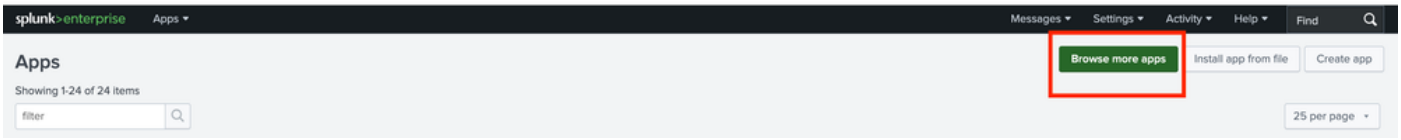


ii) Para integrar o SNA com o Splunk, é necessário instalar o Cisco Security Cloud Application, que pode ser obtido em qualquer um dos métodos mencionados:

1. Selecione Find More Apps no menu suspenso.



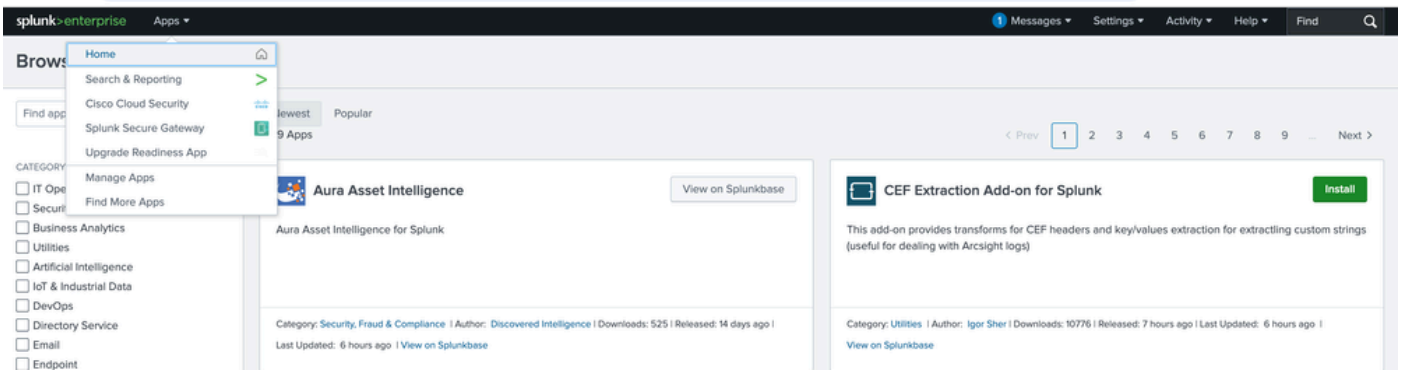
b. Procure mais aplicativos sob o ícone de equipamento Gerenciador.



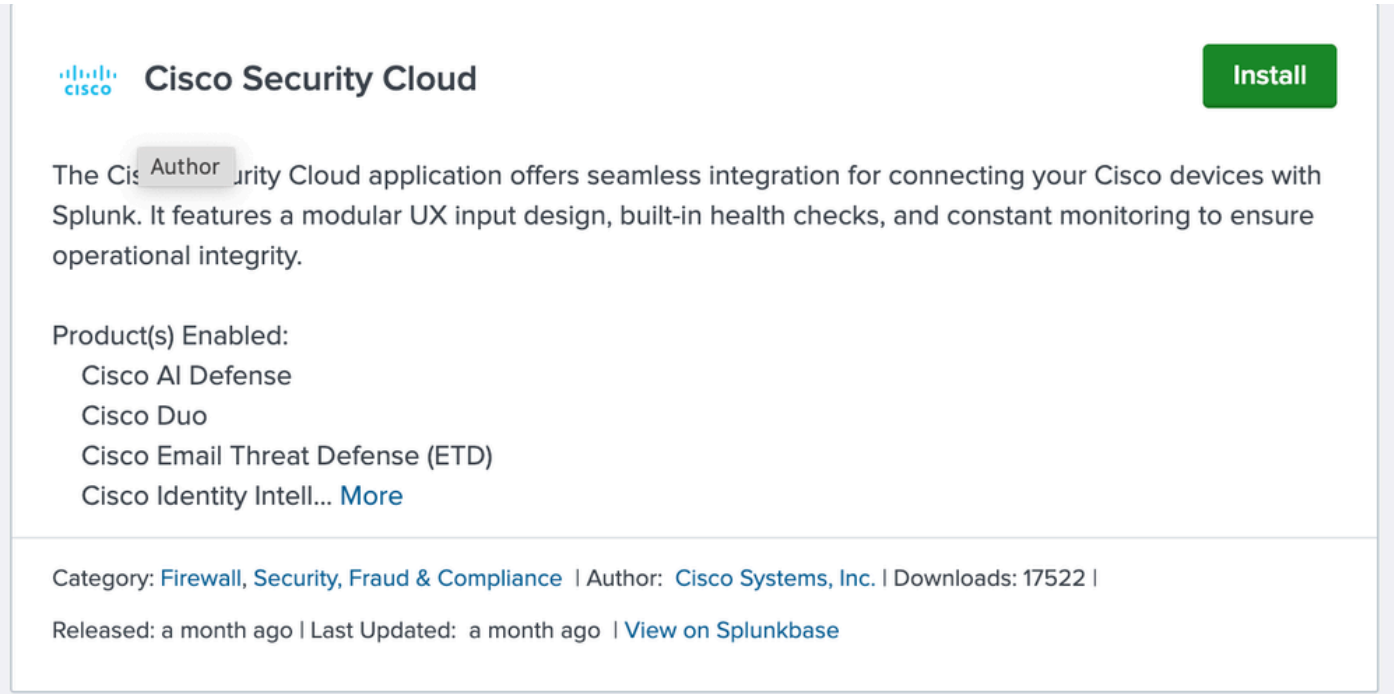
Passo 2: Instalação do Cisco Security Cloud Application.

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

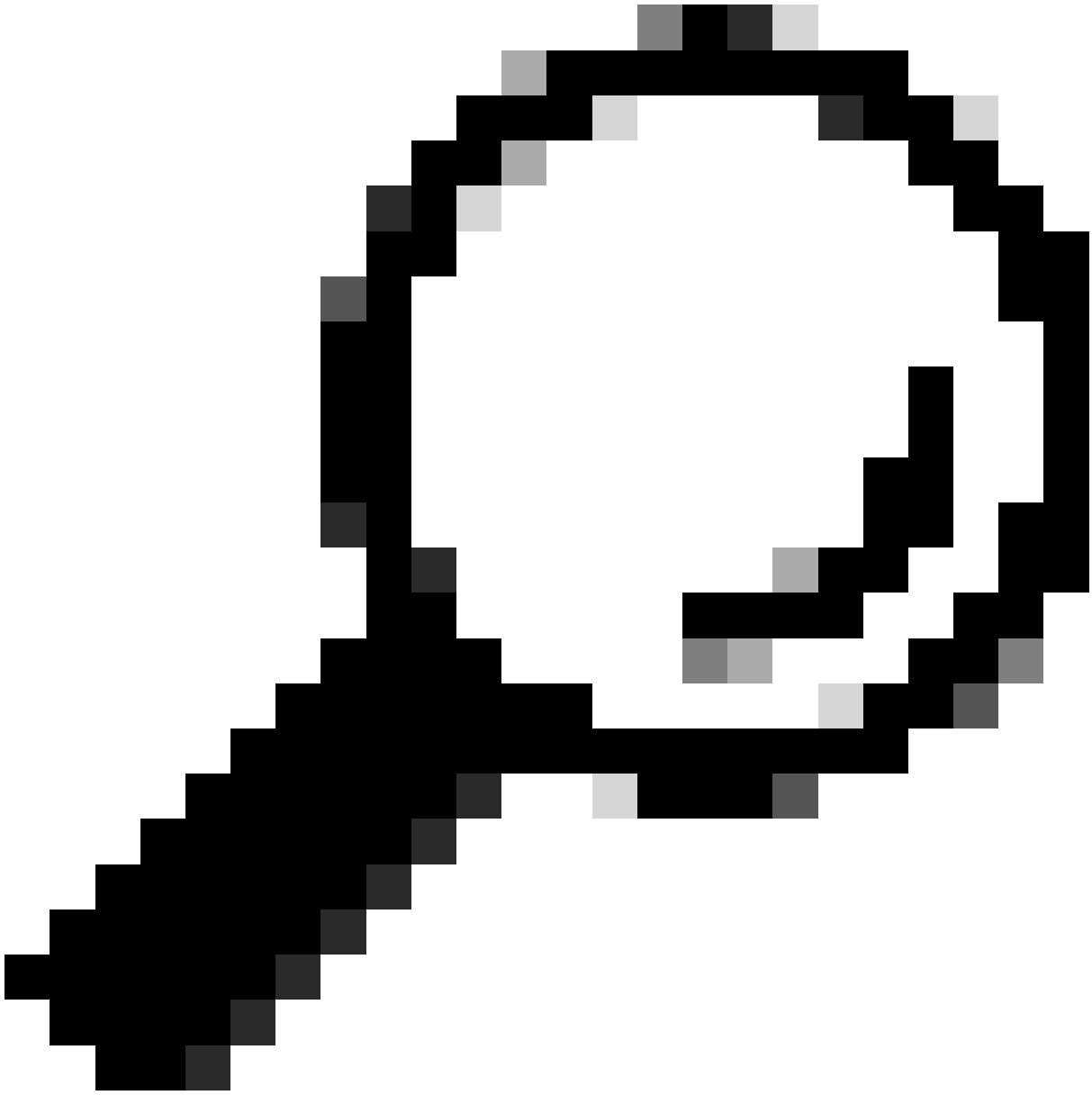
Caution: Não se confunda com o Cisco Cloud Security App.



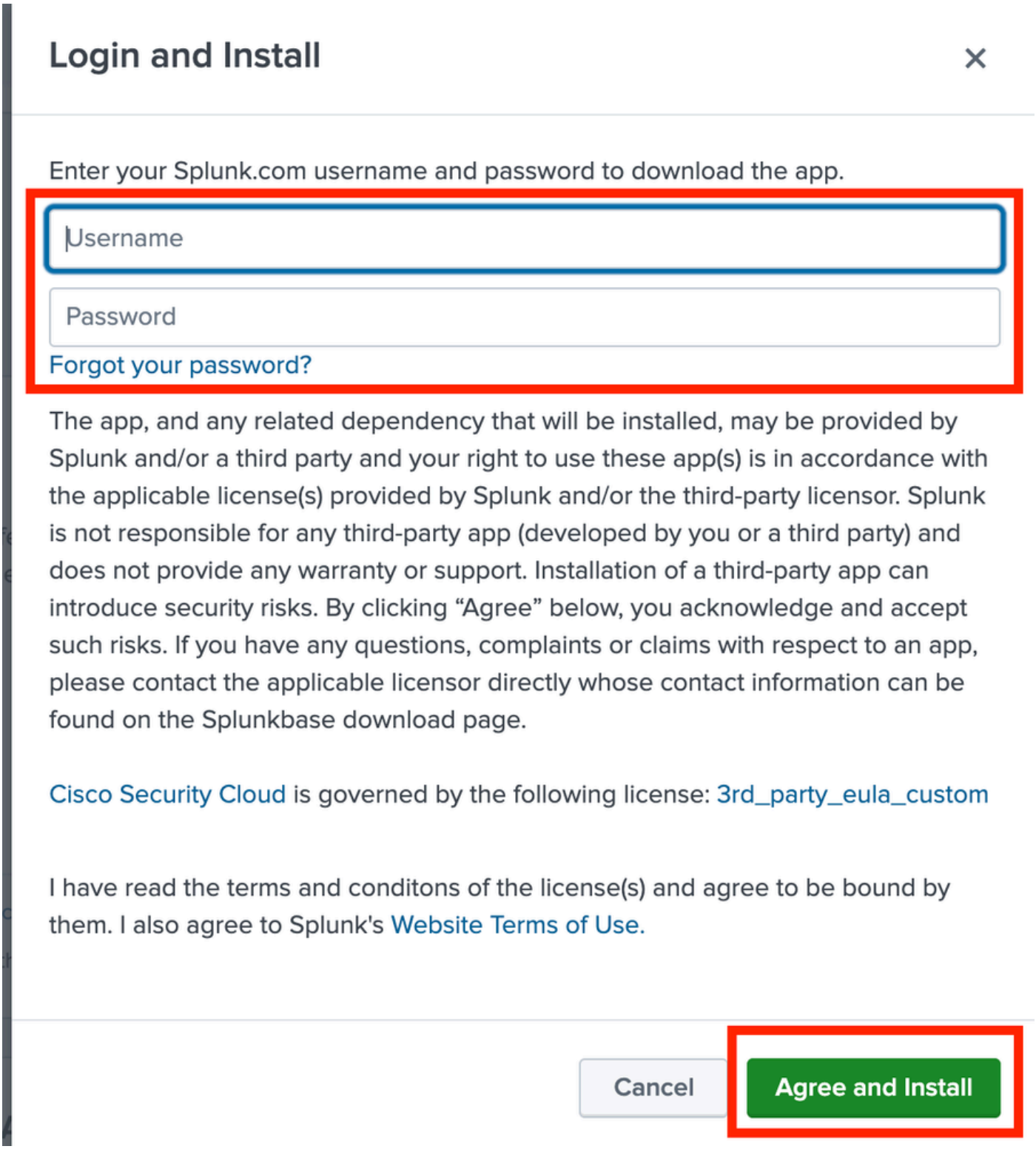
ii) Instale o aplicativo clicando no botão Instalar.



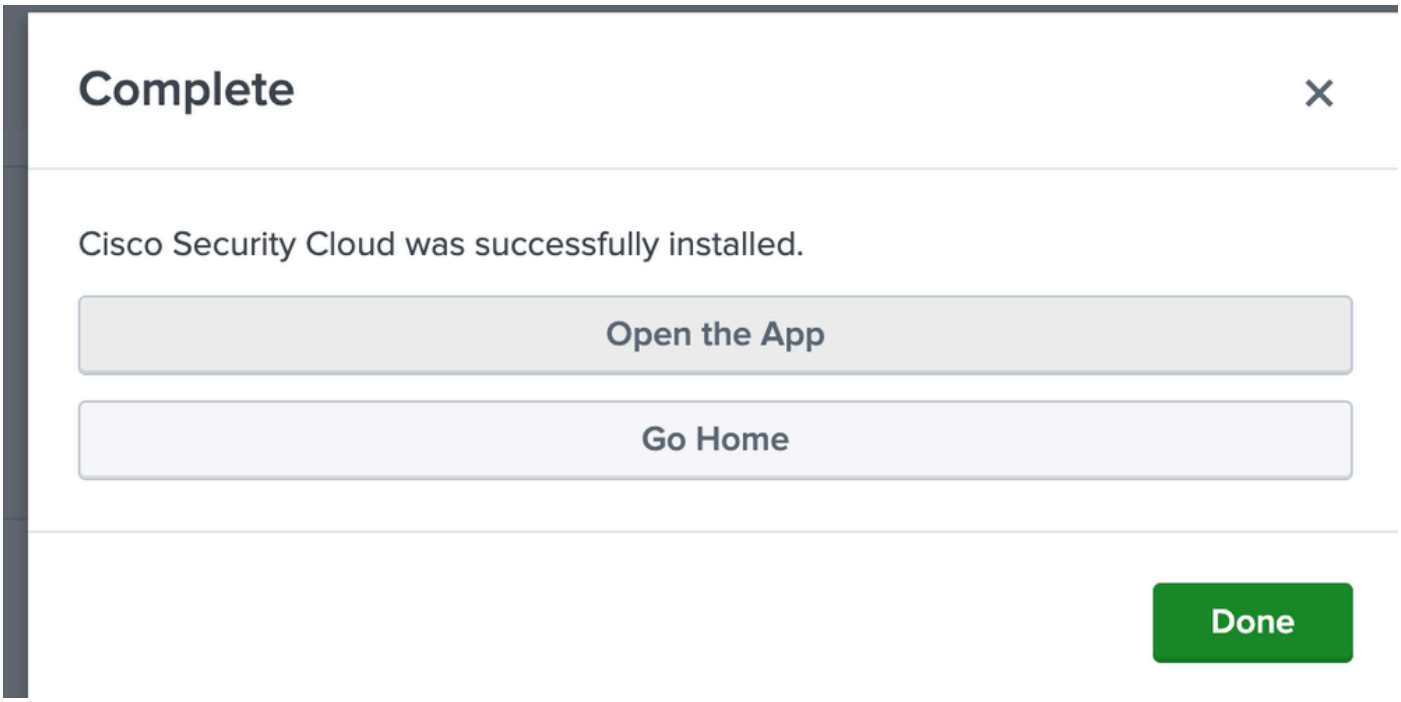
iii) No momento em que você clica no botão de instalação, uma janela aparece solicitando as credenciais da conta Splunk antes de instalar o aplicativo. Forneça as credenciais e clique em Concordo e instalar para continuar.



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

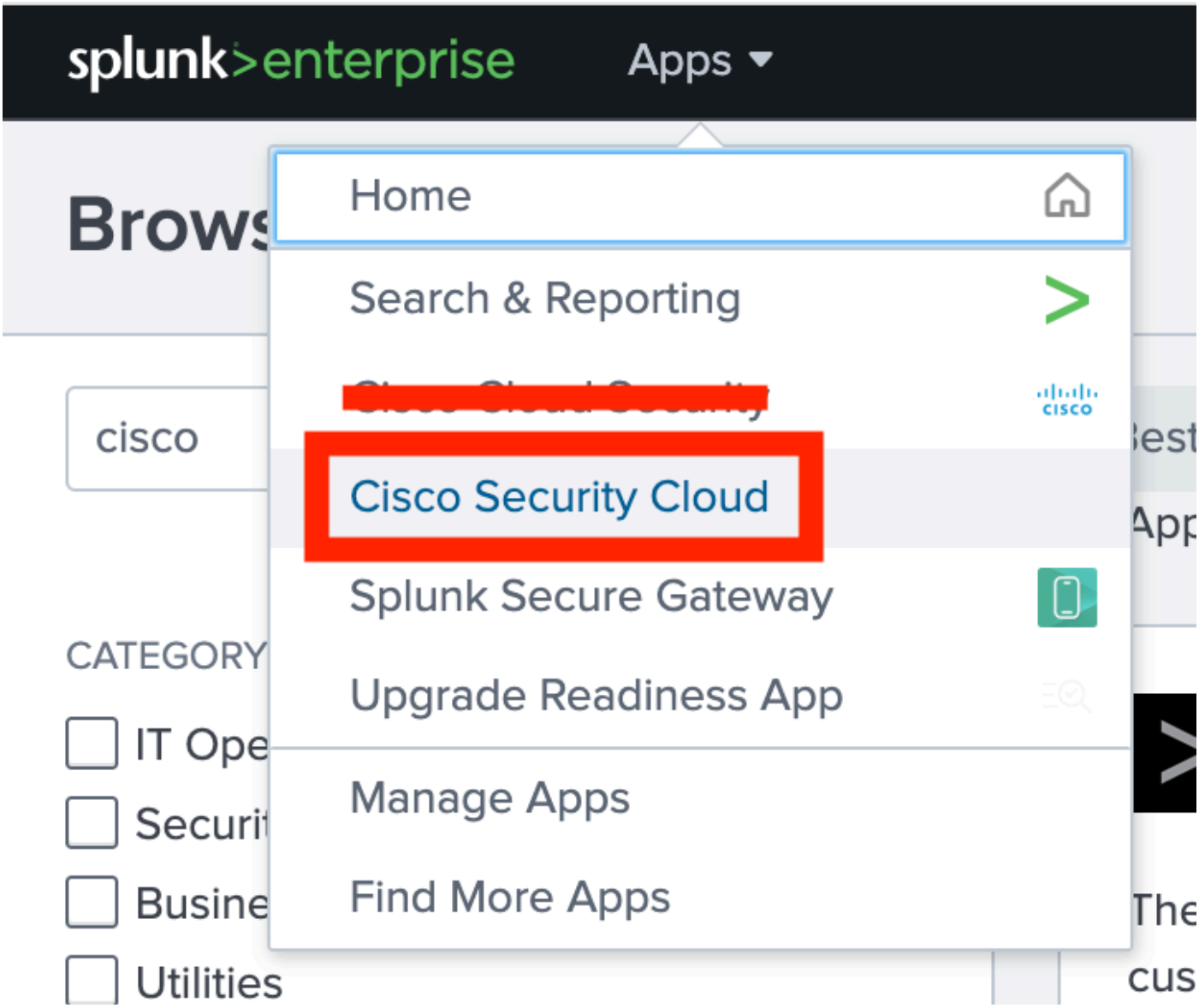


iv) Uma mensagem é exibida sobre a instalação bem-sucedida do aplicativo conforme descrito. Clique em Concluído.

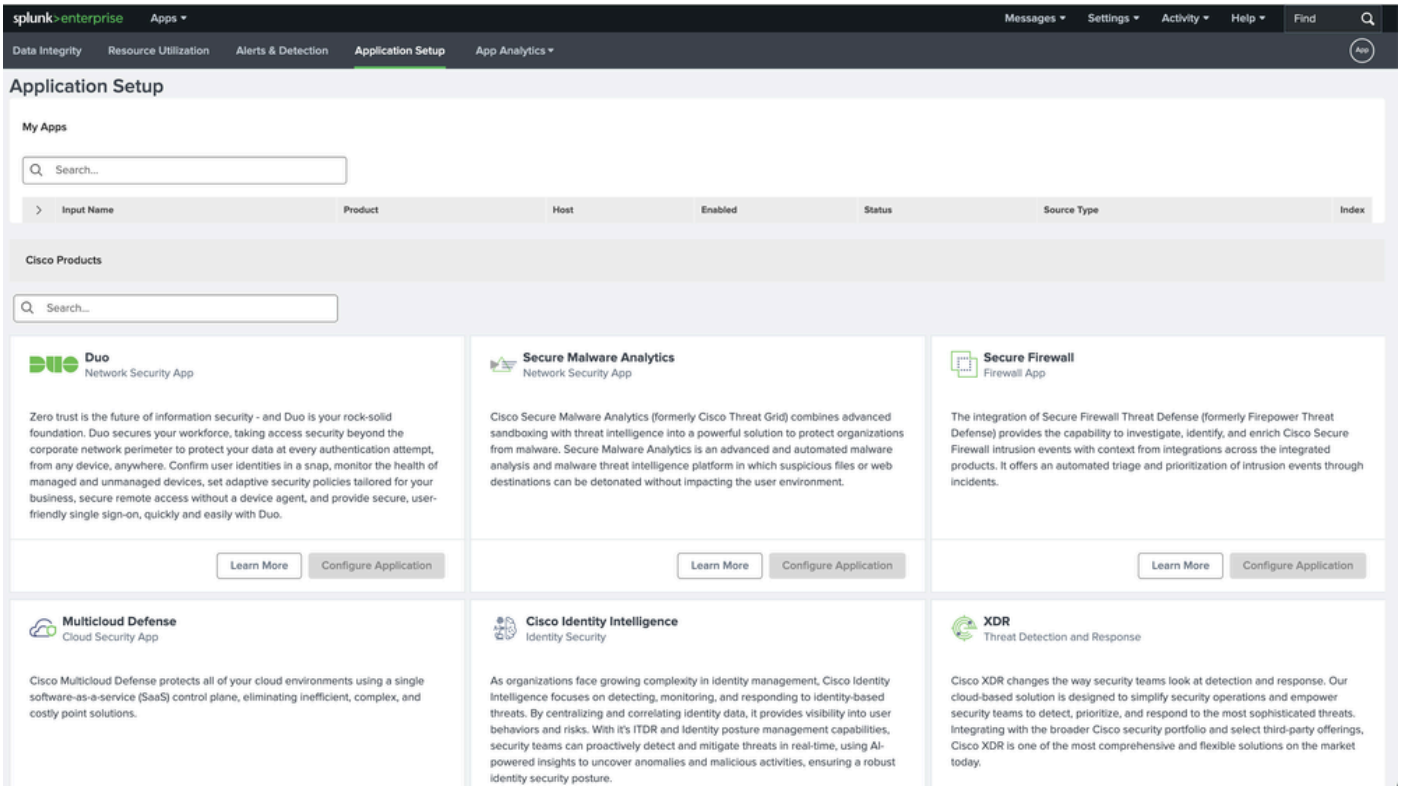


Passo 3: Verificação da instalação do aplicativo de nuvem de segurança da Cisco.

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



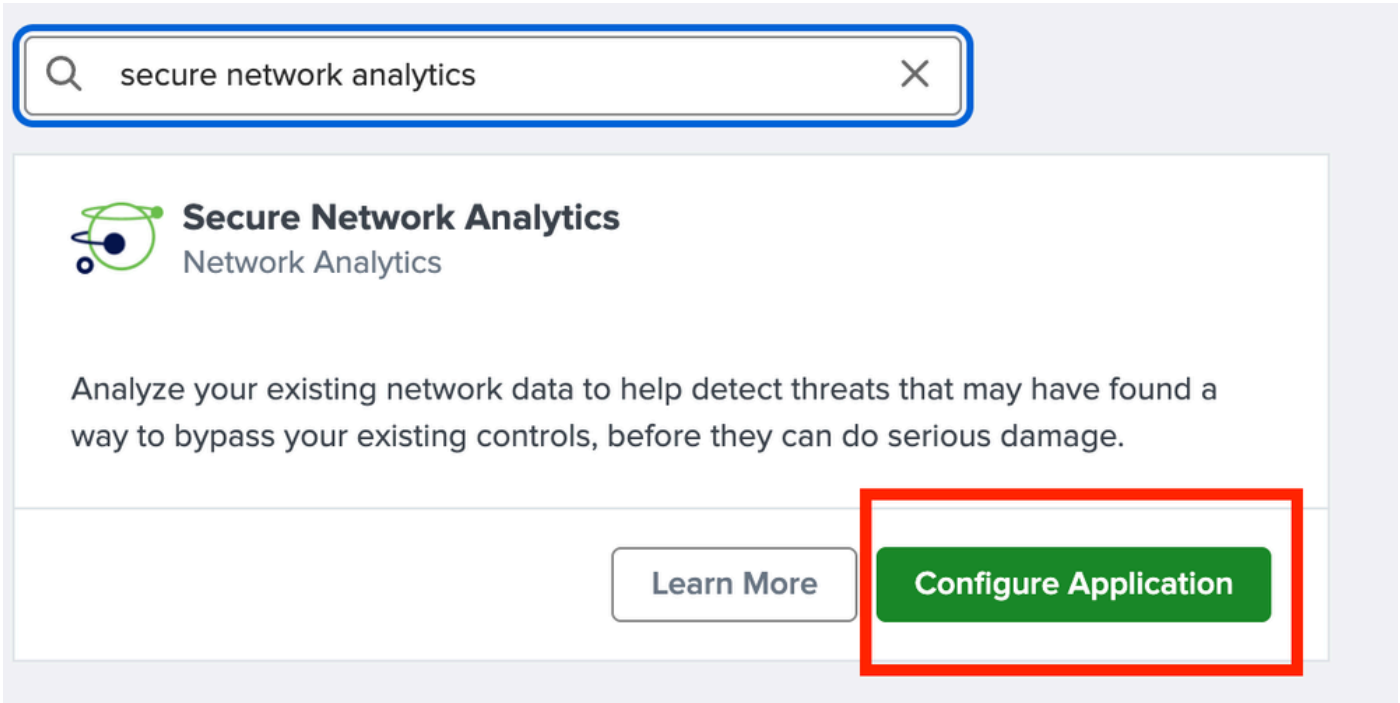
ii. Selecione Cisco Security Cloud clicando nele. Você será redirecionado para a página Configuração de aplicativos, onde todos os produtos de segurança de nuvem da Cisco disponíveis poderão ser encontrados.



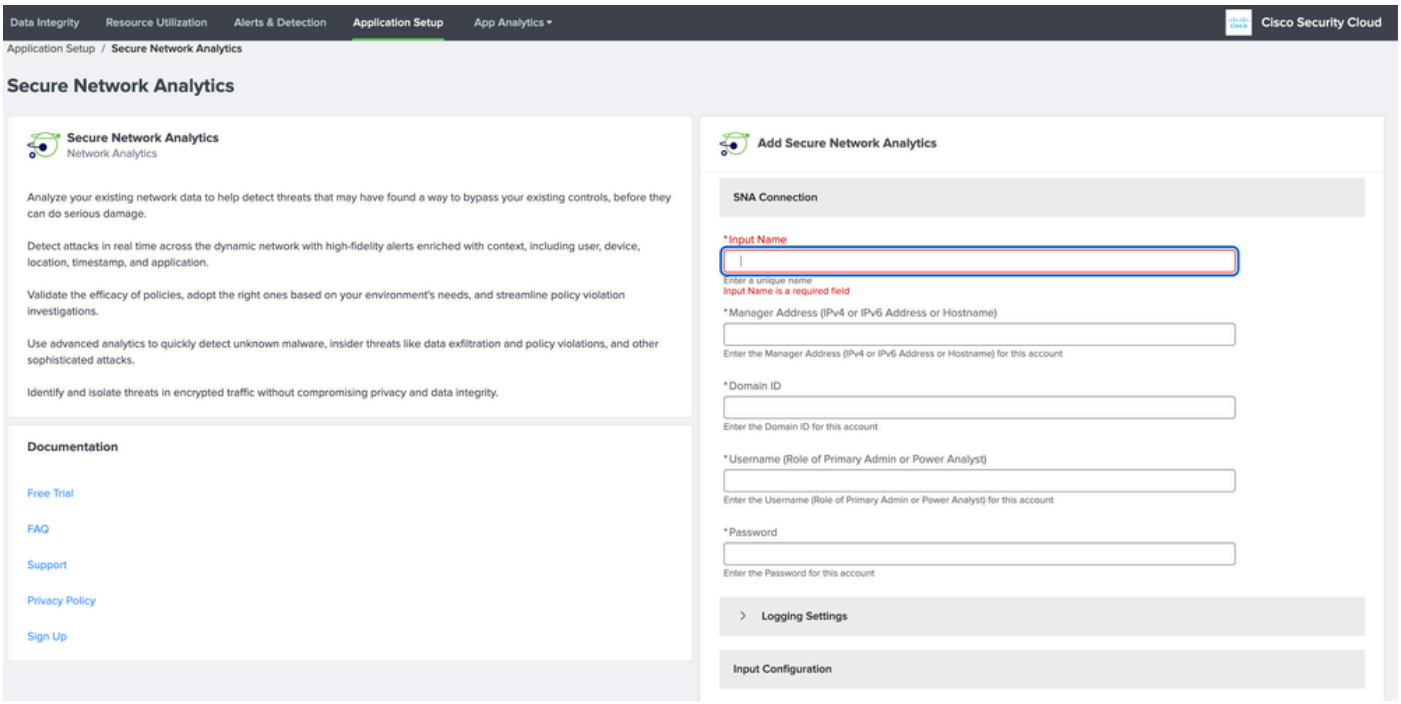
Passo 4: Integração com Secure Network Analytics (SNA).

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:

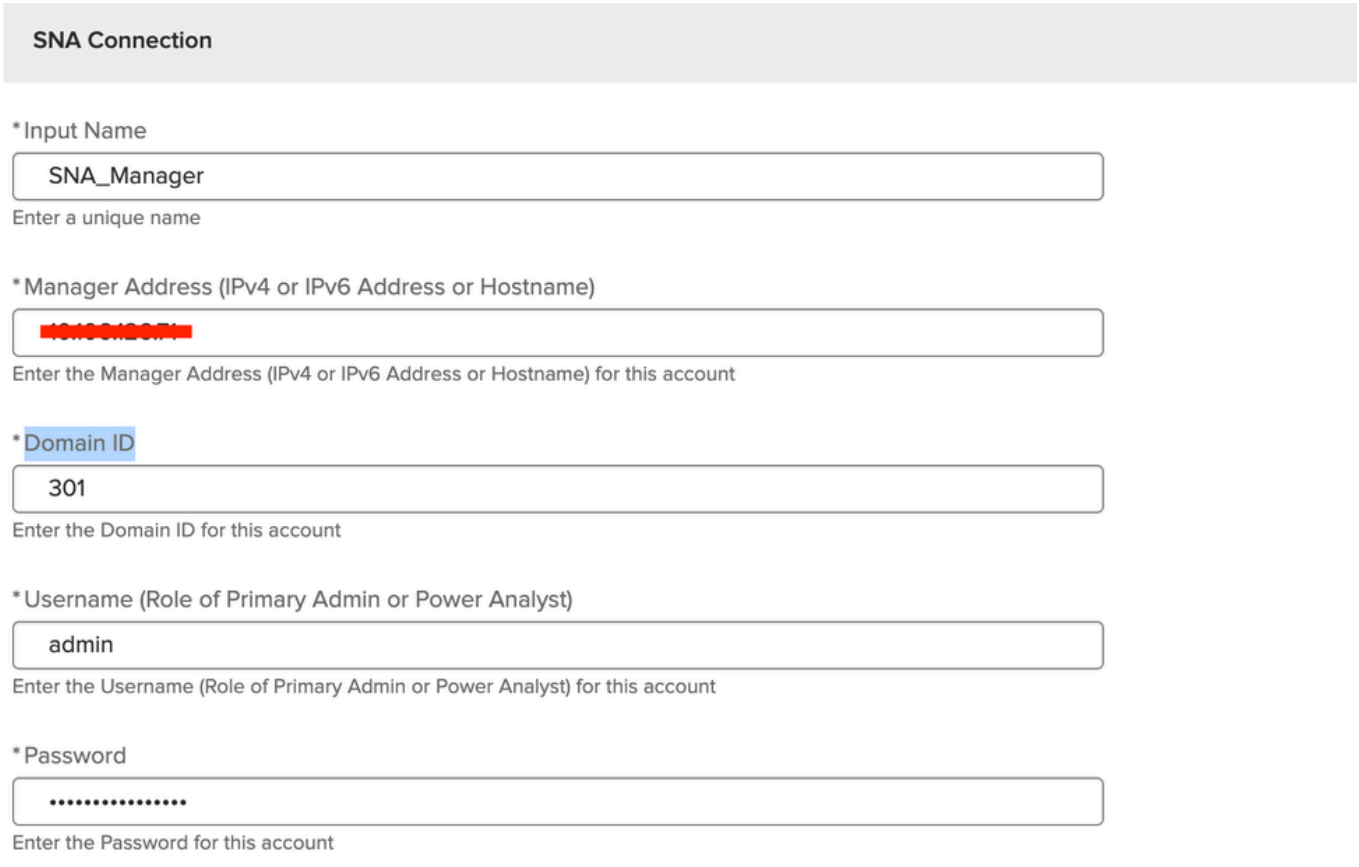


ii) Ao selecionar a opção de configuração, a página de configuração do detalhe a ser adicionado é exibida.

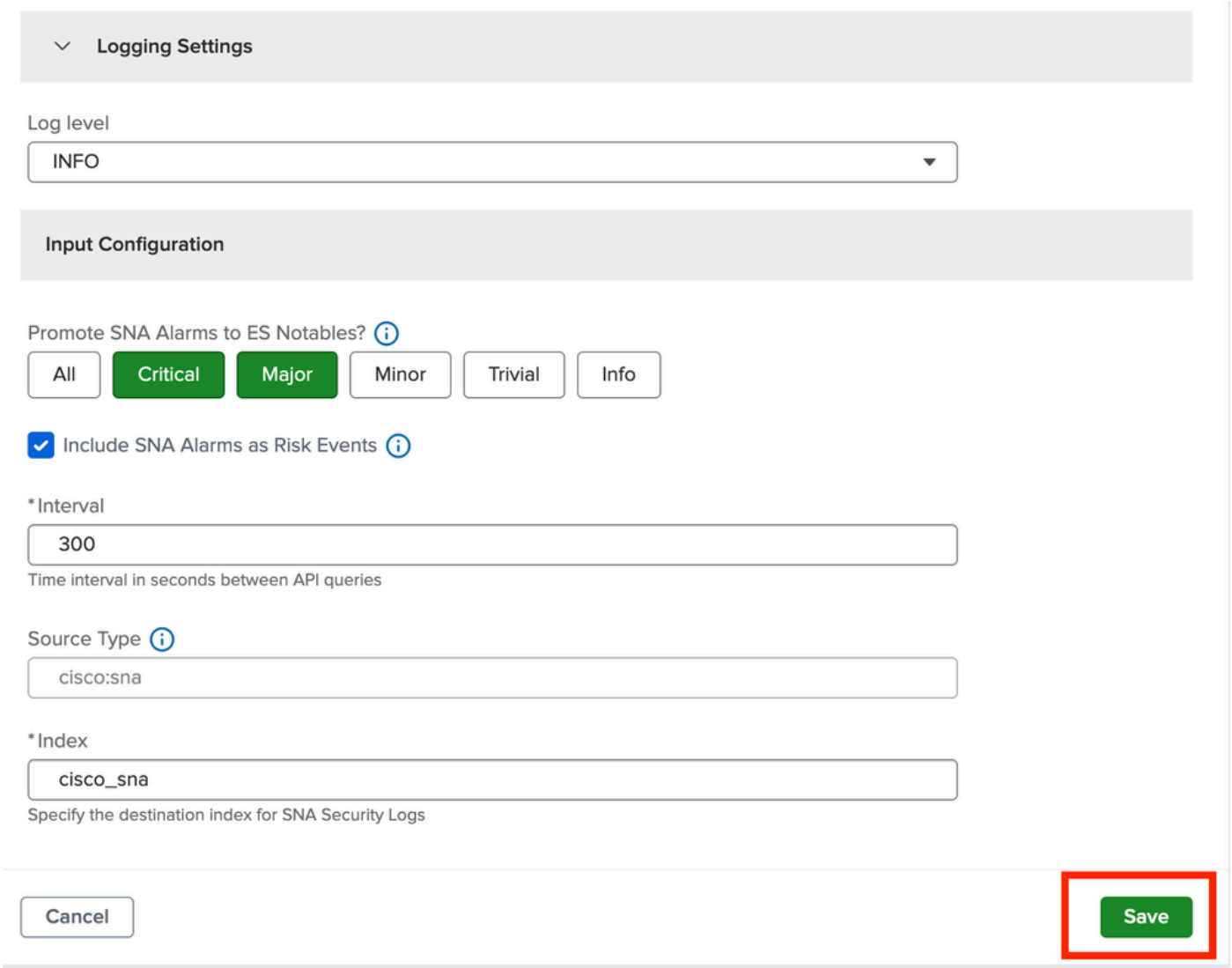


iii) Preencha todos os detalhes obrigatórios como mencionado para os Detalhes da conexão SNA:

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



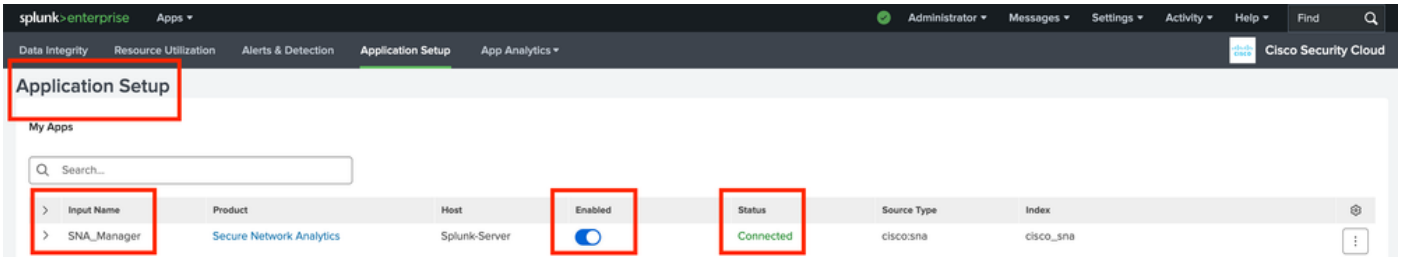
iv) Deixe as configurações restantes com seus valores padrão ou modifique-as conforme necessário e clique em Salvar. Uma mensagem bem-sucedida é exibida na tela após a conclusão.



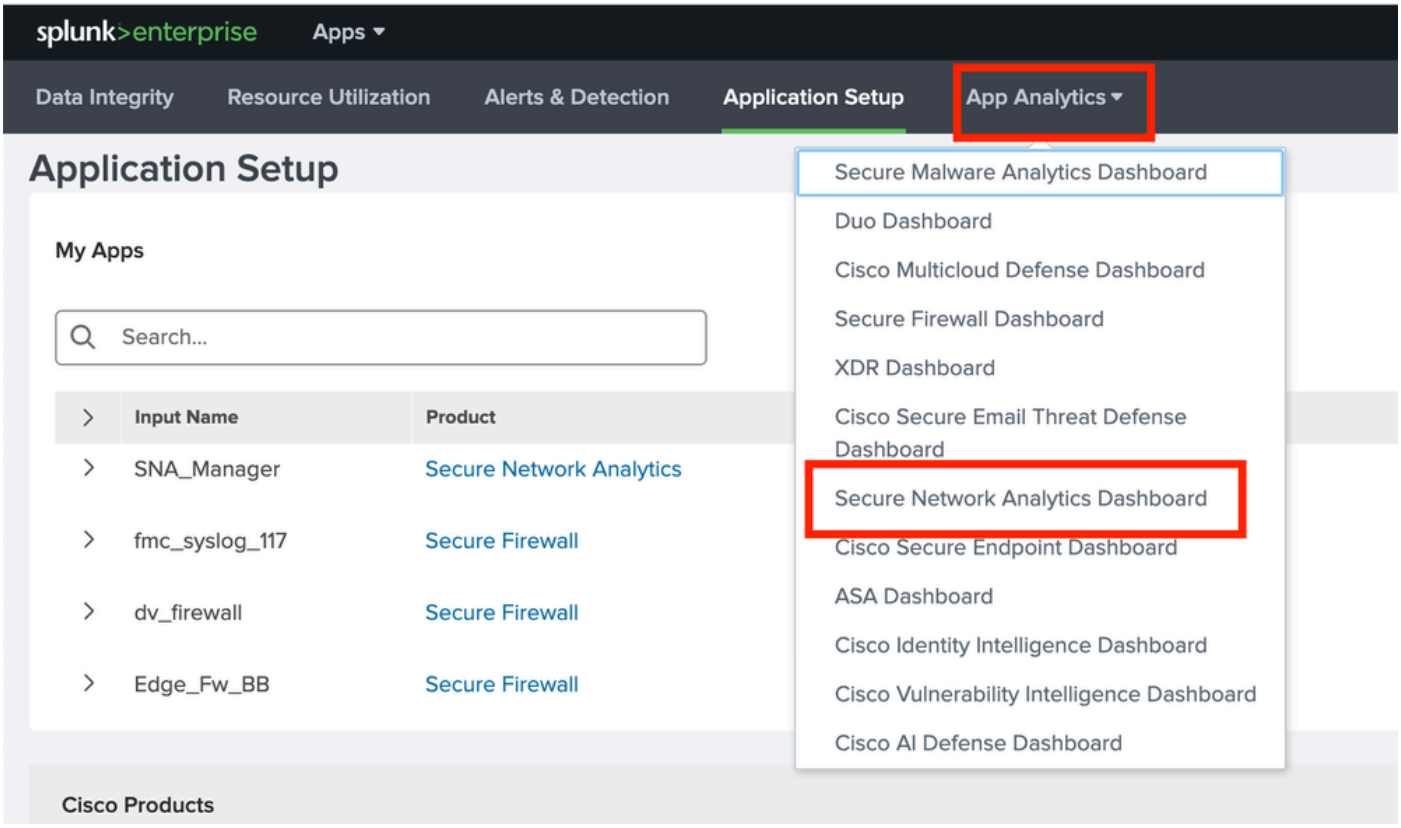
Passo 5: Verificação da integração.

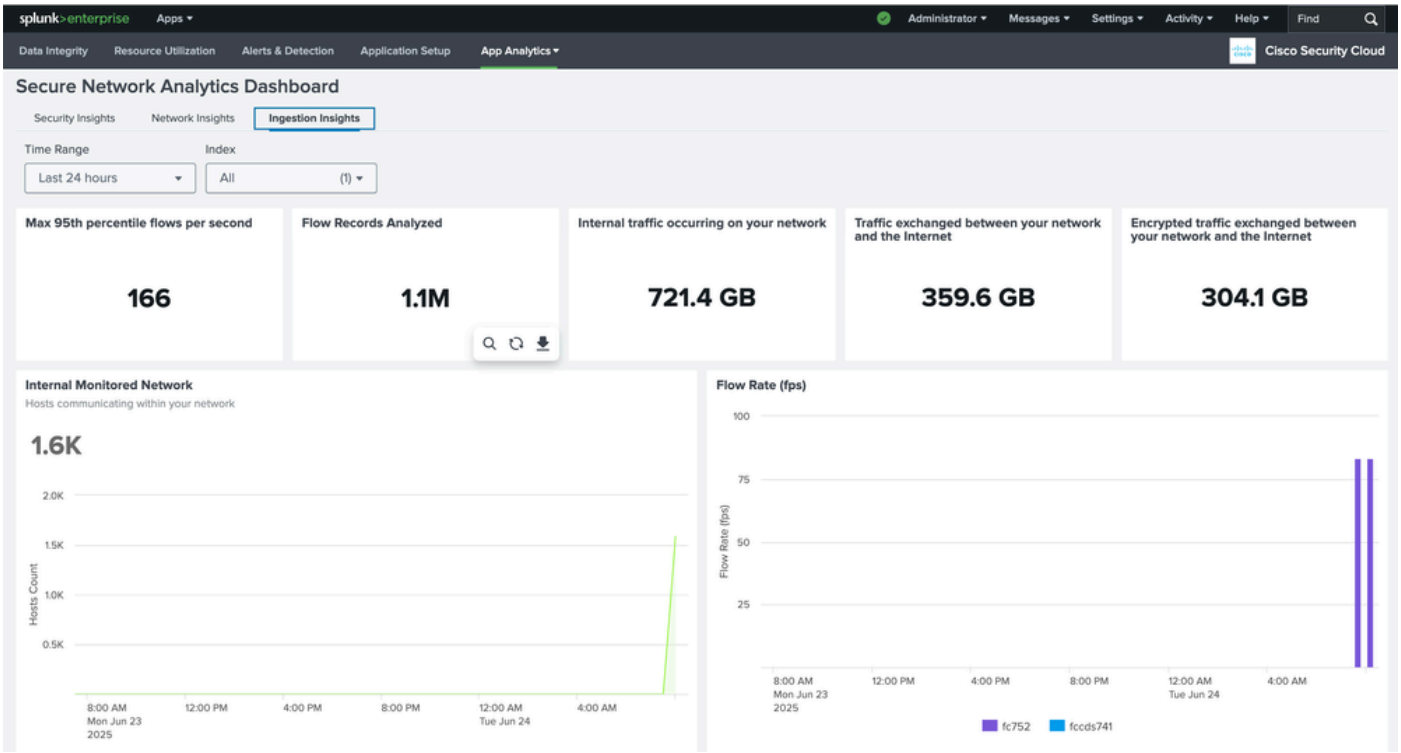
Esta é uma etapa importante na qual você precisa verificar se a integração executada na etapa anterior foi realizada com êxito ou não.

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.



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





Perguntas freqüentes

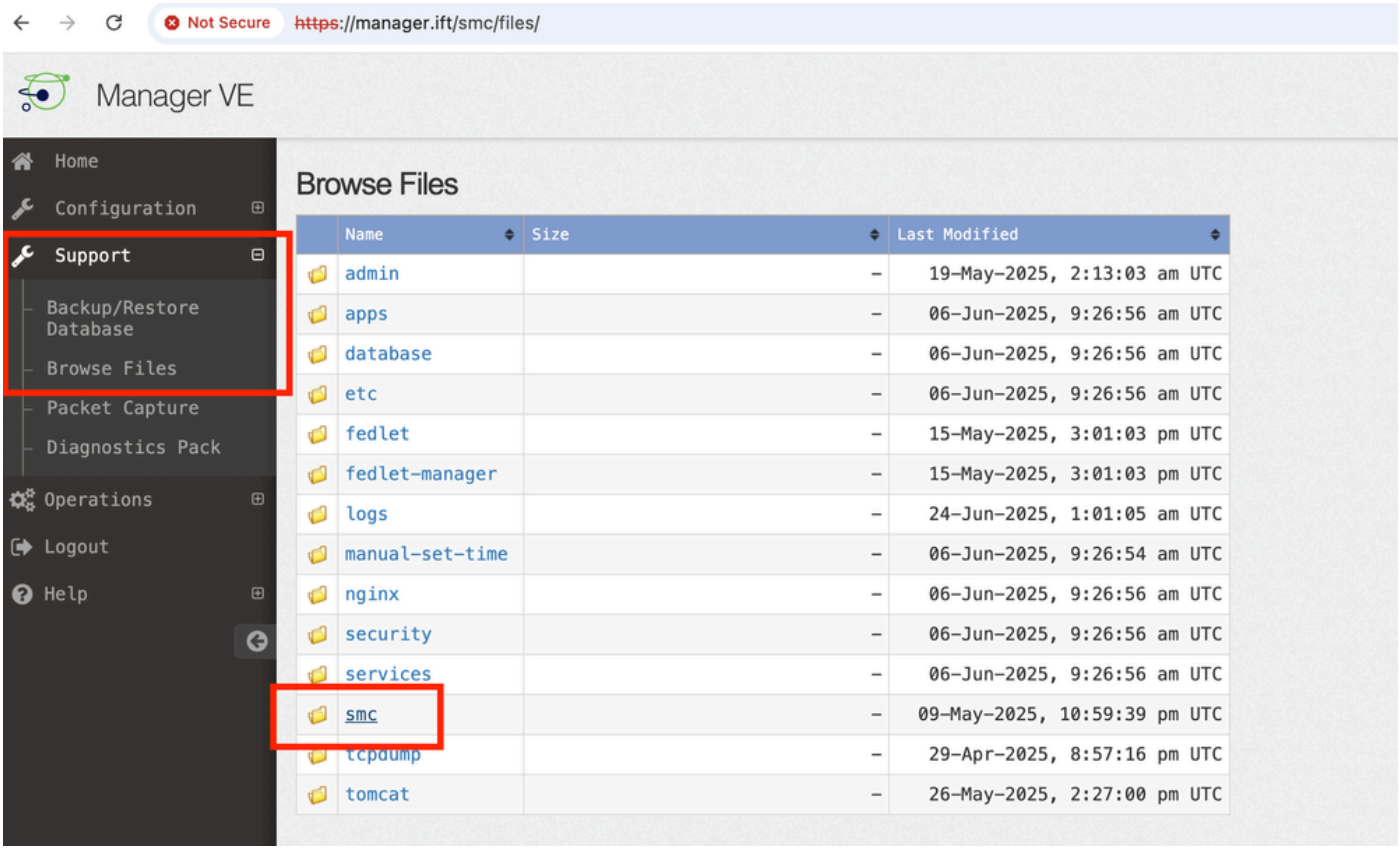
Onde encontrar a ID de domínio do gerenciador SNA?

Resposta:

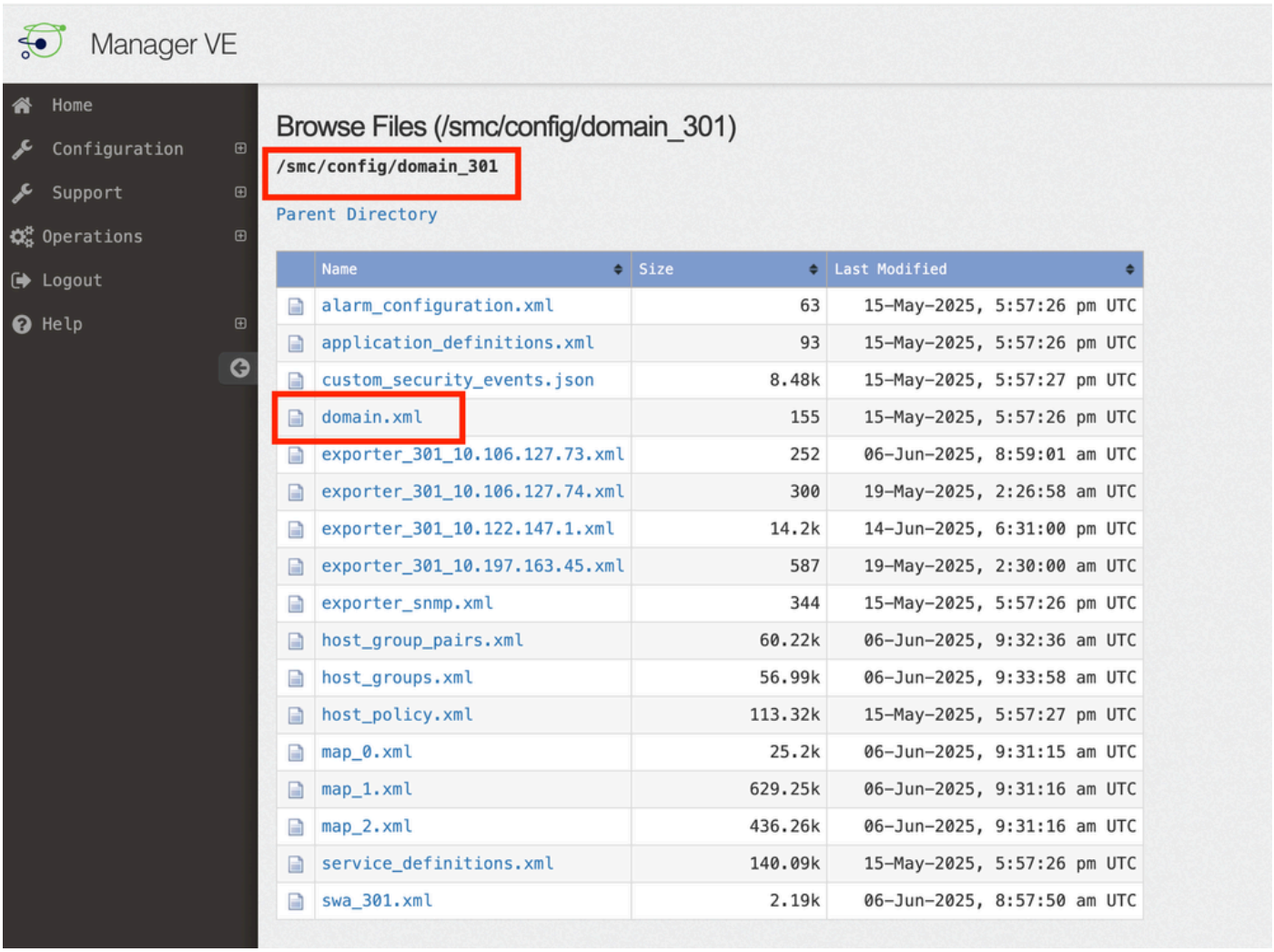
i. Faça login no gerenciador principal do SNA e redirecione para a URL da página de

administração do dispositivo ou do Índice IP do gerenciador.

ii) Procure a pasta smc na seção Suporte.



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

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.