Configure a integração do SMA com o SecureX

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[integração de SMA](#)
[Web SMA](#)
[E-mail SMA](#)
[Verificar](#)
[Troubleshoot](#)
[Módulo SMA SecureX SMA tile / Resposta seguraX a ameaças mostrando o erro "Ocorreu um erro inesperado no módulo SMA"](#)
[Vídeo](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve o processo para configurar, verificar e solucionar problemas da integração do Content Security Management Appliance (SMA) com o SecureX.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Security Management Appliance (SMA)
- ESA (Email Security Appliance)
- Web Security Appliance (WSA)
- Cisco Threat Response (CTR)
- Painel SecureX

Componentes Utilizados

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

- SMA executando AsyncOS 13.6.2 (para SMA - Módulo de e-mail)

- SMA executando AsyncOS 12.5 (para SMA - Módulo Web)

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. If your network is live, make sure that you understand the potential impact of any command.

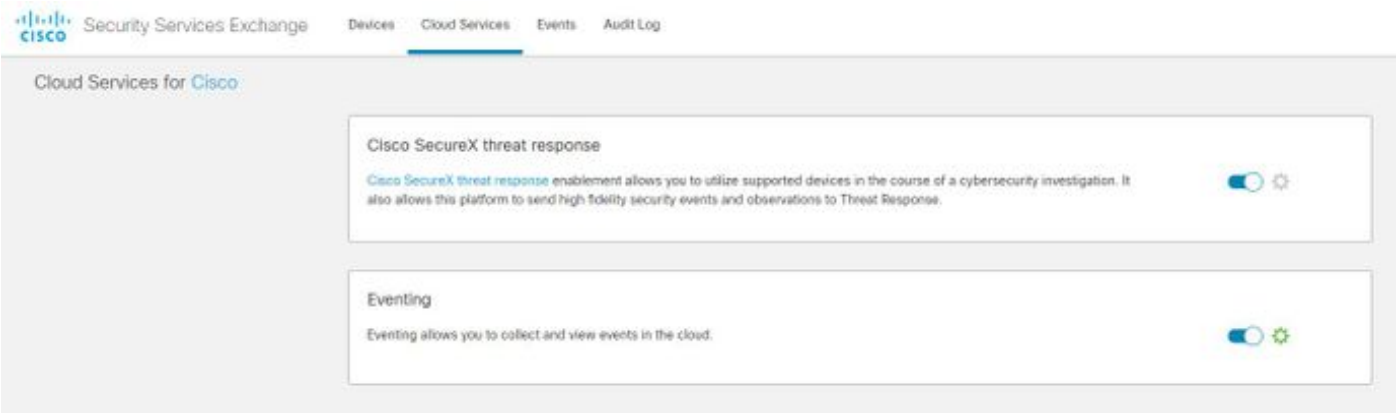
Configurar

integração de SMA

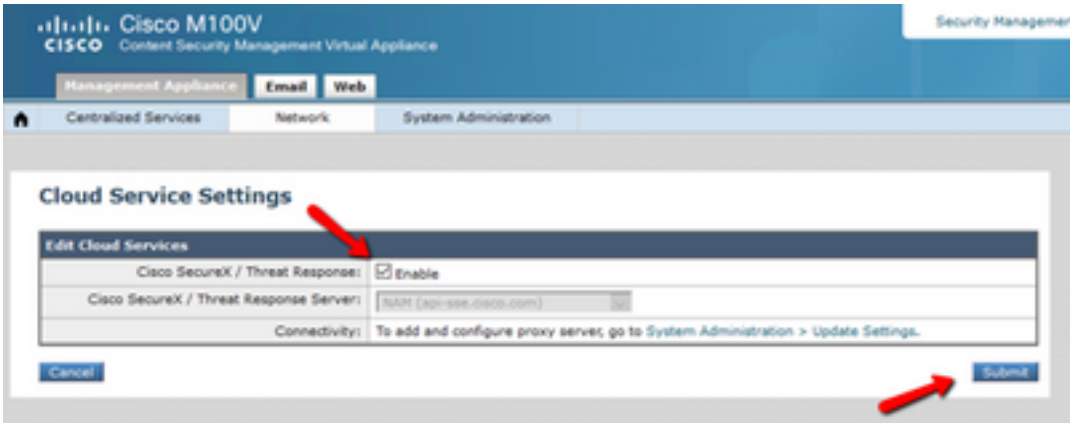
Etapa 1. No SMA, navegue até **Network > Cloud Service Settings > Edit Settings**, enable integration e confirme se o SMA está pronto para aceitar um token de registro.

Etapa 2. Clique no ícone Configurações (equipamento) e, em seguida, clique em **Dispositivos > Gerenciar dispositivos** para ser levado ao Security Services Exchange (SSE).

Verifique se todas as opções estão habilitadas em **Cloud** Services.



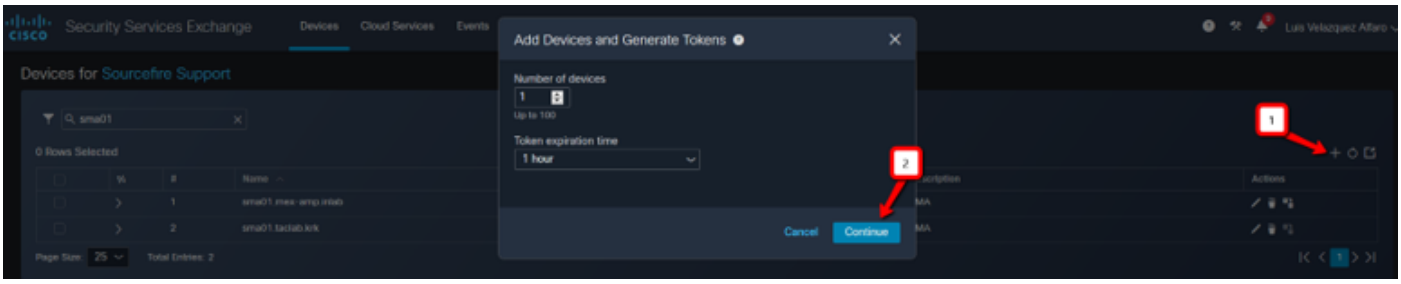
Etapa 3. Ative a integração do Cisco Threat Response na guia Cloud Services (Serviços em nuvem) e clique na guia Devices (Dispositivos) e no ícone + para adicionar um novo dispositivo (requer conta de administrador SMA).



Etapa 4. Efetue login no portal SSE a partir da instância do SecureX.

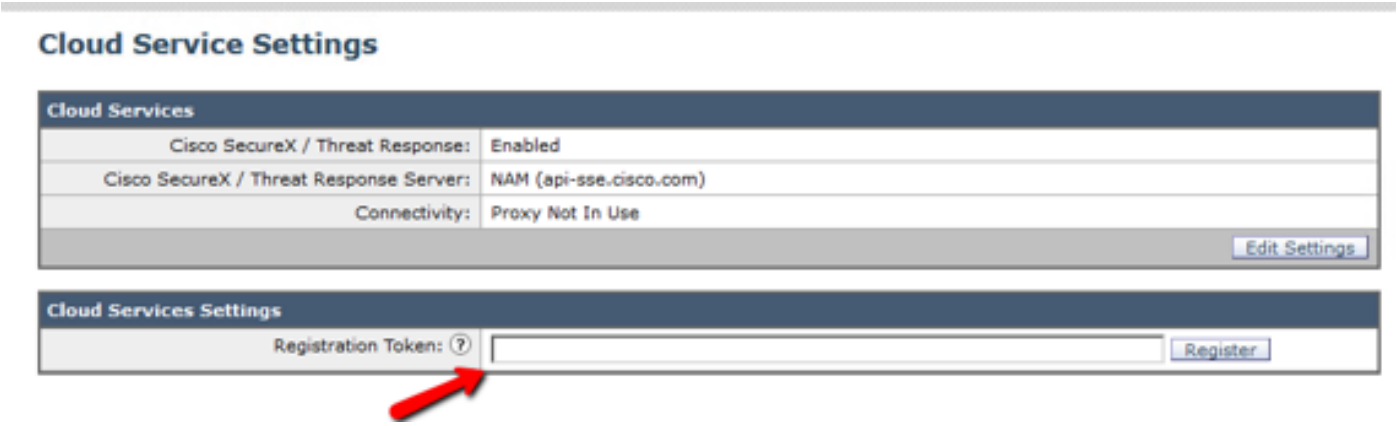
Etapa 5. No portal Secure X, navegue até **Integrations > Devices > Manage devices (Integrações > Dispositivos > Gerenciar dispositivos)**

Etapa 6. Crie um novo token no portal SSE e especifique a hora de expiração do token (o padrão é 1 hora) e clique em **Continuar**.

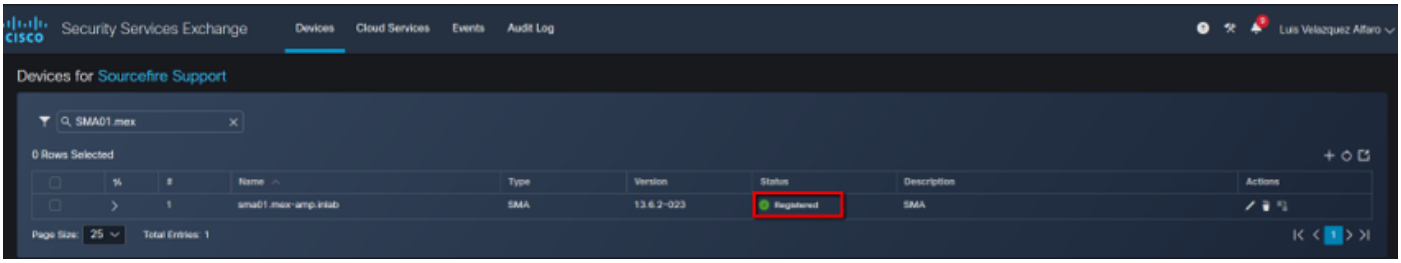


Passo 7. Copie o token gerado e confirme se o dispositivo foi criado.

Etapa 8. Navegue até seu SMA **(Network > Cloud Service Settings)** para inserir o token e clique em Register.



Para confirmar o registro bem-sucedido, revise o status no **Security Services Exchange** e confirme se o SMA é exibido na página Dispositivos.



Web SMA

Etapa 1. Preencha o formulário Adicionar novo módulo da Web SMA:

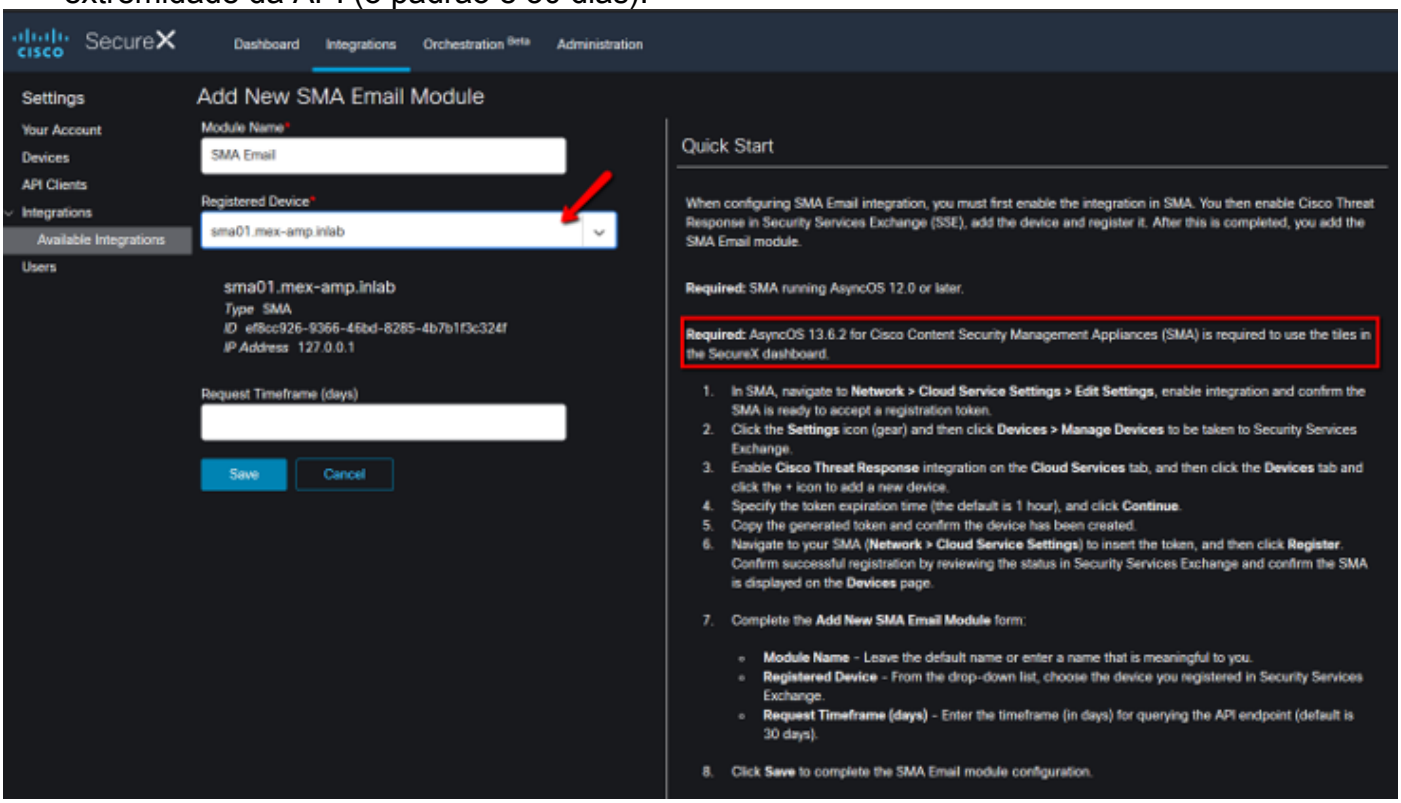
- Nome do módulo - Deixe o nome padrão ou insira um nome significativo para você.
- Dispositivo registrado - Na lista suspensa, escolha o dispositivo registrado no Security Services Exchange.
- Período de Solicitação (dias) - Insira o período (em dias) para a consulta de ponto de extremidade da API (o padrão é 30 dias).

Etapa 2. Clique em Salvar para concluir a configuração do módulo da Web SMA.

E-mail SMA

Etapa 1. Preencha o formulário Adicionar novo módulo de e-mail SMA.

- Nome do módulo - Deixe o nome padrão ou insira um nome significativo para você.
- Dispositivo registrado - Na lista suspensa, escolha o dispositivo registrado no Security Services Exchange.
- Período de Solicitação (dias) - Insira o período (em dias) para a consulta de ponto de extremidade da API (o padrão é 30 dias).



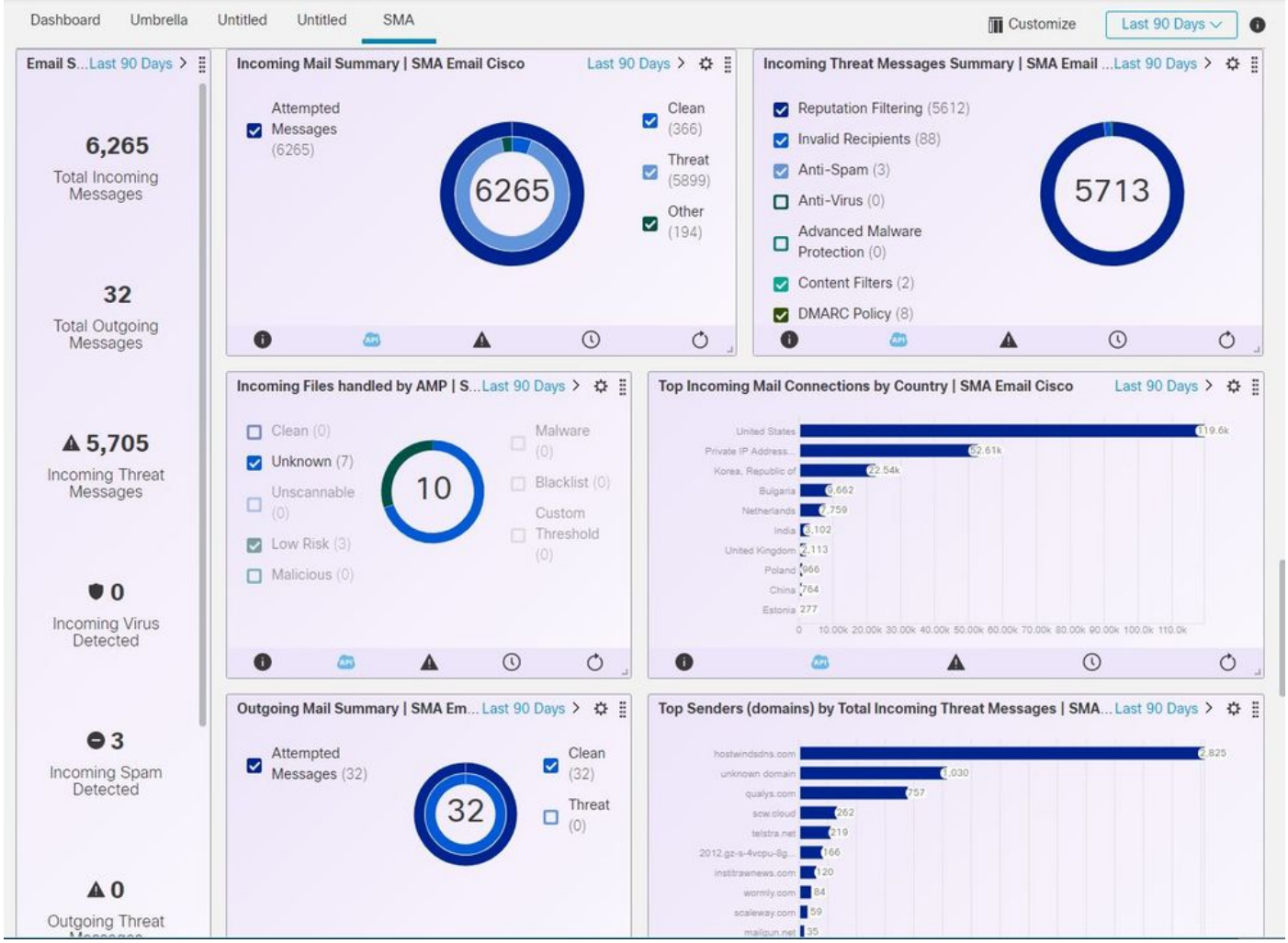
Se o nome do dispositivo SMA não estiver no menu suspenso, digite o nome no campo suspenso para pesquisá-lo.

Etapa 2. Clique em **Salvar** para concluir a configuração do módulo de e-mail SMA

Verificar

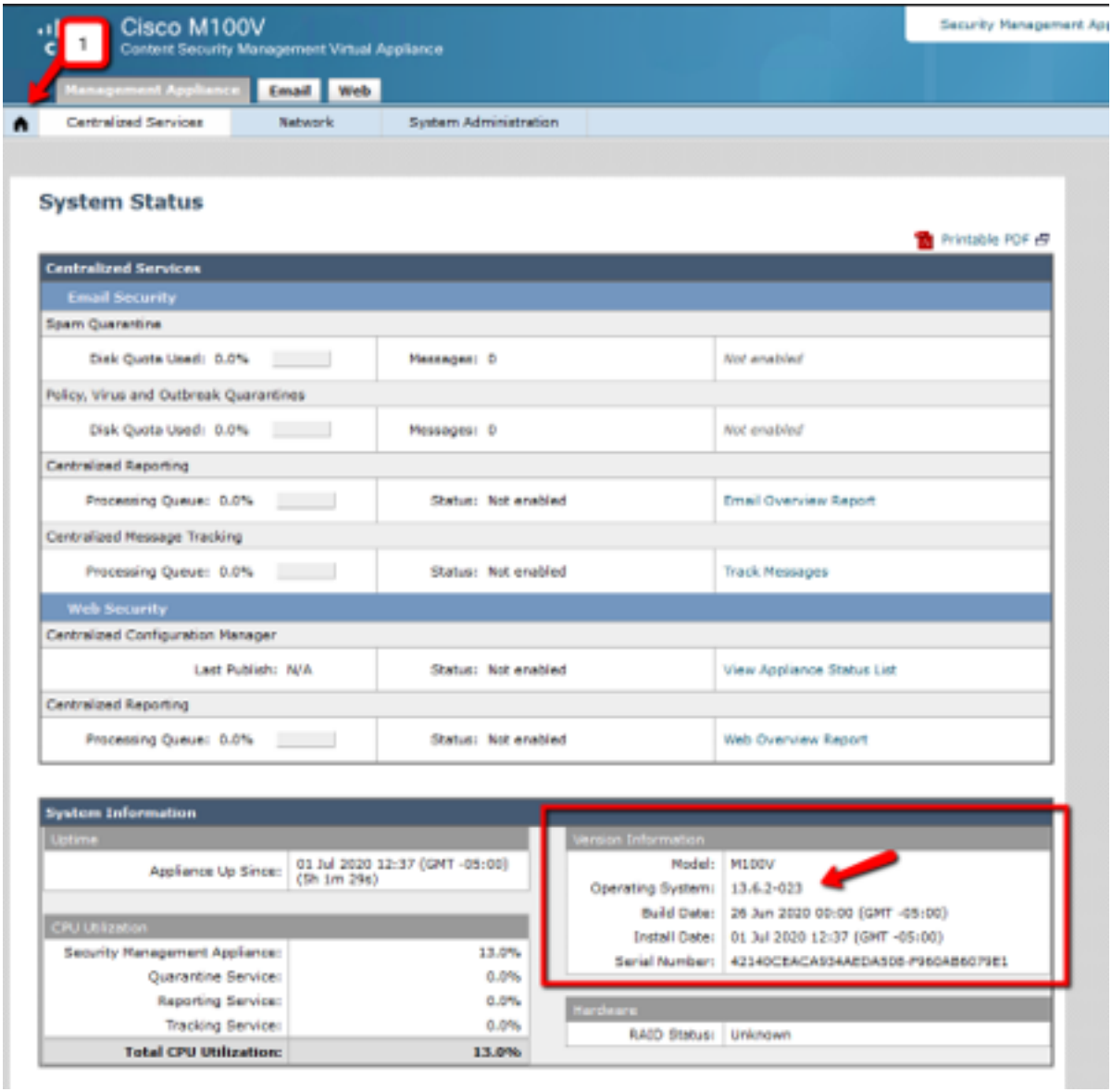
Etapa 1. Adicione um novo painel e adicione os blocos para ver as informações que você está interessado no seu módulo SMA

Você pode ver as informações do seu dispositivo refletidas nesta seção.



Etapa 2. Verificar a versão do SMA

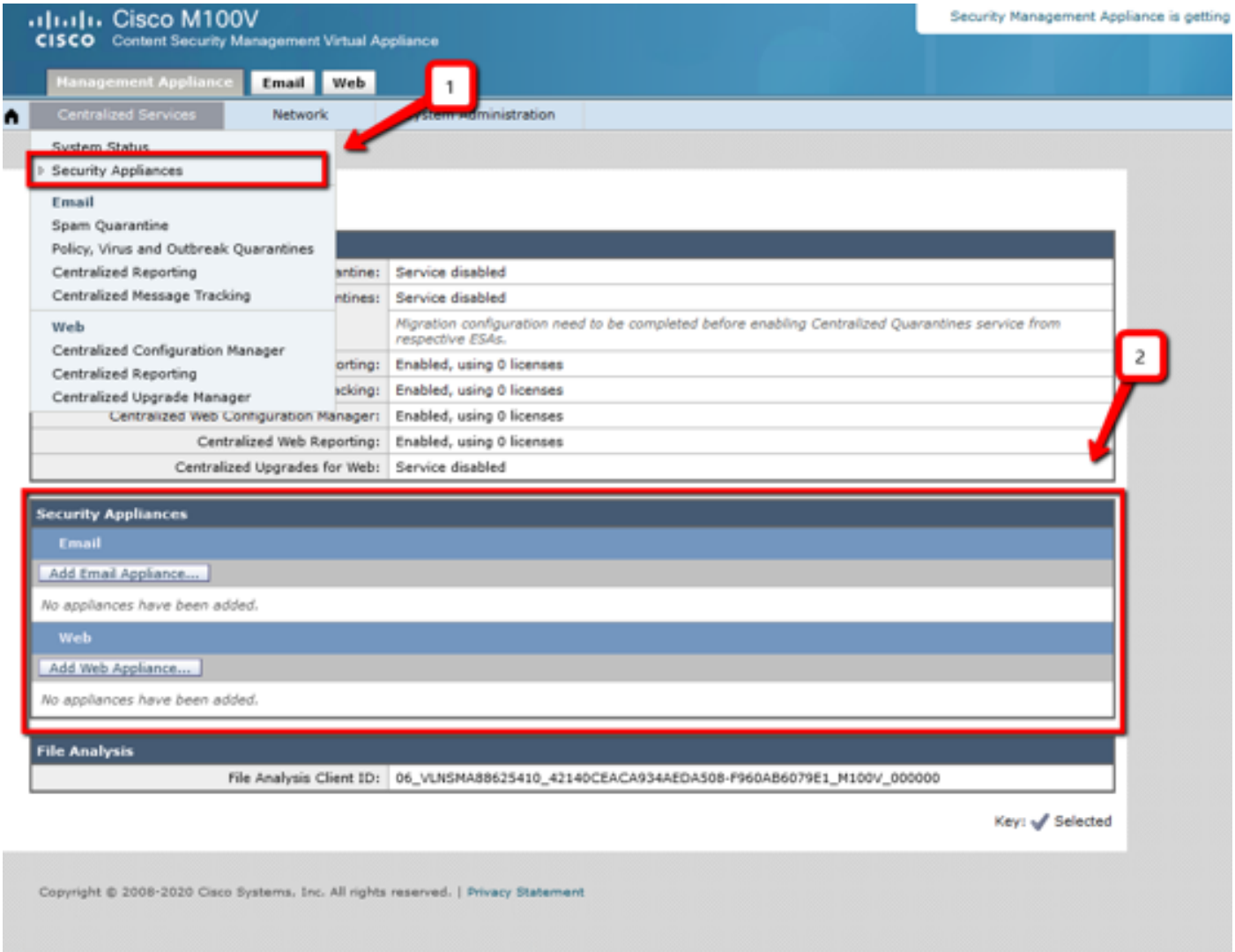
No SMA, navegue para **Home > Version Information (Página inicial > Informações da versão)**.



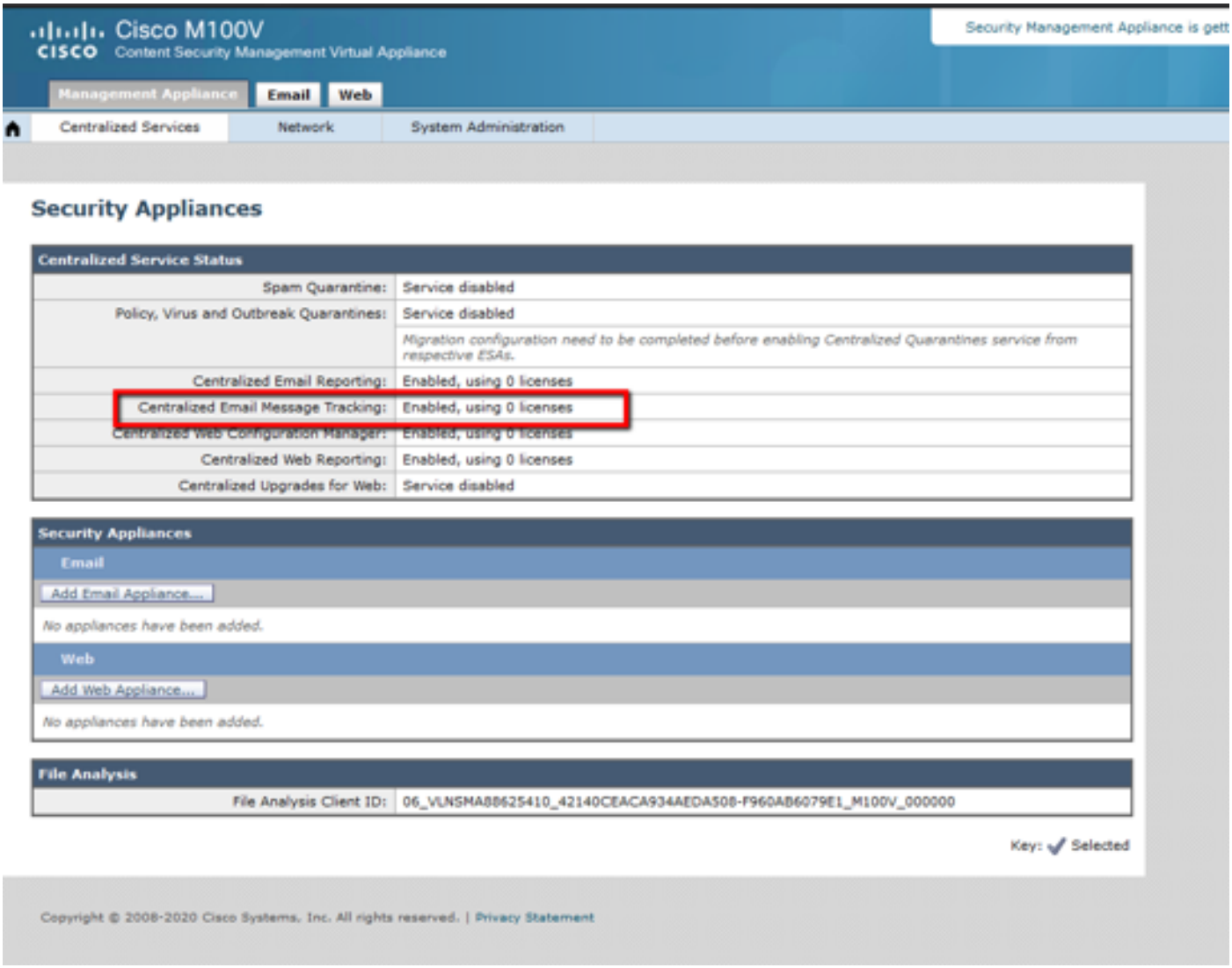
Se não houver dados disponíveis no SecureX após a integração. Você pode seguir as próximas etapas.

Etapa 1. Verificar o relatório dos dispositivos ESA/WSA para o SMA

No SMA, navegue para **Centralized Services > Security Appliances** e verifique se os dispositivos ESA/WSA aparecem em **Security Appliances**.



Etapa 2. Verifique se a licença SMA para **Rastreamento de mensagem de e-mail centralizado** está licenciada e habilitada em **Serviços centralizados > Dispositivos de segurança**.



Troubleshoot

Esta seção fornece as informações que você pode usar para solucionar problemas de sua configuração.

> **Tip**: Se você receber um erro de tempo limite enquanto executa investigações ou ao adicionar blocos ao SecureX, isso pode ser devido a um alto volume de informações enviadas de seus dispositivos. Tente reduzir a configuração **Request Timeframe (days) (Tempo de solicitação (dias))** na configuração do módulo.

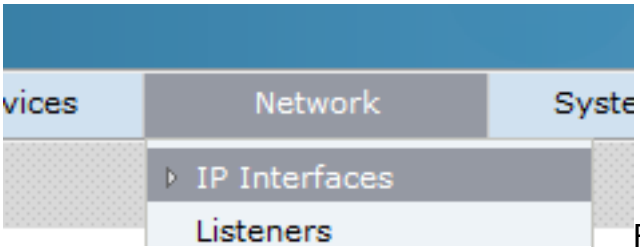
Comandos usados no console SMA SSH

- Para verificar a versão real e a licença do SMA, esses comandos podem ser usados >Showlicense>versão
- Logs de integração contendo eventos de registro >cat ctr_logs/ctr_logs.current
- Teste de conectividade com o portal SSE >telnet api-sse.cisco.com 443

Módulo SMA SecureX SMA tile / Resposta seguraX a ameaças mostrando o erro "Ocorreu um erro inesperado no módulo SMA"

O SMA requer a configuração de AsyncOS API HTTP e HTTPS habilitada na interface de gerenciamento para se comunicar com o portal SecureX/CTR.

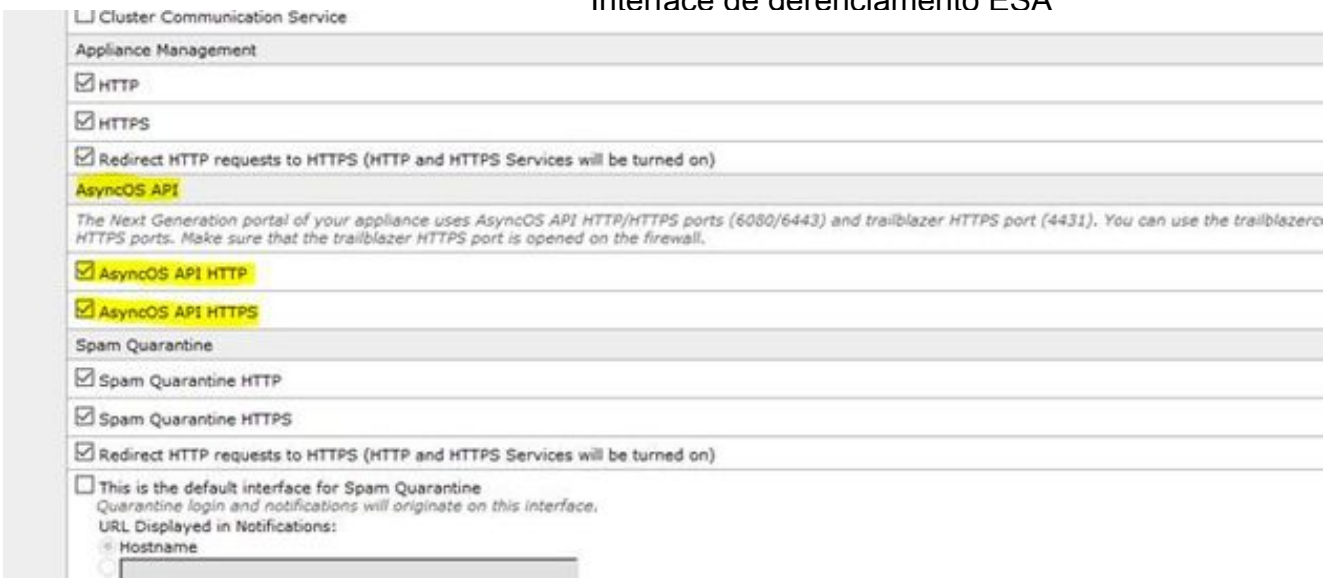
Para um SMA local, configure essa configuração a partir da GUI do portal SMA, vá para **Rede > Interfaces IP > Interface de gerenciamento > API AsyncOS** e ative HTTP e HTTPS.

1. 

Rede > Interfaces IP

2.

Interface de gerenciamento ESA

3. 

API assíncrona > HTTP e HTTPS

Para um CES (Cloud Based SMA), essa configuração precisará ser feita de back-end por um engenheiro do TAC SMA, ele exigirá acesso ao túnel de suporte do CES afetado.

Vídeo

Informações Relacionadas

- Você pode encontrar vídeos sobre como configurar suas integrações de produtos aqui.
- Se seu dispositivo não for gerenciado por um SMA, você poderá adicionar módulos para ESA ou WSA individualmente.
- Suporte Técnico e Documentação - Cisco Systems