

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](#)

[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)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. 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.

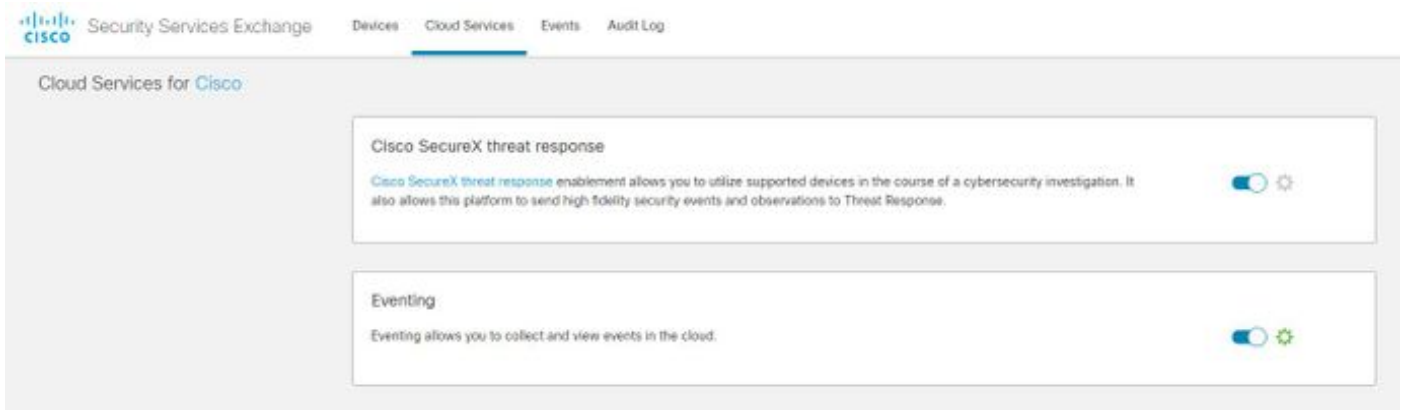
Configurar

integração de SMA

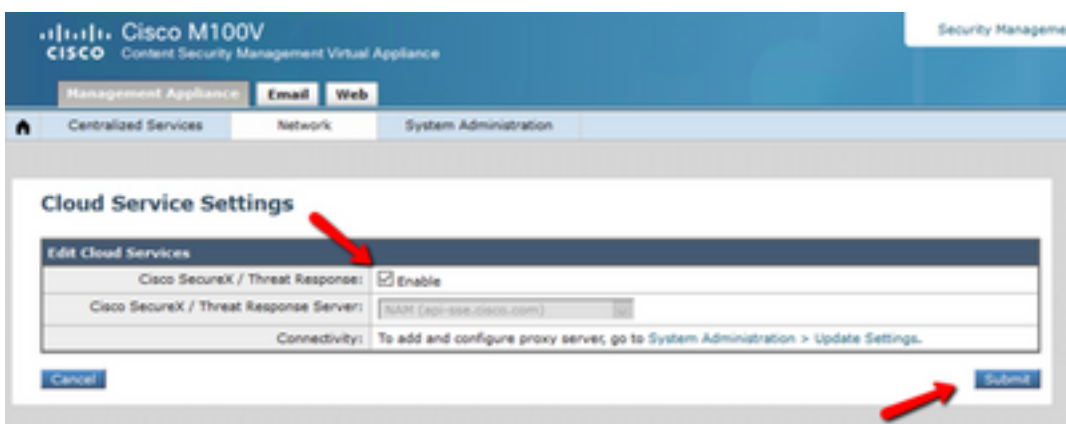
Etapa 1. No SMA, navegue até **Network > Cloud Service Settings > Edit Settings**, enable integration e confirme se o SMA está pronto para aceitar um token de registro.

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).

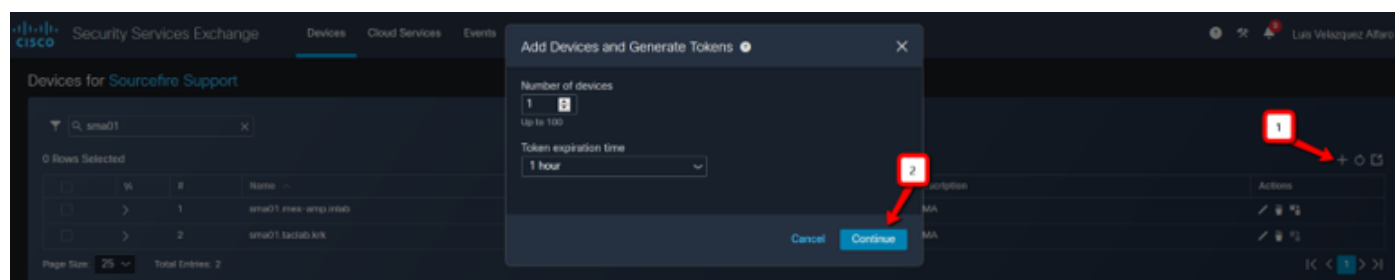


Etapa 4. Efetue login no portal SSE a partir da instância do SecureX.

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

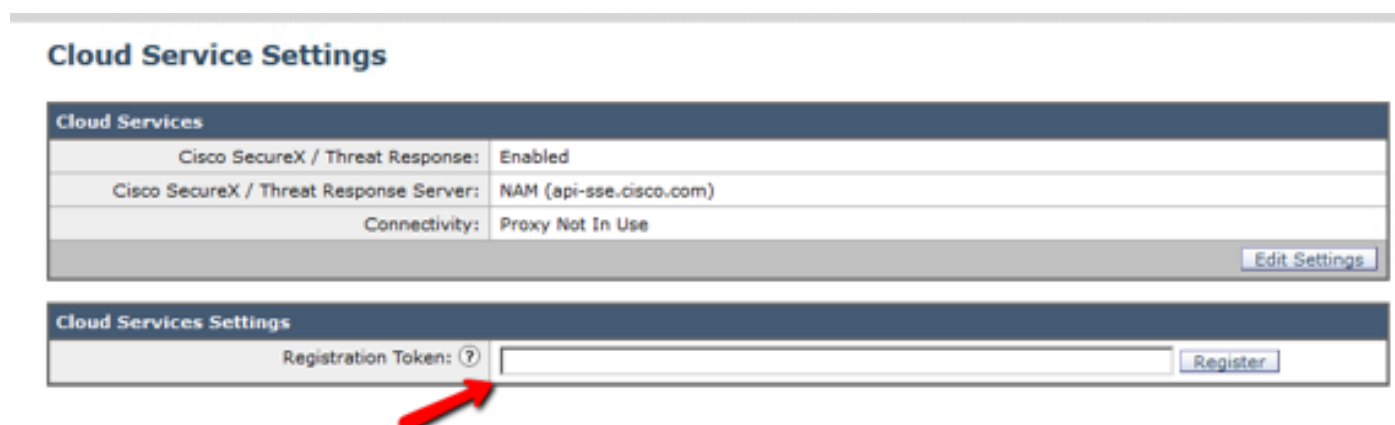
Etapa 6. Crie um novo token no portal SSE e especifique a hora de expiração do token (o padrão

é 1 hora) e clique em **Continuar**.

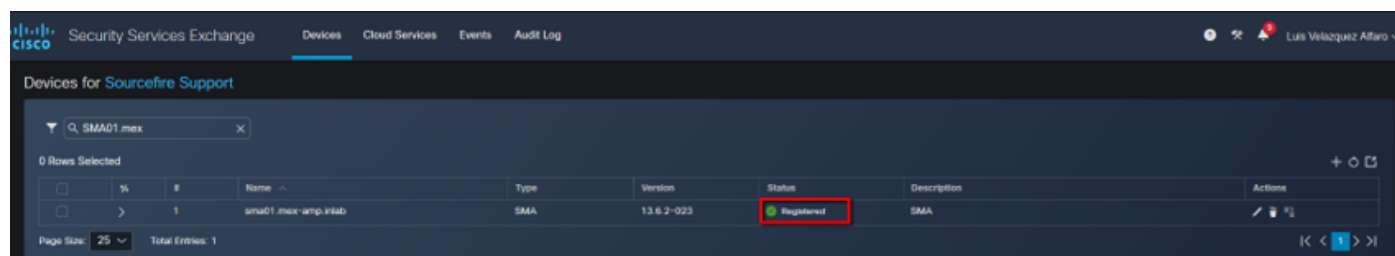


Passo 7. Copie o token gerado e confirme se o dispositivo foi criado.

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).

The screenshot shows the 'Add New SMA Email Module' configuration page in the Cisco SecureX interface. The left sidebar contains navigation links: Settings, Your Account, Devices, API Clients, Integrations (selected), Available Integrations, and Users. The main form area has the following fields:

- Module Name***: Text input with 'SMA Email' entered.
- Registered Device***: Dropdown menu showing 'sma01.mex-amp.inlab'. A red arrow points to this dropdown.
- Request Timeframe (days)**: Text input field.
- Buttons**: 'Save' and 'Cancel' buttons.

Below the form, device details are displayed:

- Device: sma01.mex-amp.inlab
- Type: SMA
- ID: ef8cc926-9366-46bd-8285-4b7b1f3c324f
- IP Address: 127.0.0.1

The right sidebar contains a 'Quick Start' section with instructions. A red box highlights a requirement: 'Required: AsyncOS 13.6.2 for Cisco Content Security Management Appliances (SMA) is required to use the tiles in the SecureX dashboard.'

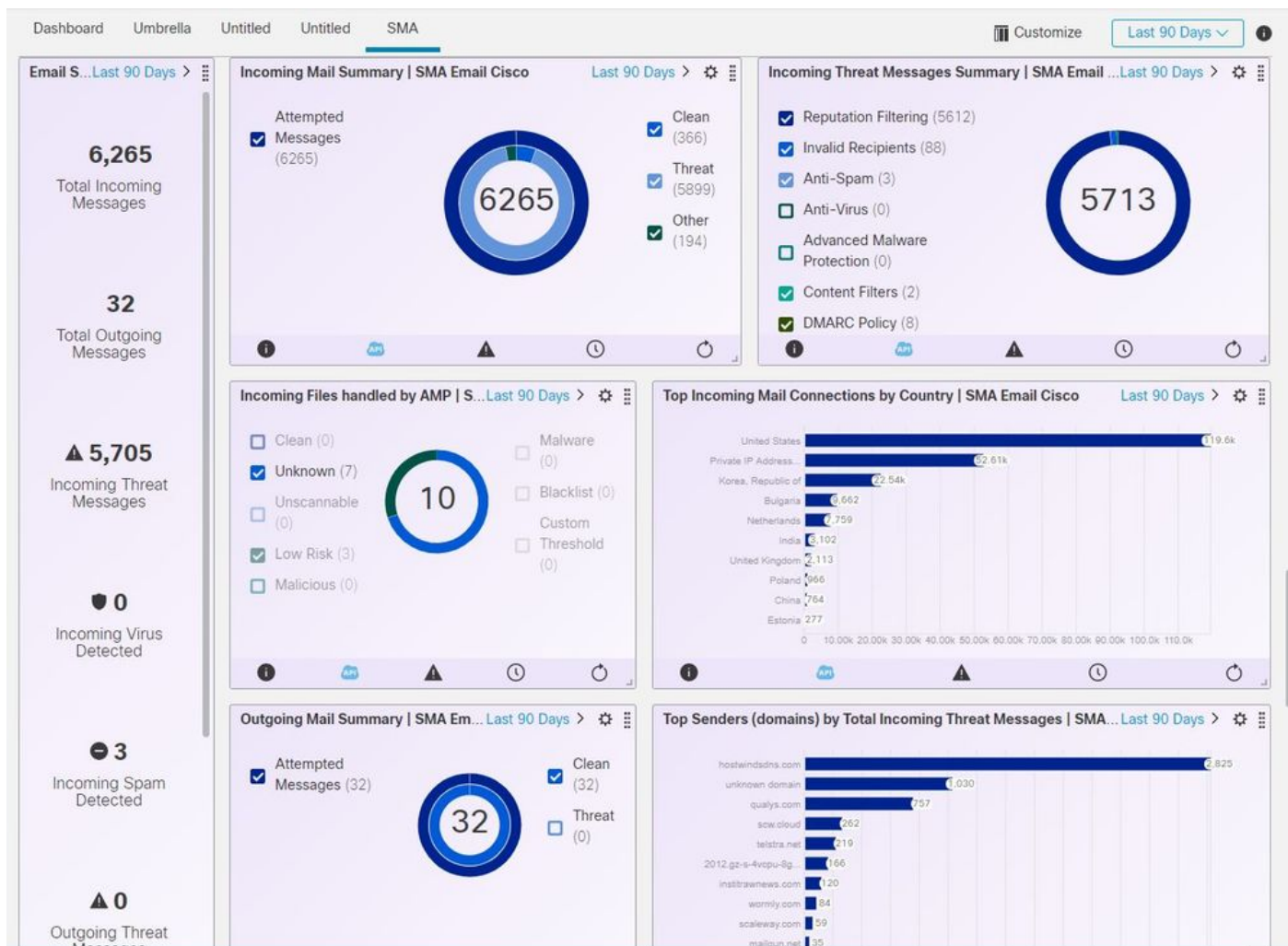
Se o nome do dispositivo SMA não estiver no menu suspenso, digite o nome no campo suspenso para pesquisá-lo.

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).

Cisco M100V
Content Security Management Virtual Appliance

Management Appliance | Email | Web

Centralized Services | Network | System Administration

System Status

Printable PDF

Centralized Services

Email Security

Spam Quarantine

Disk Quota Used: 0.0%	Messages: 0	Not enabled
-----------------------	-------------	-------------

Policy, Virus and Outbreak Quarantines

Disk Quota Used: 0.0%	Messages: 0	Not enabled
-----------------------	-------------	-------------

Centralized Reporting

Processing Queue: 0.0%	Status: Not enabled	Email Overview Report
------------------------	---------------------	-----------------------

Centralized Message Tracking

Processing Queue: 0.0%	Status: Not enabled	Track Messages
------------------------	---------------------	----------------

Web Security

Centralized Configuration Manager

Last Publish: N/A	Status: Not enabled	View Appliance Status List
-------------------	---------------------	----------------------------

Centralized Reporting

Processing Queue: 0.0%	Status: Not enabled	Web Overview Report
------------------------	---------------------	---------------------

System Information

Uptime

Appliance Up Since:	01 Jul 2020 12:37 (GMT -05:00) (5h 1m 29s)
---------------------	---

CPU Utilization

Security Management Appliance:	13.0%
Quarantine Service:	0.0%
Reporting Service:	0.0%
Tracking Service:	0.0%
Total CPU Utilization:	13.0%

Version Information

Model:	M100V
Operating System:	13.6.2-023
Build Date:	26 Jun 2020 00:00 (GMT -05:00)
Install Date:	01 Jul 2020 12:37 (GMT -05:00)
Serial Number:	42140CEACAS34AEDASDS-P960AB6079E1

Hardware

RASD Status:	Unknown
--------------	---------

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**.

Cisco M100V
Content Security Management Virtual Appliance

Management Appliance Email Web

Centralized Services Network System Administration

System Status

Security Appliances

Email

Spam Quarantine

Policy, Virus and Outbreak Quarantines

Centralized Reporting

Centralized Message Tracking

Web

Centralized Configuration Manager

Centralized Reporting

Centralized Upgrade Manager

Centralized Web Configuration Manager

Centralized Web Reporting

Centralized Upgrades for Web

Spam Quarantine:	Service disabled
Policy, Virus and Outbreak Quarantines:	Service disabled
Centralized Reporting:	Enabled, using 0 licenses
Centralized Message Tracking:	Enabled, using 0 licenses
Centralized Configuration Manager:	Enabled, using 0 licenses
Centralized Web Configuration Manager:	Enabled, using 0 licenses
Centralized Web Reporting:	Enabled, using 0 licenses
Centralized Upgrades for Web:	Service disabled

Security Appliances

Email

Add Email Appliance...

No appliances have been added.

Web

Add Web Appliance...

No appliances have been added.

File Analysis

File Analysis Client ID: 06_VLNSMA88625410_42140CEACA934AEDA508-F960AB6079E1_M100V_000000

Key: ✓ Selected

Copyright © 2008-2020 Cisco Systems, Inc. All rights reserved. | Privacy Statement

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**.

Cisco M100V
 Content Security Management Virtual Appliance

Security Management Appliance is getting...

Management Appliance
 Email
 Web

Centralized Services
 Network
 System Administration

Security Appliances

Centralized Service Status	
Spam Quarantine:	Service disabled
Policy, Virus and Outbreak Quarantines:	Service disabled
	Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.
Centralized Email Reporting:	Enabled, using 0 licenses
Centralized Email Message Tracking:	Enabled, using 0 licenses
Centralized Web Configuration Manager:	Enabled, using 0 licenses
Centralized Web Reporting:	Enabled, using 0 licenses
Centralized Upgrades for Web:	Service disabled

Security Appliances

Email

Add Email Appliance...

No appliances have been added.

Web

Add Web Appliance...

No appliances have been added.

File Analysis	
File Analysis Client ID:	06_VUNSMAB8625410_42140CEACA934AEDA508-F960AB6079E1_M100V_000000

Key: Selected

Copyright © 2008-2020 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

Troubleshoot

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

Dica: 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

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](#)