

Configure the SMA Integration With SecureX

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[SMA integration](#)

[SMA Web](#)

[SMA Email](#)

[Verify](#)

[Troubleshoot](#)

[Video](#)

[Related Information](#)

Introduction

This document describes the process to configure, verify, and troubleshoot the Content Security Management Appliance (SMA) integration with SecureX.

Prerequisites

Requirements

Cisco recommends that you have knowledge on these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- SMA running AsyncOS 13.6.2 (For SMA- Email Module)
- SMA running AsyncOS 12.5 (For SMA - Web Module)

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.

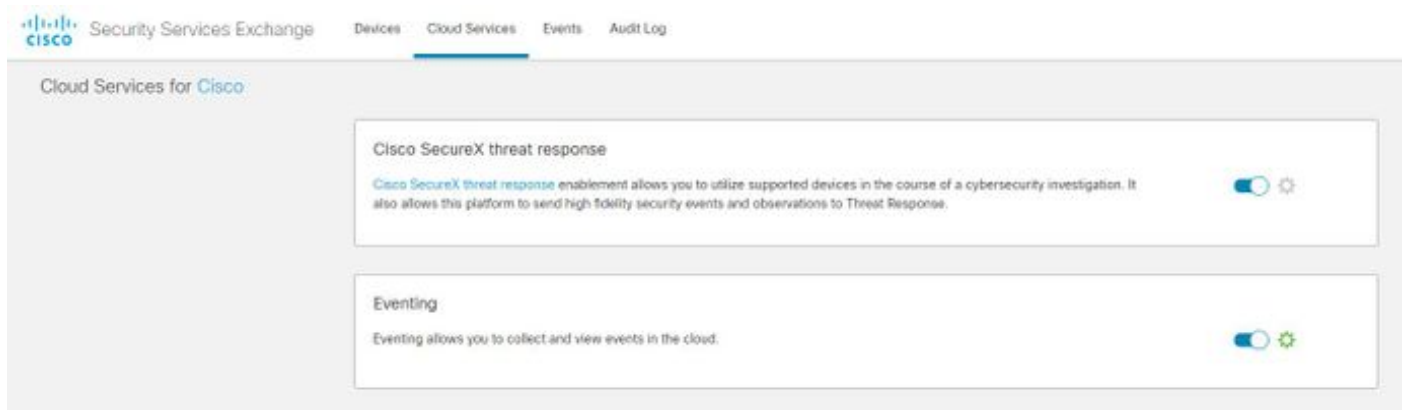
Configure

SMA integration

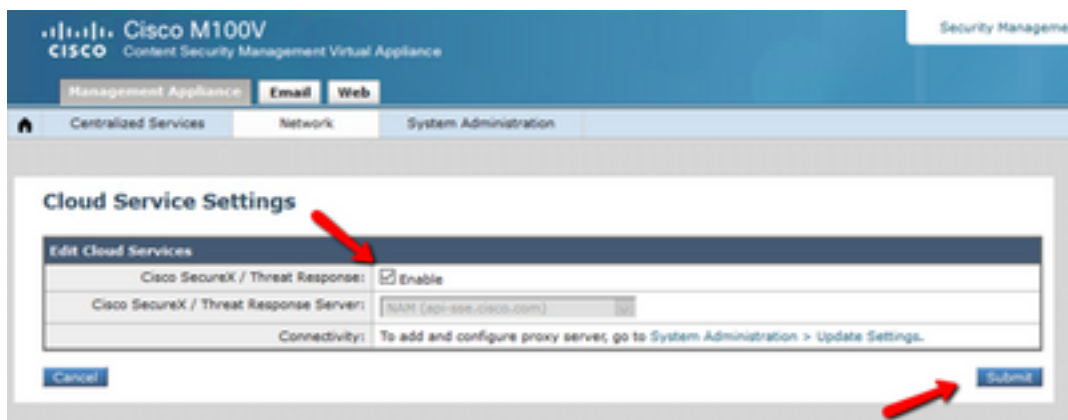
Step 1. In SMA, navigate to **Network > Cloud Service Settings > Edit Settings**, enable integration, and confirm the SMA is ready to accept a registration token.

Step 2. Click the Settings icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange (SSE).

Ensure all options are enabled under **Cloud Services**.



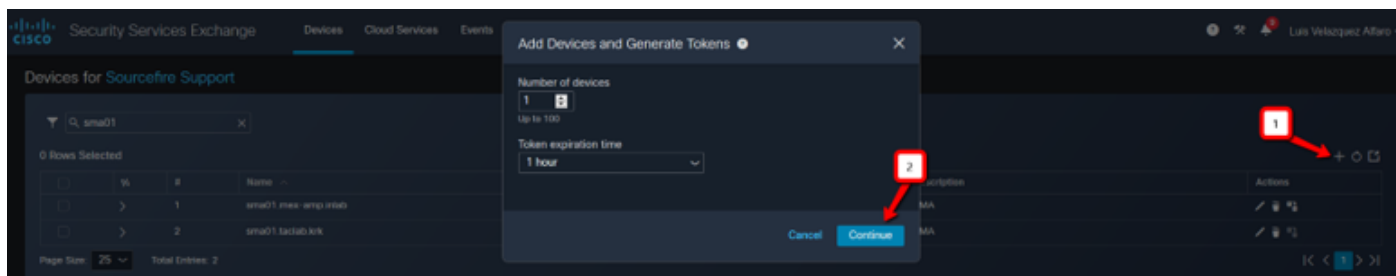
Step 3. Enable Cisco Threat Response integration on the Cloud Services tab, and then click the Devices tab and click the + icon to add a new device (requires SMA Admin account).



Step 4. Log into the SSE portal from SecureX instance.

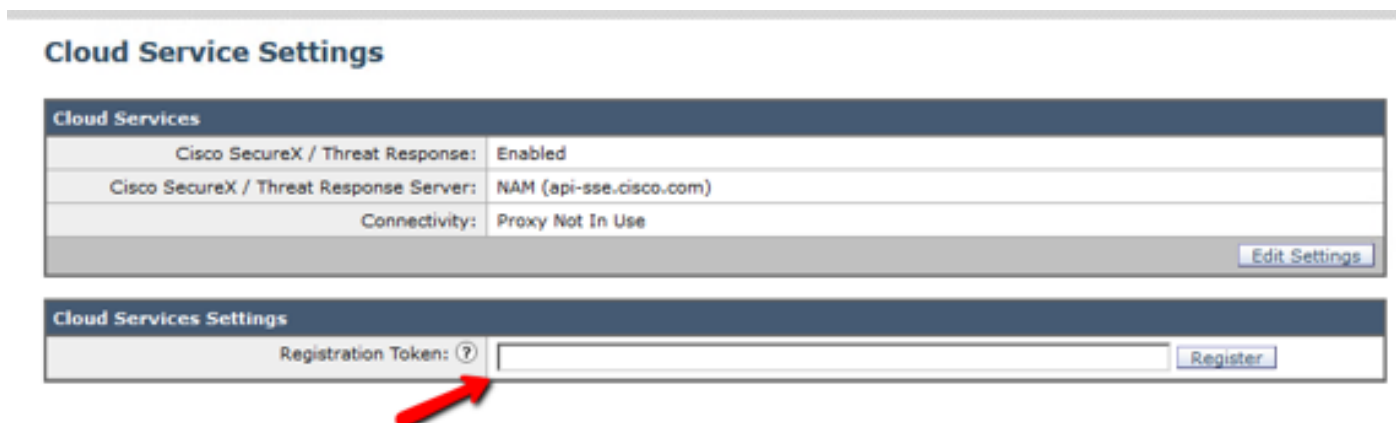
Step 5. From the Secure X portal navigate to **Integrations > Devices > Manage devices**

Step 6. Create a new token on the SSE portal and specify the token expiration time (the default is 1 hour), and click **Continue**.

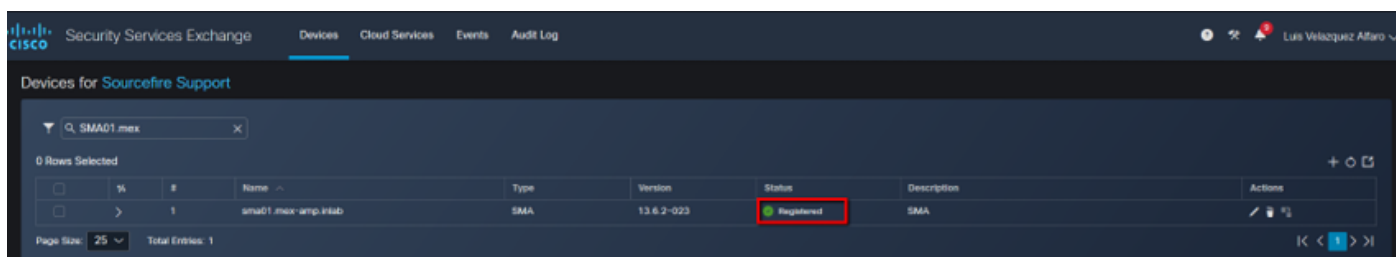


Step 7. Copy the generated token and confirm the device has been created.

Step 8. Navigate to your SMA (**Network > Cloud Service Settings**) to insert the token, and then click Register.



To confirm successful registration review the status in **Security Services Exchange** and confirm the SMA is displayed on the Devices page.



SMA Web

Step 1. Complete the Add New SMA Web Module form:

- Module Name - Leave the default name or enter a name that is meaningful to you.
- Registered Device - From the drop-down list, choose the device you registered in Security Services Exchange.
- Request Timeframe (days) - Enter the timeframe (in days) for the API endpoint query (default is 30 days).

Step 2. Click Save to complete the SMA Web module configuration.

SMA Email

Step 1. Complete the Add New SMA Email Module form.

- Module Name - Leave the default name or enter a name that is meaningful to you.
- Registered Device - From the drop-down list, choose the device you registered in Security Services Exchange.
- Request Timeframe (days) - Enter the timeframe (in days) for the API endpoint query (default is 30 days).

Add New SMA Email Module

Module Name*
SMA Email

Registered Device*
sma01.mex-amp.inlab

Request Timeframe (days)
[Input Field]

Save **Cancel**

Quick Start

When configuring SMA Email integration, you must first enable the integration in SMA. You then enable Cisco Threat Response in Security Services Exchange (SSE), add the device and register it. After this is completed, you add the SMA Email module.

Required: SMA running AsyncOS 12.0 or later.

Required: AsyncOS 13.6.2 for Cisco Content Security Management Appliances (SMA) is required to use the tiles in the SecureX dashboard.

1. In SMA, navigate to **Network > Cloud Service Settings > Edit Settings**, enable integration and confirm the SMA is ready to accept a registration token.
2. Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
3. Enable **Cisco Threat Response** integration on the **Cloud Services** tab, and then click the **Devices** tab and click the + icon to add a new device.
4. Specify the token expiration time (the default is 1 hour), and click **Continue**.
5. Copy the generated token and confirm the device has been created.
6. Navigate to your SMA (**Network > Cloud Service Settings**) to insert the token, and then click **Register**. Confirm successful registration by reviewing the status in Security Services Exchange and confirm the SMA is displayed on the **Devices** page.
7. Complete the **Add New SMA Email Module** form:
 - **Module Name** - Leave the default name or enter a name that is meaningful to you.
 - **Registered Device** - From the drop-down list, choose the device you registered in Security Services Exchange.
 - **Request Timeframe (days)** - Enter the timeframe (in days) for querying the API endpoint (default is 30 days).
8. Click **Save** to complete the SMA Email module configuration.

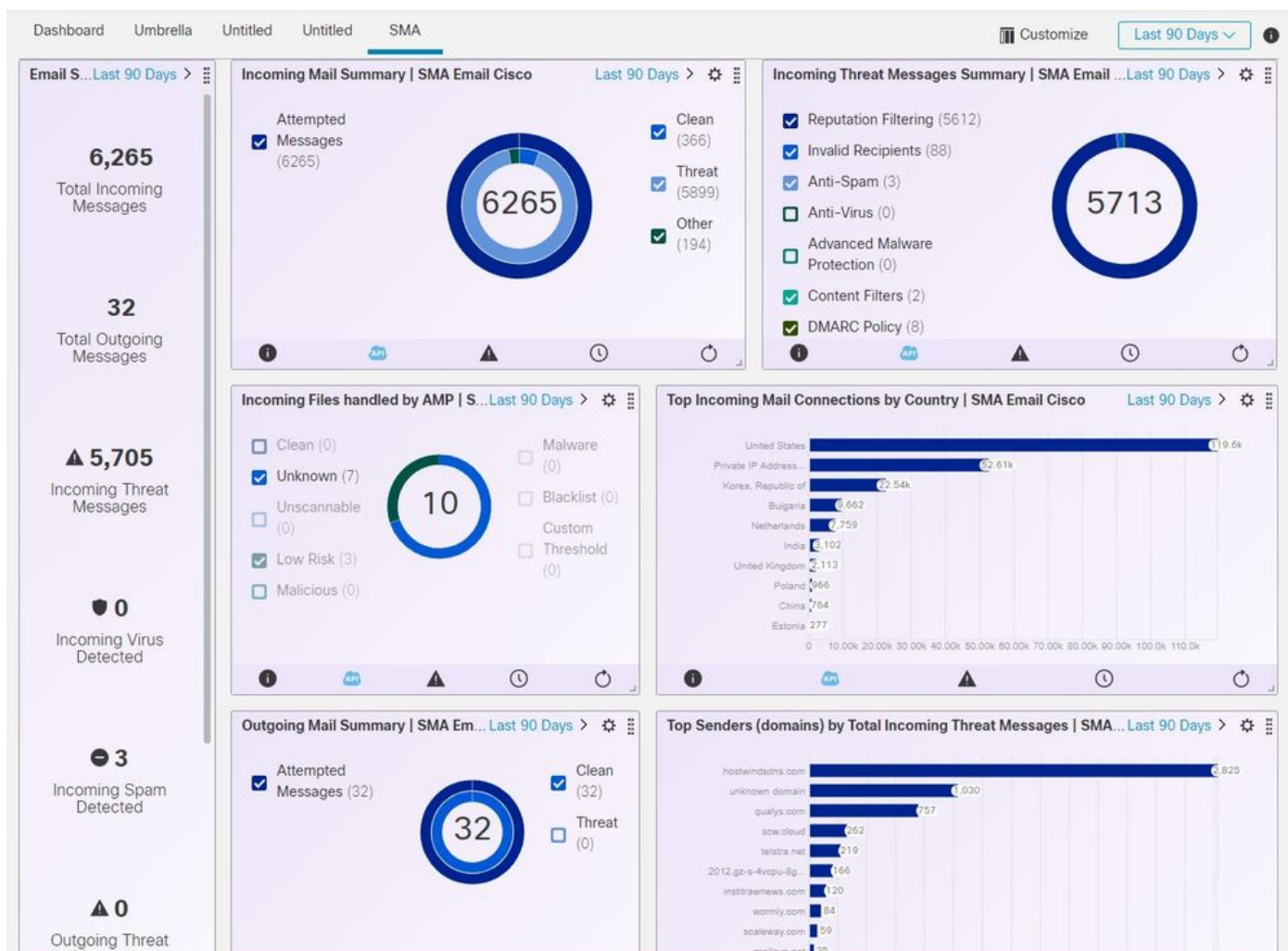
If the SMA device name is not on the dropdown menu, type the name on the dropdown field to search it.

Step 2. Click **Save** to complete the SMA Email module configuration

Verify

Step 1. Add a new Dashboard and add the Tiles to see the information you are interested in from your SMA module

You can see your device's information reflected in this section.



Step 2. Verify SMA version

On the SMA navigate to **Home > Version Information**.

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
--------------	---------

If there is no data available on SecureX after integration. You can follow the next steps.

Step 1. Verify ESA/WSA appliances report to the SMA

On the SMA navigate to **Centralized Services > Security Appliances** and verify the ESA/WSA devices appear under **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

Service disabled

Service disabled

Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.

Enabled, using 0 licenses

Enabled, using 0 licenses

Enabled, using 0 licenses

Enabled, using 0 licenses

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

Step 2. Verify the SMA license for **Centralized Email Message Tracking** is licensed and enabled under **Centralized Services > Security Appliances**.


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

This section provides the information you can use in order to troubleshoot your configuration.

Tip: If you receive a Timeout error while you perform investigations or while adding tiles to SecureX, it could be due to a high volume of information sent from your devices. Try to lower the **Request Timeframe (days)** setting in the module configuration.

Commands used on SMA SSH console

- To verify the actual version and license of the SMA, these commands can be used
>Showlicense>version
- Integration logs containin registration events >cat ctr_logs/ctr_logs.current
- Connectivity test to SSE protal >telnet api-sse.cisco.com 443

Video

Related Information

- You can find videos about how to configure your product integrations [here](#).
- If your device is not managed by an SMA you can add modules for [ESA](#) or [WSA](#) individually.
- [Technical Support & Documentation - Cisco Systems](#)