Configure the SMA Integration With SecureX

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[SMA integration](#)
[SMA Web](#)
[SMA Email](#)
[Verify](#)
[Troubleshoot](#)
[SecureX SMA tile / SecureX threat response SMA module showing error "There was an unexpected Error on the SMA module"](#)
[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.

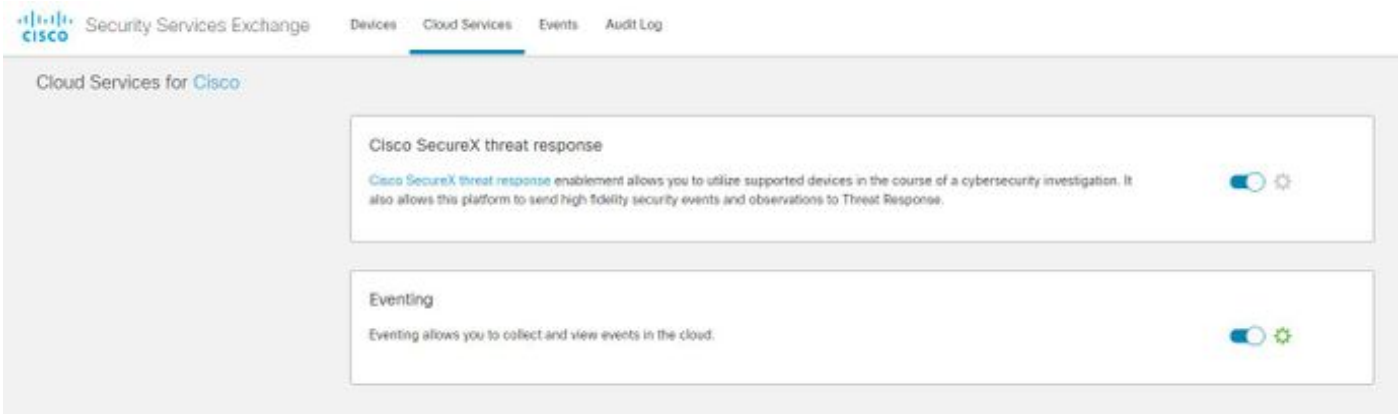
Configure

SMA integration

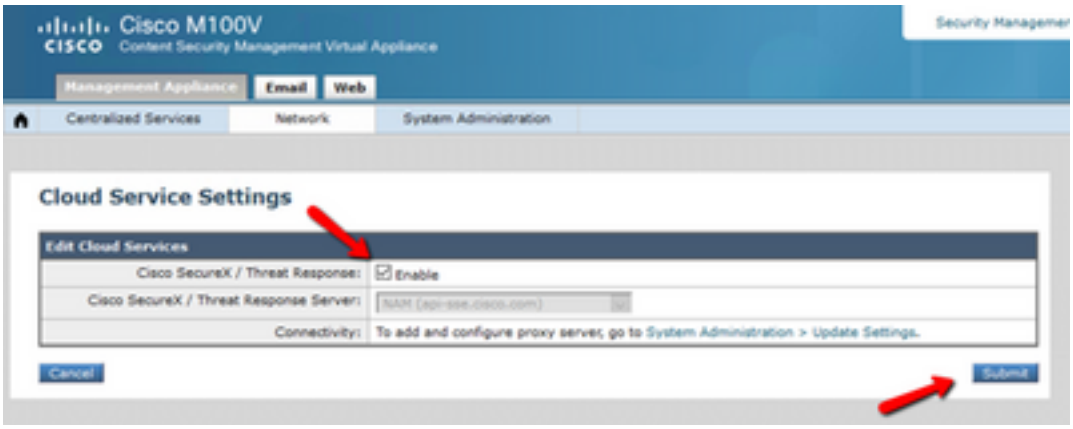
Step 1. In SMA, navigate to **Network > Cloud Service Settings > Edit Settings**, enable integration, and confirm the SMA is ready to accept a registration token.

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.



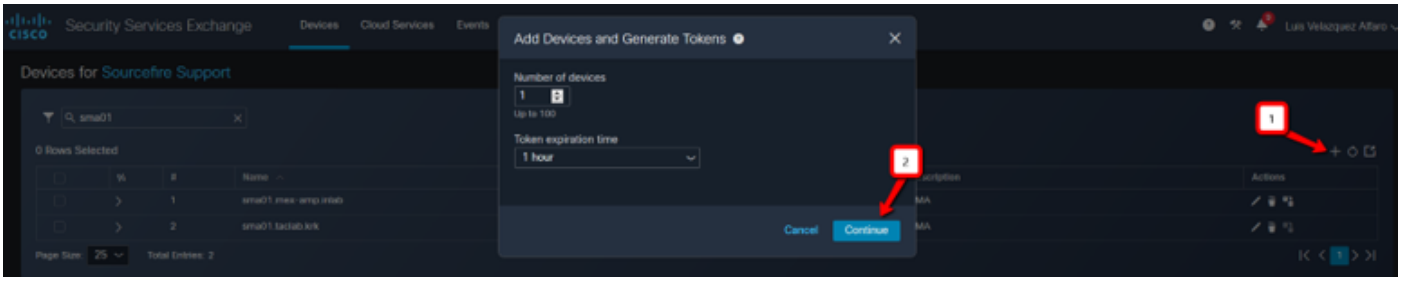
Step 3. Enable Cisco Threat Response integration on the Cloud Services tab, and then click the Devices tab and click the + icon to add a new device (requires SMA Admin account).



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

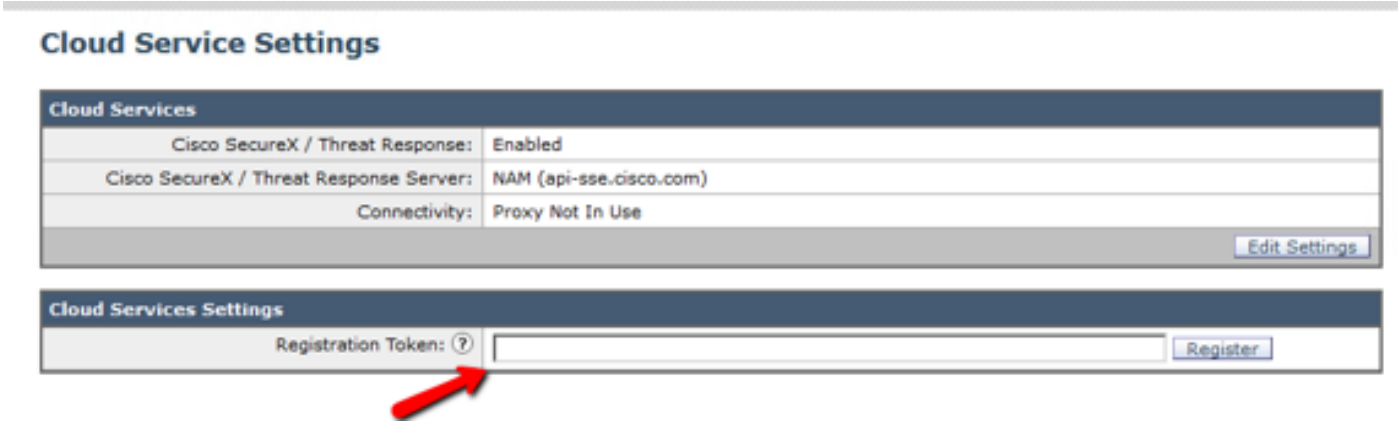
Step 5. From the Secure X portal navigate to **Integrations > Devices > Manage devices**

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

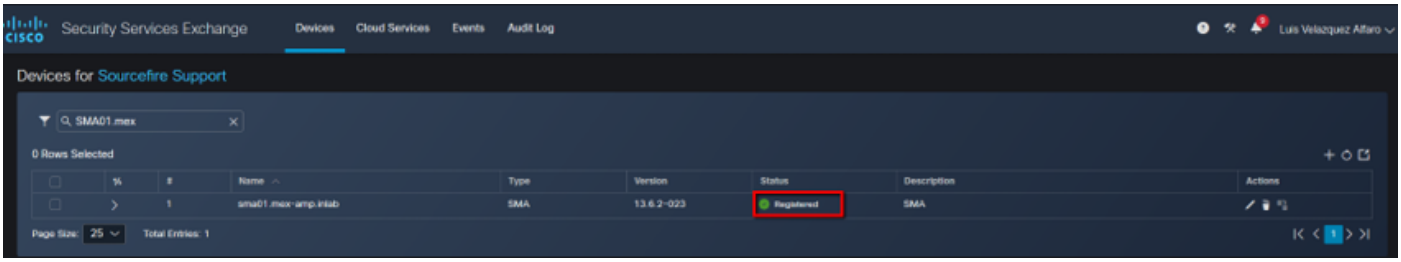


Step 7. Copy the generated token and confirm the device has been created.

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:

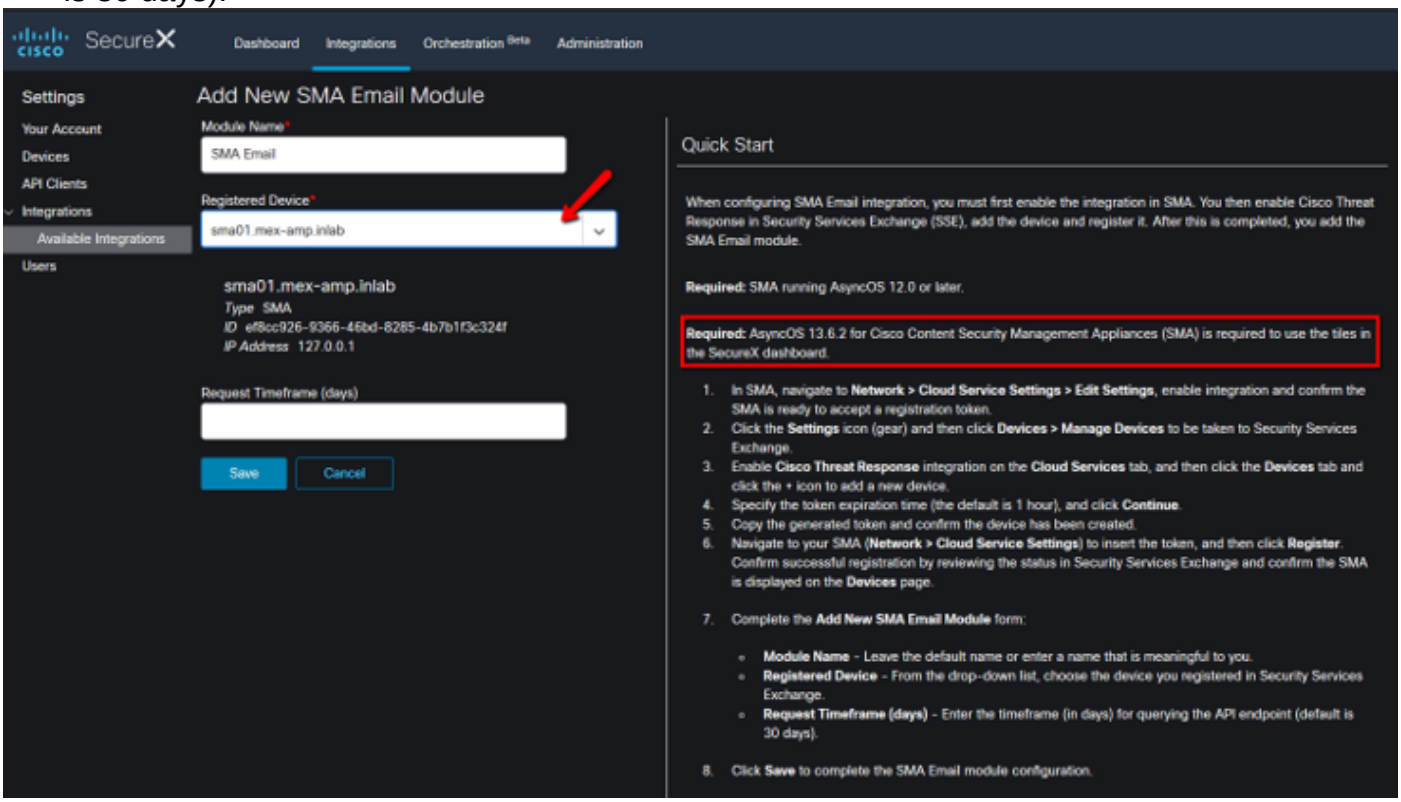
- Module Name - Leave the default name or enter a name that is meaningful to you.
- Registered Device - From the drop-down list, choose the device you registered in Security Services Exchange.
- Request Timeframe (days) - Enter the timeframe (in days) for the API endpoint query (default is 30 days).

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).



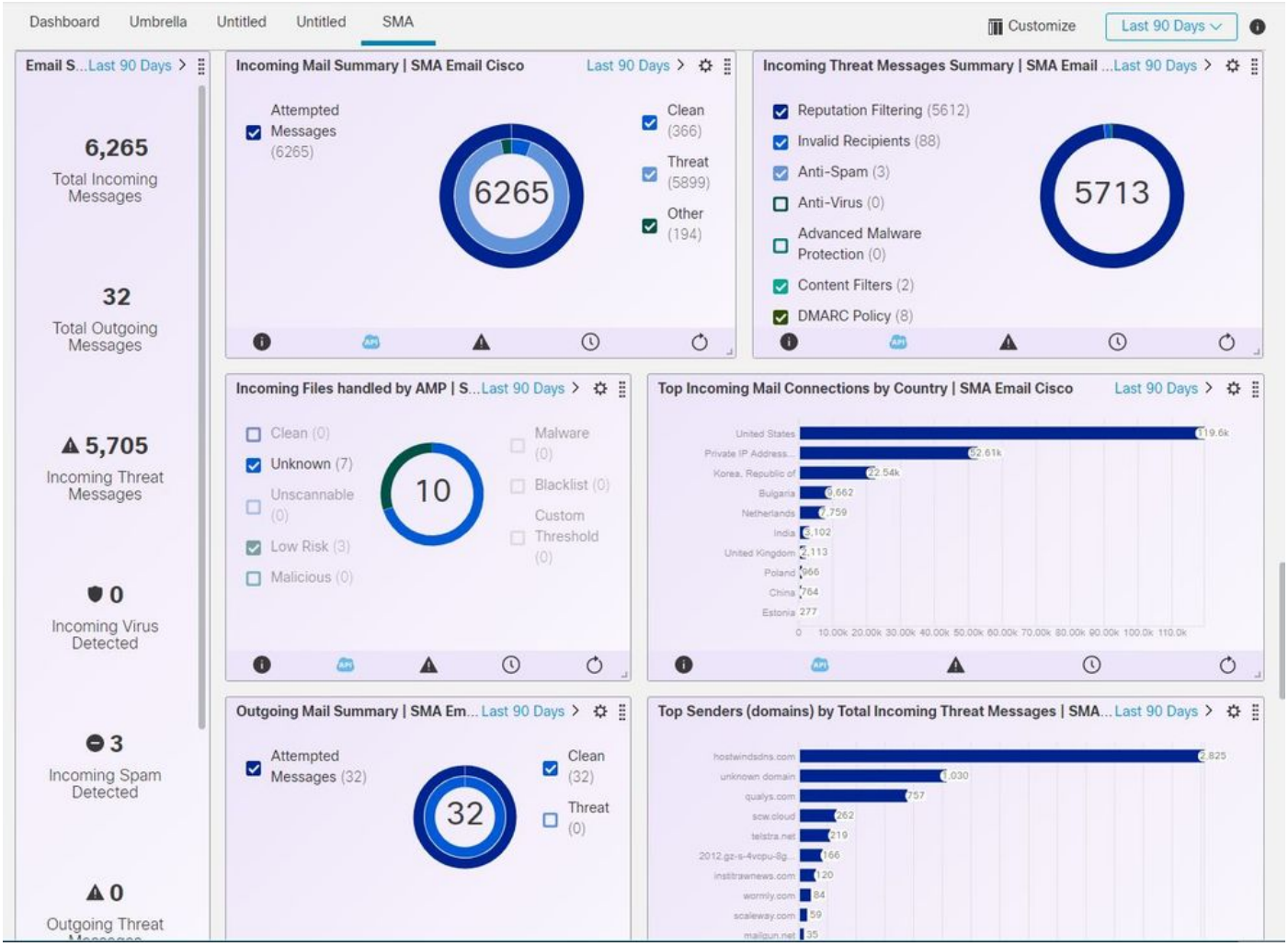
If the SMA device name is not on the dropdown menu, type the name on the dropdown field to search it.

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

Verify

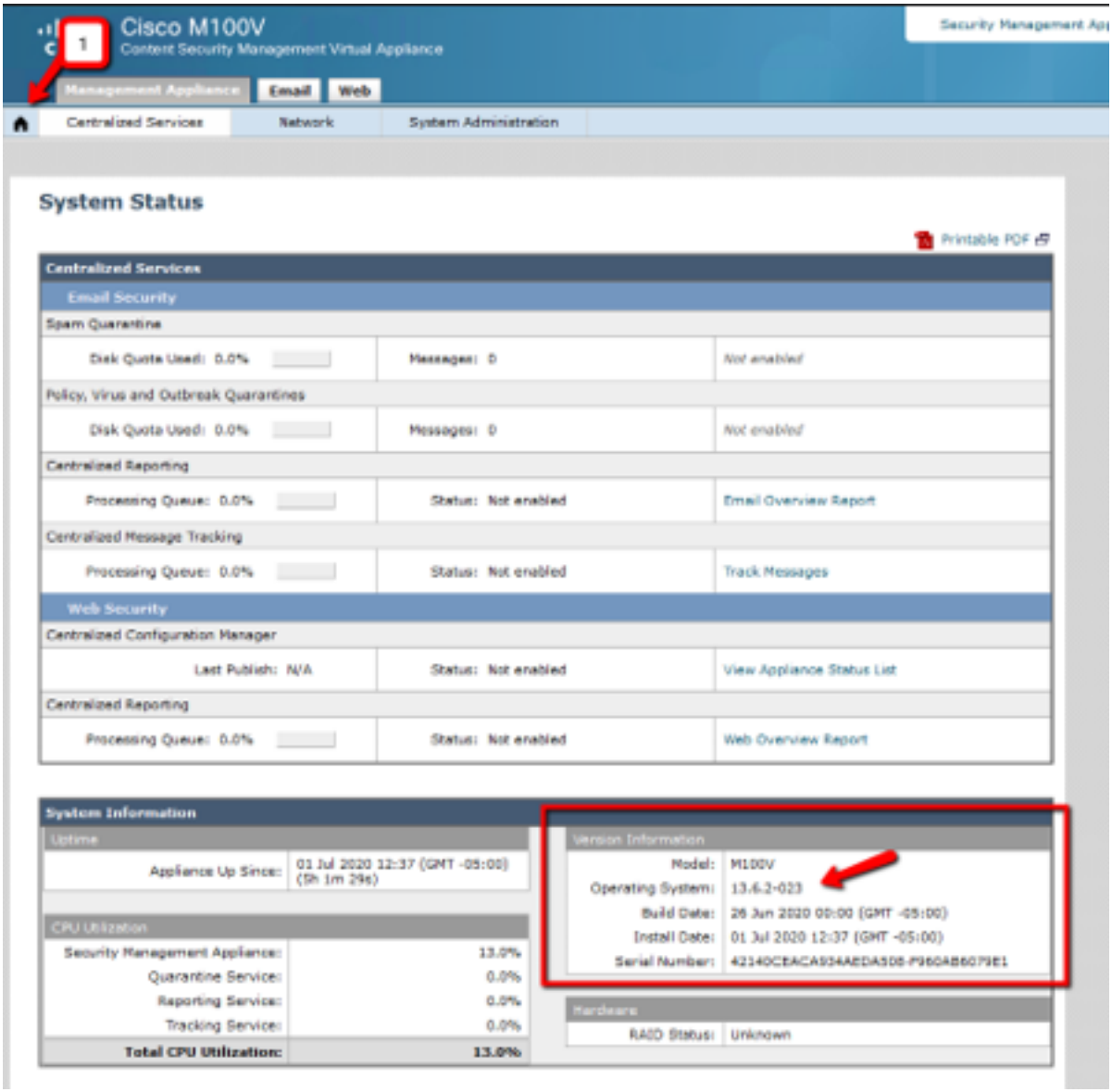
Step 1. Add a new Dashboard and add the Tiles to see the information you are interested in from your SMA module

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



Step 2. Verify SMA version

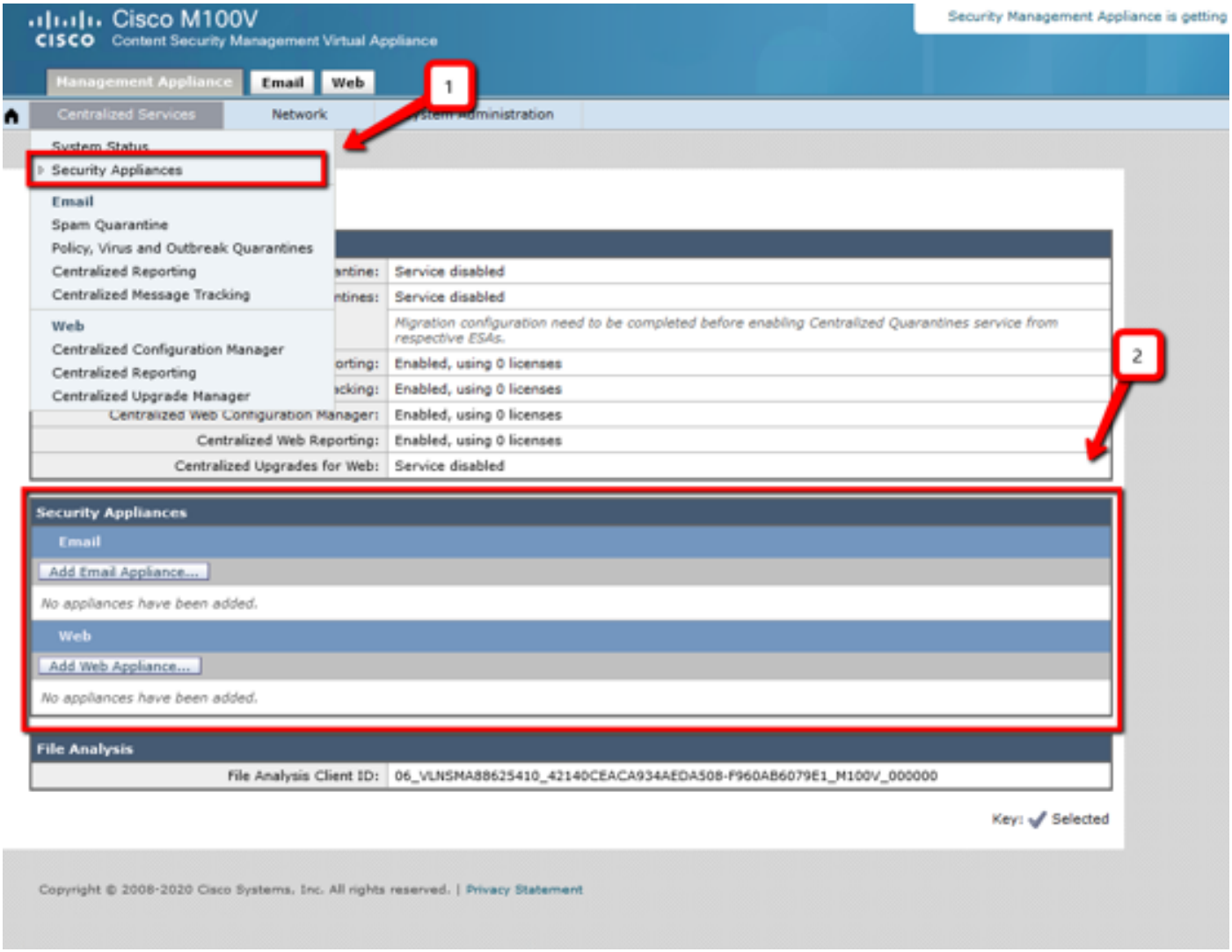
On the SMA navigate to **Home > Version Information**.



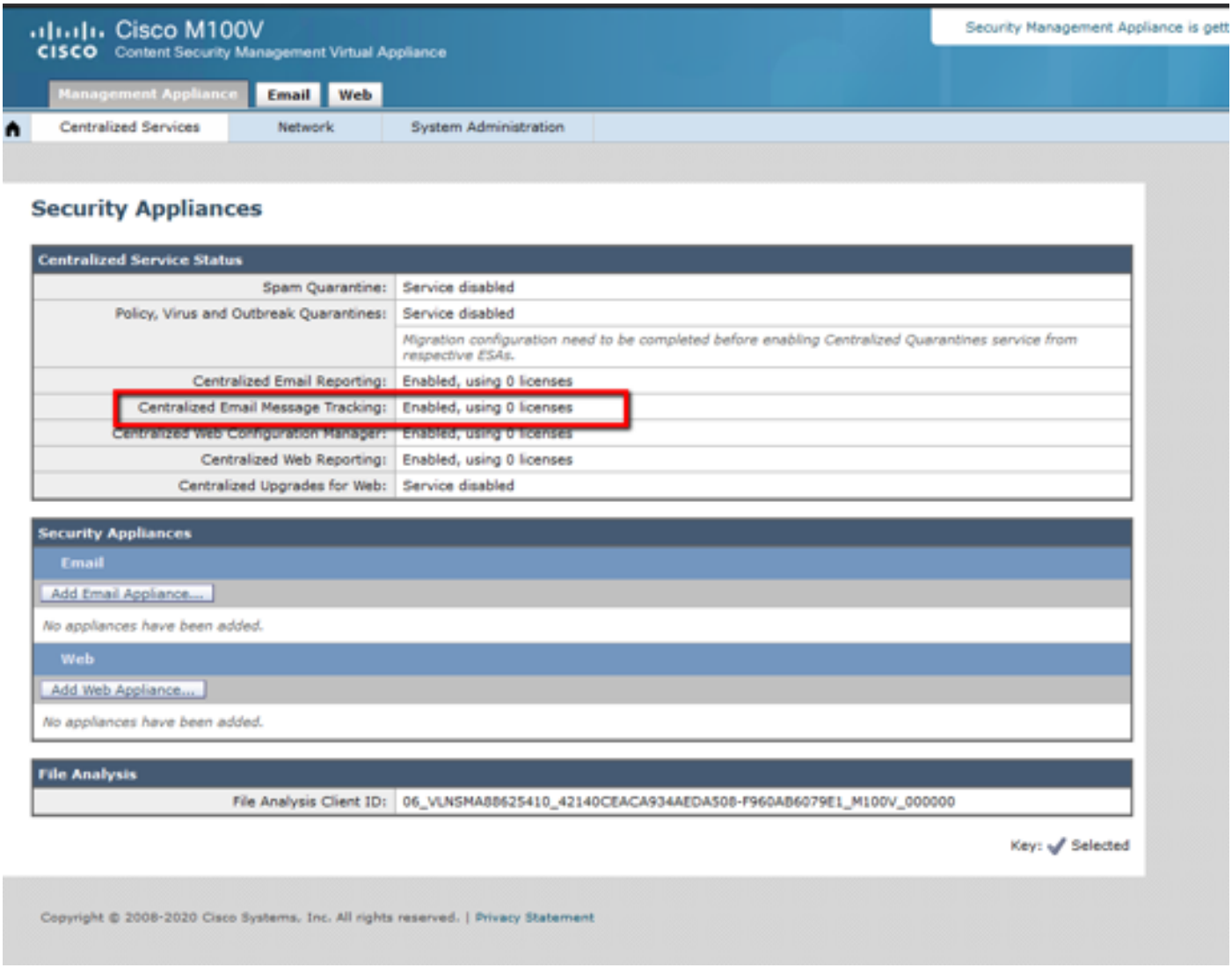
If there is no data available on SecureX after integration. You can follow the next steps.

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**.



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



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

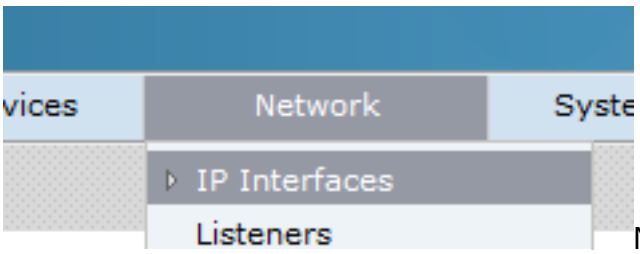
- To verify the actual version and license of the SMA, these commands can be used >Showlicense>version
- Integration logs containin registration events >cat ctr_logs/ctr_logs.current
- Connectivity test to SSE protal >telnet api-sse.cisco.com 443

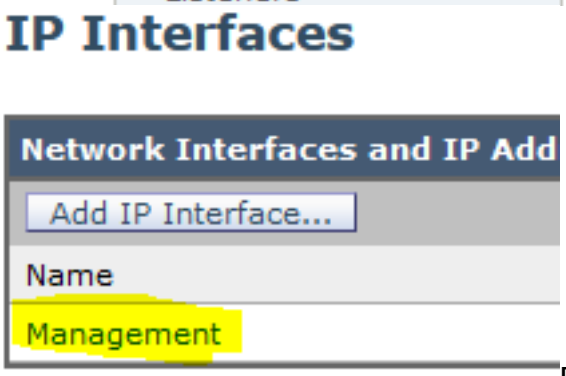
SecureX SMA tile / SecureX threat response SMA module showing error "There was an unexpected Error on the SMA module"

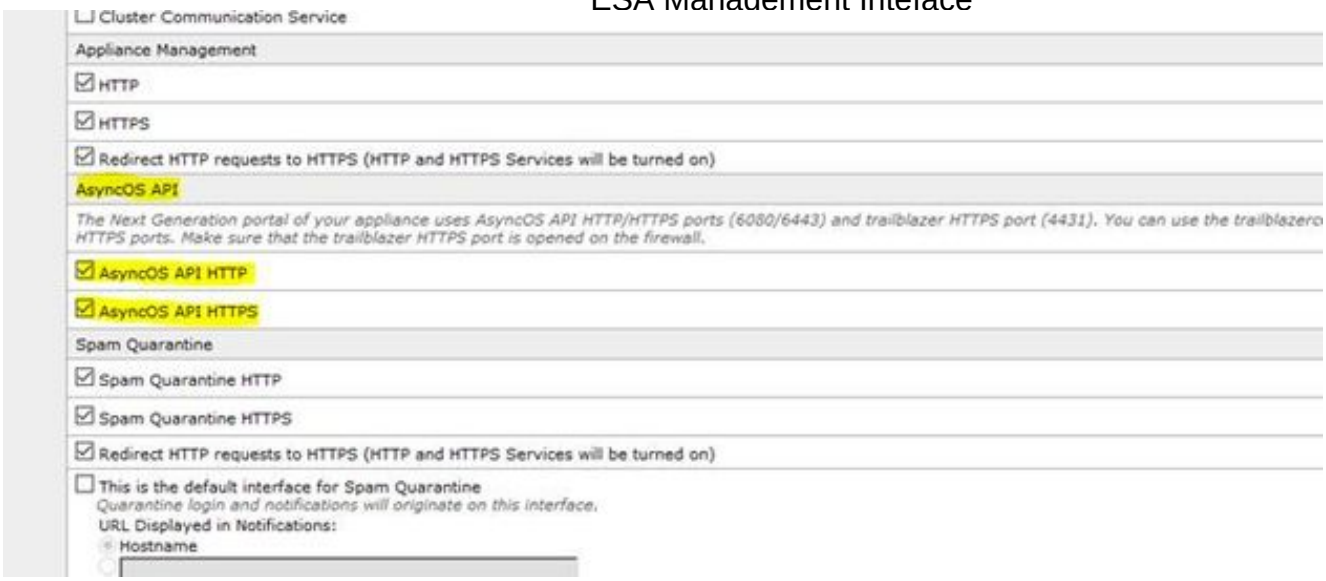
SMA requires AsyncOS API HTTP & HTTPS configuration enabled over the management

interface to communicate with SecureX/CTR portal.

For an on-prem SMA configure this setting from SMA portal GUI, go to **Network > IP Interfaces > Management interface > AsyncOS API** and enable HTTP and HTTPS.

1. 

Network > IP Interfaces


2. ESA Management Inteface
3. 

Async API > HTTP & HTTPS

For a CES (Cloud Based SMA) this configuration will need to be done from the backend by an SMA TAC engineer, it will require access to the support tunnel of the impacted CES.

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