

Configurazione dell'integrazione SMA con SecureX

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Integrazione SMA](#)

[Web SMA](#)

[E-mail SMA](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Riquadro SMA SecureX / modulo SMA di risposta alla minaccia SecureX con l'errore "Errore imprevisto nel modulo SMA"](#)

[Video](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il processo di configurazione, verifica e risoluzione dei problemi di integrazione di Content Security Management Appliance (SMA) con SecureX.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- SMA con AsyncOS 13.6.2 (per SMA- Email Module)
- SMA con AsyncOS 12.5 (per SMA - modulo Web)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

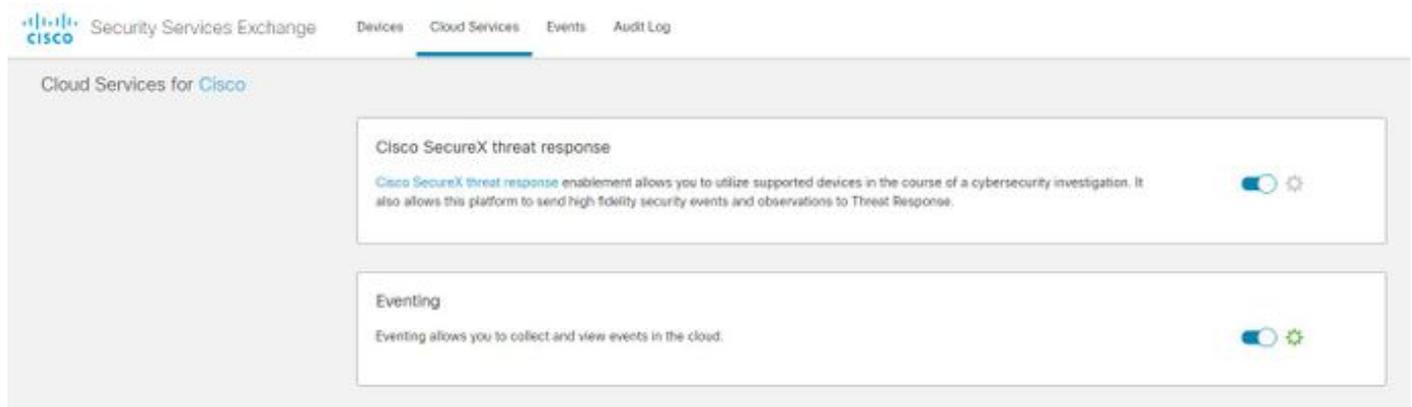
Configurazione

Integrazione SMA

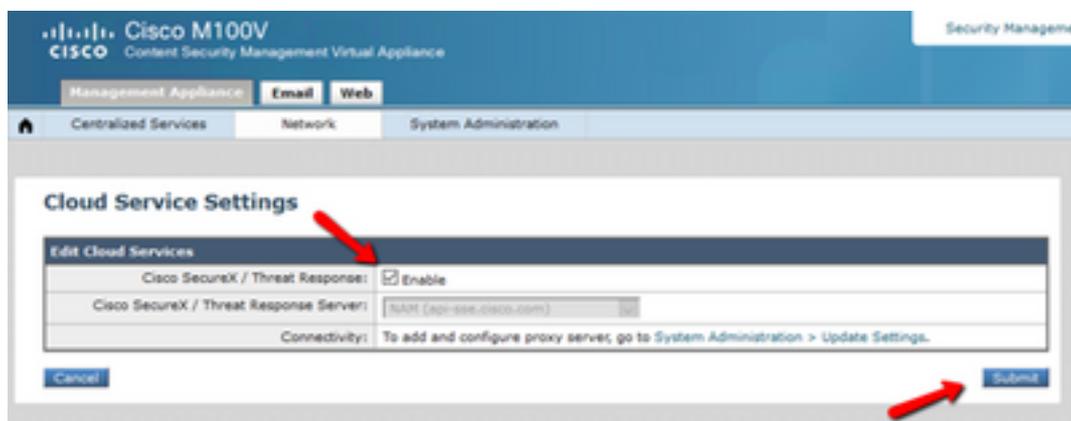
Passaggio 1. In SMA, selezionare **Rete > Impostazioni servizio cloud > Modifica impostazioni**, abilitare l'integrazione e confermare che SMA è pronto ad accettare un token di registrazione.

Passaggio 2. Fare clic sull'icona Impostazioni (gear), quindi fare clic su **Dispositivi > Gestisci dispositivi** da portare a Security Services Exchange (SSE).

Assicurarsi che tutte le opzioni siano abilitate in **Cloud Services**.



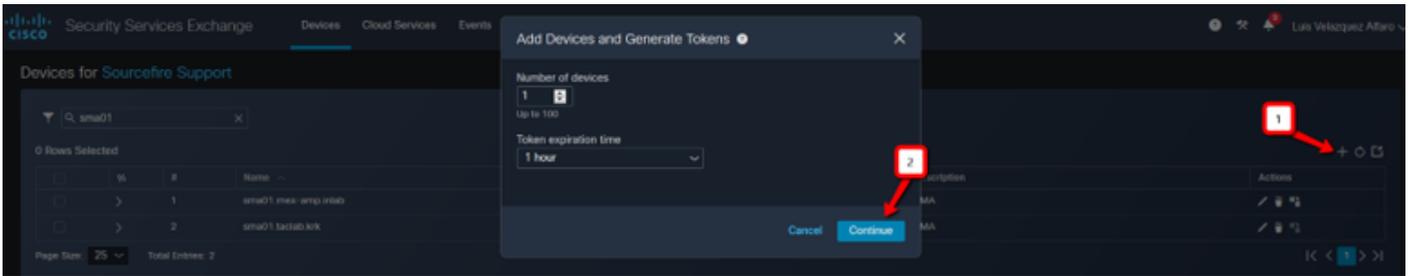
Passaggio 3. Abilitare l'integrazione di Cisco Threat Response nella scheda Servizi cloud, quindi fare clic sulla scheda Dispositivi e sull'icona + per aggiungere un nuovo dispositivo (è necessario l'account SMA Admin).



Passaggio 4. Accedere al portale SSE dall'istanza di SecureX.

Passaggio 5. Dal portale Secure X passare a **Integrations > Devices > Manage devices** (**Integrazioni > Dispositivi > Gestione dispositivi**)

Passaggio 6. Creare un nuovo token sul portale SSE e specificare l'ora di scadenza del token (il valore predefinito è 1 ora), quindi fare clic su **Continua**.



Passaggio 7. Copiare il token generato e verificare che il dispositivo sia stato creato.

Passaggio 8. Passare al proprio SMA (**Rete > Impostazioni servizio cloud**) per inserire il token, quindi fare clic su **Registra**.

Cloud Service Settings

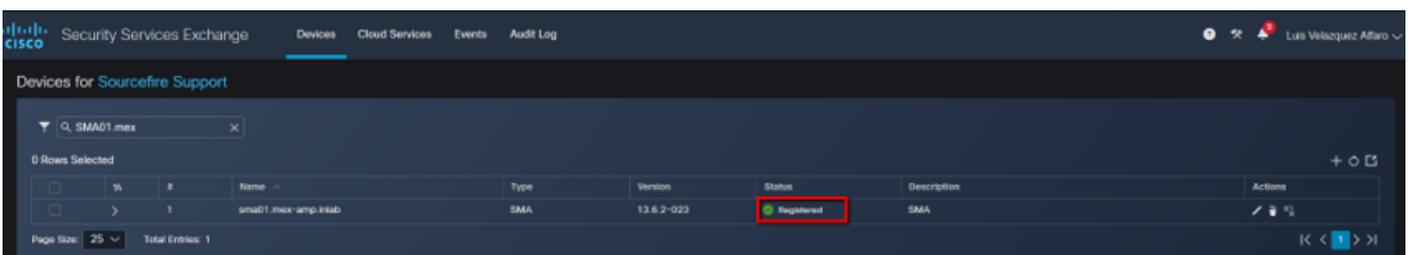
Cloud Services	
Cisco SecureX / Threat Response:	Enabled
Cisco SecureX / Threat Response Server:	NAM (api-sse.cisco.com)
Connectivity:	Proxy Not In Use

[Edit Settings](#)

Cloud Services Settings	
Registration Token: ?	<input type="text"/>

[Register](#)

Per confermare la riuscita della registrazione, controllare lo stato in **Security Services Exchange** e verificare che l'SMA sia visualizzato nella pagina **Dispositivi**.



Web SMA

Passaggio 1. Completare il modulo **Aggiungi nuovo modulo Web SMA**:

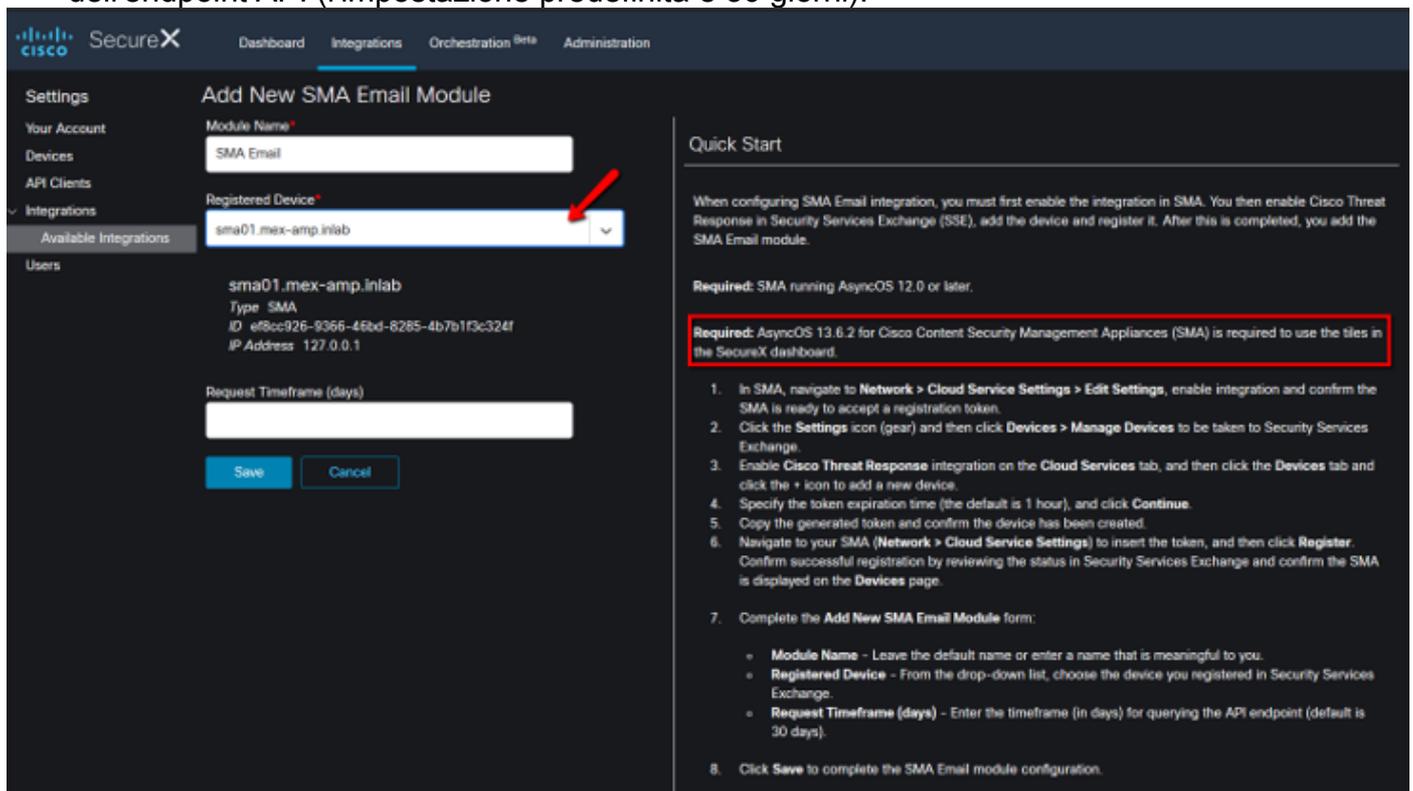
- Nome modulo: lasciare il nome predefinito o immettere un nome significativo.
- Periferica registrata: dall'elenco a discesa, scegliere la periferica registrata in Security Services Exchange.
- Timeframe richiesta (giorni): immettere l'intervallo di tempo (in giorni) per la query dell'endpoint API (l'impostazione predefinita è 30 giorni).

Passaggio 2. Fare clic su **Salva** per completare la configurazione del modulo Web SMA.

E-mail SMA

Passaggio 1. Completare il modulo Aggiungi nuovo modulo di posta elettronica SMA.

- Nome modulo: lasciare il nome predefinito o immettere un nome significativo.
- Periferica registrata: dall'elenco a discesa, scegliere la periferica registrata in Security Services Exchange.
- Timeframe richiesta (giorni): immettere l'intervallo di tempo (in giorni) per la query dell'endpoint API (l'impostazione predefinita è 30 giorni).



The screenshot shows the Cisco SecureX dashboard with the 'Add New SMA Email Module' form. The form has the following fields:

- Module Name:** Text input field containing 'SMA Email'.
- Registered Device:** A dropdown menu with 'sma01_mex-amp_inlab' selected. A red arrow points to this dropdown.
- Request Timeframe (days):** Text input field.

Below the form are 'Save' and 'Cancel' buttons. To the right, the 'Quick Start' section contains a list of steps and a red-bordered box with the following text:

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.

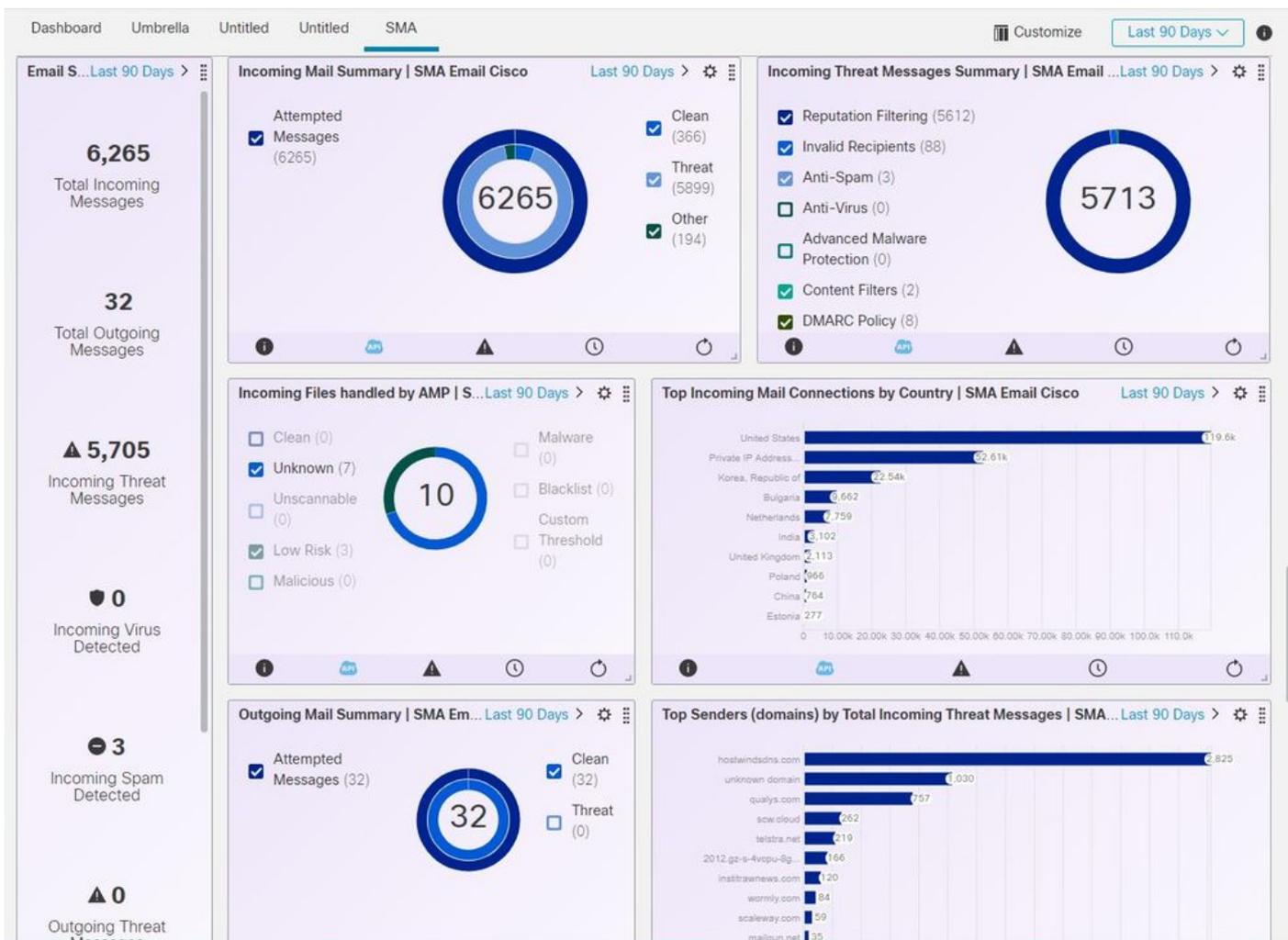
Se il nome del dispositivo SMA non è presente nel menu a discesa, digitarlo nel campo a discesa per eseguire la ricerca.

Passaggio 2. Fare clic su **Save** per completare la configurazione del modulo di posta elettronica SMA

Verifica

Passaggio 1. Aggiungere un nuovo dashboard e i riquadri per visualizzare le informazioni desiderate dal modulo SMA

In questa sezione è possibile visualizzare le informazioni sul dispositivo.



Passaggio 2. Verifica della versione SMA

Nella scheda SMA, selezionare Home > Informazioni sulla versione.

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:	42140CBACAS34A2DASD8-F960AB6079E1

Hardware	
RAID Status:	Unknown

Se non sono disponibili dati su SecureX dopo l'integrazione. Per procedere, procedere come segue.

Passaggio 1. Verificare che le appliance ESA/WSA segnalino allo SMA

In SMA, selezionare **Centralized Services > Security Appliance** e verificare che i dispositivi ESA/WSA siano visualizzati in **Security Appliance**.

Cisco M100V
Content Security Management Virtual Appliance

Management Appliance | Email | Web

Centralized Services | Network | System Administration

System Status

Security Appliances

Email

- Spam Quarantine: Service disabled
- Policy, Virus and Outbreak Quarantines: Service disabled
- Centralized Reporting: Enabled, using 0 licenses
- Centralized Message Tracking: Enabled, using 0 licenses

Web

- Centralized Configuration Manager: Enabled, using 0 licenses
- Centralized Reporting: Enabled, using 0 licenses
- Centralized Upgrade 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...

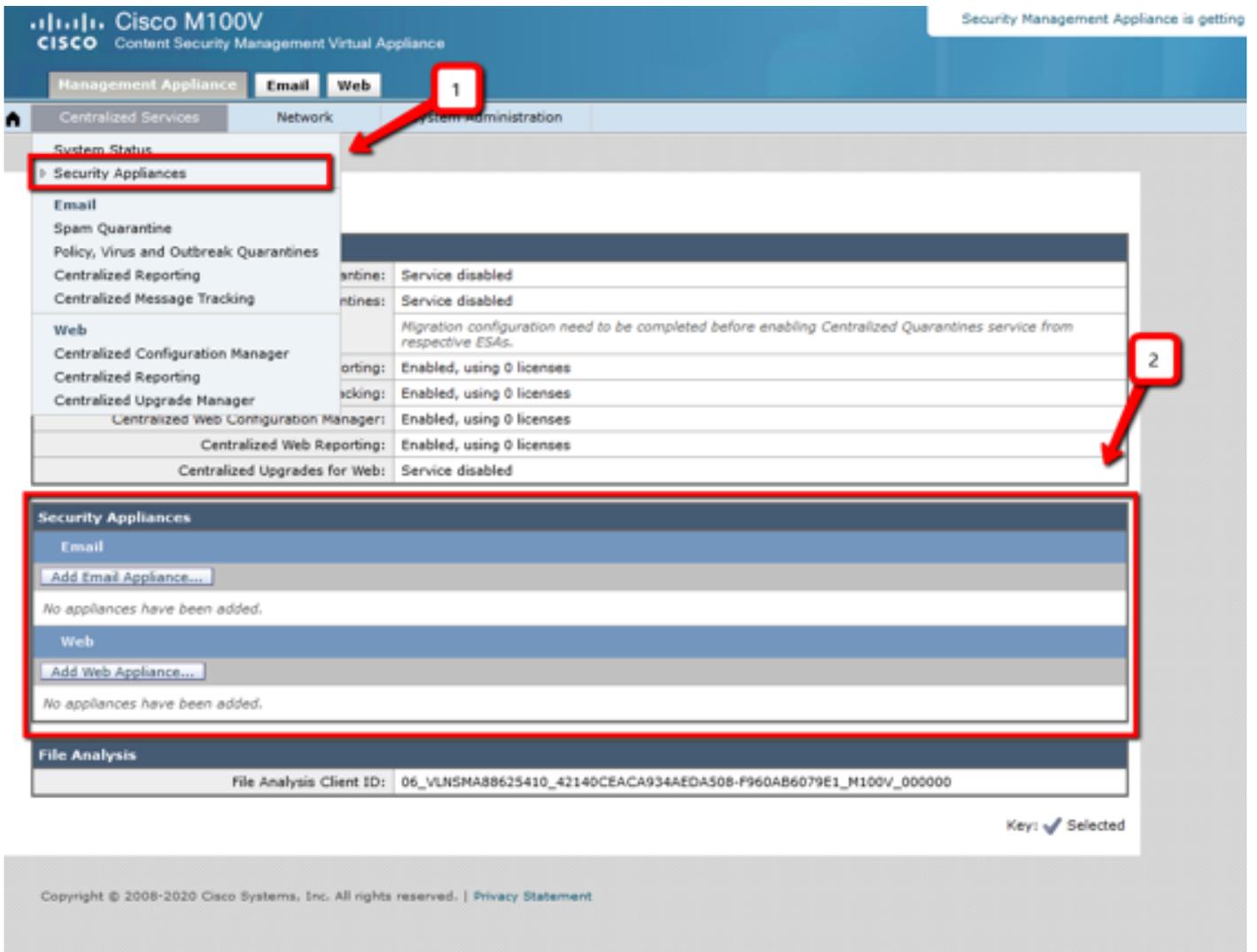
No appliances have been added.

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



Passaggio 2. Verificare che la licenza SMA per **Centralized Email Message Tracking** sia concessa in licenza e abilitata in **Centralized Services > Security Appliance**.

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
	<i>Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.</i>
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](#)

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Suggerimento: Se si riceve un errore di timeout durante l'esecuzione di indagini o l'aggiunta di riquadri a SecureX, è possibile che il volume di informazioni inviate dai dispositivi sia elevato. Provare ad abbassare l'impostazione **Request Timeframe (days)** nella configurazione del modulo.

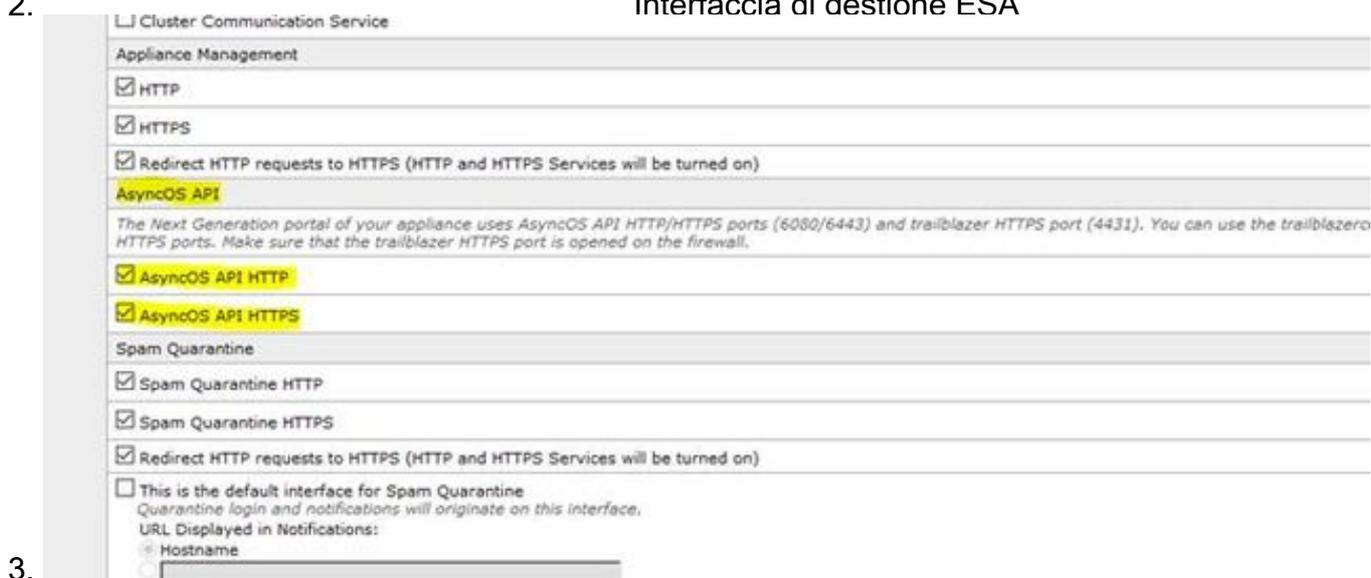
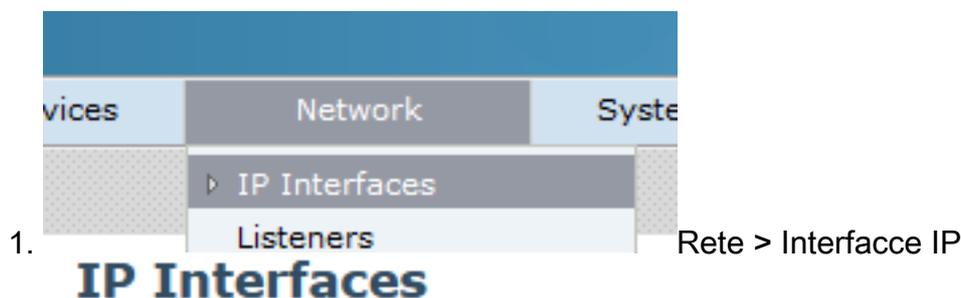
Comandi utilizzati sulla console SMA SSH

- Per verificare la versione e la licenza effettive dell'SMA, è possibile utilizzare questi comandi
>Mostra licenza>versione
- Log di integrazione contenenti eventi di registrazione >cat ctr_logs/ctr_logs.current
- Test di connettività al portale SSE >telnet api-sse.cisco.com 443

Riquadro SMA SecureX / modulo SMA di risposta alla minaccia SecureX con l'errore "Errore imprevisto nel modulo SMA"

SMA richiede che la configurazione HTTP e HTTPS dell'API AsyncOS sia abilitata sull'interfaccia di gestione per comunicare con il portale SecureX/CTR.

Per un SMA locale configurare questa impostazione dalla GUI del portale SMA, andare a **Rete > Interfacce IP > Interfaccia di gestione > API AsyncOS** e abilitare HTTP e HTTPS.



Per un CES (Cloud Based SMA) questa configurazione deve essere effettuata dal back-end da un tecnico TAC SMA, deve accedere al tunnel di supporto del CES interessato.

Video

Informazioni correlate

- [Qui](#) sono disponibili video su come configurare le integrazioni dei prodotti.
- Se il dispositivo non è gestito da un SMA, è possibile aggiungere moduli per [ESA](#) o [WSA](#) singolarmente.
- [Documentazione e supporto tecnico – Cisco Systems](#)