Configurazione dell'integrazione SMA con SecureX

Sommario

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.

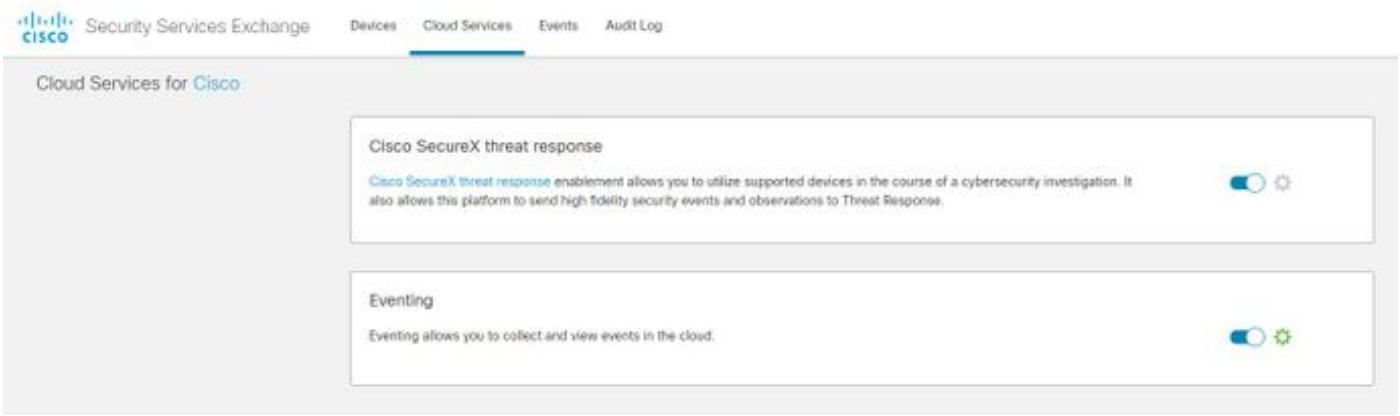
Configurazione

Integrazione SMA

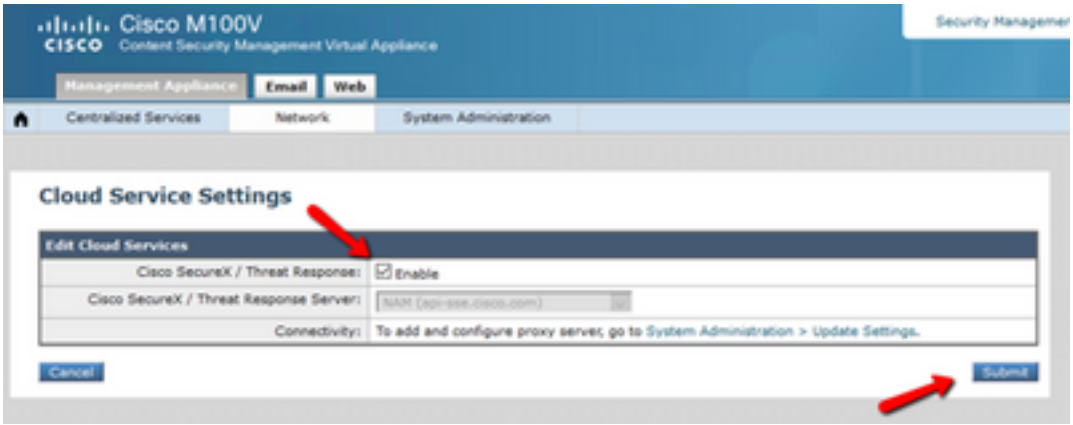
Passaggio 1. In SMA, selezionare **Rete > Impostazioni servizio cloud > Modifica impostazioni**, abilitare l'integrazione e confermare che SMA è pronto ad accettare un token di registrazione.

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.



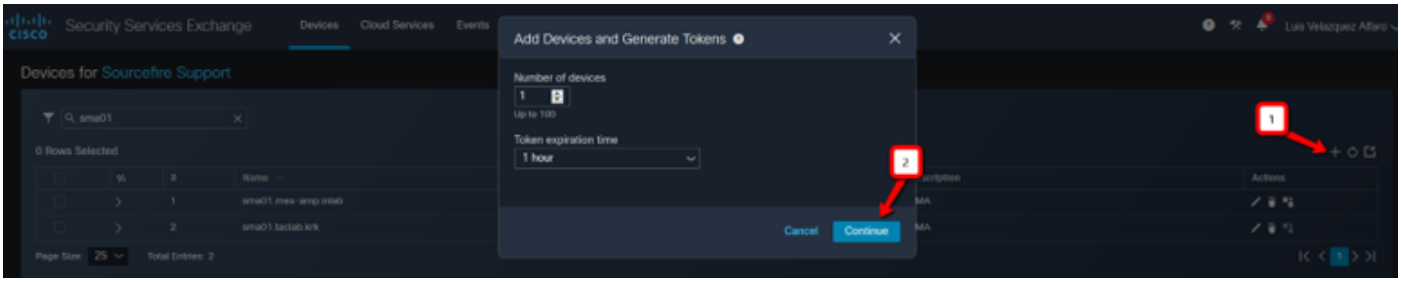
Passaggio 3. Abilitare l'integrazione di Cisco Threat Response nella scheda Servizi cloud, quindi fare clic sulla scheda Dispositivi e sull'icona + per aggiungere un nuovo dispositivo (è necessario l'account SMA Admin).



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

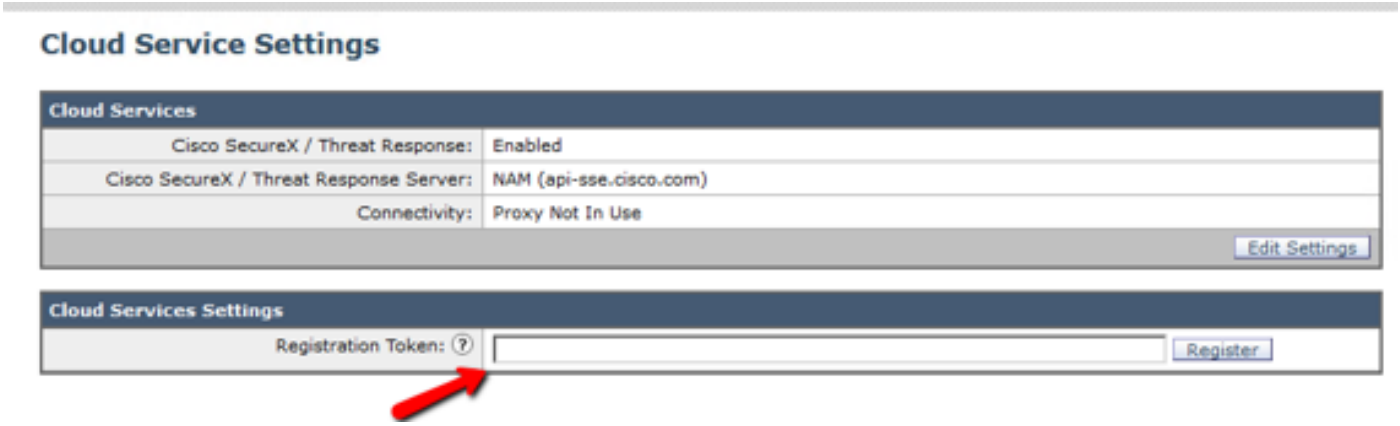
Passaggio 5. Dal portale Secure X passare a **Integrations > Devices > Manage devices (Integrazioni > Dispositivi > Gestione dispositivi)**

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**.

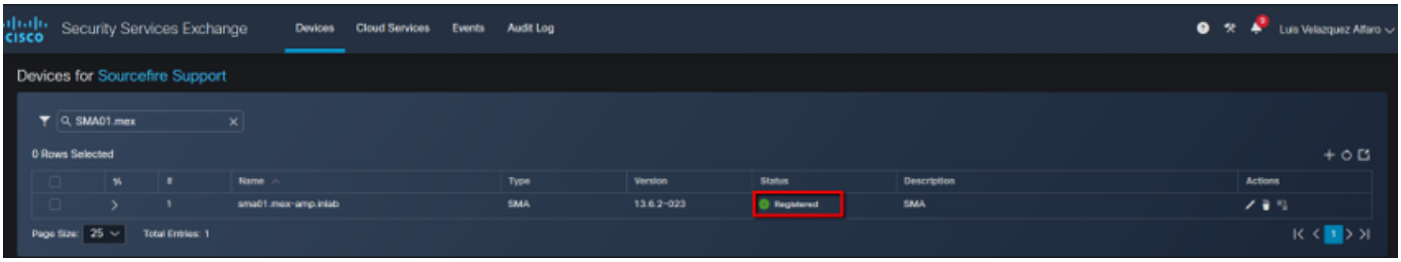


Passaggio 7. Copiare il token generato e verificare che il dispositivo sia stato creato.

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



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:

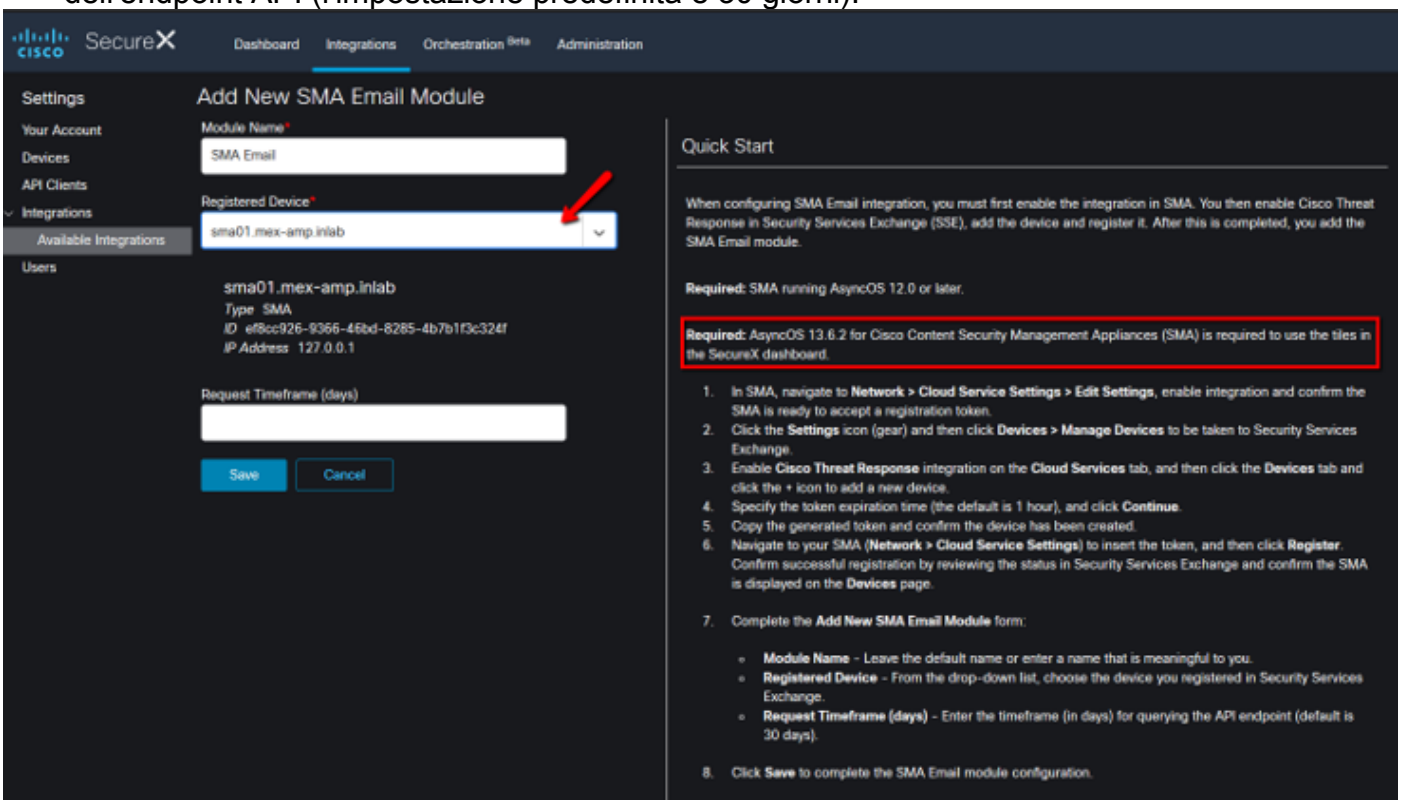
- Nome modulo: lasciare il nome predefinito o immettere un nome significativo.
- Periferica registrata: dall'elenco a discesa, scegliere la periferica registrata in Security Services Exchange.
- Timeframe richiesta (giorni): immettere l'intervallo di tempo (in giorni) per la query dell'endpoint API (l'impostazione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



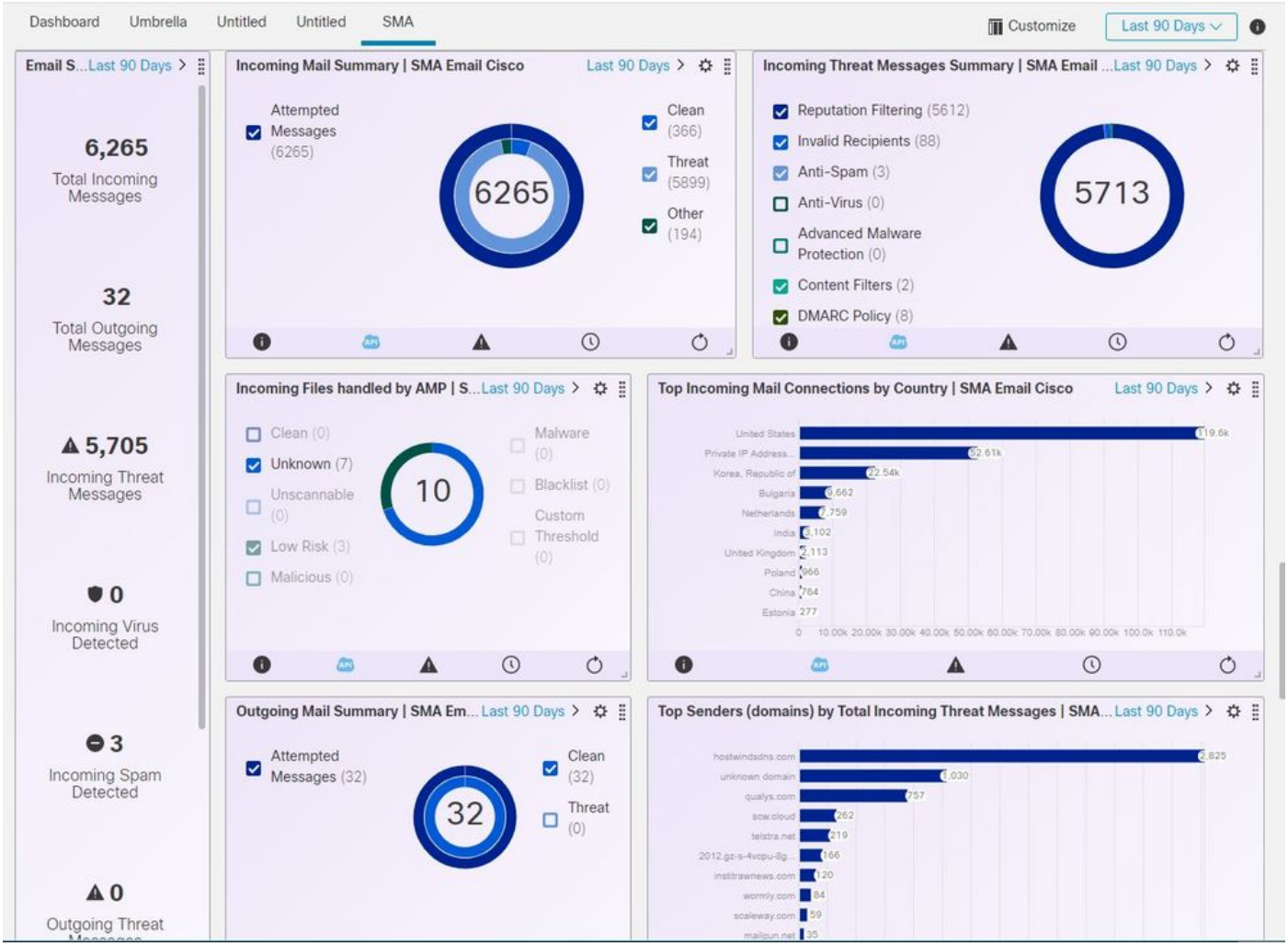
Se il nome del dispositivo SMA non è presente nel menu a discesa, digitarlo nel campo a discesa per eseguire la ricerca.

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

Verifica

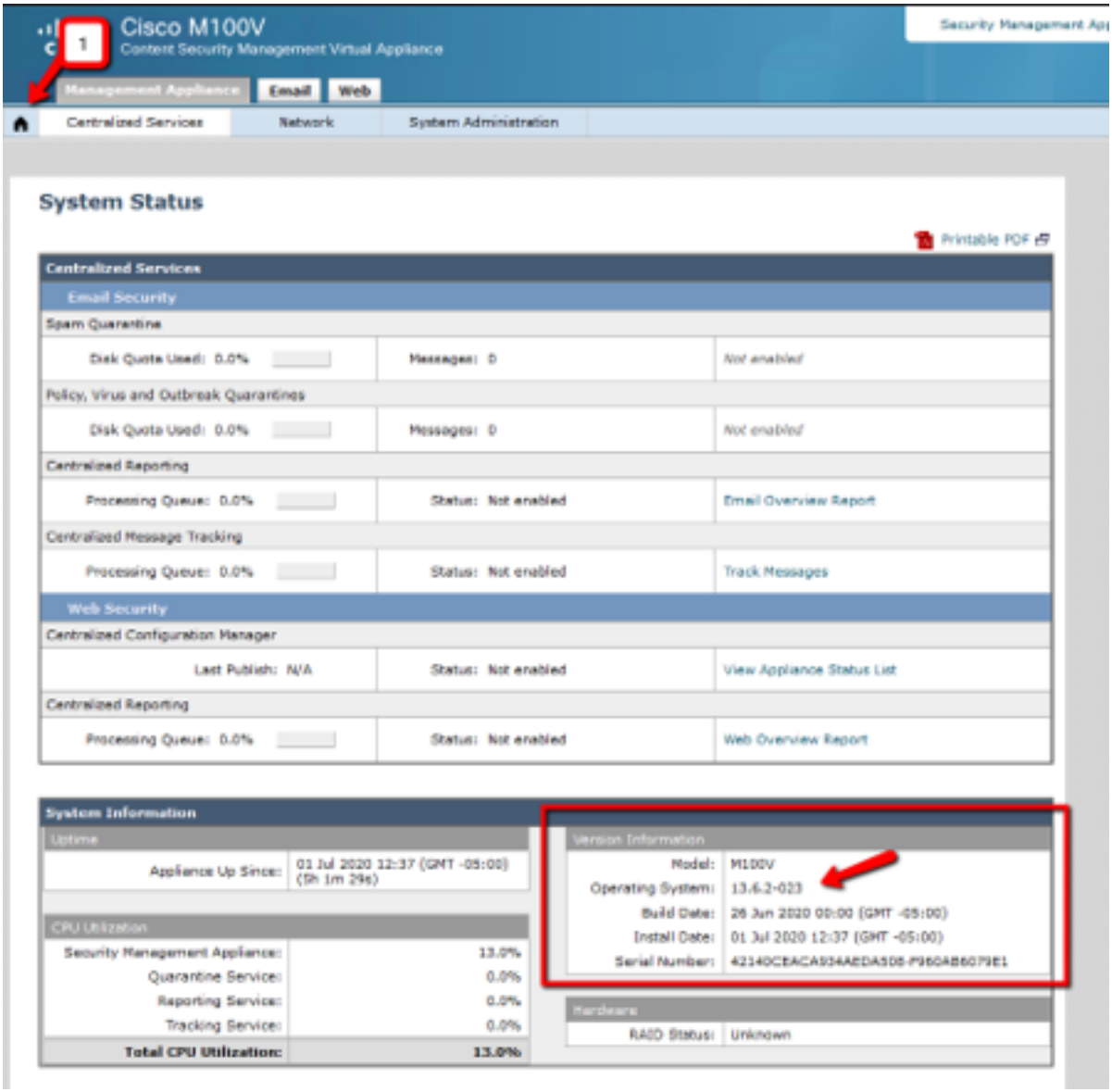
Passaggio 1. Aggiungere un nuovo dashboard e i riquadri per visualizzare le informazioni desiderate dal modulo SMA

In questa sezione è possibile visualizzare le informazioni sul dispositivo.



Passaggio 2. Verifica della versione SMA

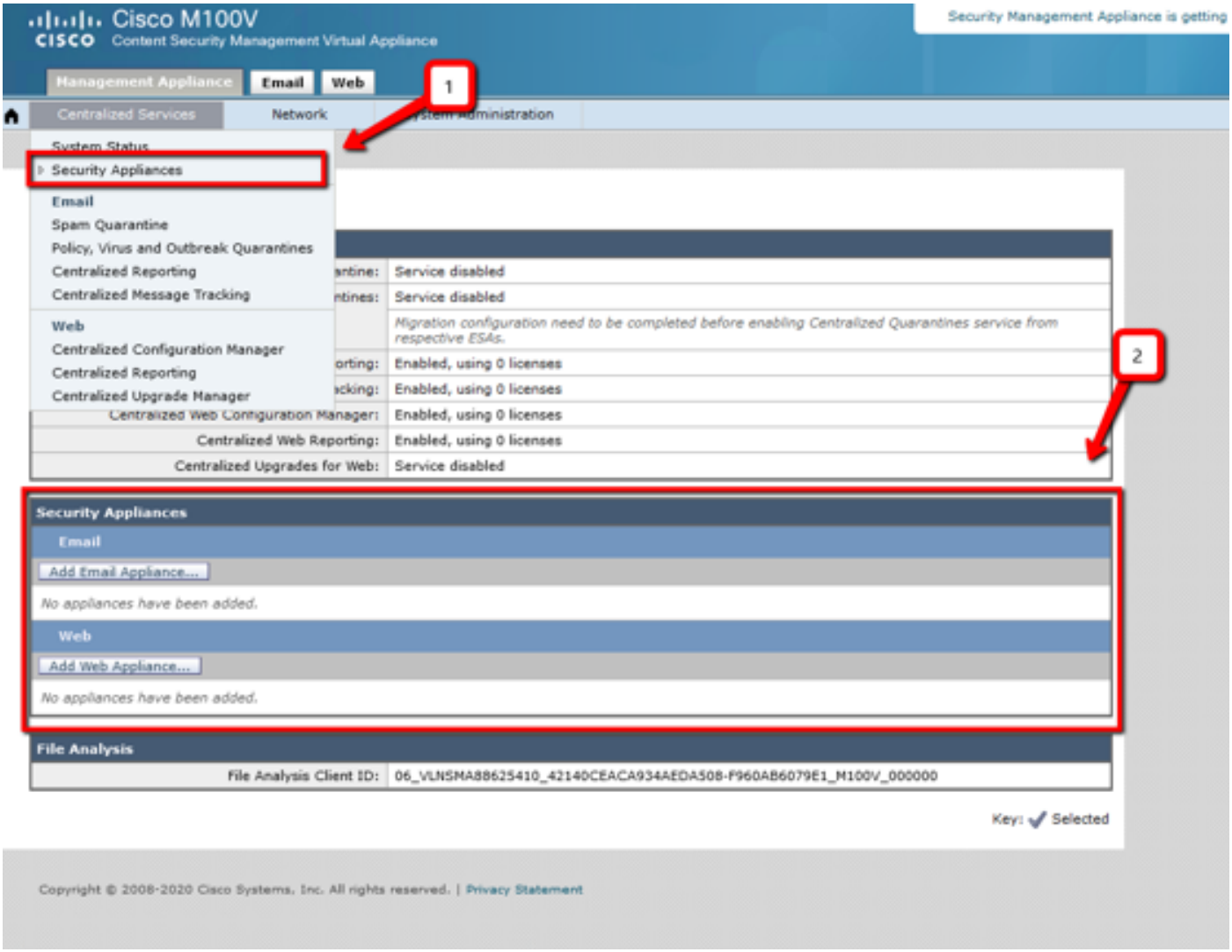
Nella scheda SMA, selezionare **Home > Informazioni sulla versione**.



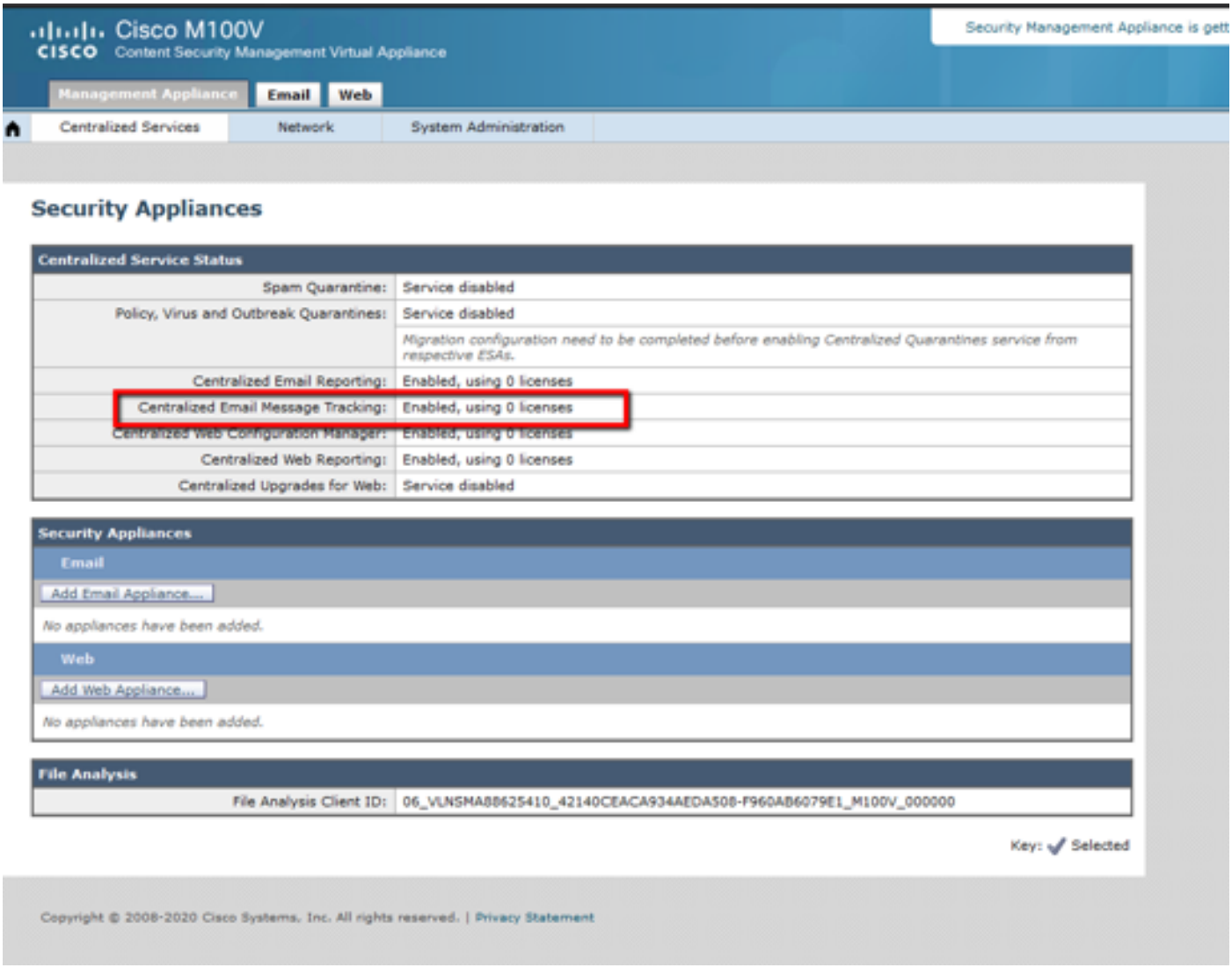
Se non sono disponibili dati su SecureX dopo l'integrazione. Per procedere, procedere come segue.

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**.



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



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.

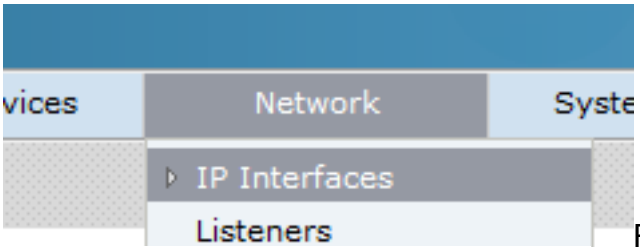
Comandi utilizzati sulla console SMA SSH

- 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.

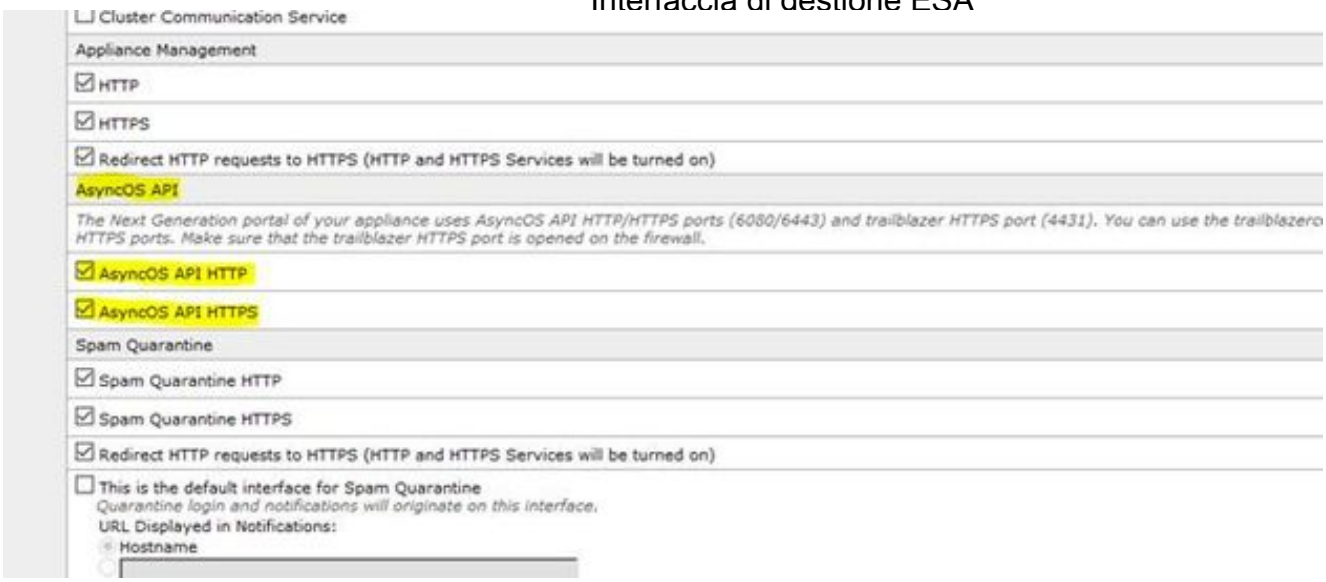
Per un SMA locale configurare questa impostazione dalla GUI del portale SMA, andare a **Rete > Interfacce IP > Interfaccia di gestione > API AsyncOS** e abilitare HTTP e HTTPS.

1. 

Rete > Interfacce IP

2. 

Interfaccia di gestione ESA

3. 

API asincrona > 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