De SMA-integratie met SecureX configureren

Inhoud

Inleiding

Dit document beschrijft het proces om de integratie van Content Security Management-applicatie (SMA) met SecureX te configureren, te controleren en op te lossen.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis over deze onderwerpen te hebben:

- Security Management-applicatie (SMA)
- E-mail security applicatie (ESR)
- Web security applicatie (WSA)
- Cisco Threat Response (CTR)
- SecureX-dashboard

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- SMA-actieve asynchrone/synchrone OS 13.6.2 (voor SMA-e-mailmodule)

- SMA-actieve AsyncOS 12.5 (voor SMA - webmodule)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

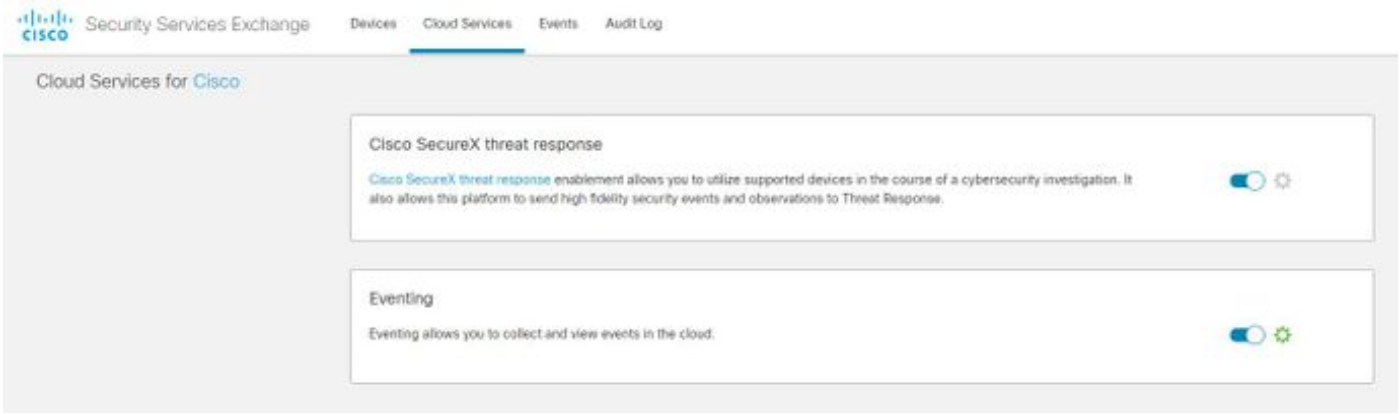
Configureren

SMA-integratie

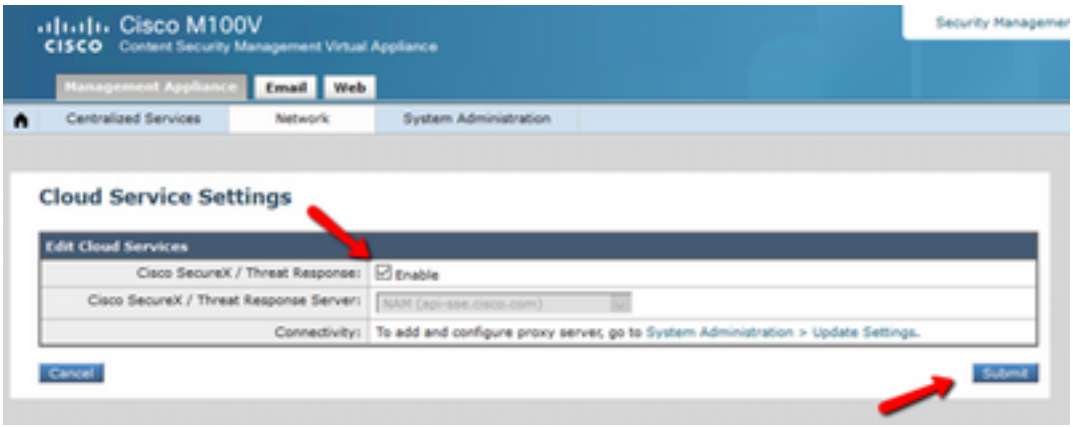
Stap 1. In SMA kunt u **navigeren** naar **Network > Cloud Service-instellingen > Instellingen bewerken**, integratie inschakelen en bevestigen dat de SMA klaar is om een registrtoken te aanvaarden.

Stap 2. Klik op het pictogram Instellingen (versnelling) en klik vervolgens op **Apparaten > Apparaten beheren** die naar Security Services Exchange (SE) moeten worden uitgevoerd.

Zorg ervoor dat alle opties zijn ingeschakeld onder **de** cloudservices.



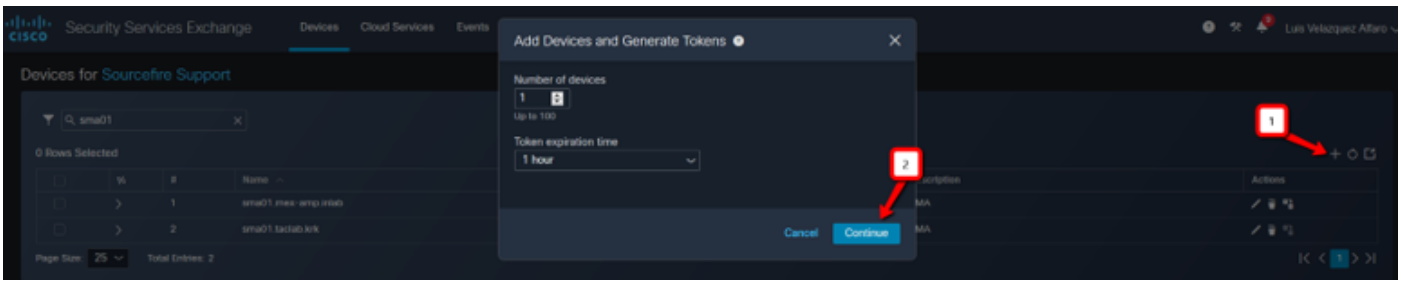
Stap 3. Schakel Cisco Threat Response in op het tabblad Cloud Services en klik vervolgens op het tabblad Apparaten en klik op het pictogram + om een nieuw apparaat toe te voegen (hiervoor is een SMA Admin-account nodig).



Stap 4. Meld u aan bij het SSE-portaal van SecureX-instantie.

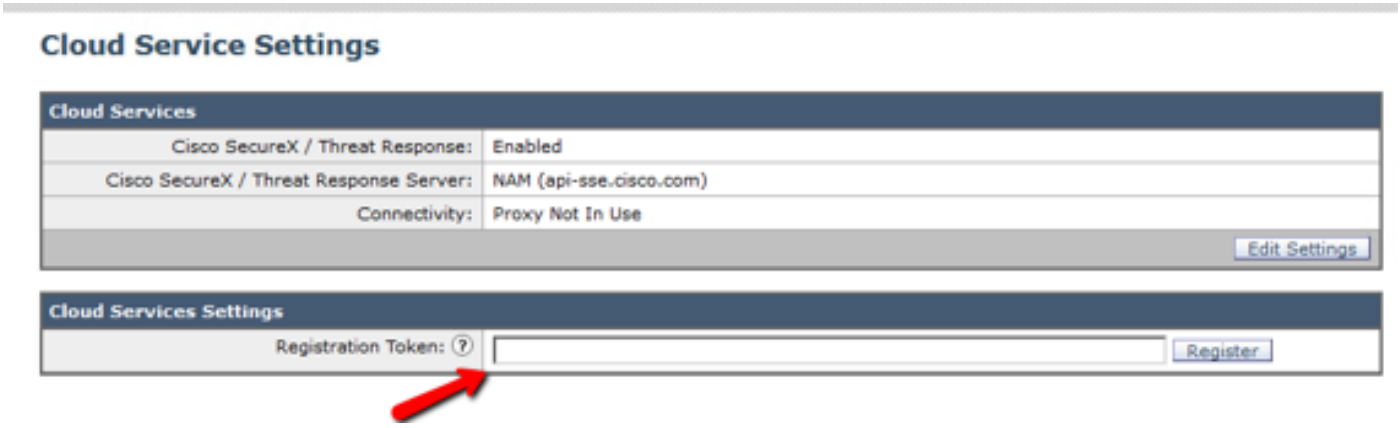
Stap 5. Van het Secure X-portaal navigeren naar **integraties > Apparaten > Apparaten beheren**

Stap 6. Maak een nieuw token op het SSE-portaal en specificeer de duur van de symbolische afloop (de standaard is 1 uur) en klik op **Doorgaan**.

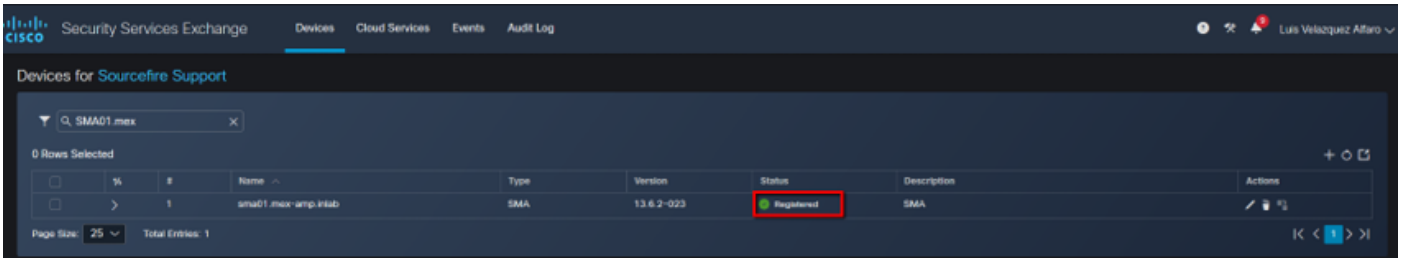


Stap 7. Kopieer het gegenereerde token en bevestig dat het apparaat is gemaakt.

Stap 8. Navigeer naar uw SMA **(Network > Cloud Service Settings)** om het token op te nemen en klik vervolgens op Registreer.



Om succesvolle registratie te bevestigen herzie de status in **Security Services Exchange** en bevestig dat het SMA op de pagina Apparaten wordt weergegeven.



SMA Web

Stap 1. Vul het formulier Add New SMA Web Module in:

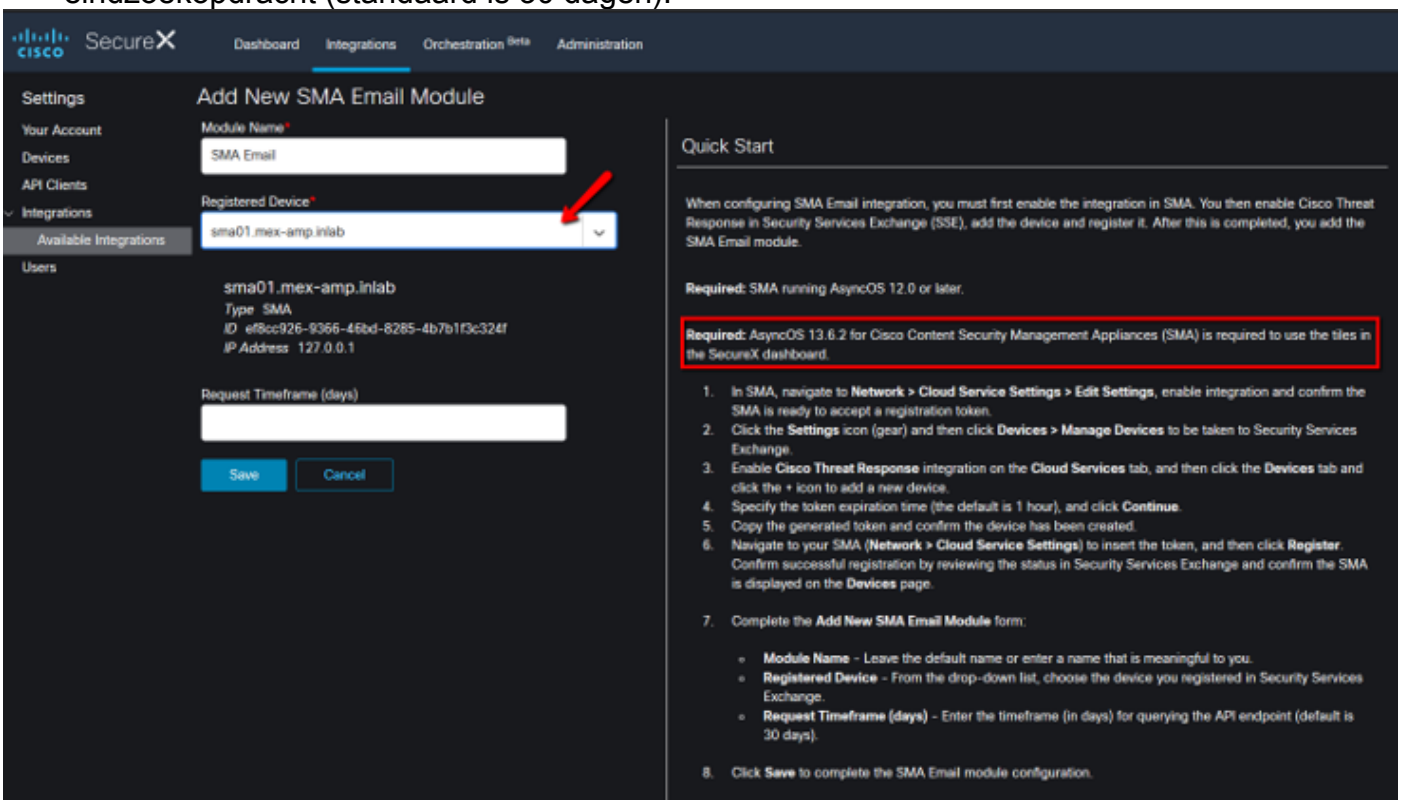
- Naam module - Laat de standaardnaam achter of voer een naam in die voor u betekenisvol is.
- Geregistreerd apparaat - Kies in de vervolgkeuzelijst het apparaat dat u in Security Services Exchange hebt geregistreerd.
- Time frame (dagen) aanvragen - Voer het tijdframe (in dagen) in voor de API-eindzoekopdracht (standaard is 30 dagen).

Stap 2. Klik op Opslaan om de configuratie van de SMA-webmodule te voltooien.

SMA-e-mail

Stap 1. Vul het formulier Nieuwe SMA-e-mailmodule toevoegen in.

- Naam module - Laat de standaardnaam achter of voer een naam in die voor u betekenisvol is.
- Geregistreerd apparaat - Kies in de vervolgkeuzelijst het apparaat dat u in Security Services Exchange hebt geregistreerd.
- Time frame (dagen) aanvragen - Voer het tijdframe (in dagen) in voor de API-eindzoekopdracht (standaard is 30 dagen).



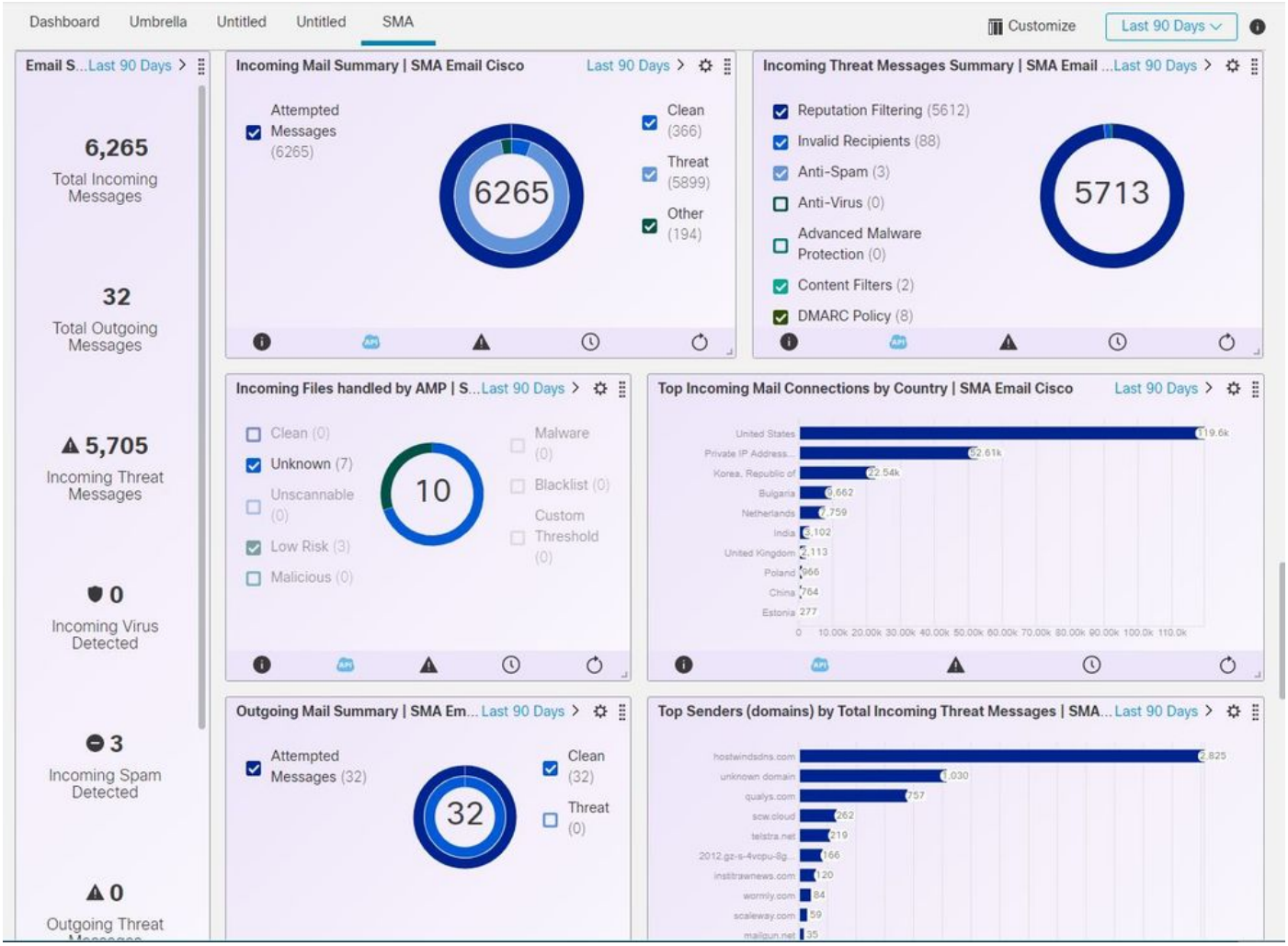
Als de naam van het SMA-apparaat niet in het uitrolmenu staat, typt u de naam in het uitrolveld om naar de naam te zoeken.

Stap 2. Klik op **Save** om de configuratie van de SMA-e-mailmodule te voltooien

Verifiëren

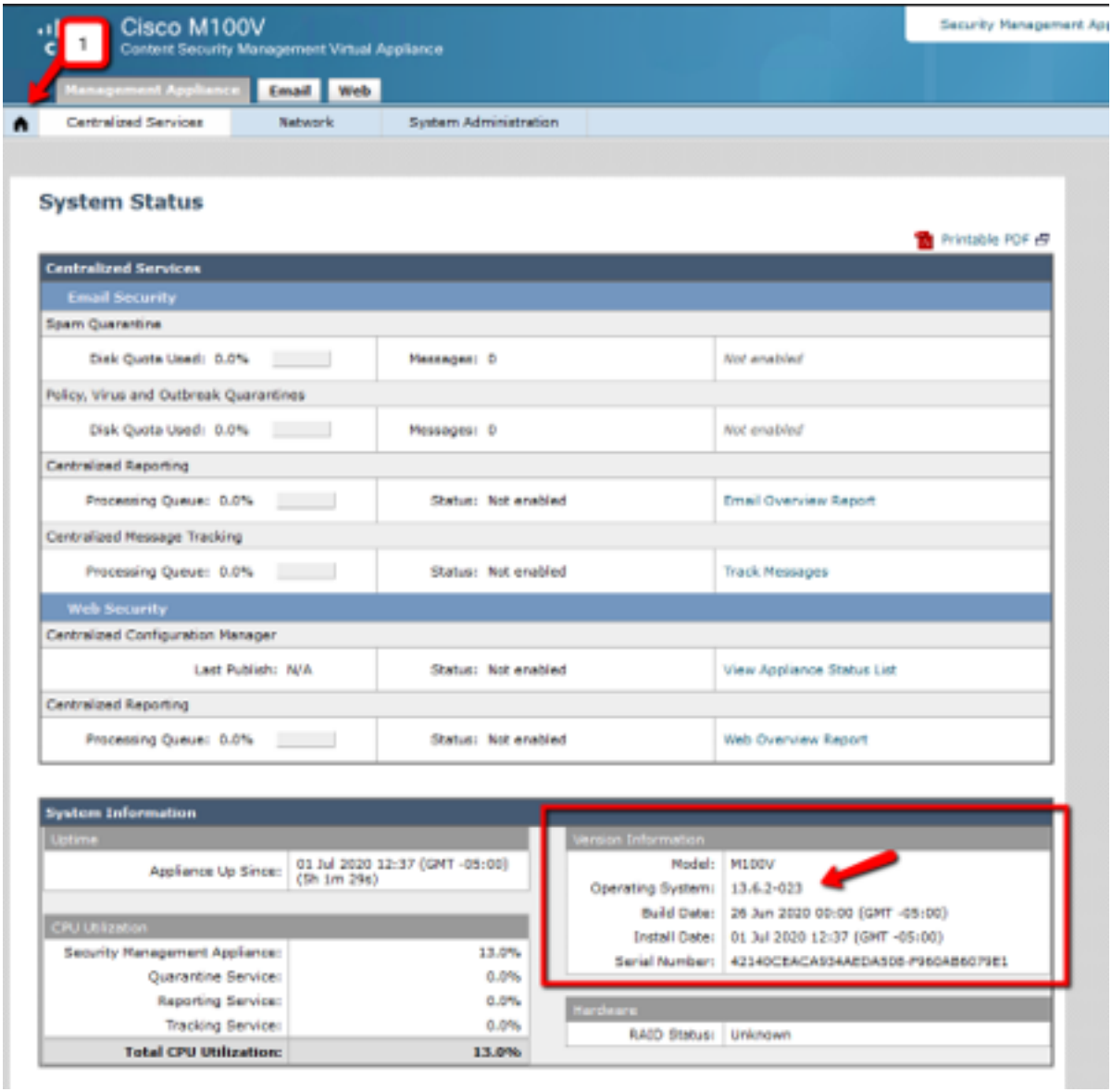
Stap 1. Voeg een nieuw Dashboard toe en voeg de tegels toe om de informatie te zien die u in uw SMA-module geïnteresseerd hebt

U kunt de informatie van uw apparaat in deze sectie zien weergegeven.



Stap 2. Controleer de SMA-versie

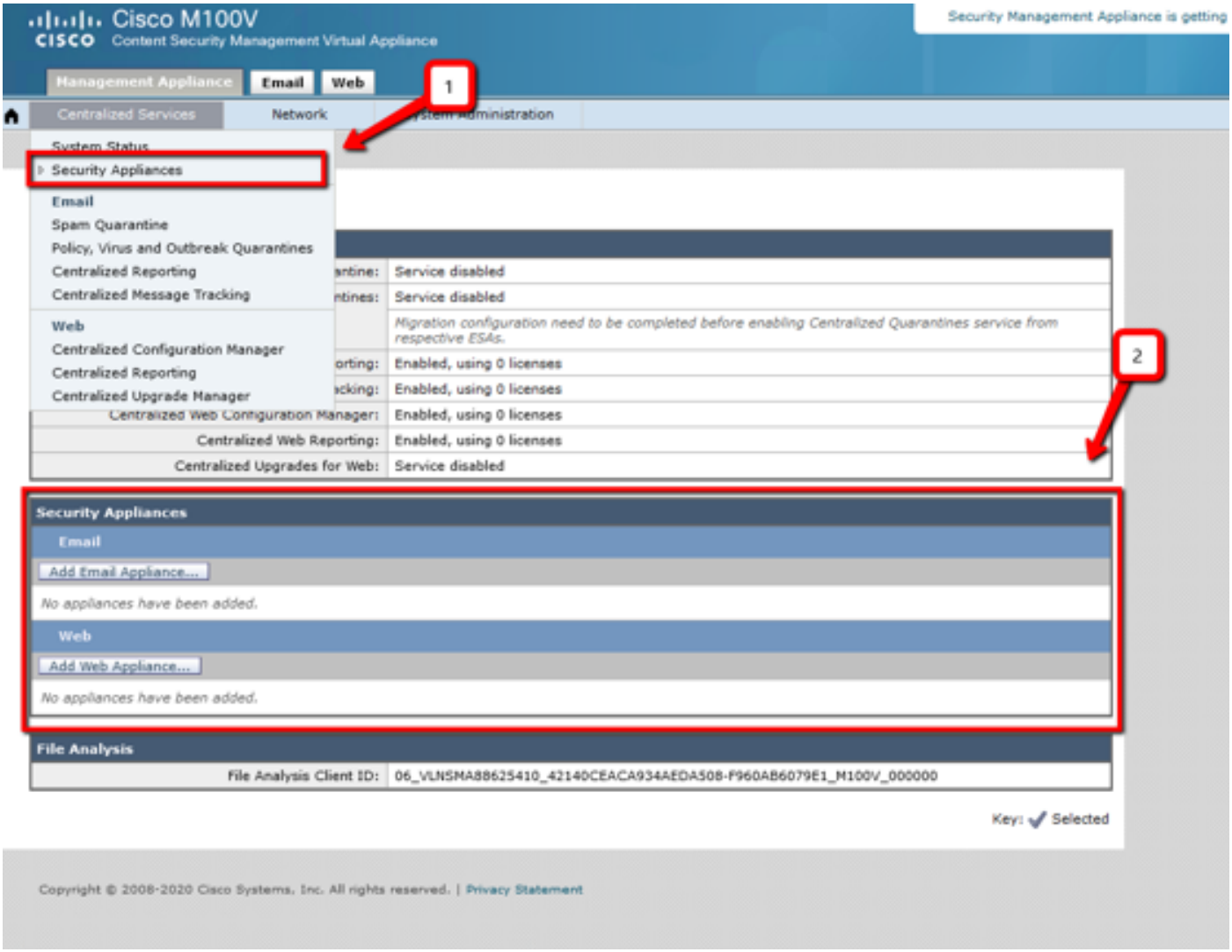
navigeer in SMA naar **startpunt > Versieverslag**.



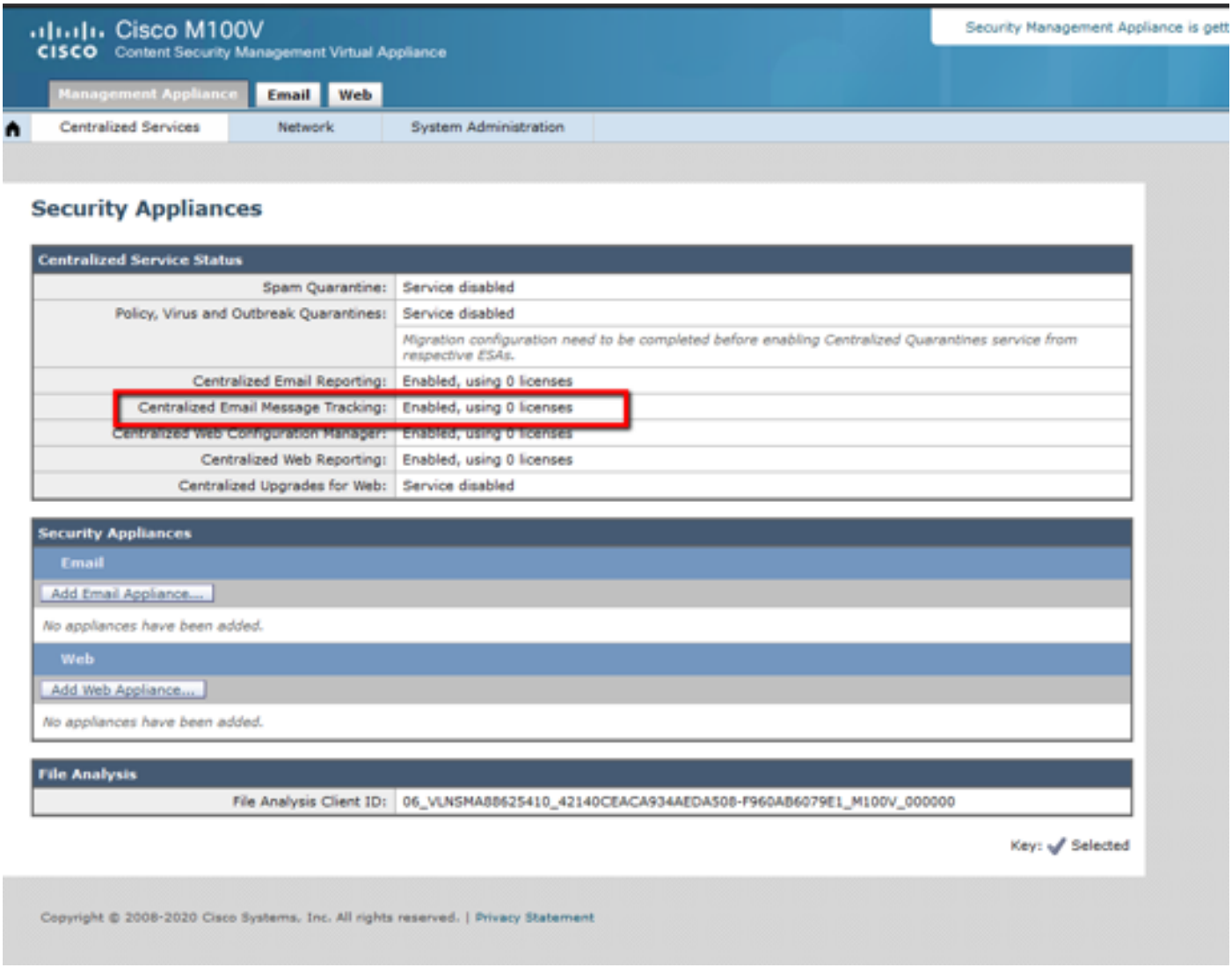
Als er geen gegevens beschikbaar zijn over SecureX na integratie. U kunt de volgende stappen volgen.

Stap 1 Controleer het rapport van de ESA/WSA-apparatuur aan de SMA

Ga op SMA naar **Gecentraliseerde services > security applicaties** en controleer of de ESA/WSA apparaten verschijnen onder **security applicaties**.



Stap 2. Controleer de SMA-licentie voor **Gecentraliseerde E-mailtracering** en laat deze **toe** onder **Gecentraliseerde services > security applicaties**.



Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

> **Tip**: Als u een Time-outfout ontvangt tijdens het uitvoeren van onderzoeken of tijdens het toevoegen van tegels aan SecureX, kan deze worden veroorzaakt door een hoog volume informatie die van uw apparaten wordt verzonden. Probeer de instelling **Time-**frame **(dagen)** voor **aanvraag** in de modemconfiguratie te verlagen.

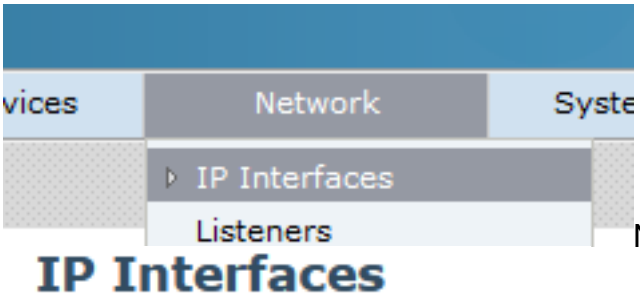
Opdrachten gebruikt op SMA SSH-console

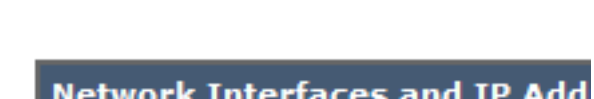
- Om de eigenlijke versie en licentie van het SMA te controleren, kunnen deze opdrachten worden gebruikt >Showlicentie>versie
- Integratie-logboeken met registratiefouten >Kat ctr_logs/ctr_logs.current
- Connectiviteitstest op SSE-profiel >telnet api-sse.cisco.com 443

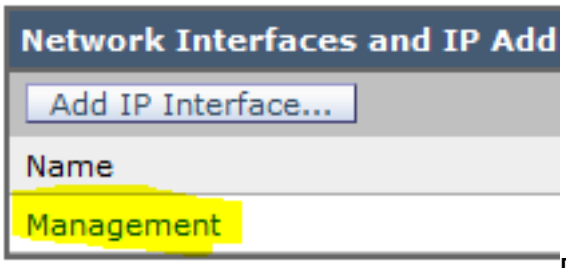
SecureX SMA-tegel / SecureX-bedreigingsrespons SMA-module met fout "Er is een onverwachte fout in de SMA-module"

SMA vereist AsyncOS API & HTTPS configuratie die via de beheerinterface kan worden ingeschakeld met SecureX/CTR-portal.

Voor een SMA-type stel deze instelling vanaf een SMA-portal GUI in, ga naar **Network > IP-interfaces > Management-interface > AsyncOS API** en schakel HTTP en HTTPS in.

1. 

Network > IP-interfaces


2. 

ESA-beheerinterface
3. 

Async API > HTTP en HTTPS

Voor een CES (Cloud Based SMA) zal deze configuratie vanaf de achterkant moeten worden uitgevoerd door een SMA TAC-ingenieur. Dit vereist toegang tot de ondersteuningstunnel van de getroffen CES.

Video

Gerelateerde informatie

- U kunt hier video's vinden over de manier waarop u uw product-integraties kunt configureren.
- Als uw apparaat niet door een SMA wordt beheerd, kunt u modules voor ESA of WSA afzonderlijk toevoegen.
- Technische ondersteuning en documentatie – Cisco Systems