Integratie van SecureX en Secure Email Applicatie (voorheen ESA) voor probleemoplossing

Inhoud

Inleiding

Dit document beschrijft de stappen om een basisanalyse uit te voeren en hoe u problemen kunt oplossen met de integratiemodule voor SecureX en Insights en Secure Email Applicance.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SecureX
- Security services exchange
- Secure-e-mail

Gebruikte componenten

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

- Security services exchange
- SecureX 1.54

- Secure Email C100V op softwareversie 13.0.0-392

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De Cisco Secure Email Applicatie (voorheen E-mail security applicatie) biedt geavanceerde mogelijkheden voor bedreigingsbescherming om bedreigingen sneller te detecteren, te blokkeren en te verhelpen, gegevensverlies te voorkomen en belangrijke informatie tijdens het transport te beveiligen met end-to-end encryptie. Na configuratie biedt de module Secure Email Application details die aan observables zijn gekoppeld. U kunt:

- Bekijk de e-mailrapporten en bericht traceert gegevens van meerdere apparaten in uw organisatie
- Identificeer, onderzoek en herstel van bedreigingen die worden waargenomen in de e-mailrapporten en berichtensporen
- De vastgestelde bedreigingen snel oplossen en aanbevolen maatregelen tegen de vastgestelde bedreigingen bieden
- Documenteer de bedreigingen om het onderzoek op te slaan en samenwerking van informatie tussen andere apparaten mogelijk te maken

Voor de integratie van een beveiligde e-mail applicatie module is het gebruik van Security Services Exchange (SSE) vereist. SSE staat een beveiligde e-mail applicatie toe om zich te registreren bij de Exchange en u geeft expliciete toestemming om toegang te krijgen tot de geregistreerde apparaten.

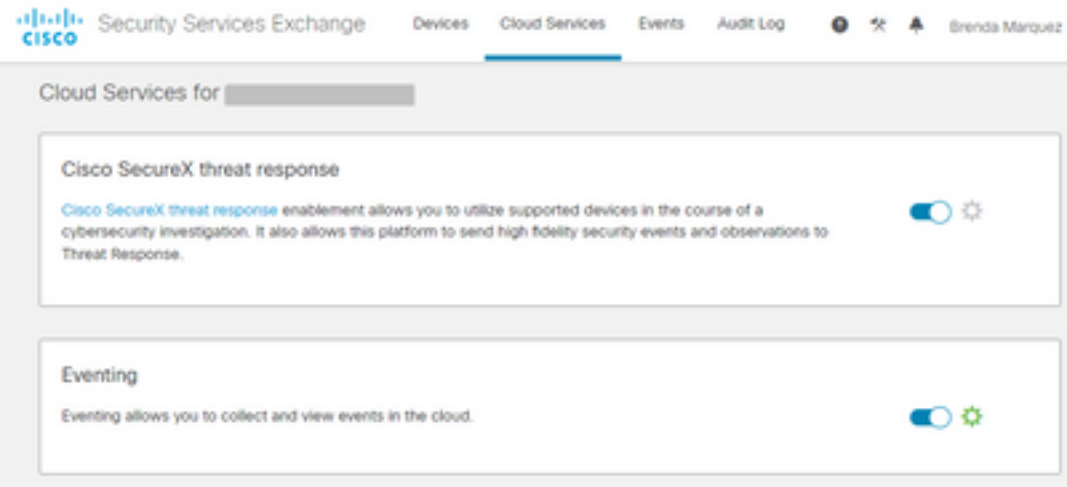
Als u meer over de configuratie wilt weten, raadpleeg dan dit artikel hier over de integratiemodule.

Problemen oplossen

Om gemeenschappelijke problemen met de integratie van SecureX en Secure Email Applicatie op te lossen, kunt u deze stappen verifiëren.

Secure Email device wordt niet weergegeven in het SecureX- of Security Services Exchange-portal

Als uw apparaat niet wordt weergegeven in het SSE-portal, zorg er dan voor dat u de **SecureX Threat Response** en **Event** services hebt ingeschakeld in het SSE-portal, navigeer naar **Cloud Services** en schakel de services in zoals de onderstaande afbeelding:

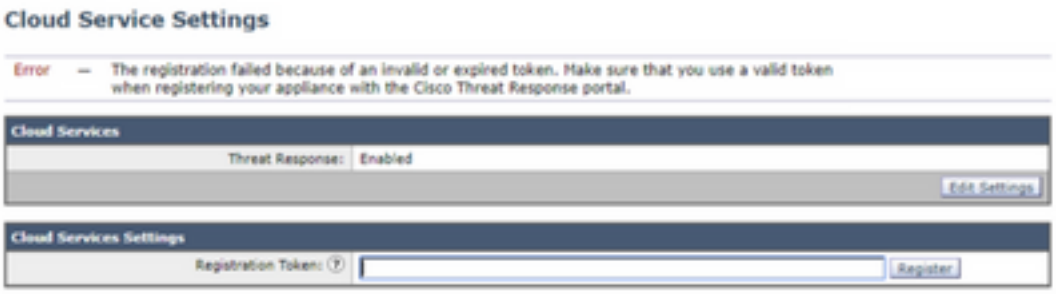


Secure Email vraagt geen registratietoken

Zorg ervoor dat de wijzigingen worden vastgelegd zodra de Cisco SecureX / Threat Response-service is ingeschakeld. Anders worden de wijzigingen niet toegepast op de sectie Cloud-service in het beveiligde e-mailadres, zie de onderstaande afbeelding.

Registratie is mislukt vanwege een ongeldig of verlopen token

Als u de foutmelding ziet: "De registratie is mislukt vanwege een ongeldig of verlopen token. Zorg ervoor dat u een geldig token voor uw apparaat gebruikt met het Cisco Threat Response-portal" in de Secure Email GUI, zoals in de afbeelding hieronder:



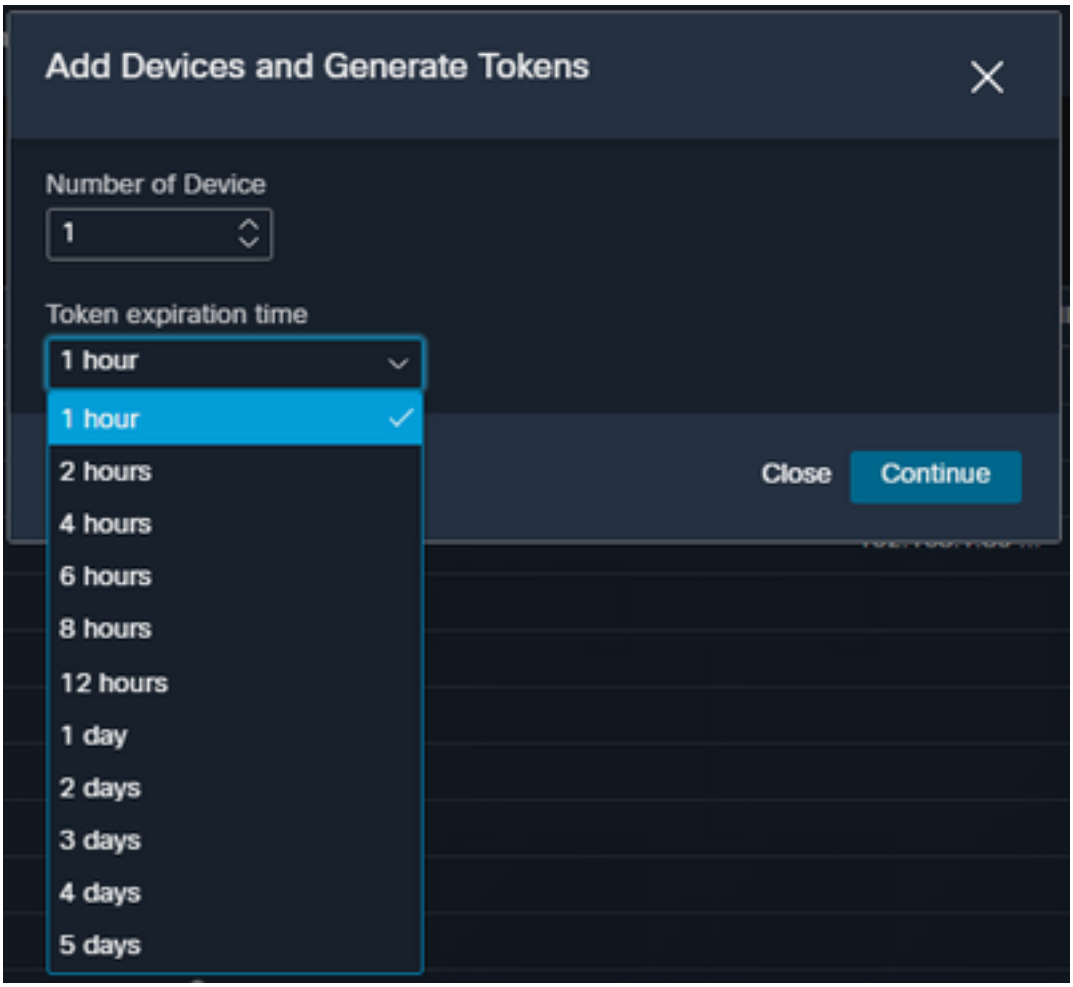
Zorg ervoor dat de token worden gegenereerd uit de juiste Cloud:

Als u Europe (EU) Cloud for Secure Email gebruikt, genereert u het token via https://admin.eu.sse.itd.cisco.com/

Als u Americas (NAM) Cloud for Secure Email gebruikt, genereert u het token vanaf https://admin.sse.itd.cisco.com/

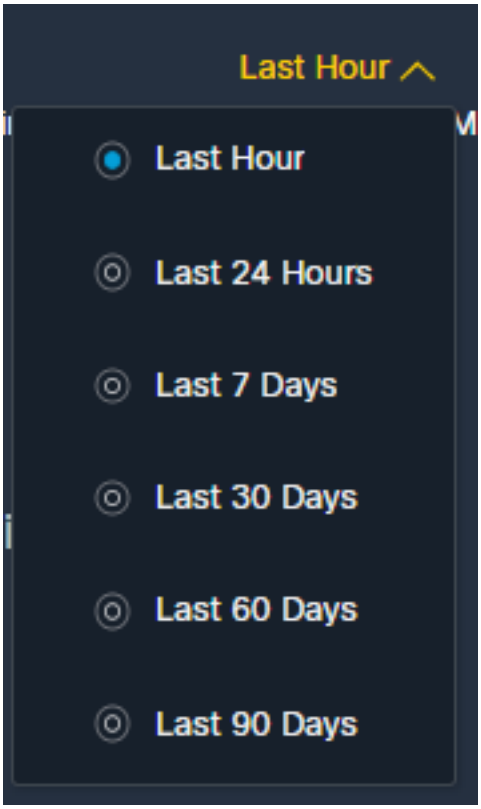
Security Services Exchange (SSE)-portal:	NAM: https://admin.sse.itd.cisco.com/ EU: https://admin.eu.sse.itd.cisco.com/
Cisco SecureX-portal	NAM: https://securex.us.security.cisco.com/ EU: https://securex.eu.security.cisco.com/
Secure e-mail Cisco SecureX/Threat Response Server:	NAM: api-sse.cisco.com EU: api.eu.sse.itd.cisco.com

Denk er ook aan dat het Registratietoken een verlooptijd heeft (selecteer de meest geschikte tijd om de Integratie op tijd te voltooien), zoals in de afbeelding.



SecureX Dashboard geeft geen informatie weer van de Secure Email module

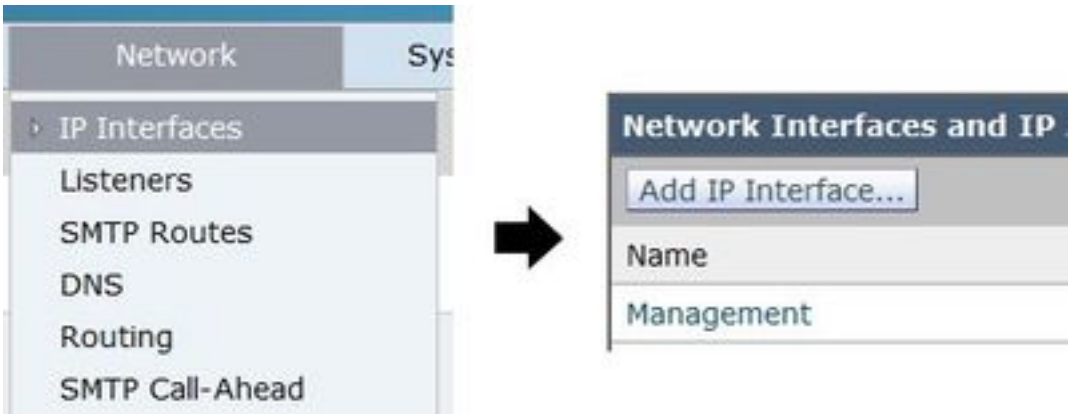
U kunt een breder tijdbereik in de beschikbare tegels selecteren, van **Laatste uur** tot **Laatste 90 dagen**, zoals in de afbeelding hieronder.

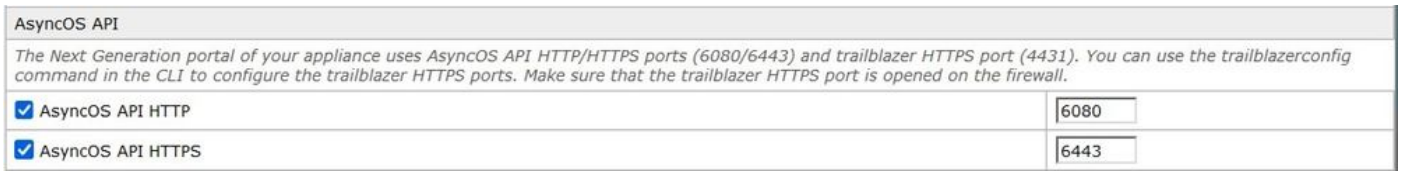


Andere voorbeelden kunnen zijn dat we de boodschap 'Er was een probleem. Probeer het later opnieuw." of zelfs de foutmelding "Er was een client fout in de Secure Email module: E4017: Apparaat is offline [409]". Controleer of het apparaat nog steeds wordt weergegeven als geregistreerd via het SSE-portal, waarschijnlijk is het apparaat niet meer geregistreerd en is het niet meer zichtbaar. Probeer een nieuwe module aan het SecureX-portal toe te voegen.

SecureX Secure Email tile module geeft fout weer "Er is een onverwachte fout opgetreden op de Secure Email module"

Secure Email vereist AsyncOS API HTTP- en HTTPS-configuratie ingeschakeld via de beheerinterface om te communiceren met SecureX/CTR-portal. Voor een on-prem beveiligde e-mail configureer deze functie vanuit de Secure Email portal GUI, navigeer naar **Network > IP-interfaces > Management-interface > AsyncOS API** en schakel HTTP en HTTPS in, zoals in de afbeelding.



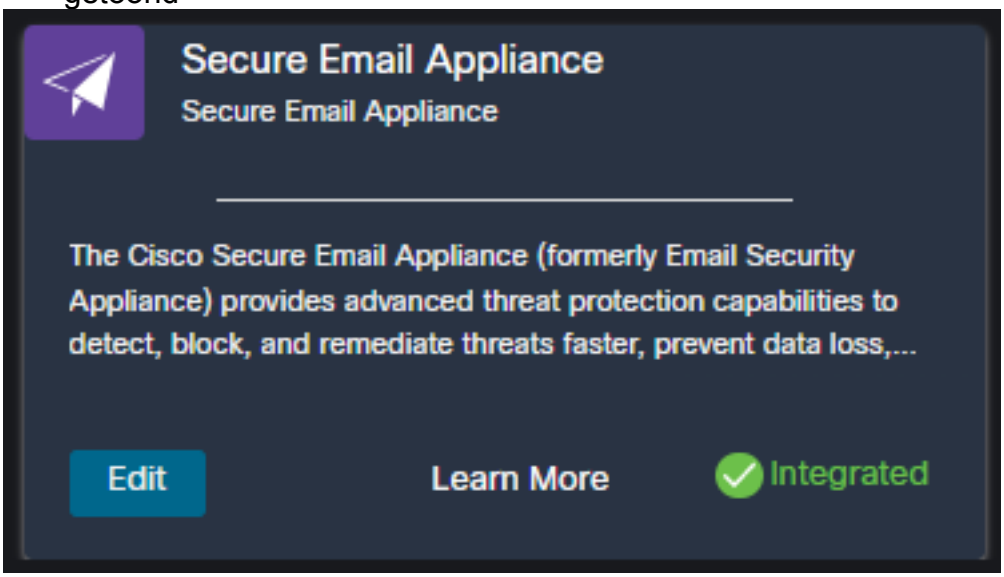


Voor een CES (Cloud-Based Secure Email) moet deze configuratie vanaf de backend door een Secure Email TAC-engineer worden uitgevoerd, het vereist toegang tot de ondersteuningstunnel van de getroffen CES.

Verifiëren

Zodra Secure Email wordt toegevoegd als een bron aan Device Insights, kunt u een succesvolle **REST API** verbindingsstatus zien.

- U kunt de **REST API** verbinding met een groene status zien
- Druk op **SYNC NOW** om de eerste volledige sync te activeren, zoals in het beeld wordt getoond



Als het probleem blijft bestaan met de integratie van SecureX en Secure Email Applicatie, raadpleeg dit artikel om HAR-logbestanden te verzamelen van de browser en contact op te nemen met TAC-ondersteuning om een diepere analyse uit te voeren.

Gerelateerde informatie

- **U vindt de informatie in dit artikel in deze SecureX en Secure Email Integration video.**
- **Hier vindt u video's over het configureren van productintegraties**
- **Technische ondersteuning en documentatie – Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.