# De SMA-integratie met SecureX configureren

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren SMA-integratie SMA-integratie SMA Web SMA-e-mail Verifiëren Problemen oplossen SecureX SMA-tegel / SecureX-bedreigingsrespons SMA-module met fout "Er is een onverwachte fout in de SMA-module" Video Gerelateerde informatie

# 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).

the second se	Email Web	
Centralized Services	Network	System Administration
		Parente.
Cinese Research / Th	Annual Descention	
Cisco SecureX / Th	hreat Response:	E3 Enable
Cisco SecureX / Th Cisco SecureX / Threat Re	hreat Response: esponse Server:	ED Enable NAM (api-ssa.ciscs.com)

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**.

cisco Security Services Exchange Devices	Cloud Services Events	Add Devices and Generate Tokens • ×	¢ 0	🛠 🤌 Luis Veliszguez Alfaro 🗸
Devices for Sourcefire Support		Number of devices		
▼ [0, sma01 X] 0 Rows Selected		1 B ty to 100 Token explorition time 1 hour		1 + o []
D 94 # Name ~			scription	Actions
> 1 sma01.mex-amp.iniat				Z # %
> 2 smað t. tadab krk		Cancel Continue	MA	Z 8 15
Page Size: 25 🛩 Total Entries: 2				IC < 1> >I

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.

#### Cloud Service Settings

oud 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: (?)	Register			

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

aliada cisco	Secu	rity Ser	vices Exchar	ige Devices	Cloud Services	Events	Audit Log				o 🛠 🧍 Luis Velazquez Alfaro ∨
Devi	ces for	Source	efire Support								
,	ଦ୍ ୨୦୦	N01.mex									
0.8	lows Selec	:ted									+05
				Name 🗠			Туре	Version	Status	Description	Actions
				sma01.mex-amp.inlab			SMA	13.6.2-023	Registered	SMA	Z # 1
Pag	po Size: 2	5 ~	Total Entries: 1								K < 🚺 > XI

#### 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 APIeindzoekopdracht (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 APIeindzoekopdracht (standaard is 30 dagen).

cisco Secure×	Dashboard Integrations Orchestration Beta	Administration	
Settings Your Account Devices API Clients V Integrations Available Integrations	Add New SMA Email Module Module Name* SMA Email Registered Device* sma01.mex-amp.inlab	/	Quick Start When configuring SMA Email integration, you must first enable the integration in SMA. You then enable Cisco Threat Response in Security Services Exchange (SSE), add the device and register it. After this is completed, you add the SMA Email module.
Users	sma01.mex-amp.inlab Type SMA W ef8cc926-9366-46bd-8285-4b7b1f3c324f IP Address 127.0.0.1 Request Timeframe (days)		<ul> <li>Required: SMA running AsyncOS 12.0 or later.</li> <li>Required: AsyncOS 13.6.2 for Cisco Content Security Management Appliances (SMA) is required to use the tiles in the SecureX dashboard.</li> <li>In SMA, navigate to Network &gt; Cloud Service Settings &gt; Edit Settings, enable integration and confirm the SMA is ready to accept a negisfration token.</li> <li>Click the Settings icon (gear) and then click Devices &gt; Manage Devices to be taken to Security Services Exchange.</li> <li>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.</li> <li>Specify the token expiration time (the default is 1 hour), and click Continue.</li> <li>Capy the generated token and confirm the device has been created.</li> <li>Navigate to your SMA (Network &gt; 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.</li> <li>Complete the Add New SMA Email Module form: <ul> <li>Module Name - Leave the default name or enter a name that is meaningful to you.</li> <li>Registered Device - From the drop-down list, choose the device you registered in Security Services Exchange.</li> <li>Required Device + From the drop-down list, choose the device you registered in Security Services Exchange.</li> <li>Required Device + SMA Email module configuration.</li> </ul> </li> </ul>

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.

Cisco M10	0V Management Virtual	Applance			Security Manageme
Nanagement Appliance	Email Web				
Certralized Services	Network	System Administration			
System Status					
					Selecteda DOE 🖉
Centralized Services					THE PARTY OF B
Email Security					
Spam Quarantine					
Disk Quote Used: 0.01		Messages; D		Not enabled	
Belley Mean and Outbreak Or	aratteat				
rendy, whos and outpreak Qu	Aranenes				
Disk Quota Used: 0.01		Messagesi D		Not enabled	
Centralized Reporting					
Processing Queue: 0.0	N	Status: Not enabled		Email Overview Report	I
Centralized Message Tracking					
Processing Queue: 0.0	5	Status: Not enabled	1	Track Messages	
Web Security					
Centralized Configuration Mar	nager				
Last Pu	blish: N/A	Status: Not enabled	1	View Appliance Status List	
Centralized Reporting					
Processing Queue: 0.0	s	Status: Not enabled	1	Web Overview Report	
System Information					
Uptime			Version Information	-	
Appliance Up	Since: (5h 1m 29s	12:37 (GMT -05:00)	Model: Operation System	M100V	
			Build Date:	26 Jun 2020 00:00 [GMT -	05:00)
CPU Utilization			Install Date:	01 Jul 2020 12:37 (GHT -0	5:00)
Security Management App	lance:	13.0%	Serial Number:	42140CEACA934A8DA508	-P960A86079E1
Quarantine Se	srvice:	0.0%			
Reporting Se	PVICE:	0.0%	Hardware		
tracking Se	evice:	0.0%	RADD Status	Unknown	
Total CPU Utiliz	etion	13.0%			

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**.

Hanagement Appliance Email	Web		
Centralized Services Networ	k	rstem red ministration	
Sustem Status			
Security Appliances	-		
Email Spam Quarantine Policy, Virus and Outbreak Quarantines			
Centralized Reporting	snone:	Service disabled	-
Web	nunes:	Higration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.	
Centralized Configuration Manager	orting:	Enabled, using 0 licenses	2
Centralized Upgrade Nanager	cking:	Enabled, using 0 licenses	
Centralized Web Configuration #	Manager:	Enabled, using 0 licenses	
Centralized Web R	eporting:	Enabled, using 0 licenses	4
Centralized Upgrades	for Web:	Service disabled	
ecurity Appliances Email Add Email Appliance			
lo appliances have been added.			
Web			
Add Web Appliance			
lo appliances have been added.			
le Analysis			
File Analysis G	lient ID:	06_VLNSMA88625410_42140CEACA934AEDA508-F960AB6079E1_M100V_000000	
		Key: 🗸 Selecte	٥

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

	Indu Cisco M10	00V		Security Management Appliance is gett
	CISCO Content Security	Management Virtual	Appliance	
	Forming enterine represente	cmail web		
•	Centralized Services	Network	System Administration	

#### Security Appliances

entralized Service Status	
Spam Quarantine:	Service disabled
Policy, Virus and Outbreak Quarantines:	Service disabled
	Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.
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
Email Add Email Appliance Io appliances have been added.	
Web Add Web Appliance	
ile Analysis	
File Analysis Client ID:	06_VLNSMA88625410_42140CEACA934AEDA508-F960AB6079E1_M100V_000000
	Key: 🖋 Selecte
opyright © 2008-2020 Cisco Systems, Inc. All rights	reserved.   Privacy Statement

## 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.

vices	Network	Syste
	▶ IP Interfaces	
	Listeners	Network > IP-interfaces
<b>ΙΡ Ι</b>	nterfaces	Network > II -Interfaces
_		
Netw	ork Interfaces and IP	Add
Add	ID Interface	
Add	TP Interface	
Name	e	
Mana	a a mart	
Mana		
LJ Clust	ter Communication Service	ESA-beheerinterface
Appliance	ter Communication Service ce Management	ESA-beheerinterface
Appliant	ter Communication Service ce Management p	ESA-beheerinterface
Appliance MHTTP	ter Communication Service ce Management P	ESA-beheerinterface
Appliance MITTP	ter Communication Service ce Management P PS rect HTTP requests to HTTPS (HTTP and HTTPS Se	ESA-beheerinterface
Appliance Appliance HTTP Redu Asynco	ter Communication Service ce Management p PS rect HTTP requests to HTTPS (HTTP and HTTPS Se <mark>S API</mark>	ESA-beheerinterface
Appliance MITTP MITTP Reduin Asyncol HITTPS p	ter Communication Service ce Management P PS rect HTTP requests to HTTPS (HTTP and HTTPS Se S API st Generation portal of your appliance uses Async ports. Make sure that the trailblazer HTTPS port is	ESA-beheerinterface ervices will be turned on)  OS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazerc opened on the firewall.
Appliance MHTTP MHTTP Redu Asyncol The Nex HTTPS p	ter Communication Service ce Management p PS rect HTTP requests to HTTPS (HTTP and HTTPS Se S API xt Generation portal of your appliance uses Async ports. Make sure that the trailblazer HTTPS port is NOCS API HTTP	ESA-beheerinterface ervices will be turned on) OS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazer opened on the firewall.
Appliant Appliant HTTP HTTP Redui Asynco: The Nex HTTPS p Asyn Asyn Asyn	ter Communication Service ce Management p PS rect HTTP requests to HTTPS (HTTP and HTTPS Se S API ext Generation portal of your appliance uses Async ports. Make sure that the trailblazer HTTPS port is NCOS API HTTP NCOS API HTTPS	ESA-beheerinterface ervices will be turned on) OS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazer opened on the firewall.
Appliance Appliance HTTP HTTP Redur Asyncol HTTPS p Asyn Asyn Spam Q Spam Q	ter Communication Service ce Management p PS rect HTTP requests to HTTPS (HTTP and HTTPS Se S API ext Generation portal of your appliance uses Async ports. Make sure that the trailblazer HTTPS port is NOOS API HTTP NOOS API HTTPS Quarantine	ESA-beheerinterface ervices will be turned on) OS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazers opened on the firewall.
Appliance Appliance HTTP HTTP Redu Asynco HTTPS p Asyn Spam Q Spam Q	ter Communication Service ce Management p PS rect HTTP requests to HTTPS (HTTP and HTTPS Se S API ext Generation portal of your appliance uses Async ports. Make sure that the trailblazer HTTPS port is NOOS API HTTP NOOS API HTTPS Quarantine m Quarantine HTTP	ESA-beheerinterface ervices will be turned on) OS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazerc opened on the firewall.
Applians Applians HTTP HTTP Redu Asyncol The Nex HTTPS p Asyn Spam Q Spam Q Spam	ter Communication Service ce Management P PS rect HTTP requests to HTTPS (HTTP and HTTPS Se S API ext Generation portal of your appliance uses Async ports. Make sure that the trailblazer HTTPS port is INCOS API HTTP INCOS API HTTPS Quarantine In Quarantine HTTP In Quarantine HTTPS	ESA-beheerinterface ervices will be turned on) OS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazer opened on the firewall.
Appliance Appliance HTTP HTTP Redur Asyncol Asyncol Asyncol Asyncol Spam Spam Spam Spam Spam Spam	ter Communication Service ce Management p PS rect HTTP requests to HTTPS (HTTP and HTTPS Se S API Art Generation portal of your appliance uses Async ports. Make sure that the trailblazer HTTPS port is NOOS API HTTP NOOS API HTTP Quarantine m Quarantine HTTP m Quarantine HTTPS rect HTTP requests to HTTPS (HTTP and HTTPS Se	ESA-beheerinterface ervices will be turned on) OS API HTTP/HTTPS ports (6080/6443) and trailblazer HTTPS port (4431). You can use the trailblazerc opened on the firewall. ervices will be turned on)

#### 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 <u>ESA</u> of <u>WSA</u> afzonderlijk toevoegen.
- Technische ondersteuning en documentatie Cisco Systems