

Konfigurieren der SMA-Integration mit SecureX

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[SMA-Integration](#)

[SMA-Web](#)

[SMA-E-Mail](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[SecureX SMA-Kachel / SecureX Threat Response SMA-Modul zeigt den Fehler "Es ist ein unerwarteter Fehler auf dem SMA-Modul aufgetreten" an](#)

[Video](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt den Prozess zur Konfiguration, Verifizierung und Fehlerbehebung der Integration der Content Security Management Appliance (SMA) in SecureX.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- SMA mit AsyncOS 13.6.2 (für SMA-E-Mail-Modul)

- SMA mit AsyncOS 12.5 (für SMA - Web-Modul)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

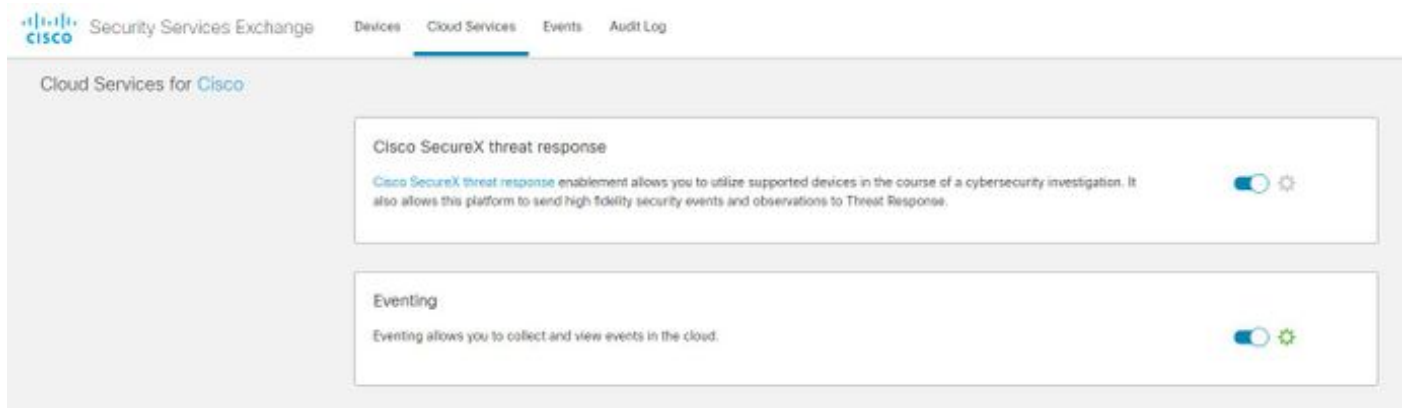
Konfiguration

SMA-Integration

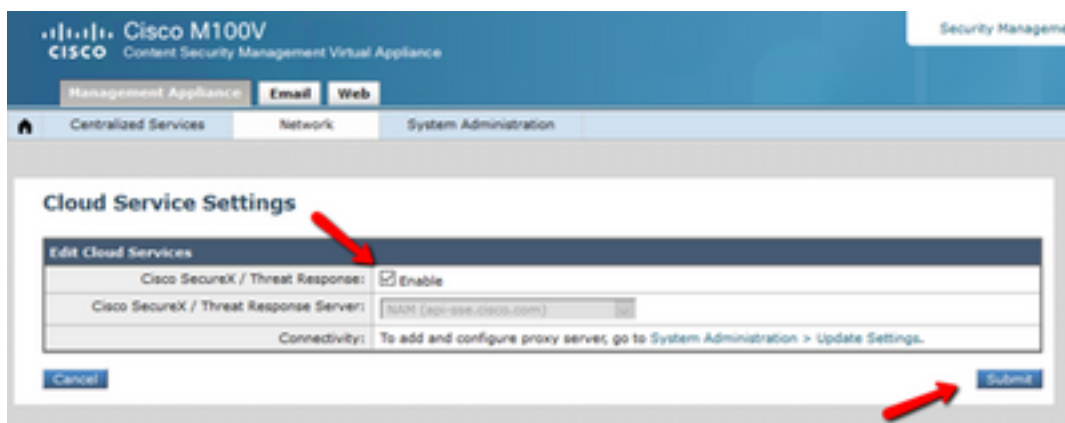
Schritt 1: Navigieren Sie in SMA zu **Network > Cloud Service Settings > Edit Settings**, aktivieren Sie Integration, und bestätigen Sie, dass SMA bereit ist, ein Registrierungstoken zu akzeptieren.

Schritt 2: Klicken Sie auf das Symbol Settings (Geräte), und klicken Sie dann auf **Devices (Geräte) > Manage Devices (Geräte verwalten)**, um zum Security Services Exchange (SSE) zu gelangen.

Stellen Sie sicher, dass alle Optionen unter **Cloud-Services** aktiviert sind.



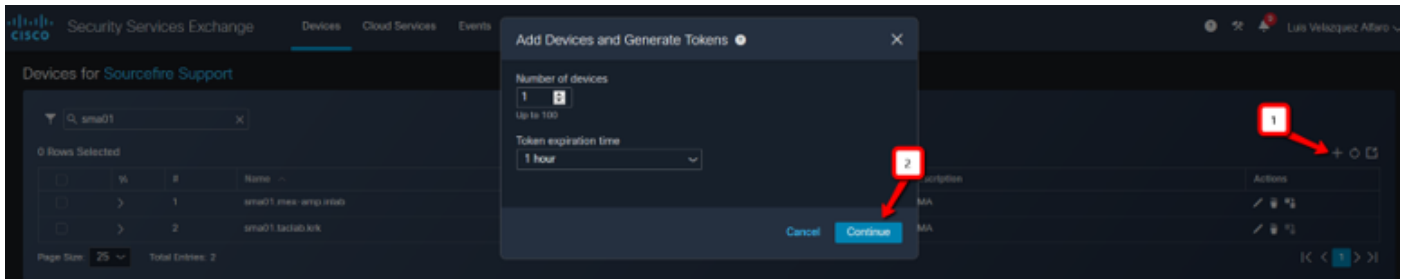
Schritt 3: Aktivieren Sie auf der Registerkarte "Cloud-Services" die Integration von Cisco Threat Response, und klicken Sie dann auf die Registerkarte "Geräte", und klicken Sie auf das Symbol +, um ein neues Gerät hinzuzufügen (erfordert ein SMA-Administratorkonto).



Schritt 4: Melden Sie sich von der SecureX-Instanz beim SSE-Portal an.

Schritt 5: Navigieren Sie im Secure X-Portal zu **Integrationen > Geräte > Geräte verwalten**.

Schritt 6: Erstellen Sie im SSE-Portal ein neues Token, geben Sie die Ablaufzeit des Tokens an (standardmäßig 1 Stunde), und klicken Sie auf **Weiter**.



Schritt 7: Kopieren Sie das generierte Token, und bestätigen Sie, dass das Gerät erstellt wurde.

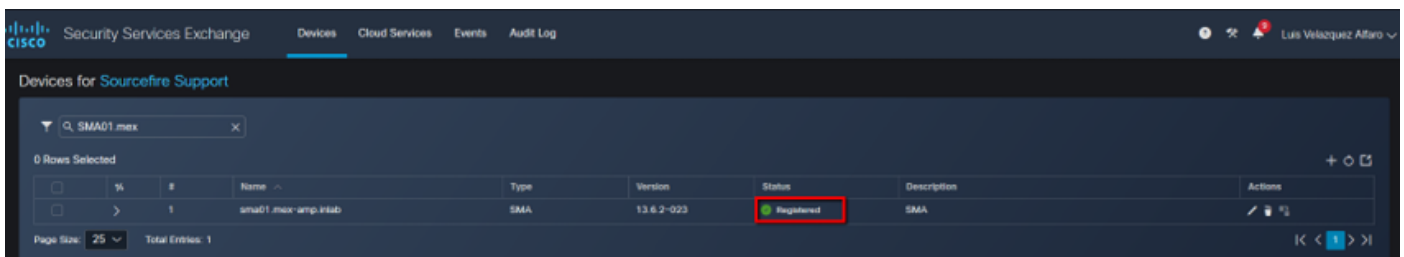
Schritt 8: Navigieren Sie zu Ihrem SMA (**Netzwerk > Cloud Service Settings**), um das Token einzufügen, und klicken Sie dann auf Registrieren.

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

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

Um eine erfolgreiche Registrierung zu bestätigen, überprüfen Sie den Status in **Security Services Exchange** und bestätigen Sie, dass SMA auf der Seite Geräte angezeigt wird.



SMA-Web

Schritt 1: Füllen Sie das Formular Neues SMA-Webmodul hinzufügen aus:

- Modulname: Behalten Sie den Standardnamen bei, oder geben Sie einen für Sie sinnvollen Namen ein.
- Registriertes Gerät: Wählen Sie aus der Dropdown-Liste das Gerät aus, das Sie bei Security Services Exchange registriert haben.
- Anforderungszeitrahmen (Tage) - Geben Sie den Zeitrahmen (in Tagen) für die API-Endpunktanfrage ein (Standardwert: 30 Tage).

Schritt 2: Klicken Sie auf Speichern, um die SMA-Webmodulkonfiguration abzuschließen.

SMA-E-Mail

Schritt 1: Füllen Sie das Formular Neues SMA-E-Mail-Modul hinzufügen aus.

- Modulname: Behalten Sie den Standardnamen bei, oder geben Sie einen für Sie sinnvollen Namen ein.
- Registriertes Gerät: Wählen Sie aus der Dropdown-Liste das Gerät aus, das Sie bei Security Services Exchange registriert haben.
- Anforderungszeitrahmen (Tage) - Geben Sie den Zeitrahmen (in Tagen) für die API-Endpunktanfrage ein (Standardwert: 30 Tage).

The screenshot displays the 'Add New SMA Email Module' configuration page in the Cisco SecureX interface. The page is divided into a left sidebar with navigation options (Settings, Your Account, Devices, API Clients, Integrations, Users) and a main content area. The main content area contains a form with the following fields:

- Module Name:** SMA Email
- Registered Device:** sma01_mex-amp.inlab (indicated by a red arrow)
- Request Timeframe (days):** (empty field)

Below the form are 'Save' and 'Cancel' buttons. On the right side, a 'Quick Start' section provides instructions. A red-bordered box highlights a requirement: 'Required: AsyncOS 13.6.2 for Cisco Content Security Management Appliances (SMA) is required to use the tiles in the SecureX dashboard.' Below this, a numbered list of 8 steps provides detailed instructions for enabling the integration and registering the device.

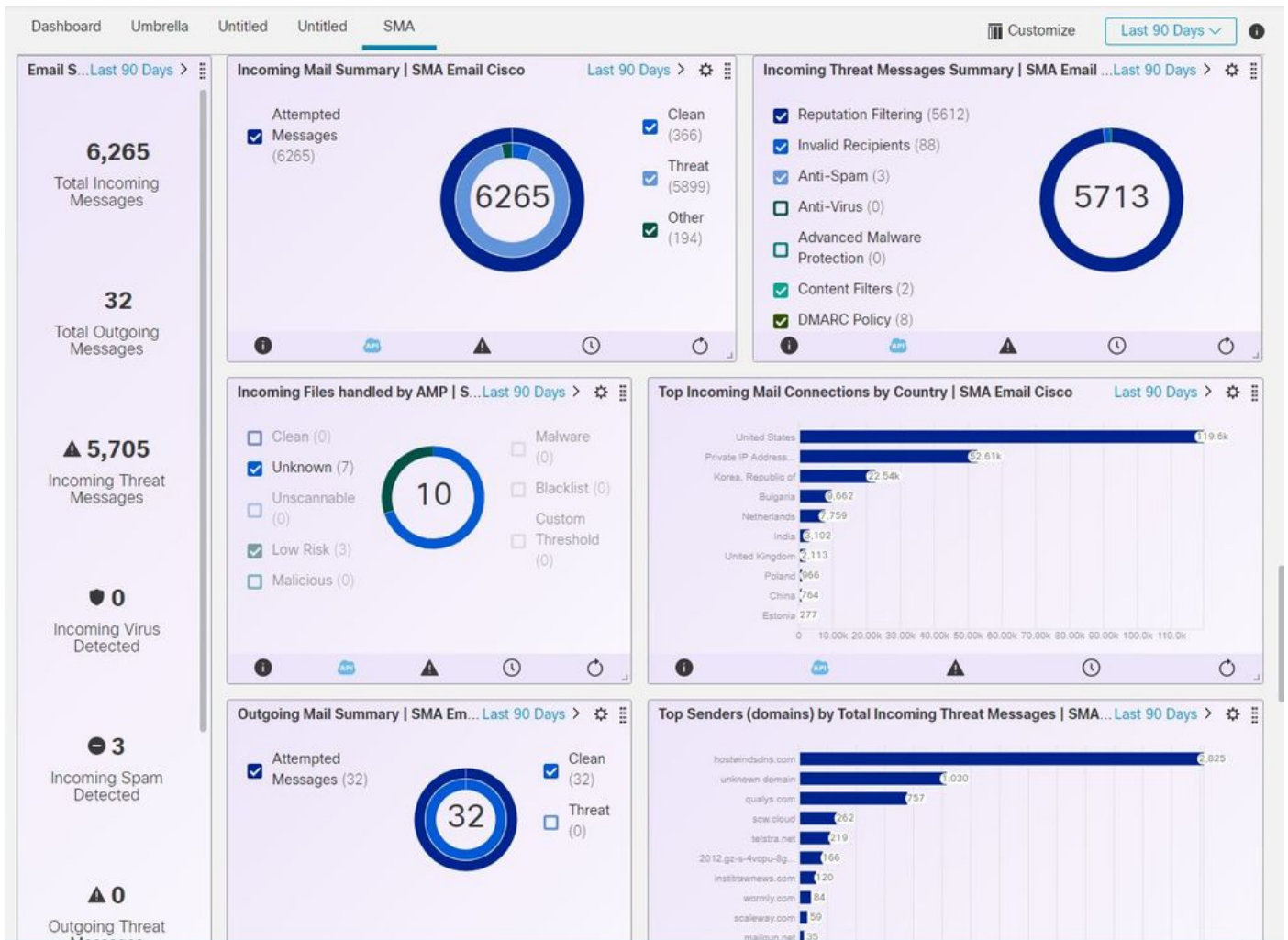
Wenn der Name des SMA-Geräts nicht im Dropdown-Menü angezeigt wird, geben Sie den Namen in das Dropdown-Feld ein, um den Namen zu durchsuchen.

Schritt 2: Klicken Sie auf **Speichern**, um die Konfiguration des SMA-E-Mail-Moduls abzuschließen.

Überprüfung

Schritt 1: Fügen Sie ein neues Dashboard hinzu, und fügen Sie die Kacheln hinzu, um die Informationen anzuzeigen, die Sie von Ihrem SMA-Modul interessieren.

Die Geräteinformationen finden Sie in diesem Abschnitt.



Schritt 2: SMA-Version überprüfen

Navigieren Sie im SMA zu **Home > Version Information (Startseite > Versionsinformationen)**.

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:	42140CBACAS34A2DASDB-F960AB6079E1
Hardware	
RAID Status:	Unknown

Wenn nach der Integration keine Daten für SecureX verfügbar sind. Sie können die nächsten Schritte ausführen.

Schritt 1: Überprüfen Sie, ob ESA/WSA-Appliances dem SMA Bericht erstatten.

Navigieren Sie auf der SMA zu **Zentrale Dienste > Sicherheitslösungen**, und überprüfen Sie, ob die ESA/WSA-Geräte unter **Sicherheitslösungen** angezeigt werden.

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: Migration configuration need to be completed before enabling Centralized Quarantines service from respective ESAs.

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

Schritt 2: Überprüfen Sie, ob die SMA-Lizenz für **zentrales E-Mail-Tracking** unter **Zentrale Dienste > Sicherheitslösungen** lizenziert und aktiviert ist.

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
	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

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](#)

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Tip: Wenn Sie beim Durchführen von Untersuchungen oder beim Hinzufügen von Kacheln zu SecureX einen Timeout-Fehler erhalten, kann dies auf eine große Menge an Informationen zurückzuführen sein, die von Ihren Geräten gesendet werden. Versuchen Sie, die Einstellung (**Tag**) für die **Anforderung Timeframe (Tage)** in der Modulkonfiguration zu senken.

Auf der SMA SSH-Konsole verwendete Befehle

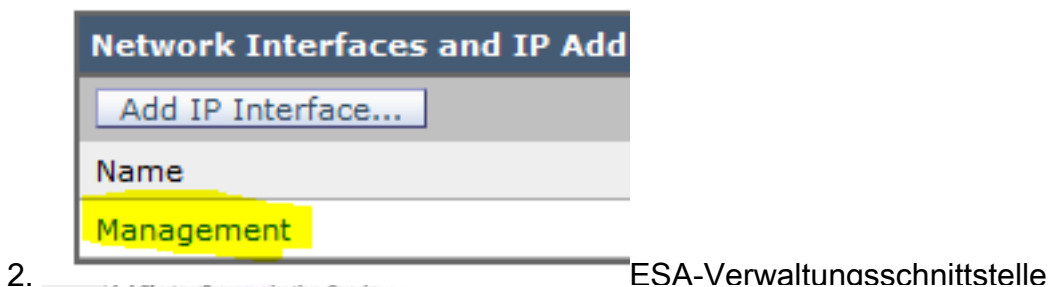
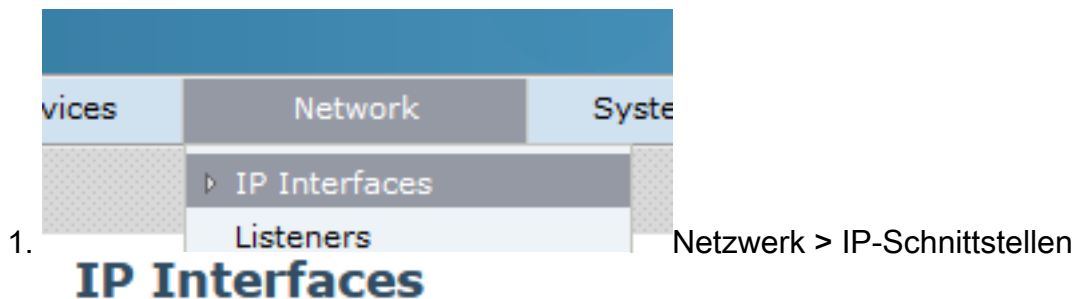
- Um die tatsächliche Version und Lizenz der SMA zu überprüfen, können diese Befehle verwendet werden. >Showlizenz>Version
- Integrationsprotokolle mit Registrierungseignissen >ctr_logs/ctr_logs.current
- Verbindungstest zum SSE-Proton >telnet api-sse.cisco.com 443

SecureX SMA-Kachel / SecureX Threat Response SMA-Modul zeigt den Fehler "Es

ist ein unerwarteter Fehler auf dem SMA-Modul aufgetreten" an

SMA erfordert die über die Verwaltungsschnittstelle aktivierte HTTP- und HTTPS-Konfiguration der AsyncOS-API für die Kommunikation mit dem SecureX/CTR-Portal.

Wenn Sie diese Einstellung über die Benutzeroberfläche des SMA-Portals am Standort konfigurieren möchten, gehen Sie zu **Network > IP Interfaces > Management Interface > AsyncOS API** und aktivieren Sie HTTP und HTTPS.



Async-API > HTTP und HTTPS

Für eine CES (Cloud-basierte SMA) muss diese Konfiguration vom Backend aus von einem SMA TAC-Techniker vorgenommen werden. Es ist der Zugriff auf den Support-Tunnel der betroffenen CES erforderlich.

Video

Zugehörige Informationen

- Videos zur Konfiguration Ihrer Produktintegrationen finden Sie [hier](#).

- Wenn Ihr Gerät nicht von einem SMA verwaltet wird, können Sie Module für [ESA](#) oder [WSA](#) einzeln hinzufügen.
- [Technischer Support und Dokumentation für Cisco Systeme](#)