Konfigurieren der SMA-Integration mit SecureX

Inhalt

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.

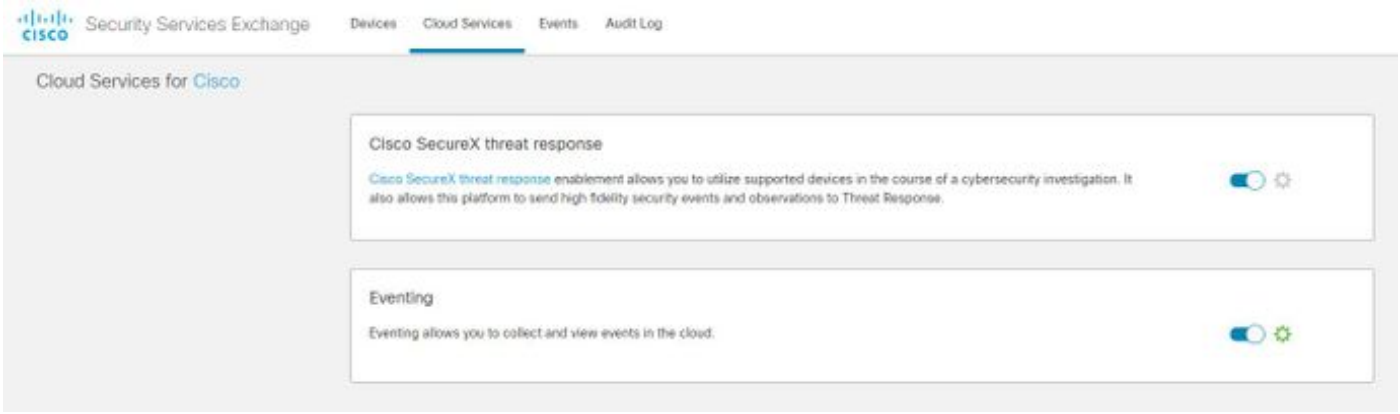
Konfiguration

SMA-Integration

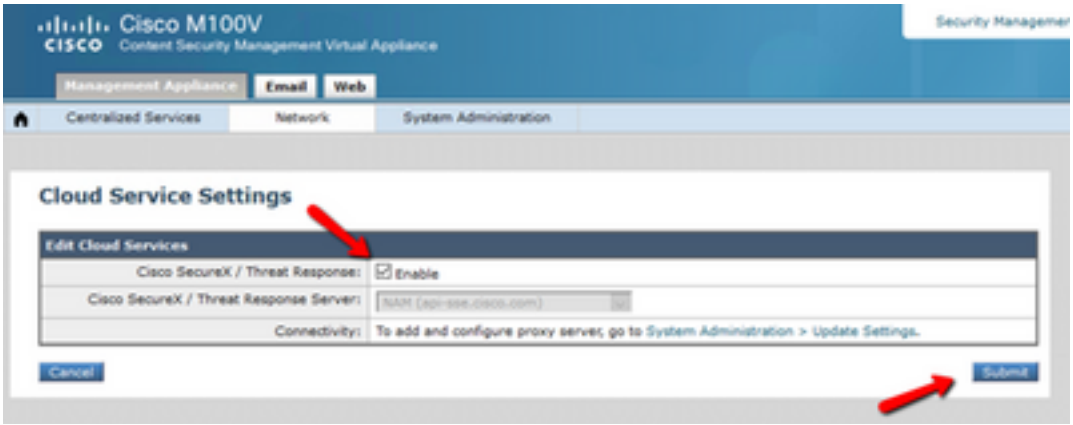
Schritt 1: Navigieren Sie in SMA zu **Network > Cloud Service Settings > Edit Settings**, aktivieren Sie Integration, und bestätigen Sie, dass SMA bereit ist, ein Registrierungstoken zu akzeptieren.

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.



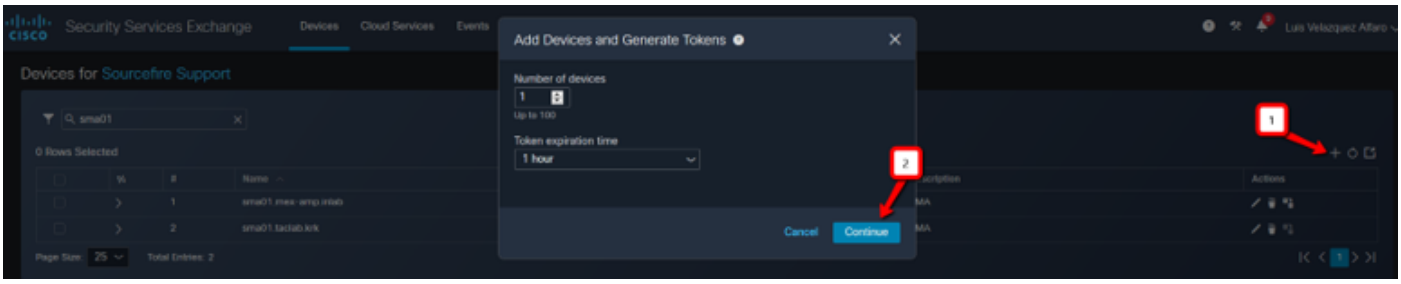
Schritt 3: Aktivieren Sie auf der Registerkarte "Cloud-Services" die Integration von Cisco Threat Response, und klicken Sie dann auf die Registerkarte "Geräte", und klicken Sie auf das Symbol +, um ein neues Gerät hinzuzufügen (erfordert ein SMA-Administratorkonto).



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

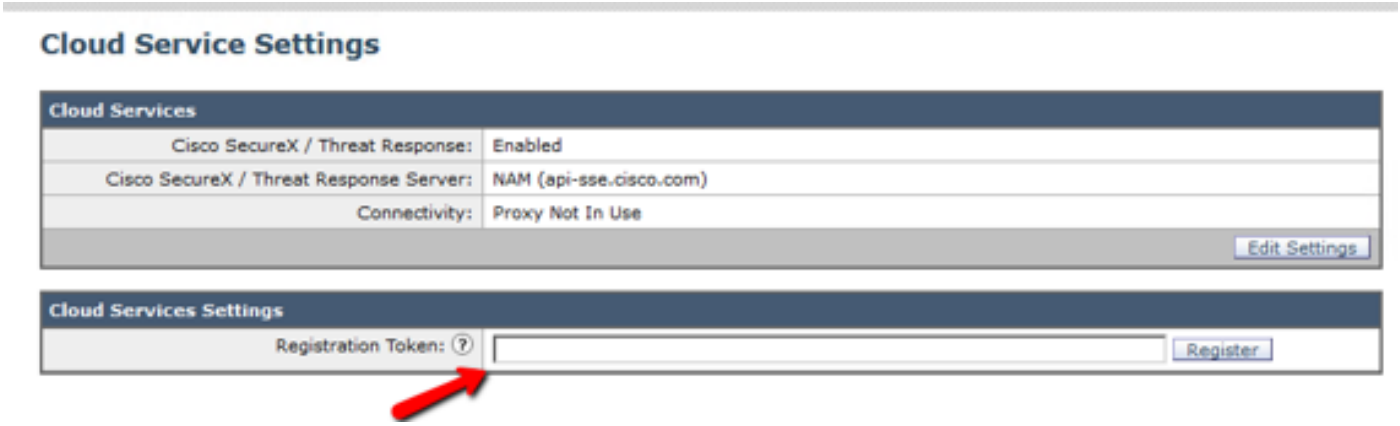
Schritt 5: Navigieren Sie im Secure X-Portal zu **Integrationen > Geräte > Geräte verwalten.**

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**.

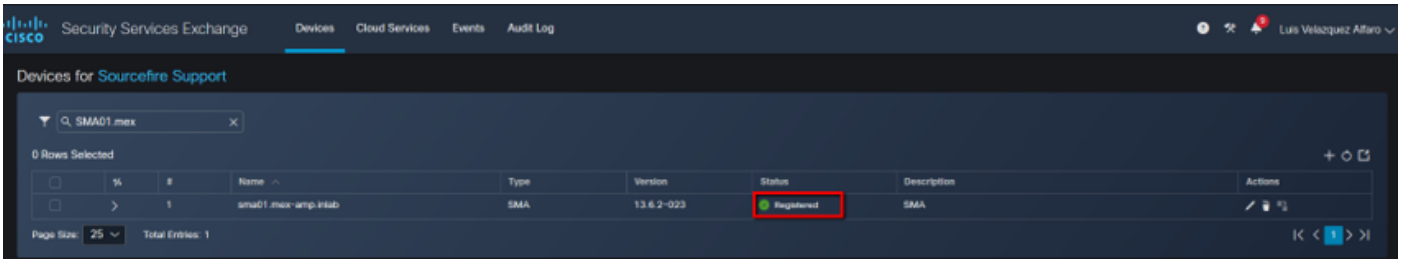


Schritt 7: Kopieren Sie das generierte Token, und bestätigen Sie, dass das Gerät erstellt wurde.

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



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:

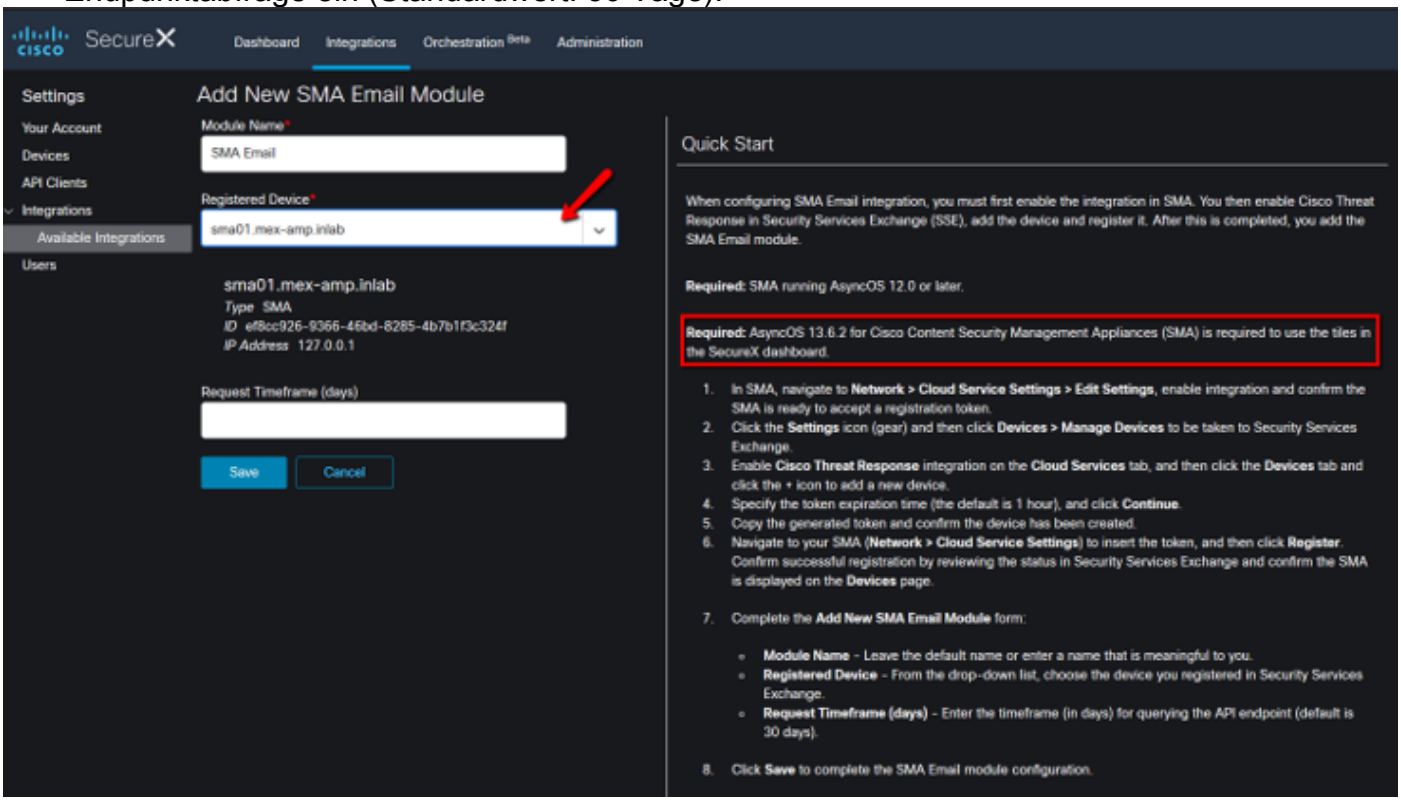
- Modulname: Behalten Sie den Standardnamen bei, oder geben Sie einen für Sie sinnvollen Namen ein.
- Registriertes Gerät: Wählen Sie aus der Dropdown-Liste das Gerät aus, das Sie bei Security Services Exchange registriert haben.
- Anforderungszeitrahmen (Tage) - Geben Sie den Zeitrahmen (in Tagen) für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



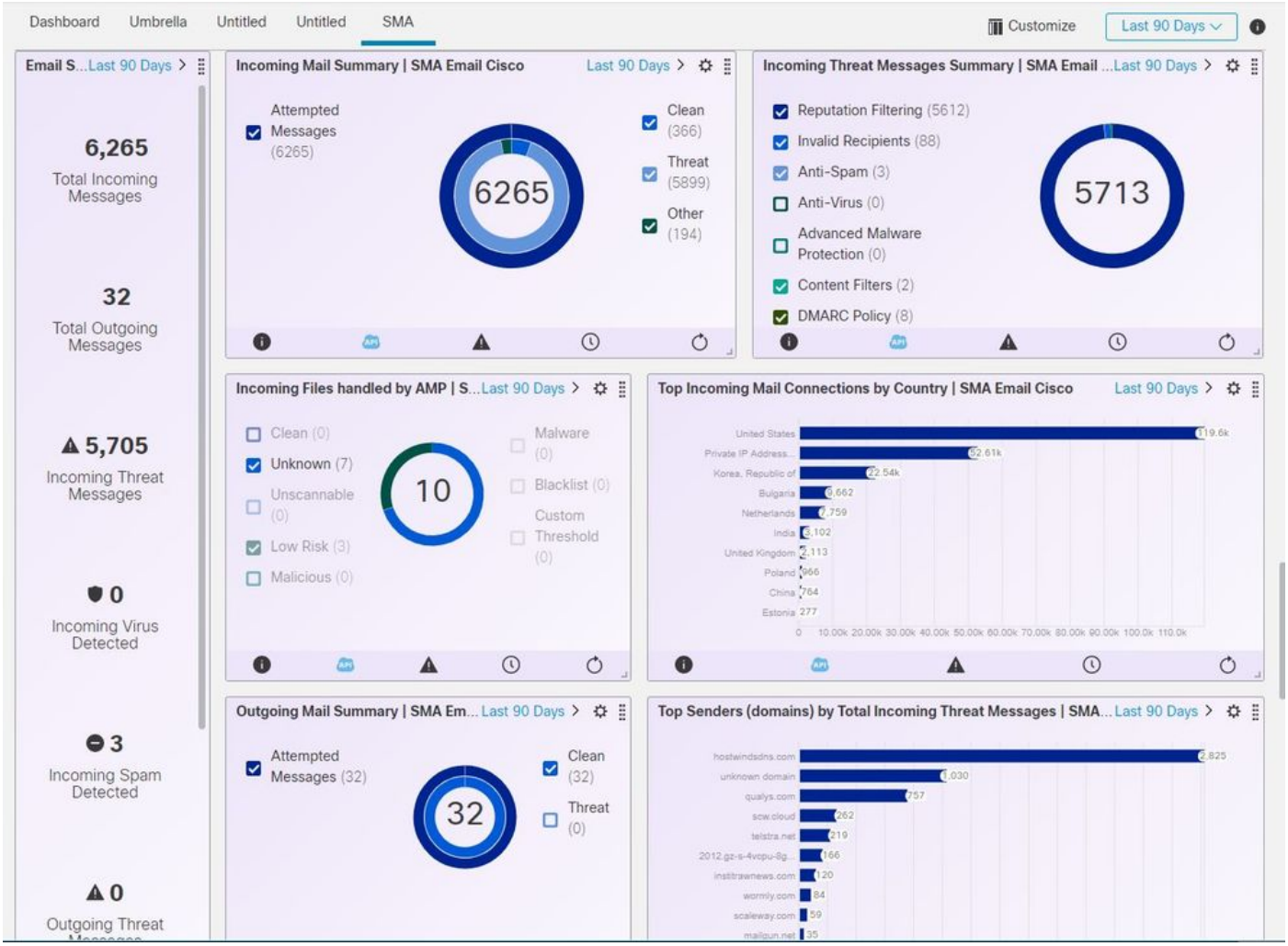
Wenn der Name des SMA-Geräts nicht im Dropdown-Menü angezeigt wird, geben Sie den Namen in das Dropdown-Feld ein, um den Namen zu durchsuchen.

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

Überprüfung

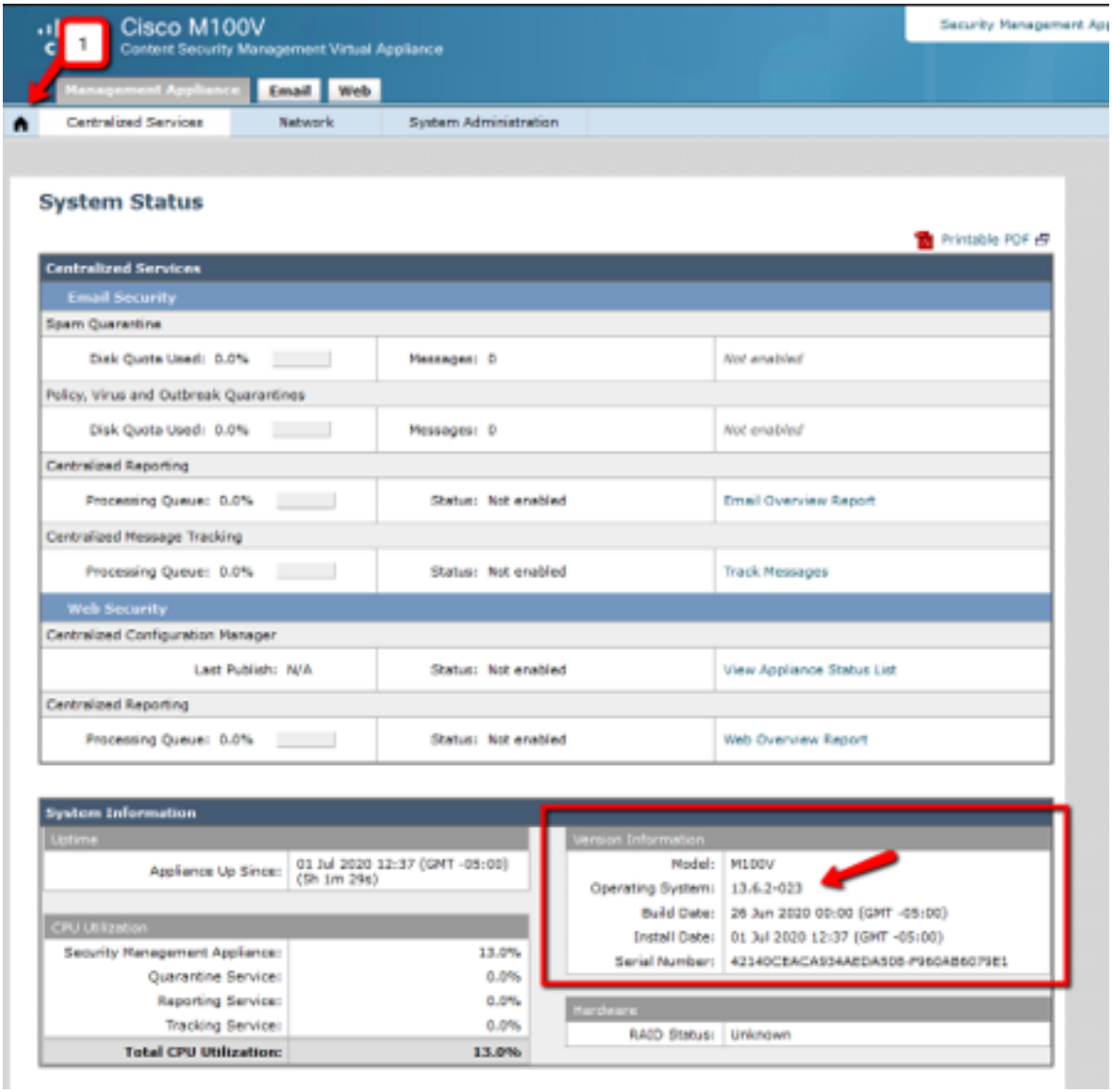
Schritt 1: Fügen Sie ein neues Dashboard hinzu, und fügen Sie die Kacheln hinzu, um die Informationen anzuzeigen, die Sie von Ihrem SMA-Modul interessieren.

Die Geräteinformationen finden Sie in diesem Abschnitt.



Schritt 2: SMA-Version überprüfen

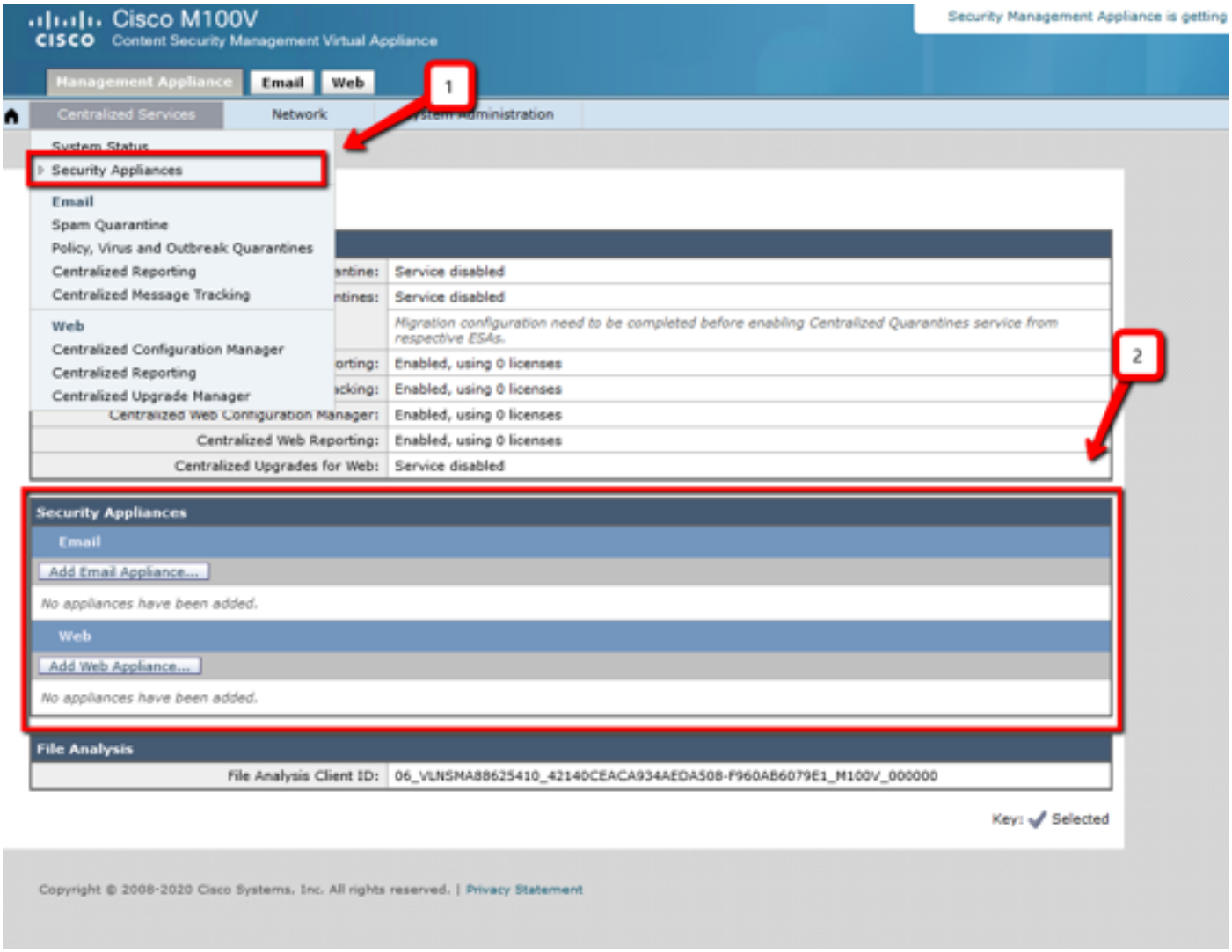
Navigieren Sie im SMA zu **Home > Version Information (Startseite > Versionsinformationen)**.



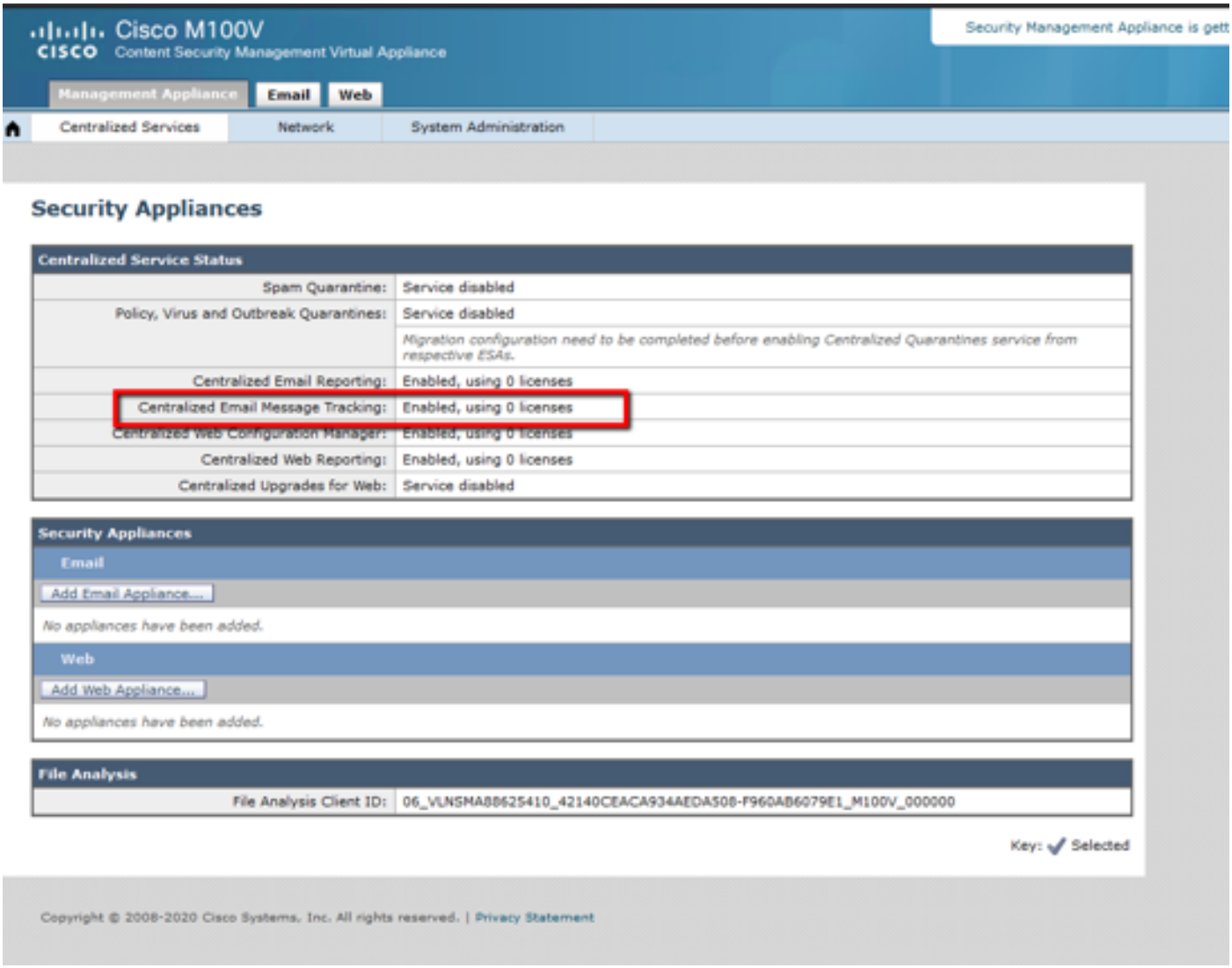
Wenn nach der Integration keine Daten für SecureX verfügbar sind. Sie können die nächsten Schritte ausführen.

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.



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



Fehlerbehebung

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

> **Tipp:** 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 **(Tage) für** die **Anforderung Timeframe (Tage)** in der Modulkonfiguration zu senken.

Auf der SMA SSH-Konsole verwendete Befehle

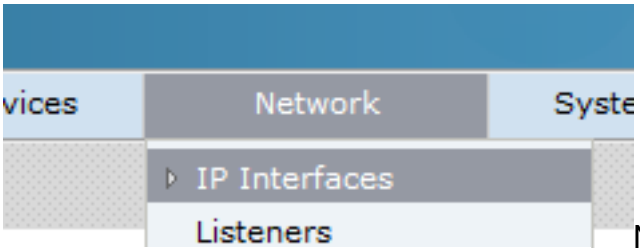
- Um die tatsächliche Version und Lizenz der SMA zu überprüfen, können diese Befehle verwendet werden. >Showlizenz>Version
- Integrationsprotokolle mit Registrierungsereignissen >ctr_logs/ctr_logs.current
- Verbindungstest zum SSE-Proton >telnet api-sse.cisco.com 443

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

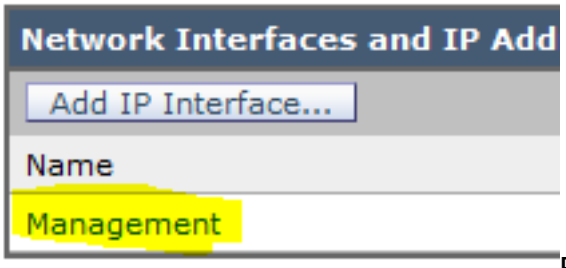
ist ein unerwarteter Fehler auf dem SMA-Modul aufgetreten" an

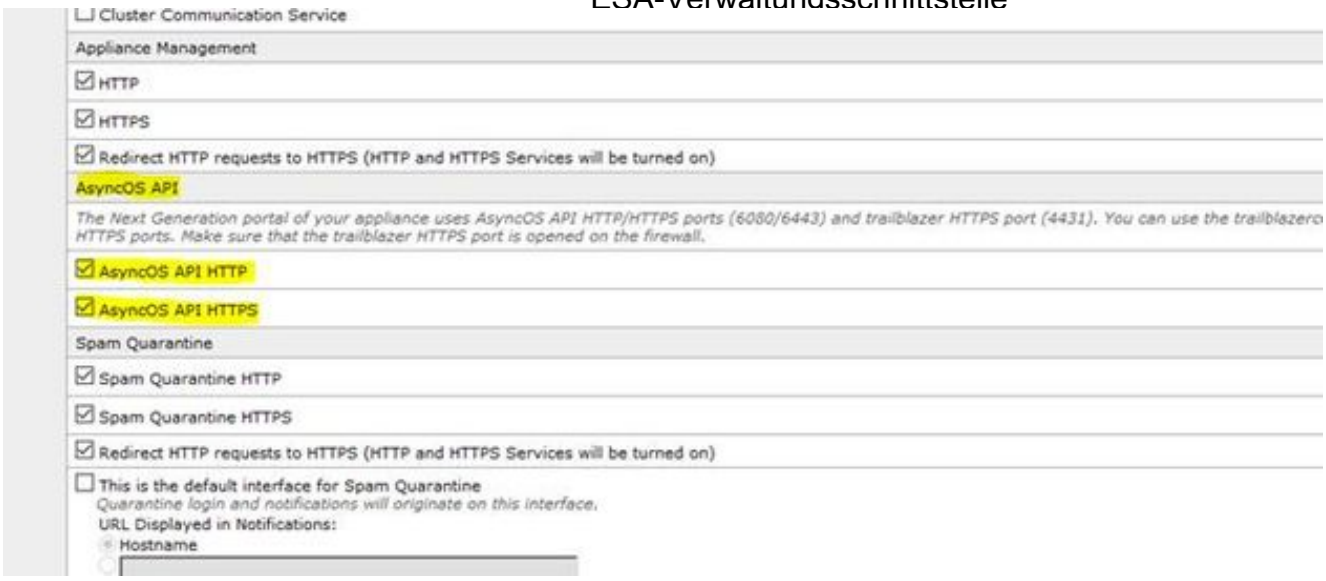
SMA erfordert die über die Verwaltungsschnittstelle aktivierte HTTP- und HTTPS-Konfiguration der AsyncOS-API für die Kommunikation mit dem SecureX/CTR-Portal.

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.

1. 

Netzwerk > IP-Schnittstellen


2. 

ESA-Verwaltungsschnittstelle
3. 

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