Fehlerbehebung: Integration von SecureX und Secure Email Appliance (ehemals ESA)

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Fehlerbehebung
ESA-Gerät wird weder im SecureX- noch im Security Services Exchange-Portal angezeigt
Die ESA fordert kein Registrierungstoken an.
Fehler bei der Registrierung aufgrund eines ungültigen oder abgelaufenen Tokens.
SecureX Dashboard zeigt keine Informationen des ESA-Moduls an.
Das SecureX ESA-Kachelmodul zeigt den Fehler "Es gab einen unerwarteten Fehler auf dem ESA-Modul" an.
Überprüfung
Integration von Video
Zugehörige Informationen

Einleitung

In diesem Dokument werden die Schritte zur Durchführung einer grundlegenden Analyse und die Fehlerbehebung für das Integrationsmodul SecureX und Insights and Secure Email Appliance beschrieben.

Brenda Marquez, Cisco TAC Engineer

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SecureX
- Austausch von Security Services
- Sichere E-Mails

Verwendete Komponenten

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

- Austausch von Security Services
- SecureX 1,54
- Secure Email C100V auf Softwareversion 13.0.0-392

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 Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die Cisco Secure E-Mail Appliance (ehemals E-Mail Security Appliance) bietet erweiterten Schutz vor Bedrohungen, um Bedrohungen schneller zu erkennen, zu blockieren und zu beseitigen, Datenverluste zu verhindern und wichtige Informationen bei der Übertragung mit End-to-End-Verschlüsselung zu schützen. Nach der Konfiguration enthält das Secure E-Mail Appliance-Modul Details zu den Observables. Sie können:

- Anzeigen von E-Mail-Berichten und Nachverfolgen von Daten aus mehreren Appliances in Ihrer Organisation
- Erkennung, Untersuchung und Beseitigung von Bedrohungen, die in E-Mail-Berichten und Nachrichtenspuren beobachtet wurden
- Schnelle Behebung der identifizierten Bedrohungen und Bereitstellung von empfohlenen Maßnahmen zur Abwehr der identifizierten Bedrohungen
- Dokumentieren der Bedrohungen, um die Untersuchung zu retten und die Zusammenarbeit von Informationen zwischen anderen Geräten zu ermöglichen

Die Integration eines Secure E-Mail Appliance-Moduls erfordert die Verwendung von Security Services Exchange (SSE). SSE ermöglicht einer sicheren E-Mail-Appliance die Registrierung bei Exchange, und Sie gewähren die ausdrückliche Berechtigung für den Zugriff auf die registrierten Geräte.

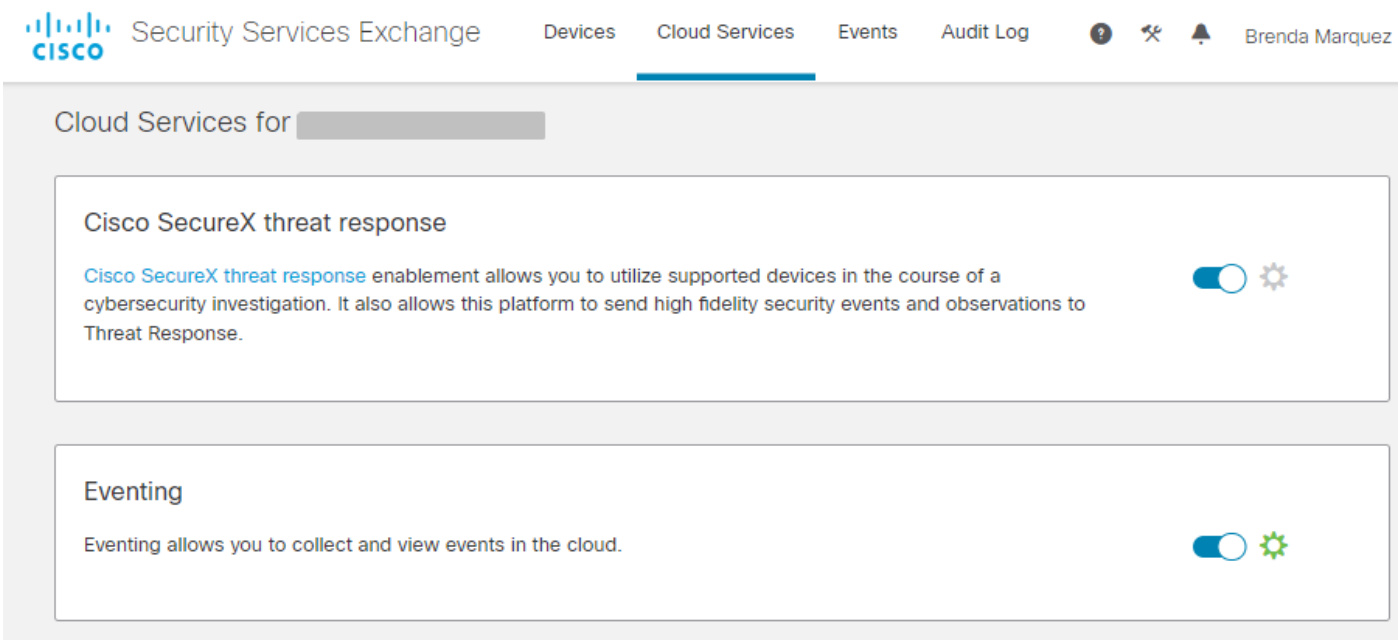
Wenn Sie mehr über die Konfiguration erfahren möchten, lesen Sie bitte die Details zum Integrationsmodul.

Fehlerbehebung

Um häufige Probleme bei der Integration von SecureX und Secure Email Appliance zu beheben, können Sie diese Schritte überprüfen.

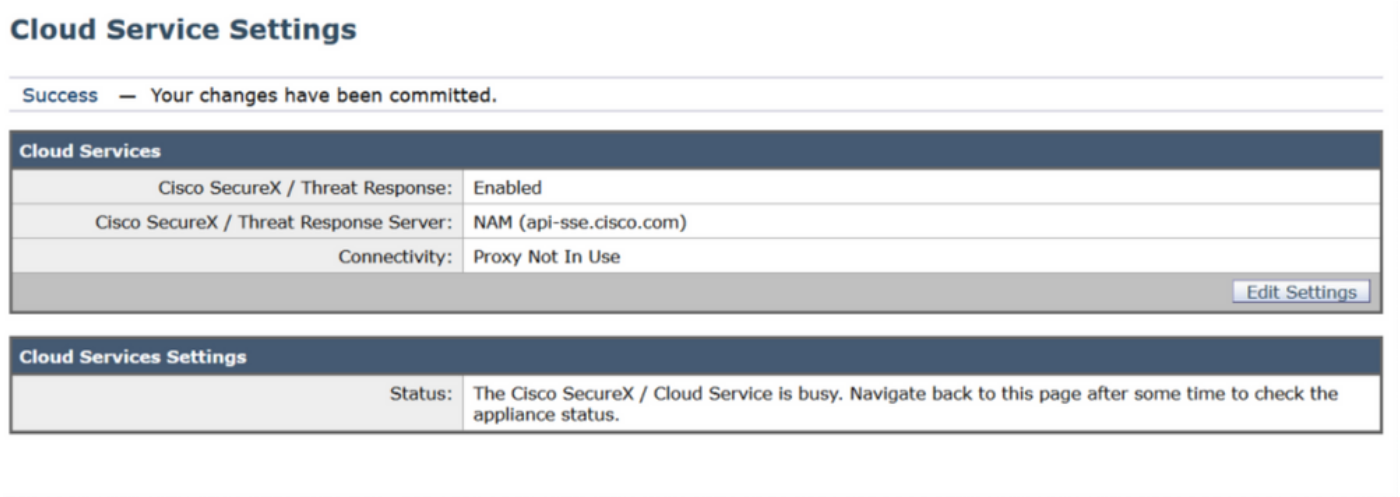
ESA-Gerät wird weder im SecureX- noch im Security Services Exchange-Portal angezeigt

Wenn Ihr Gerät nicht im SSE-Portal angezeigt wird, stellen Sie sicher, dass die **SecureX Threat Response-** und **Event-**Services im SSE-Portal aktiviert sind, navigieren Sie zu **Cloud-Services,** und aktivieren Sie die Services wie im folgenden Bild:



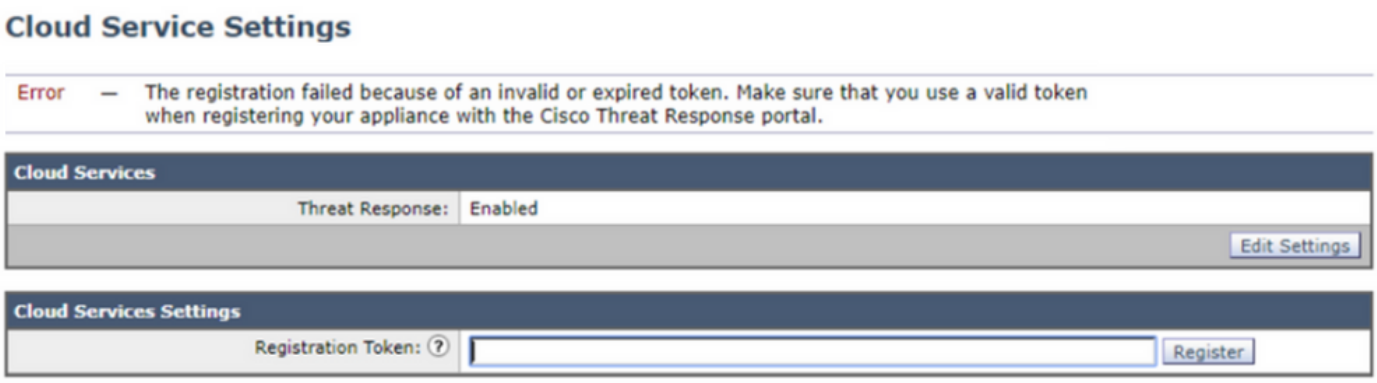
Die ESA fordert kein Registrierungstoken an.

Bitte bestätigen Sie die Änderungen, sobald Cisco SecureX/Threat Response aktiviert wurde. Andernfalls werden die Änderungen nicht auf den Cloud-Service-Abschnitt der ESA angewendet. Siehe Abbildung unten.



Fehler bei der Registrierung aufgrund eines ungültigen oder abgelaufenen Tokens.

Wenn die Fehlermeldung angezeigt wird: "Die Registrierung ist aufgrund eines ungültigen oder abgelaufenen Tokens fehlgeschlagen. Stellen Sie sicher, dass Sie ein gültiges Token für Ihre Appliance mit dem "Cisco Threat Response Portal" in der ESA-GUI wie in der Abbildung unten verwenden:



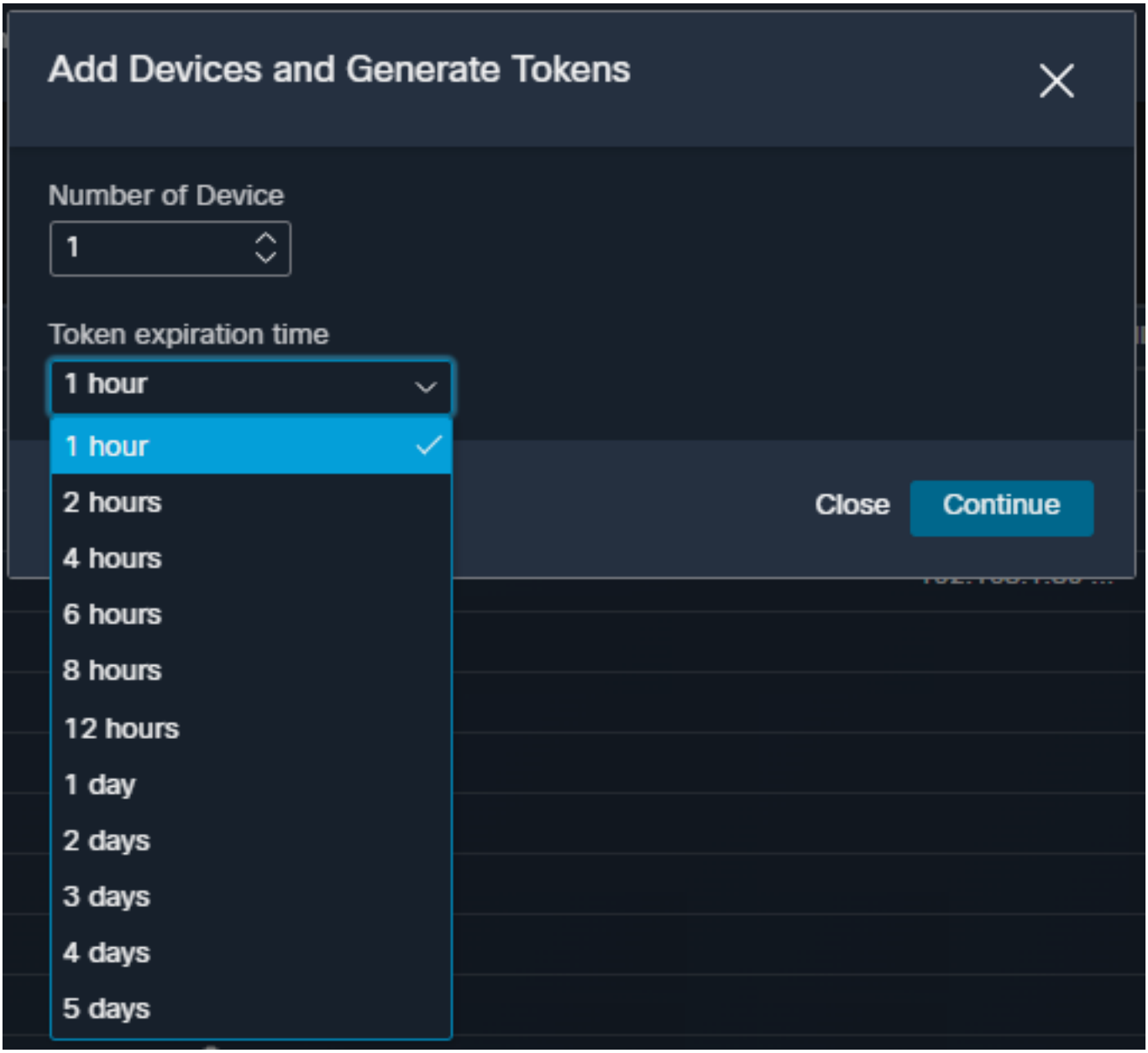
Stellen Sie sicher, dass das Token aus der richtigen Cloud generiert wird:

Wenn Sie die Europa-Cloud (EU) für die ESA verwenden, generieren Sie den Token unter https://admin.eu.sse.itd.cisco.com/

Wenn Sie Americas (NAM) Cloud für die ESA verwenden, generieren Sie das Token unter https://admin.sse.itd.cisco.com/

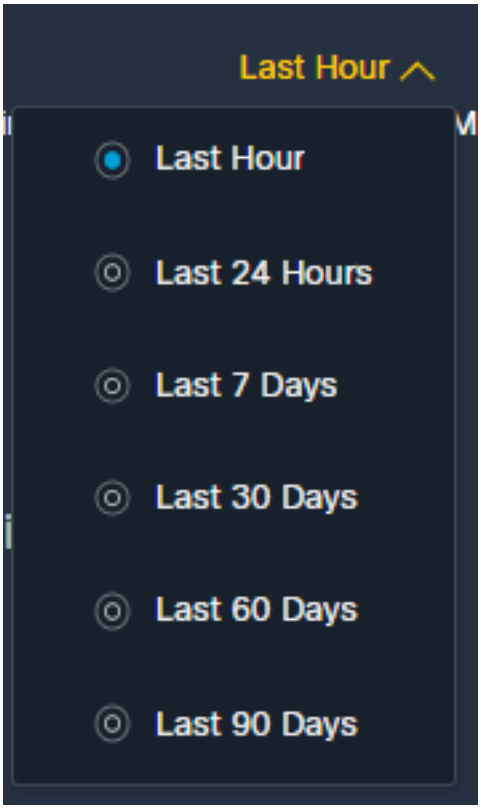
Security Services Exchange (SSE)-Portal:	NAM: https://admin.sse.itd.cisco.com/ EU: https://admin.eu.sse.itd.cisco.com/
Cisco SecureX-Portal	NAM: https://securex.us.security.cisco.com/ EU: https://securex.eu.security.cisco.com/
ESA Cisco SecureX/Threat Response Server:	NAM: api-sse.cisco.com EU: api.eu.sse.itd.cisco.com

Denken Sie auch daran, dass das Registrierungs-Token eine Ablaufzeit hat (wählen Sie die günstigste Zeit aus, um die Integration rechtzeitig abzuschließen), wie im Bild gezeigt.



SecureX Dashboard zeigt keine Informationen des ESA-Moduls an.

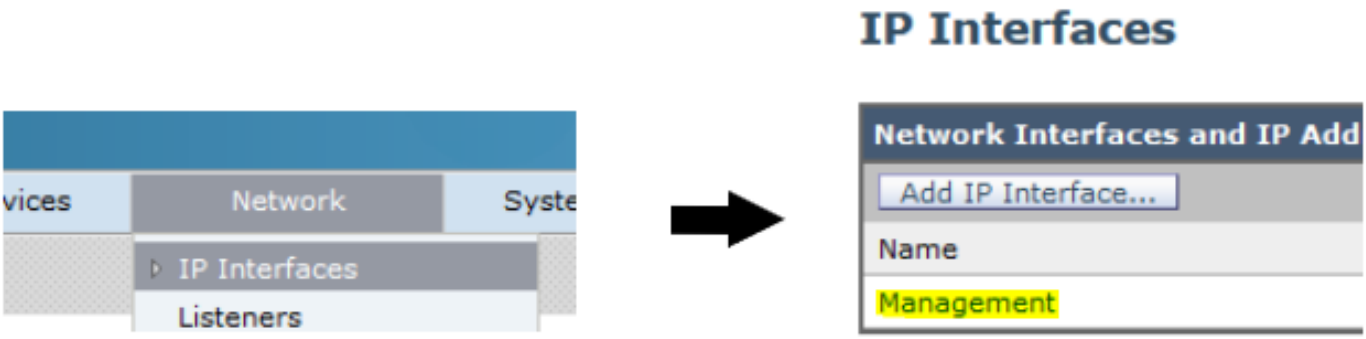
Sie können einen größeren Zeitraum in den verfügbaren Kacheln auswählen, von **Letzte Stunde** bis **Letzte 90 Tage**, wie im Bild unten gezeigt.

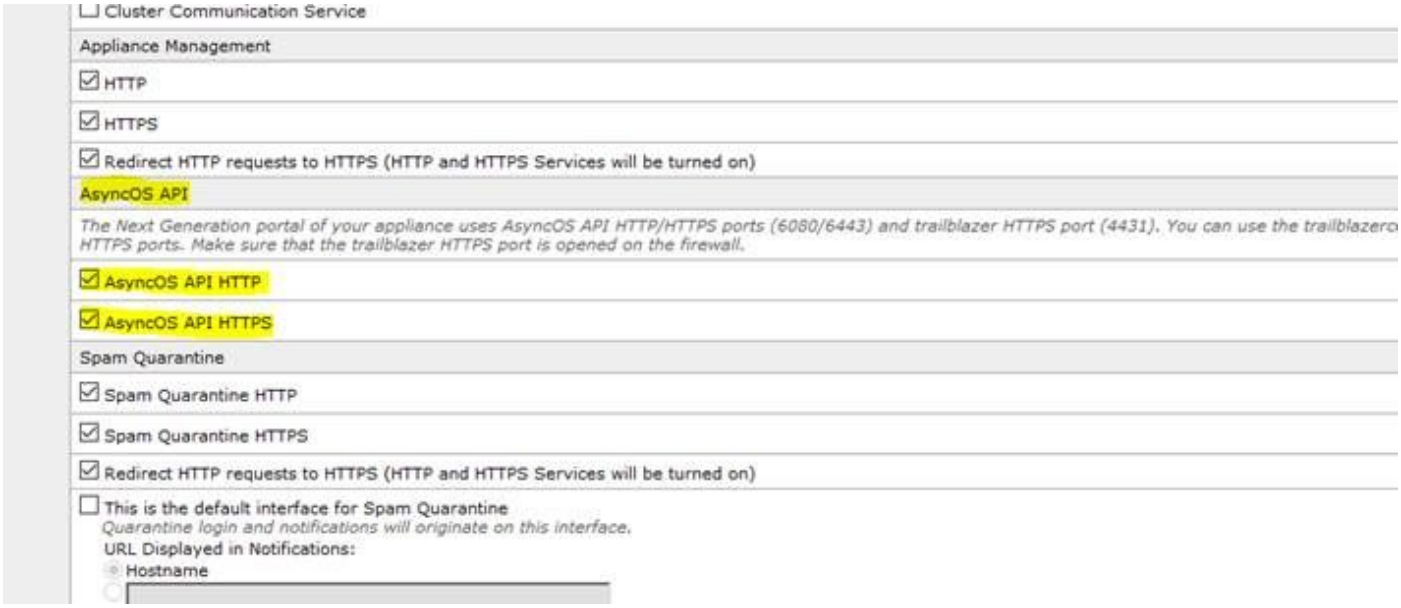


Andere Beispiele könnten sein, dass wir die Nachricht "Es gab ein Problem. Versuchen Sie es später erneut." oder sogar die Fehlermeldung "Es gab einen Client-Fehler im ESA-Modul: E4017 Gerät ist offline [409]". Überprüfen Sie, ob das Gerät noch als über das SSE-Portal registriert angezeigt wird. Wahrscheinlich wurde das Gerät deaktiviert und ist nicht mehr sichtbar. Versuchen Sie, dem SecureX-Portal ein neues Modul hinzuzufügen.

Das SecureX ESA-Kachelmodul zeigt den Fehler "Es gab einen unerwarteten Fehler auf dem ESA-Modul" an.

Für die ESA ist die Aktivierung der HTTP- und HTTPS-Konfiguration der AsyncOS-API über die Verwaltungsschnittstelle erforderlich, um mit dem SecureX/CTR-Portal zu kommunizieren. Für eine standortbasierte ESA-Konfiguration dieser Funktion über die ESA-Portal-GUI navigieren Sie zu **Netzwerk > IP-Schnittstellen > Verwaltungsschnittstelle > AsyncOS-API,** und aktivieren Sie HTTP und HTTPS, wie im Bild dargestellt.





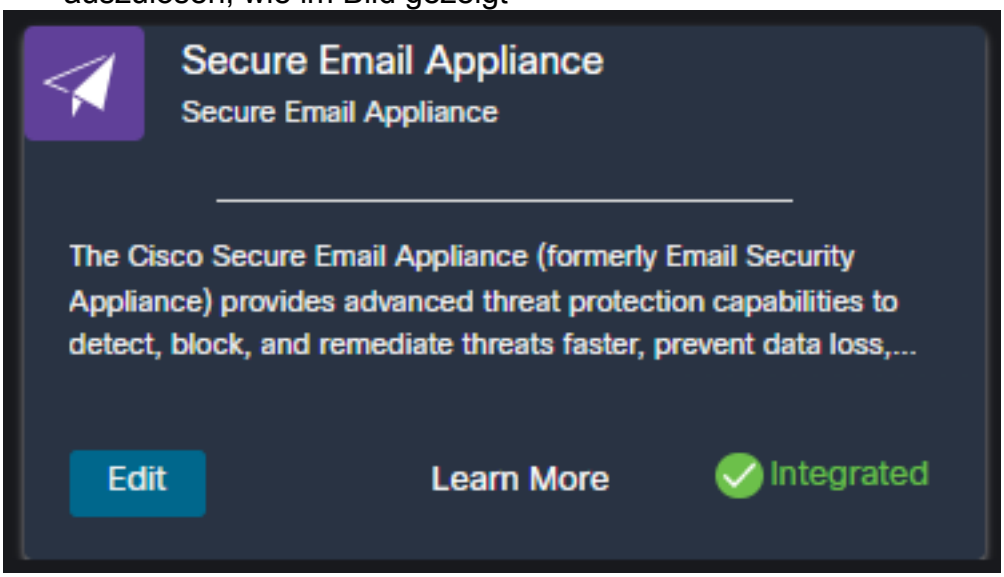
HTTP & HTTPS" />*Async API > HTTP & HTTPS*

Bei einer CES (Cloud Based ESA) muss diese Konfiguration vom Backend aus durch einen ESA TAC-Techniker durchgeführt werden. Sie erfordert Zugriff auf den Support-Tunnel der betroffenen CES.

Überprüfung

Sobald MobileIron als Quelle für Device Insights hinzugefügt wurde, wird der Verbindungsstatus einer **erfolgreichen REST**-API angezeigt.

- Sie sehen **den** Status **der REST**-APIverbindung
- Drücken Sie **aufSync** Now (Jetzt synchronisieren), um die erste vollständige Synchronisierung auszulösen, wie im Bild gezeigt



Sollte das Problem weiterhin mit der Integration von SecureX und Secure Email Appliance bestehen, lesen Sie diesen Artikel, um HAR-Protokolle vom Browser zu erfassen, und wenden Sie sich an den TAC-Support, um eine tiefere Analyse durchzuführen.

Integration von Video

Die Schritte zur Konfiguration der SecureX- und ESA-Integration finden Sie im nächsten Video.

Zugehörige Informationen

- Die Informationen in diesem Artikel finden Sie in diesem Video zur Integration von SecureX und ESA.
- Videos zur Konfiguration Ihrer Produktintegration finden Sie hier.
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.