Fehlerbehebung bei der Integration von XDR und Secure Email Appliance (ehemals ESA)

Inhalt

Einleitung

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

Voraussetzungen

Anforderungen

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

- XDR
- 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
- XDR
- 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 kennen.

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 stellt das Secure E-Mail Appliance-Modul Details zu den Observables bereit. Sie können:

- Anzeigen von E-Mail-Berichten und Nachverfolgen von Daten aus mehreren Appliances in Ihrer Organisation

- Identifizieren, Untersuchen und Beseitigen 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.

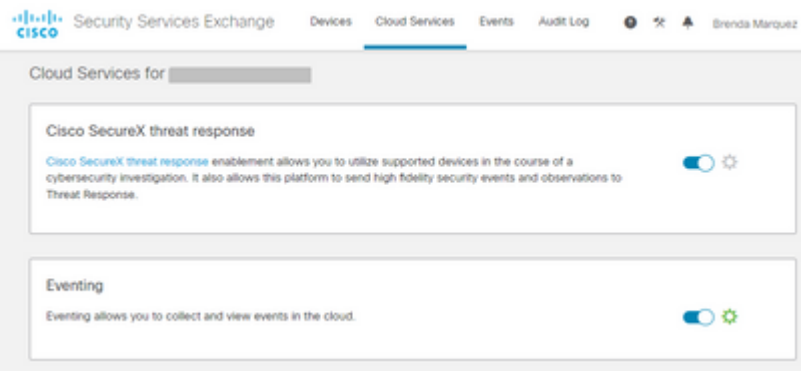
Wenn Sie mehr über die Konfiguration erfahren möchten, lesen Sie bitte diesen Artikel hier in den Details zum Integrationsmodul.

Fehlerbehebung

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

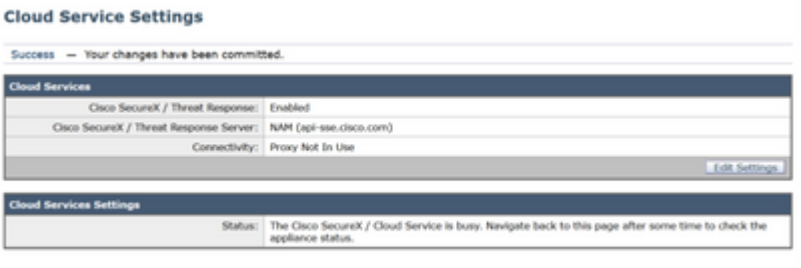
Das sichere E-Mail-Gerät wird im XDR- oder Security Services Exchange-Portal nicht angezeigt.

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



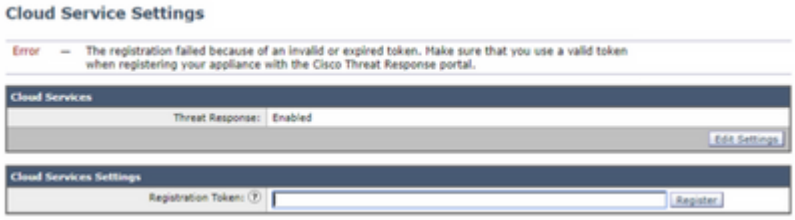
Secure Email fordert das Registrierungstoken nicht an

Bitte bestätigen Sie die Änderungen, sobald der Cisco XDR/Threat Response-Service aktiviert wurde. Andernfalls werden die Änderungen nicht auf den Cloud-Service-Abschnitt in der sicheren E-Mail angewendet. Weitere Informationen finden Sie in der 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 XDR Threat Response-Portal in der Secure Email GUI wie in der Abbildung unten verwenden:



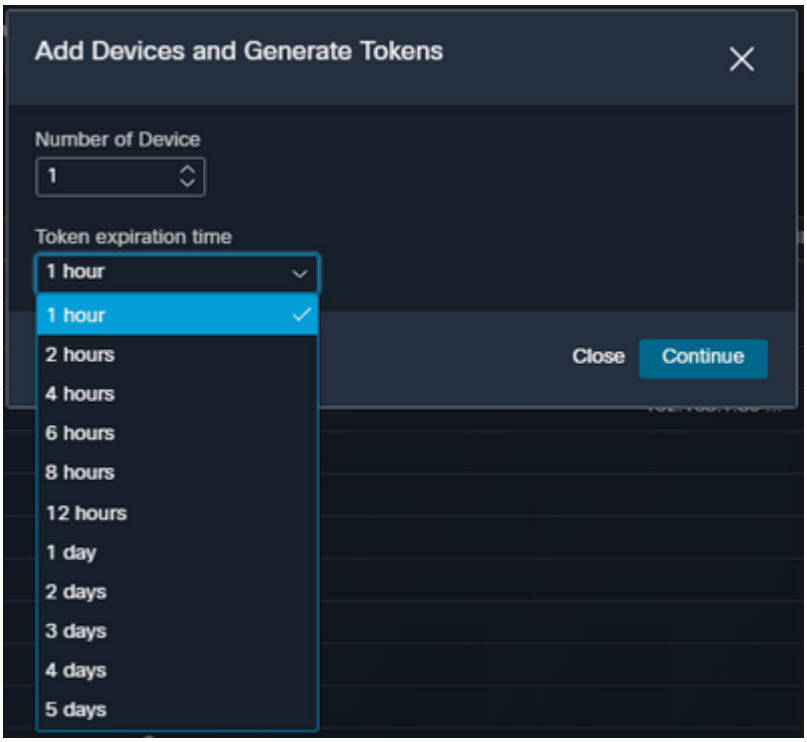
Stellen Sie sicher, dass das Token aus der richtigen Cloud generiert wird:

Wenn Sie für sichere E-Mails eine Cloud in Europa (EU) verwenden, generieren Sie den Token unter https://admin.eu.sse.itd.cisco.com/

Wenn Sie Americas (NAM) Cloud für sichere E-Mail verwenden, generieren Sie das Token unter https://admin.sse.itd.cisco.com/

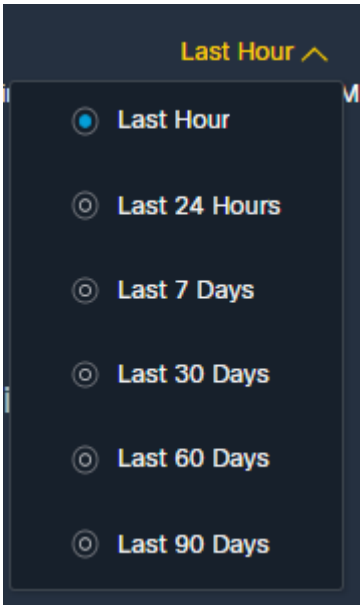
Security Services Exchange (SSE)-Portal:	NAM: https://admin.sse.itd.cisco.com/ EU: https://admin.eu.sse.itd.cisco.com/
Cisco XDR-Portal	NAM: https://XDR.us.security.cisco.com/ EU: https://XDR.eu.security.cisco.com/
Sicherer E-Mail-Schutz Cisco XDR/Threat Response Server:	NAM: api-sse.cisco.com EU: api.eu.sse.itd.cisco.com

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.



Das XDR-Dashboard zeigt keine Informationen zum Secure Email-Modul an.

Sie können eine größere Zeitspanne in den verfügbaren Kacheln auswählen, von **Letzte Stunde** bis **Letzte 90 Tage**, wie im Bild unten.

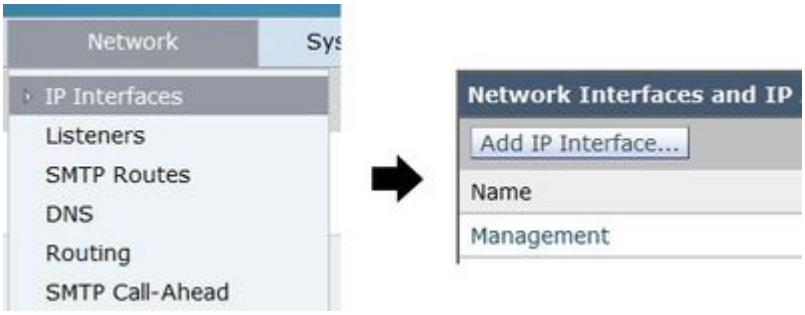


Andere Beispiele könnten sein, dass wir die Nachricht sehen "Es gab ein Problem. Versuchen Sie es später erneut." oder sogar die Fehlermeldung "Es gab einen Client-Fehler im Secure Email-Modul: E4017: Gerät ist offline [409]". Überprüfen Sie, ob das Gerät weiterhin als über das SSE-Portal registriert angezeigt wird. Wahrscheinlich wurde die Registrierung des Geräts aufgehoben, und es ist nicht mehr sichtbar. Versuchen Sie, ein neues Modul zum XDR-Portal hinzuzufügen.

Das XDR-Kachelmodul für sichere E-Mails zeigt den Fehler "Es gab einen unerwarteten Fehler auf dem sicheren E-Mail-Modul" an.

Für sichere E-Mails muss die AsyncOS-API für die HTTP- und HTTPS-Konfiguration über die

Verwaltungsschnittstelle aktiviert sein, damit die Kommunikation mit dem XDR/CTR-Portal möglich ist. Konfigurieren Sie diese Funktion für eine sichere E-Mail vor Ort über die Benutzeroberfläche des sicheren E-Mail-Portals. Navigieren Sie zu **Netzwerk > IP-Schnittstellen > Management-Schnittstelle > AsyncOS API,** und aktivieren Sie HTTP und HTTPS, wie im Bild dargestellt.

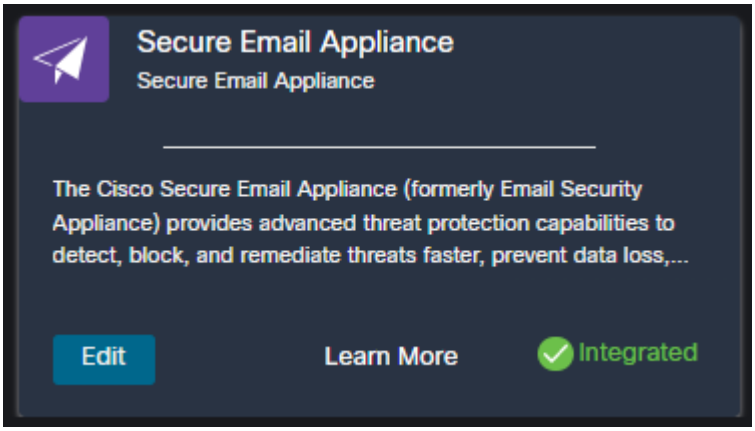


Bei einer CES (Cloud-Based Secure Email) muss diese Konfiguration vom Backend aus durch einen Secure Email TAC-Techniker durchgeführt werden. Sie erfordert Zugriff auf den Support-Tunnel der betroffenen CES.

Überprüfung

Sobald Secure Email als Quelle zu Device Insights hinzugefügt wurde, wird der Verbindungsstatus einer erfolgreichen **REST-API** angezeigt.

- Die **REST-API**-Verbindung wird grün angezeigt.
- Drücken Sie auf **JETZT SYNCHRONISIEREN**, um die erste vollständige Synchronisierung auszulösen, wie im Bild gezeigt.



Sollte das Problem weiterhin mit der XDR- und Secure Email Appliance-Integration 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.

Zugehörige Informationen

- **Die Informationen in diesem Artikel finden Sie in diesem XDR- und Secure Email Integration-Video.**
- **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.