Dépannage de l'intégration XDR et Secure Email Appliance (anciennement ESA)

Table des matières

Introduction

Ce document décrit les étapes pour effectuer une analyse de base et comment dépanner le module d'intégration XDR et Insights and Secure Email Appliance.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- XDR
- échange de services de sécurité
- E-mail sécurisé

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- échange de services de sécurité
- XDR
- E-mail sécurisé C100V sur la version logicielle 13.0.0-392

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco Secure Email Appliance (anciennement Email Security Appliance) offre des fonctionnalités

avancées de protection contre les menaces pour détecter, bloquer et éliminer les menaces plus rapidement, empêcher la perte de données et sécuriser les informations importantes en transit grâce au cryptage de bout en bout. Une fois configuré, le module Secure Email Appliance fournit des détails associés aux éléments observables. Vous pouvez :

- Afficher les rapports d'e-mails et les données de suivi des messages de plusieurs appliances de votre organisation
- Identifier, analyser et éliminer les menaces observées dans les rapports d'e-mail et les suivis des messages
- Résoudre rapidement les menaces identifiées et recommander des mesures à prendre contre les menaces identifiées
- Documentez les menaces pour enregistrer l'investigation et permettre la collaboration des informations entre les autres périphériques

L'intégration d'un module Secure Email Appliance nécessite l'utilisation de Security Services Exchange (SSE). SSE permet à un appareil de messagerie électronique sécurisé de s'enregistrer auprès d'Exchange et vous fournissez une autorisation explicite d'accès aux périphériques enregistrés.

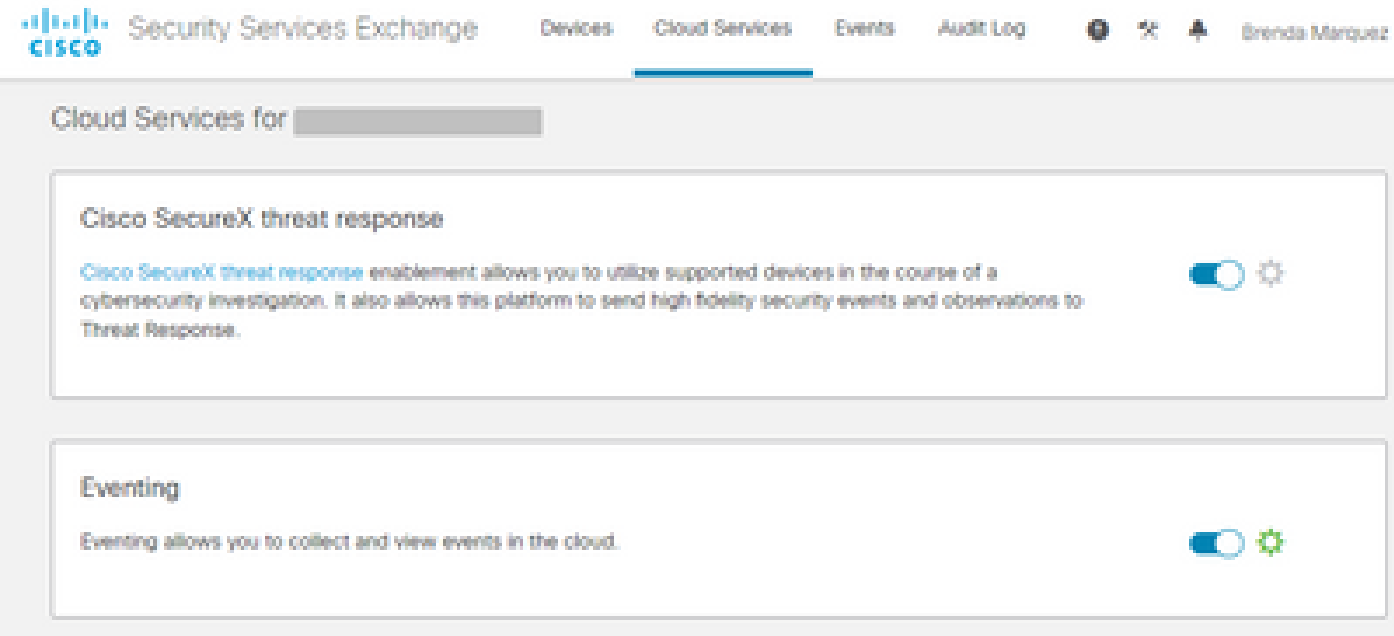
Si vous voulez en savoir plus sur la configuration, veuillez lire cet article ici pour plus de détails sur le module d'intégration.

Dépannage

Afin de dépanner les problèmes courants avec l'intégration de XDR et Secure Email Appliance, vous pouvez vérifier ces étapes.

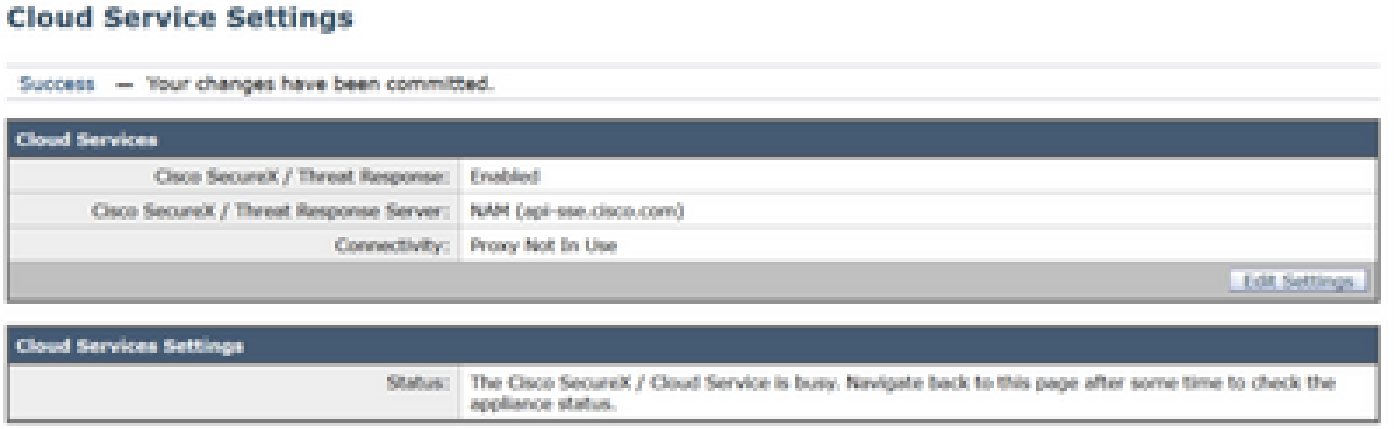
Le périphérique de messagerie sécurisée n'est pas affiché dans le portail XDR ou Security Services Exchange

Si votre périphérique n'est pas affiché dans le portail SSE, assurez-vous d'avoir activé les services XDR Threat Response et Event Services dans le portail SSE, accédez à Cloud Services, et activez les services, comme l'image ci-dessous :



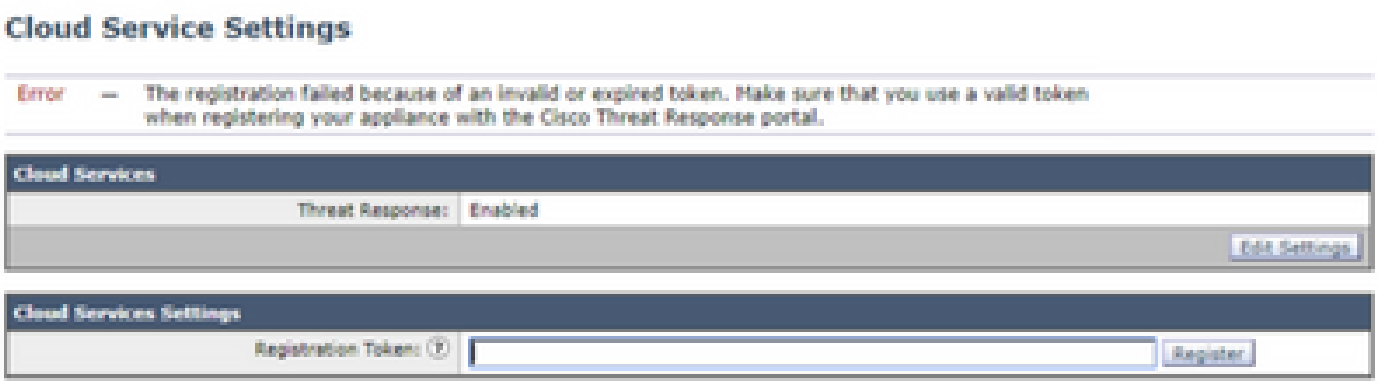
La messagerie sécurisée ne demande pas le jeton d'enregistrement

Assurez-vous de valider les modifications, une fois que le service Cisco XDR / Threat Response a été activé. Sinon, les modifications ne seront pas appliquées à la section Cloud Service de l'e-mail sécurisé, voir l'image ci-dessous.



Échec de l'enregistrement en raison d'un jeton non valide ou expiré

Si le message d'erreur suivant s'affiche : "L'enregistrement a échoué en raison d'un jeton non valide ou expiré. Assurez-vous d'utiliser un jeton valide pour votre appliance avec le « portail de réponse aux menaces Cisco XDR » dans l'interface utilisateur graphique de la messagerie sécurisée, comme dans l'image ci-dessous :



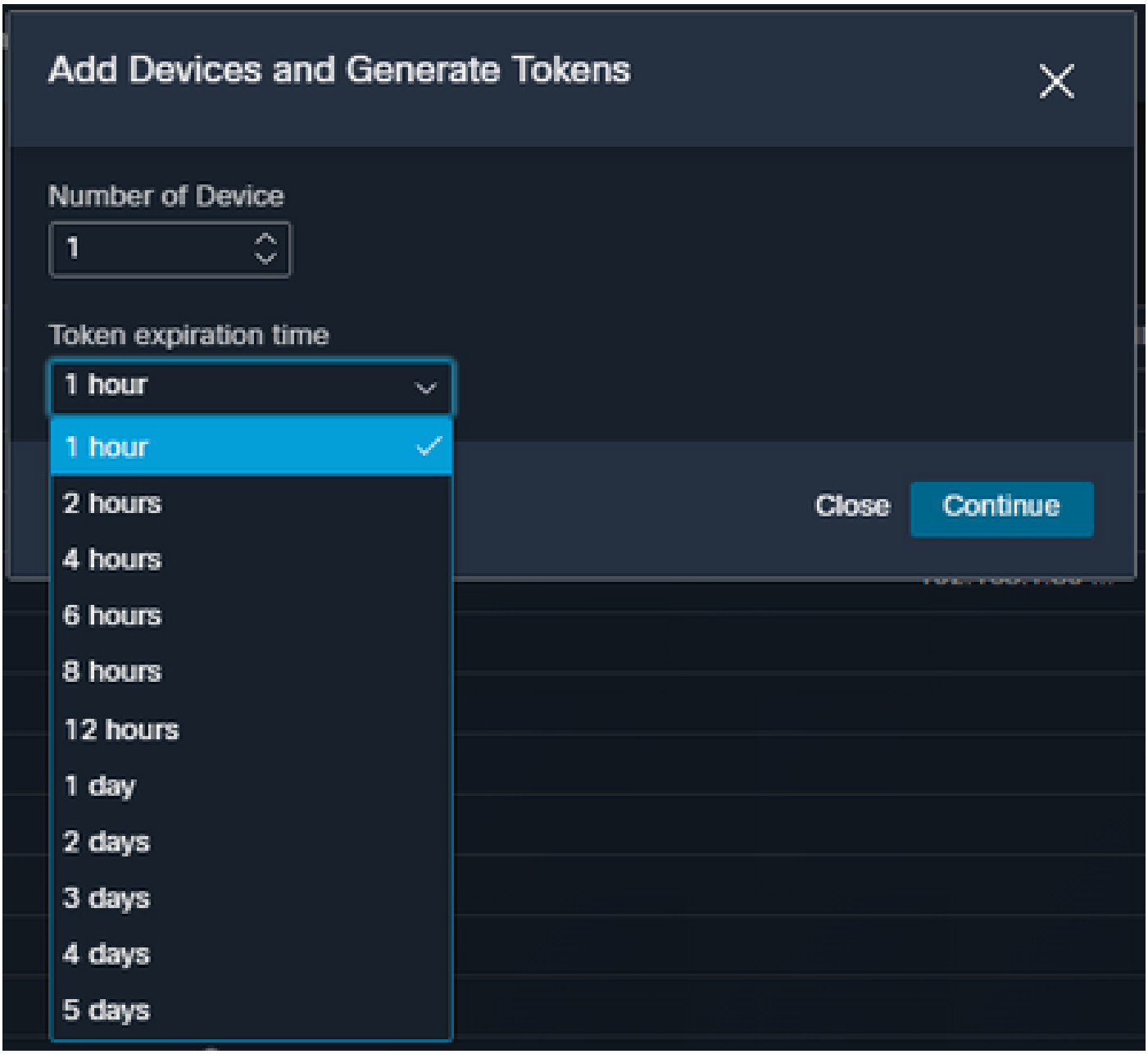
Assurez-vous que le jeton est généré à partir du cloud approprié :

Si vous utilisez le cloud Europe (EU) pour la sécurisation de la messagerie électronique, générez le jeton à partir de https://admin.eu.sse.itd.cisco.com/

Si vous utilisez le cloud Amériques (NAM) pour sécuriser la messagerie électronique, générez le jeton à partir de https://admin.sse.itd.cisco.com/

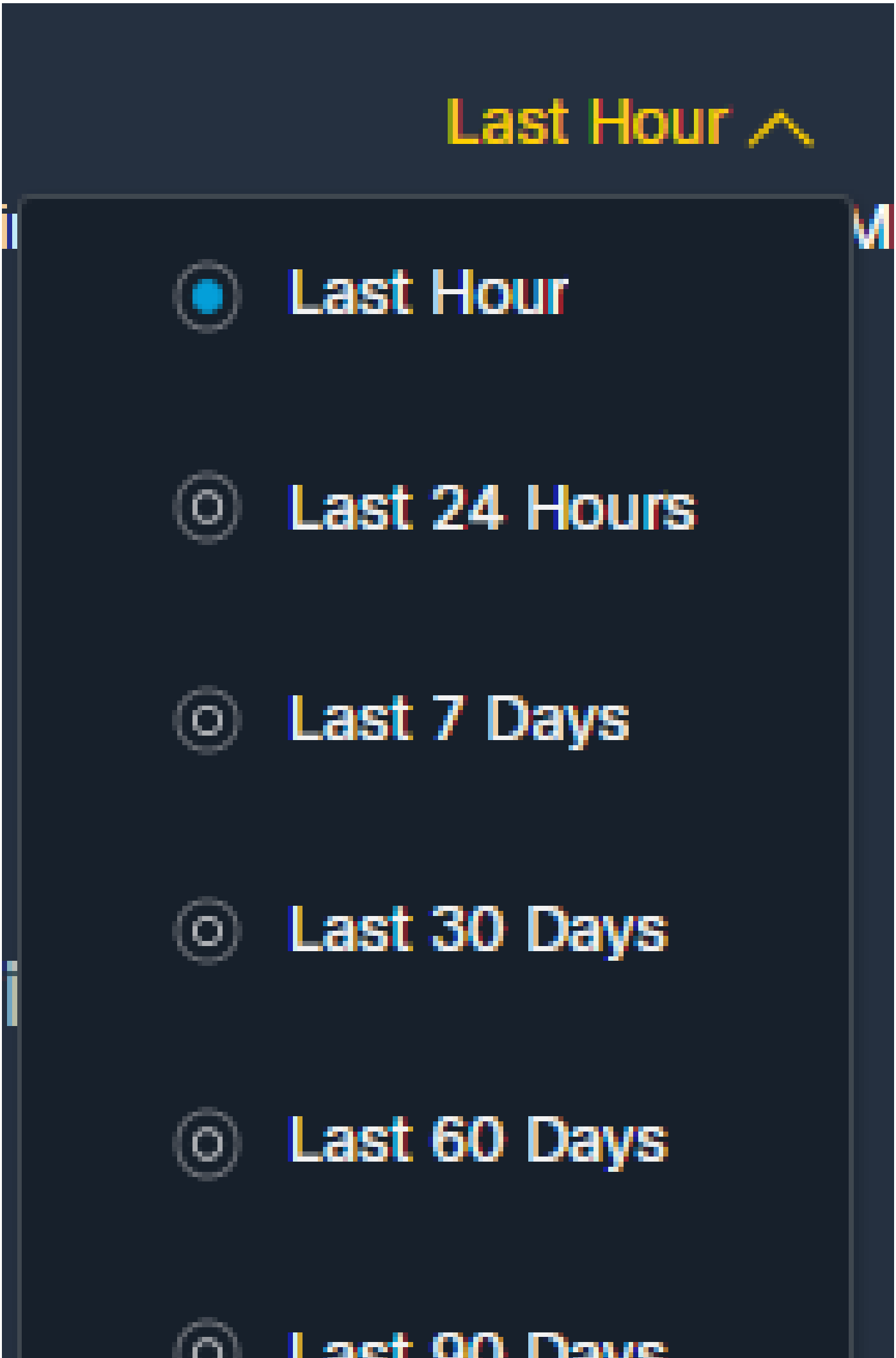
Portail Security Services Exchange (SSE) :	NAM : https://admin.sse.itd.cisco.com/ UE : https://admin.eu.sse.itd.cisco.com/
Portail Cisco XDR	NAM : https://XDR.us.security.cisco.com/ UE : https://XDR.eu.security.cisco.com/
E-mail sécurisé Cisco XDR / Threat Response Server :	NAM : api-sse.cisco.com UE : api.eu.sse.itd.cisco.com

N'oubliez pas non plus que le jeton d'enregistrement a un délai d'expiration (sélectionnez le délai le plus approprié pour terminer l'intégration dans le temps), comme indiqué dans l'image.



Le tableau de bord XDR n'affiche pas d'informations sur le module Secure Email

Vous pouvez sélectionner une plage de temps plus large dans les vignettes disponibles, de la Dernière Heure aux 90 derniers Jours, comme dans l'image ci-dessous.


Last Hour
Last Hour
Last 24 Hours
Last 7 Days
Last 30 Days
Last 60 Days

pour collecter les journaux HAR à partir du navigateur et contactez le support TAC afin d'effectuer une analyse plus approfondie.

Informations connexes

- Vous trouverez les informations de cet article dans cette vidéo XDR et Secure Email Integration.
- Vous pouvez trouver des vidéos sur la façon de configurer vos intégrations de produits ici
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.