# Risoluzione dei problemi di integrazione di XDR e Secure Email Appliance (in precedenza ESA)

## Sommario



## Introduzione

In questo documento viene descritto come eseguire un'analisi di base e come risolvere i problemi relativi al modulo di integrazione di XDR, Insights e Secure Email Appliance.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- XDR
- Security Services Exchange
- Posta elettronica protetta

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Security Services Exchange
- XDR
- Secure Email C100V sul software versione 13.0.0-392

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Cisco Secure Email Appliance (in precedenza Email Security Appliance) fornisce funzionalità avanzate di protezione dalle minacce per rilevare, bloccare e correggere più rapidamente le minacce, prevenire la perdita di dati e proteggere le informazioni importanti in transito con la crittografia end-to-end. Una volta configurato, il modulo Secure Email Appliance fornisce i dettagli associati agli osservatori. È possibile:

- Visualizzare i report e-mail e tenere traccia dei messaggi provenienti da più appliance dell'organizzazione
- Identificazione, analisi e risoluzione delle minacce osservate nei report e-mail e nelle tracce dei messaggi
- Risolvere rapidamente le minacce identificate e fornire le azioni consigliate per contrastare le minacce identificate
- Documentare le minacce per salvare l'indagine e consentire la collaborazione di informazioni tra altri dispositivi

L'integrazione di un modulo Secure Email Appliance richiede l'utilizzo di Security Services Exchange (SSE). SSE consente a un dispositivo Secure Email Appliance di registrarsi con Exchange e fornisce l'autorizzazione esplicita per accedere ai dispositivi registrati.

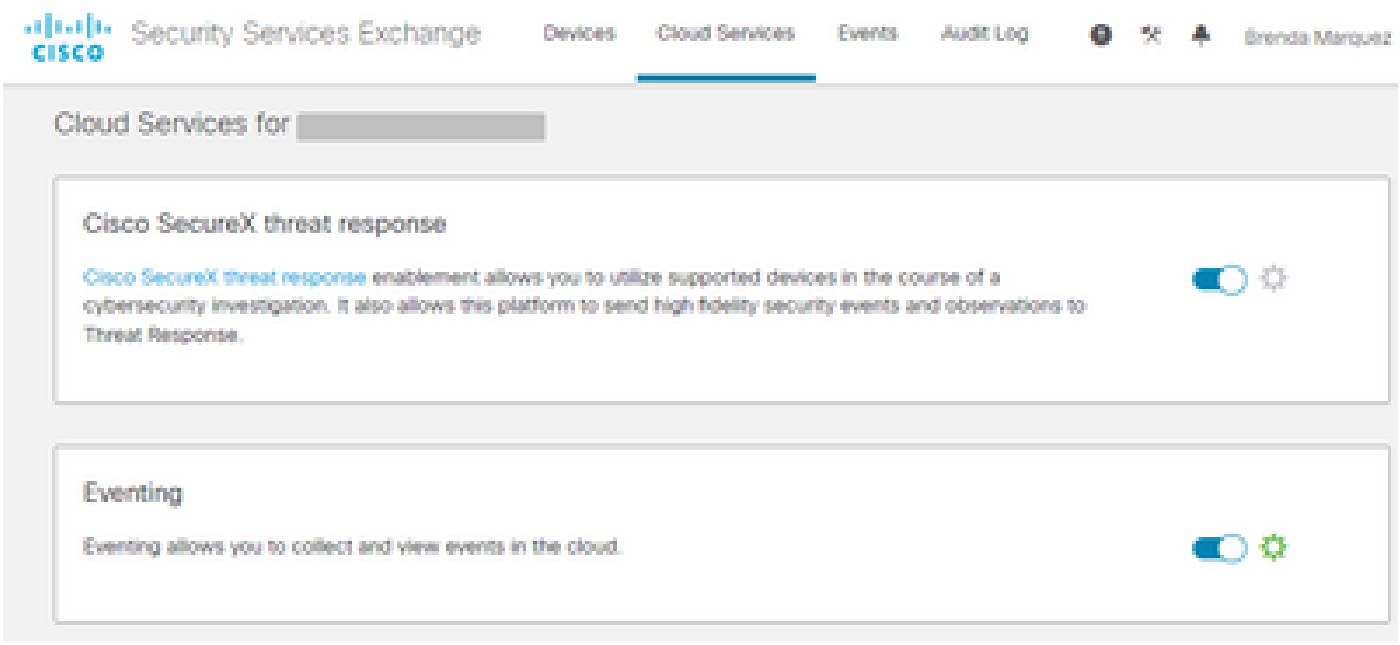
Per ulteriori informazioni sulla configurazione, fare riferimento a questo articolo contenente i dettagli del modulo di integrazione.

# Risoluzione dei problemi

Per la risoluzione dei problemi più comuni relativi all'integrazione di XDR e Secure Email Appliance, è possibile verificare i passaggi descritti di seguito.

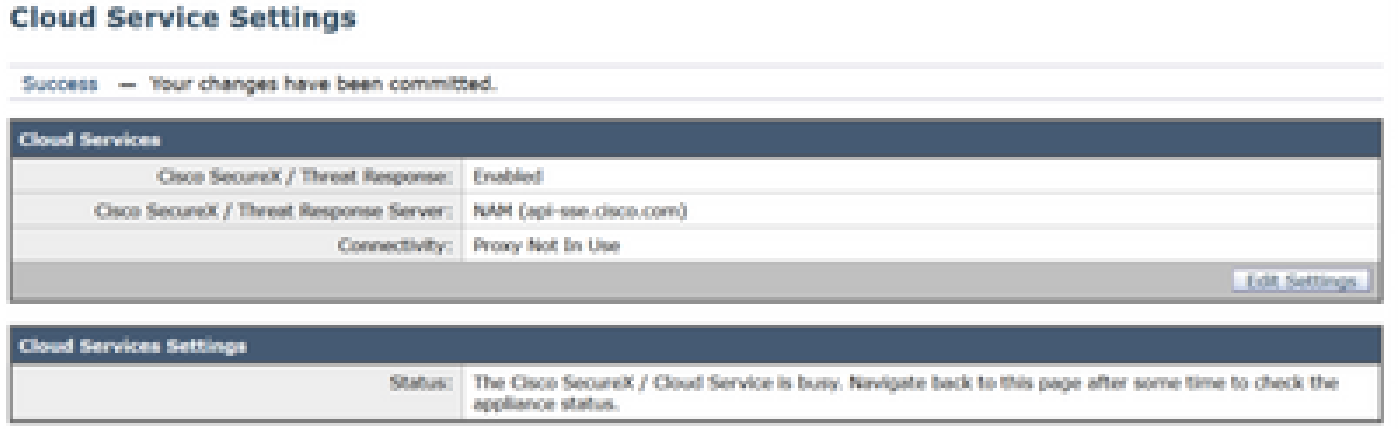
## Il dispositivo di posta elettronica sicura non è visualizzato nel portale XDR né nel portale Exchange dei servizi di sicurezza

Se il dispositivo non è visualizzato nel portale SSE, assicurarsi di aver abilitato XDR Threat Response and Event Services nel portale SSE, passare a Cloud Services e abilitare i servizi, come illustrato nell'immagine seguente:



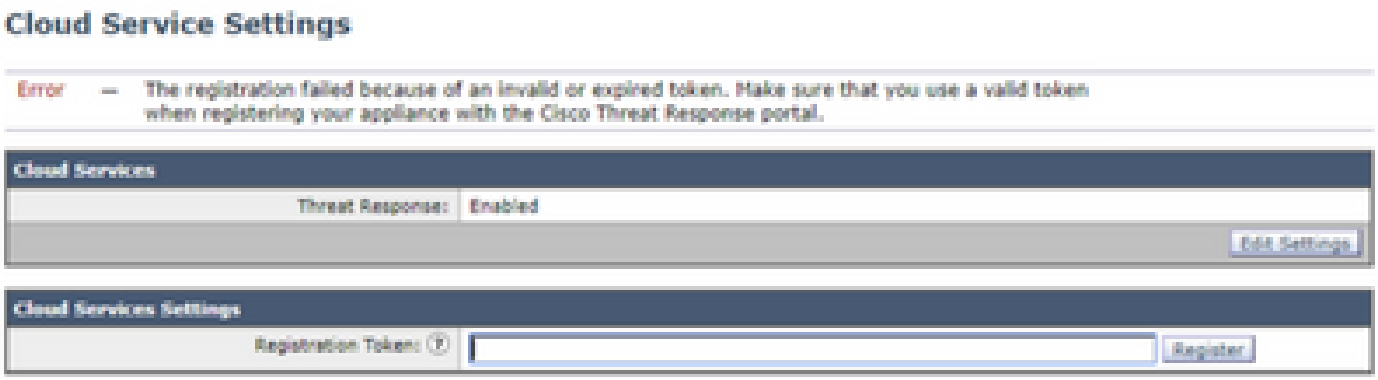

## Secure Email non richiede il token di registrazione

Assicurarsi di eseguire il commit delle modifiche, una volta abilitato il servizio Cisco XDR / Threat Response, altrimenti le modifiche non verranno applicate alla sezione Cloud Service (Servizio cloud) dell'e-mail sicura. Vedere l'immagine seguente.




## Registrazione non riuscita a causa di un token non valido o scaduto

Se viene visualizzato il messaggio di errore: "Registrazione non riuscita a causa di un token non valido o scaduto. Verificare di utilizzare un token valido per l'appliance con il portale Cisco XDR Threat Response nell'interfaccia utente di Secure Email, come nell'immagine seguente:



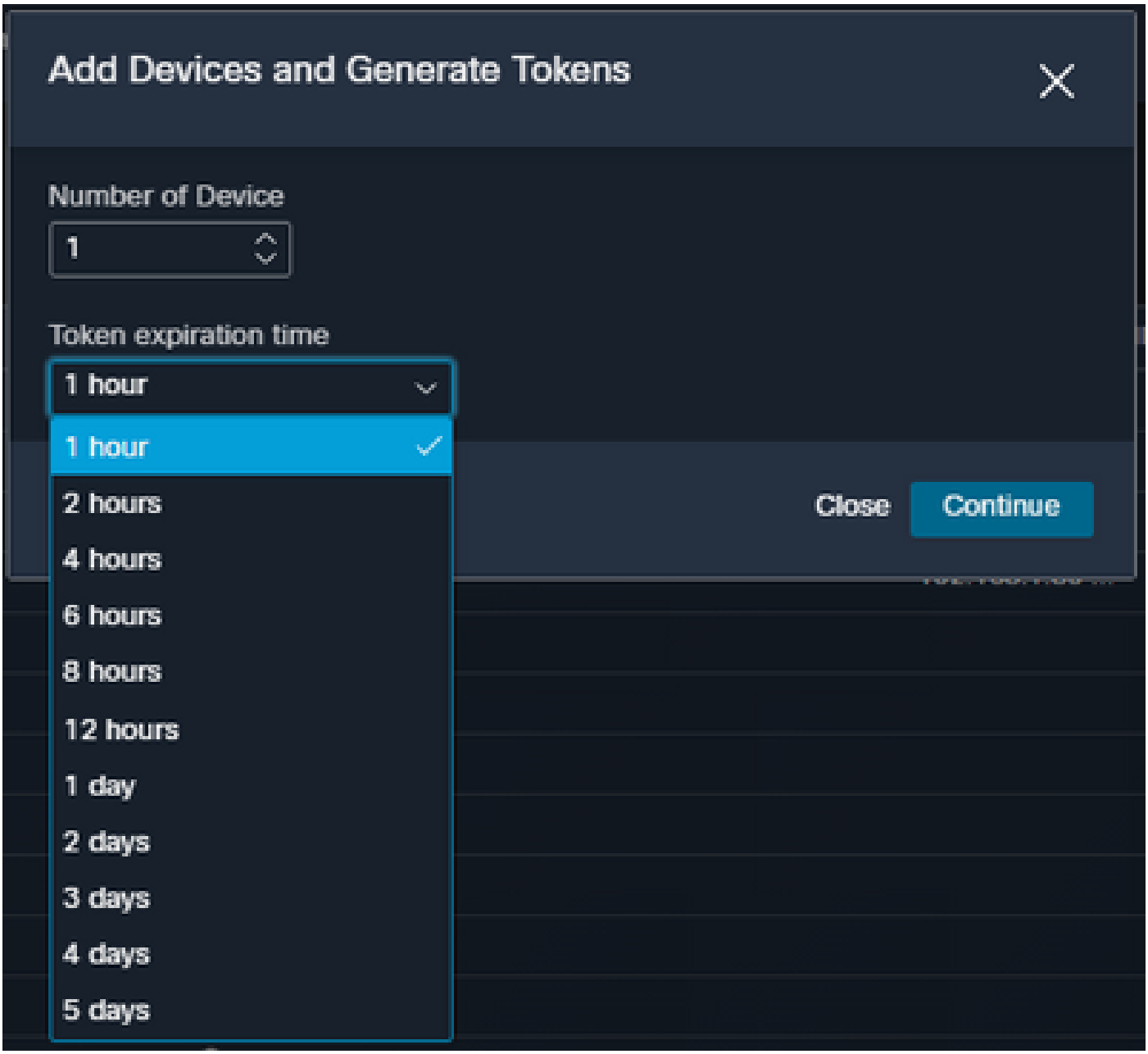

Verificare che il token sia generato dal cloud corretto:

Se utilizzi Europe (EU) Cloud per Secure Email, genera il token da https://admin.eu.sse.itd.cisco.com/

Se usi Americas (NAM) Cloud per Secure Email, genera il token da https://admin.sse.itd.cisco.com/

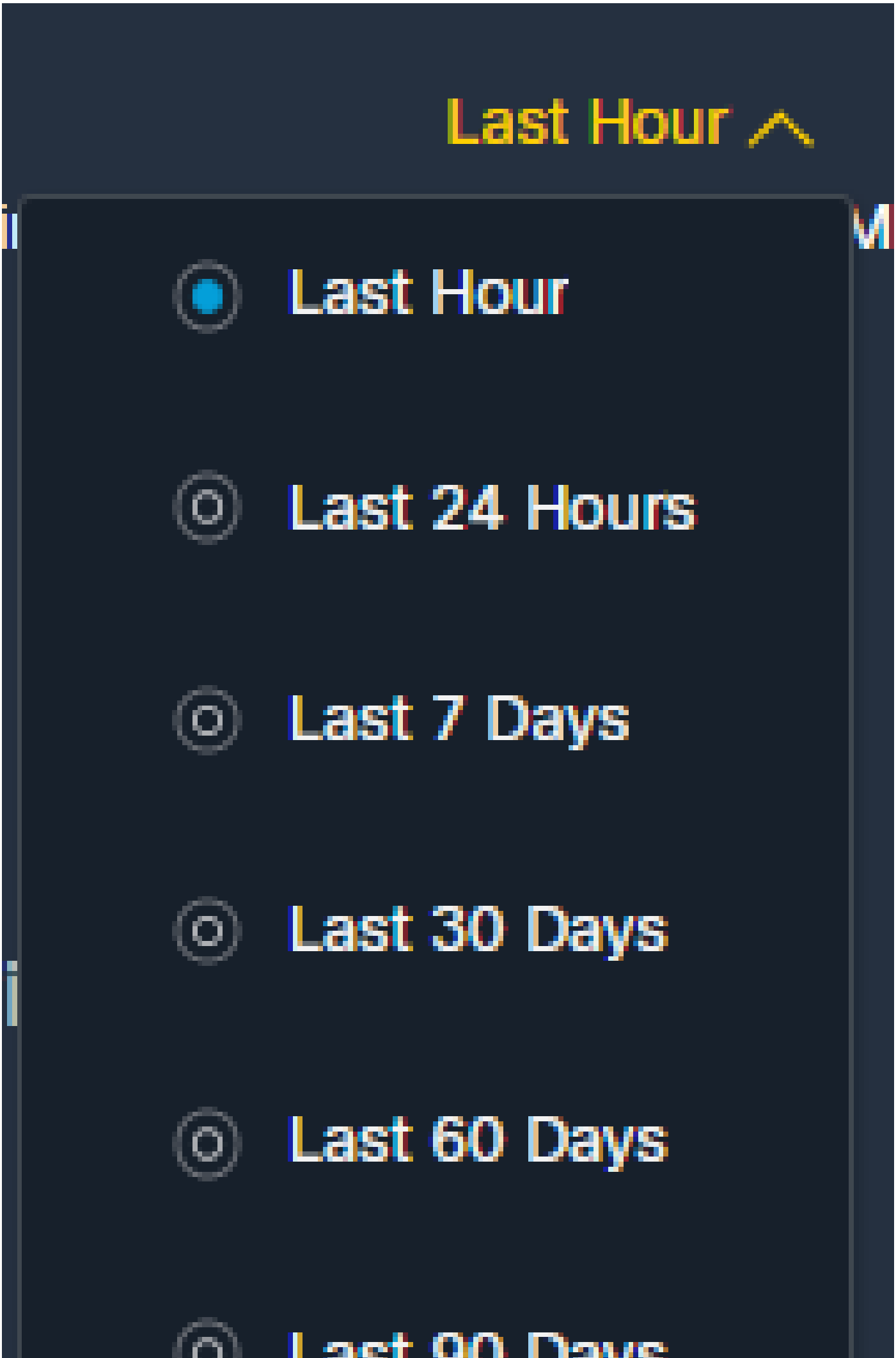
| | |
|---|---|
| Portale SSE (Security Services Exchange): | NOME: https://admin.sse.itd.cisco.com/<br>UE: https://admin.eu.sse.itd.cisco.com/ |
| Portale Cisco XDR | NOME: https://XDR.us.security.cisco.com/<br>UE: https://XDR.eu.security.cisco.com/ |
| Secure Email Cisco XDR / Server di risposta alle minacce: | NOME: api-sse.cisco.com<br>UE: api.eu.sse.itd.cisco.com |

Tenere inoltre presente che il token di registrazione ha una scadenza (selezionare l'ora più conveniente per completare l'integrazione in tempo), come mostrato nell'immagine.




XDR Dashboard non visualizza informazioni sul modulo Secure Email

È possibile selezionare un intervallo di tempo più ampio nelle tessere disponibili, da Ultima ora a Ultimi 90 giorni, come nell'immagine seguente.


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

per raccogliere i log HAR dal browser e contattare il supporto TAC per eseguire un'analisi più approfondita.

## Informazioni correlate

- Le informazioni di questo articolo sono disponibili in questo video su XDR e Secure Email Integration.
- Qui sono disponibili video su come configurare le integrazioni dei prodotti
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).