Integrazione Cisco Threat Response (CTR) ed ESA

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Configurazione
Passaggio 1. Selezionare Rete > Impostazioni servizio cloud
Passaggio 2. Fare clic su Modifica impostazioni
Passaggio 3. Selezionare la casella di controllo Abilita e il server di risposta alla minaccia
Passaggio 4. Sottomettere e confermare le modifiche
Passaggio 5. Accedere al portale del CTR e generare il token di registrazione richiesto nell'ESA
Passaggio 6. Incollare il token di registrazione (generato dal portale del CTR) nell'ESA
Passaggio 7. Verificare che il dispositivo ESA si trovi nel portale SSE
Passaggio 8. Passare al portale CTR e aggiungere un nuovo modulo ESA
Verifica
Risoluzione dei problemi
Il dispositivo ESA non è visualizzato nel portale CTR
L'inchiesta sul CTR non mostra dati forniti dall'ESA
L'ESA non richiede il token di registrazione
Registrazione non riuscita a causa di un token non valido o scaduto
Informazioni correlate

Introduzione

Questo documento descrive il processo per integrare Cisco Threat Response (CTR) con Email Security Appliance (ESA) e come verificarlo per eseguire alcune indagini CTR.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Threat Response
- Email Security Appliance

Componenti usati

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

- Account CTR
- Cisco Security Services Exchange
- ESA C100V sul software versione 13.0.0-392

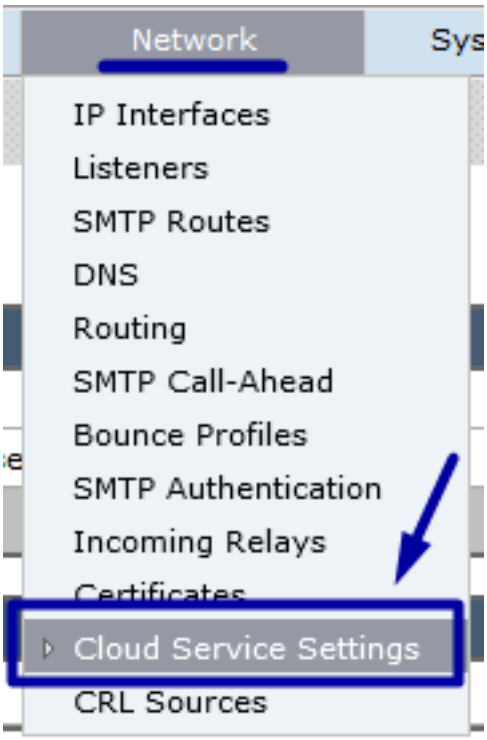
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

Per configurare Integration CTR ed ESA, accedere a Email Security Virtual Appliance e attenersi alla seguente procedura rapida:

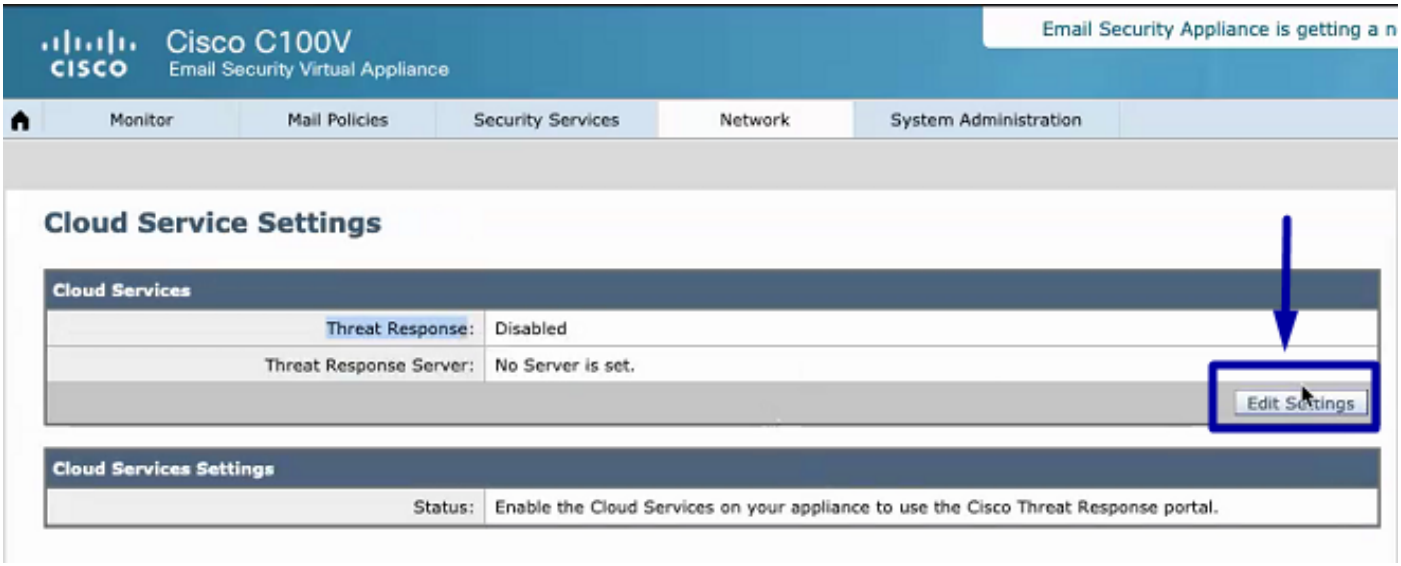
Passaggio 1. Selezionare Rete > Impostazioni servizio cloud

Nell'ESA, passare al menu di scelta rapida Network > Cloud Service Settings (Rete > Impostazioni servizio cloud) per visualizzare lo stato attuale della risposta alla minaccia (Disabilitato/Abilitato), come mostrato nell'immagine.



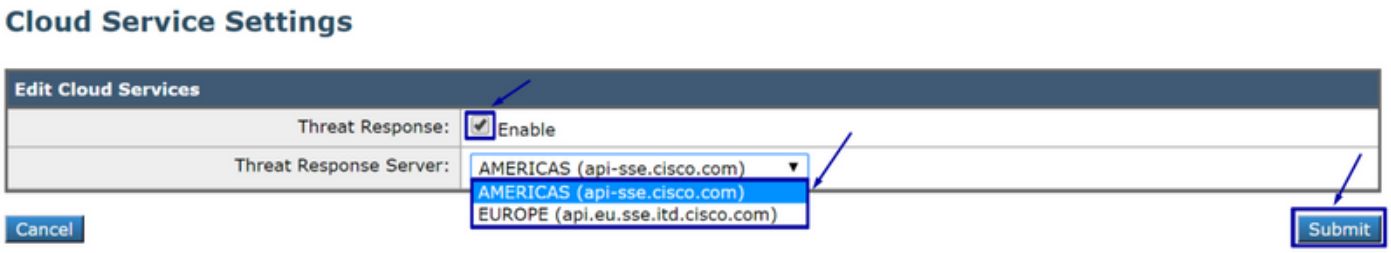
Passaggio 2. Fare clic su Modifica impostazioni

Finora la funzione Threat Response dell'ESA è disabilitata, per abilitarla, fare clic su Edit Settings (Modifica impostazioni) come mostrato nell'immagine:



Passaggio 3. Selezionare la casella di controllo Abilita e il server di risposta alla minaccia

Selezionare la casella di controllo Abilita, quindi scegliere il server di risposta alla minaccia. Vedere l'immagine seguente:

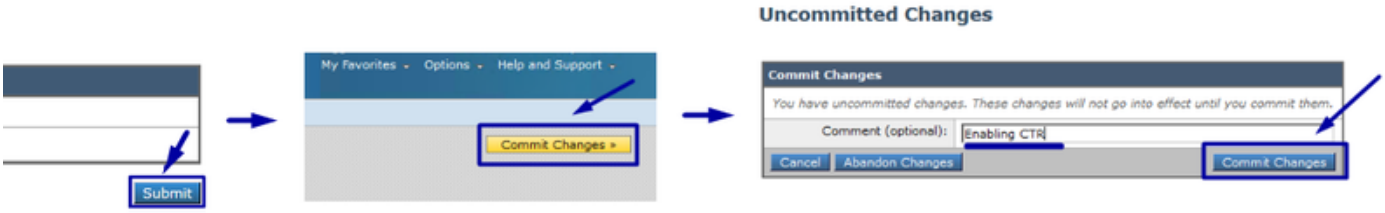


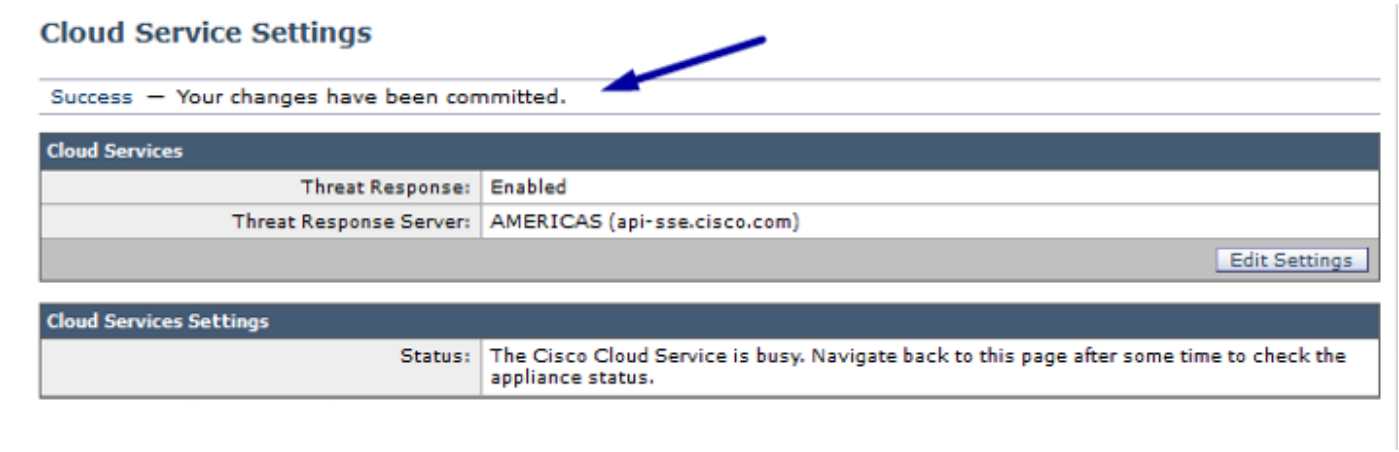
Nota: La selezione predefinita per l'URL del server di risposta alle minacce è AMERICAS (api-sse.cisco.com). Per le aziende europee, fare clic sul menu a discesa e scegliere EUROPA (api.eu.sse.itd.cisco.com)

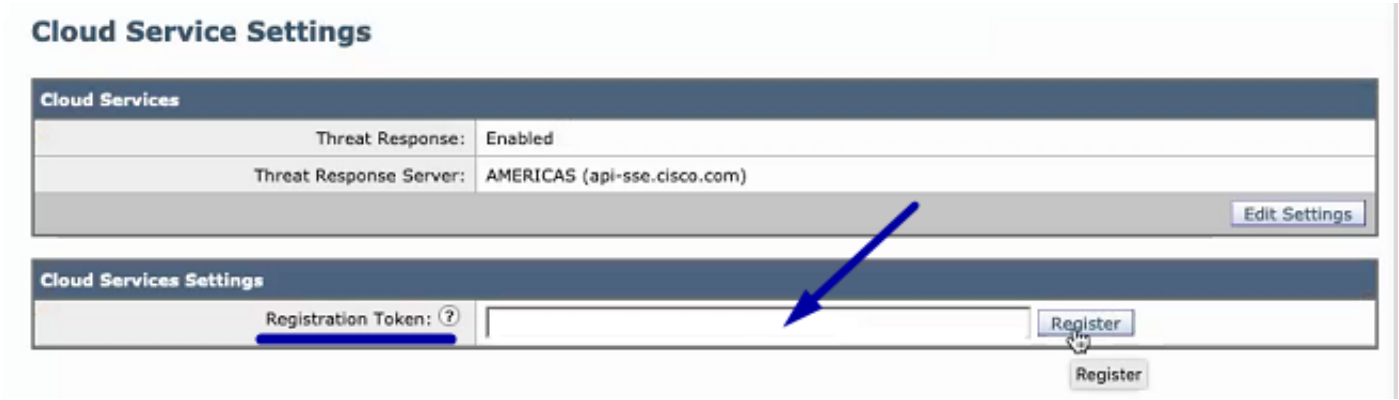
Passaggio 4. Sottomettere e confermare le modifiche

Ènecessario inviare ed eseguire il commit delle modifiche per salvare e applicare le modifiche. Ora, se l'interfaccia ESA viene aggiornata, è necessario un token di registrazione per registrare l'integrazione, come mostrato nell'immagine qui sotto.

Nota: Viene visualizzato il messaggio Operazioni riuscite: Commit delle modifiche eseguito.

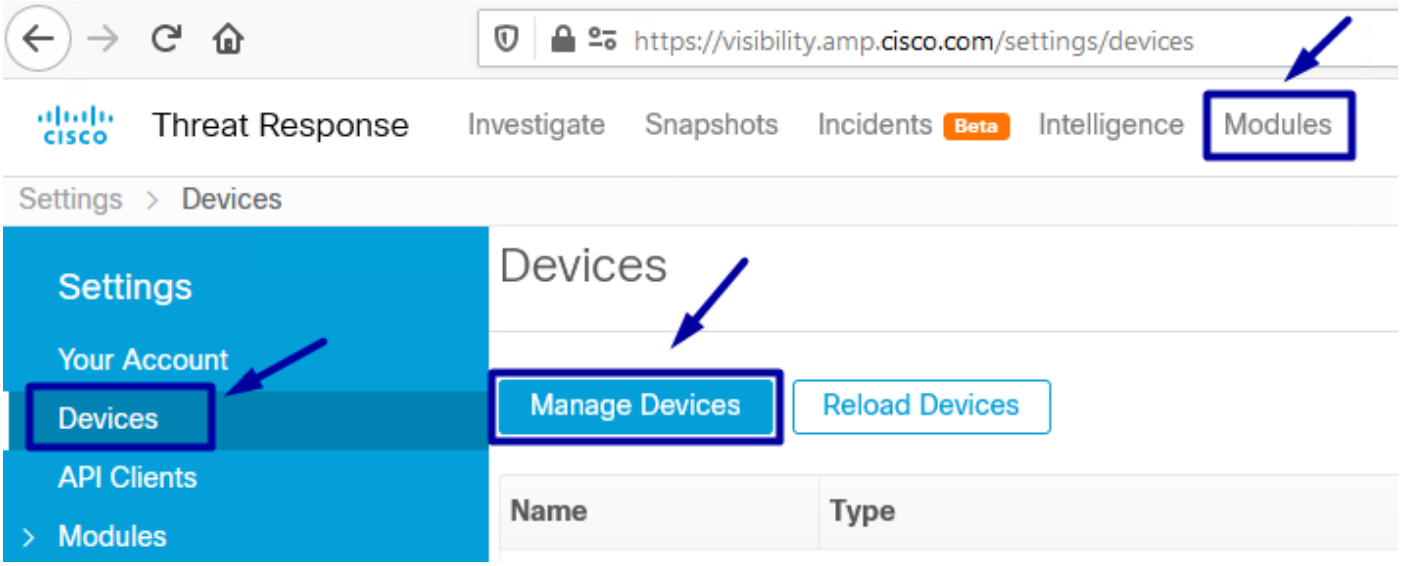




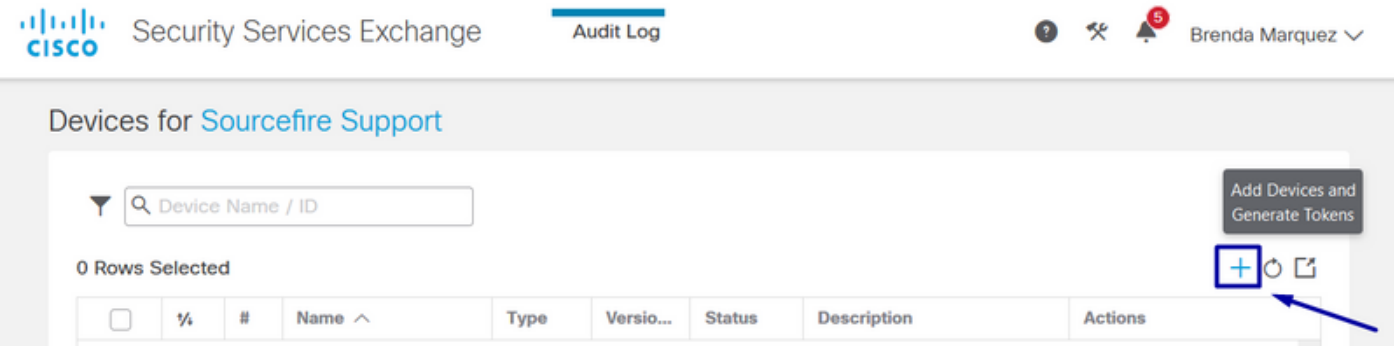


Passaggio 5. Accedere al portale del CTR e generare il token di registrazione richiesto nell'ESA

1.- Una volta nel portale CTR, passare a Moduli > Dispositivi > Gestisci dispositivi, vedere l'immagine successiva.

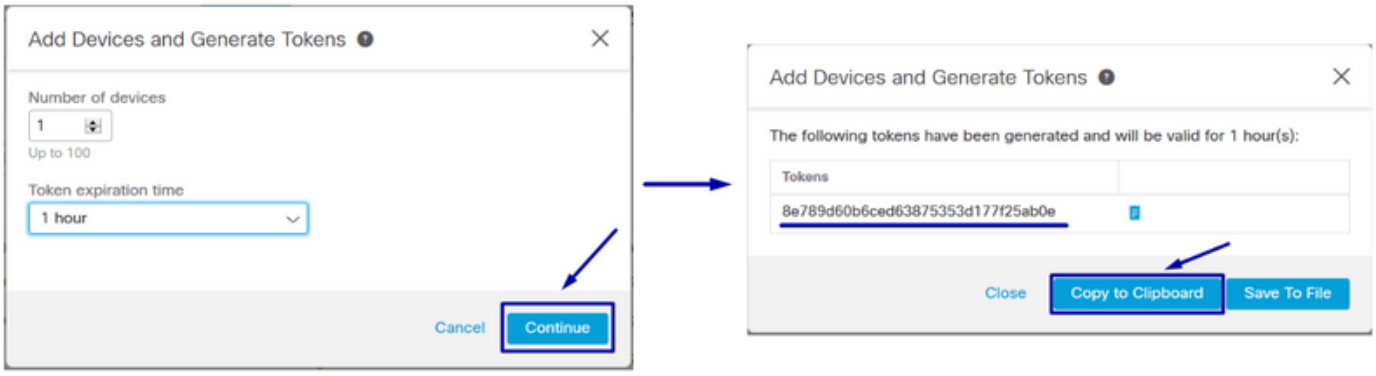


2.- Il collegamento Gestisci dispositivi reindirizza l'utente a Security Services Exchange (SSE), una volta lì, fare clic sull'icona Add Devices and Generate Tokens (Aggiungi dispositivi e genera token) come mostrato nell'immagine.



3.- Per generare il Token, fare clic su Continue (Continua). Una volta generato il Token, fare clic su Copy to Clipboard (Copia negli Appunti), come mostrato nell'immagine.

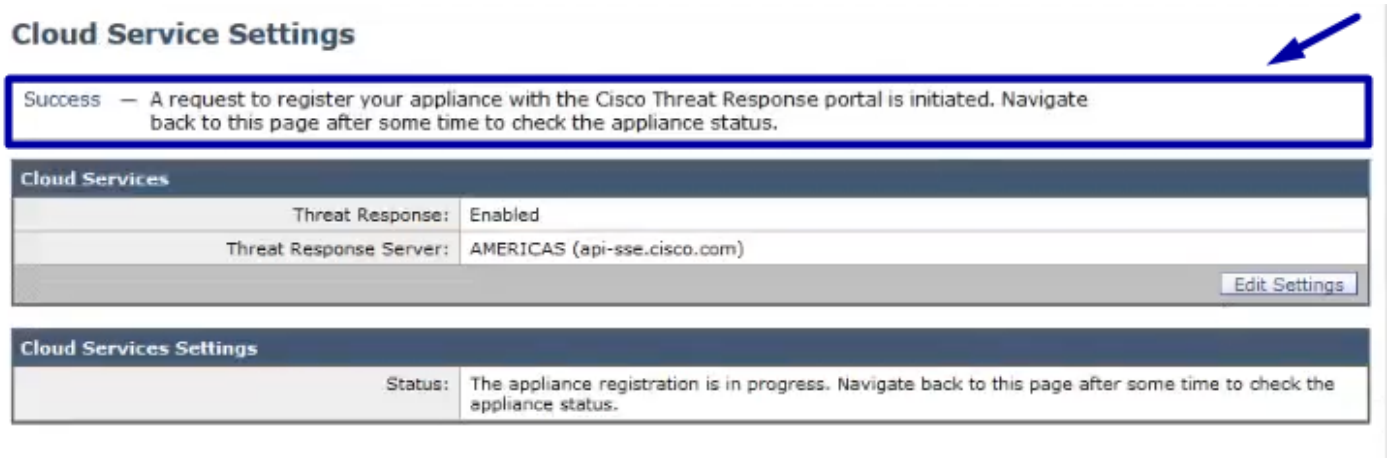
> **Suggerimento**: È possibile selezionare il numero di dispositivi da aggiungere (da 1 e fino a 100) e anche l'ora di scadenza del token (1h, 2h, 4h, 6h, 8h, 12h, 01 giorni, 02 giorni, 03 giorni, 04 giorni e 05 giorni).



Passaggio 6. Incollare il token di registrazione (generato dal portale del CTR) nell'ESA

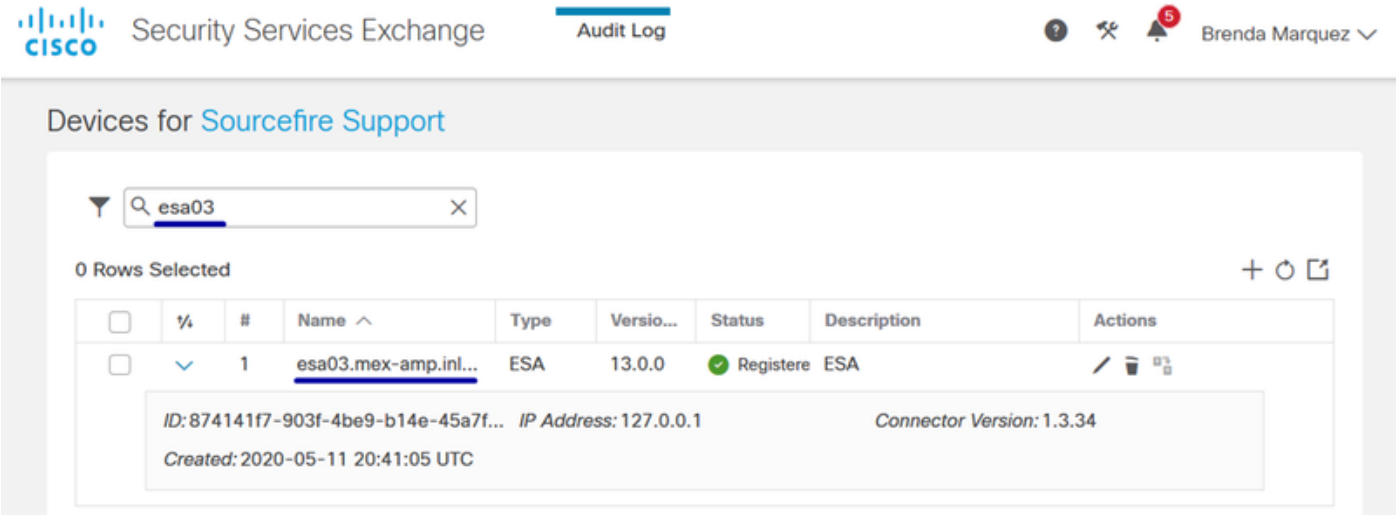
Una volta generato il token di registrazione, incollarlo nella sezione Cloud Services Settings dell'ESA, come nell'immagine seguente.

> **Nota:** Viene visualizzato il messaggio Operazioni riuscite: Verrà inviata una richiesta di registrazione dell'appliance sul portale Cisco Threat Response. Tornare a questa pagina in seguito per verificare lo stato dell'accessorio.



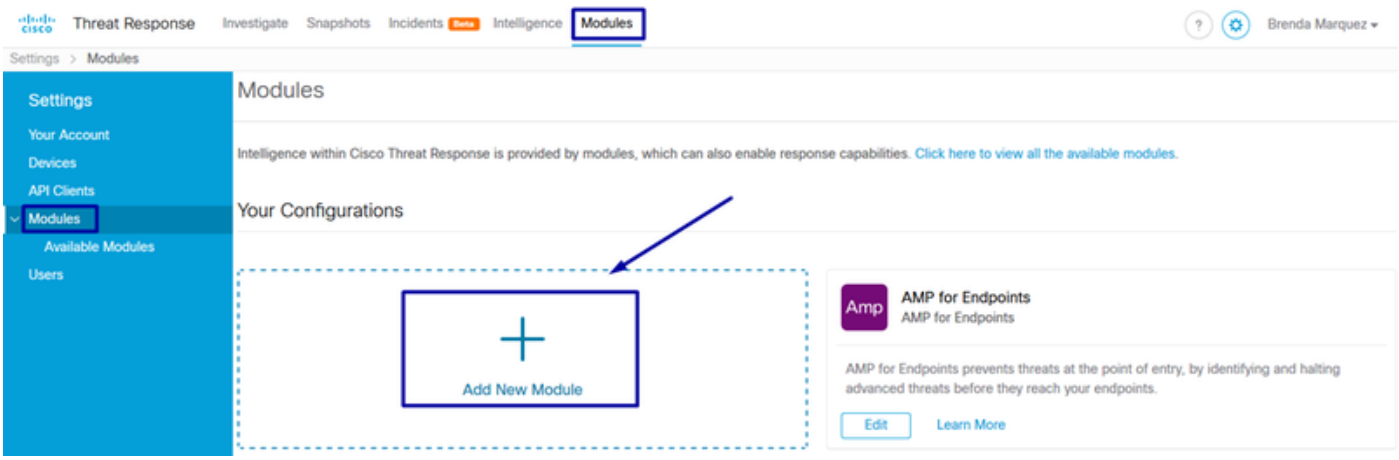
Passaggio 7. Verificare che il dispositivo ESA si trovi nel portale SSE

Èpossibile passare al portale SSE (CTR > Moduli > Dispositivi > Gestisci dispositivi) e nella scheda Ricerca osservare il dispositivo ESA, come mostrato nell'immagine.

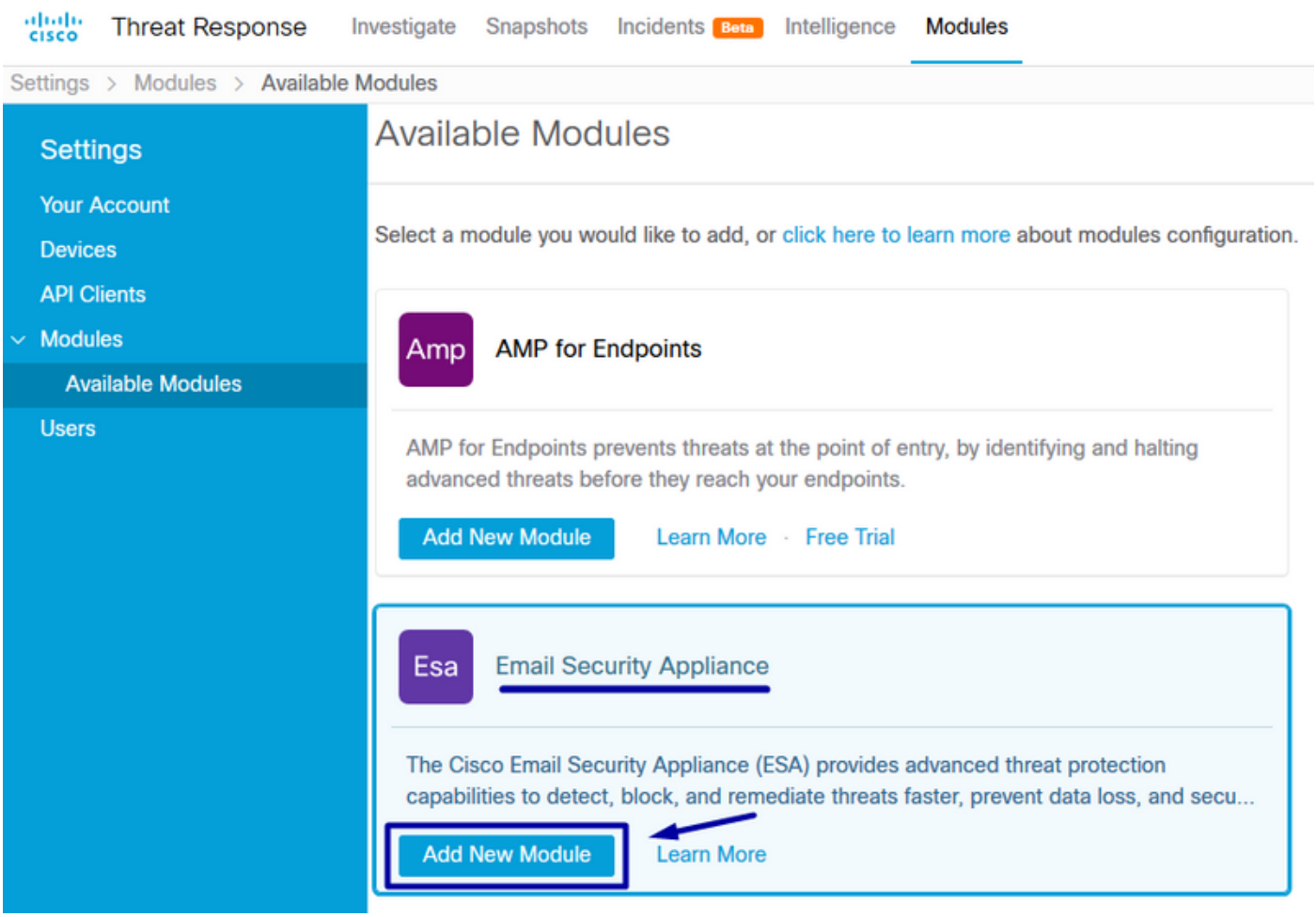


Passaggio 8. Passare al portale CTR e aggiungere un nuovo modulo ESA

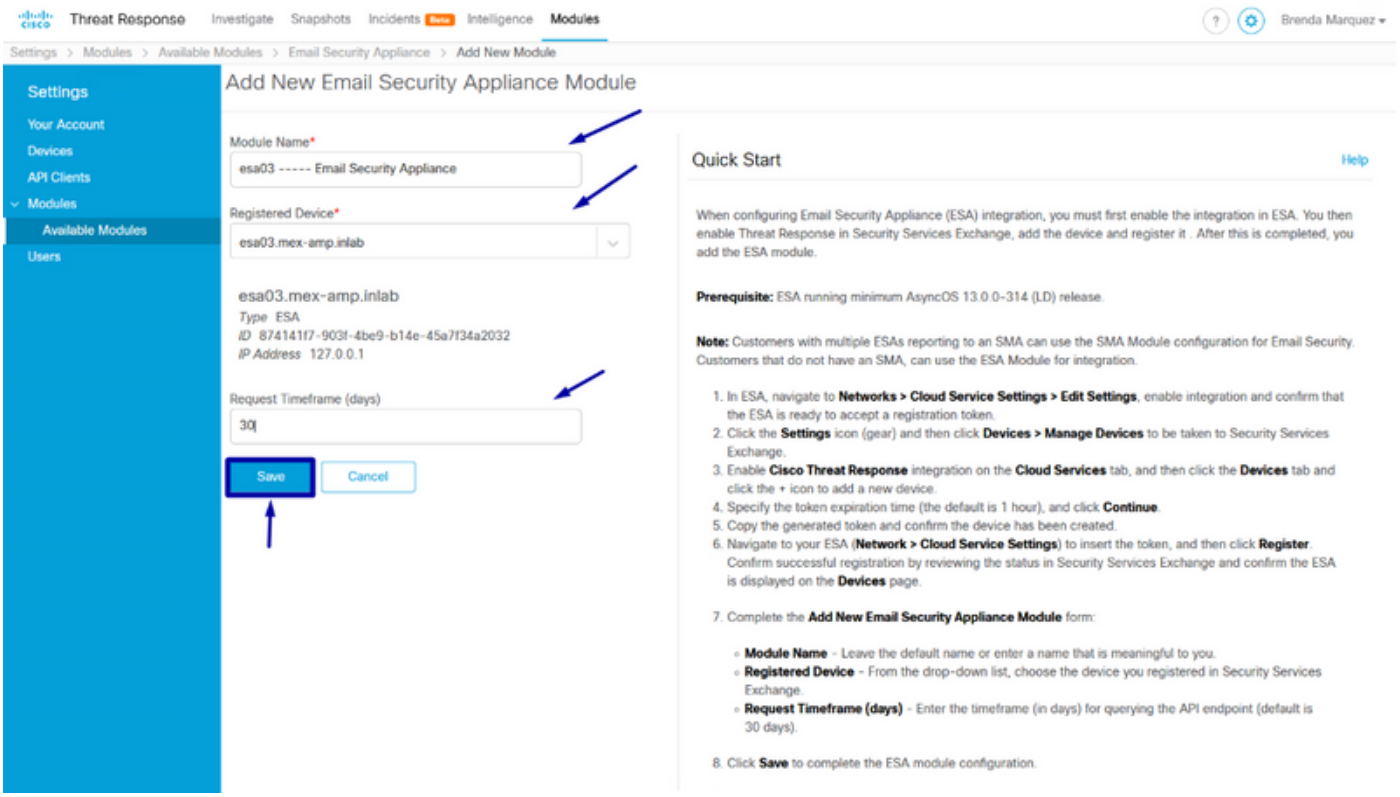
1.- Una volta entrati nel portale CTR, passare a Moduli > Aggiungi nuovo modulo, come mostrato nell'immagine.



2.- Scegliere il tipo di modulo, in questo caso il modulo è un modulo di Email Security Appliance come immagine di seguito.

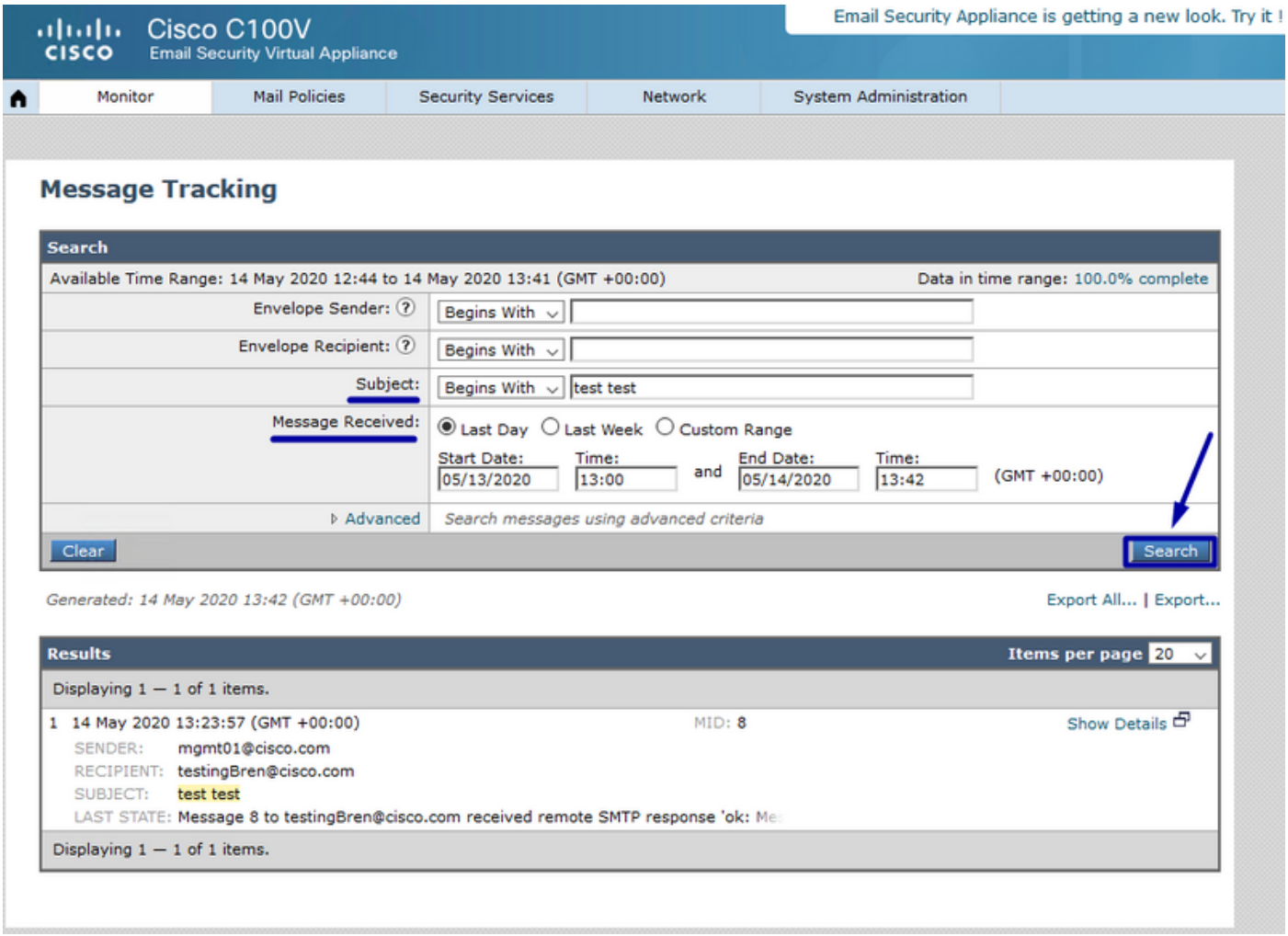


3.- Inserire i campi: Nome modulo, Periferica registrata (selezionare quella registrata in precedenza), Tempo richiesta (giorni) e Salva, come mostrato nell'immagine.

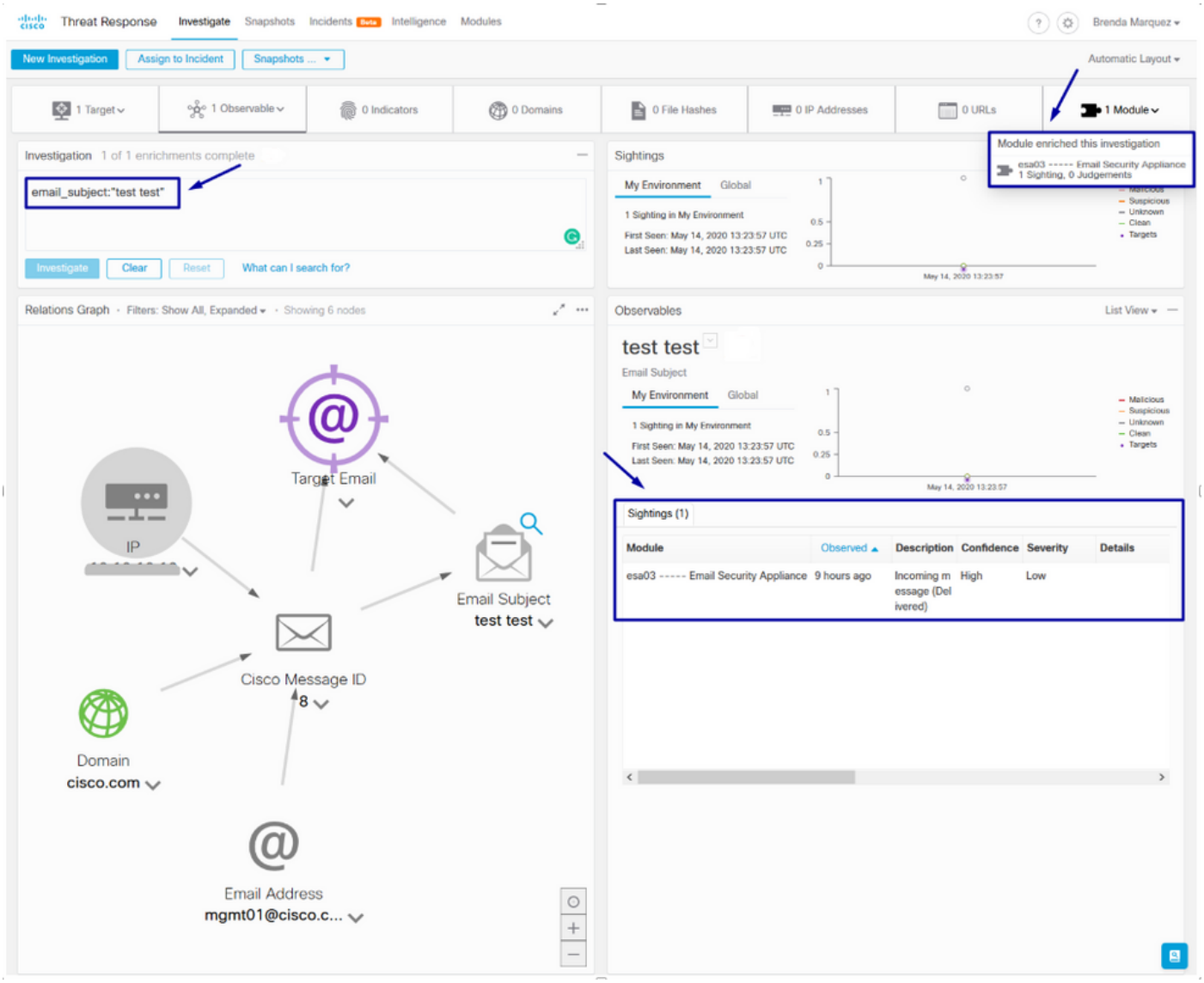


Verifica

Per verificare l'integrazione di CTR ed ESA, è possibile inviare un messaggio di prova, che può essere visualizzato anche dall'ESA, selezionare Monitor > Message Tracking e trovare l'e-mail di prova. In questo caso, ho filtrato per Oggetto e-mail come immagine qui sotto.



Ora, dal portale CTR, è possibile eseguire un'Indagine, passare a Indaga e utilizzare alcuni e-mail osservabili, come mostrato nell'immagine.



Suggerimento: È possibile utilizzare la stessa sintassi per altri oggetti osservabili tramite e-mail come indicato di seguito nell'immagine.

IP address	ip:"4.2.2.2"
Domain	domain:"cisco.com"
Sender email address	email:"noreply@cisco.com"
Email message header	email_messageid:"123-abc-456@cisco.com"

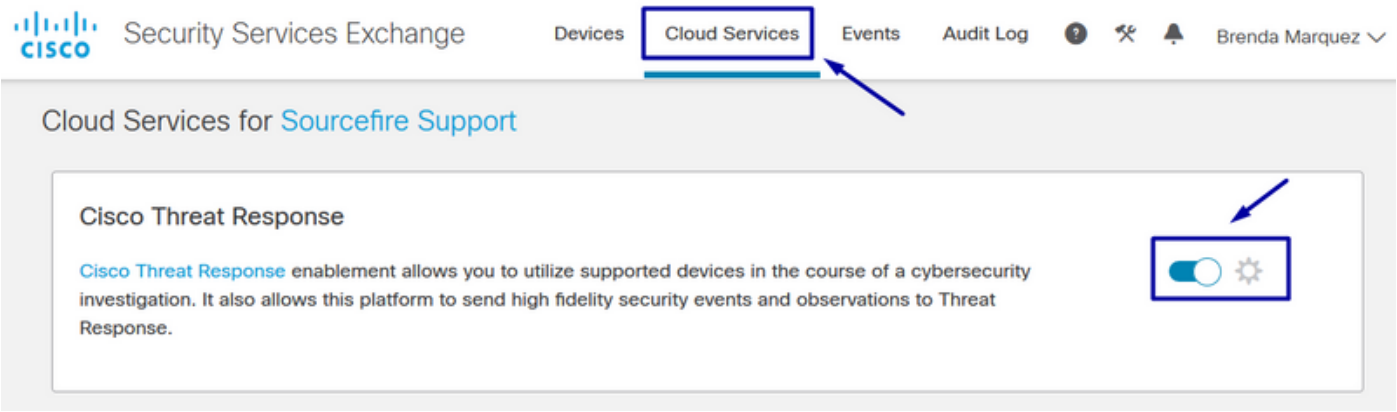
Email subject	email_subject:"Invoice Due"
Cisco Message ID (MID)	cisco_mid:"12345"
SHA256 filehash	sha256:"sha256filehash"
Email attachment file name	file_name:"invoice.pdf"

Risoluzione dei problemi

I clienti CES o che gestiscono i dispositivi ESA tramite SMA possono connettersi solo a Threat Response tramite SMA. Verificare che il modulo SMA esegua AsyncOS 12.5 o versione successiva. Se l'ESA non viene gestita con un SMA e viene integrata direttamente, verificare che sia AsyncOS versione 13.0 o successive.

Il dispositivo ESA non è visualizzato nel portale CTR

Se il dispositivo ESA non viene visualizzato nell'elenco a discesa Periferica registrata mentre il modulo ESA viene aggiunto nel portale CTR, assicurarsi di aver abilitato CTR in SSE, in CTR passare a Moduli > Dispositivi > Gestisci dispositivi, quindi in Portale SSE passare a Servizi cloud e abilitare CTR, come nell'immagine seguente:



L'inchiesta sul CTR non mostra dati forniti dall'ESA

Assicurarsi che:

- La sintassi dell'indagine è corretta, gli e-mail osservabili sono mostrati sopra nella sezione Verifica.
- Èstato selezionato il server di risposta alla minaccia appropriato o il cloud (Americhe/Europa).

L'ESA non richiede il token di registrazione

Assicurarsi di eseguire il commit delle modifiche, quando la funzionalità Threat Response è stata abilitata, altrimenti le modifiche non verranno applicate alla sezione Threat Response dell'ESA.

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

Verificare che il token sia generato dal cloud corretto:

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

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

Inoltre, ricorda che il token di registrazione ha una scadenza (seleziona l'ora più conveniente per completare l'integrazione in tempo).

Informazioni correlate

- **Le informazioni contenute in questo articolo sono disponibili nel video Cisco Threat Response e ESA Integration.**
- Documentazione e supporto tecnico – Cisco Systems