

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

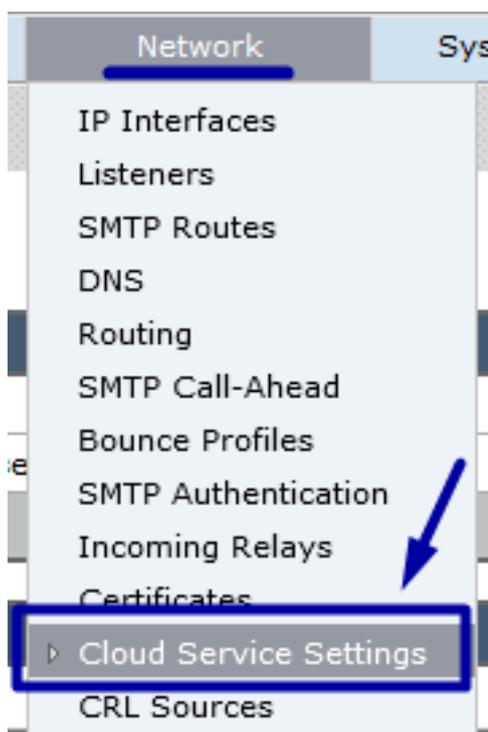
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Cloud Service Settings

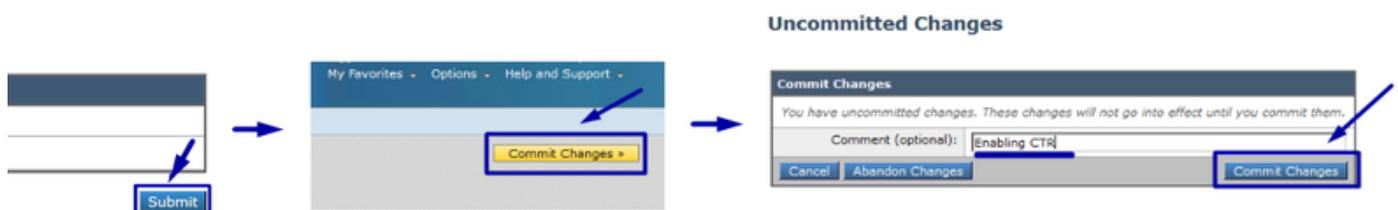


Nota: La selezione predefinita per l'URL del server di risposta alle minacce è AMERICAS (api-sse.cisco.com). Per le aziende europee, fare clic sul menu a discesa e scegliere EUROPA (api.eu.sse.itd.cisco.com)

Passaggio 4. Sottomettere e confermare le modifiche

È necessario 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.



Cloud Service Settings

Success — Your changes have been committed.

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

Cloud Services Settings	
Status:	The Cisco Cloud Service is busy. Navigate back to this page after some time to check the appliance status.

Cloud Service Settings

Cloud Services	
Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)
Edit Settings	

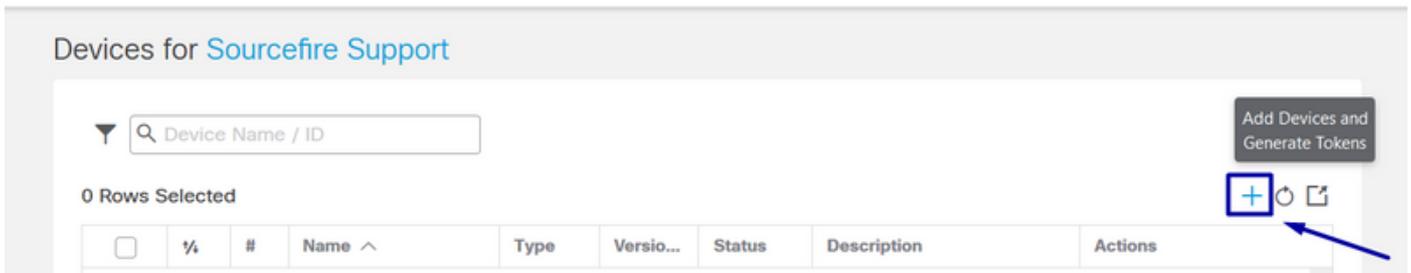
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	
Register	

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.

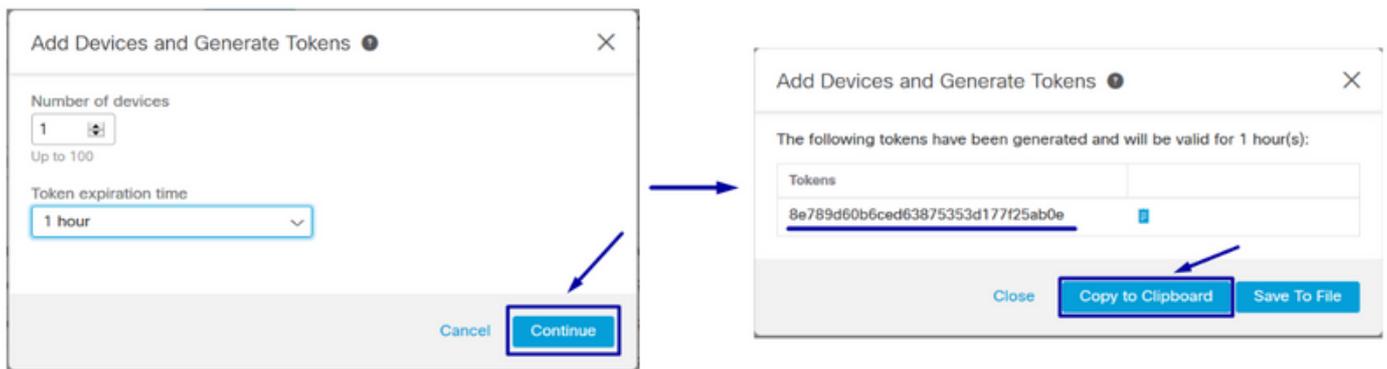
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu item is highlighted with a blue box and an arrow. Below the navigation, the breadcrumb 'Settings > Devices' is shown. The 'Devices' section has a blue sidebar with 'Settings', 'Your Account', 'Devices', 'API Clients', and '> Modules'. The 'Devices' item in the sidebar is highlighted with a blue box and an arrow. In the main content area, the 'Manage Devices' button is highlighted with a blue box and an arrow, along with the 'Reload Devices' button. Below these buttons is a table with columns 'Name' and 'Type'.

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.



Cloud Service Settings

Success — A request to register your appliance with the Cisco Threat Response portal is initiated. Navigate back to this page after some time to check the appliance status.

Cloud Services

Threat Response:	Enabled
Threat Response Server:	AMERICAS (api-sse.cisco.com)

[Edit Settings](#)

Cloud Services Settings

Status:	The appliance registration is in progress. Navigate back to this page after some time to check the appliance status.
---------	--

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

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

Security Services Exchange Audit Log Brenda Marquez

Devices for Sourcefire Support

Search: esa03

0 Rows Selected

	%	#	Name ^	Type	Versio...	Status	Description	Actions
<input type="checkbox"/>	▼	1	esa03.mex-amp.inl...	ESA	13.0.0	Registere	ESA	

ID: 874141f7-903f-4be9-b14e-45a7f... IP Address: 127.0.0.1 Connector Version: 1.3.34
Created: 2020-05-11 20:41:05 UTC

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.

Threat Response Investigate Snapshots Incidents Intelligence **Modules** Brenda Marquez

Settings > Modules

Modules

Intelligence within Cisco Threat Response is provided by modules, which can also enable response capabilities. [Click here to view all the available modules.](#)

Your Configurations

[Add New Module](#)

Amp AMP for Endpoints
AMP for Endpoints
AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.
[Edit](#) [Learn More](#)

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

Settings

Your Account

Devices

API Clients

Modules

Available Modules

Users

Available Modules

Select a module you would like to add, or [click here to learn more](#) about modules configuration.

Amp AMP for Endpoints

AMP for Endpoints prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.

[Add New Module](#)
[Learn More](#)
[Free Trial](#)

Esa Email Security Appliance

The Cisco Email Security Appliance (ESA) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent data loss, and secu...

[Add New Module](#)
[Learn More](#)

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


[Threat Response](#)
[Investigate](#)
[Snapshots](#)
[Incidents](#)
Beta
[Intelligence](#)
[Modules](#)



Brenda Marquez

Settings > Modules > Available Modules > Email Security Appliance > Add New Module

Add New Email Security Appliance Module

esa03.mex-amp.inlab
 Type ESA
 ID 874141f7-903f-4be9-b14e-45a7f34a2032
 IP Address 127.0.0.1

Quick Start [Help](#)

When configuring Email Security Appliance (ESA) integration, you must first enable the integration in ESA. You then enable Threat Response in Security Services Exchange, add the device and register it. After this is completed, you add the ESA module.

Prerequisite: ESA running minimum AsyncOS 13.0.0-314 (LD) release.

Note: Customers with multiple ESAs reporting to an SMA can use the SMA Module configuration for Email Security. Customers that do not have an SMA, can use the ESA Module for integration.

- In ESA, navigate to **Networks > Cloud Service Settings > Edit Settings**, enable integration and confirm that the ESA is ready to accept a registration token.
- Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
- Enable **Cisco Threat Response** integration on the **Cloud Services** tab, and then click the **Devices** tab and click the + icon to add a new device.
- Specify the token expiration time (the default is 1 hour), and click **Continue**.
- Copy the generated token and confirm the device has been created.
- Navigate to your ESA (**Network > Cloud Service Settings**) to insert the token, and then click **Register**. Confirm successful registration by reviewing the status in Security Services Exchange and confirm the ESA is displayed on the **Devices** page.
- Complete the **Add New Email Security Appliance Module** form:
 - Module Name** - Leave the default name or enter a name that is meaningful to you.
 - Registered Device** - From the drop-down list, choose the device you registered in Security Services Exchange.
 - Request Timeframe (days)** - Enter the timeframe (in days) for querying the API endpoint (default is 30 days).
- Click **Save** to complete the ESA module configuration.

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.

Cisco C100V
Email Security Virtual Appliance

Home Monitor Mail Policies Security Services Network System Administration

Message Tracking

Search

Available Time Range: 14 May 2020 12:44 to 14 May 2020 13:41 (GMT +00:00) Data in time range: 100.0% complete

Envelope Sender: ? Begins With []

Envelope Recipient: ? Begins With []

Subject: Begins With test test

Message Received: Last Day Last Week Custom Range

Start Date: 05/13/2020 Time: 13:00 and End Date: 05/14/2020 Time: 13:42 (GMT +00:00)

Advanced Search messages using advanced criteria

Clear Search

Generated: 14 May 2020 13:42 (GMT +00:00) Export All... | Export...

Results

Items per page 20

Displaying 1 — 1 of 1 items.

1	14 May 2020 13:23:57 (GMT +00:00)	MID: 8	Show Details
---	-----------------------------------	--------	--------------

SENDER: mgmt01@cisco.com
RECIPIENT: testingBren@cisco.com
SUBJECT: test test
LAST STATE: Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:

Displaying 1 — 1 of 1 items.

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

The screenshot shows the Cisco Threat Response Investigate interface. At the top, there are navigation tabs: Threat Response, Investigate (selected), Snapshots, Incidents, Intelligence, and Modules. The user is Brenda Marquez. The interface displays search filters: 1 Target, 1 Observable, 0 Indicators, 0 Domains, 0 File Hashes, 0 IP Addresses, 0 URLs, and 1 Module. The search query is `email_subject:"test test"`. The Results section shows a Relations Graph with nodes for IP, Target Email, Email Subject test test, Cisco Message ID 8, Domain cisco.com, and Email Address mgmt01@cisco.c... The Sighting panel shows 1 Sighting in My Environment with a graph and details: First Seen: May 14, 2020 13:23:57 UTC, Last Seen: May 14, 2020 13:23:57 UTC. The Observables panel shows 1 Sighting in My Environment with a graph and details: First Seen: May 14, 2020 13:23:57 UTC, Last Seen: May 14, 2020 13:23:57 UTC. A table of Sighting (1) is shown below:

Module	Observed	Description	Confidence	Severity	Details
esa03 ----- Email Security Appliance	9 hours ago	Incoming m essage (Del ivered)	High	Low	

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

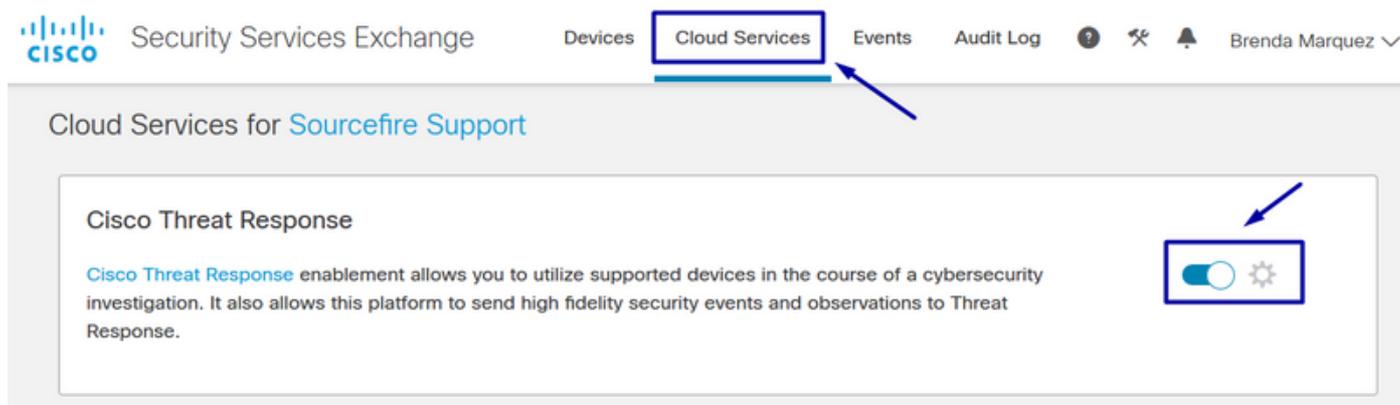
IP address	<code>ip:"4.2.2.2"</code>	Email subject	<code>email_subject:"Invoice Due"</code>
Domain	<code>domain:"cisco.com"</code>	Cisco Message ID (MID)	<code>cisco_mid:"12345"</code>
Sender email address	<code>email:"noreply@cisco.com"</code>	SHA256 filehash	<code>sha256:"sha256filehash"</code>
Email message header	<code>email_messageid:"123-abc-456@cisco.com"</code>	Email attachment file name	<code>file_name:"invoice.pdf"</code>

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.
- È stato 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](#)