

Solutions de sécurité pour neutraliser les menaces réseau Cisco (CTR) et intégration ESA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurer](#)

[Étape 1. Naviguez vers des configurations de réseau > de service en nuage](#)

[Étape 2. Cliquez sur éditer en fonction des configurations](#)

[Étape 3. Sélectionnez l'enable de case à cocher et le serveur de réponse de menace](#)

[Étape 4. Soumettez et commettez les modifications](#)

[Étape 5. Connectez-vous dans le CTR portail et générez le jeton d'enregistrement demandé dans l'ESA](#)

[Étape 6. Collez le jeton d'enregistrement \(généralisé du portail CTR\) dans l'ESA](#)

[Étape 7. Vérifiez que votre périphérique ESA est dans le portail SSE](#)

[Étape 8. Naviguez vers le CTR portail et ajoutez un nouveau module ESA](#)

[Vérifier](#)

[Dépanner](#)

[Le périphérique ESA n'est pas affiché dans le portail CTR](#)

[L'enquête CTR n'affiche pas des données de l'ESA](#)

[L'ESA ne demande pas le jeton d'enregistrement](#)

[L'enregistrement a manqué en raison d'un jeton non valide ou expiré](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus pour intégrer les Solutions de sécurité pour neutraliser les menaces réseau Cisco (CTR) avec l'appliance de sécurité du courrier électronique (ESA) et comment vérifier ceci afin d'exécuter quelques investigations CTR.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solutions de sécurité pour neutraliser les menaces réseau Cisco
- [Dispositif de sécurité de la messagerie](#)

[Composants utilisés](#)

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

- Compte CTR
- Échange de services de sécurité Cisco
- ESA C100V sur la version de logiciel 13.0.0-392

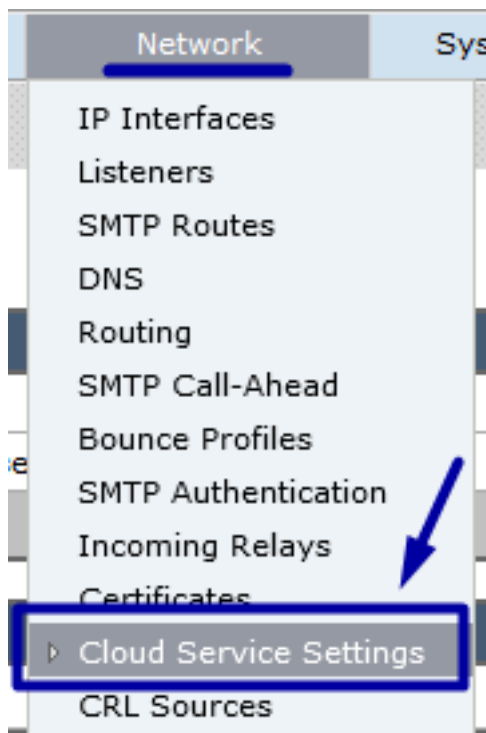
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Afin de configurer le CTR et l'ESA d'intégration, ouvrez une session à votre appliance virtuelle de sécurité du courrier électronique et suivez ces étapes rapides :

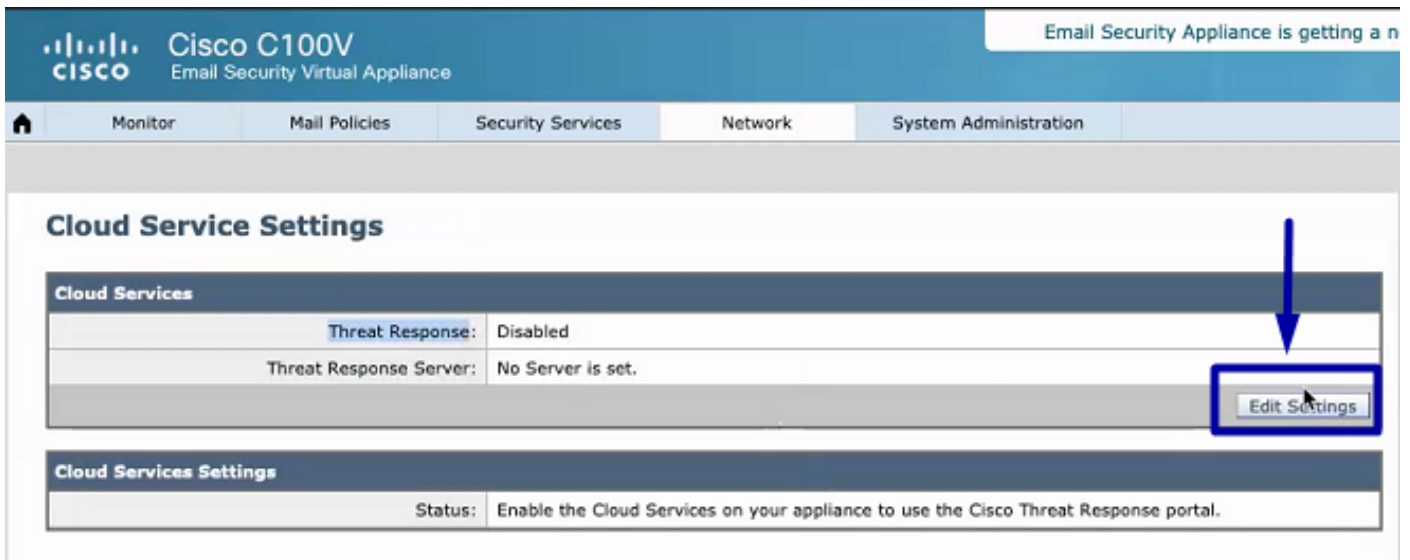
Étape 1. Naviguez vers des configurations de réseau > de service en nuage

Une fois dans l'ESA, naviguez vers les configurations de réseau > de service en nuage de menu contextuel, afin de voir actuellement l'état de réponse de menace (désactivé/activé) suivant les indications de l'image.



Étape 2. Cliquez sur éditer en fonction des configurations

Jusqu'ici la caractéristique de réponse de menace dans l'ESA est désactivée, afin d'activer la caractéristique, cliquez sur en fonction des configurations Edit suivant les indications de l'image :



Étape 3. Sélectionnez l'enable de case à cocher et le serveur de réponse de menace

Sélectionnez l'enable de case à cocher, puis choisissez le serveur de réponse de menace, voyez s'il vous plaît l'image ci-dessous :

Cloud Service Settings



Remarque: La sélection par défaut pour l'URL de serveur de réponse de menace est l'AMÉRIQUES (api-sse.cisco.com). Pour des entreprises de l'EUROPE, cliquez sur le menu déroulant et choisissez l'EUROPE (api.eu.sse.itd.cisco.com)

Étape 4. Soumettez et commettez les modifications

On l'exige pour soumettre et commettre les modifications, afin de sauvegarder et appliquer n'importe quelle modification. Maintenant si l'interface ESA est régénérée un jeton d'enregistrement est demandé afin d'enregistrer l'intégration, suivant les indications de l'image ci-dessous.

Remarque: Vous pouvez voir un message de succès : Vos modifications ont été commises.



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	

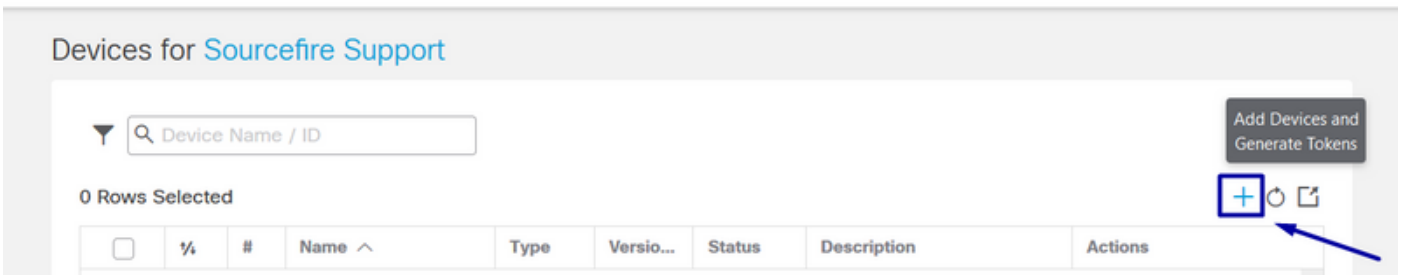
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	

Étape 5. Connectez-vous dans le CTR portail et générez le jeton d'enregistrement demandé dans l'ESA

1. Une fois dans le portail CTR, naviguez vers des modules > des périphériques > gèrent des périphériques, voici s'il vous plaît la prochaine image.

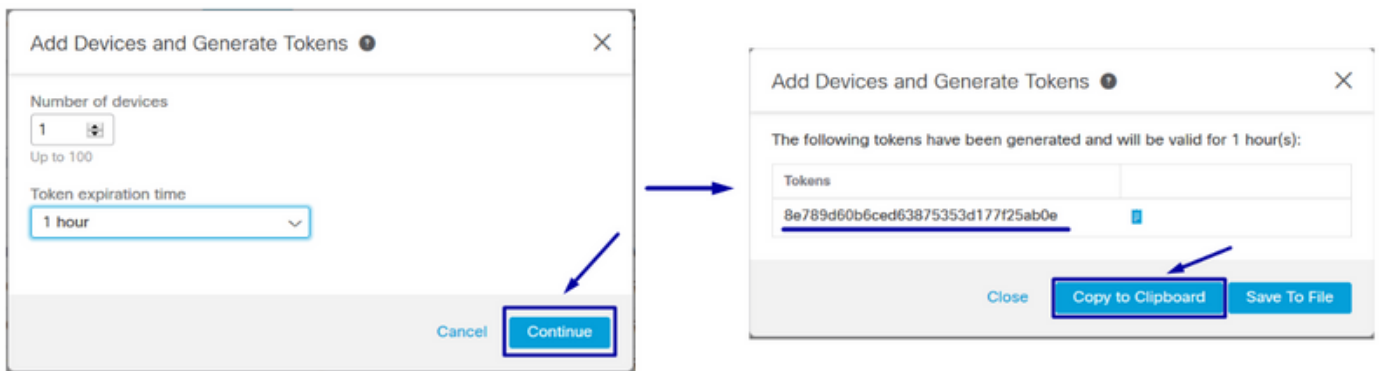
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu item is highlighted with a blue box and an arrow. Below the navigation, the breadcrumb 'Settings > Devices' is shown. The 'Devices' page title is also highlighted with an arrow. In the left sidebar, the 'Devices' menu item 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. Below the buttons, a table with columns 'Name' and 'Type' is visible.

2. Gérez les périphériques que le lien vous réoriente à l'échange de Services de sécurité (SSE), une fois que là, cliquez sur en fonction l'icône ajoutent des périphériques et génèrent des jetons suivant les indications de l'image.



3. Cliquez sur en fonction Continue afin de générer le jeton, une fois que le jeton est généré, cliquent sur en fonction la copie au presse-papier, suivant les indications de l'image.

Conseil : Vous pouvez sélectionner le nombre de périphériques pour ajouter (de 1 et jusqu'à de 100) et pour sélectionner également le temps d'expiration symbolique (1hr, 2hrs, 4hrs, 6hrs, 8hrs, 12hrs, 01 jours, 02 jours, 03 jours, 04 jours et 05 jours).



Étape 6. Collez le jeton d'enregistrement (généralisé du portail CTR) dans l'ESA

Une fois que le jeton d'enregistrement est généré, collez-le dans la section de configurations de services en nuage dans l'ESA, comme image ci-dessous.

Remarque: Vous pouvez voir un message de succès : Une demande d'enregistrer votre appliance avec le portail de Solutions de sécurité pour neutraliser les menaces réseau Cisco est initiée. Naviguez de nouveau à cette page après un certain temps pour vérifier l'état d'appareils.

Cloud Service Settings



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.
---------	--

Étape 7. Vérifiez que votre périphérique ESA est dans le portail SSE

Vous pouvez naviguer vers le portail SSE (le CTR > les modules > les périphériques > gèrent des périphériques), et dans l'onglet de recherche regardez votre périphérique ESA, suivant les indications de l'image.

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

Étape 8. Naviguez vers le CTR portail et ajoutez un nouveau module ESA

1. Une fois que vous êtes dans le portail CTR, naviguez vers des modules > ajoutent le nouveau module, suivant les indications de l'image.

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

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. Choisissez le type de module, dans ce cas, le module est un module d'appareils de sécurité du

courrier électronique comme image ci-dessous.

Settings > Modules > Available Modules

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. Entrez dans les champs : Nom du module, périphérique enregistré (sélectionnez celui précédemment enregistré) et délai de demande (jours), et sauvegarde, suivant les indications de l'image.

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

Add New Email Security Appliance Module

Module Name*

Registered Device*

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

Request Timeframe (days)

[Save](#) [Cancel](#)

Quick Start

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.

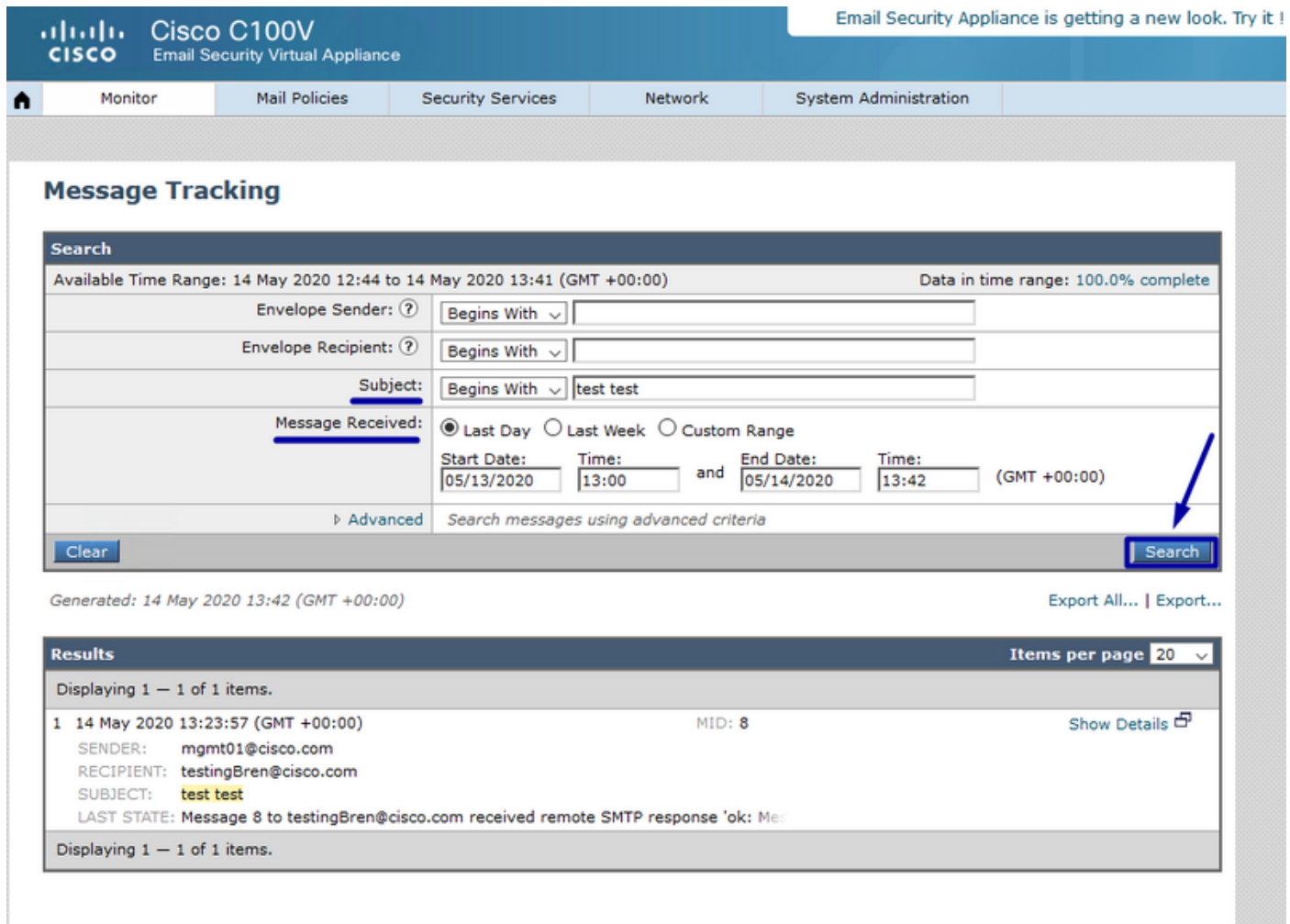
Prerequisite: ESA running minimum AsyncOS 13.0 0-314 (LD) release.

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.

1. In ESA, navigate to **Networks > Cloud Service Settings > Edit Settings**, enable integration and confirm that the ESA is ready to accept a registration token.
2. Click the **Settings** icon (gear) and then click **Devices > Manage Devices** to be taken to Security Services Exchange.
3. 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.
4. Specify the token expiration time (the default is 1 hour), and click **Continue**.
5. Copy the generated token and confirm the device has been created.
6. 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.
7. 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).
8. Click **Save** to complete the ESA module configuration.

Vérifiez

Afin de vérifier l'intégration CTR et ESA, vous pouvez envoyer un email de test, que vous pouvez également le voir de votre ESA, naviguer pour surveiller > message dépistant, et trouver l'email de test. Dans ce cas, j'ai filtré par le sujet d'email comme image ci-dessous.



The screenshot displays the Cisco C100V Email Security Virtual Appliance interface. At the top, the Cisco logo and 'Cisco C100V Email Security Virtual Appliance' are visible. A navigation bar includes 'Monitor', 'Mail Policies', 'Security Services', 'Network', and 'System Administration'. The main content area is titled 'Message Tracking' and contains a search form. The search form includes fields for 'Envelope Sender', 'Envelope Recipient', and 'Subject', each with a 'Begins With' dropdown and a text input. The 'Subject' field contains 'test test'. Below these fields are radio buttons for 'Last Day', 'Last Week', and 'Custom Range', with 'Last Day' selected. The 'Custom Range' section shows 'Start Date: 05/13/2020 13:00' and 'End Date: 05/14/2020 13:42 (GMT +00:00)'. A blue arrow points to the 'Search' button. Below the search form, the text 'Generated: 14 May 2020 13:42 (GMT +00:00)' and 'Export All... | Export...' are visible. The 'Results' section shows 'Displaying 1 — 1 of 1 items.' and a table with one entry: '1 14 May 2020 13:23:57 (GMT +00:00) MID: 8 Show Details'. The email details include 'SENDER: mgmt01@cisco.com', 'RECIPIENT: testingBren@cisco.com', and 'SUBJECT: test test'. The 'LAST STATE' is 'Message 8 to testingBren@cisco.com received remote SMTP response 'ok: Me:'. The bottom of the results section shows 'Displaying 1 — 1 of 1 items.'

Maintenant, du portail CTR, vous pouvez exécuter une enquête, naviguer pour étudier, et en utiliser envoyez les choses observables, suivant les indications de l'image.

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 bar contains the query `email_subject:'test test'`. Below the search bar is a 'Relations Graph' showing connections between entities like IP, Target Email, Email Subject, Cisco Message ID, Domain, and Email Address. On the right, there are 'Sightings' and 'Observables' sections. The 'Sightings' section shows a graph and a table with one sighting. The table is highlighted with a blue box:

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

Conseil : Vous pouvez utiliser la même syntaxe pour d'autres choses observables d'email comme suit dans l'image.

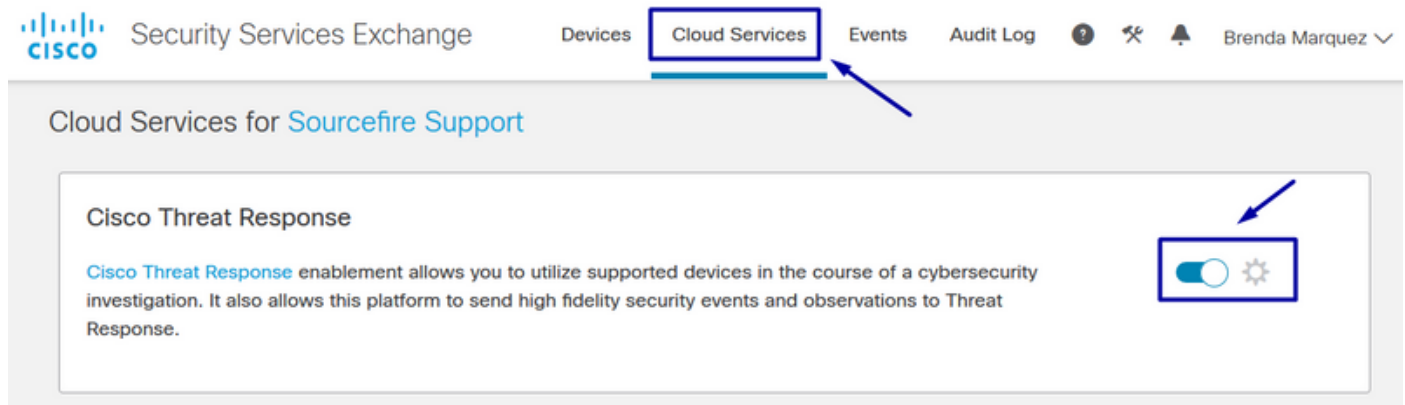
IP address	<code>ip:"4.2.2.2"</code>	Email subject	<code>email_subject:"Invoice Due"</code>
Domain	<code>domain:"cisco.com"</code>	Cisco Message ID (MID)	<code>cisco_mid:"12345"</code>
Sender email address	<code>email:"noreply@cisco.com"</code>	SHA256 filehash	<code>sha256:"sha256filehash"</code>
Email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

Dépanner

Si vous êtes un client de CES ou si vous gérez vos périphériques ESA par l'intermédiaire d'un SMA, vous pouvez seulement se connecter à la réponse de menace par l'intermédiaire de votre SMA. Veuillez assurer vos passages AsyncOS 12.5 SMA ou plus élevé. Si vous ne gérez pas votre ESA avec un SMA et vous intégrez l'ESA directement, assurez qu'il est à la version 13.0 ou ultérieures d'AsyncOS.

Le périphérique ESA n'est pas affiché dans le portail CTR

Si votre périphérique ESA n'est pas affiché dans le périphérique enregistré par déroulant tandis que le module ESA est ajouté dans le portail CTR, assurez s'il vous plaît pour avoir activé le CTR dans le SSE, dans le CTR naviguez vers des modules > des périphériques > gèrent des périphériques, alors dans le portail SSE naviguez vers les services en nuage et le CTR d'enable, comme image ci-dessous :



L'enquête CTR n'affiche pas des données de l'ESA

Veillez assurer cela :

- La syntaxe de l'enquête est correcte, les choses observables d'email sont affichées ci-dessus dans la section de vérifier.
- Vous avez sélectionné le serveur de réponse de menace ou le nuage approprié (Amériques/Europe).

L'ESA ne demande pas le jeton d'enregistrement

Assurez s'il vous plaît pour commettre les modifications, quand la réponse de menace a été activée, autrement, les changements ne seront pas appliqués à la section de réponse de menace de l'ESA.

L'enregistrement a manqué en raison d'un jeton non valide ou expiré

Veillez s'assurer que le jeton est généré du nuage correct :

Si vous utilisez le nuage de l'Europe (UE) pour l'ESA, générez le jeton de :
<https://admin.eu.sse.itd.cisco.com/>

Si vous utilisez le nuage de l'Amériques (NAM) pour l'ESA, générez le jeton de :
<https://admin.sse.itd.cisco.com/>

En outre, souvenez-vous que le jeton d'enregistrement a un temps d'expiration (sélectionnez l'heure la plus commode de se terminer l'intégration à temps).

[Informations connexes](#)

- Vous pouvez trouver les informations contenues en cet article dans le vidéo de [Solutions de sécurité pour neutraliser les menaces réseau Cisco et d'intégration ESA](#).
- [Support et documentation techniques - Cisco Systems](#)