

Intégration Cisco Threat Response (CTR) et ESA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Étape 1. Naviguez jusqu'à Network > Cloud Service Settings](#)

[Étape 2. Cliquez sur Modifier les paramètres](#)

[Étape 3. Cochez la case Enable \(Activer\) et Threat Response Server \(Serveur de réponse aux menaces\).](#)

[Étape 4. Soumettre et valider les modifications](#)

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

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

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

[Étape 8. Accédez au portail CTR et ajoutez un nouveau module ESA](#)

[Vérification](#)

[Dépannage](#)

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

[L'enquête du CTR ne montre pas les données de l'ESA](#)

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

[Échec de l'enregistrement en raison d'un jeton non valide ou expiré](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus d'intégration de Cisco Threat Response (CTR) avec l'appliance de sécurité de la messagerie électronique (ESA) et comment le vérifier afin d'effectuer certaines enquêtes CTR.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réponse Cisco aux menaces
- Dispositif de sécurité de la messagerie

Components Used

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

- Compte CTR
- Cisco Security Services Exchange
- ESA C100V sur la version logicielle 13.0.0-392

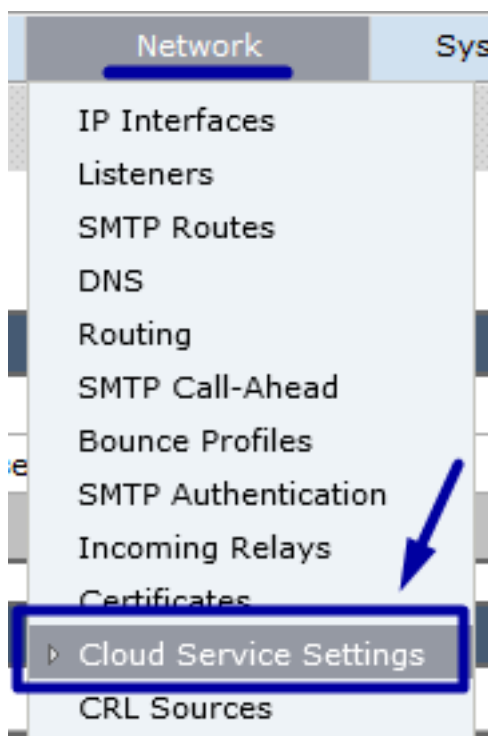
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Afin de configurer le CTR d'intégration et le ESA, connectez-vous à votre appliance virtuelle de sécurité de la messagerie et suivez les étapes rapides suivantes :

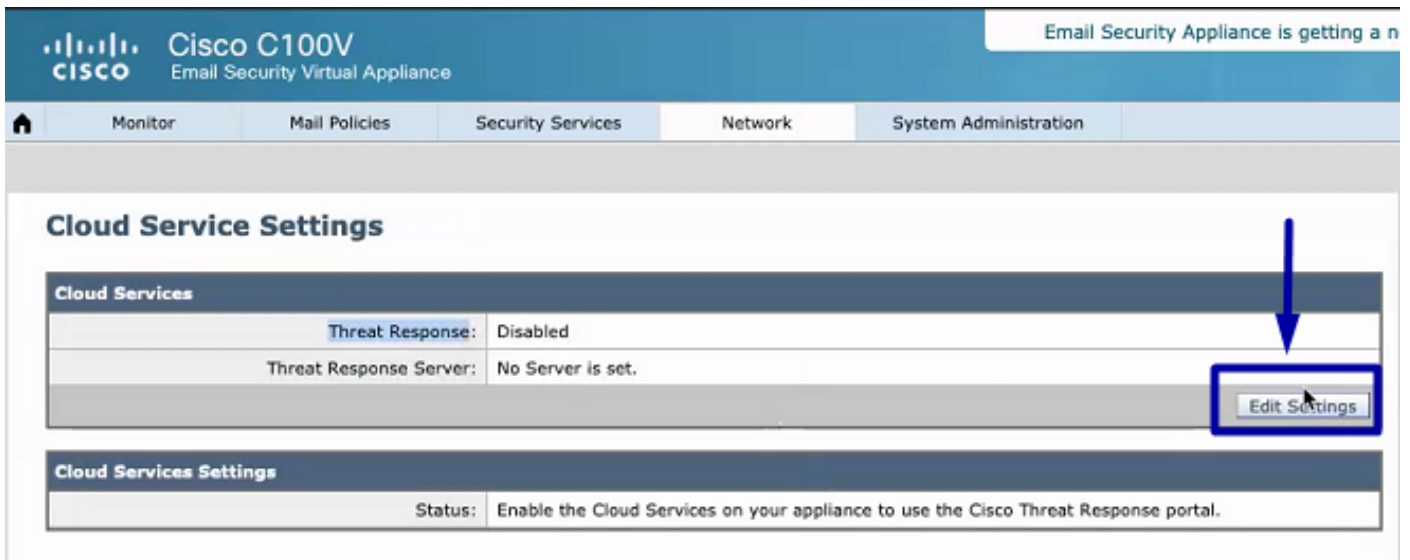
Étape 1. Naviguez jusqu'à Network > Cloud Service Settings

Une fois dans l'ESA, accédez au menu contextuel Network > Cloud Service Settings, afin de voir l'état actuel de la réponse aux menaces (Disabled / Enabled) tel qu'illustré dans l'image.



Étape 2. Cliquez sur Modifier les paramètres

Jusqu'à présent, la fonction de réponse aux menaces dans l'ESA est désactivée, afin d'activer cette fonction, cliquez sur Modifier les paramètres comme indiqué dans l'image :



Étape 3. Cochez la case Enable (Activer) et Threat Response Server (Serveur de réponse aux menaces).

Cochez la case Activer, puis sélectionnez le serveur de réponse aux menaces. Reportez-vous à l'image ci-dessous :

Cloud Service Settings

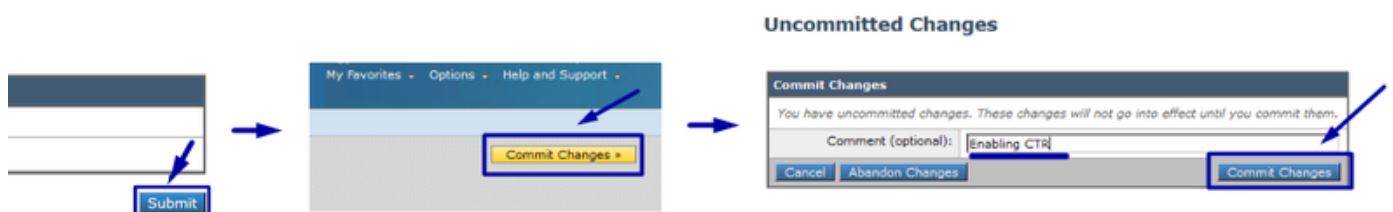


Note: La sélection par défaut pour l'URL du serveur de réponse aux menaces est AMERICAS (api-sse.cisco.com). Pour les entreprises EUROPE, cliquez sur le menu déroulant et choisissez EUROPE (api.eu.sse.itd.cisco.com)

Étape 4. Soumettre et valider les modifications

Il est nécessaire d'envoyer et de valider les modifications, afin d'enregistrer et d'appliquer toute modification. Maintenant, si l'interface ESA est actualisée, un jeton d'enregistrement est demandé afin d'enregistrer l'intégration, comme indiqué dans l'image ci-dessous.

Note: Vous pouvez voir un message de réussite : Vos modifications ont été validées.



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	

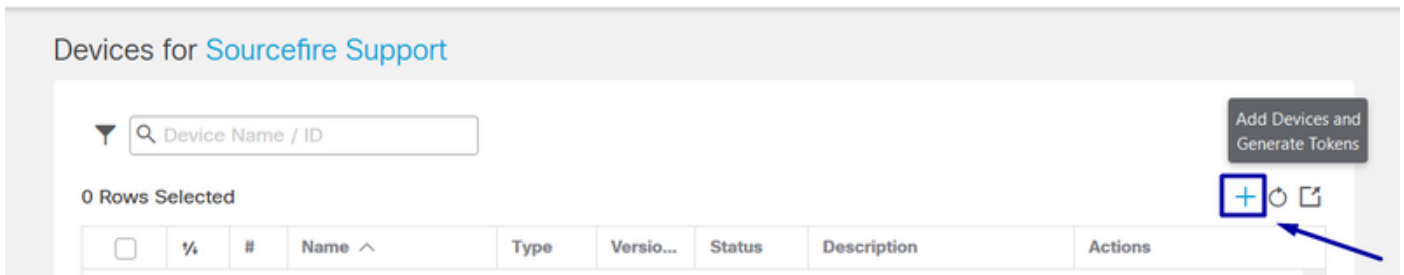
Cloud Services Settings	
Registration Token: ?	<input type="text"/>
Register	

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

1.- Une fois dans le portail CTR, accédez à Modules > Périphériques > Gérer les périphériques. Reportez-vous à l'image suivante.

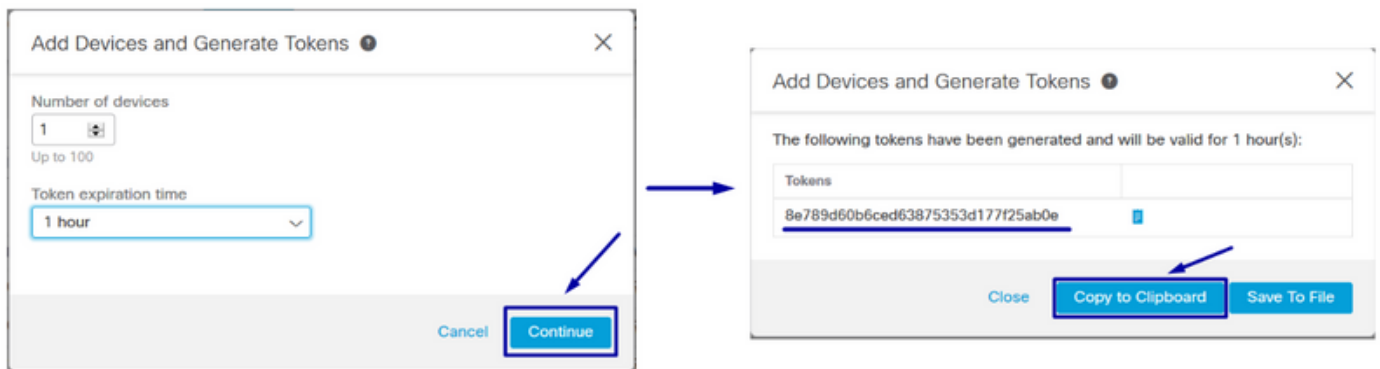
The screenshot shows a web browser at the URL <https://visibility.amp.cisco.com/settings/devices>. The navigation menu includes Threat Response, Investigate, Snapshots, Incidents (Beta), Intelligence, and Modules. The 'Modules' menu item is highlighted with a blue box and an arrow. Below the navigation,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

2.- Le lien Manage Devices (Gérer les périphériques) vous redirige vers Security Services Exchange (SSE). Une fois sur ce lien, cliquez sur l'icône Add Devices and Generate Tokens (Ajouter des périphériques et générer des jetons), comme illustré dans l'image.



3.- Cliquez sur Continuer afin de générer le jeton, une fois le jeton généré, cliquez sur Copier dans le Presse-papiers, comme illustré dans l'image.

Astuce : Vous pouvez sélectionner le nombre de périphériques à ajouter (de 1 et jusqu'à 100) et également sélectionner le délai d'expiration du jeton (1h, 2h, 4h, 6h, 8h, 12h, 01 jours, 02 jours, 03 jours, 04 jours et 05 jours).



Étape 6. Coller le jeton d'enregistrement (généré à partir du portail CTR) dans l'ESA

Une fois le jeton d'enregistrement généré, collez-le dans la section Cloud Services Settings de l'ESA, comme l'image ci-dessous.

Note: Vous pouvez voir un message de réussite : Une demande d'enregistrement de votre appareil auprès du portail Cisco Threat Response est lancée. Revenez à cette page après un certain temps pour vérifier l'état de l'appliance.

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 se trouve dans le portail SSE

Vous pouvez accéder au portail SSE (CTR > Modules > Périphériques > Gérer les périphériques), et dans l'onglet Rechercher, consultez votre périphérique ESA, comme illustré dans l'image.

Security Services Exchange Audit Log Brenda Marquez

Devices for Sourcefire Support

Search:

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. Accédez au portail CTR et ajoutez un nouveau module ESA

1.- Une fois que vous êtes dans le portail CTR, accédez à Modules > Add New Module, comme illustré dans l'image.

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.- Choisissez le type de module, dans ce cas, le module est un module de dispositif de sécurité de la messagerie comme l'image ci-dessous.

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.- Entrez les champs suivants : Nom du module, Périphérique enregistré (sélectionnez celui précédemment enregistré), Délai de demande (jours) et Enregistrer, comme l'illustre l'image.

Threat Response Investigate Snapshots Incidents **Beta** Intelligence Modules

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.

- 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.

Vérification

Afin de vérifier l'intégration CTR et ESA, vous pouvez envoyer un e-mail de test, que vous pouvez également voir à partir de votre ESA, naviguer jusqu'à Monitor > Message Tracking et trouver l'e-mail de test. Dans ce cas, j'ai filtré par Objet e-mail comme l'image ci-dessous.

The screenshot shows the Cisco C100V Message Tracking interface. The top navigation bar includes 'Monitor', 'Mail Policies', 'Security Services', 'Network', and 'System Administration'. The 'Message Tracking' section is active, displaying search criteria and results.

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.

À présent, à partir du portail CTR, vous pouvez effectuer une enquête, naviguer jusqu'à Enquêter et utiliser certains observables de messagerie, comme l'illustre 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 main search bar contains the query `email_subject:'test test'`. Below the search bar, there are statistics for the investigation: 1 Target, 1 Observable, 0 Indicators, 0 Domains, 0 File Hashes, 0 IP Addresses, 0 URLs, and 1 Module. The Sighting panel shows a single sighting in the 'My Environment' with a score of 1. The Observables panel shows the search results for 'test test', including a table of sightings.

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

Astuce : Vous pouvez utiliser la même syntaxe pour d'autres observables de messagerie, comme suit dans l'image.

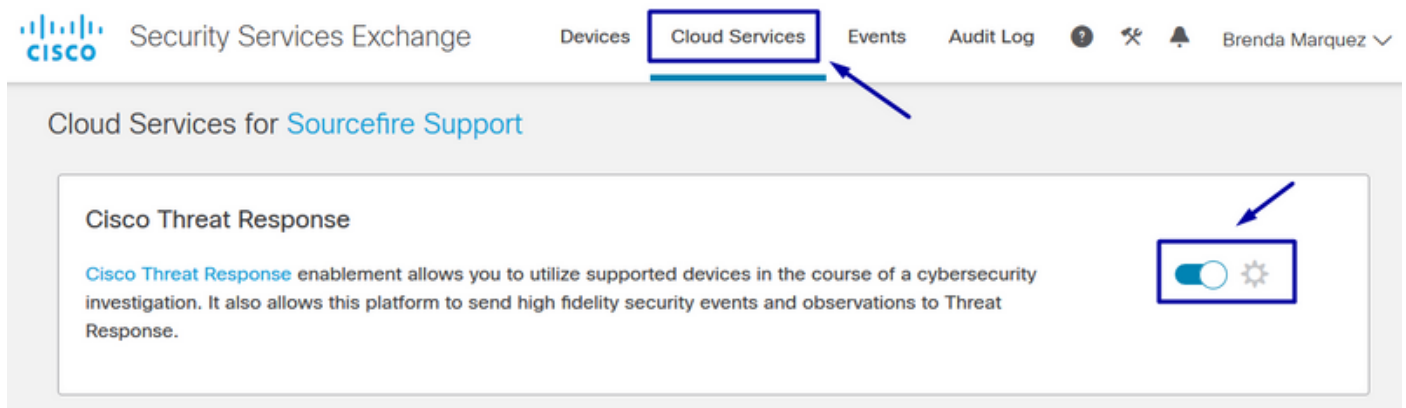
IP address	<code>ip:"4.2.2.2"</code>	Email subject	<code>email_subject:"Invoice Due"</code>
Domain	<code>domain:"cisco.com"</code>	Cisco Message ID (MID)	<code>cisco_mid:"12345"</code>
Sender email address	<code>email:"noreply@cisco.com"</code>	SHA256 filehash	<code>sha256:"sha256filehash"</code>
Email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

Dépannage

Si vous êtes un client CES ou si vous gérez vos périphériques ESA via un SMA, vous ne pouvez vous connecter à Threat Response que via votre SMA. Assurez-vous que votre SMA exécute AsyncOS 12.5 ou version ultérieure. Si vous ne gérez pas votre ESA avec un SMA et que vous l'intégrez directement, assurez-vous qu'il est dans AsyncOS version 13.0 ou ultérieure.

Le périphérique ESA n'apparaît pas dans le portail CTR

Si votre périphérique ESA n'apparaît pas dans la liste déroulante Registered Device alors que le module ESA est ajouté dans le portail CTR, assurez-vous d'avoir activé CTR dans SSE, dans CTR, accédez à Modules > Devices > Manage Devices, puis dans le portail SSE, accédez aux services cloud et activez CTR, comme l'image ci-dessous :



L'enquête du CTR ne montre pas les données de l'ESA

Veillez vous assurer que :

- La syntaxe de l'enquête est correcte, les observables de messagerie sont affichés ci-dessus dans la section Vérification.
- Vous avez sélectionné le serveur de réponse aux menaces ou le cloud approprié (Amériques/Europe).

ESA ne demande pas le jeton d'enregistrement

Assurez-vous de valider les modifications lorsque la réponse aux menaces a été activée, sinon les modifications ne seront pas appliquées à la section Réponse aux menaces dans l'ESA.

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

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

Si vous utilisez le cloud Europe (UE) pour l'ESA, générez le jeton à partir de :

<https://admin.eu.sse.itd.cisco.com/>

Si vous utilisez le cloud Americas (NAM) pour ESA, générez le jeton à partir de :

<https://admin.sse.itd.cisco.com/>

De plus, n'oubliez pas que le jeton d'enregistrement a une date d'expiration (sélectionnez l'heure la plus pratique pour terminer l'intégration dans le temps).

Informations connexes

- Vous trouverez les informations contenues dans cet article dans la vidéo [Cisco Threat Response et ESA Integration](#).
- [Support et documentation techniques - Cisco Systems](#)