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

## Contenu



## Introduction

Ce document décrit le processus pour intégrer le 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

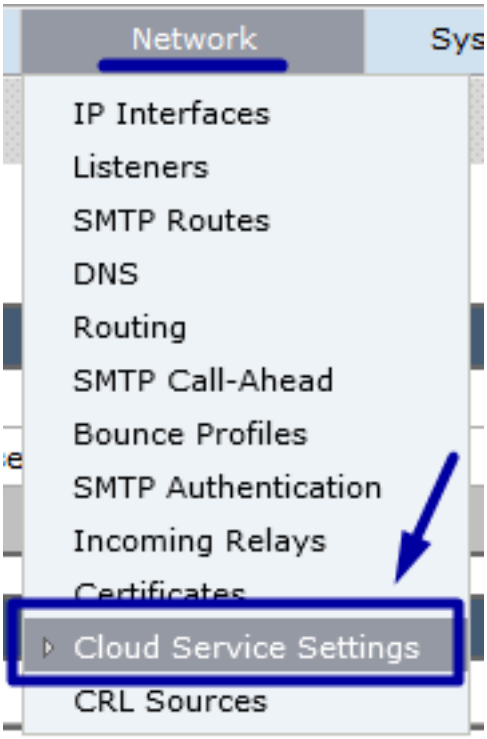
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence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

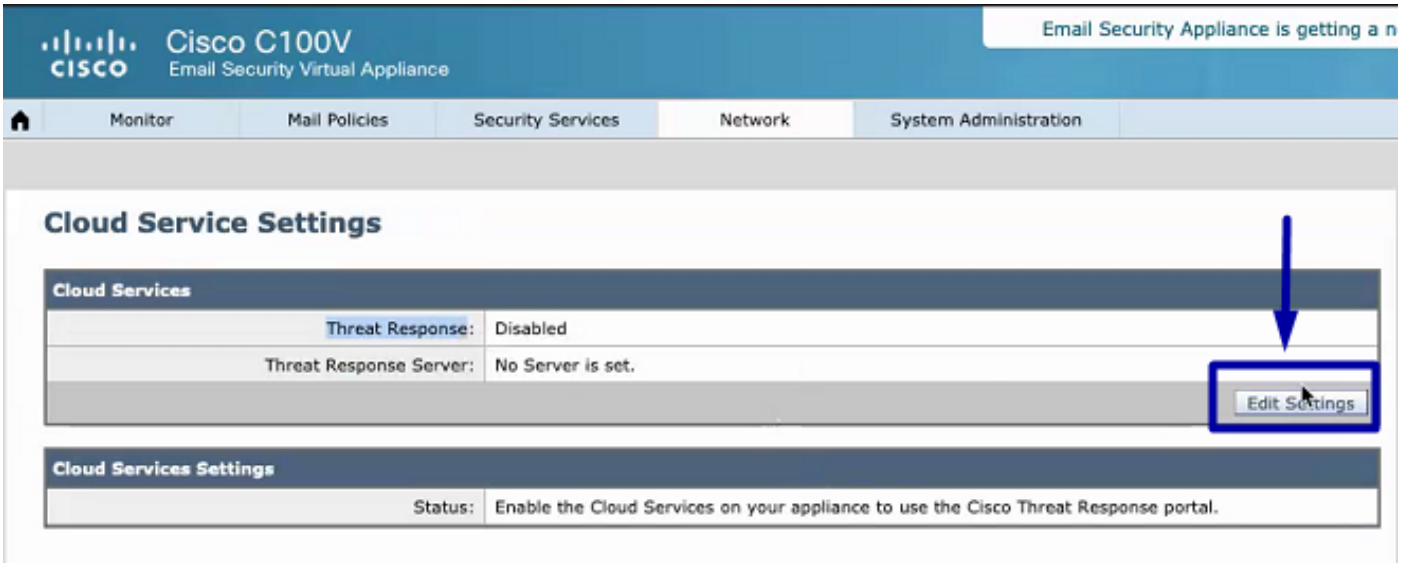
## Étape 1. Naviguez vers des configurations de réseau > de service en nuage

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.



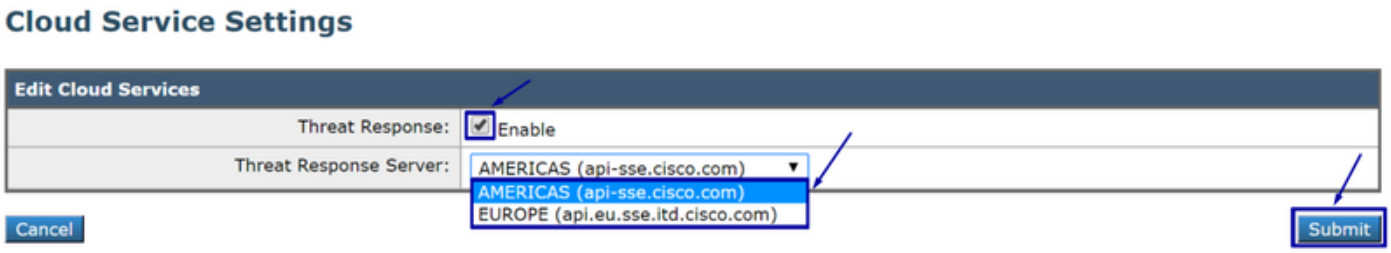

## Étape 2. Cliquez sur éditent en fonction des configurations

Jusqu'ici la caractéristique de réponse de menace dans l'ESA est désactivée, afin d'activer la caractéristique, cliquent 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 :

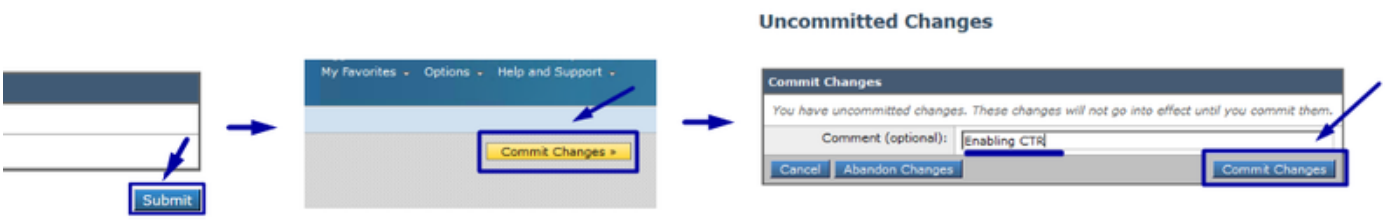


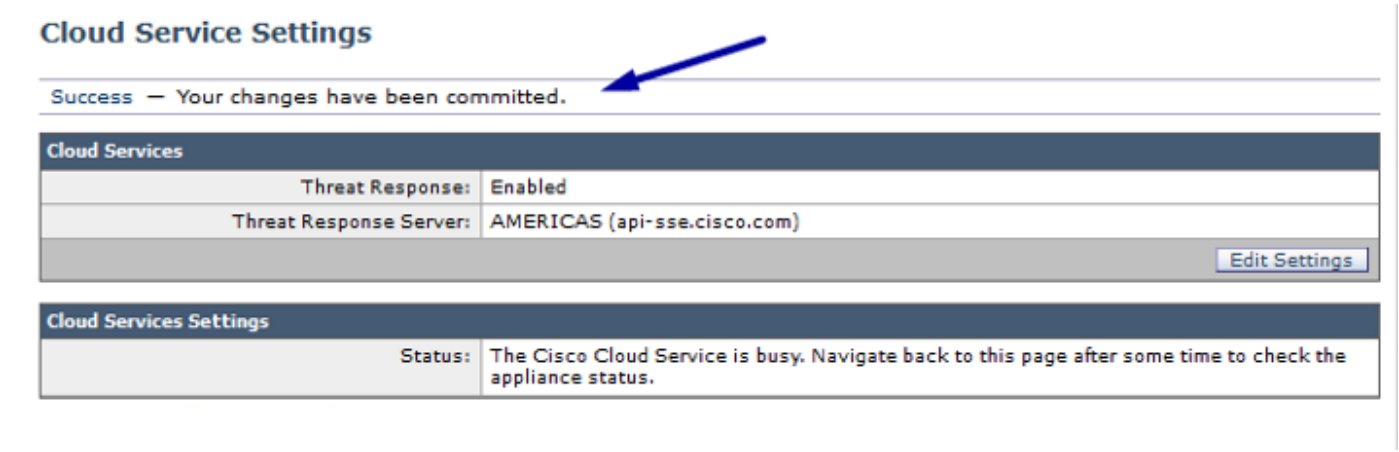

> Remarque: La sélection par défaut pour l'URL de serveur de réponse de menace est l'AMÉRIQUES (api-sse.cisco.com). Pour des entreprises de l'EUROPE, cliquez sur le menu déroulant et choisissez l'EUROPE (api.eu.sse.itd.cisco.com)

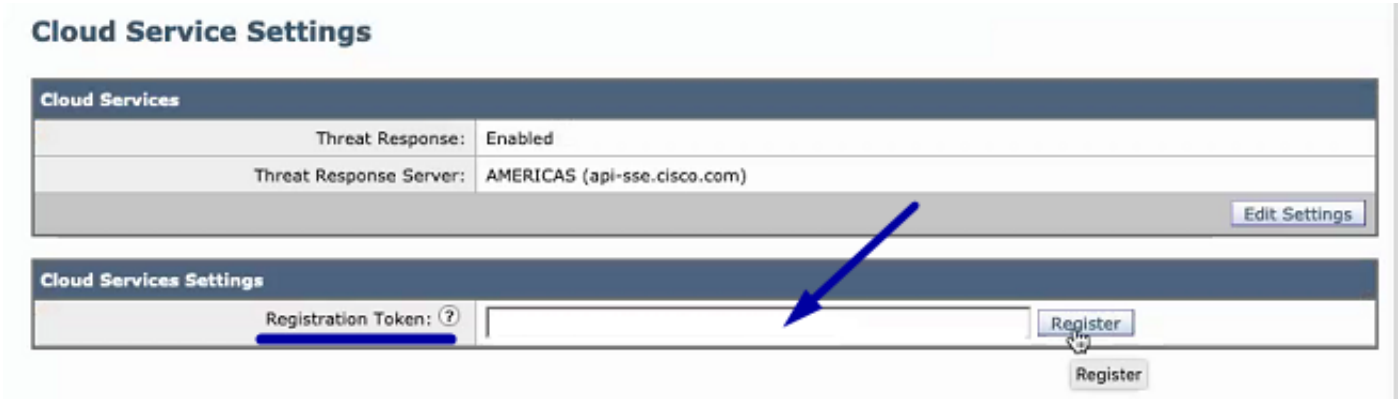
## Étape 4. Soumettez et commettez les modifications

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.

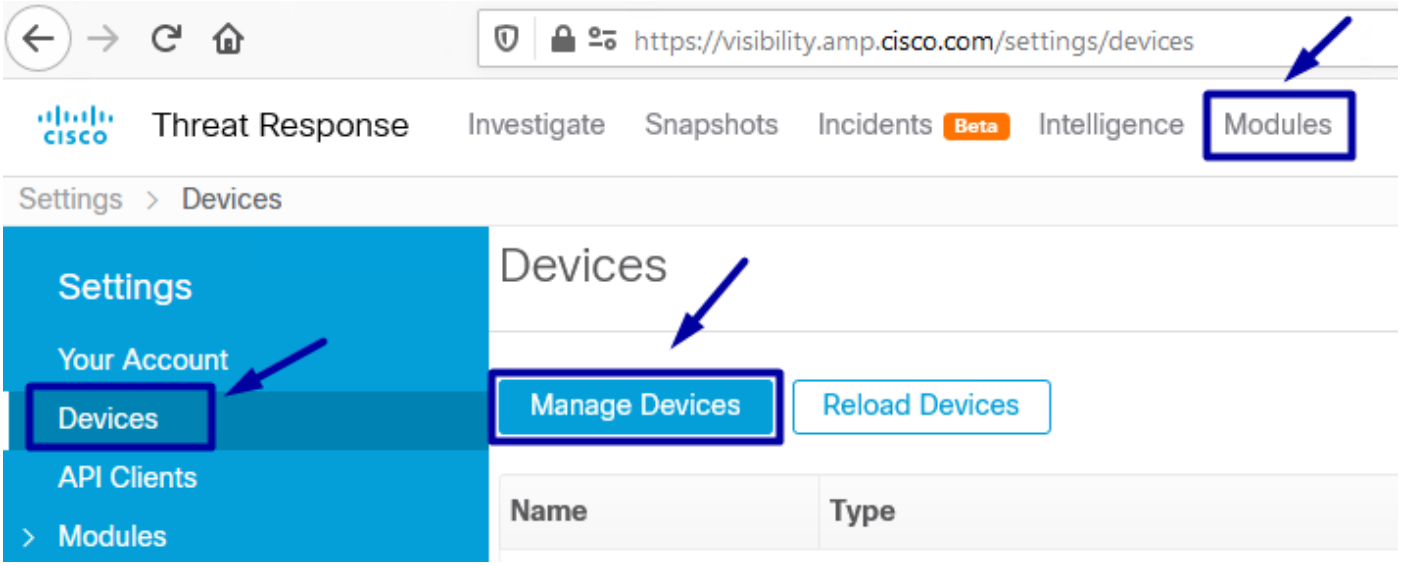




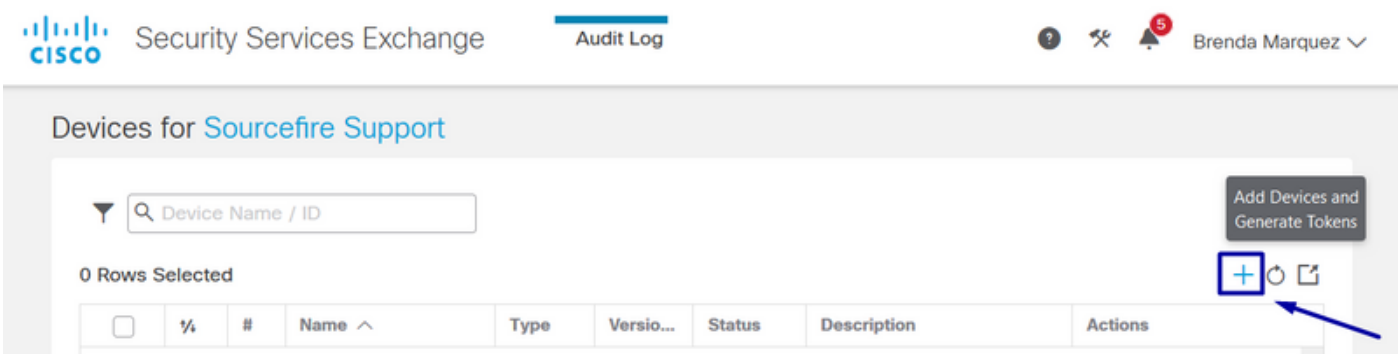




## Étape 5. Connectez-vous dans le CTR portail et générez le jeton d'enregistrement demandé dans l'ESA

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

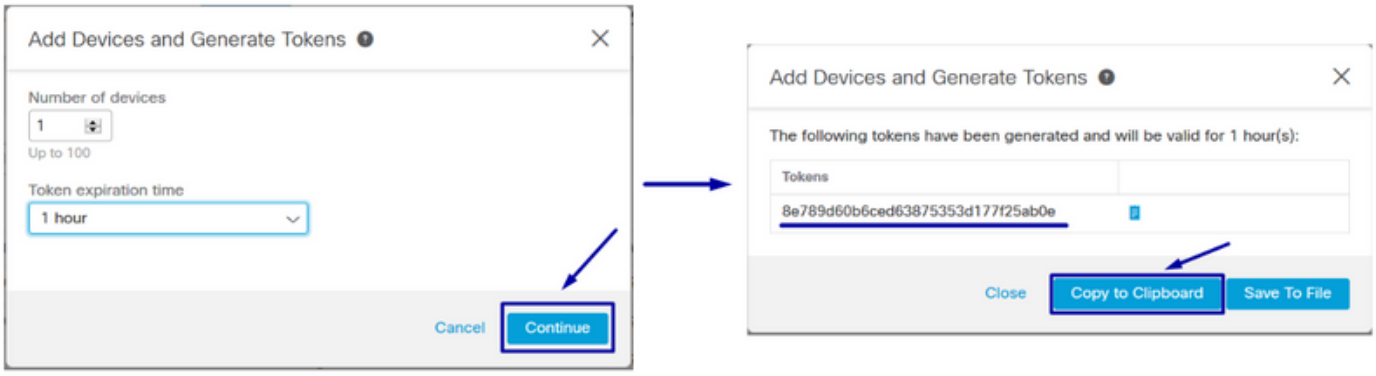



2. Gérez les périphériques que le lien vous réoriente à l'échange de Services de sécurité (SSE), une fois que là, cliquez sur en fonction l'icône ajoutent des périphériques et génèrent des jetons suivant les indications de l'image.




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.

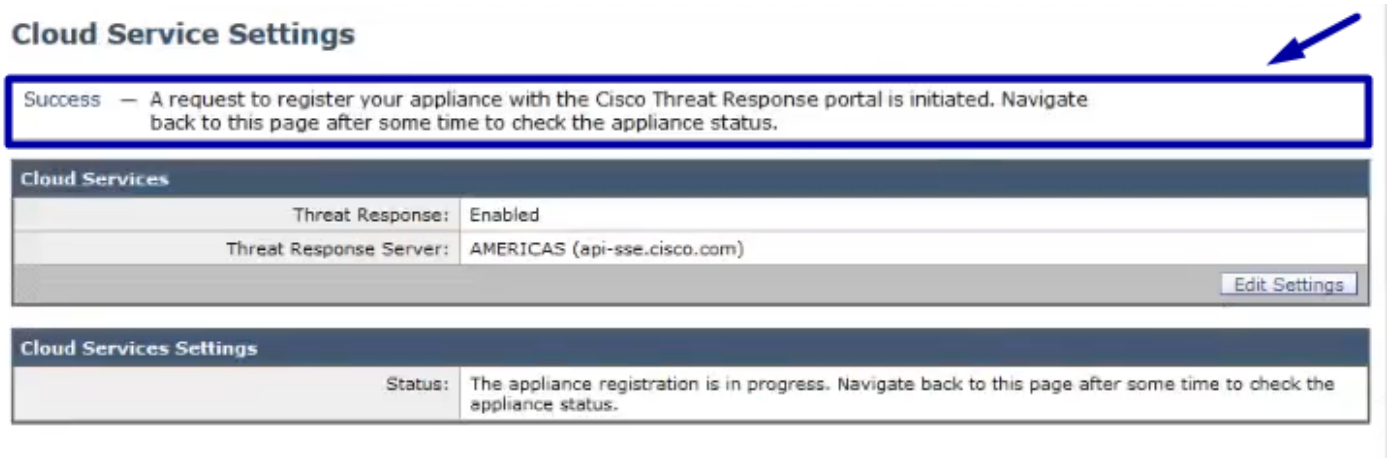
> **Conseil** : Vous pouvez sélectionner le nombre de périphériques pour ajouter (de 1 et jusqu'à de 100) et pour sélectionner également le temps d'expiration symbolique (1hr, 2hrs, 4hrs, 6hrs, 8hrs, 12hrs, 01 jours, 02 jours, 03 jours, 04 jours et 05 jours).




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

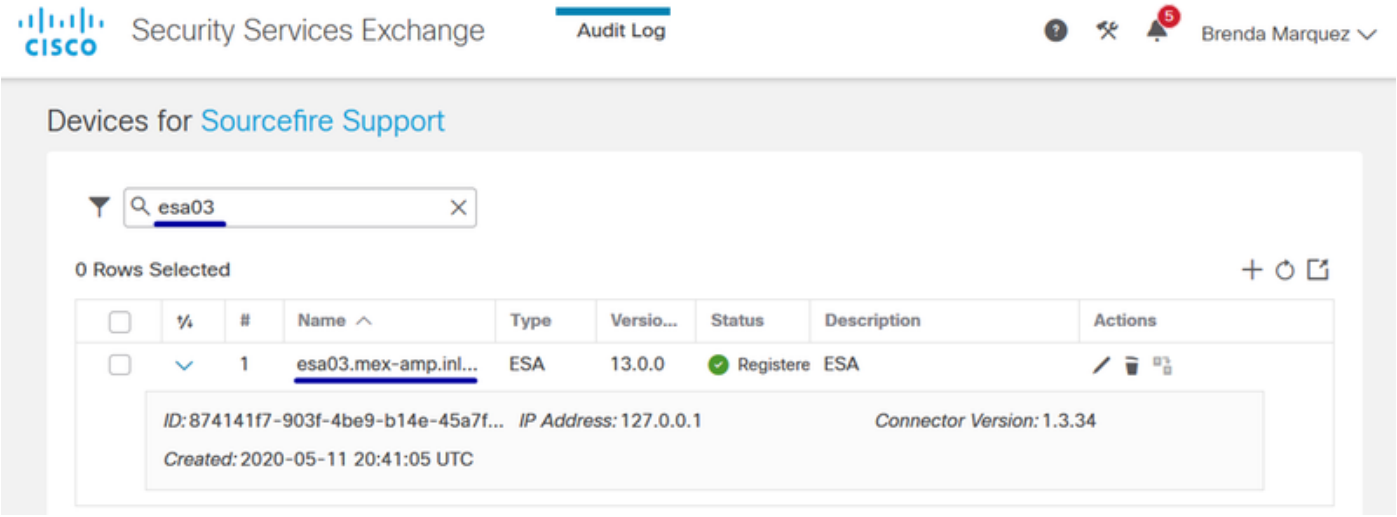
Une fois que le jeton d'enregistrement est généré, collez-le dans la section de configurations de services en nuage dans l'ESA, comme image ci-dessous.

> 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.



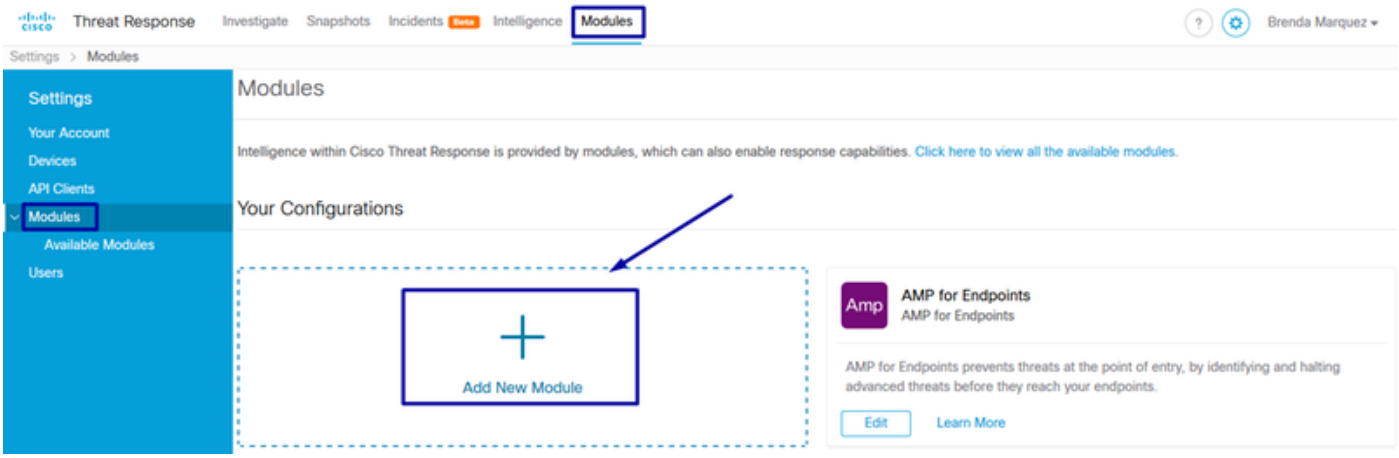

## Étape 7. Vérifiez que votre périphérique ESA est dans le portail SSE

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.



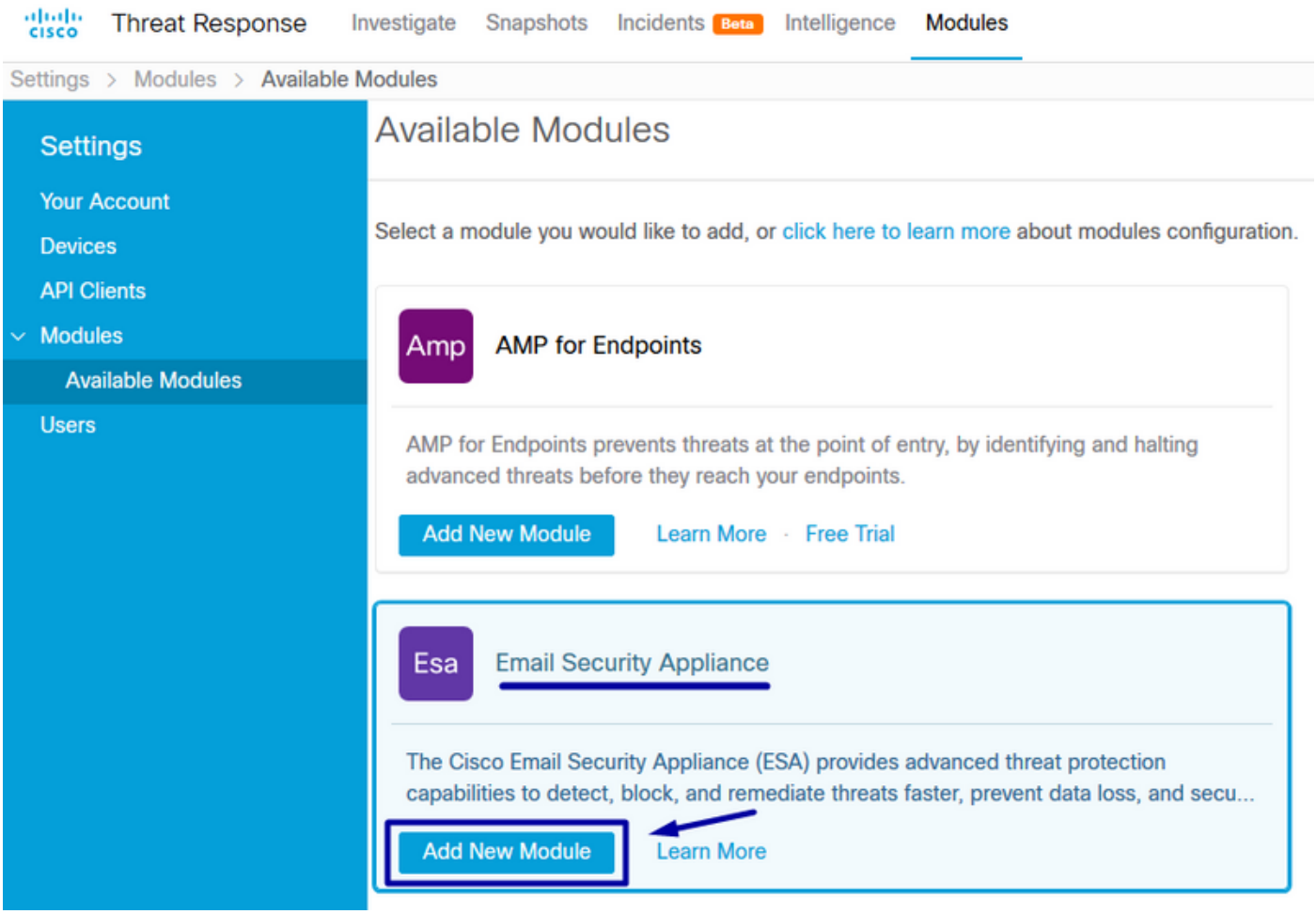

## Étape 8. Naviguez vers le CTR portail et ajoutez un nouveau module ESA

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

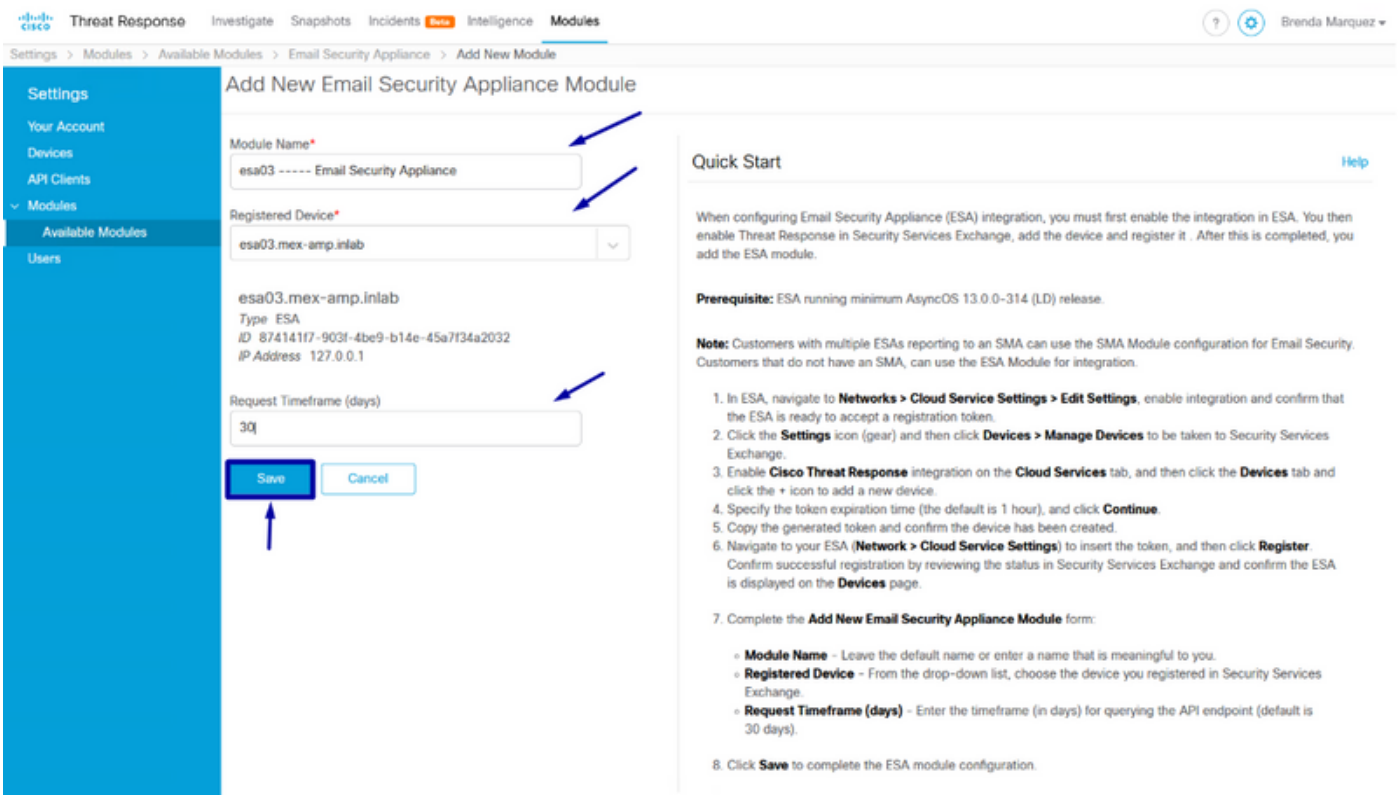



2. Choisissez le type de module, dans ce cas, le module est un module d'appareils de sécurité du

courrier électronique comme image ci-dessous.

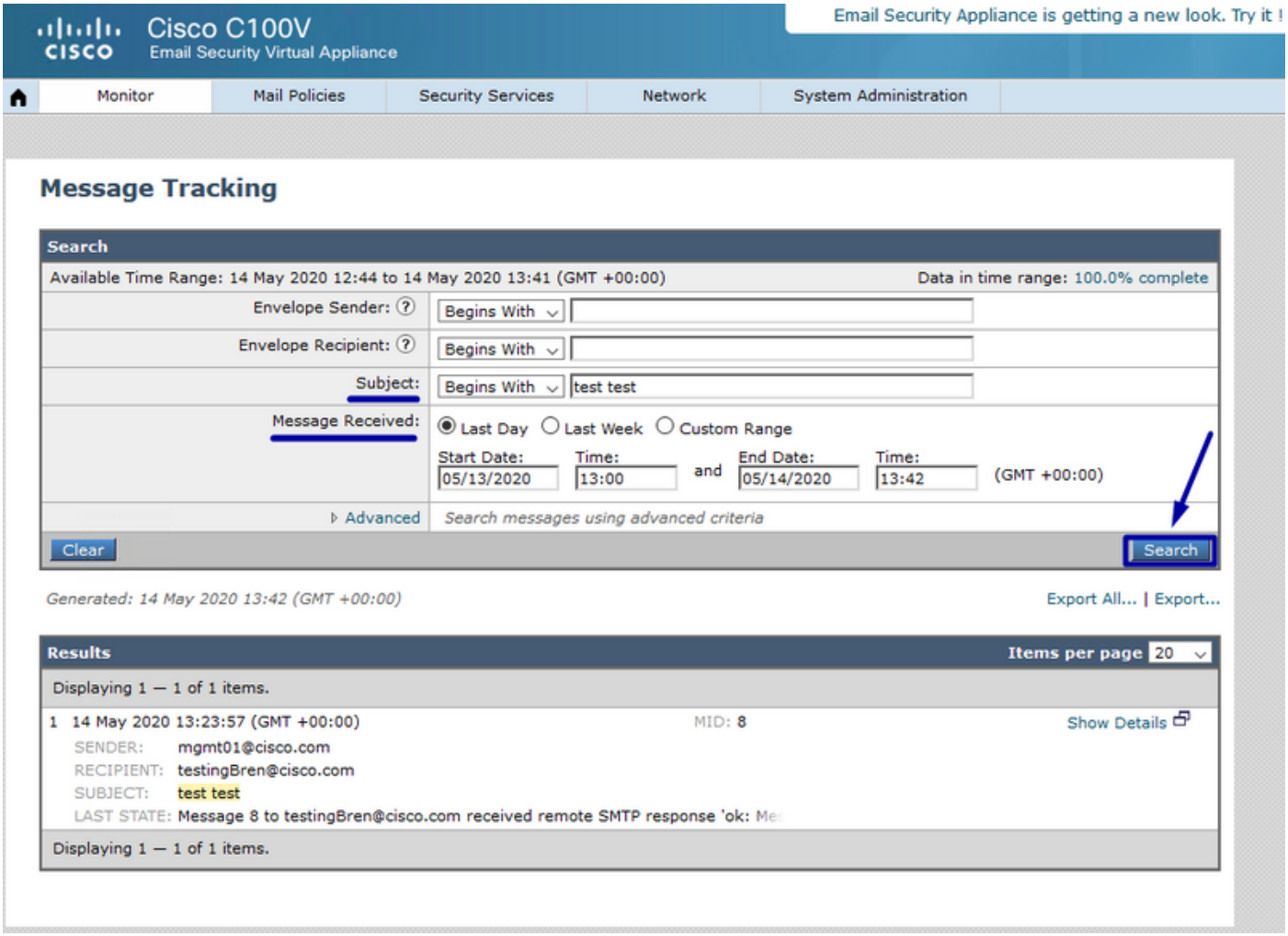



3. Entrez dans les champs : Nom du module, périphérique enregistré (sélectionnez celui précédemment enregistré) et délai de demande (jours), et sauvegarde, suivant les indications de l'image.

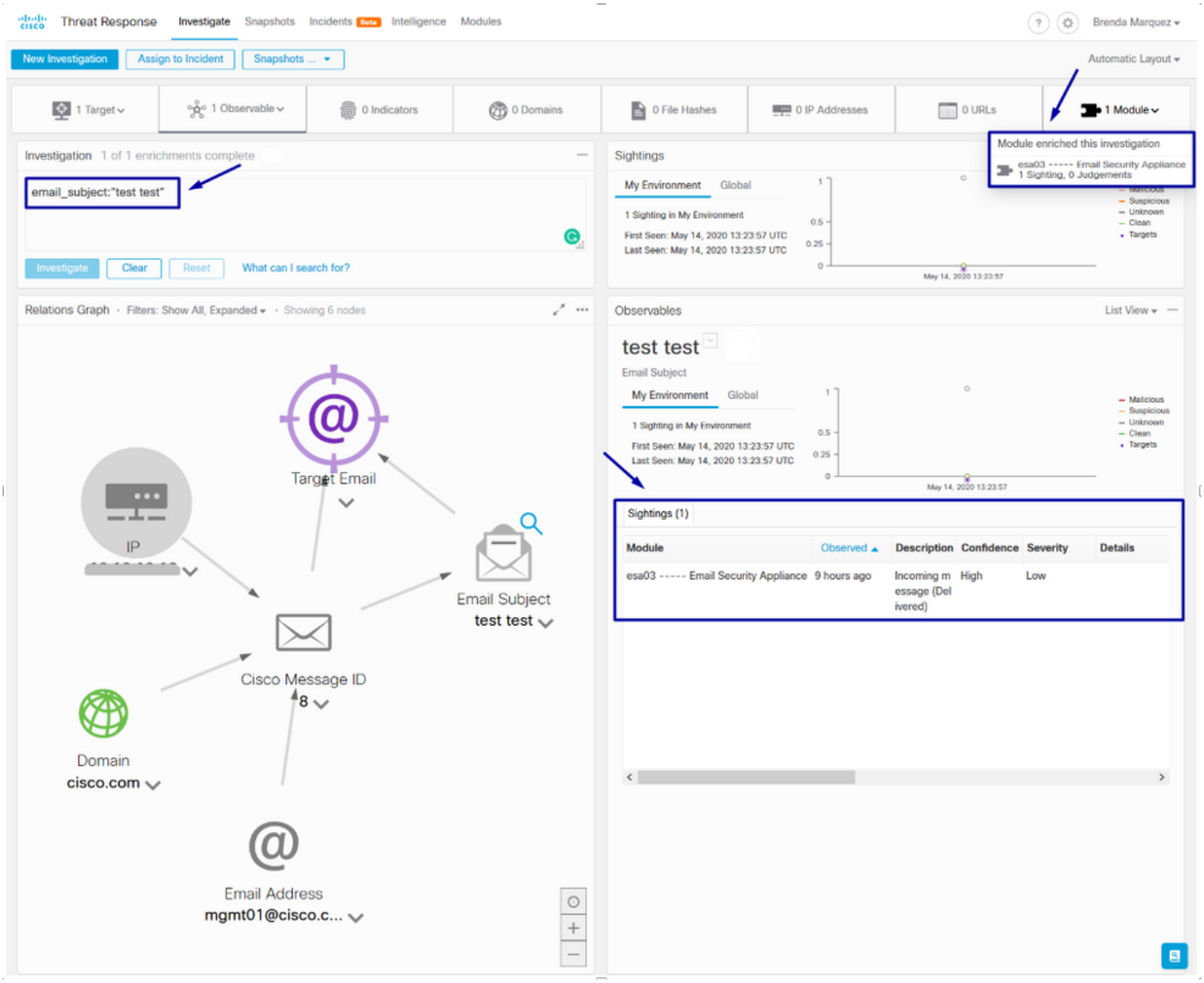


# Vérifiez

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.




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.




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

| | |
|---|---|
| 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" |

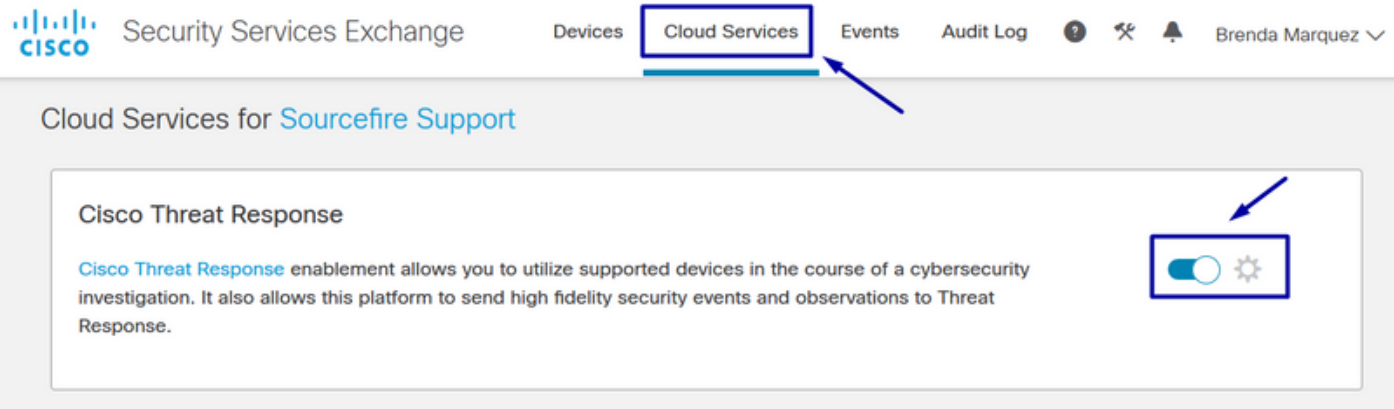
| | |
|---|---|
| Email subject | email_subject:"Invoice Due" |
| Cisco Message ID (MID) | cisco_mid:"12345" |
| SHA256 filehash | sha256:"sha256filehash" |
| Email attachment file name | file_name:"invoice.pdf" |

# 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 naviguent 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

Veuillez 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

Veuillez 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