Intégration Cisco Threat Response (CTR) et ESA

Contenu

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

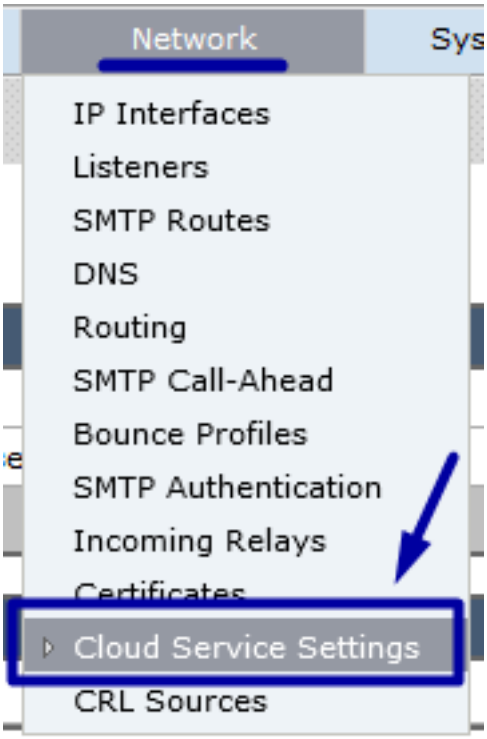
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

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 :

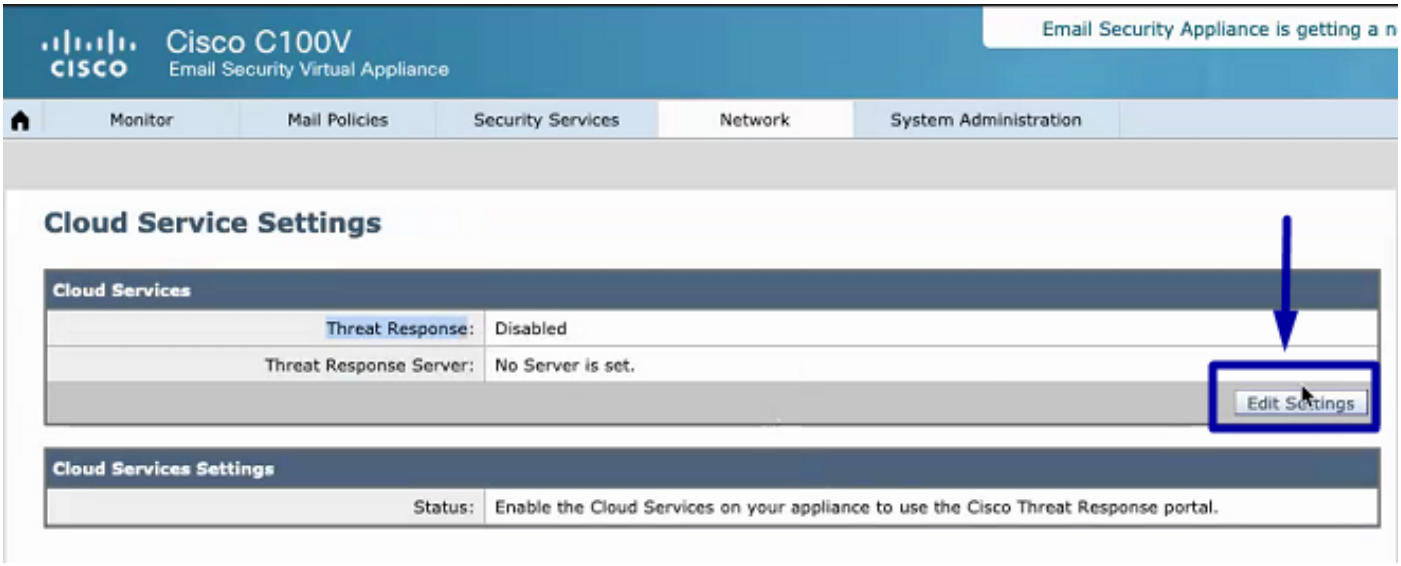
Étape 1. Naviguez jusqu'à Network > Cloud Service Settings

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.



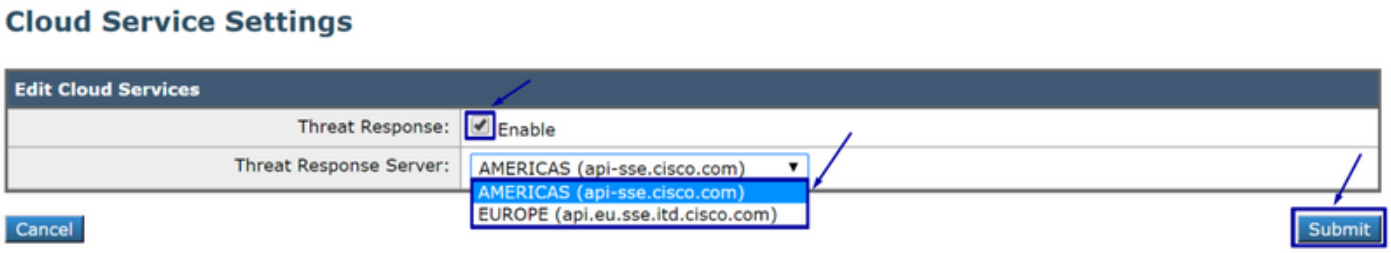
Étape 2. Cliquez sur Modifier les paramètres

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 :

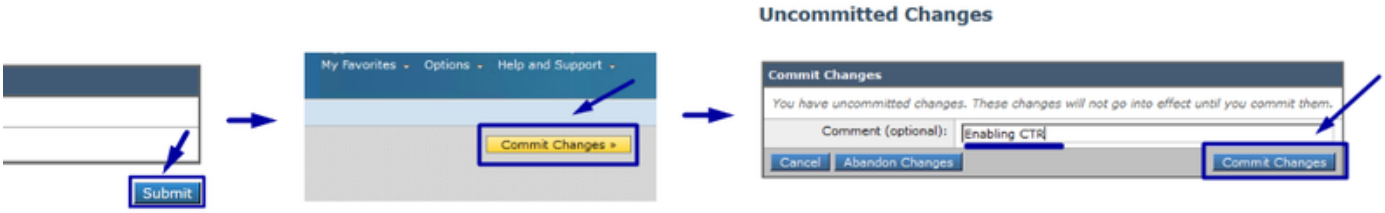


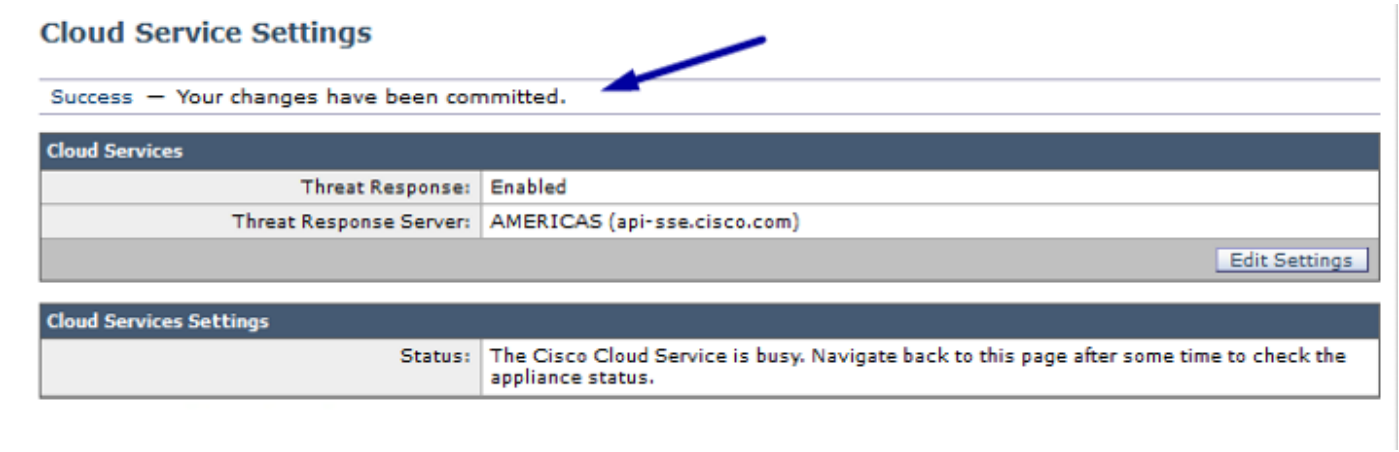
Note: La sélection par défaut pour l'URL du serveur de réponse aux menaces est AMERICAS (api-sse.cisco.com). Pour les entreprises EUROPE, cliquez sur le menu déroulant et choisissez EUROPE (api.eu.sse.itd.cisco.com)

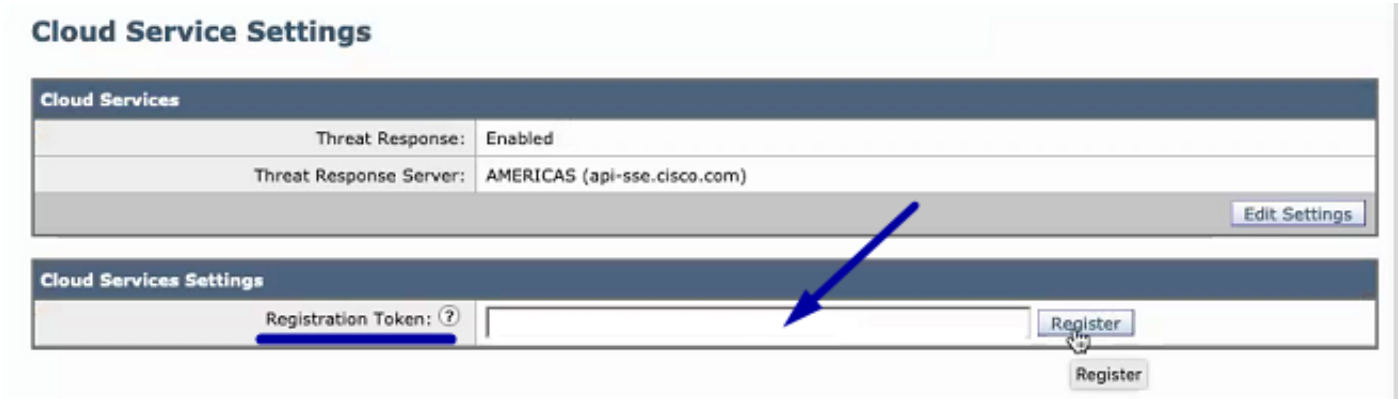
Étape 4. Soumettre et valider les modifications

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.

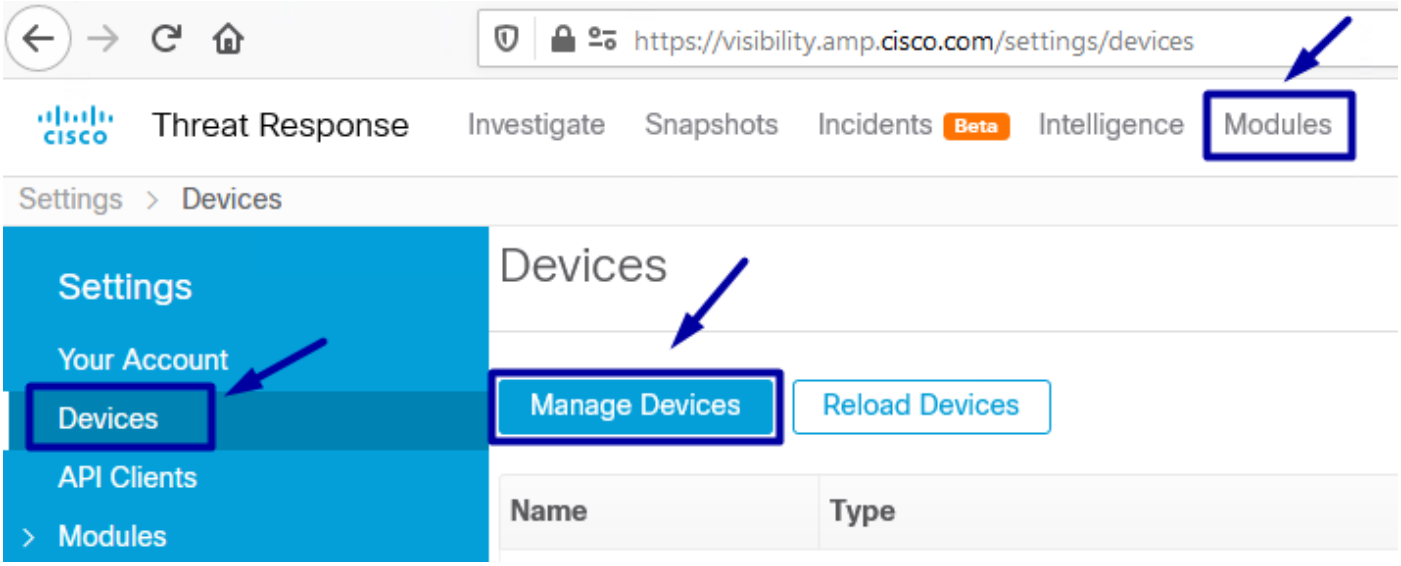




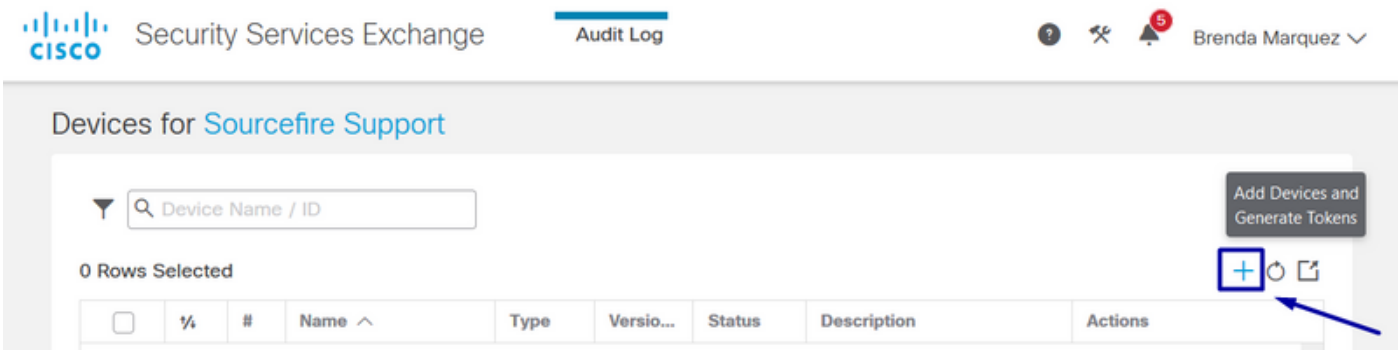


Étape 5. Connectez-vous au portail CTR et générez le jeton d'enregistrement demandé dans l'ESA

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

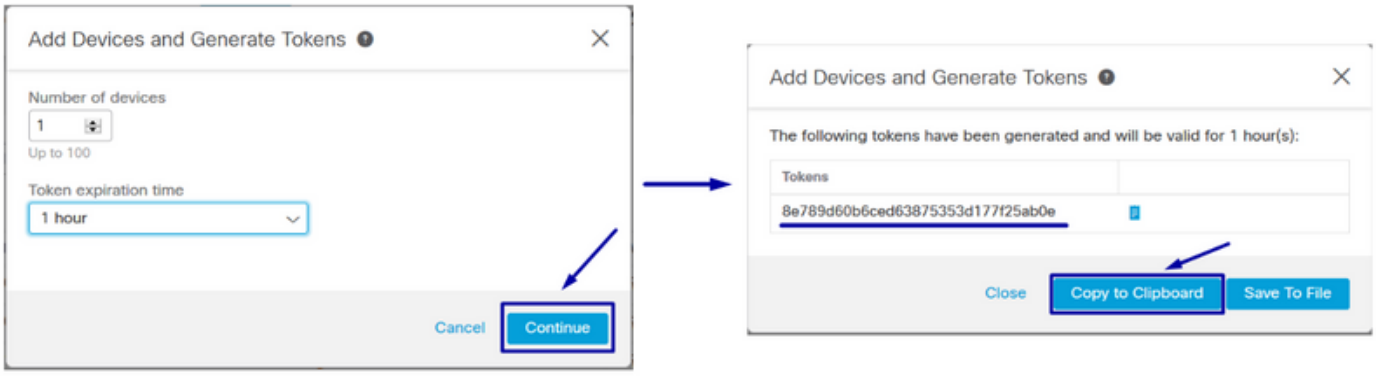


2.- Le lien Manage Devices (Gérer les périphériques) vous redirige vers Security Services Exchange (SSE). Une fois sur ce lien, cliquez sur l'icône Add Devices and Generate Tokens (Ajouter des périphériques et générer des jetons), comme illustré dans l'image.



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.

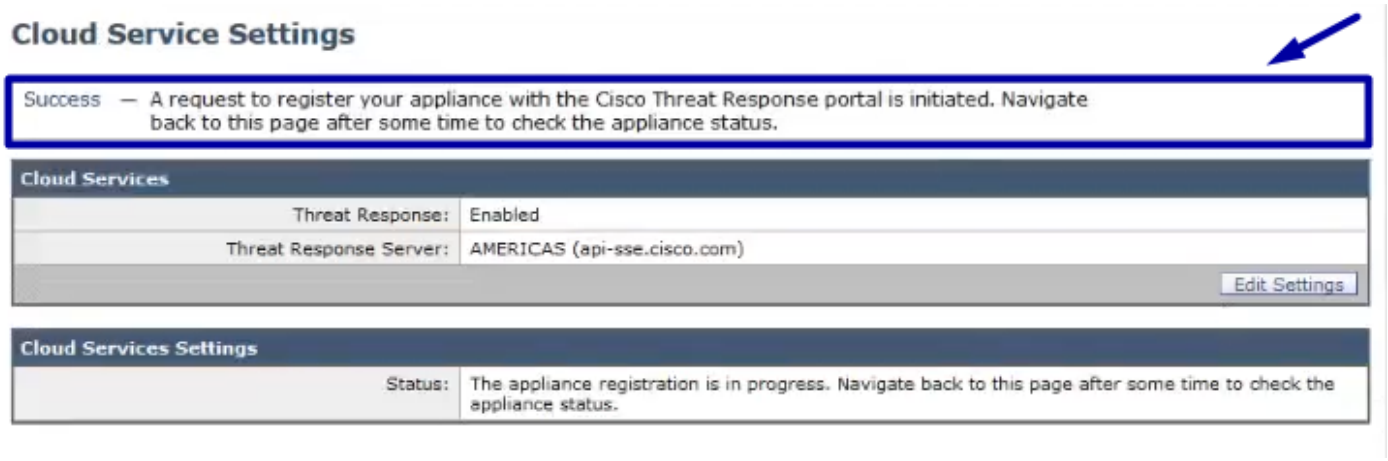
> **Astuce** : Vous pouvez sélectionner le nombre de périphériques à ajouter (de 1 et jusqu'à 100) et également sélectionner le délai d'expiration du jeton (1h, 2h, 4h, 6h, 8h, 12h, 01 jours, 02 jours, 03 jours, 04 jours et 05 jours).



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

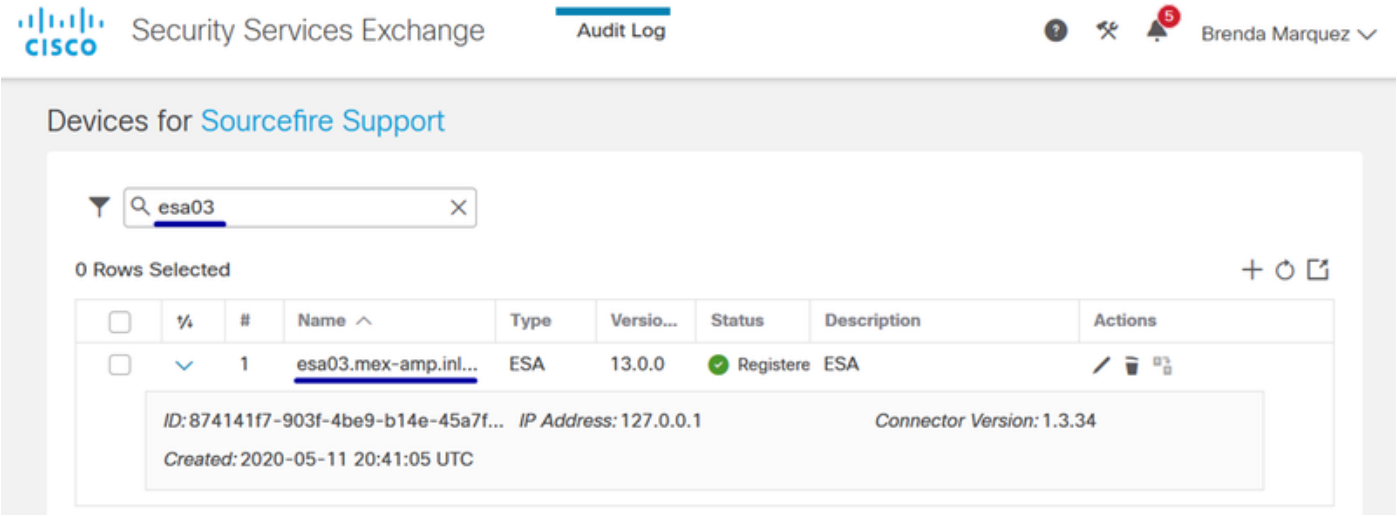
Une fois le jeton d'enregistrement généré, collez-le dans la section Cloud Services Settings de l'ESA, comme l'image ci-dessous.

> **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.



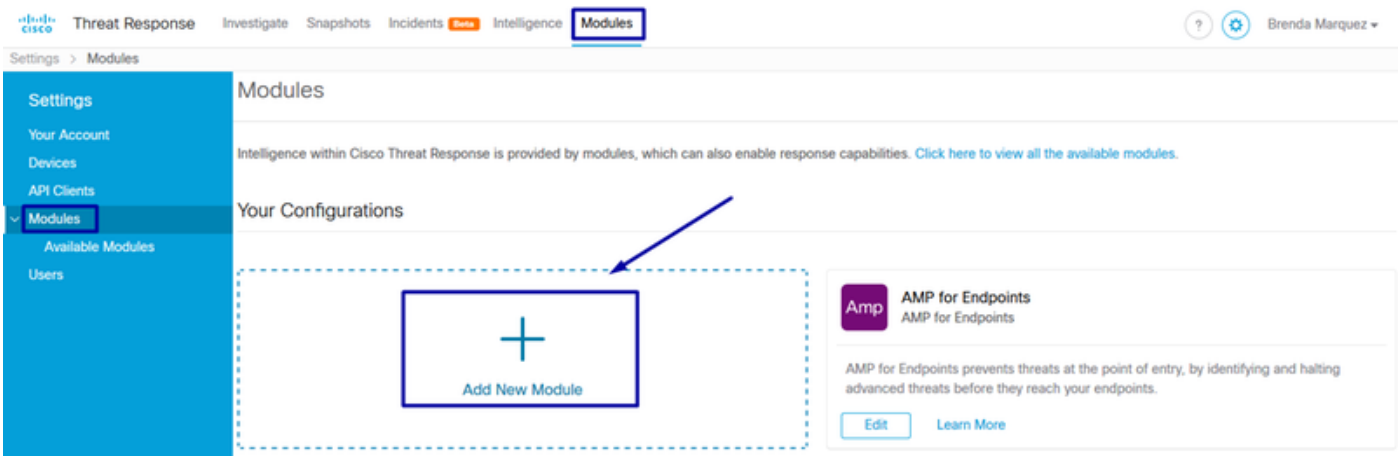
Étape 7. Vérifiez que votre périphérique ESA se trouve dans le portail SSE

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.

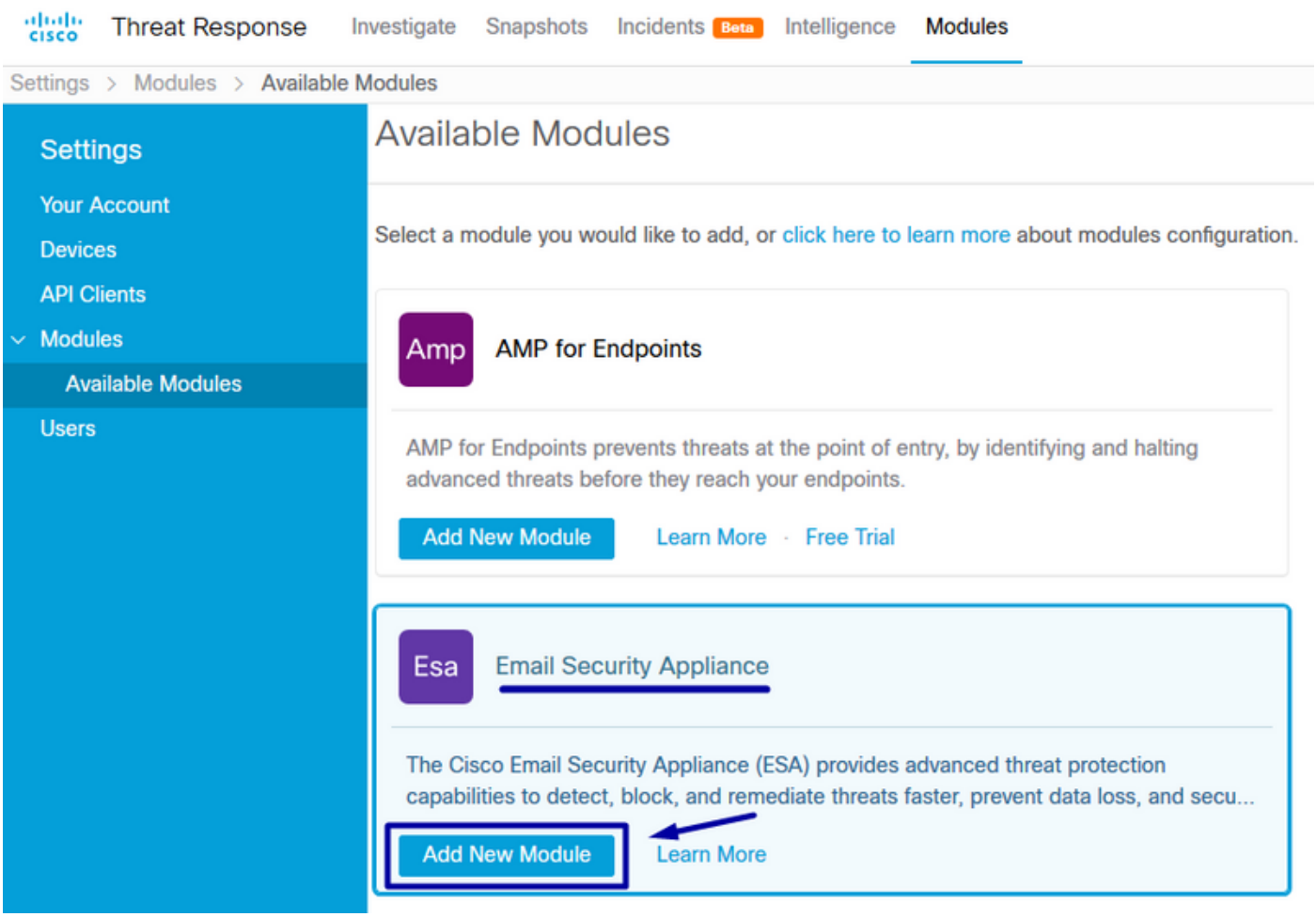


Étape 8. Accédez au portail CTR et ajoutez un nouveau module ESA

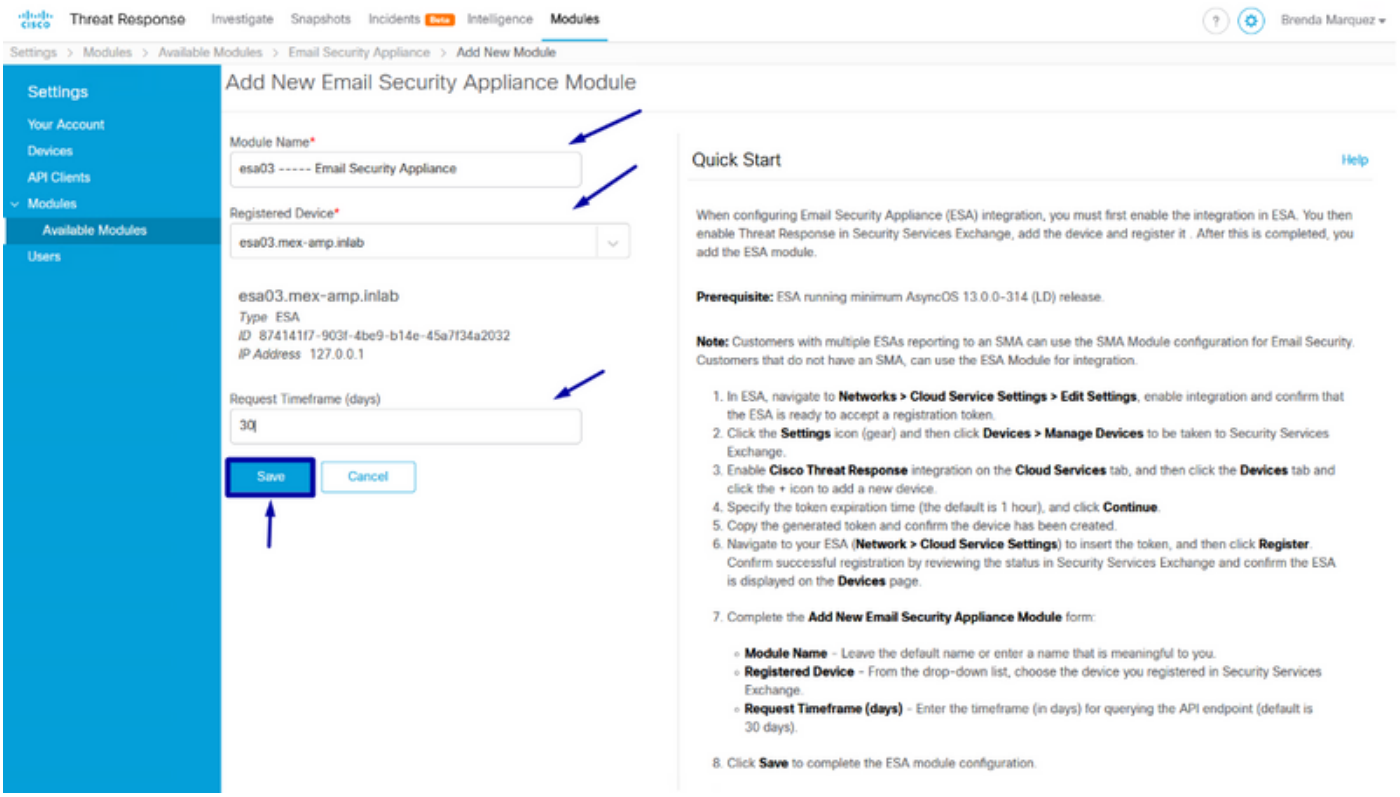
1.- Une fois que vous êtes dans le portail CTR, accédez à Modules > Add New Module, comme illustré dans l'image.



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.

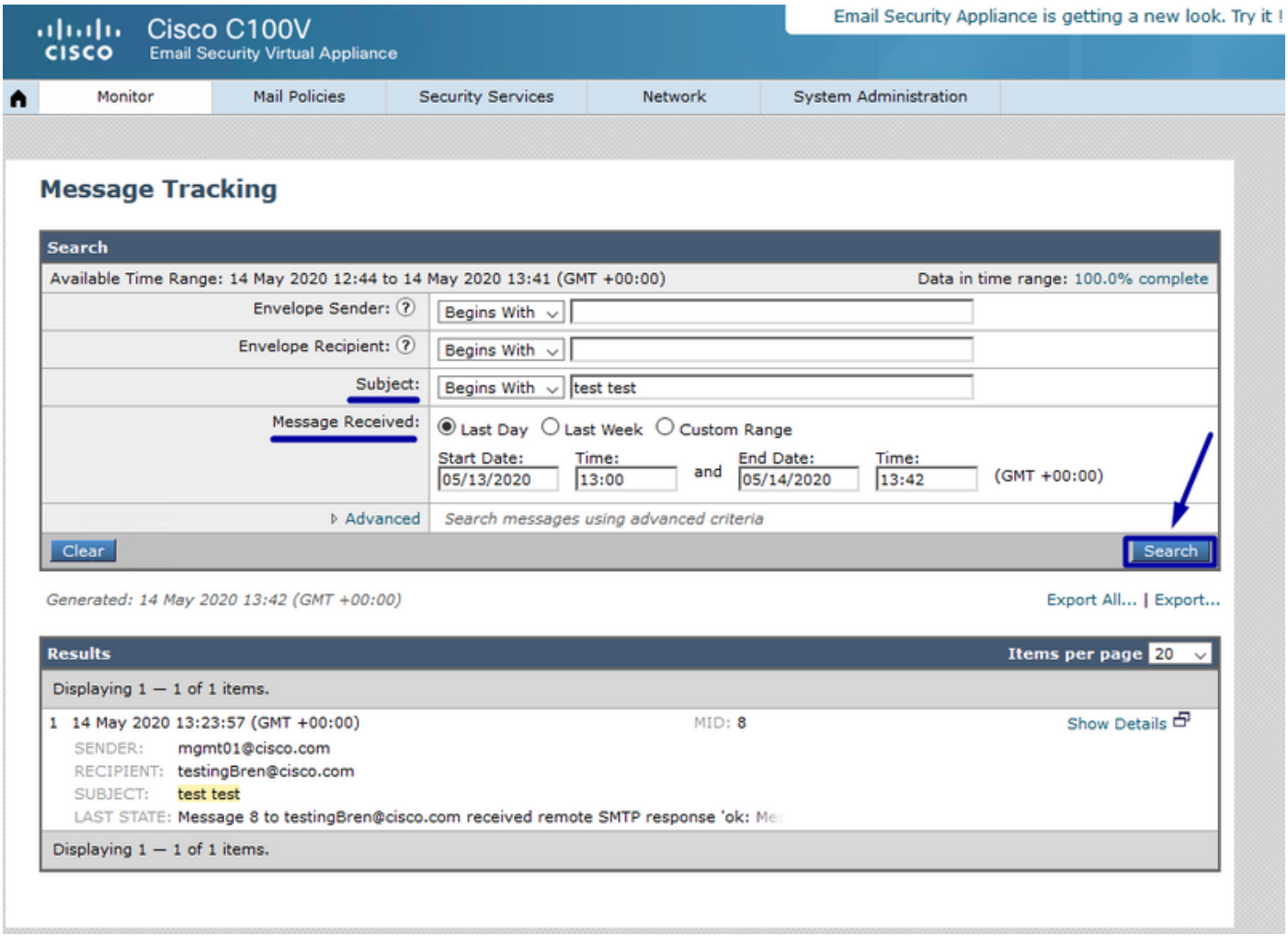


3.- Entrez les champs suivants : Nom du module, Périphérique enregistré (sélectionnez celui précédemment enregistré), Délai de demande (jours) et Enregistrer, comme l'illustre l'image.

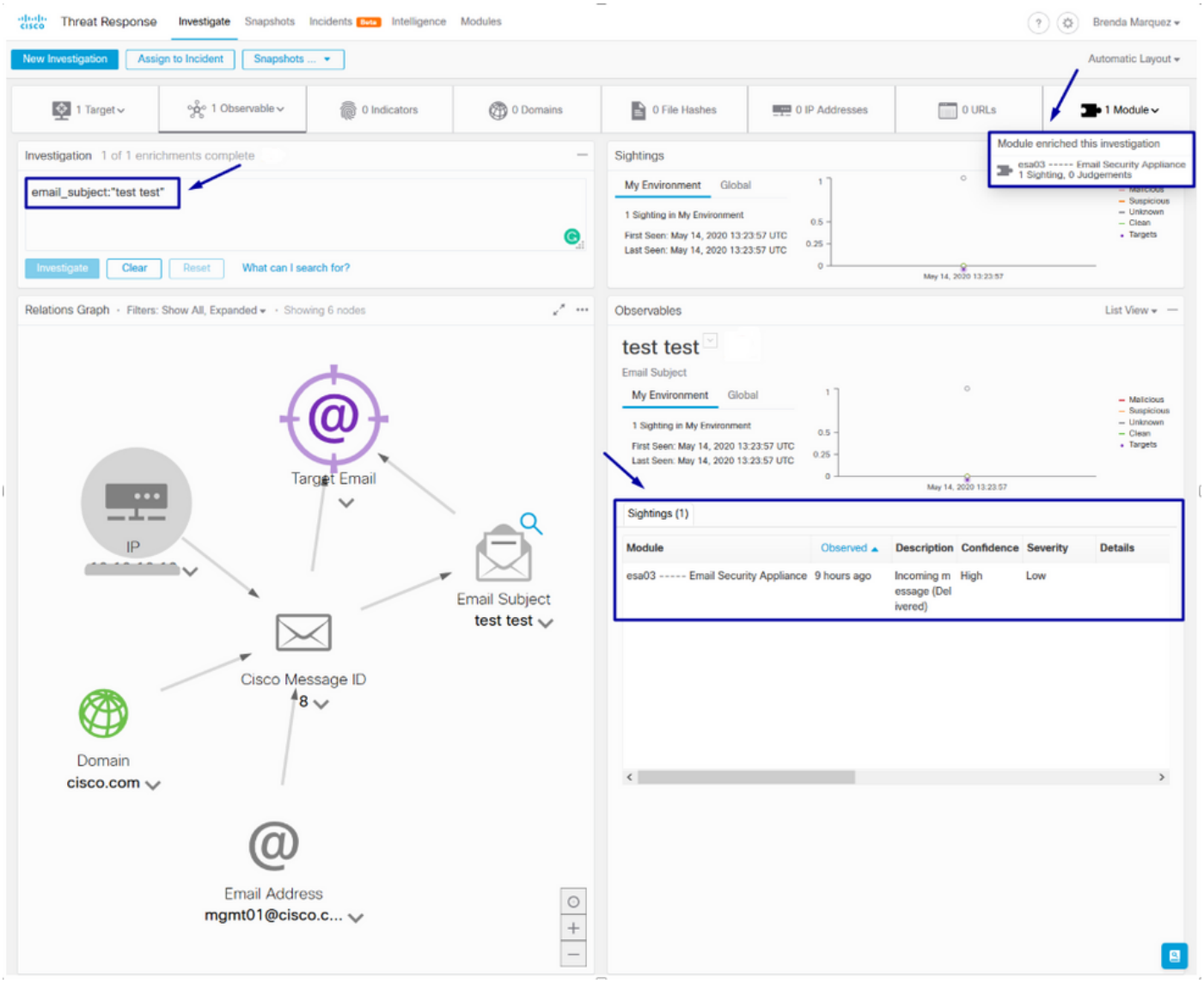


Vérification

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.



Àprésent, 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.



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

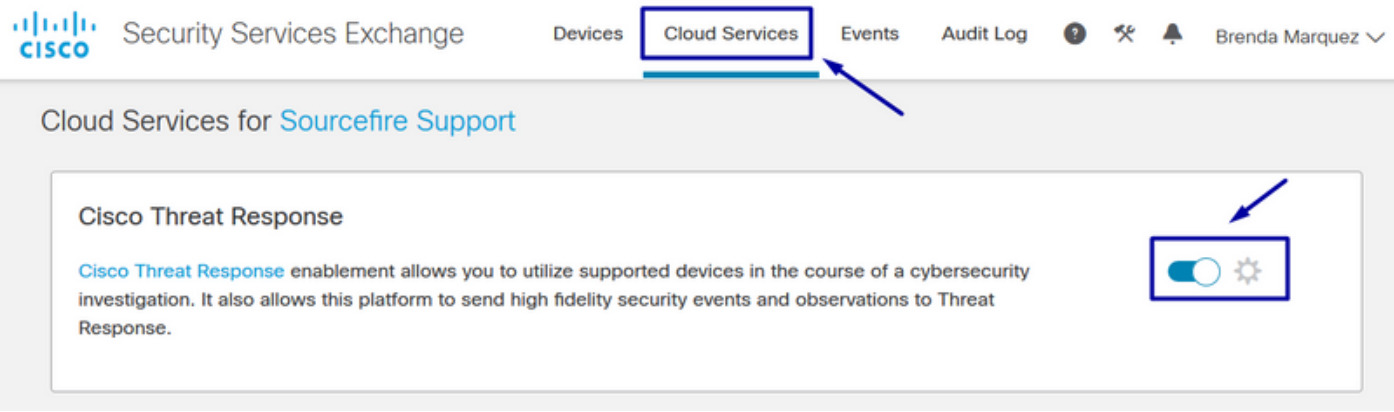
IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file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

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

Veuillez 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