Configurer l'intégration SMA avec SecureX

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Configuration](#)
[Intégration SMA](#)
[Web SMA](#)
[E-mail SMA](#)
[Vérification](#)
[Dépannage](#)
[Module SMA de réponse aux menaces SecureX SMA/tile SecureX indiquant l'erreur « Une erreur inattendue s'est produite sur le module SMA »](#)
[Vidéo](#)
[Informations connexes](#)

Introduction

Ce document décrit le processus de configuration, de vérification et de dépannage de l'intégration de Content Security Management Appliance (SMA) avec SecureX.

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir des connaissances sur ces sujets :

- Appliance de gestion de la sécurité (SMA)
- Dispositif de sécurité de la messagerie (ESA)
- Appareil de sécurité Web (WSA)
- Cisco Threat Response (CTR)
- Tableau de bord SecureX

Components Used

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

- SMA exécutant AsyncOS 13.6.2 (pour SMA- Module de messagerie)

- SMA exécutant AsyncOS 12.5 (pour SMA - Module Web)

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. If your network is live, make sure that you understand the potential impact of any command.

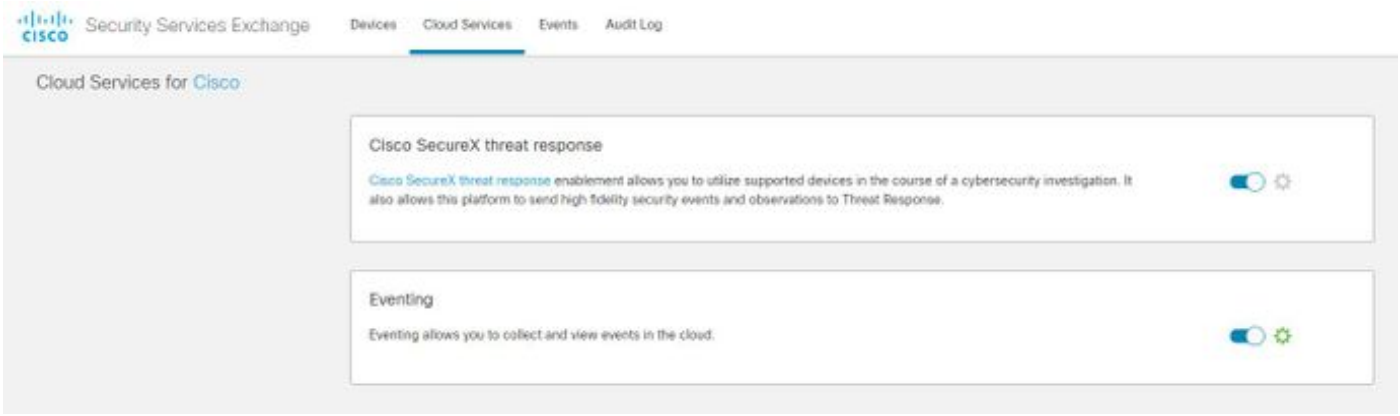
Configuration

Intégration SMA

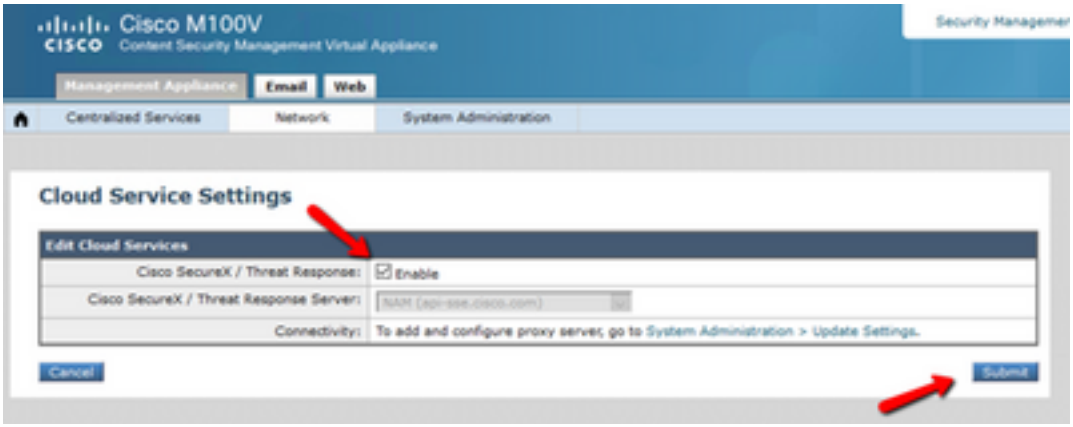
Étape 1. Dans SMA, accédez à **Network > Cloud Service Settings > Edit Settings**, activez l'intégration et vérifiez que SMA est prêt à accepter un jeton d'enregistrement.

Étape 2. Cliquez sur l'icône Paramètres (engrenage), puis cliquez sur **Périphériques > Gérer les périphériques** pour accéder à Security Services Exchange (SSE).

Assurez-vous que toutes les options sont activées sous **Cloud** Services.



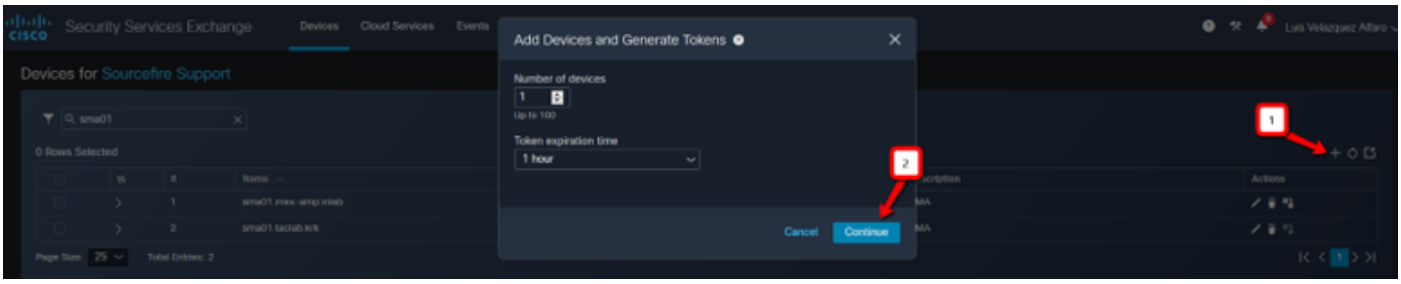
Étape 3. Activez l'intégration de Cisco Threat Response dans l'onglet Cloud Services, puis cliquez sur l'onglet Devices et cliquez sur l'icône + pour ajouter un nouveau périphérique (compte d'administrateur SMA requis).



Étape 4. Connectez-vous au portail SSE à partir de l'instance SecureX.

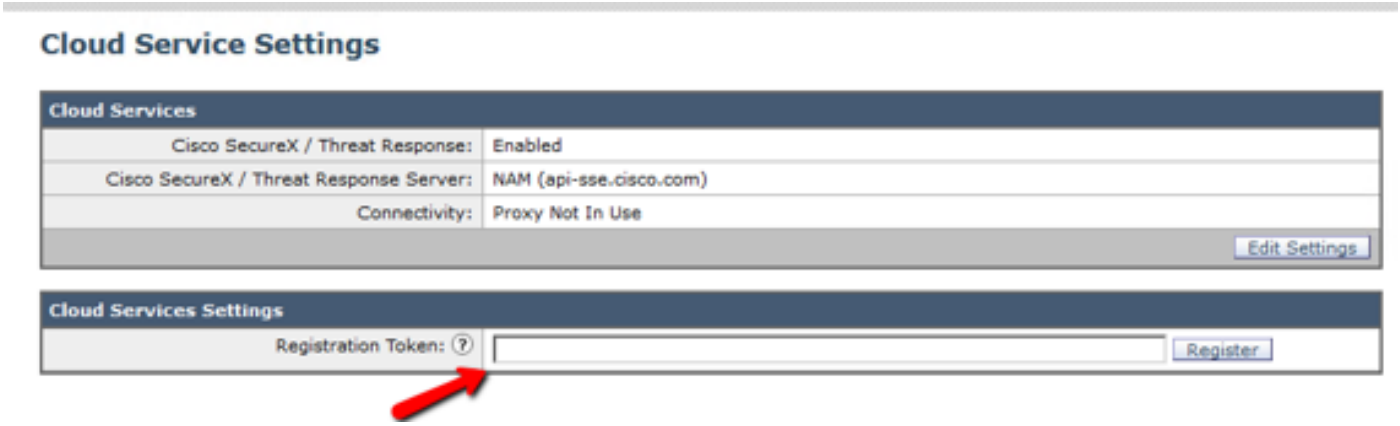
Étape 5. À partir du portail Secure X, accédez à **Intégrations > Périphériques > Gérer les périphériques.**

Étape 6. Créez un nouveau jeton sur le portail SSE et spécifiez le délai d'expiration du jeton (la valeur par défaut est 1 heure), puis cliquez sur **Continuer**.

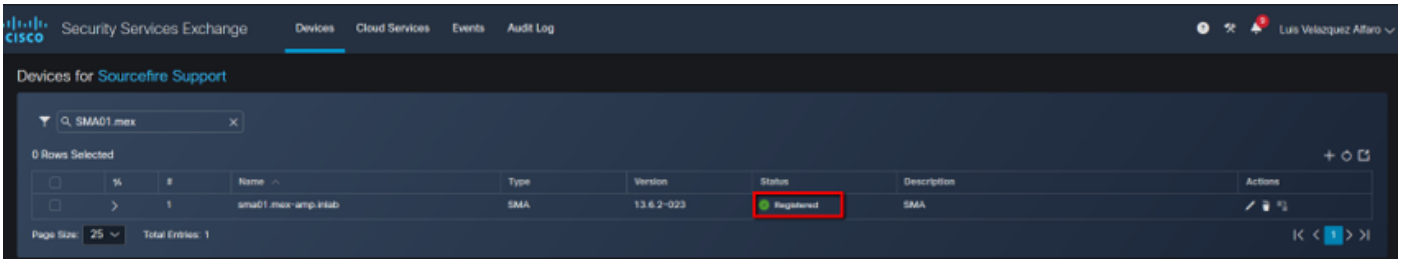


Étape 7. Copiez le jeton généré et confirmez que le périphérique a été créé.

Étape 8. Accédez à votre SMA **(Réseau > Paramètres du service cloud)** pour insérer le jeton, puis cliquez sur Enregistrer.



Pour confirmer l'enregistrement réussi, vérifiez l'état dans **Security Services Exchange** et vérifiez que le SMA est affiché sur la page Devices.



Web SMA

Étape 1. Complétez le formulaire Ajouter un nouveau module Web SMA :

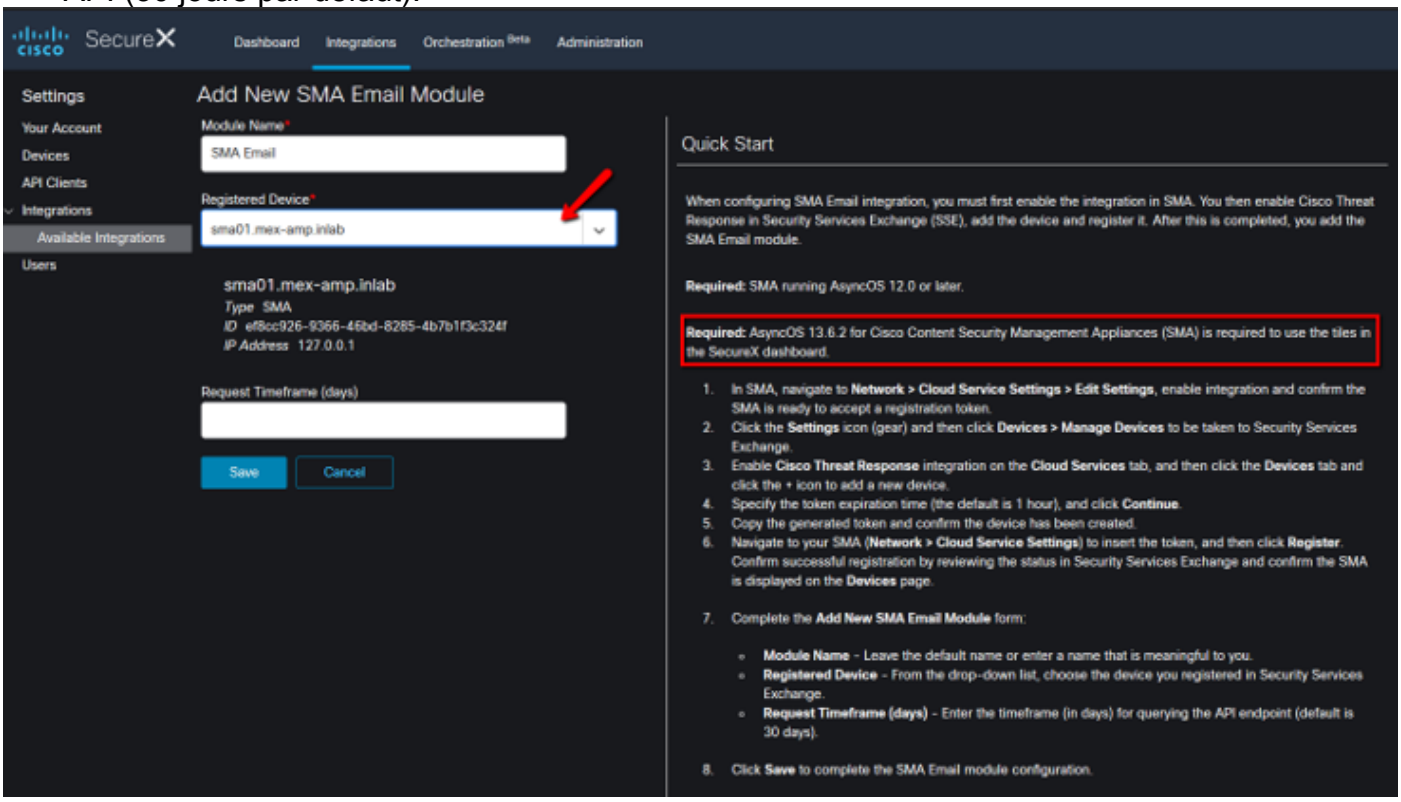
- Module Name (Nom du module) : laissez le nom par défaut ou entrez un nom qui vous intéresse.
- Périphérique enregistré : dans la liste déroulante, sélectionnez le périphérique que vous avez enregistré dans Security Services Exchange.
- Request Timeframe (days) : saisissez le délai (en jours) de la requête de point de terminaison API (30 jours par défaut).

Étape 2. Cliquez sur Enregistrer pour terminer la configuration du module Web SMA.

E-mail SMA

Étape 1. Remplissez le formulaire Ajouter un nouveau module de messagerie SMA.

- Module Name (Nom du module) : laissez le nom par défaut ou entrez un nom qui vous intéresse.
- Périphérique enregistré : dans la liste déroulante, sélectionnez le périphérique que vous avez enregistré dans Security Services Exchange.
- Request Timeframe (days) : saisissez le délai (en jours) de la requête de point de terminaison API (30 jours par défaut).



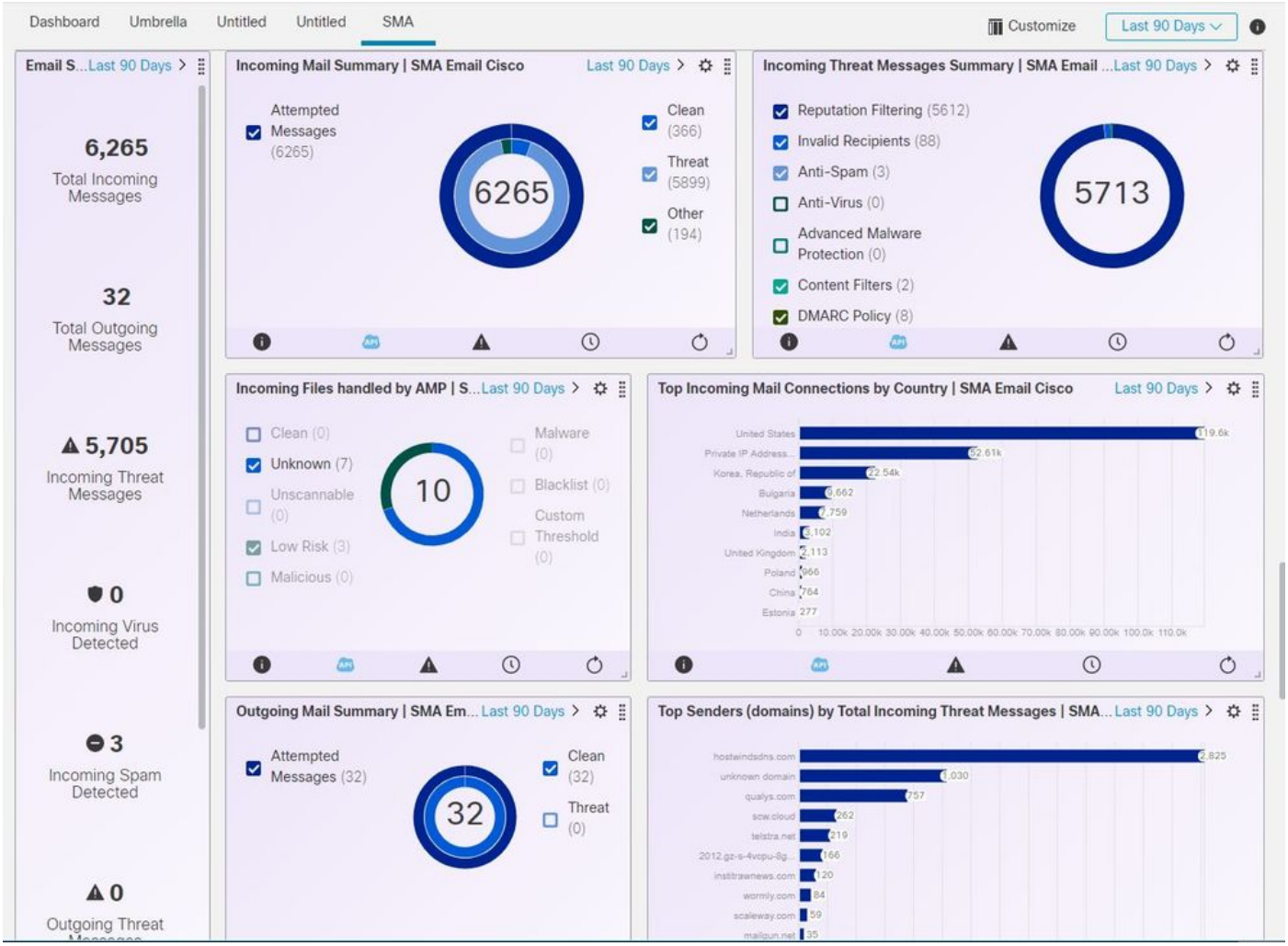
Si le nom du périphérique SMA ne figure pas dans le menu déroulant, tapez le nom dans le champ déroulant pour effectuer une recherche.

Étape 2. Cliquez sur **Enregistrer** pour terminer la configuration du module de messagerie SMA

Vérification

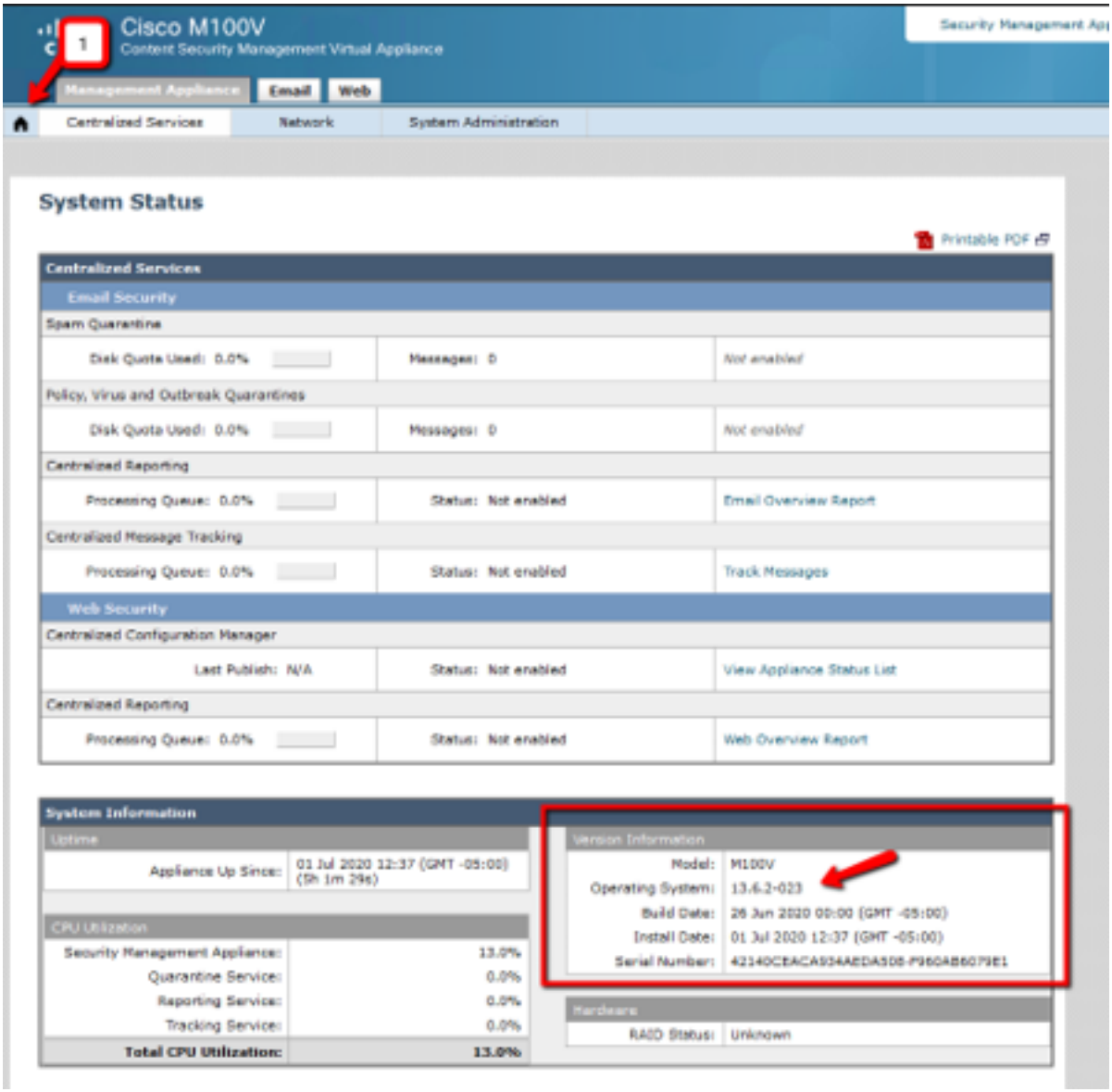
Étape 1. Ajoutez un nouveau tableau de bord et ajoutez les mosaïques pour afficher les informations qui vous intéressent à partir de votre module SMA

Vous pouvez voir les informations de votre périphérique reflétées dans cette section.



Étape 2. Vérifier la version SMA

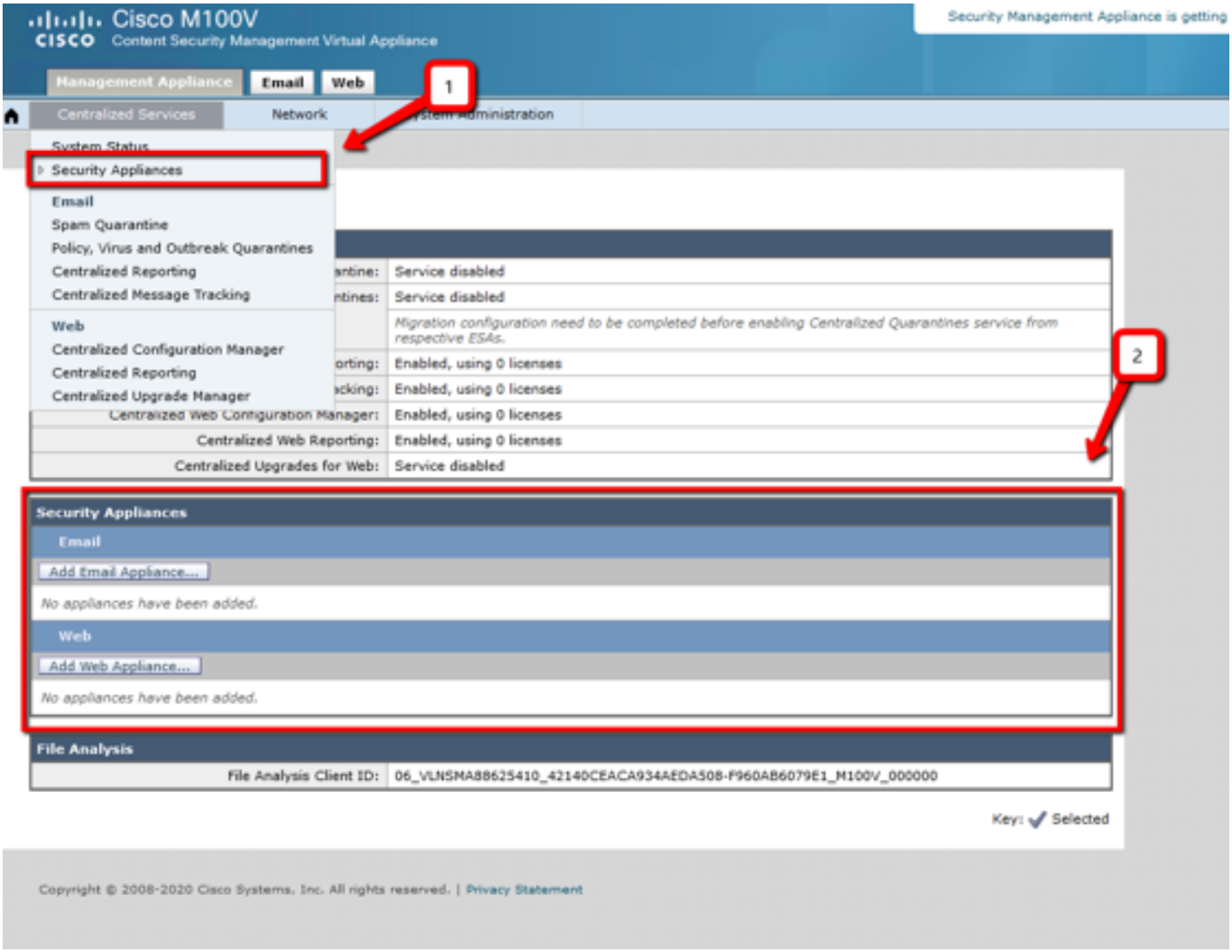
Sur le SMA, accédez à **Accueil > Informations de version**.



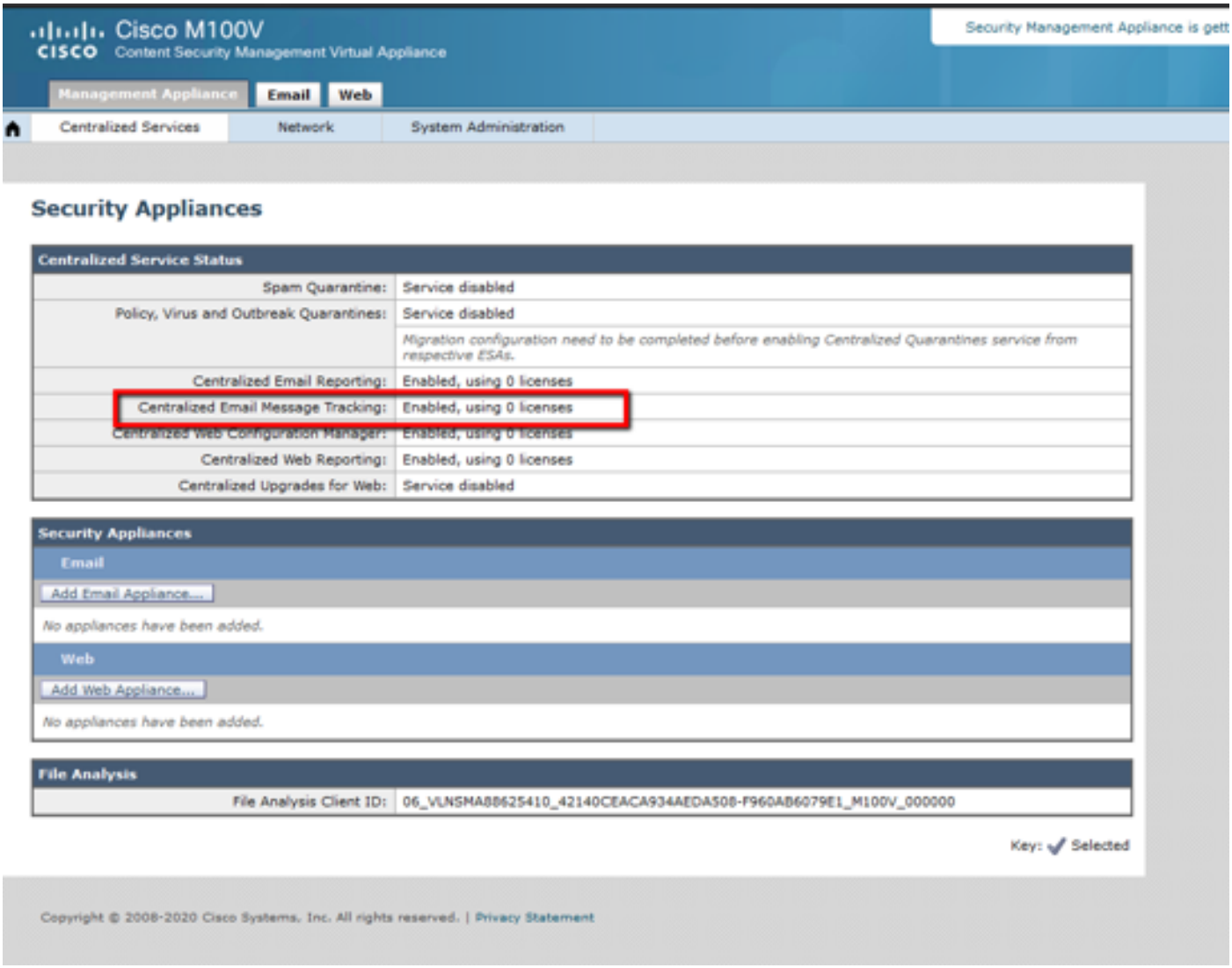
Si aucune donnée n'est disponible sur SecureX après l'intégration. Vous pouvez suivre les étapes suivantes.

Étape 1. Vérifier le rapport des appliances ESA/WSA au SMA

Sur le SMA, accédez à **Services centralisés > Appliances de sécurité** et vérifiez que les périphériques ESA/WSA apparaissent sous **Appliances de sécurité**.



Étape 2. Vérifiez que la licence SMA pour le **suivi centralisé des messages électroniques** est sous licence et activée sous **Services centralisés > Appliances de sécurité**.



Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

> **Astuce** : Si vous recevez une erreur Timeout pendant que vous effectuez des investigations ou lors de l'ajout de vignettes à SecureX, cela peut être dû à un volume élevé d'informations envoyées par vos périphériques. Essayez de diminuer le paramètre **Délai de demande (jours)** dans la configuration du module.

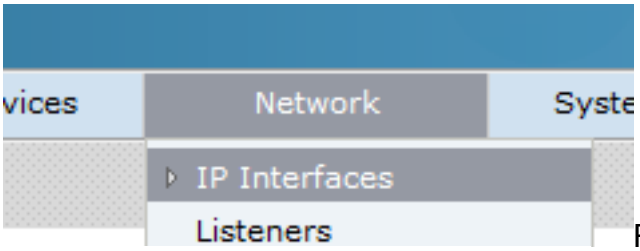
Commandes utilisées sur la console SSH SMA

- Pour vérifier la version et la licence réelles du SMA, ces commandes peuvent être utilisées >Afficher la licence>version
- Journaux d'intégration contenant les événements d'enregistrement >cat ctr_logs/ctr_logs.current
- Test de connectivité vers le portail SSE >telnet api-sse.cisco.com 443

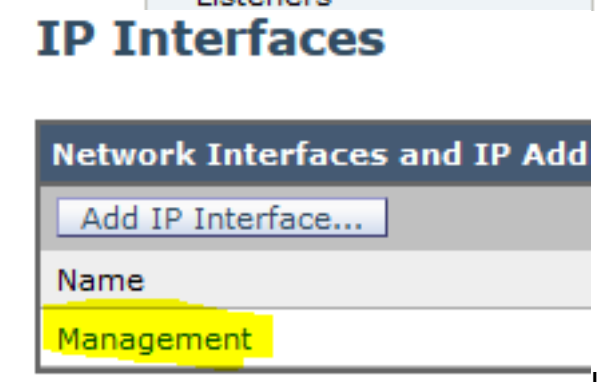
Module SMA de réponse aux menaces SecureX SMA/tile SecureX indiquant l'erreur « Une erreur inattendue s'est produite sur le module SMA »

SMA nécessite la configuration HTTP et HTTPS de l'API AsyncOS activée sur l'interface de gestion pour communiquer avec le portail SecureX/CTR.

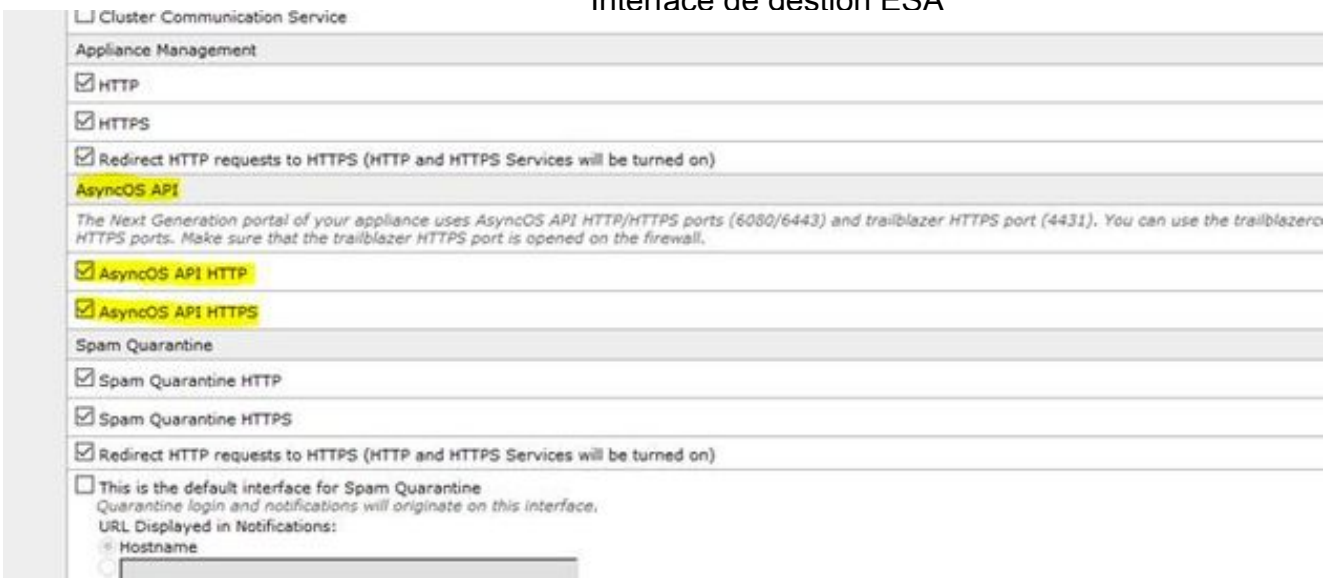
Pour configurer un SMA sur site à partir de l'interface graphique du portail SMA, accédez à **Réseau > Interfaces IP > Interface de gestion > API AsyncOS** et activez HTTP et HTTPS.

1. 

Réseau > Interfaces IP



2. Interface de gestion ESA

3. 

API asynchrone > HTTP et HTTPS

Pour un CES (Cloud Based SMA), cette configuration doit être effectuée à partir de l'arrière-plan par un ingénieur du centre d'assistance technique SMA. Elle nécessite l'accès au tunnel d'assistance de la CES affectée.

Vidéo

Informations connexes

- Vous pouvez trouver des vidéos sur la façon de configurer vos intégrations de produits ici.
- Si votre périphérique n'est pas géré par un SMA, vous pouvez ajouter des modules pour ESA ou WSA individuellement.
- Support et documentation techniques - Cisco Systems