Guide des meilleures pratiques pour Advanced Malware Protection (AMP) sur la sécurité de la messagerie Cisco

Contenu

[Introduction](#)
[Vérifier les clés de fonction](#)
[Activer la protection avancée contre les programmes malveillants (AMP)](#)
[Personnaliser les paramètres globaux d'Advanced Malware Protection (AMP)](#)
[Définition du seuil d'analyse de fichiers](#)
[Intégration du ESA à la console AMP for Endpoints](#)
[Activer la correction automatique de la boîte aux lettres (MAR)](#)
[Configurer Advanced Malware Protection (AMP) dans la stratégie de messagerie](#)
[Intégrer SMA à Cisco Threat Response (CTR)](#)
[Conclusion](#)

Introduction

Advanced Malware Protection (AMP) est une solution complète qui permet la détection et le blocage des programmes malveillants, l'analyse continue et les alertes rétrospectives. L'utilisation d'AMP avec la solution de sécurisation de la messagerie Cisco permet une protection supérieure à tous les stades de l'attaque : avant, pendant et après l'attaque, grâce à l'approche la plus économique et la plus facile à déployer pour la protection avancée contre les programmes malveillants.

Ce document de bonnes pratiques couvre les principales fonctionnalités d'AMP sur l'appliance de sécurité de la messagerie Cisco (ESA), comme indiqué ci-dessous :

- **Réputation des fichiers** - capture l'empreinte digitale de chaque fichier lorsqu'il traverse l'ESA et l'envoie au réseau de veille cloud d'AMP pour obtenir un verdict de réputation. Dans ces résultats, vous pouvez bloquer automatiquement les fichiers malveillants et appliquer une stratégie définie par l'administrateur.
- **Analyse des fichiers** : permet d'analyser les fichiers inconnus qui traversent le SEEE. Un environnement de sandbox hautement sécurisé permet à AMP d'obtenir des détails précis sur le comportement du fichier et de combiner ces données avec une analyse humaine et machine détaillée pour déterminer le niveau de menace du fichier. Cette disposition est ensuite intégrée au réseau d'intelligence basé sur le cloud AMP et utilisée pour mettre à jour et étendre dynamiquement le jeu de données cloud AMP afin d'améliorer la protection.
- **Mailbox Auto Remediation (MAR)** - pour Microsoft Office 365 et Exchange 2013/2016 automatise la suppression des e-mails avec des fichiers qui deviennent malveillants après le point d'inspection initial. Cela permet aux administrateurs d'économiser des heures de travail et de limiter l'impact d'une menace.
- **Cisco AMP Unity** - est la fonctionnalité qui permet à une organisation d'enregistrer son périphérique AMP, y compris ESA avec abonnement AMP dans la console AMP for

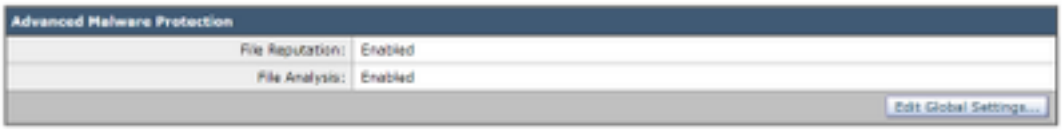
Endpoints. Grâce à cette intégration, Cisco Email Security peut être vu et interrogé pour des exemples d'observations de la même manière que la console AMP for Endpoints offre déjà pour les terminaux et permet de corréler les données de propagation des fichiers sur tous les vecteurs de menace dans une interface utilisateur unique.
- **Cisco Threat Response** : plate-forme d'orchestration qui regroupe les informations relatives à la sécurité provenant de sources Cisco et tierces dans une console unique et intuitive d'analyse et de réponse. Il le fait par le biais d'une conception modulaire qui sert de cadre d'intégration pour les journaux d'événements et les informations sur les menaces. Les modules permettent une corrélation rapide des données en créant des graphiques de relation qui permettent aux équipes de sécurité d'obtenir une vue claire de l'attaque et de prendre rapidement des mesures efficaces.

Vérifier les clés de fonction

- Sur l'ESA, accédez à **Administration système> Clés de fonction**
- Recherchez les clés de fonction Réputation des fichiers et Analyse des fichiers et assurez-vous que les statuts sont **actifs**

Activer la protection avancée contre les programmes malveillants (AMP)

- Sur l'ESA, accédez à **Security Services >Advanced Malware Protection - File Reputation and Analysis.**
- Cliquez sur le bouton **Activer** dans **Advanced Malware Protection** Global Settings :



- **Validez** vos modifications.

Personnaliser les paramètres globaux d'Advanced Malware Protection (AMP)

- AMP est maintenant activé, cliquez sur **Modifier les paramètres globaux** pour personnaliser les paramètres globaux.
- La liste des extensions de fichier sera automatiquement mise à jour de temps en temps. Veuillez donc toujours consulter ce paramètre et vous assurer que toutes les extensions de fichier sont sélectionnées :

- Développer **les paramètres avancés pour la réputation des fichiers**
- La sélection par défaut pour le serveur de réputation de fichiers est **AMERICA (cloud-sa.amp.cisco.com)**
- Cliquez sur le menu déroulant et choisissez les serveurs de réputation de fichier les plus proches (en particulier pour les clients APJC et EUROPE) :

- Développer **les paramètres avancés pour l'analyse des fichiers**
- La sélection par défaut pour l'URL du serveur d'analyse de fichiers est **AMERICAS (https://panacea.threatgrid.com)**
- Cliquez sur le menu déroulant et choisissez les serveurs de réputation de fichier les plus proches (particulièrement pour les clients EUROPE) :

Définition du seuil d'analyse de fichiers

(Facultatif) Vous pouvez définir la limite supérieure du score d'analyse de fichier acceptable. Les fichiers bloqués en fonction des paramètres de seuil s'affichent en tant que seuil personnalisé dans la section Fichiers de menace de programme malveillant entrants du rapport Advanced Malware Protection.

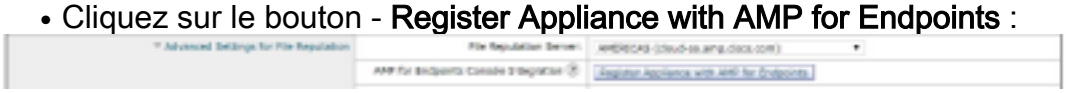
- Dans la page de paramètres globaux AMP, développez **Threshold** Settings.
- La valeur par défaut du service cloud est **95**.
- Sélectionnez la case d'option **Entrer une valeur personnalisée** et modifiez la valeur (par exemple, 70) :

- Cliquez sur **Soumettre et valider** vos modifications

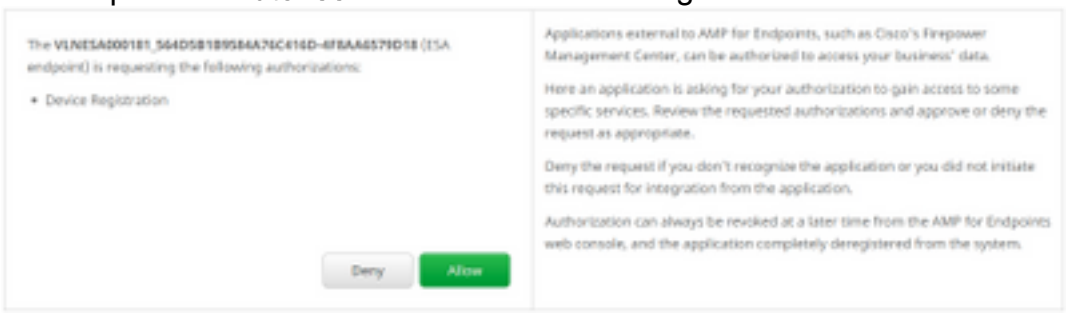
Intégration du ESA à la console AMP for Endpoints

(Uniquement pour le client AMP for Endpoints) Une liste de blocage de fichiers personnalisée unifiée (ou une liste d'autorisations de fichiers) peut être créée via la console AMP for Endpoints et peut distribuer de manière transparente la stratégie de confinement à travers l'architecture de sécurité, y compris l'ESA.

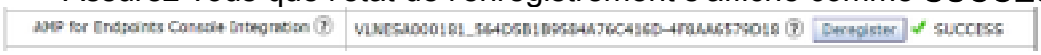
- Dans la page de paramètres globaux d'AMP, développez **Paramètres avancés pour la réputation des fichiers**
- Cliquez sur le bouton - **Register Appliance with AMP for Endpoints** :



- Cliquez sur **OK** pour rediriger vers le site de la console AMP for Endpoints pour terminer l'enregistrement.
- Connectez-vous à la console AMP for Endpoints avec vos informations d'identification utilisateur
- Cliquez sur **Autoriser** l'autorisation de l'enregistrement ESA :



- La console AMP for Endpoints fait pivoter automatiquement la page vers ESA.
- Assurez-vous que l'état de l'enregistrement s'affiche comme **SUCCESS** :



- Cliquez sur **Soumettre** et **valider** vos modifications

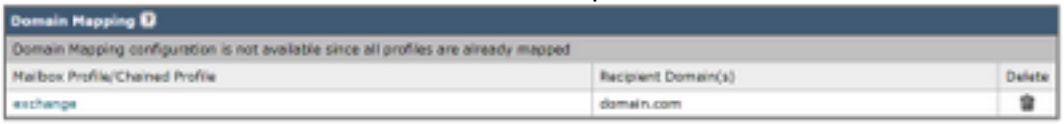
Activer la correction automatique de la boîte aux lettres (MAR)

Si vous avez des boîtes aux lettres O365 ou Microsoft Exchange 2013/2016, la fonction de correction automatique de boîte aux lettres (MAR) permet d'effectuer l'action lorsque le verdict de réputation du fichier passe de Clean/Unknown à Malicious.

- Accédez à **Administration système > Paramètres du compte**
- Sous **Profil de compte**, cliquez sur **Créer un profil de compte** pour créer un profil de connexion API avec les boîtes aux lettres Office 365 et/ou Microsoft Exchange :

- Cliquez sur **Soumettre** et **valider** vos modifications

- (Facultatif) Le profil enchaîné est un ensemble de profils. Vous ne configurez le profil enchaîné que lorsque les comptes à accéder résident sur différents locataires de différents types de déploiements.
- Cliquez sur le bouton **Créer un mappage de domaine** pour mapper votre profil de compte avec le domaine du destinataire. Les paramètres recommandés sont affichés ci-dessous :

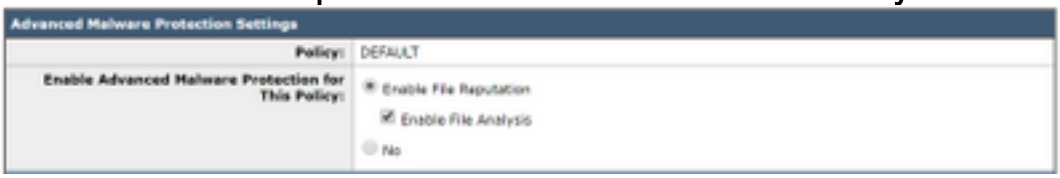


- Cliquez sur **Soumettre** et **valider** vos modifications

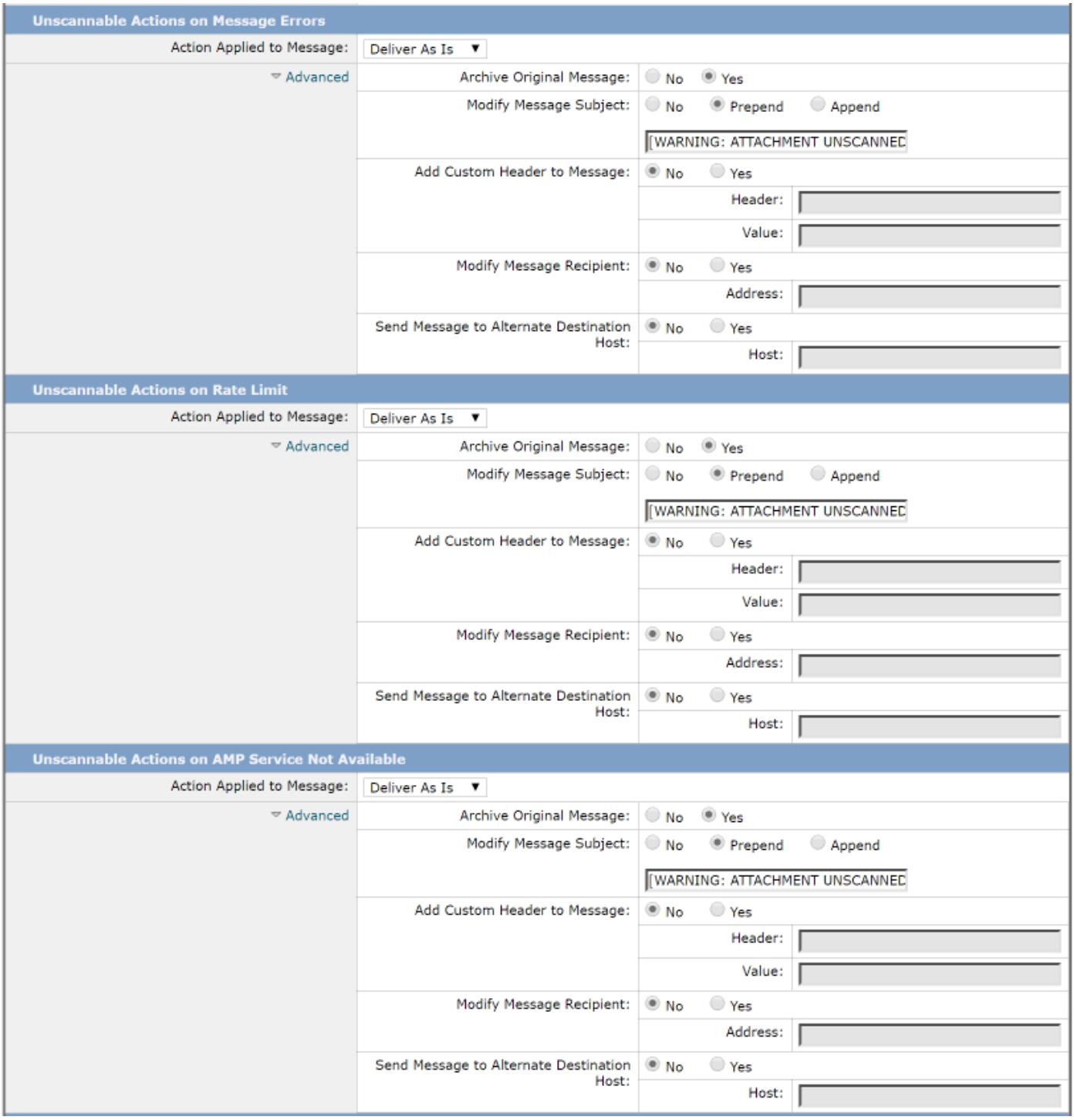
Configurer Advanced Malware Protection (AMP) dans la stratégie de messagerie

Une fois AMP et MAR configurés globalement, vous pouvez maintenant activer les services pour les stratégies de messagerie.

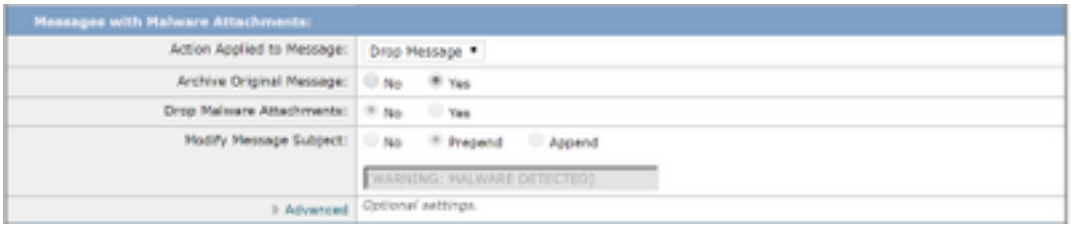
- Accédez à **Politiques de messagerie > Stratégies de messagerie entrante**
- Personnalisez les paramètres **Advanced Malware Protection** pour une stratégie de messagerie entrante en cliquant sur le lien bleu sous **Advanced Malware Protection** pour la stratégie que vous souhaitez personnaliser.
- Pour les besoins de ce document de bonnes pratiques, cliquez sur la case d'option en regard de **Enable File Reputation** et sélectionnez **Enable File Analysis** :



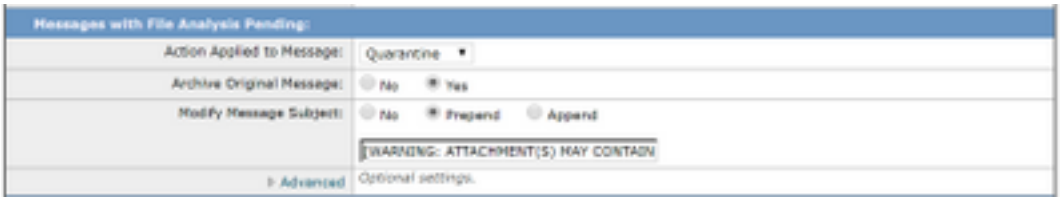
- Il est recommandé d'**inclure un en-tête X avec le résultat AMP dans un message**.
- Les trois sections suivantes vous permettent de sélectionner l'action que l'ESA doit effectuer si une pièce jointe est considérée comme non analysable en raison d'erreurs de message, de la limite de débit ou si le service AMP n'est pas disponible. L'action recommandée consiste à **fournir l'état actuel** avec **un texte d'avertissement préfixé sur l'objet du message** :



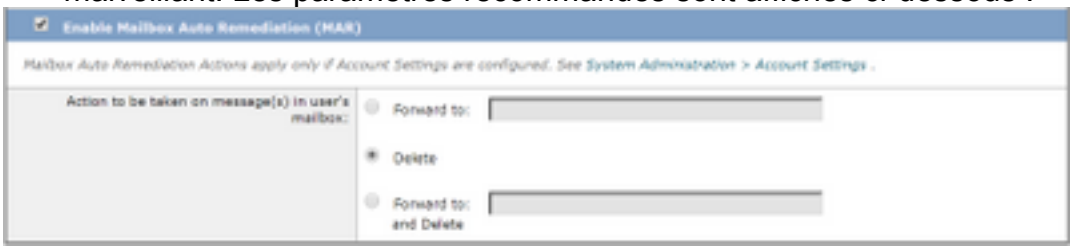
- La section suivante configure le ESA pour supprimer le message si une pièce jointe est considérée comme malveillante :



- L'action recommandée consiste à mettre en quarantaine le message si la pièce jointe est envoyée pour l'analyse de fichiers :



- (Pour la stratégie de messagerie entrante uniquement) Configurez les actions correctives à effectuer sur le message remis aux utilisateurs finaux lorsque le verdict de menace devient malveillant. Les paramètres recommandés sont affichés ci-dessous :

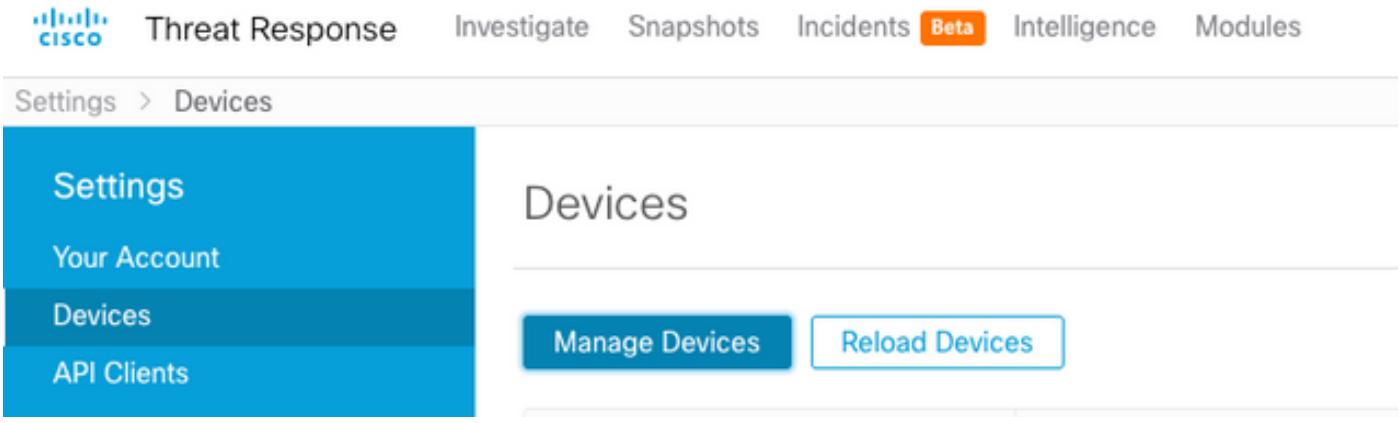


- Cliquez sur **Soumettre** et **valider** vos modifications

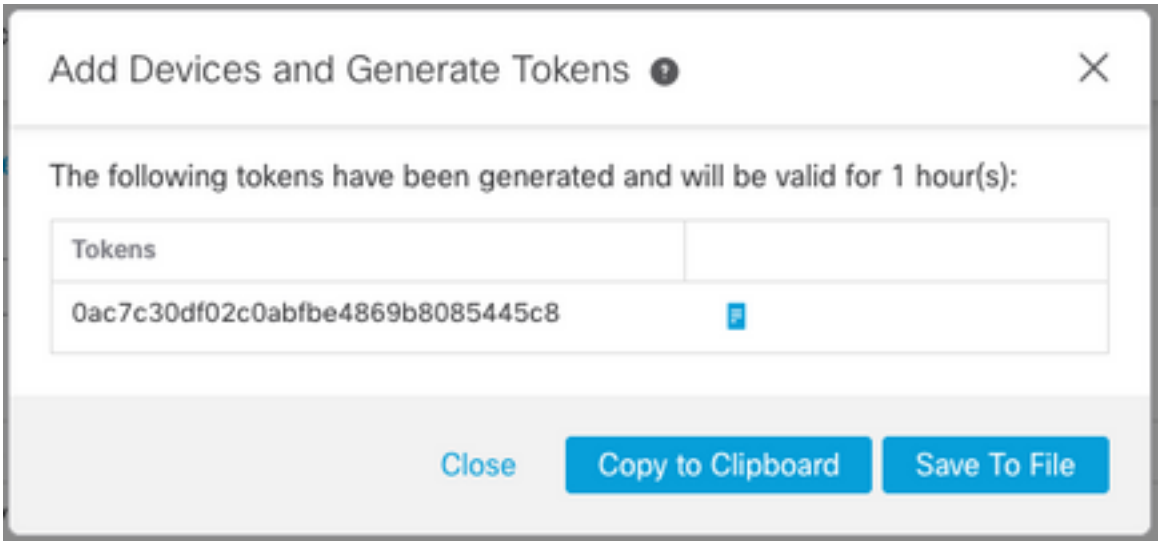
Intégrer SMA à Cisco Threat Response (CTR)

L'intégration d'un module de messagerie SMA nécessite l'utilisation de Security Services Exchange (SSE) via CTR. SSE permet à un SMA de s'enregistrer auprès d'Exchange et vous autorisez explicitement Cisco Threat Response à accéder aux périphériques enregistrés. Le processus implique de lier votre SMA à SSE via un jeton généré lorsque vous êtes prêt à le lier.

- Sur le portail CTR (https://visibility.amp.cisco.com), connectez-vous avec vos informations d'identification utilisateur.
- CTR utilise un module pour s'intégrer à d'autres produits de sécurité Cisco, notamment ESA. Cliquez sur l'onglet **Modules**.
- Choisissez **Périphériques** et cliquez sur **Gérer les périphériques :**



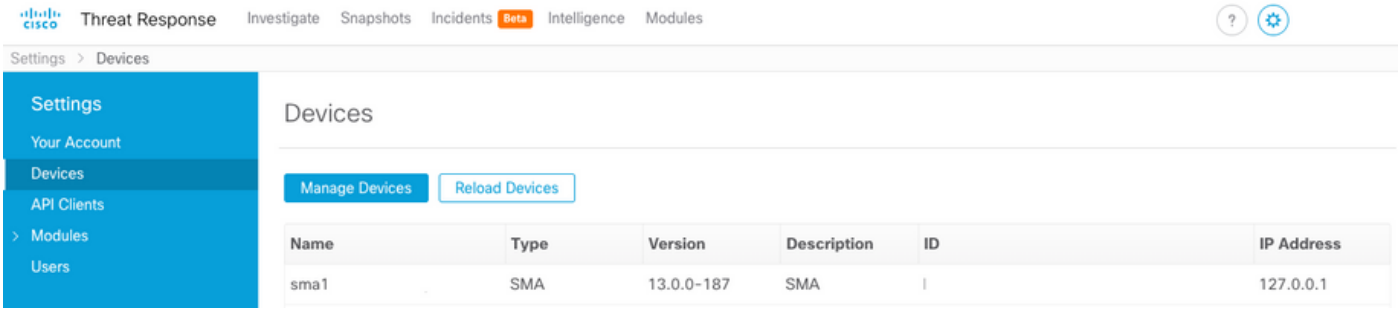
- CTR fait pivoter la page vers SSE.
- Cliquez sur l'icône **+** pour générer un nouveau jeton et cliquez sur **Continuer**.
- Copiez le nouveau jeton avant de fermer la boîte :



- Sur votre SMA, accédez à l'onglet **Appliances de gestion > Réseau > Paramètres du service cloud**
- Cliquez sur **Modifier le paramètre** et assurez-vous que l'option Réponse aux menaces est **Activer**.
- La sélection par défaut pour l'URL du serveur de réponse aux menaces est **AMERICAS (api-sse.cisco.com).** Pour les clients EUROPE, cliquez sur le menu déroulant et choisissez **EUROPE (api.eu.sse.itd.cisco.com)** :

- Cliquez sur **Soumettre** et **valider** vos modifications
- Collez la clé de jeton (que vous avez générée à partir du portail CTR) dans le paramètre Cloud Services et cliquez sur **Register** :

- La procédure d'inscription prendra un certain temps. Veuillez revenir à cette page après quelques minutes pour vérifier à nouveau l'état.
- Revenez à **CTR > Modules > Périphérique** et cliquez sur le bouton **Recharger le périphérique** pour vous assurer que le SMA apparaît dans la liste :



Conclusion

Ce document visait à décrire les configurations par défaut ou les meilleures pratiques pour Cisco

Advanced Malware Protection (AMP) dans l'appliance de sécurité de la messagerie. La plupart de ces paramètres sont disponibles sur les stratégies de messagerie entrante et sortante, et la configuration et le filtrage sont recommandés dans les deux directions.