Intégrer AMP for Endpoints and Threat Grid à WSA

Contenu

Introduction

Ce document décrit les étapes à suivre pour intégrer Advanced Malware Protection (AMP) pour les terminaux et Threat Grid (TG) avec l'appareil de sécurité Web (WSA).

Contribué par Uriel Montero et édité par Yeraldin Sanchez, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- AMP pour l'accès aux terminaux
- Accès Premium TG
- WSA avec clés de fonction d'analyse de fichiers et de réputation de fichiers

Components Used

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

- Console de cloud public AMP
- Interface utilisateur WSA
- Console TG

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.

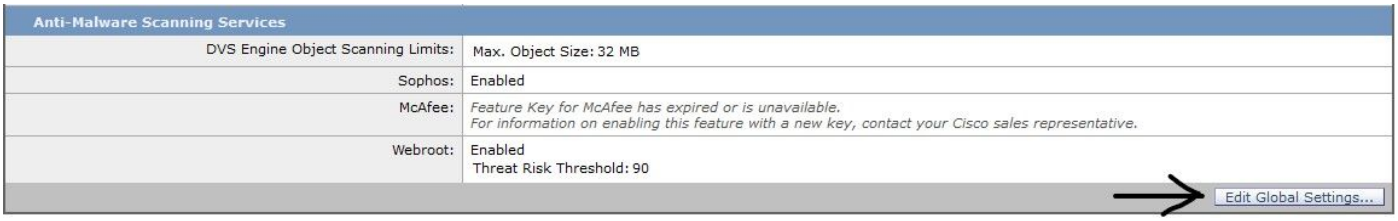
Configuration

Connectez-vous à la console WSA.

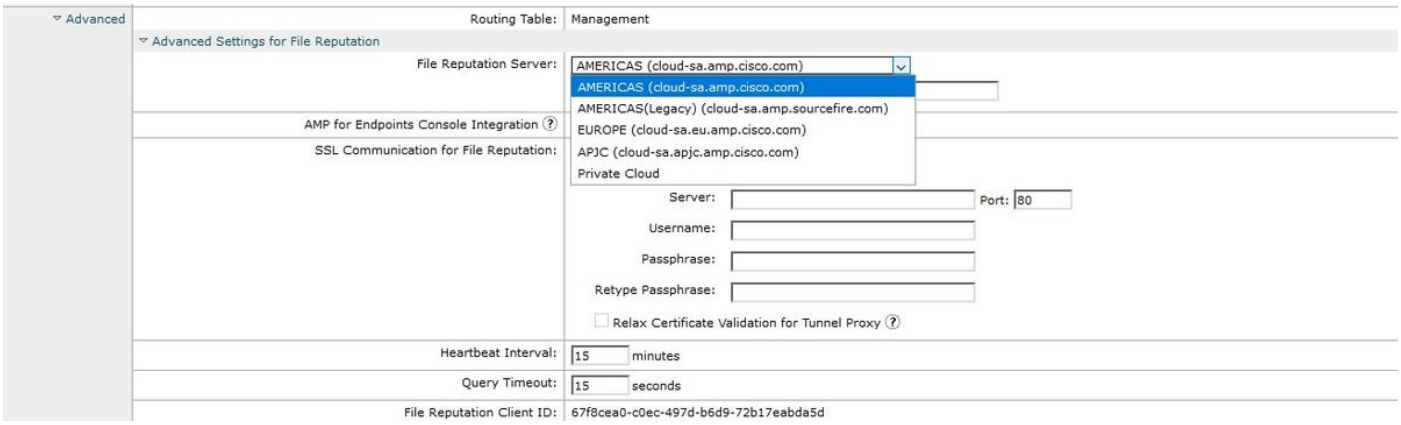
Une fois connecté, accédez à **Security Services > Anti-Malware and Reputation,** dans cette section vous trouverez les options d'intégration d'AMP et TG.

Intégration AMP

Dans la section Anti-Malware Scanning Services, cliquez sur **Edit Global Settings**, comme illustré dans l'image.

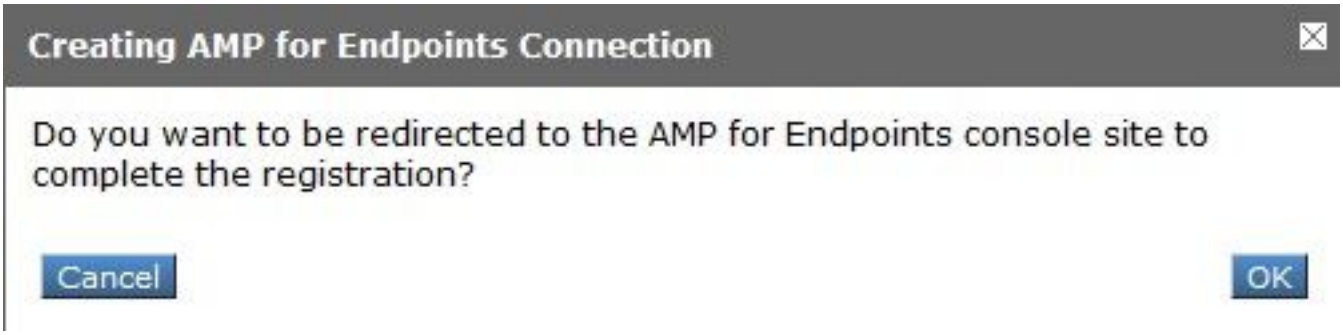


Recherchez la section **Advanced > Advanced Settings for File Reputation** et développez-la, puis une série d'options de serveurs cloud s'affiche, choisissez la plus proche de votre emplacement.

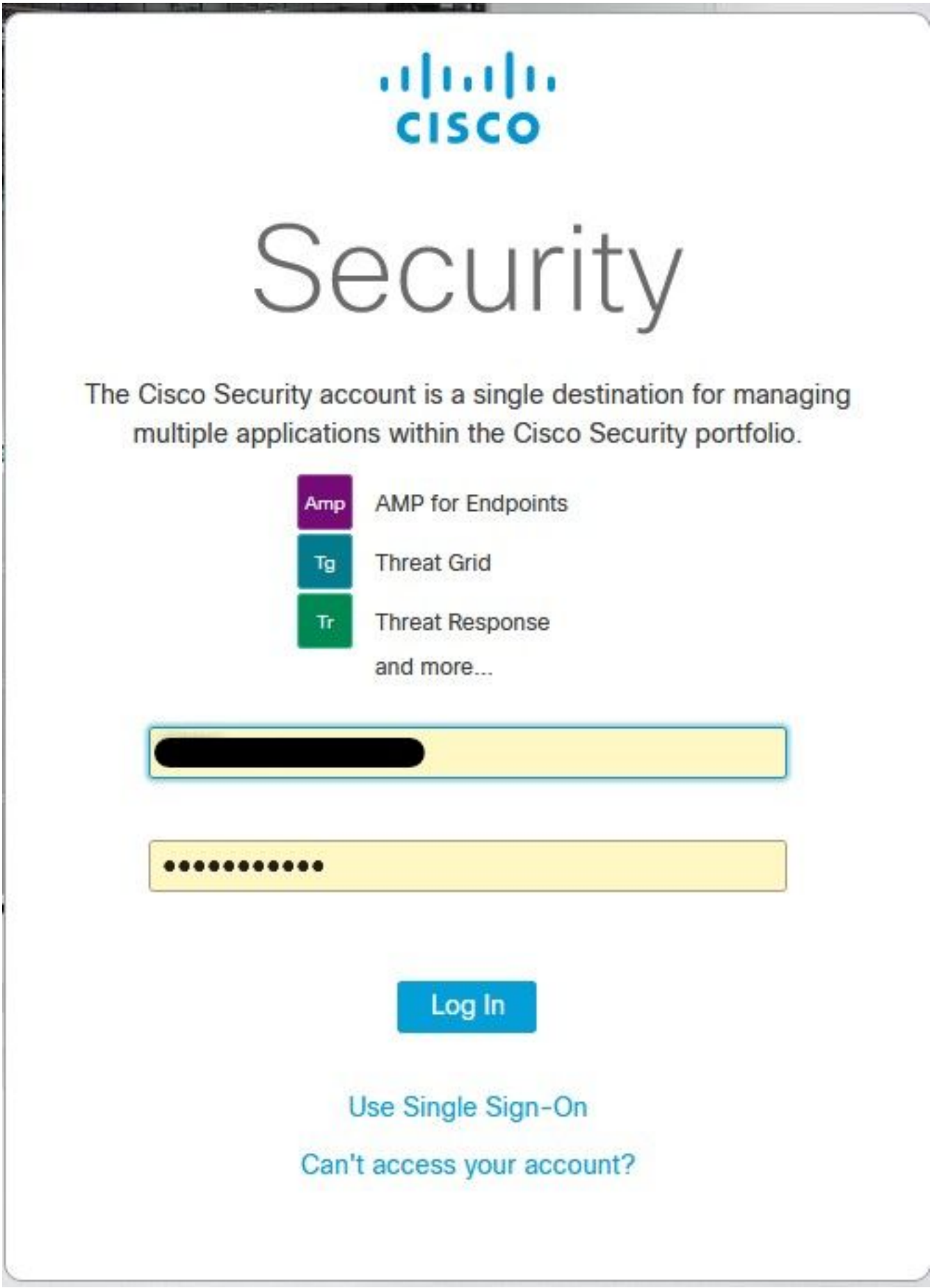


Une fois le cloud sélectionné, cliquez sur le bouton **Register Appliance with AMP for Endpoints**.

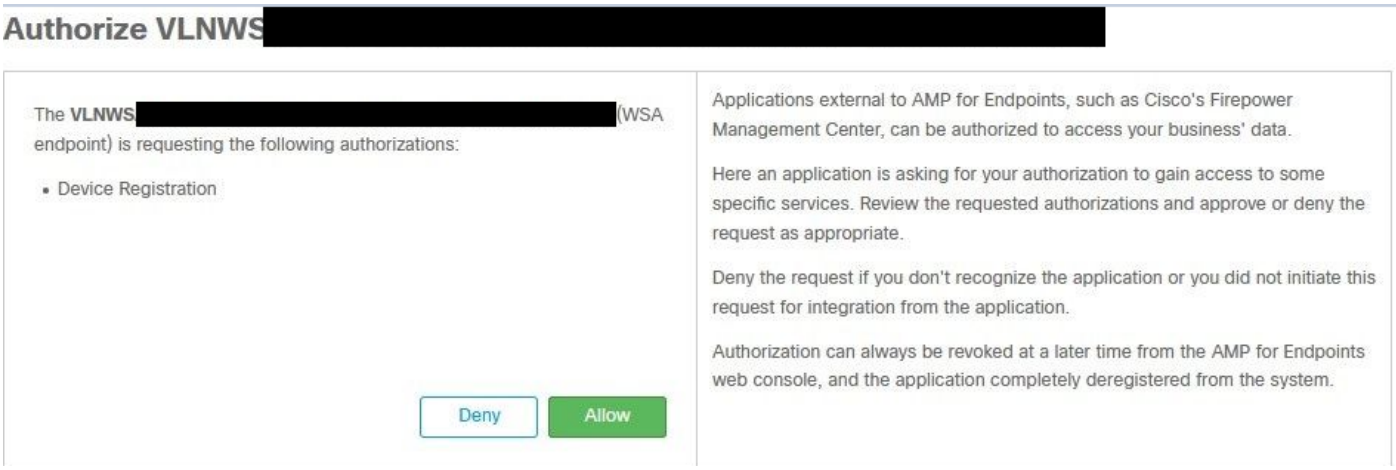
Une fenêtre contextuelle s'affiche et redirige vers la console AMP, cliquez sur le **bouton Ok,** comme indiqué dans l'image.



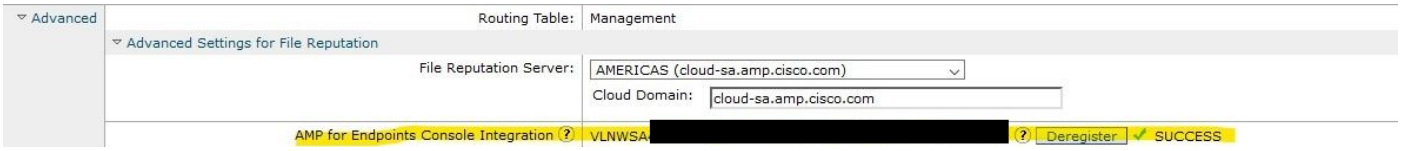
Vous devez saisir des informations d'identification AMP valides et cliquer sur **Se connecter,** comme indiqué dans l'image.



Acceptez l'enregistrement du périphérique, prenez note de l'ID du client, car il permet de trouver le WSA ultérieurement sur la console.



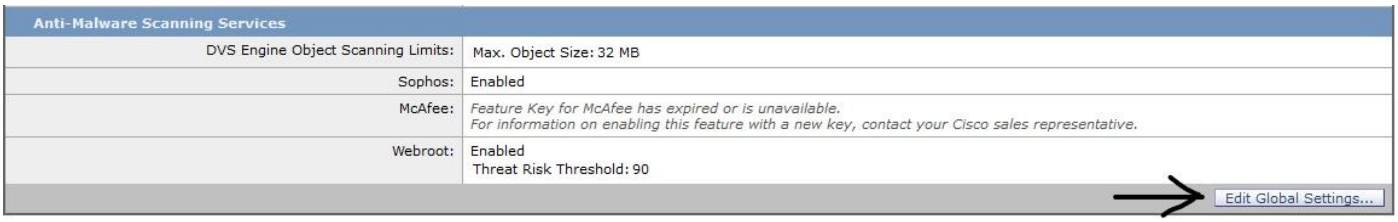
Revenez à la console WSA, une vérification s'affiche dans la section Amp for Endpoints Console Integration, comme illustré dans l'image.



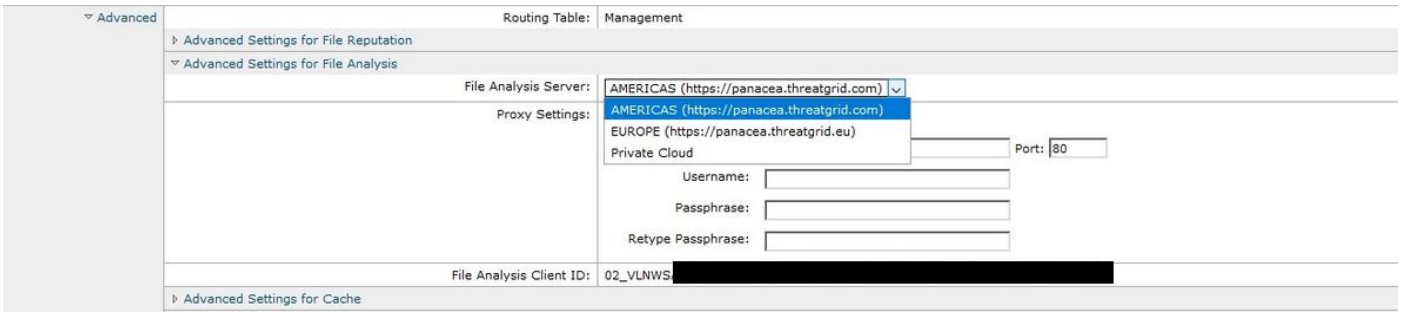
> **Remarque** : n'oubliez pas de cliquer sur **Soumettre** et **valider** les modifications (si vous y êtes invité), sinon le processus doit être recommencé.

Intégration de Threat Grid

Naviguez jusqu'à **Services de sécurité > Anti-Malware and Reputation**, puis dans les Services de protection contre les programmes malveillants, cliquez sur le bouton **Edit Global Settings**, comme illustré dans l'image.

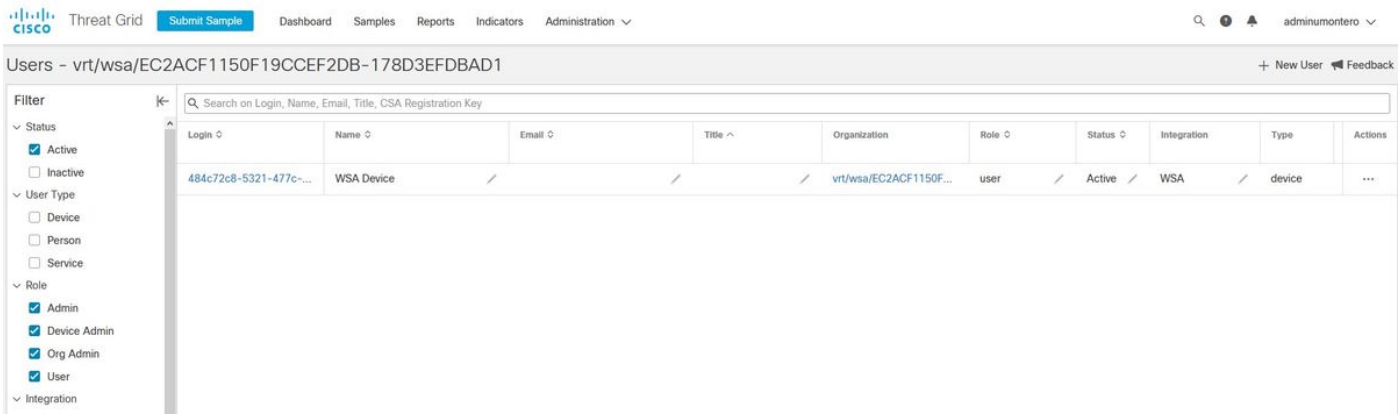


Recherchez la section **Advanced> Advanced Settings for File Analysis** et développez-la, choisissez l'option la plus proche de votre emplacement, comme illustré dans l'image.



Cliquez sur **Soumettre** et **valider** les modifications.

Du côté du portail TG, recherchez le périphérique WSA sous l'onglet Users si l'appliance a été correctement intégrée à AMP/TG.



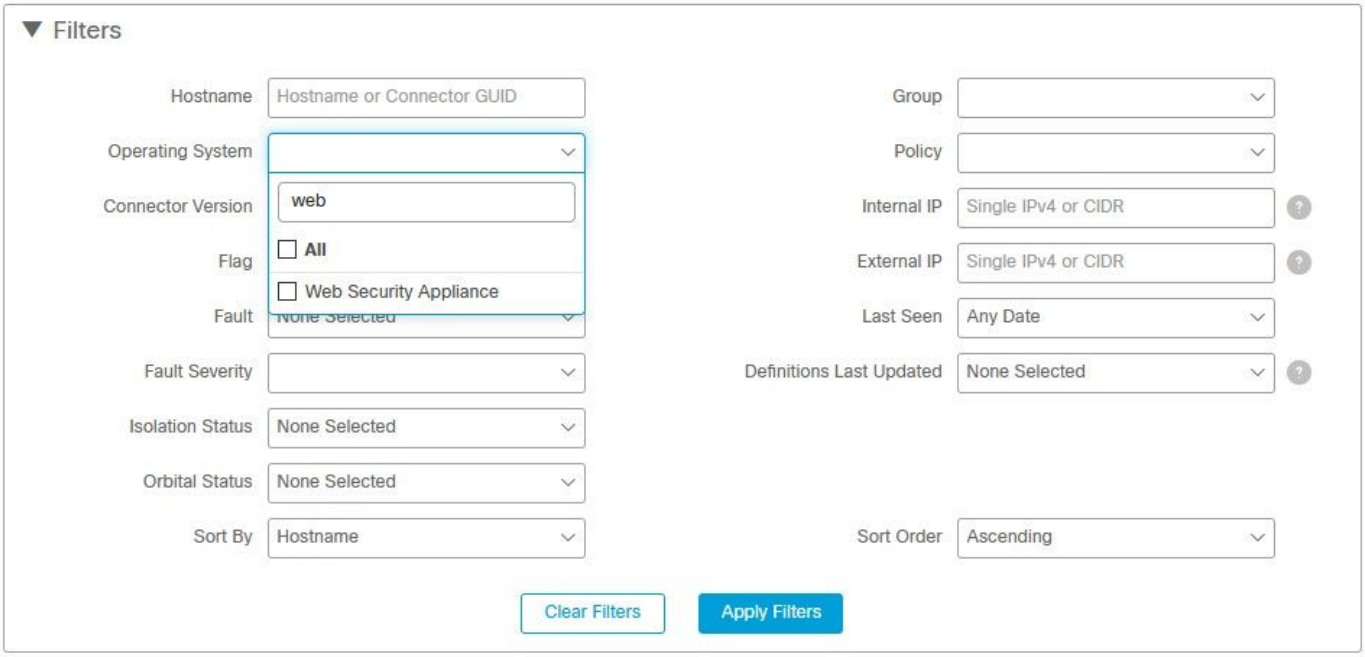
Si vous cliquez sur Connexion, vous pouvez accéder aux informations de ladite appliance.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

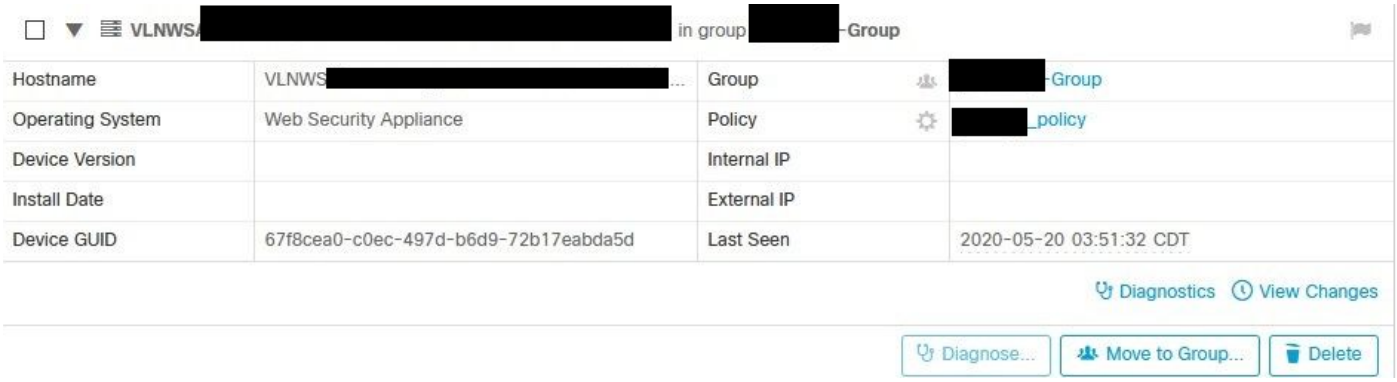
Afin de vérifier que l'intégration entre AMP et WSA est réussie, vous pouvez vous connecter à la console AMP et rechercher votre périphérique WSA.

Accédez à **Management > Computers**, dans la section Filtres, recherchez **Web Security Appliance** et appliquez le filtre

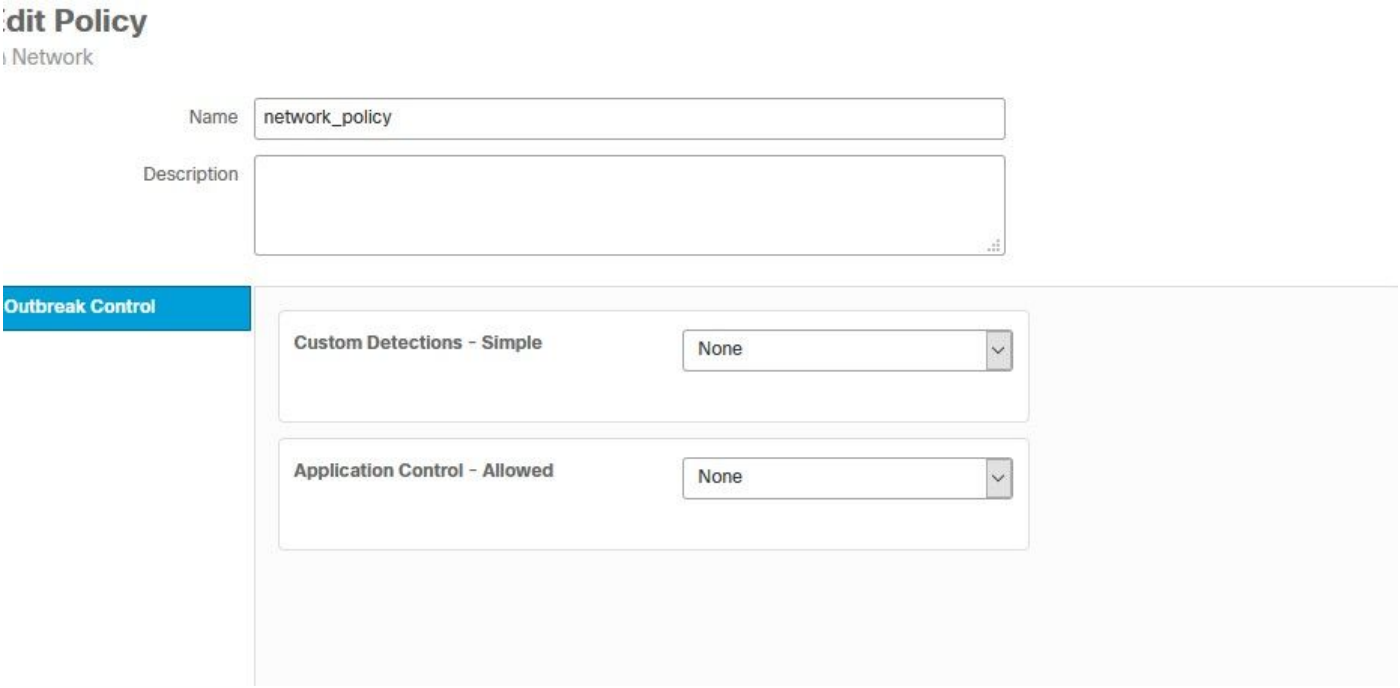


Si plusieurs périphériques WSA sont enregistrés, vous pouvez les identifier avec l'ID client d'analyse de fichiers.

Si vous développez le périphérique, vous pouvez voir à quel groupe il appartient, la stratégie appliquée et le GUID du périphérique peuvent être utilisés pour afficher la trajectoire du périphérique.

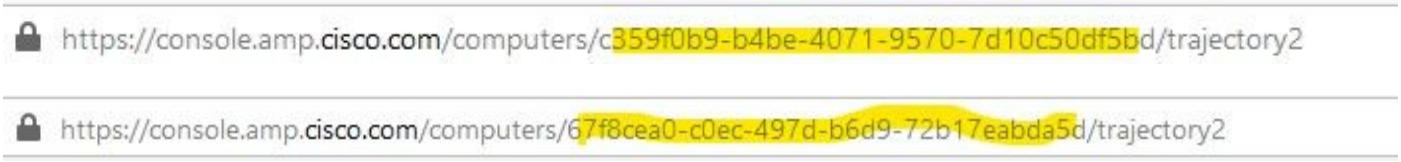


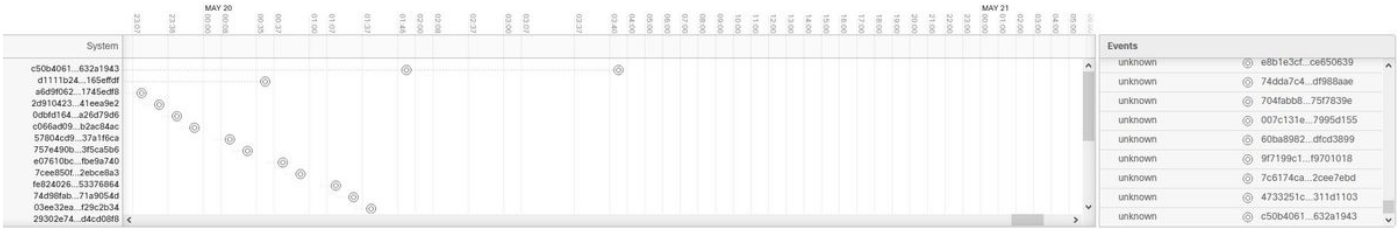
Dans la section Stratégie, vous pouvez configurer des détections personnalisées simples et le contrôle d'application - Autorisé qui est appliqué au périphérique.



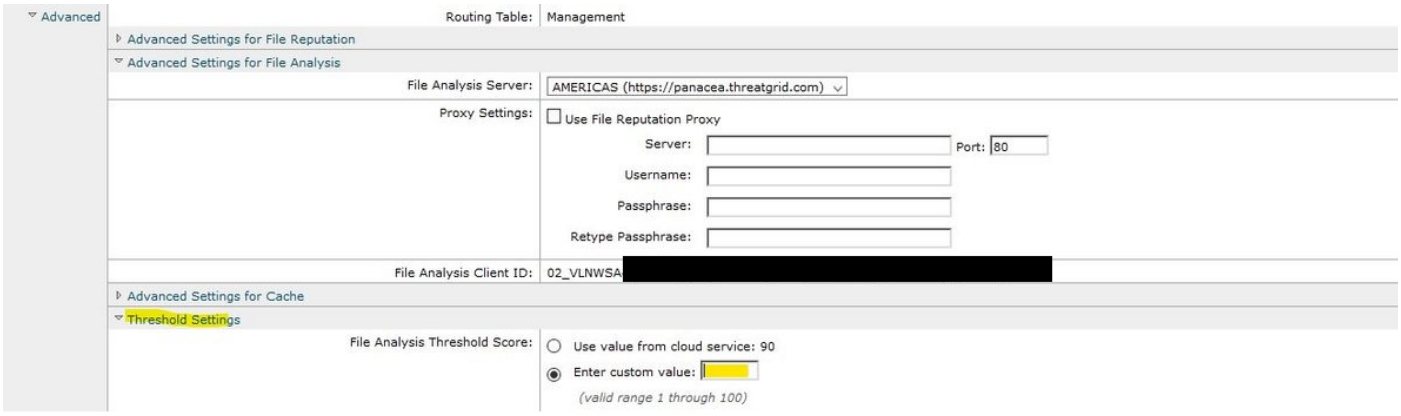
Il y a une astuce pour afficher la section Trajectoire du périphérique du WSA, vous devez ouvrir la trajectoire du périphérique d'un autre ordinateur et utiliser le GUID du périphérique.

La modification est appliquée à l'URL, comme le montrent les images.





Pour Threat Grid, il y a un seuil de 90, si un fichier obtient un score sous ce numéro, le fichier n'est pas placé malveillant, mais vous pouvez configurer un seuil personnalisé sur le WSA.



Dépannage

WSA ne redirige pas vers la page AMP

- Assurez-vous que le pare-feu autorise les adresses requises pour AMP, cliquez ici.
- Vérifiez que vous avez sélectionné le cloud AMP approprié (évitez de choisir le cloud hérité).

WSA ne bloque pas les SHA spécifiés

- Assurez-vous que votre WSA se trouve dans le groupe approprié.
- Assurez-vous que votre WSA utilise la stratégie appropriée.
- Assurez-vous que le SHA n'est pas propre sur le cloud, sinon WSA ne pourrait pas le bloquer.

WSA n'apparaît pas sur mon organisation TG

- Vérifiez que vous avez sélectionné le cloud TG approprié (Amérique ou Europe).
- Assurez-vous que le pare-feu autorise les adresses requises pour TG.
- Prenez note de l'ID du client d'analyse de fichiers.
- Recherchez-le dans la section Utilisateurs.
- Si vous ne le trouvez pas, contactez l'assistance Cisco afin qu'elle vous aide à le déplacer d'une organisation à l'autre.