ID client d'analyse de fichiers de Threat Grid sur les appliances de sécurité de contenu (ESA, SMA, WSA) et DC/FMC

Contenu

Introduction

Ce document décrit comment trouver ou construire l'ID client d'analyse de fichiers de Threat Grid de 65 caractères associé aux appliances de sécurité de contenu Cisco, aux appliances de sécurité de la messagerie électronique (ESA), aux appliances de gestion de la sécurité (SMA) et aux appliances de sécurité Web (WSA), ou à partir de Cisco Defense Center (DC) ou de FirePower Management Center (FMC).

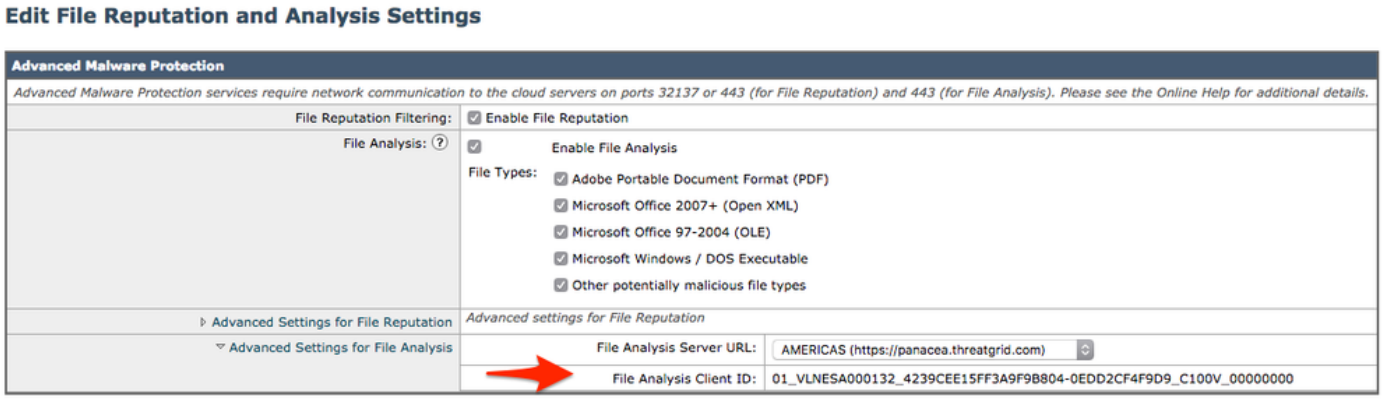
ID client d'analyse de fichiers sur les appliances de sécurité de contenu

Interface utilisateur ESA

1. **Services de sécurité > Réputation et analyse des fichiers**
2. Cliquez sur **Modifier les paramètres globaux...**
3. Développer **les paramètres avancés pour l'analyse des fichiers**

L'ID du client d'analyse de fichiers est répertorié ici.

vESA exécutant AsyncOS 10.0.0-203 pour la sécurité de la messagerie eexemple :



Remarque: Il y a une différence dans l'ID du client d'analyse de fichiers pour l'appliance virtuelle par rapport à l'appliance matérielle.

L'ID du client d'analyse de fichiers est basé sur le format de chaîne de 65 caractères suivant :

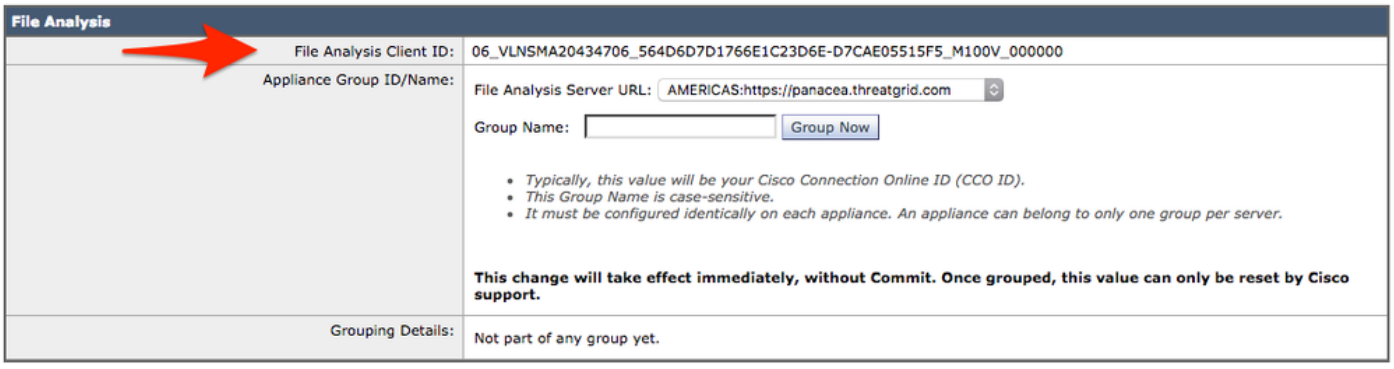
Valeur	Explication
01_	ESA
VLNESAXXXYYY_	S'il s'agit d'un appareil virtuel, il utilise le numéro de licence VLN (qui se trouve dans l'interface de ligne de commande avec **show license**). S'il s'agit d'une appliance maté il n'y a aucun champ.
SÉRIE_	Ceci sera la série COMPLÈTE de l'appliance (qui est trouvée à partir de l'interface de de commande avec **version**).
CX00V_	TIl s'agit du modèle de l'appliance (encore une fois, à partir de **la version** de l'interface ligne de commande). Cette valeur varie à nouveau, s'il s'agit d'un appareil virtuel par rapport à un appareil matériel.
00000000	Des zéros de fin. Celles-ci varieront en fonction des champs précédents, afin de term le champ de 65 caractères.

Interface utilisateur SMA

1. **Gestion centralisée > Appareils de sécurité**

Dans la section inférieure, *Analyse de fichiers*, l'ID du client d'analyse de fichiers est indiqué ici.

vSMA exécutant AsyncOS 9.6.0-051 pour la gestion de la sécurité eexemple :



Remarque: Il y a une différence dans l'ID du client d'analyse de fichiers pour l'appliance virtuelle par rapport à l'appliance matérielle.

L'ID du client d'analyse de fichiers est basé sur le format de chaîne de 65 caractères suivant :

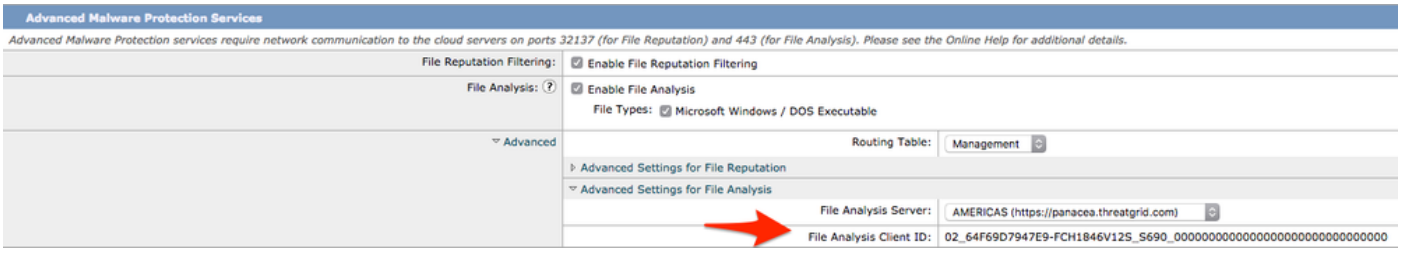
Valeur	Explication
06_	SMA
VLNSMAXXXYYY_	S'il s'agit d'un appareil virtuel, il utilise le numéro de licence VLN (qui se trouve dans l'interface de ligne de commande avec **show license**). S'il s'agit d'une appliance matéri n'y a aucun champ.
SÉRIE_	Ceci sera la série COMPLÈTE de l'appliance (qui est trouvée à partir de l'interface de li de commande avec **version**).
MX00V_	TIl s'agit du modèle de l'appliance (encore une fois, à partir de **la version** de l'interface c ligne de commande). Cette valeur varie à nouveau, s'il s'agit d'un appareil virtuel par ra à un appareil matériel.
000000	Des zéros de fin. Celles-ci varieront en fonction des champs précédents, afin de termin champ de 65 caractères.

Interface utilisateur WSA

1. **Services de sécurité > Anti-programme malveillant et réputation**
2. Cliquez sur **Modifier les paramètres globaux...**
3. Dans la section *Advanced Malware and Protection Services*, développez **Advanced**
4. Développez les **paramètres avancés pour l'analyse des fichiers**

L'ID du client d'analyse de fichiers est répertorié ici.

WSA exécutant AsyncOS 9.1.1-041 pour la sécurité Web, exemple :



Remarque: Il y a une différence dans l'ID du client d'analyse de fichiers pour l'appliance virtuelle par rapport à l'appliance matérielle.

L'ID du client d'analyse de fichiers est basé sur le format de chaîne de 65 caractères suivant :

Valeur	Explication
02_	WSA
VLNWSAXXXYYY_	S'il s'agit d'un appareil virtuel, il utilise le numéro de licence VLN (qui se trouve dans l'interface de ligne de commande avec **show license**). S'il s'agit d'une appliance matérielle, il n'y a aucun champ.
SÉRIE_	Ceci sera la série COMPLÈTE de l'appliance (qui est trouvée à partir de l'interface de de commande avec **version**).
SX00V_	TIl s'agit du modèle de l'appliance (encore une fois, à partir de **la version** de l'interfac ligne de commande). Cette valeur varie à nouveau, s'il s'agit d'un appareil virtuel par rapport à un appareil matériel.
000000	Des zéros de fin. Celles-ci varieront en fonction des champs précédents, afin de terr le champ de 65 caractères.

Interface utilisateur FMC/DC

Pour obtenir la clé API (ID d'analyse de fichier) pour FMC/DC, à partir de l'exécution CLI :

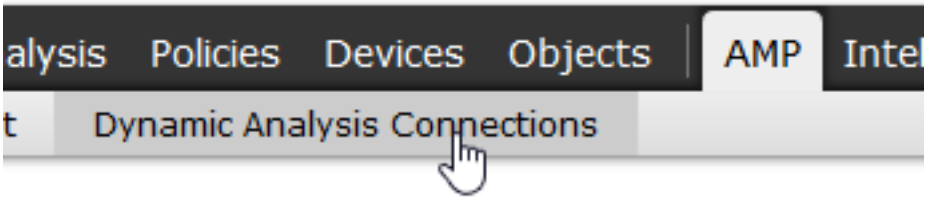
```
perl -MFlyLoader -e "print SF::Files::Analysis::get_apikey()"
```

> **Remarque:** Sur certains matériels il y a plusieurs installations de Perl. L'exécution de l'installation par défaut de Perl risque de ne pas exécuter correctement la commande. S'il y a des erreurs de sortie, spécifiez le chemin suivant, direct lors de l'appel de Perl : **/ngfw/usr/bin/perl -MFlyLoader -e « print SF::Files::Analysis::get_apikey()"**

1. Accédez à **AMP > Connexions d'analyse dynamique**
2. Sur le côté droit de l'élément de menu **panacea.mengrid.com** cliquez sur l'icône **Associer**.
3. Une fenêtre contextuelle s'affiche, cliquez sur **Oui** pour terminer l'association.
4. Vérifiez à la fin de l'URL l'ID du client d'analyse de fichiers. L'ID commence après les **périphériques%3D** jusqu'à la fin de l'URL.

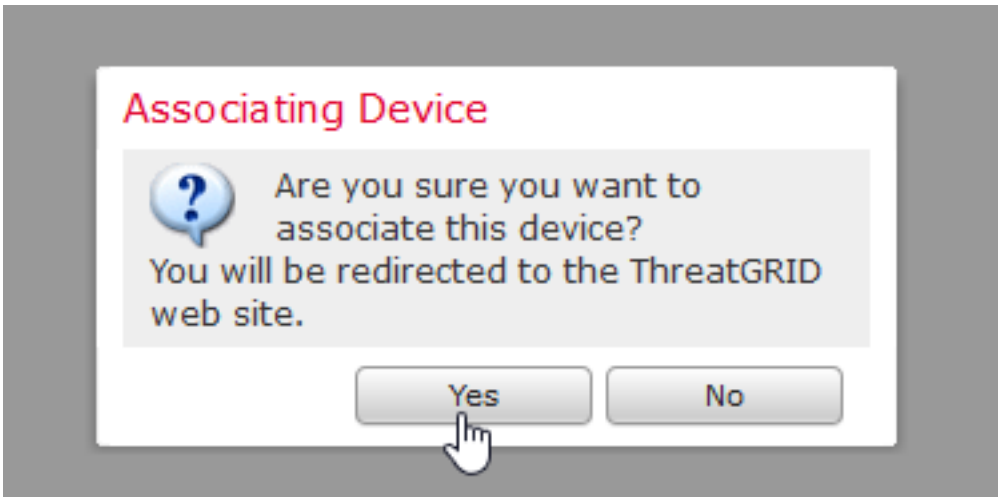
Exemple :

1. Menu Navigation



2. Associer le FMC

3. Confirmation de l'association



4. Vérification de l'ID du client d'analyse de fichiers

Comment utiliser l'ID de client dans le cloud Threat Grid

L'ID client peut ensuite être recherché dans la grille de menaces pour trouver les échantillons soumis par le périphérique.

1. Connectez-vous au portail Threat Grid (par exemple https://panacea.threatgrid.com) avec votre compte d'administrateur d'organisation.

2. Accédez à **Administration > Manage Users**.

3. Collez votre ID client dans le champ **Filtre** et appuyez sur **Retour**.

> **Astuce** : Si vous ne trouvez pas votre périphérique dans la liste, vérifiez les filtres de recherche.

4. Si le périphérique a accès au cloud, vous pouvez vous attendre à ce qu'il apparaisse dans la liste.

5. Lorsque vous cliquez sur **Connexion** du périphérique, les détails s'affichent avec la liste d'exemples.

Informations connexes

- Support et documentation techniques - Cisco Systems
- Cisco Email Security Appliance - Guides de l'utilisateur final
- Cisco Web Security Appliance - Guides de l'utilisateur final
- Cisco Security Management Appliance - Guides de l'utilisateur final
- Cisco Firepower Management Console - Guides de l'utilisateur final