

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

Contenu

[Introduction](#)

[ID client d'analyse de fichiers sur les appliances de sécurité de contenu](#)

[Interface utilisateur ESA](#)

[Interface utilisateur SMA](#)

[Interface utilisateur WSA](#)

[Interface utilisateur FMC/DC](#)

[Comment utiliser l'ID de client dans le cloud Threat Grid](#)

[Informations connexes](#)

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 :

Edit File Reputation and Analysis Settings

Advanced Malware Protection

Advanced Malware Protection services require network communication to the cloud servers on ports 32137 or 443 (for File Reputation) and 443 (for File Analysis). Please see the Online Help for additional details.

File Reputation Filtering:	<input checked="" type="checkbox"/> Enable File Reputation
File Analysis: (?)	<input checked="" type="checkbox"/> Enable File Analysis
	File Types:
	<input checked="" type="checkbox"/> Adobe Portable Document Format (PDF)
	<input checked="" type="checkbox"/> Microsoft Office 2007+ (Open XML)
	<input checked="" type="checkbox"/> Microsoft Office 97-2004 (OLE)
	<input checked="" type="checkbox"/> Microsoft Windows / DOS Executable
	<input checked="" type="checkbox"/> Other potentially malicious file types
Advanced Settings for File Reputation	Advanced settings for File Reputation
Advanced Settings for File Analysis	File Analysis Server URL: AMERICAS (https://panacea.threatgrid.com)
	File Analysis Client ID: 01_VLNESA000132_4239CEE15FF3A9F9B804-0EDD2CF4F9D9_C100V_00000000



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 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 ligne de commande avec version).
CX00V_	Il s'agit du modèle de l'appliance (encore une fois, à partir de la version de l'interface de 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 terminer 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 exemple :

File Analysis

File Analysis Client ID:	06_VLNSMA20434706_564D6D7D1766E1C23D6E-D7CAE05515F5_M100V_000000
Appliance Group ID/Name:	File Analysis Server URL: AMERICAS:https://panacea.threatgrid.com
	Group Name: <input type="text"/> <input type="button" value="Group Now"/>
	<ul style="list-style-type: none">Typically, this value will be your Cisco Connection Online ID (CCO ID).This Group Name is case-sensitive.It must be configured identically on each appliance. An appliance can belong to only one group per server.
	This change will take effect immediately, without Commit. Once grouped, this value can only be reset by Cisco support.
Grouping Details:	Not part of any group yet.



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
VLNSMAXXXYY Y_	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, n'y a aucun champ.
SÉRIE_	Ceci sera la série COMPLÈTE de l'appliance (qui est trouvée à partir de l'interface de ligne de commande avec version).
MX00V_	TII s'agit du modèle de l'appliance (encore une fois, à partir de la version de l'interface de 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 terminer le 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 :

The screenshot shows the configuration page for Advanced Malware Protection Services. Under the 'Advanced' section, the 'Advanced Settings for File Analysis' are expanded. The 'File Analysis Client ID' field is highlighted with a red arrow and contains the value: 02_64F69D7947E9-FCH1846V12S_5690_00000000000000000000000000000000.

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 ligne de commande avec version).
SX00V_	TII s'agit du modèle de l'appliance (encore une fois, à partir de la version de l'interface de 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 terminer 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 :

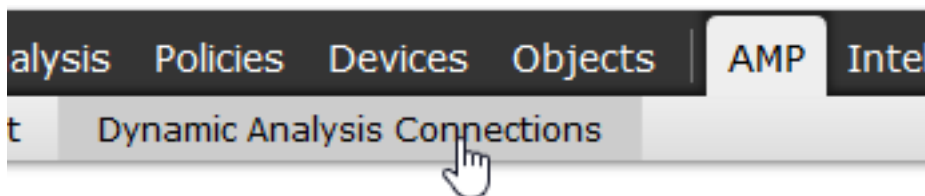
```
perl -MFlyLoader -e "print SF::Files::Analysis::get_apikey()"
```

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 :

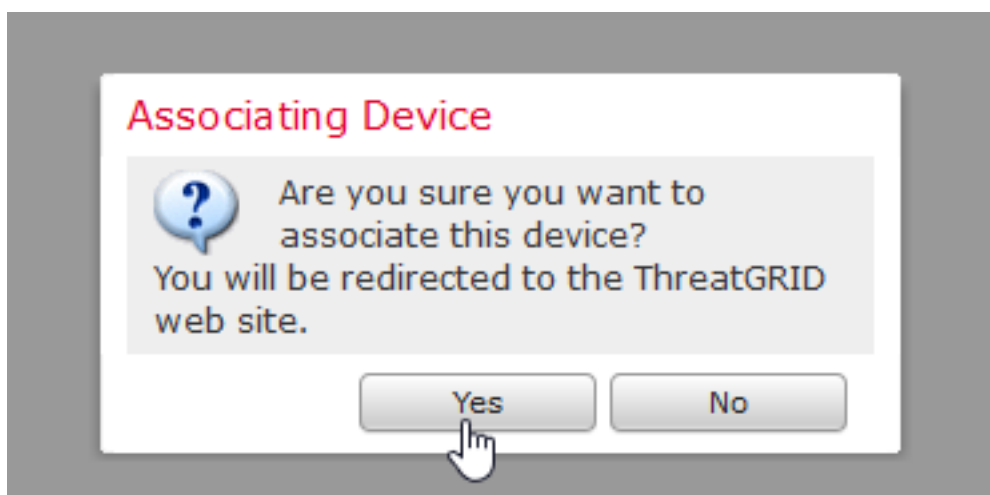
1. Menu Navigation



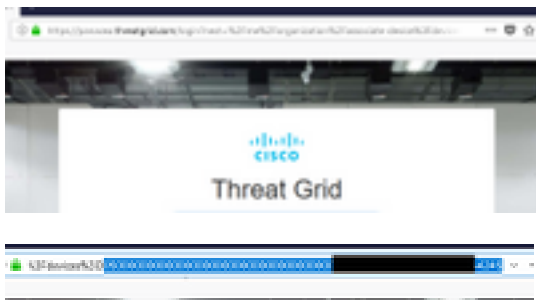
2. Associer le FMC



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](#)