

Expliquer l'ID du client d'analyse de fichiers pour la passerelle, la passerelle cloud et Email and Web Manager

Contenu

[Introduction](#)

[ID client d'analyse de fichiers pour Gateway, Cloud Gateway et Email and Web Manager](#)

[Passerelle ou passerelle cloud](#)

[Gestionnaire de messagerie et Web](#)

[Regroupement des appliances pour File Analysis Reporting](#)

[Appareils de groupe](#)

[Passerelle ou passerelle cloud](#)

[Gestionnaire de messagerie et Web](#)

[Afficher les appareils](#)

[Passerelle ou passerelle cloud](#)

[Gestionnaire de messagerie et Web](#)

[Additional Information](#)

[Documentation de Cisco Secure Email Gateway](#)

[Documentation sur Secure Email Cloud Gateway](#)

[Documentation de Cisco Secure Email and Web Manager](#)

[Analyse des programmes malveillants sécurisés Cisco](#)

[Documentation produit Cisco Secure](#)

Introduction

Ce document décrit comment rechercher l'ID client d'analyse de fichiers pour Cisco Secure Email Gateway, Cloud Gateway et Email and Web Manager. L'ID du client d'analyse de fichiers est une clé d'enregistrement unique de 65 caractères utilisée lorsque la passerelle, la passerelle cloud ou le gestionnaire de messagerie et de Web s'enregistre auprès de Cisco Malware Analytics (anciennement Threat Grid) pour l'envoi de fichiers et le sandboxing. Par exemple, si vous avez activé le service d'analyse de fichiers et que le service de réputation ne dispose d'aucune information sur la pièce jointe trouvée dans un message, et que la pièce jointe répond aux critères des fichiers pouvant être analysés ([voir Fichiers pris en charge pour File Reputation et Analysis Services](#)), le message peut être mis en quarantaine ([voir Mise en quarantaine des messages avec pièces jointes envoyées pour analyse](#)) et le fichier envoyé pour analyse.

Pour « Regroupement d'appliances pour l'analyse de fichiers et le reporting », assurez-vous que vous connaissez vos ID d'analyse de fichiers.

Pour plus d'informations, reportez-vous au chapitre « Filtrage par réputation de fichiers et analyse de fichiers » du Guide de l'utilisateur :

- [Guides d'utilisation de Cisco Secure Email Gateway](#)

- [Guides d'utilisation de la passerelle cloud de messagerie sécurisée Cisco](#)

ID client d'analyse de fichiers pour Gateway, Cloud Gateway et Email and Web Manager

L'ID du client d'analyse de fichiers est automatiquement généré pour les appliances lorsque vous activez l'analyse de fichiers.

Avant de commencer à utiliser la passerelle ou la passerelle cloud, assurez-vous que vous disposez des clés de fonction nécessaires et que vous avez activé les fonctions File Reputation et File Analysis. Pour afficher vos touches de fonction, accédez à **Administration système > Touches de fonction**. La réputation et l'analyse des fichiers sont répertoriées séparément et ont l'état Actif.

Passerelle ou passerelle cloud

1. Connectez-vous à l'interface utilisateur.
2. Accédez à **Services de sécurité > File Reputation and Analysis**.
3. Cliquez sur **Modifier les paramètres généraux...**
4. Développez **Advanced Settings for File Analysis**.

L'ID du client d'analyse de fichier est indiqué ici.

Exemple :

Edit File Reputation and Analysis Settings

Advanced Malware Protection

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

File Reputation Filtering: Enable File Reputation

File Analysis: Enable File Analysis

Select All Expand All Collapse All Reset

- Archived and compressed
- Configuration
- Database
- Document
- Email
- Encoded and Encrypted
- Executables
- Microsoft Documents
- Miscellaneous

Advanced Settings for File Reputation

Advanced Settings for File Analysis

File Analysis Server URL: AMERICAS (https://panacea.threatgrid.com)

File Analysis Client ID: 01_VLNESA -423AA9781B67 -25CC6 -C600V_000000

Proxy Settings: Use File Reputation Proxy

Server: Port:

Username:

Passphrase:

Retype Passphrase:

Cache Settings Advanced settings for Cache

Threshold Settings Advanced Settings for File Analysis Threshold Score

Note: Il existe une différence entre l'ID du client d'analyse de fichier pour les appliances virtuelles et les appliances matérielles.

L'ID du client d'analyse de fichiers pour la passerelle ou la passerelle cloud est basé sur un format de chaîne de 65 caractères :

Valeur	Explication
01_	«01 » est spécifique à la passerelle ou à la passerelle cloud.
VLNESAXXYYYY_	S'il s'agit d'un appareil virtuel, il utilise le numéro de licence VLAN (trouvé à partir de la commande CLI showlicense). S'il s'agit d'une appliance matérielle, il n'y a aucun caractère.
SERIAL_	Série COMPLÈTE du matériel.
CX00V_	Modèle de l'appliance.
00000000	Zéros de champ. En fonction des champs précédents, ceux-ci varient pour terminer le champ de 65 caractères.

Gestionnaire de messagerie et Web

1. Connectez-vous à l'interface utilisateur.
2. Accédez à **Gestion centralisée > Appliance de sécurité**.

Au bas de cette page se trouve la section Analyse de fichiers. L'ID du client d'analyse de fichier est indiqué ici.

Exemple :

Security Appliances

Centralized Service Status	
Spam Quarantine:	Enabled, using 1 license
Policy, Virus and Outbreak Quarantines:	Enabled, using 1 license
	Alternate Quarantine Release Appliance (?) : esa5 Specify Alternate Release Appliance...
Centralized Email Reporting:	Enabled, using 1 license
Centralized Email Message Tracking:	Enabled, using 1 license
Centralized Web Configuration Manager:	Service disabled
Centralized Web Reporting:	Service disabled
Centralized Upgrades for Web:	Service disabled

Security Appliances							
Email							
Add Email Appliance...							
Appliance Name	IP Address or Hostname	Services				Connection Established?	Delete
		Spam Quarantine	Policy, Virus and Outbreak Quarantines	Reporting	Tracking		
■	■	✓	✓	✓	✓	Yes	
Web							
No centralized services are currently available.							

File Analysis	
File Analysis Client ID:	06_VLNSMA ■_420D5DE07A468■ -006DAF ■_M300V_00000000
Appliance Group ID/Name:	File Analysis Server URL: <input type="text" value="AMERICAS:https://panacea.threatgrid.com"/> Group Name: <input type="text"/> 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. <p>This change will take effect immediately, without Commit. Once grouped, this value can only be reset by Cisco support.</p>
Grouping Details:	You can use any appliance in a group to view detailed File Analysis results in the cloud for files uploaded from any appliance in the group. View Appliances in Group

Note: Il existe une différence entre l'ID du client d'analyse de fichier pour les appliances virtuelles et les appliances matérielles.

L'ID du client d'analyse de fichiers pour Email and Web Manager est basé sur un format de chaîne de 65 caractères :

Valeur	Explication
06_	"06" est spécifique au gestionnaire de messagerie et de Web.
VLNSMAXXXYY	S'il s'agit d'un appareil virtuel, il utilise le numéro de licence VLAN (trouvé à partir de la commande CLI showlicense). S'il s'agit d'une appliance matérielle, il n'y a aucun champ
Y_	
SERIAL_	Série COMPLÈTE du matériel.
MX00V_	Modèle de l'appliance.
000000	Zéros de champ. En fonction des champs précédents, ceux-ci varient pour terminer le champ de 65 caractères.

Regroupement des appliances pour File Analysis Reporting

Si votre licence inclut l'accès à Cisco Secure Malware Analytics (<https://panacea.threatgrid.com>), la meilleure pratique pour votre passerelle ou Cloud Gateway est de les associer au compte de votre entreprise. Pour permettre à toutes les appliances de sécurité du contenu de votre organisation d'afficher dans le cloud des résultats détaillés sur les fichiers envoyés pour analyse depuis n'importe quelle passerelle ou passerelle cloud de votre organisation, vous devez joindre toutes les appliances au même groupe d'appliances. Lorsque vous vous connectez à Malware Analytics, vos envois et les échantillons de menaces envoyés au cloud pour analyse sont tous affichés dans le tableau de bord Malware Analytics de votre organisation.

Note: Les clients de Cloud Gateway ont configuré cette fonctionnalité lors des activations et du déploiement effectués par Cisco.

Appareils de groupe

Note: Si vous disposez d'une passerelle cloud et que cette opération n'est pas terminée, ouvrez un dossier d'[assistance](#) avant de configurer un ID/nom de groupe d'appareils.

Passerelle ou passerelle cloud

1. Dans l'interface utilisateur, accédez à **Security Services > File Reputation and Analysis**.
2. Cliquez sur **Cliquez ici pour regrouper ou afficher les appliances pour le reporting d'analyse de fichiers**.
3. Saisissez votre **ID/nom de groupe d'appareils**. Les valeurs par défaut sont : Il est conseillé d'utiliser votre CCOID pour cette valeur. Un appareil ne peut appartenir qu'à un seul groupe. Après avoir configuré la fonction Analyse de fichiers, vous pouvez ajouter une machine à un groupe.
4. Cliquez sur **Grouper maintenant**.

Gestionnaire de messagerie et Web

Note: L'option permettant de configurer un ID/nom de groupe d'appiances n'est disponible qu'une fois que le Gestionnaire de messagerie et de sites Web a ajouté une appliance de messagerie à des fins de gestion centralisée et a migré les quarantaines des stratégies, des virus et des attaques.

1. Dans l'interface utilisateur, accédez à **Centralized Services > Security Appliances**. Saisissez votre **ID/nom de groupe d'appareils**. Les valeurs par défaut sont :En général, cette valeur correspond à votre ID Cisco Connection Online (ID CCO).Ce nom de groupe est sensible à la casse.Il doit être configuré de manière identique sur chaque appliance. Une appliance ne peut appartenir qu'à un seul groupe par serveur.
2. Cliquez sur **Grouper maintenant**.

Remarque :

- Lorsque vous ajoutez un ID de groupe, il prend effet immédiatement, sans validation. Si vous devez modifier un ID de groupe, vous devez contacter le TAC Cisco.
- Ce nom est sensible à la casse et doit être configuré de manière identique sur chaque appliance du groupe d'analyse.

Afficher les appareils

Passerelle ou passerelle cloud

1. Dans l'interface utilisateur, accédez à **Security Services > File Reputation and Analysis**.
2. Cliquez sur **Cliquez ici pour regrouper ou afficher les appliances pour le reporting d'analyse de fichiers**.
3. Cliquez sur **View Appliances**.

Gestionnaire de messagerie et Web

1. Dans l'interface utilisateur, accédez à **Centralized Services > Security Appliances**.
2. Cliquez sur **View Appliances in Group** dans la section File Analysis.

L'ID client d'analyse de fichiers de toutes les appliances associées à l'ID/au nom du groupe d'appiances est répertorié ici.

Exemple :

Appliance Grouping for File Analysis Reporting.

Appliance Grouping for File Analysis Reporting

Appliance Group ID/Name: ?

Cancel

Change Group

View Appliances

List of Appliances in the Group: (https://panacea.threatgrid.com)

Number	File Analysis Client ID
1	01_7C0EC-FCH: _C380_00000000000000000000000000000000
2	01_EC2B20195 -FB7E4' _C300V_00000000000000000000000000000000
3	01_VLNESA _4239CEE15 -0EDD _C100V_00000000
4	01_VLNESA _564D9931D -9-1856 _C100V_00000000
5	01_VLNESA _420D4F3 -B4F-B9 _1_C300V_000000
6	01_VLNESA _420DF63 -17-A5 _C_100V_000000
7	01_VLNESA _423A11C -9AA-20 _A_C100V_000000
8	01_VLNESA _423AA97 -AAE-25 _33_C600V_000000
9	01_VLNESA _564D3DE -AFFD-9: _F9_C100V_000000
10	01_VLNESA _564DA24 -97E-EA _3D_C100V_000000
11	01_VLNESA _564D78E -E52-6C _2_C100V_000000
12	01_VLNESA _420D39D -7D6-62 _24_C100V_000000
13	01_VLNESA _423A59C -22E-8B _9_C100V_000000
14	01_VLNESA _4239CEE -04-0E _9_C100V_000000
15	01_VLNESA _4216676B -28-A95 _C_100V_000000
16	01_VLNESA _423F2B99 -38-776 _C100V_000000
17	01_VLNESA _420D39DE -D6-62 _4_C100V_000000
18	01_VLNESA _420D4E75 -E3-0A _C_100V_000000
19	01_VLNESA _423A09B8 -5A-5B6 _C100V_000000
20	01_VLNESA _423A59C6 -2E-8B _C100V_000000
21	06_VLNSMA _420D5DE0: -4-0060 _M300V_00000000
22	06_VLNSMA _420D4B6 -C57-CE _9C_M100V_000000
23	06_VLNSMA _420D538E -9F-8FC _M100V_000000
24	06_VLNSMA _420D704E -62-17F _M100V_000000
25	06_VLNSMA _420D8737 -34-608 _M100V_000000
26	06_VLNSMA _420DEE32 -4B-F5C _2_M100V_000000

OK

Additional Information

Documentation de Cisco Secure Email Gateway

- [notes de version](#)
- [Guide de l'utilisateur](#)
- [Guide de référence CLI](#)
- [Guides de programmation API pour Cisco Secure Email Gateway](#)
- [Open Source utilisé dans Cisco Secure Email Gateway](#)
- [Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco \(inclut vESA\)](#)

Documentation sur Secure Email Cloud Gateway

- [notes de version](#)
- [Guide de l'utilisateur](#)

Documentation de Cisco Secure Email and Web Manager

- [Notes de version et matrice de compatibilité](#)
- [Guide de l'utilisateur](#)
- [Guides de programmation API pour Cisco Secure Email and Web Manager](#)
- [Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco](#) (inclut vSMA)

Analyse des programmes malveillants sécurisés Cisco

- [Cisco Secure Malware Analytics \(Threat Grid\)](#)

Documentation produit Cisco Secure

- [Architecture d'attribution de noms Cisco Secure](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.