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

## Contenu



## 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 (voirFichiers pris en charge pour File Reputation et Analysis Services), le message peut être mis en quarantaine (voirMise 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.

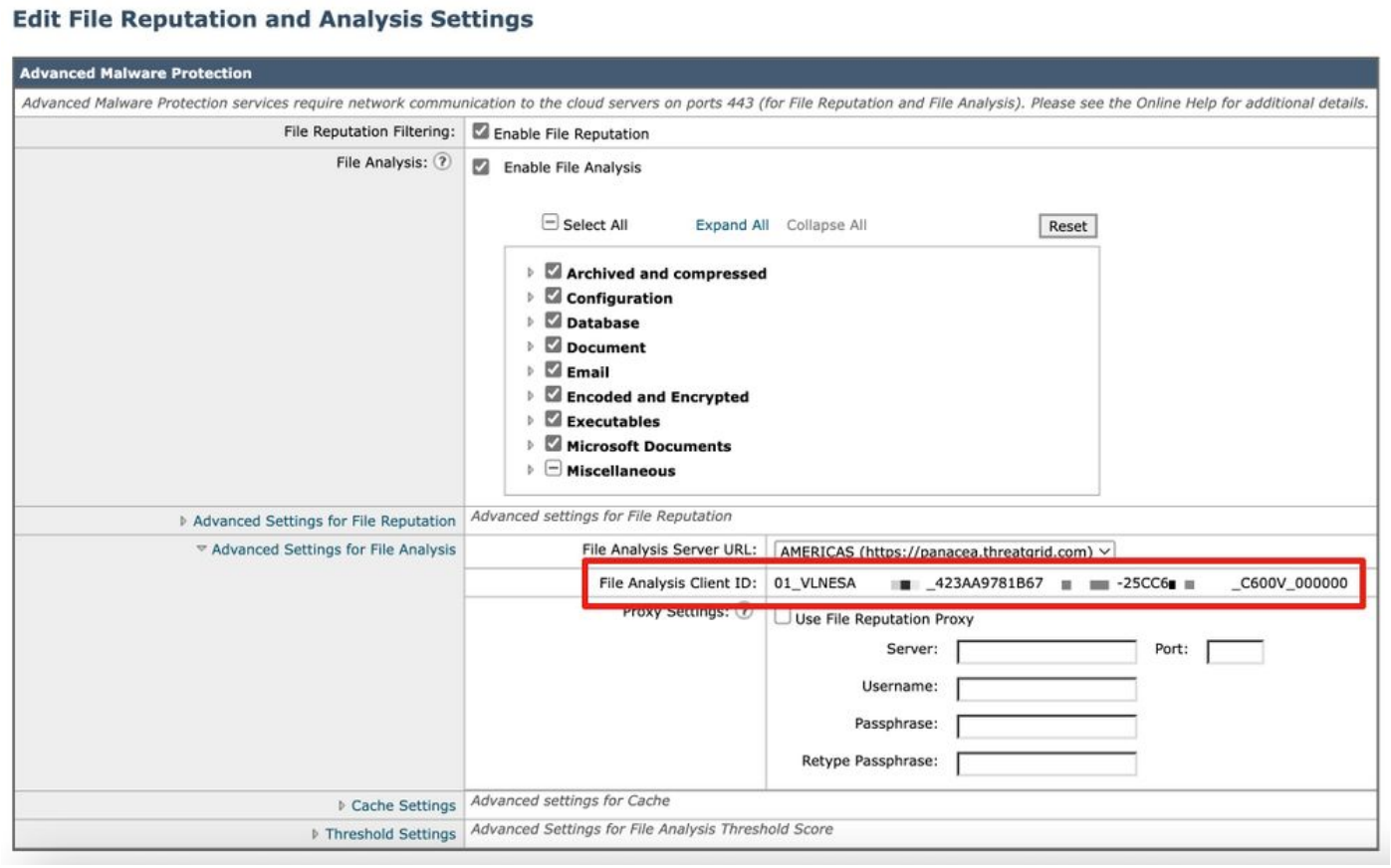
Avant de commencer à utiliser la passerelle ou la passerelle cloud, assurez-vous que vous disposez des clés de fonction nécessaires et que vous avez activé les fonctions File Reputation et File Analysis. Pour afficher vos touches de fonction, accédez à **Administration système > Touches de fonction**. 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.

EExemple :




**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 :

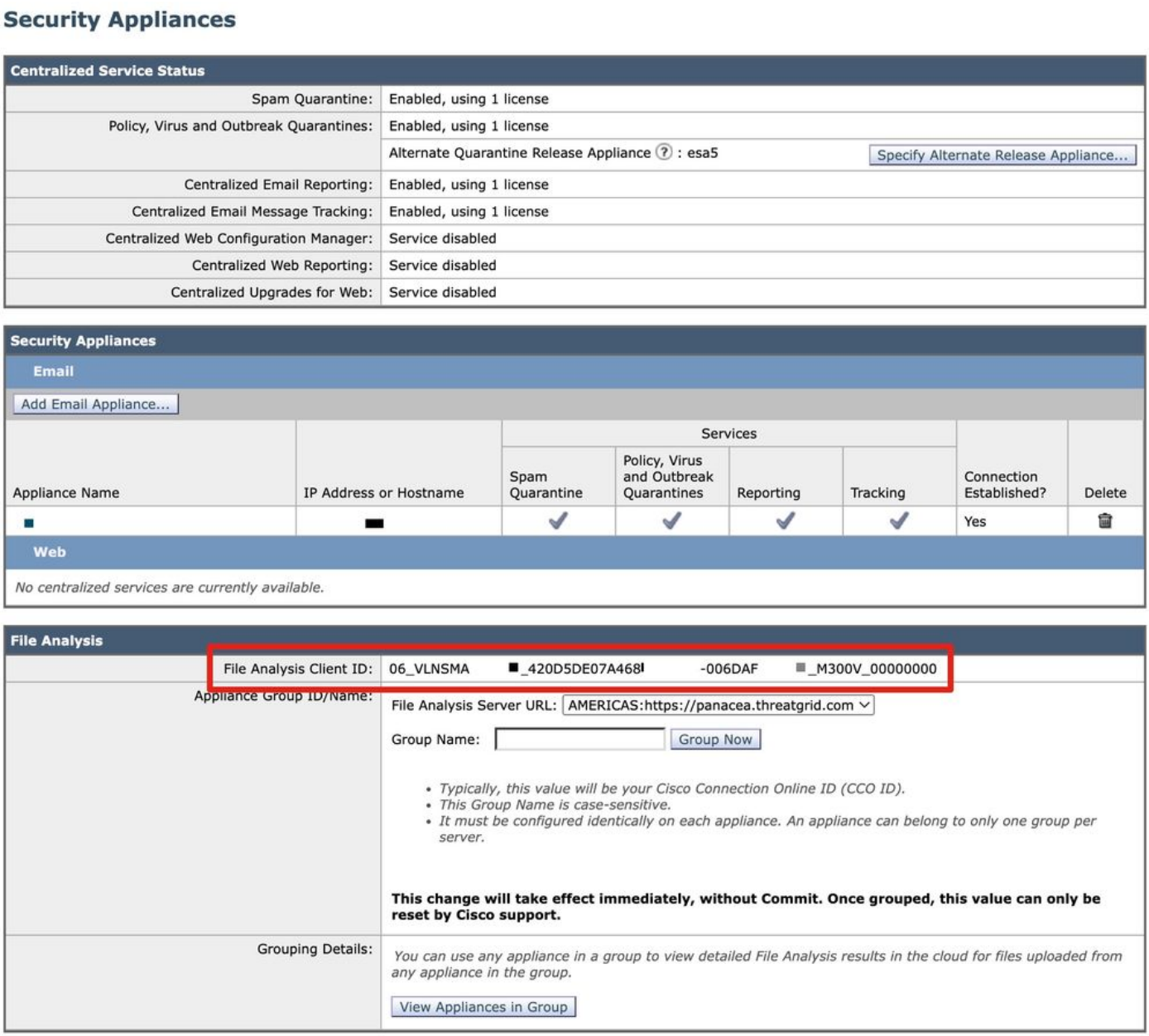
| Valeur | Explication |
| --- | --- |
| 01_ | «01 » est spécifique à la passerelle ou à la passerelle cloud. |
| VLNESAXXXYYY_ | S'il s'agit d'un appareil virtuel, il utilise le numéro de licence VLAN (trouvé à partir de l commande CLI **showlicense**). S'il s'agit d'une appliance matérielle, il n'y a aucun char |
| 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 :




**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 Y_ | 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 |
| 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'appliances 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

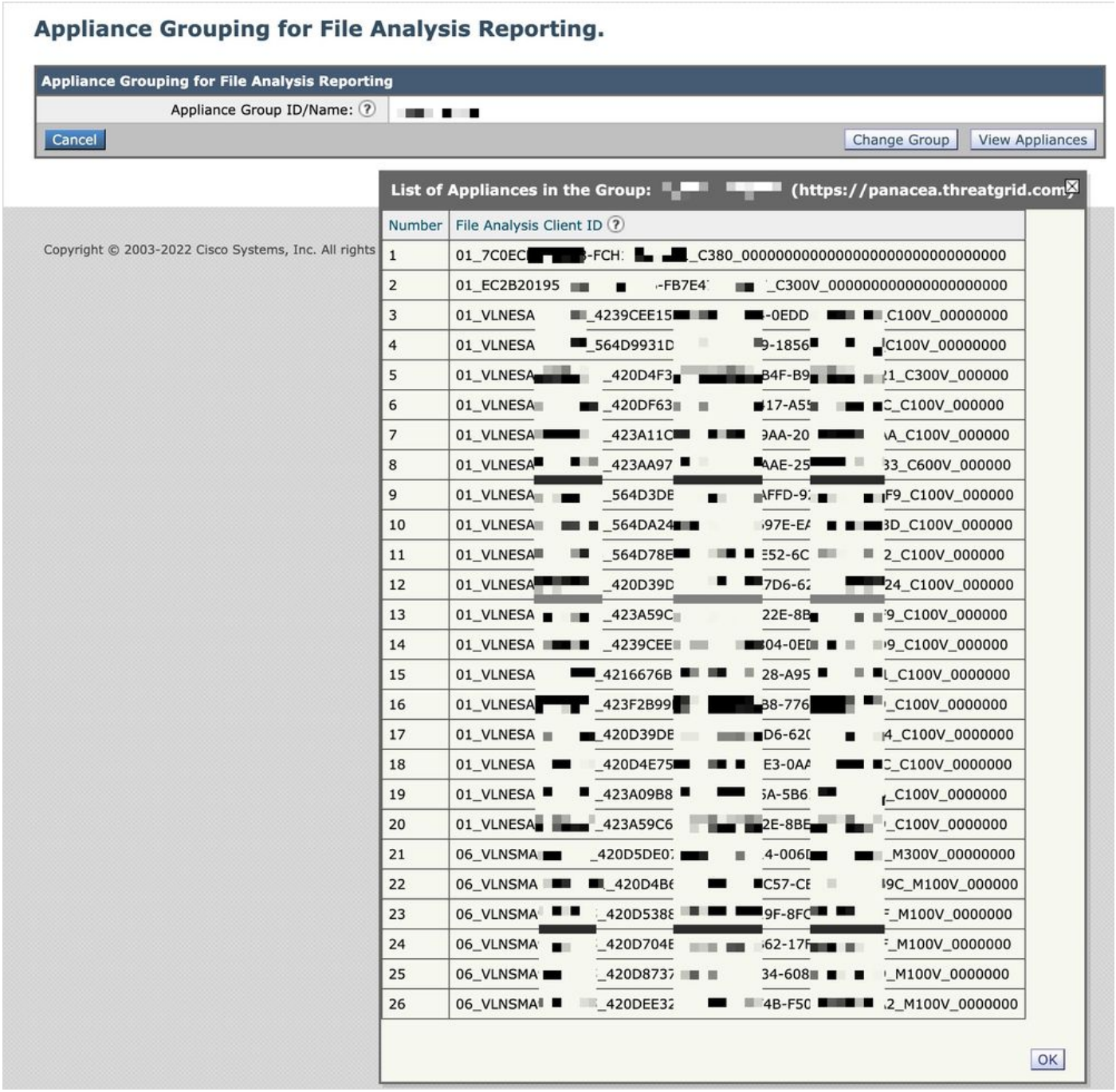
1. Dans l'interface utilisateur, accédez à **Security Services > File Reputation and Analysis.**
2. Cliquez sur **Cliquez ici pour regrouper ou afficher les appliances pour le reporting d'analyse de fichiers**.
3. Cliquez sur **View Appliances**.

### 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'appliances est répertorié ici.

Exemple :




# 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.