ゲートウェイ、クラウドゲートウェイ、EメールおよびWebマネージャのファイル分析クライアントIDについて説明する

内容

概要
ゲートウェイ、クラウドゲートウェイ、EメールおよびWebマネージャのファイル分析クライアントID
ゲートウェイまたはクラウドゲートウェイ
EメールおよびWebマネージャ
File Analysis Reportingのアプライアンス・グループ化
グループアプライアンス
ゲートウェイまたはクラウドゲートウェイ
EメールおよびWebマネージャ
アプライアンスの表示
ゲートウェイまたはクラウドゲートウェイ
EメールおよびWebマネージャ
追加情報
Cisco Secure Email Gatewayのドキュメント
Secure Email Cloud Gatewayドキュメント
Cisco Secure Email and Web Managerのドキュメント
Cisco SecureX Malware Analytics
Cisco Secure製品ドキュメント

概要

このドキュメントでは、Cisco Secure Email Gateway、Cloud Gateway、およびEmail and Web Managerのファイル分析クライアントIDを見つける方法について説明します。File Analysis Client IDは一意の65文字の登録キーで、Gateway、Cloud Gateway、またはEmail and Web ManagerをCisco Malware Analytics（以前のThreat Grid）に登録してファイルの送信やサンドボックスに使用します。たとえば、File Analysisサービスを有効にしていて、レピュテーションサービスがメッセージ内の添付ファイルに関する情報を持たず、その添付ファイルが分析可能なファイルの基準を満たしている場合(「Supported Files for File Reputation and Analysis Services」を参照)、メッセージを検疫し(「Quarantining Messages with Attachments Sent for Analysis」を参照)、ファイルを分析に送信できます。

「Appliance Grouping for File Analysis Reporting」では、ファイル分析IDを確認してください。

詳細については、ユーザガイドの「ファイルレピュテーションフィルタリングとファイル分析」の章を参照してください。

- Cisco Secure Email Gatewayエンドユーザガイド
- Cisco Secure Email Cloud Gatewayエンドユーザガイド

ゲートウェイ、クラウドゲートウェイ、EメールおよびWebマネージャのファイル分析クライアントID

ファイル分析を有効にすると、アプライアンスのファイル分析クライアントIDが自動的に生成されます。

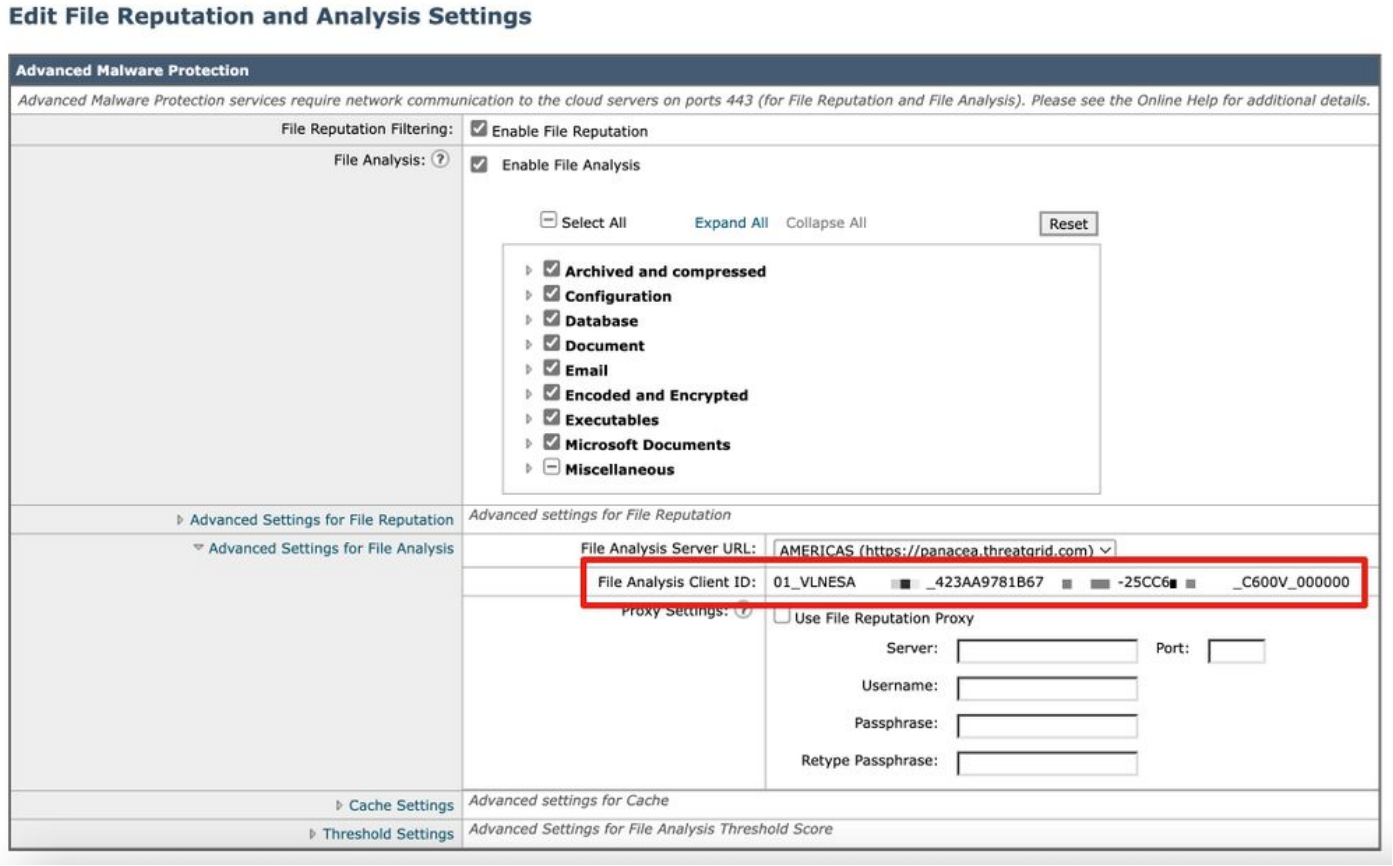
ゲートウェイまたはクラウドゲートウェイから開始する前に、必要な機能キーがあり、ファイルレピュテーションとファイル分析が有効になっていることを確認してください。機能キーを表示するには、[System Administration] > [Feature Keys] に移動します。ファイルレピュテーションとファイル分析は別々に表示され、ステータスは[Active]になっています。

ゲートウェイまたはクラウドゲートウェイ

1. ユーザインターフェイスにログインします。
2. [Security Services] > [File Reputation and Analysis] に移動します。
3. [Edit Global Settings...] をクリックします。
4. [Advanced Settings for File Analysis] を展開します。

ファイル分析クライアントIDが表示されます。

E例：



注：仮想アプライアンスとハードウェアアプライアンスのファイル分析クライアントIDには違いがあります。

ゲートウェイまたはクラウドゲートウェイのファイル分析クライアントIDは、65文字の文字列形式に基づいています。

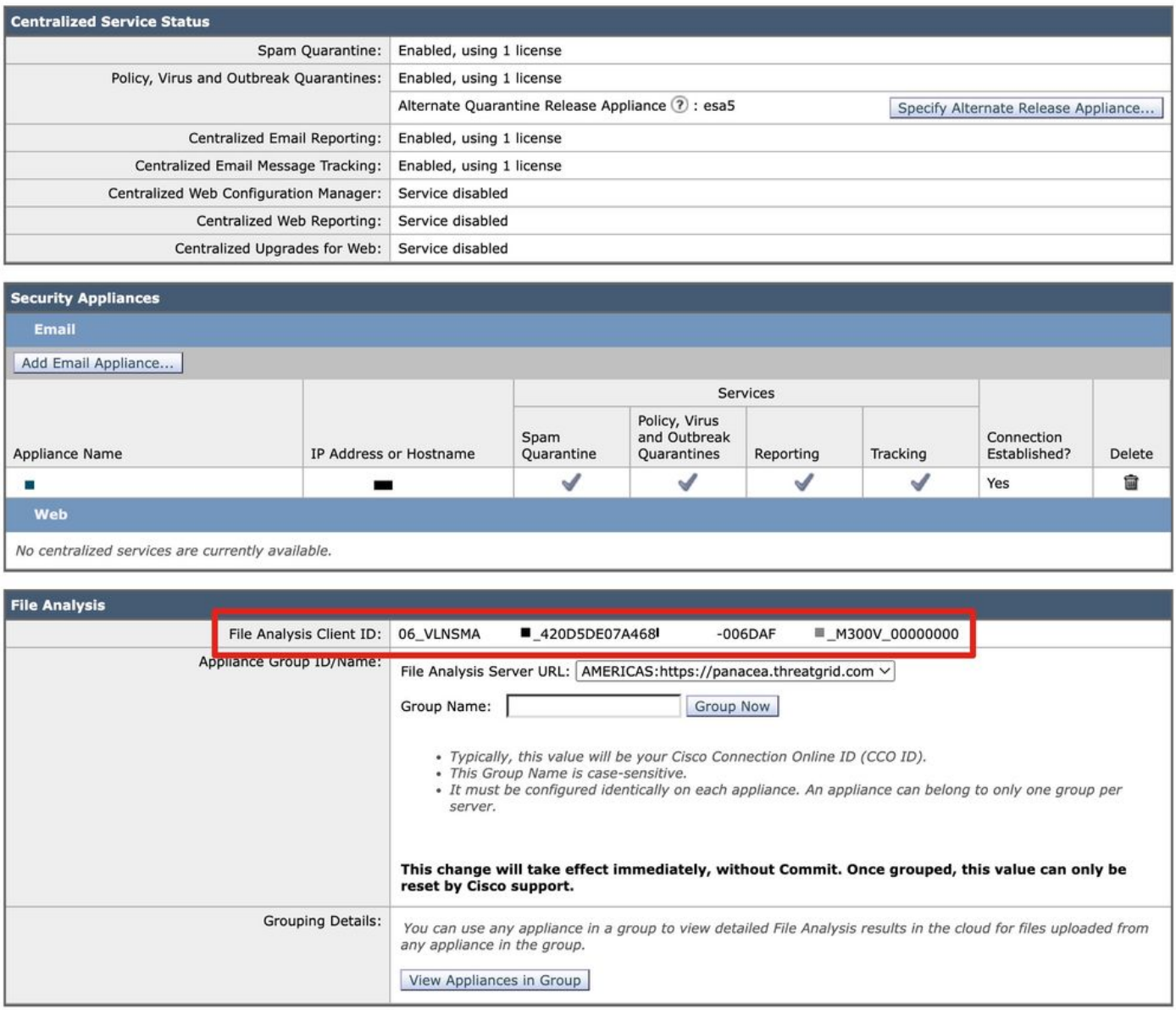
値	説明
01_	「01」はゲートウェイまたはクラウドゲートウェイに固有です。
VLNEAXXXYYY_	これが仮想アプライアンスの場合は、VLNライセンス番号(CLIコマンドshowlicenseか ハードウェアアプライアンスの場合、フィールドはありません。
シリアル_	アプライアンスのフルシリアル。
CX00V_	アプライアンスのモデル。
00000000	フィールドのゼロ。前のフィールドに基づいて、これらは65文字のフィールドを完了

EメールおよびWebマネージャ

1. ユーザインターフェイスにログインします。
2. [Centralized Management] > [Security Appliance] に移動します。

このページの下部には、[File Analysis]セクションがあります。ファイル分析クライアントIDが表示されます。

例：



注：仮想アプライアンスとハードウェアアプライアンスのファイル分析クライアントIDには違いがあります。

Email and Web ManagerのFile Analysis Client IDは、65文字の文字列フォーマットに基づいています。

値	説明
06_	「06」はEメールおよびWebマネージャに固有です。
VLNSMAXXXYYY_	これが仮想アプライアンスの場合は、VLNライセンス番号(CLIコマンド**showlicense**から得)を使用します。 ハードウェアアプライアンスの場合、フィールドはありません。
シリアル_	アプライアンスのフルシリアル。
MX00V_	アプライアンスのモデル。
000000	フィールドのゼロ。前のフィールドに基づいて、これらは65文字のフィールドを完了するように変化します。

File Analysis Reportingのアプライアンス・グループ化

ライセンスにCisco Secure Malware Analytics(https://panacea.threatgrid.com)へのアクセスが含まれている場合、ゲートウェイまたはクラウドゲートウェイのベストプラクティスは、これらを個々の組織アカウントに関連付けることです。組織内のすべてのコンテンツセキュリティアプライアンスで、組織内の任意のゲートウェイまたはクラウドゲートウェイから分析用に送信されたファイルに関する詳細な結果をクラウドに表示できるようにするには、すべてのアプライアンスを同じアプライアンスグループに参加させる必要があります。Malware Analyticsに口グインすると、分析用にクラウドに送信された提出物と脅威サンプルがすべて、組織のMalware Analyticsダッシュボードに表示されます。

注：Cloud Gatewayをご利用のお客様は、シスコによるアクティベーションと導入の際にこの設定を行います。

グループアプライアンス

注：クラウドゲートウェイを使用していて、この作業が完了していない場合は、アプライアンスグループIDおよび名前を設定する前にサポートケースをオープンしてください。

ゲートウェイまたはクラウドゲートウェイ

1. ユーザインターフェイスから、[Security Services] > [File Reputation and Analysis] に移動します。
2. [Click here to group or view appliances for File Analysis reporting] をクリックします。
3. **アプライアンスグループID/名前**を入力します。デフォルトの値は次のとおりです。 この値にはCCOIDを使用することを推奨します。アプライアンスは1つのグループにのみ属することができます。ファイル分析機能を設定した後、マシンをグループに追加できます。
4. [Group Now] をクリックします。

EメールおよびWebマネージャ

注：アプライアンスグループID/名前を設定するオプションは、EメールおよびWeb

Managerに集中管理目的でEメールアプライアンスが追加され、ポリシー、ウイルス、アウトブレイク隔離が移行された後にのみ使用できます。

1. ユーザインターフェイスから、[Centralized Services] > [Security Appliances] に移動します。 **アプライアンスグループID/名前**を入力します。デフォルトの値は次のとおりです。通常、この値はCisco Connection Online ID(CCO ID)です。このグループ名では大文字と小文字が区別されます。各アプライアンスで同じように設定する必要があります。アプライアンスは、サーバごとに1つのグループにのみ属することができます。
2. [Group Now] をクリックします。

注：

- グループIDを追加すると、コミットなしで直ちに有効になります。グループIDを変更する必要がある場合は、Cisco TACにお問い合わせください。
- この名前では大文字と小文字が区別されるため、分析グループ内の各アプライアンスで同じように設定する必要があります。

アプライアンスの表示

ゲートウェイまたはクラウドゲートウェイ

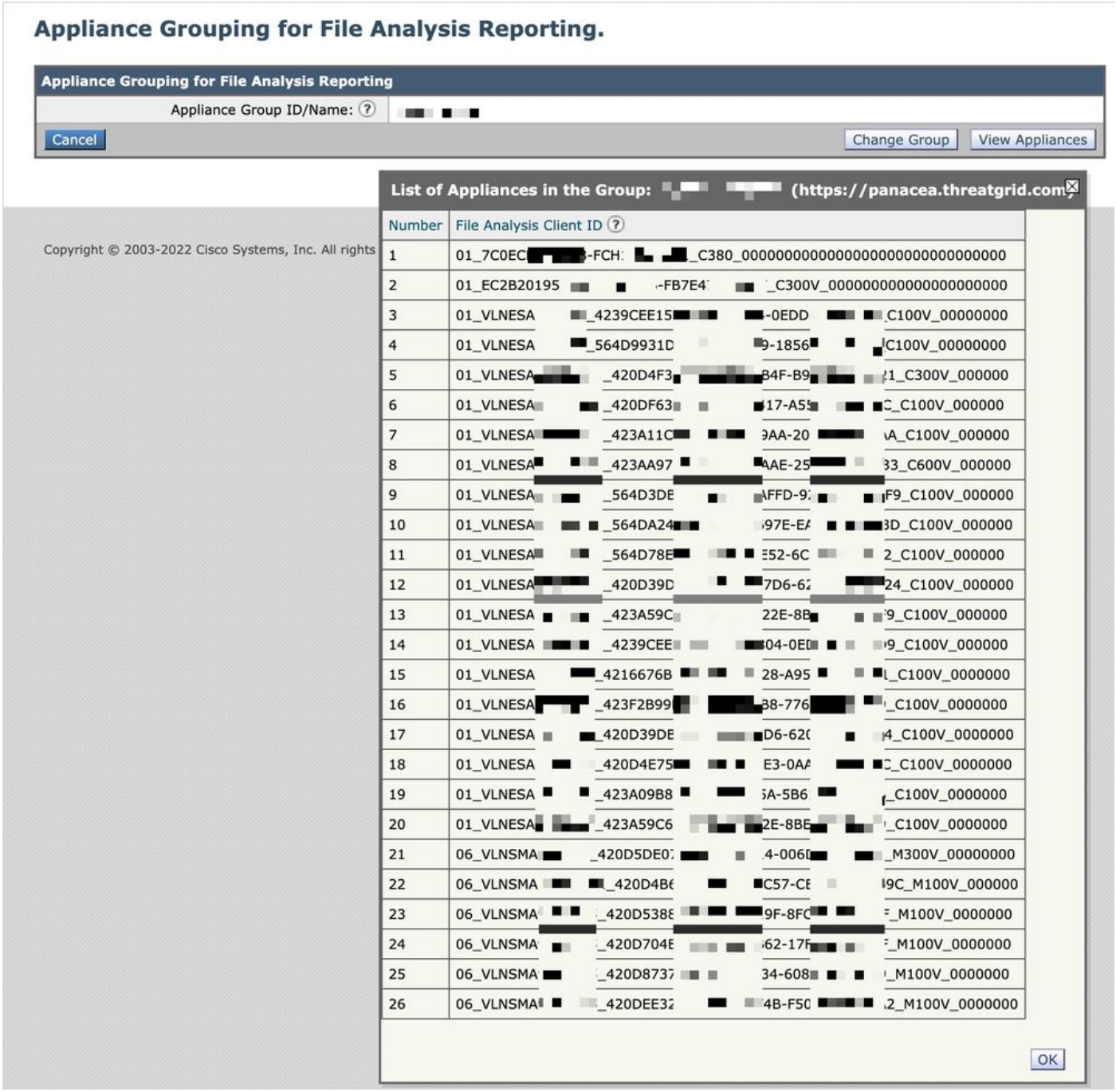
1. ユーザインターフェイスから、[**Security Services**] > [**File Reputation and Analysis**]**に移動します。**
2. [Click here to group or view appliances for File Analysis reporting] をクリックします。
3. [View Appliances] をクリックします。

EメールおよびWebマネージャ

1. ユーザインターフェイスから、[Centralized Services] > [Security Appliances] に移動します。
2. [File Analysis]セクションで[View Appliances in Group] をクリックします。

アプライアンスグループID/名前に関連付けられたすべてのアプライアンスのファイル分析クライアントIDを次に示します。

例：



追加情報

Cisco Secure Email Gatewayのドキュメント

- リリース ノート
- ユーザガイド
- CLIリファレンスガイド
- Cisco Secure Email GatewayのAPIプログラミングガイド
- Cisco Secure Email Gatewayで使用されるオープンソース
- Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド（vESAを含む）

Secure Email Cloud Gatewayドキュメント

- リリース ノート
- ユーザガイド

Cisco Secure Email and Web Managerのドキュメント

- リリースノートと互換性マトリクス
- ユーザガイド
- Cisco Secure Email and Web ManagerのAPIプログラミングガイド
- Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド（vSMAを含む）

Cisco SecureX Malware Analytics

- Cisco Secure Malware Analytics(Threat Grid)

Cisco Secure製品ドキュメント

- Cisco Secureポートフォリオの命名アーキテクチャ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。