

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のアプリアンス・グループ化](#)

[グループアプリアンス](#)

[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](#)

[アプリアンスの表示](#)

[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る、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. ユーザー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：

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

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が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. ユーザー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：

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

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。
VLNSMAXXXYY	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にログインすると、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. ユーザー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：

Appliance Grouping for File Analysis Reporting.

Appliance Grouping for File Analysis Reporting

Appliance Group ID/Name: [?] [] [] []

Cancel Change Group View Appliances

Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved.

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_00000000000000000000000000
3	01_VLNESA []_4239CEE15 [] -0EDD []_C100V_00000000
4	01_VLNESA []_564D9931D [] 9-1856 []_C100V_00000000
5	01_VLNESA []_420D4F3 []_B4F-B9 []_C100V_00000000
6	01_VLNESA []_420DF63 []_17-A5 []_C100V_00000000
7	01_VLNESA []_423A11C []_9AA-20 []_C100V_00000000
8	01_VLNESA []_423AA97 []_AAE-25 []_33_C600V_00000000
9	01_VLNESA []_564D3DE []_AFFD-9 []_F9_C100V_00000000
10	01_VLNESA []_564DA24 []_97E-EA []_3D_C100V_00000000
11	01_VLNESA []_564D78E []_E52-6C []_2_C100V_00000000
12	01_VLNESA []_420D39D []_7D6-62 []_24_C100V_00000000
13	01_VLNESA []_423A59C []_22E-8B []_9_C100V_00000000
14	01_VLNESA []_4239CEE []_04-0E []_9_C100V_00000000
15	01_VLNESA []_4216676B []_28-A95 []_C100V_00000000
16	01_VLNESA []_423F2B99 []_38-776 []_C100V_00000000
17	01_VLNESA []_420D39DE []_D6-62 []_4_C100V_00000000
18	01_VLNESA []_420D4E75 []_E3-0A []_C100V_00000000
19	01_VLNESA []_423A09B8 []_5A-5B6 []_C100V_00000000
20	01_VLNESA []_423A59C6 []_2E-8B []_C100V_00000000
21	06_VLNSMA []_420D5DE0 []_4-006 []_M300V_00000000
22	06_VLNSMA []_420D4B []_C57-CE []_9C_M100V_00000000
23	06_VLNSMA []_420D538 []_9F-8FC []_M100V_00000000
24	06_VLNSMA []_420D704E []_62-17 []_M100V_00000000
25	06_VLNSMA []_420D8737 []_34-608 []_M100V_00000000
26	06_VLNSMA []_420DEE32 []_4B-F5C []_2_M100V_00000000

OK

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。