解釋網關、雲網關以及電子郵件和網路管理器的檔案分析客戶端ID

目錄

簡介

本文檔介紹如何查詢Cisco Secure Email Gateway、Cloud Gateway以及Email and Web Manager的檔案分析客戶端ID。File Analysis Client ID是一個唯一的65個字元的註冊金鑰，當網關、雲網關或電子郵件和Web管理器註冊到Cisco Malware Analytics（以前稱為Threat Grid）進行檔案提交和沙盒處理時使用。例如，如果您已啟用File Analysis服務，而reputation服務沒有有關在郵件中找到的檔案附件的資訊，並且檔案附件符合可分析檔案的標準(請參閱Supported Files for File Reputation and Analysis Services)，則郵件將被隔離(請參閱Quarantining Messages with Attachments Sent for Analysis)，並且檔案將傳送以供分析。

對於「檔案分析報告的裝置分組」，請確保您知道檔案分析ID。

有關完整的詳細資訊，請參閱《使用手冊》的「檔案信譽過濾和檔案分析」一章：

- Cisco Secure Email Gateway最終使用手冊
- Cisco Secure Email Cloud Gateway最終使用手冊

網關、雲網關以及電子郵件和網路管理器的檔案分析客戶端ID

啟用「檔案分析」(File Analysis)時，會自動為裝置生成「檔案分析客戶端ID」(File Analysis Client ID)。

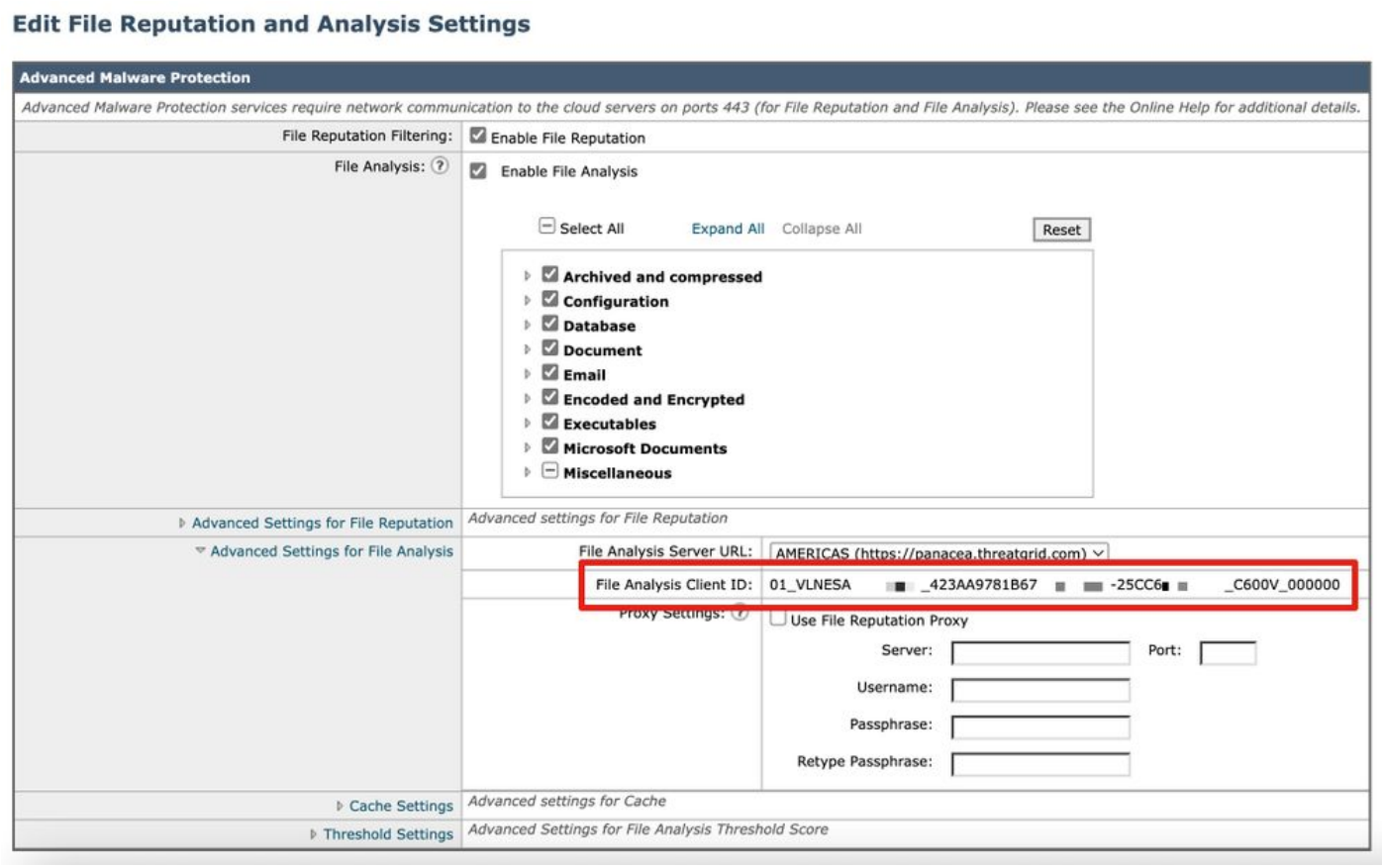
從網關或雲網關開始之前，請確保您具有所需的功能金鑰並啟用檔案信譽和檔案分析。要檢視功能金鑰，請導航到**系統管理>功能金鑰**。檔案信譽和檔案分析單獨列出，並且處於「活動」狀態。

網關或雲網關

1. 登入到使用者介面。
2. 導覽至Security Services > File Reputation and Analysis。
3. 按一下**編輯全域性設定……**
4. 展開Advanced Settings for File Analysis。

此處列出檔案分析客戶端ID。

E範例：



附註：虛擬裝置的檔案分析客戶端ID與硬體裝置存在差異。

網關或雲網關的檔案分析客戶端ID基於65個字元的字串格式：

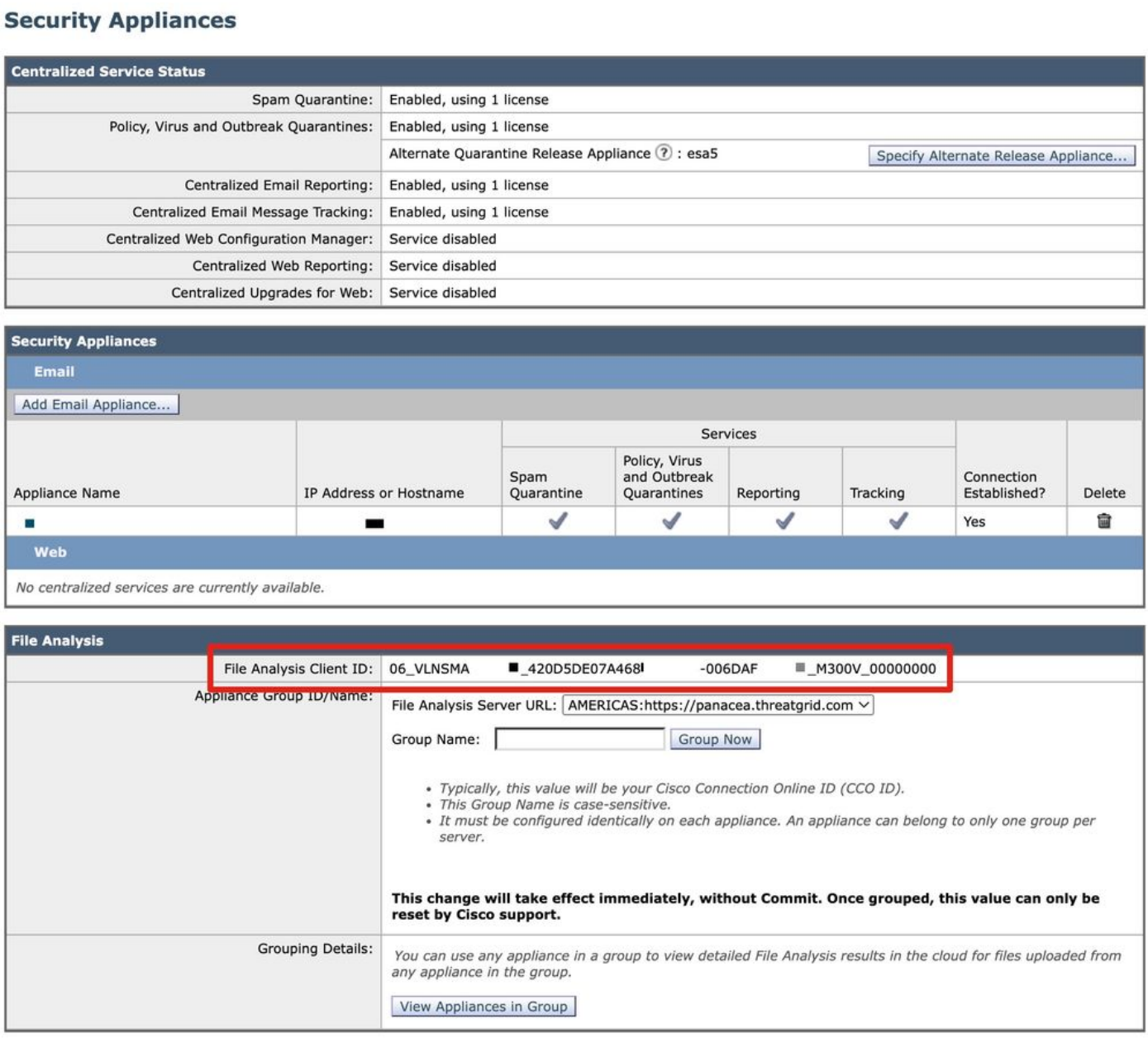
價值	說明
01_	「01」特定於網關或雲網關。
VLNEAXXXYYY_	如果這是虛擬裝置，則使用VLAN許可證號(可在CLI命令**show license**中找到)。 如果這是裝置，則沒有欄位。
SERIAL_	裝置的完整串列。
CX00V_	裝置的型號。
00000000	欄位零。根據前面的欄位，這些欄位會有所不同，以完成包含65個字元的欄位。

電子郵件和網路管理器

1. 登入到使用者介面。
2. 導航到**集中管理>安全裝置**。

此頁底部是「檔案分析」部分。此處列出檔案分析客戶端ID。

範例：



附註：虛擬裝置的檔案分析客戶端ID與硬體裝置存在差異。

Email and Web Manager的檔案分析客戶端ID基於65個字元的字串格式：

價值	說明

06_	「06」特定於電子郵件和Web管理器。
VLNSMAXXXYY_	如果這是虛擬裝置，則使用VLAN許可證號(可在CLI命令**show license**中找到)。 如果這是裝置，則沒有欄位。
SERIAL_	裝置的完整串列。
MX00V_	裝置的型號。
000000	欄位零。根據前面的欄位，這些欄位會有所不同，以完成包含65個字元的欄位。

檔案分析報告的裝置分組

如果您的許可證包含對思科安全惡意軟體分析(https://panacea.threatgrid.com)的訪問，則您的網關或雲網關的最佳做法是將它們與您的各個組織帳戶相關聯。若要允許組織中的所有內容安全裝置在雲中顯示有關組織中任何網關或雲網關傳送用於分析的檔案的詳細結果，您需要將所有裝置加入同一裝置組。當您登入到Malware Analytics時，傳送到雲以供分析的提交和威脅示例都顯示在您組織的Malware Analytics控制面板中。

附註：雲網關客戶在思科執行啟用和部署期間對此進行了配置。

組裝置

附註：如果您有雲網關且未完成，請在配置裝置組ID/名稱之前開啟支援案例。

網關或雲網關

1. 從使用者介面導航到**安全服務>檔案信譽和分析**。
2. 點選**Click here to group or view appliances for File Analysis reporting**。
3. 輸入設**備組ID/名稱**。預設值為： 建議對此值使用CCOID。一個裝置只能屬於一個組。配置「檔案分析」功能後，可以將電腦新增到組中。
4. 按一下**Group Now**。

電子郵件和網路管理器

附註：僅當郵件和Web Manager新增郵件裝置以進行集中管理並且遷移了策略、病毒和爆發隔離區後，才能使用配置裝置組ID/名稱的選項。

1. 從使用者介面導航至**集中服務>安全裝置**。 輸入設**備組ID/名稱**。預設值為：通常，此值是您的Cisco Connection Online ID(CCO ID)。此組名區分大小寫。必須在每台裝置上以相同方式配置。一台裝置只能屬於每台伺服器的一個組。
2. 按一下Group Now。

請注意：

- 新增組ID時，它將立即生效，無需提交。如果您需要變更群組ID，必須聯絡Cisco TAC。
- 此名稱區分大小寫，並且必須在分析組中的每台裝置上以相同方式配置。

檢視裝置

網關或雲網關

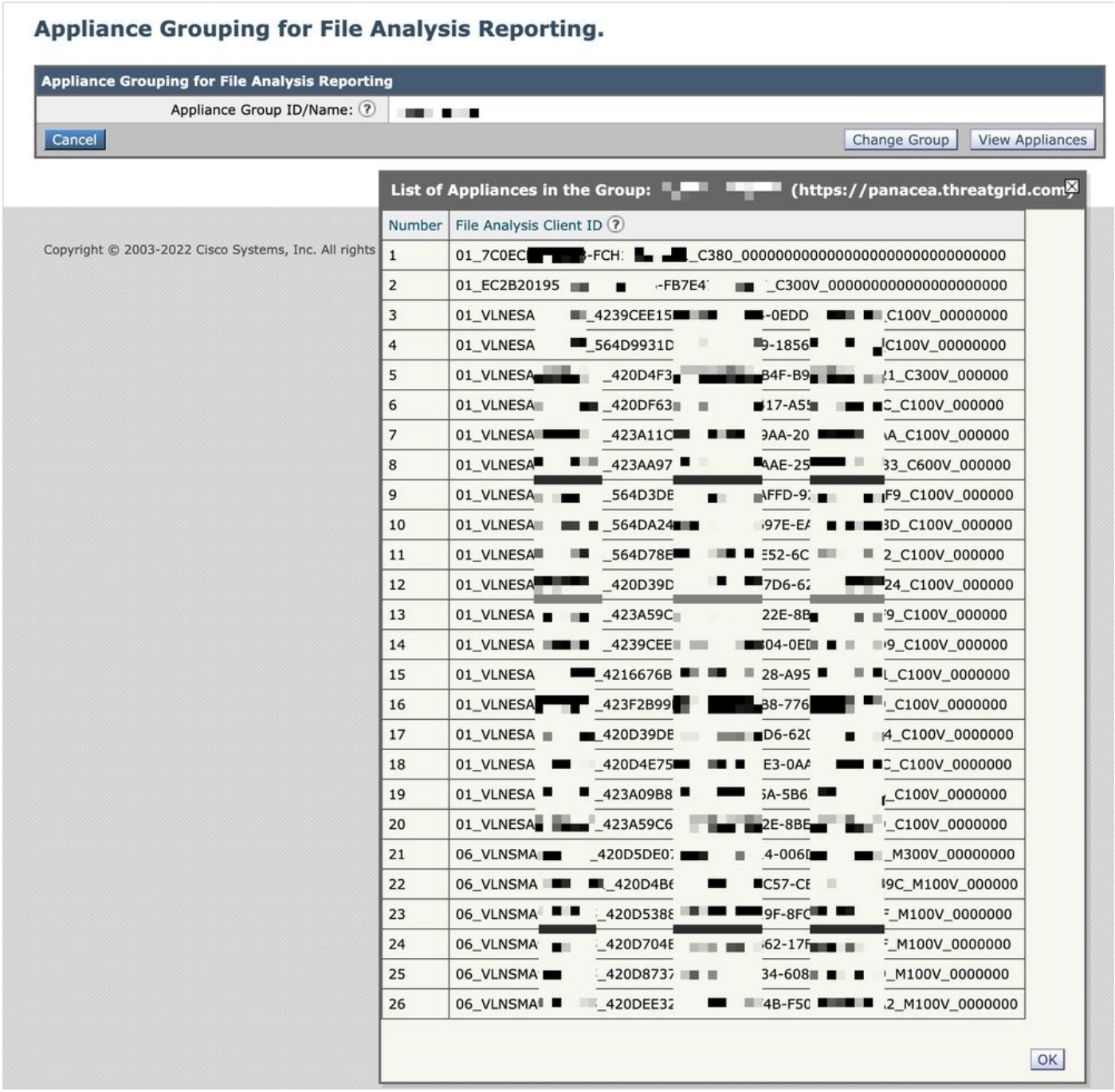
1. 從使用者介面導航至Security Services > File Reputation and Analysis。
2. 點選Click here to group or view appliances for File Analysis reporting。
3. 按一下View Appliances。

電子郵件和網路管理器

1. 從使用者介面導航至**集中服務>安全裝置**。
2. 在File Analysis部分中按一下View Appliances in Group。

此處列出了與裝置組ID/名稱相關聯的所有裝置的檔案分析客戶端ID。

範例：



其他資訊

思科安全電子郵件閘道檔案

- 發佈通知
- 使用手冊
- CLI參考指南
- 思科安全電子郵件網關API程式設計指南
- 思科安全電子郵件網關中使用的開源
- 思科內容安全虛擬裝置安裝指南（包括vESA）

安全電子郵件雲網關文檔

- 發佈通知
- 使用手冊

Cisco Secure Email and Web Manager文檔

- 發行說明和相容表
- 使用手冊
- Cisco Secure Email and Web Manager的API程式設計指南
- 思科內容安全虛擬裝置安裝指南（包括vSMA）

Cisco Secure 惡意軟體分析

- 思科安全惡意軟體分析(Threat Grid)

思科安全產品檔案

- 思科安全產品組合命名架構

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。