Descrizione dell'ID del client di analisi file per gateway, gateway cloud, e-mail e Web Manager

Sommario

Introduzione

In questo documento viene descritto come trovare l'ID del client di analisi dei file per Cisco Secure Email Gateway, Cloud Gateway, e-mail e Web Manager. L'ID del client di analisi file è una chiave di registrazione univoca di 65 caratteri utilizzata quando il gateway, il gateway cloud o l'e-mail e Web Manager si registrano con Cisco Malware Analytics (in precedenza Threat Grid) per l'invio dei file e la modalità sandbox. Ad esempio, se è stato abilitato il servizio Analisi file e il servizio di reputazione non dispone di informazioni sull'allegato trovato in un messaggio e l'allegato soddisfa i criteri per i file che possono essere analizzati (vedere File supportati per la reputazione dei file e Analysis Services), il messaggio può essere messo in quarantena (vedere Messa in quarantena di messaggi con allegati inviati per l'analisi) e il file inviato per l'analisi.

Per "Raggruppamento di appliance per report analisi file", verificare di conoscere gli ID analisi file.

Per informazioni dettagliate, vedere il capitolo "File Reputation Filtering and File Analysis" del manuale dell'utente:

- Guide per l'utente finale di Cisco Secure Email Gateway
- Guide per l'utente finale di Cisco Secure Email Cloud Gateway

ID client di analisi file per gateway, gateway cloud, e-mail e Web

Manager

L'ID del client di analisi dei file viene generato automaticamente per gli accessori quando si attiva l'analisi dei file.

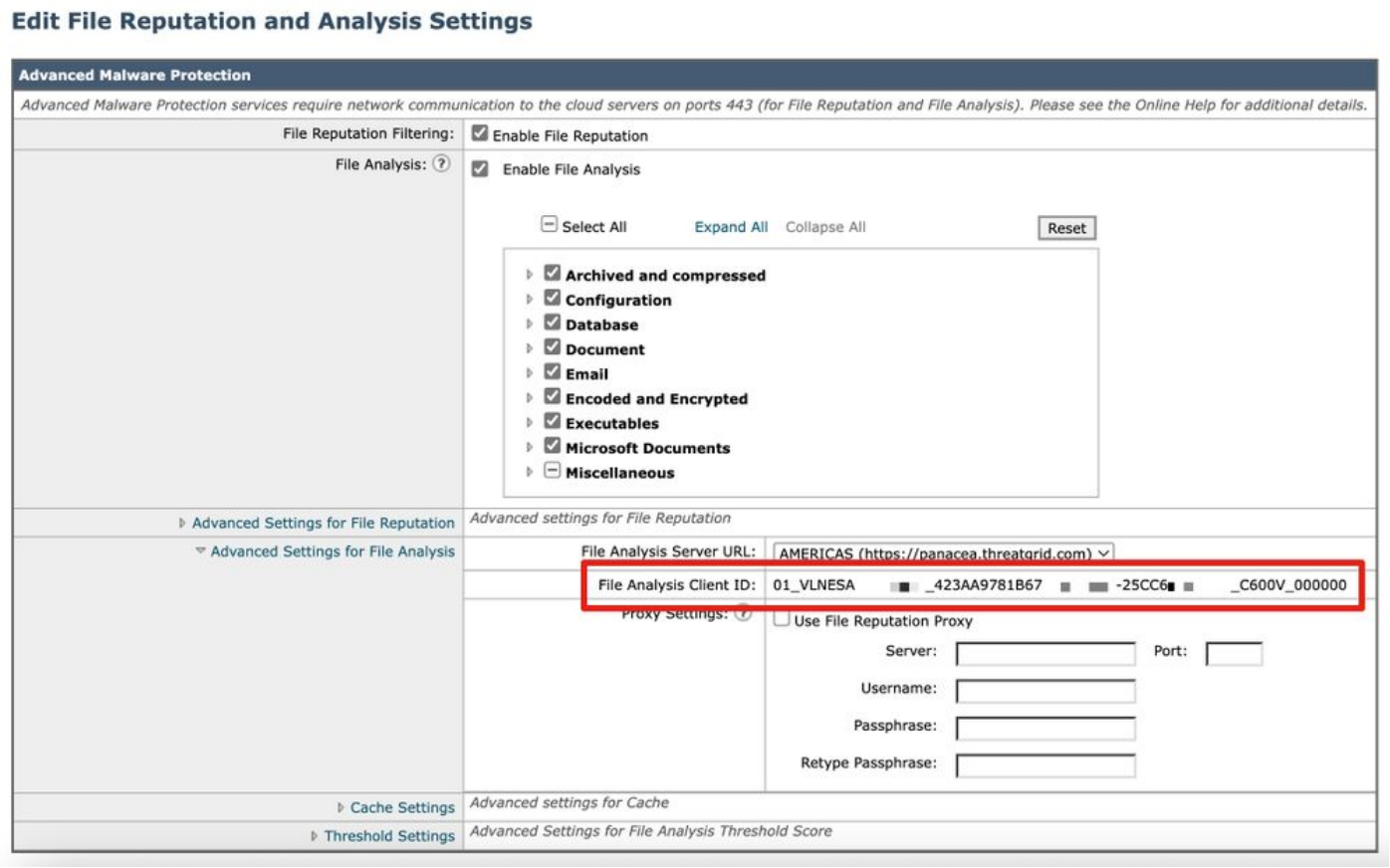
Prima di iniziare dal gateway o dal gateway del cloud, assicurarsi di avere le chiavi delle funzionalità necessarie e di avere abilitato la reputazione dei file e l'analisi dei file. Per visualizzare i tasti funzione, selezionare **Amministrazione sistema > Tasti funzione**. La reputazione e l'analisi dei file sono elencate separatamente e hanno lo stato Attivo.

Gateway o gateway cloud

1. Accedere all'interfaccia utente.
2. Selezionare **Security Services > File Reputation and Analysis** (Servizi di sicurezza > Reputazione e analisi file).
3. Fare clic su **Modifica impostazioni globali...**
4. Espandere **Impostazioni avanzate per analisi file**.

L'ID del client di analisi file è elencato di seguito.

SEsempio:



Nota: L'ID del client di analisi dei file per le appliance virtuali è diverso da quello delle appliance hardware.

L'ID del client di analisi file per il gateway o il gateway cloud si basa su un formato stringa di 65 caratteri:

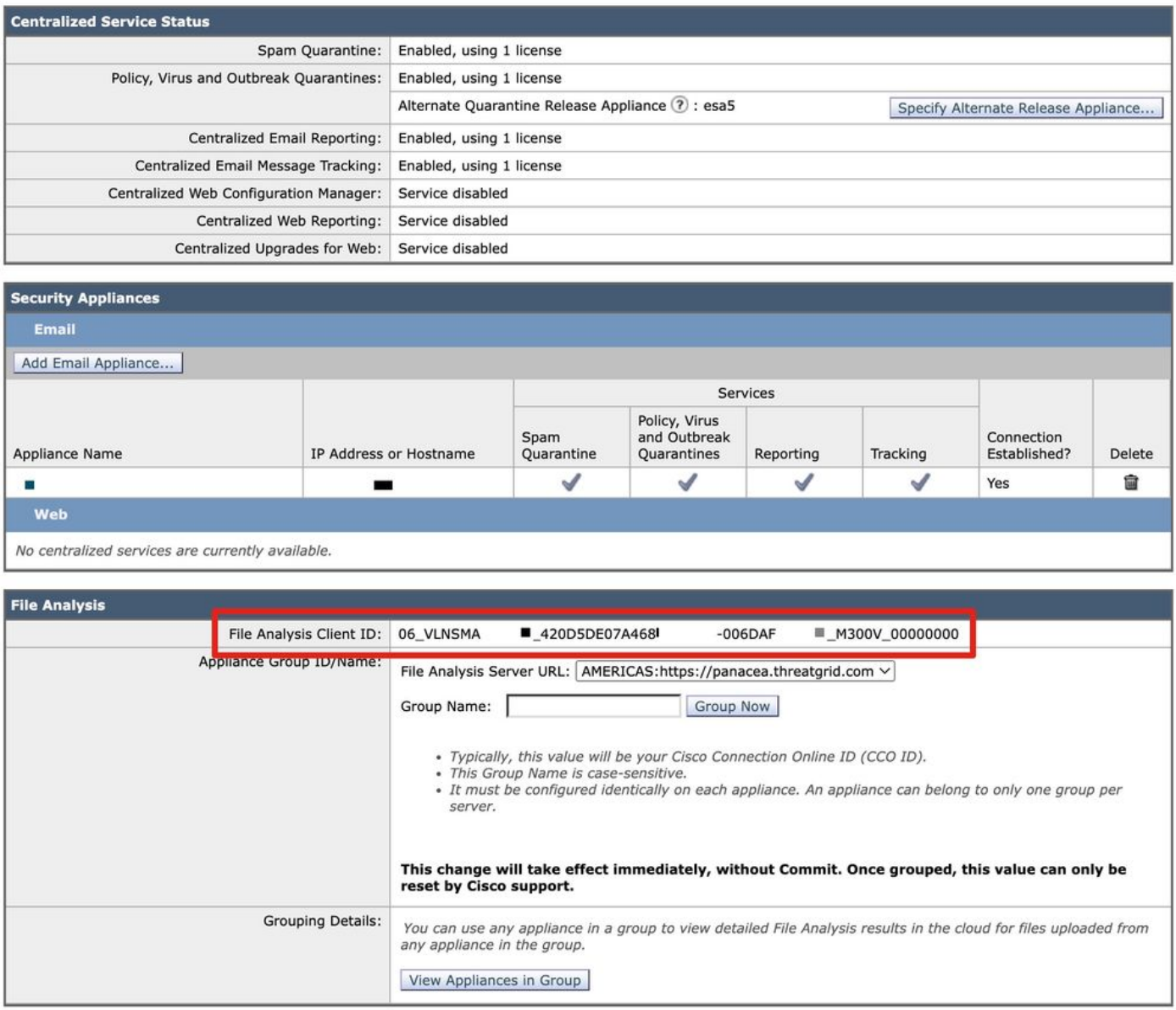
Valore	Spiegazione
01_	"01" è specifico del gateway o del gateway cloud.
VLNESAXXXYYY	Se si tratta di un'appliance virtuale, viene utilizzato il numero di licenza VLAN (indicato comando **show license** della CLI). Se si tratta di un accessorio hardware, non è presen alcun campo.
SERIALE_	Serie COMPLETA dell'accessorio.
CX00V_	Modello dell'accessorio.
00000000	Zeri campo. In base ai campi precedenti, questi variano per completare il campo di 65 caratteri.

E-mail e Web Manager

1. Accedere all'interfaccia utente.
2. Passare a **Gestione centralizzata > Appliance di sicurezza**.

Nella parte inferiore della pagina è disponibile la sezione Analisi file. L'ID del client di analisi file è elencato di seguito.

Esempio:



Nota: L'ID del client di analisi dei file per le appliance virtuali è diverso da quello delle appliance hardware.

L'ID del client di analisi file per e-mail e Web Manager si basa su un formato stringa di 65 caratteri:

Valore	Spiegazione
06_	"06" è specifico di Email and Web Manager.
VLNSMAXXXYYY	Se si tratta di un'appliance virtuale, viene utilizzato il numero di licenza VLAN (indicato c comando **show license** della CLI). Se si tratta di un accessorio hardware, non è present alcun campo.
SERIALE_	Serie COMPLETA dell'accessorio.
MX00V_	Modello dell'accessorio.
000000	Zeri campo. In base ai campi precedenti, questi variano per completare il campo di 65 caratteri.

Raggruppamento di appliance per report di analisi dei file

Se la licenza include l'accesso a Cisco Secure Malware Analytics (https://panacea.threatgrid.com), la procedura ottimale per il gateway o il gateway cloud è associarli al proprio account aziendale. Per consentire a tutte le appliance di sicurezza dei contenuti dell'organizzazione di visualizzare nel cloud risultati dettagliati sui file inviati per l'analisi da qualsiasi gateway o gateway cloud dell'organizzazione, è necessario unire tutte le appliance allo stesso gruppo. Quando si accede a Malware Analytics, gli invii e gli esempi di minaccia inviati al cloud per l'analisi vengono tutti visualizzati nel dashboard di Malware Analytics per l'organizzazione.

Nota: I clienti di Cloud Gateway lo hanno configurato durante le attivazioni e l'installazione eseguite da Cisco.

Appliance di gruppo

Nota: Se si dispone di un gateway cloud e l'operazione non è stata completata, aprire una richiesta di assistenza prima di configurare un ID/nome del gruppo di accessori.

Gateway o gateway cloud

1. Dall'interfaccia utente, selezionare **Security Services > File Reputation and Analysis** (Servizi di sicurezza > Reputazione e analisi file).
2. Fare clic su **Fare clic qui per raggruppare o visualizzare gli accessori per il report di analisi dei file**.
3. Inserire l'**ID/nome del gruppo di accessori**. I valori predefiniti sono: Si consiglia di utilizzare il CCOID per questo valore.Un accessorio può appartenere a un solo gruppo.Dopo aver configurato la feature di analisi file, potete aggiungere un computer a un gruppo.
4. Fare clic su **Raggruppa**.

E-mail e Web Manager

Nota: L'opzione per la configurazione di un ID/nome di un gruppo di appliance è disponibile

solo dopo l'aggiunta di Email and Web Manager a scopo di gestione centralizzata e la migrazione di Policy, Virus, Outbreak Quarantines.

1. Dall'interfaccia utente, passare a **Servizi centralizzati > Appliance di sicurezza**. Inserire l'**ID/nome del gruppo di accessori**. I valori predefiniti sono:In genere, questo valore corrisponde all'ID Cisco Connection Online (ID CCO).Per questo nome gruppo viene fatta distinzione tra maiuscole e minuscole.La configurazione deve essere identica per ciascun accessorio. Un accessorio può appartenere a un solo gruppo per server.
2. Fare clic su **Raggruppa**.

Nota:

- L'aggiunta di un ID gruppo ha effetto immediato, senza commit. Per modificare l'ID di un gruppo, è necessario contattare Cisco TAC.
- Il nome fa distinzione tra maiuscole e minuscole e deve essere configurato in modo identico su ciascun accessorio del gruppo di analisi.

Visualizza accessori

Gateway o gateway cloud

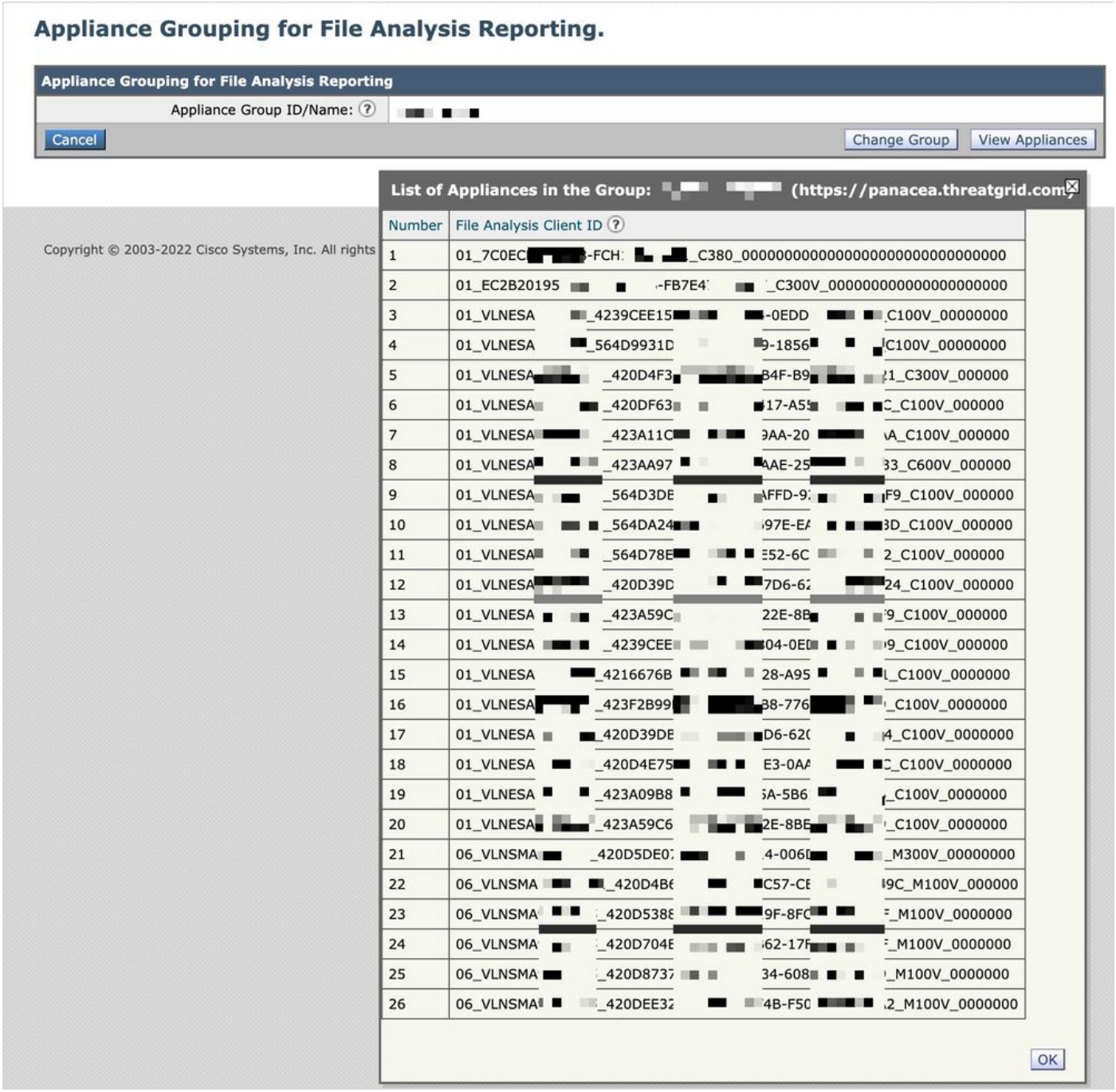
1. Dall'interfaccia utente, passare a **Servizi di sicurezza > Reputazione e analisi file.**
2. Fare clic su **Fare clic qui per raggruppare o visualizzare gli accessori per il report di analisi dei file**.
3. Fare clic su **View Appliance** (Visualizza accessori).

E-mail e Web Manager

1. Dall'interfaccia utente, passare a **Servizi centralizzati > Appliance di sicurezza**.
2. Fare clic su **Visualizza accessori in gruppo** nella sezione Analisi file.

Di seguito sono elencati gli ID di tutti gli accessori associati all'ID/nome del gruppo di accessori.

Esempio:



Ulteriori informazioni

Documentazione di Cisco Secure Email Gateway

- Note sulla release
- Guida dell'utente
- Guida di riferimento CLI
- Guide alla programmazione API per Cisco Secure Email Gateway
- Open Source utilizzato in Cisco Secure Email Gateway
- Guida all'installazione di Cisco Content Security Virtual Appliance (include vESA)

Documentazione su Secure Email Cloud Gateway

- Note sulla release
- Guida dell'utente

Documentazione di Cisco Secure Email e Web Manager

- Note sulla versione e matrice di compatibilità
- Guida dell'utente
- Guide alla programmazione API per Cisco Secure Email e Web Manager
- Guida all'installazione di Cisco Content Security Virtual Appliance (include vSMA)

Cisco Secure Malware Analytics

- Cisco Secure Malware Analytics (Threat Grid)

Documentazione del prodotto Cisco Secure

- Architettura di denominazione del portafoglio Cisco Secure

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).