Explique la ID de cliente de análisis de archivos para el gateway, el gateway de la nube y el gestor de correo electrónico y web

Contenido

Introducción

Este documento describe cómo encontrar la ID de cliente de análisis de archivos para Cisco Secure Email Gateway, Cloud Gateway y Email and Web Manager. La ID de cliente de análisis de archivos es una clave de registro única de 65 caracteres que se utiliza cuando el gateway, el gateway de la nube o Email and Web Manager se registra con Cisco Malware Analytics (anteriormente conocido como Threat Grid) para el envío de archivos y el sandboxing. Por ejemplo, si ha activado el servicio Análisis de archivos y el servicio de reputación no tiene información sobre los archivos adjuntos encontrados en un mensaje, y los archivos adjuntos cumplen los criterios de los archivos que se pueden analizar (consulteArchivos admitidos para Reputación de archivos y Analysis Services), el mensaje se puede poner en cuarentena (consulteCuarentena de mensajes con archivos adjuntos enviados para análisis) y el archivo se envía para análisis.

Para "Agrupación de dispositivos para informes de análisis de archivos", asegúrese de conocer sus ID de análisis de archivos.

Para obtener más información, consulte el capítulo sobre filtrado y análisis de la reputación de archivos de la guía del usuario:

- Guías de usuario final de Cisco Secure Email Gateway
- Guías para usuarios finales de Cisco Secure Email Cloud Gateway

ID de cliente de análisis de archivos para gateway, gateway de nube y gestor de correo electrónico y web

El ID de cliente de análisis de archivos se genera automáticamente para los dispositivos cuando se habilita el análisis de archivos.

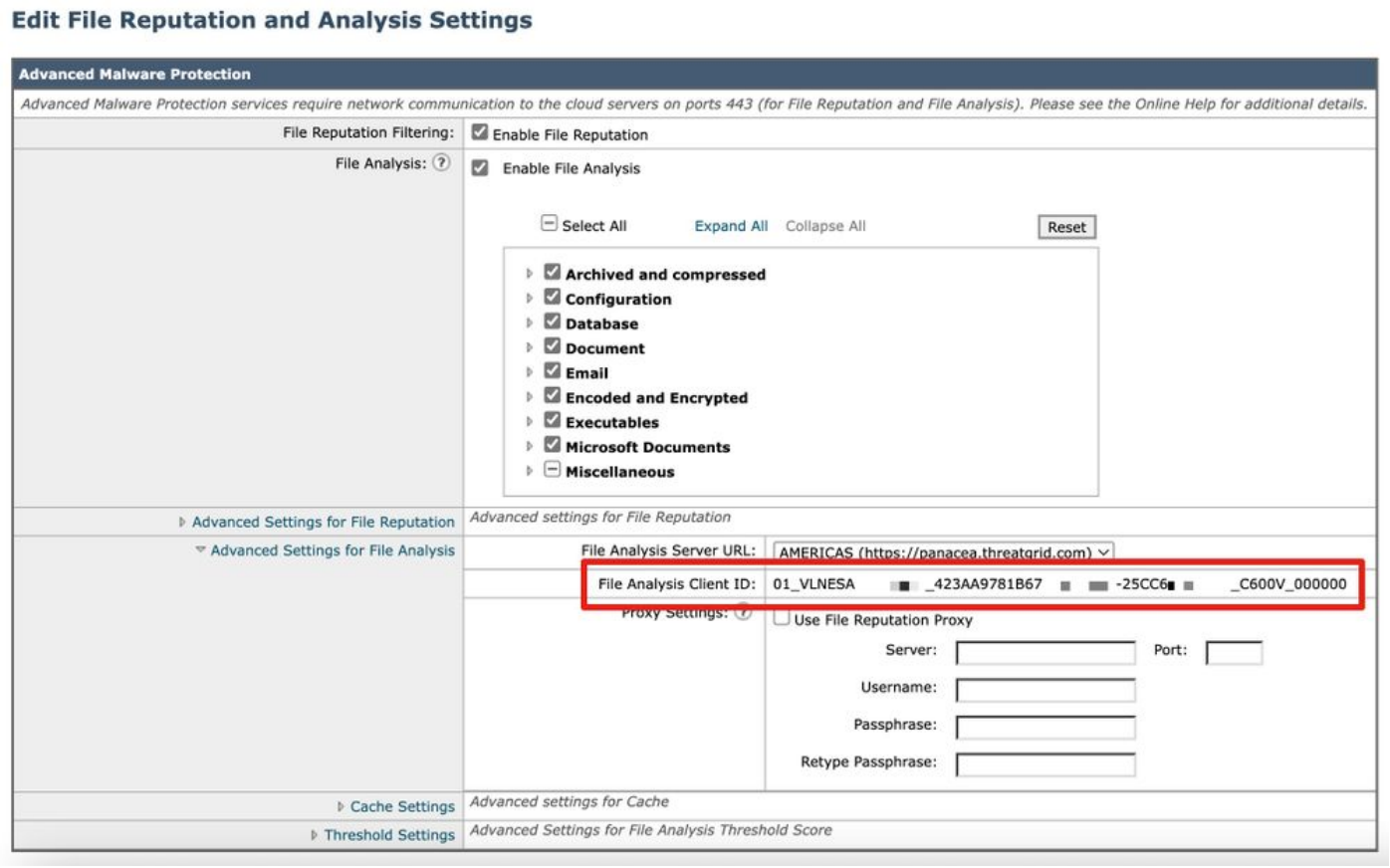
Antes de empezar desde la puerta de enlace o la puerta de enlace en la nube, asegúrese de que dispone de las claves de funciones necesarias y de que ha activado Reputación de archivos y Análisis de archivos. Para ver las teclas de función, navegue hasta **Administración del sistema > Claves de función**. Reputación de archivos y Análisis de archivos se muestran por separado y tienen el estado Activo.

Gateway o gateway de nube

1. Inicie sesión en la interfaz de usuario.
2. Vaya a **Servicios de seguridad > Reputación y análisis de archivos**.
3. Haga clic en **Editar configuración global...**
4. Expanda **Configuración avanzada para Análisis de archivos**.

Aquí se muestra la ID de cliente de análisis de archivos.

EEjemplo:



Nota: Existe una diferencia entre el ID de cliente de análisis de archivos para dispositivos virtuales y los dispositivos de hardware.

El ID de cliente de análisis de archivos para la puerta de enlace o la puerta de enlace de la nube se basa en un formato de cadena de 65 caracteres:

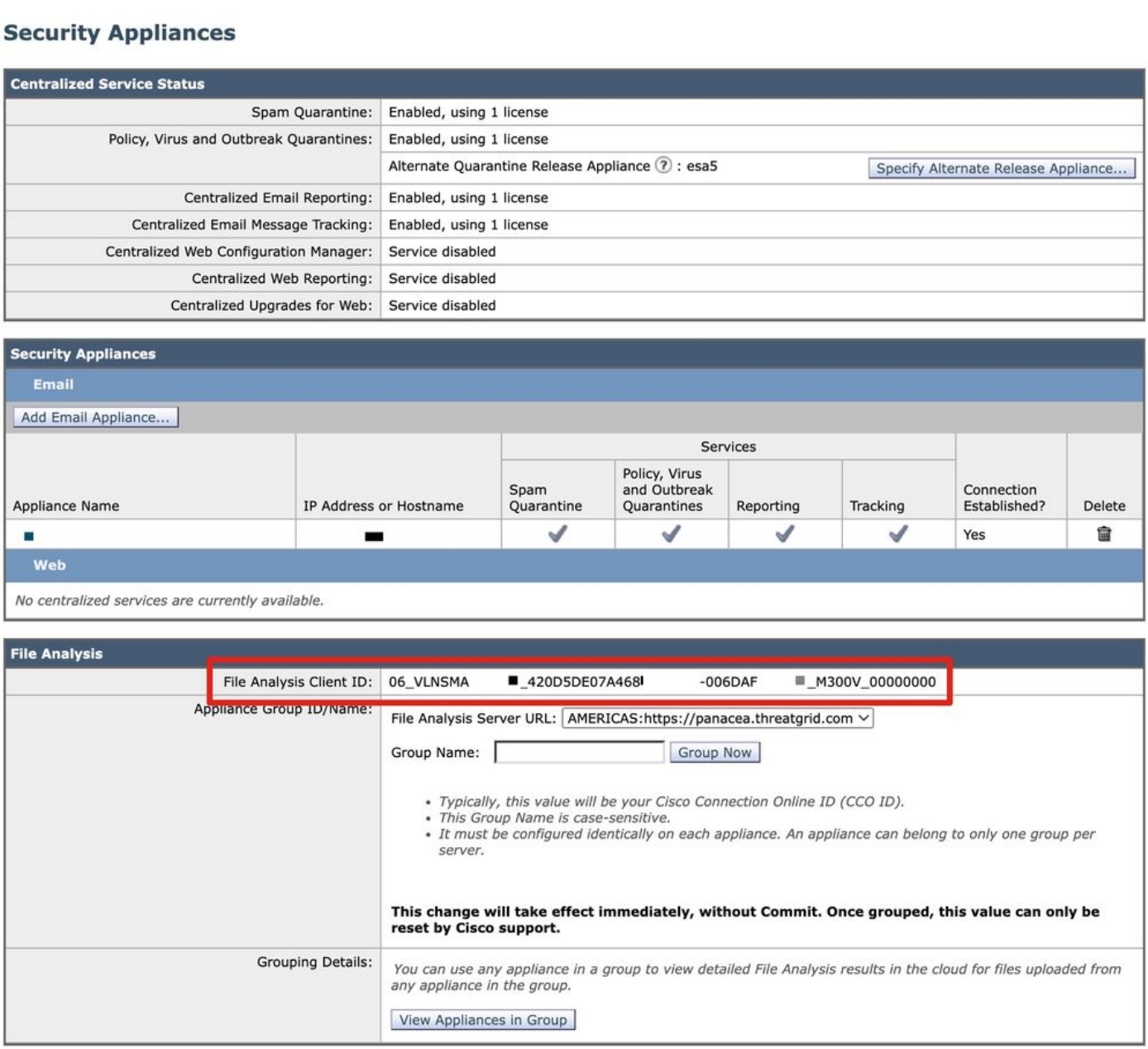
Valor	Explicación
01_	"01" es específico de la puerta de enlace o de la puerta de enlace de nube.
VLNESAXXXYYY_	Si se trata de un dispositivo virtual, utiliza el nº de licencia de VLAN (que se encuentra el comando de CLI **show license**). Si se trata de un dispositivo de hardware, no hay n campo.
SERIAL_	Serie COMPLETA del dispositivo.
CX00V_	Modelo del dispositivo.
00000000	Campo ceros. Según los campos anteriores, estos varían para finalizar el campo de 6 caracteres.

Administrador de correo electrónico y web

1. Inicie sesión en la interfaz de usuario.
2. Vaya a **Administración centralizada > Dispositivo de seguridad**.

En la parte inferior de esta página se encuentra la sección Análisis de archivos. Aquí se muestra la ID de cliente de análisis de archivos.

Ejemplo:



Nota: Existe una diferencia entre el ID de cliente de análisis de archivos para dispositivos virtuales y los dispositivos de hardware.

El ID de cliente de análisis de archivos para Email and Web Manager se basa en un formato de cadena de 65 caracteres:

Valor	Explicación
06_	"06" es específico del gestor de correo electrónico y web.
VLNSMAXXXYYY_	Si se trata de un dispositivo virtual, utiliza el nº de licencia de VLAN (que se encuentra comando de CLI **show license**). Si se trata de un dispositivo de hardware, no hay ningú campo.
SERIAL_	Serie COMPLETA del dispositivo.
MX00V_	Modelo del dispositivo.
000000	Campo ceros. Según los campos anteriores, estos varían para finalizar el campo de 65 caracteres.

Agrupación de dispositivos para informes de análisis de archivos

Si su licencia incluye acceso a Cisco Secure Malware Analytics (https://panacea.threatgrid.com), la práctica recomendada para su gateway o gateway de nube es asociarlos a su cuenta de organización individual. Para permitir que todos los dispositivos de seguridad de contenido de su organización muestren resultados detallados en la nube sobre los archivos enviados para su análisis desde cualquier gateway o gateway de nube de su organización, debe unir todos los dispositivos al mismo grupo de dispositivos. Al iniciar sesión en Malware Analytics, los envíos y las muestras de amenazas que se envían a la nube para su análisis se muestran en el panel de análisis de malware de su organización.

> **Nota:** Los clientes de Cloud Gateway lo tienen configurado durante las activaciones y la implementación realizadas por Cisco.

Dispositivos de grupo

> **Nota:** Si tiene un gateway de nube y esto no se ha completado, abra un caso de soporte antes de configurar un ID/nombre de grupo de dispositivos.

Gateway o gateway de nube

1. Desde la interfaz de usuario, navegue hasta **Servicios de seguridad > Reputación y análisis de archivos**.
2. Haga clic en **Haga clic aquí para agrupar o ver los dispositivos para los informes de análisis de archivos**.
3. Introduzca la **ID/nombre del grupo de dispositivos**. Los valores predeterminados son: Se recomienda utilizar la ID de CCO para este valor.Un dispositivo solo puede pertenecer a un grupo.Después de configurar la función Análisis de archivos, puede agregar un equipo a un grupo.
4. Haga clic en **Agrupar ahora**.

Administrador de correo electrónico y web

Nota: La opción para configurar un ID/nombre de grupo de dispositivos solo está disponible después de que Email and Web Manager haya agregado un dispositivo de correo electrónico para la administración centralizada y haya migrado las cuarentenas de brotes, virus y políticas.

1. Desde la interfaz de usuario, navegue hasta **Servicios centralizados > Dispositivos de seguridad**. Introduzca la **ID/nombre del grupo de dispositivos**. Los valores predeterminados son:Normalmente, este valor es su ID de Cisco Connection Online (ID de CCO).Este nombre de grupo distingue entre mayúsculas y minúsculas.Se debe configurar de forma idéntica en cada dispositivo. Un dispositivo sólo puede pertenecer a un grupo por servidor.
2. Haga clic en **Agrupar ahora**.

Tenga en cuenta:

- Cuando agrega una ID de grupo, tiene efecto inmediatamente, sin una confirmación. Si necesita cambiar una ID de grupo, debe ponerse en contacto con el TAC de Cisco.
- Este nombre distingue entre mayúsculas y minúsculas y debe configurarse de forma idéntica en cada dispositivo del grupo de análisis.

Ver dispositivos

Gateway o gateway de nube

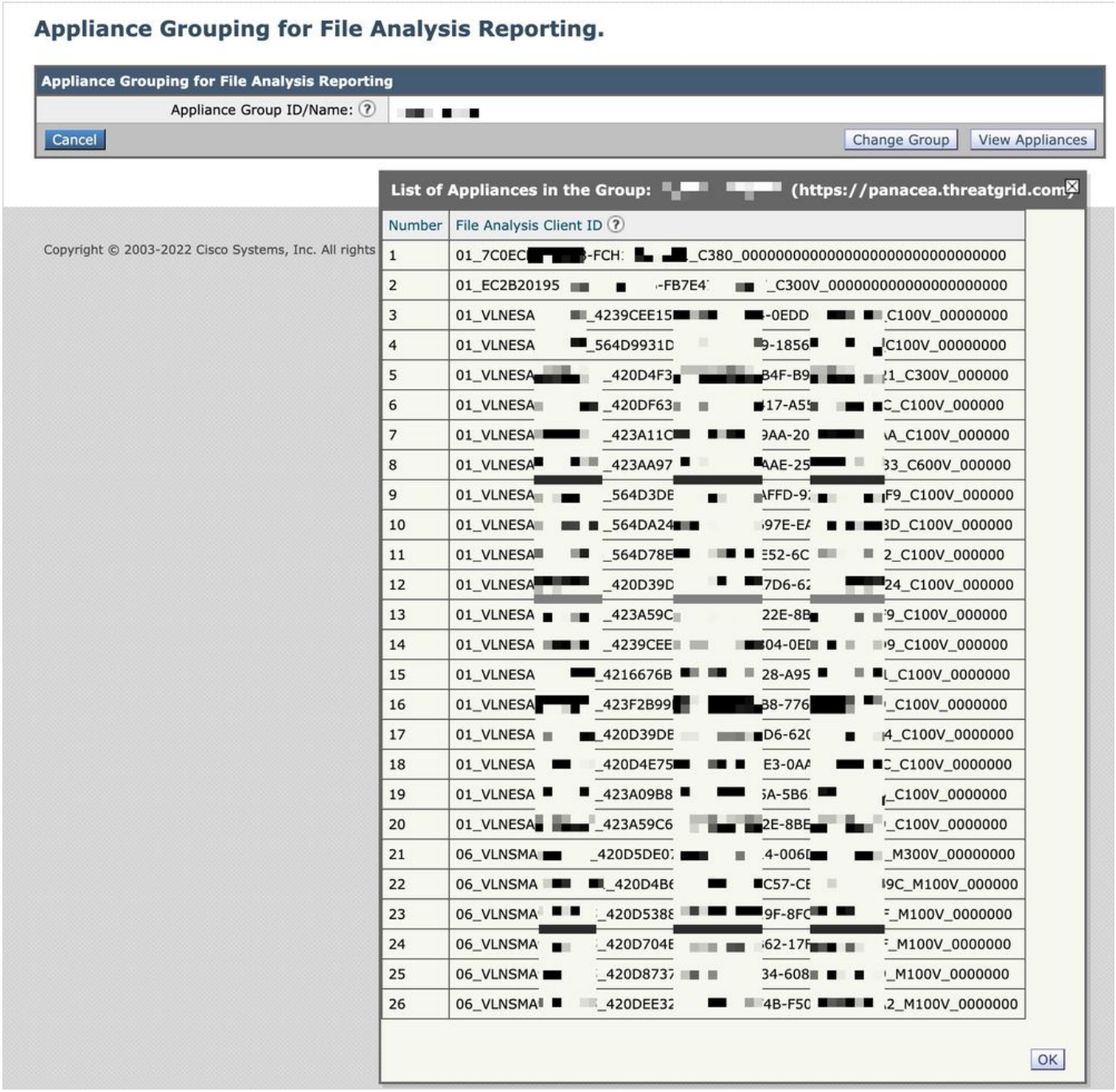
1. En la interfaz de usuario, vaya a **Servicios de seguridad > Reputación y análisis de archivos.**
2. Haga clic en **Haga clic aquí para agrupar o ver los dispositivos para los informes de análisis de archivos**.
3. Haga clic en **Ver dispositivos**.

Administrador de correo electrónico y web

1. Desde la interfaz de usuario, navegue hasta **Servicios centralizados > Dispositivos de seguridad**.
2. Haga clic en **Ver dispositivos en grupo** en la sección Análisis de archivos.

Aquí se muestra el ID de cliente de análisis de archivos de todos los dispositivos asociados con el ID/nombre de grupo de dispositivos.

Ejemplo:



Additional Information

Documentación de Cisco Secure Email Gateway

- Release Notes
- Guía del usuario
- Guía de referencia de CLI
- Guías de programación de API para Cisco Secure Email Gateway
- Código abierto utilizado en Cisco Secure Email Gateway
- Guía de instalación del appliance virtual de seguridad de contenido de Cisco(incluye vESA)

Documentación de Secure Email Cloud Gateway

- Release Notes
- Guía del usuario

Documentación de Cisco Secure Email and Web Manager

- Notas de la versión y matriz de compatibilidad
- Guía del usuario
- Guías de programación de API para Cisco Secure Email y Web Manager
- Guía de instalación del appliance virtual de seguridad de contenido de Cisco(incluye vSMA)

Cisco Secure Malware Analytics

- Análisis de malware seguro de Cisco (Threat Grid)

Documentación del producto Cisco Secure

- Arquitectura de nomenclatura de la cartera Cisco Secure

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).