Guía del producto de McAfee Client Proxy 4.1.x

Trellix

Contenido

Descripción general del producto. 3

Descripción general. 3

Funciones clave. 3

Cómo funciona. 4

Administración de las directivas de Client Proxy. 6

Metadatos de Client Proxy. 6

Conjuntos de permisos (McAfee ePO). 6

Permisos de usuario. 6

Configurar un conjunto de permisos. 7

Permisos necesarios para administrar Client Proxy. 7

Revisión y aprobación de directivas. 9

Cómo se utiliza la contraseña compartida. 10

Consideraciones al cambiar la contraseña compartida (McAfee ePO Cloud). 10

Importar el ID de cliente y la contraseña compartida (MVISION ePO). 11

Crear una instancia de Common Catalog (McAfee ePO o McAfee ePO Cloud). 11

Configurar una directiva. 13

Crear una directiva de Client Proxy. 13

Cómo Client Proxy administra la lista de servidores proxy. 14

Configurar la lista de servidores proxy. 14

Configurar la lista de servidores proxy alternativos. 16

Configurar los ajustes de cliente. 18

Configurar la lista de omisión (McAfee ePO o McAfee ePO Cloud). 21

Configuración de la lista de redirecciones alternativas (McAfee ePO o McAfee ePO Cloud). 22

Configurar la lista de omisión (MVISION ePO). 23

Configuración de la lista de redirecciones alternativas (MVISION ePO). 24

Importación o exportación de la lista de omisión (MVISION ePO). 25

Importación o exportación de la lista de redirecciones alternativas (MVISION ePO). 26

Configuración de la lista de bloqueos. 27

Asignar una directiva a los endpoints. 27

Exportar una directiva a un archivo .xml u .opg. 28

Suspenda la implementación de directivas en un equipo basado en Windows o macOS. 29

Consultas e informes. 31

Crear y ejecutar una consulta de base de datos (McAfee ePO). 31

Crear un informe de Client Proxy (McAfee ePO o MVISION ePO). 32

Descripción general del producto

Descripción general

El software de McAfee® Client Proxy ayuda a proteger a los usuarios de endpoint frente a las amenazas de seguridad que surgen cuando acceden a la web desde dentro o fuera de la red.

El software cliente, que se instala en los endpoints que tienen Microsoft Windows o macOS, redirige las solicitudes web o les permite continuar con un proxy para el filtrado. El software del servidor se ejecuta en una de las tres plataformas de administración: McAfee ePO, McAfee ePO Cloud, o MVISION ePO.

Solución híbrida de Web Protection

Client Proxy es un componente esencial de la solución híbrida de McAfee® Web Protection. Esta solución le permite integrar las funciones de seguridad basadas en la red y en la nube proporcionadas por McAfee® Web Gateway y McAfee® Web Gateway Cloud Service (McAfee® WGCS) respectivamente.

El software de Client Proxy permite o redirige el tráfico web en función de la ubicación del endpoint:

- **Endpoints ubicados dentro de la red o conectados por VPN**: se permite que el tráfico continúe a un appliance de Web Gateway instalado en la red para el filtrado.
- **Endpoints ubicados fuera de la red**: el tráfico se redirige a McAfee WGCS para el filtrado.

Integración con Endpoint Security

Al desplegar Client Proxy con McAfee® Endpoint Security en los endpoints, instala y administra cada producto por separado mediante McAfee® ePolicy Orchestrator® (McAfee® ePO™) , McAfee ePO Cloud o MVISION ePO.

- Administradores de Client Proxy: configuran las directivas y llevan a cabo las tareas como de costumbre.
- Administradores de Endpoint Security: tienen la opción de configurar el Control web de Control web de McAfee® Endpoint Security para que esté desactivado mientras se instala el Client Proxy redirige el tráfico web de forma activa.

En los endpoints con Windows, puede ver si Client Proxy está instalado y en ejecución en el endpoint y si está redirigiendo el tráfico de forma activa mediante la apertura de la ventana **Acerca de McAfee Client Proxy** desde el menú **Inicio**.

Funciones clave

Client Proxy permite o redirige las solicitudes web de los usuarios en función de las directivas que configure.

- **Redireccionamiento del tráfico**: el software redirige el tráfico web a servidores proxy para su filtrado según la configuración de la directiva de Client Proxy.
- **Reconocimiento de ubicación**: los ajustes del reconocimiento de ubicación permiten que una directiva cubra a los usuarios que trabajan dentro de la red, fuera de la red o conectados a la red por VPN.
- **Administración centralizada**: el software se administra con McAfee ePO, McAfee ePO Cloud o MVISION ePO.

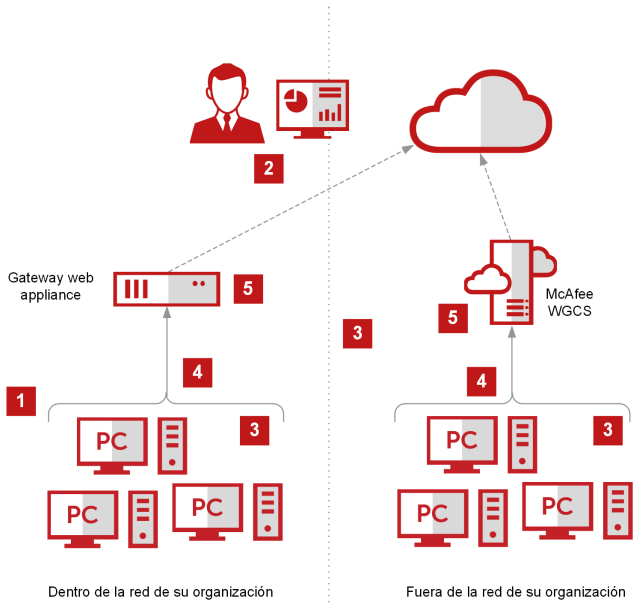
- **Independencia del navegador**: los ajustes del servidor proxy se configuran en Client Proxy y no en los navegadores que se ejecutan en los endpoints.
- **Autenticación transparente**: Client Proxy autentica a los usuarios sin solicitar credenciales y pasa la pertenencia a grupos y otra información de los metadatos que agrega a solicitudes HTTP/HTTPS.
- **Resistencia a manipulación**: no se permite que los usuarios eliminen el software de Client Proxy del endpoint sin solicitar y recibir un código de liberación temporal de un administrador.
- **Canal seguro**: el software establece un canal de comunicación segura entre Client Proxy y McAfee WGCS para todas las solicitudes de HTTP/HTTPS. Esto solo es aplicable a servidores proxy en la nube.

Cómo funciona

El software de Client Proxy redirige, bloquea o permite el tráfico web de acuerdo con la directiva de Client Proxy y la ubicación de los endpoints.

Flujo de trabajo de Client Proxy

1. El software de Client Proxy está instalado en los endpoints de su organización.
2. Mediante McAfee ePO, McAfee ePO Cloud o MVISION ePO, el administrador crea una directiva de Client Proxy y asigna la directiva a todos los endpoints gestionados.
3. Los endpoints gestionados se pueden localizar dentro de la red de su organización, conectados a la red por medio de VPN o ubicados fuera de la red.
4. Los usuarios que trabajan en los endpoints solicitan acceso a los recursos web.
5. El software determina la ubicación del usuario y, a continuación, permite o redirige la solicitud web:
    - Dentro de la red o conectado mediante VPN: permite que la solicitud web continúe a un appliance de Web Gateway instalado en la red, donde se filtra. Client Proxy es pasivo.
    - Fuera de la red: redirige la solicitud web a McAfee WGCS para el filtrado. Client Proxy es activo.



Administración de las directivas de Client Proxy

Metadatos de Client Proxy

Cuando el software de Client Proxy redirige el tráfico HTTP/HTTPS, añade metadatos a las solicitudes.

Otros productos, como Web Gateway y McAfee WGCS, utilizan los metadatos (por ejemplo, la pertenencia a grupos) cuando aplican directivas de protección web.

- Tokens de autenticación: tokens que contienen información de identidad sobre el usuario que realiza la solicitud web
- Versión de autenticación: versión de los metadatos que está compartiendo Client Proxy
- Dirección IP del cliente: dirección IP del endpoint donde se originó el tráfico
- Dirección IP de destino original: dirección IP guardada del servidor donde está destinado el tráfico
- ID de cliente: identifica de forma exclusiva la organización del cliente
- ID de usuario: identifica de forma exclusiva al usuario que realiza la solicitud web
- Grupos de usuarios: nombres de los grupos de los que el usuario es miembro
- ID de inquilino: ID compartido por los nodos de un clúster (McAfee ePO Cloud o MVISION ePO)
- Nombre del proceso: nombre del proceso que genera tráfico
- Ruta del proceso ejecutable: ruta del proceso que genera tráfico
- Información del sistema: información del sistema como el nombre del sistema operativo host (Windows, Mac), la hora local (segundos desde 1/1/1970), la dirección MAC, el tiempo de actividad del proceso, el nombre del sistema y el nombre de la directiva de MCP

Conjuntos de permisos (McAfee ePO)

Permisos de usuario

Permite administrar los permisos de usuario mediante la configuración de conjuntos de permisos en la interfaz de McAfee ePO, un conjunto de permisos para cada rol.

La interfaz de usuario incluye roles predefinidos y conjuntos de permisos que se pueden editar. También puede agregar un rol y configurar un conjunto de permisos para ese rol.

Usuarios administrativos

Un rol predefinido, **Administrador de catálogos de MCP**, tiene todos los permisos necesarios para crear, eliminar y administrar las directivas de Client Proxy. Se requiere un conjunto de permisos completo para dar a los administradores de Client Proxy permiso para:

- Crear, eliminar y administrar directivas
- Insertar directivas en endpoints
- Ver consultas

- Administrar el software de extensión de Client Proxy
- Realizar funciones del repositorio principal
- Realizar funciones de Help Desk

Solo los administradores de McAfee ePO tienen permisos para administrar el software de extensión, incluido el permiso para:

- Instalar extensiones en un servidor de McAfee ePO
- Eliminar extensiones de un servidor de McAfee ePO
- Actualizar extensiones en un servidor de McAfee ePO

Configurar un conjunto de permisos

Puede actualizar los conjuntos de permisos para un rol existente o configurarlos para un rol nuevo.

Antes de empezar

Debe haber iniciado sesión en el servidor de McAfee ePO como administrador.

Procedimiento

1. En el menú de McAfee ePO, seleccione **Administración de usuarios** → **Conjuntos de permisos**.
2. En **Conjuntos de permisos**, seleccione un rol.
3. En el panel de configuración, haga clic en **Editar** para abrir cualquier conjunto de permisos.
4. Actualice la configuración en el conjunto de permisos y, a continuación, haga clic en **Guardar**.

Permisos necesarios para administrar Client Proxy

Se requieren permisos específicos para administrar Client Proxy.

Permisos de administrador de Client Proxy

Permisos	Configuración	Necesario para...
Controlador de agentes	Seleccione **Ver controladores de agentes**	• Insertar directivas en endpoints • Ver consultas
Eventos de cliente	Seleccionar **Ver eventos de cliente**	• Insertar directivas en endpoints • Ver consultas

Permisos	Configuración	Necesario para...
Common Catalog	Seleccione una **Plantilla de permisos de catálogo** y, a continuación, seleccione todas las acciones de Common Catalog: • **Crear, cambiar nombre y duplicar catálogos** • **Eliminar catálogos** • **Importar elementos de catálogo de otros catálogos** • **Importar elementos de catálogo de archivos** • **Exportar elementos de catálogo a archivos**	Crear, eliminar y administrar directivas
Acciones de Help Desk	Seleccione todas las acciones de Client Proxy: • **Generar clave de desinstalación de cliente** • **Generar clave de cliente de omisión** • **Generar clave de respuesta principal para las claves anteriores**	Realizar funciones de Help Desk **Note:** Los administradores de McAfee ePO los administradores tienen todos los permisos de Help Desk de forma predeterminada. Antes de poder otorgar estos permisos a otros administradores, primero debe instalar la extensión de Help Desk.
McAfee Agent	• **McAfee Agent: directiva**: seleccione **Ver y cambiar configuración** • **McAfee Agent: tareas**: seleccione **Ver y cambiar configuración**	• Insertar directivas en endpoints • Ver consultas
Directiva de MCP	Seleccione **Ver y cambiar la configuración de directivas y tareas**	Crear, eliminar y administrar directivas
Consultas e informes	Seleccione **Editar grupos públicos, crear y editar consultas e informes privados, hacer públicos las consultas e informes privados**	• Insertar directivas en endpoints • Ver consultas
Software	**Repositorio principal**: seleccione **Agregar, eliminar y cambiar paquetes; realizar tareas de extracción**	Realizar funciones del repositorio principal: • Agregar paquetes de software

Permisos	Configuración	Necesario para...
	Repositorios distribuidos: seleccione **Agregar, eliminar y cambiar repositorios; realizar tareas de replicación**	• Eliminar paquetes de software • Actualizar paquetes incorporados
Sistemas	**Árbol de sistemas**: seleccione **Ver la ficha "Árbol de sistemas"** **Acciones**: seleccione: • **Activar agentes; ver registro de actividad del agente** • **Editar sistemas y grupos del Árbol de sistemas** • **Desplegar agentes** **Uso de etiquetas**: seleccione **Aplicar, excluir y borrar etiquetas** **Catálogo de etiquetas**: seleccione **Crear y editar etiquetas, grupos de etiquetas y criterios de etiquetado**	• Insertar directivas en endpoints • Ver consultas
Acceso al Árbol de sistemas	Seleccione **Mi organización**	• Insertar directivas en endpoints • Ver consultas

Revisión y aprobación de directivas

Puede configurar la revisión y aprobación de directivas de Client Proxy en la interfaz de McAfee ePO.

Las tareas de configuración incluyen la creación de conjuntos de permisos, su asignación a los usuarios y la configuración de las opciones de aprobación en la página **Configuración del servidor**.

1. Creación de conjuntos de permisos de administración de directivas:
   - Conjunto de permisos de usuario de directivas: los usuarios de directivas tienen permiso para crear o editar directivas y deben enviar los cambios para su revisión.
   - Conjunto de permisos de administrador de directivas: los administradores de directivas tienen permiso para aprobar y guardar directivas nuevas o modificadas, o para rechazar los cambios.
2. Creación de usuarios de administración de directivas:
   - Usuario de directivas: cree este usuario y asígnele el conjunto de permisos de usuario de directivas.
   - Administrador de directivas: cree este usuario y asígnele el conjunto de permisos de administrador de directivas.

3. Configure las opciones de aprobación para los cambios de directiva en el panel **Aprobaciones** de la página **Configuración del servidor**.
    - Usuario de directivas: para requerir que los usuarios de directivas envíen los cambios de la directiva para su revisión, seleccione **Los usuarios necesitan aprobación para los cambios de la directiva**.
    - Administrador de directivas: para requerir que los administradores de directivas envíen también los cambios de la directiva para su revisión, seleccione **Los administradores y aprobadores necesitan aprobación para los cambios de la directiva**.

Para obtener más información, consulte la *Guía del producto de McAfee ePolicy Orchestrator*.

Cómo se utiliza la contraseña compartida

La contraseña compartida es la contraseña que asegura la comunicación entre Client Proxy y Web Gateway o McAfee WGCS. A veces, la contraseña compartida se denomina secreto compartido.

Si está configurando Client Proxy en un despliegue local, solo en la nube o híbrido, una contraseña compartida asegura la comunicación entre los productos y las directivas. Los detalles de configuración dependen de la plataforma de administración.

Administrado con McAfee ePO

1. Descargue su ID de cliente y la contraseña compartida desde un servidor de Web Gateway a un archivo .xml.
2. En la interfaz de McAfee ePO, importe sus credenciales desde el archivo .xml en la página **Configuración de cliente** mientras configura una directiva de Client Proxy.

Administrado con McAfee ePO Cloud

1. En la interfaz de McAfee ePO Cloud, configure la contraseña compartida en la página **Configuración de cliente** mientras configura una directiva de Client Proxy.
2. Para compartir sus credenciales de forma manual, exporte su ID de cliente y la contraseña compartida a un archivo .xml.

Administrado con MVISION ePO

1. Descargue su ID de cliente y la contraseña compartida desde un servidor de Web Gateway a un archivo .xml.
2. En la interfaz de MVISION ePO, importe sus credenciales desde el archivo .xml en la página **Administración de MCP**.

Despliegue híbrido

1. En la interfaz de McAfee ePO Cloud, configure la contraseña compartida y exporte sus credenciales a un archivo .xml.
2. En la interfaz de McAfee ePO, importe sus credenciales desde el archivo .xml.

Consideraciones al cambiar la contraseña compartida (McAfee ePO Cloud)

Al cambiar la contraseña compartida en la interfaz de McAfee ePO Cloud, conceda el tiempo suficiente para que se actualice en el sistema.

La actualización de la contraseña compartida implica estas acciones del sistema y estimaciones de tiempo:

1. McAfee ePO Cloud despliega la directiva de Client Proxy actualizada en los endpoints de su organización. El tiempo que tarda esta acción depende del valor configurado para el ajuste **Intervalo de implementación de directivas** en la directiva de McAfee Agent.
2. El software de Client Proxy en los endpoints comparte la nueva contraseña con McAfee WGCS. Esta acción puede tardar hasta 20 minutos.

Caution

La contraseña compartida debe estar sincronizada en McAfee WGCS o la autenticación falla.

Importar el ID de cliente y la contraseña compartida (MVISION ePO)

Al crear directivas de Client Proxy en MVISION ePO o migrar las directivas de Client Proxy desde el entorno local a MVISION ePO, descargue el ID de cliente y la contraseña compartida desde un servidor de gateway web a un archivo .xml e importe el archivo en la página **Administración de MCP**.

Note

La migración de directivas de Client Proxy del entorno local a MVISION ePO se admite desde Client Proxy 3.0.0 local y versiones posteriores. Para obtener información sobre cómo migrar McAfee ePO local a MVISION ePO, véase *Migración a MVISION ePO - Guía de inicio rápido* en el portal de documentación de productos de McAfee *(docs.mcafee.com)*.

Procedimiento

1. En el menú de MVISION ePO, seleccione **Configuración** → **Administración de MCP**.
2. Al lado del **Identificador de cliente**, haga clic en **Elegir archivo**. Vaya a la carpeta que contiene el archivo .xml, selecciónelo y haga clic en **Abrir**.

Resultados

El ID de cliente y la contraseña compartida se importan a Client Proxy. Todas las directivas existentes y nuevas se actualizan con el ID de cliente y la contraseña compartida importados.

Crear una instancia de Common Catalog (McAfee ePO o McAfee ePO Cloud)

Puede crear una instancia de Common Catalog para Client Proxy y, a continuación, seleccionarla cuando configure la lista de omisión en una directiva.

Antes de empezar

Debe iniciar sesión en el servidor de McAfee ePO o McAfee ePO Cloud como administrador.

Las instancias de catálogo de Client Proxy están disponibles globalmente. Puede asociar cada instancia con más de una directiva.

Un catálogo de Client Proxy consta de listas de elementos agrupados por estas categorías o tipos:

- Nombres de dominio
- Direcciones de red
- Puertos de red
- Nombres de proceso

En la página Common Catalog, puede crear y configurar una instancia de catálogo. Puede ver las listas de elementos de cada categoría y agregar, editar o eliminar elementos de las listas. Agregue tantas listas a la instancia del catálogo como necesite.

Procedimiento

1. En el menú de McAfee ePO o McAfee ePO Cloud, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista desplegable **Acciones** de la página **Lista de catálogos**, seleccione **Nuevo catálogo**.
3. Especifique un nombre para el nuevo catálogo y una descripción opcional y, a continuación, haga clic en **Aceptar**.
4. En **Origen/destino** en el panel **Common Catalog**, seleccione una categoría:
   - **Nombre de dominio**: el tráfico web enviado a los dominios de esta lista omite el servidor proxy. Ejemplo: google.com
   - **Dirección de red (IP)**: el tráfico web enviado a las direcciones IP de esta lista omite el servidor proxy. Las direcciones se pueden configurar individualmente, como un intervalo o mediante una subred.
     Entre los ejemplos se incluyen:
     - 192.168.1.1
     - 172.31.255.10–172.31.255.20
     - 10.50.0.0/255.255.128.0
     - 10.50.0.0/17
   - **Puerto de red**: el tráfico web enviado a los puertos de esta lista omite el servidor proxy. Ejemplos: 40, 80, 400–500
   - **Lista de nombres de procesos**: el tráfico web procedente de los procesos de esta lista omite el servidor proxy. Se ejecuta un proceso en los endpoints. Los nombres de proceso de Windows deben terminar con la extensión .exe. Los nombres de procesos de macOS no requieren una extensión de nombre de archivo. Agregue McAfee y otros procesos de confianza a esta lista.
5. En la lista desplegable **Acciones**, seleccione **Nueva**.
6. Especifique un nombre exclusivo para la lista o utilice el nombre predeterminado.
7. Haga clic en **Agregar** para agregar elementos a la lista y, a continuación, haga clic en **Guardar**.
   La lista se agrega a Common Catalog.

Resultados

La instancia de Common Catalog está configurada y guardada.

Configurar una directiva

Crear una directiva de Client Proxy

Una directiva de Client Proxy consta de una lista de servidores proxy, de ajustes de redireccionamiento, de una lista de omisión y de una lista de bloqueos que, en conjunto, determinan si y dónde Client Proxy redirige las solicitudes web.

Antes de empezar

Debe haber iniciado sesión en el servidor de McAfee ePO, McAfee ePO Cloud o MVISION ePO como administrador.

Puede crear una directiva nueva mediante una directiva existente como plantilla. Como plantilla, la directiva predeterminada es de solo lectura y no se puede cambiar de nombre, eliminarla, exportarla, importarla ni asignarla a los endpoints.

Procedimiento

1. En el menú principal, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista **Productos**, seleccione la versión actual de Client Proxy.
3. Haga clic en **Nueva directiva**.
4. En la lista desplegable **Crear una directiva basada en esta directiva existente**, seleccione una directiva existente para utilizarla como plantilla para la nueva directiva.
5. Especifique un nombre para la nueva directiva y, a continuación, haga clic en **Aceptar** para guardarlo.

   Note

   Cuando configure la primera directiva en un sistema Mac con Big Sur 11.2 o posterior, se mostrará una alerta para permitir el adaptador de red McAfeeSystemExtensions. Haga clic en **Permitir** para cargar McAfeeSystemExtensions. Client Proxy no redirigirá el tráfico hasta que usted elija la opción "permitir". Debe reiniciar Client Proxy manualmente para ver el panel de consentimiento de nuevo. Para obtener más información, consulte el artículo de la base de conocimiento de McAfee KB94092.

Resultados

Puede configurar la nueva directiva ahora o cancelar la configuración y seleccionar y editar la directiva desde el

Catálogo de directivas más tarde.

Cómo Client Proxy administra la lista de servidores proxy

El software de Client Proxy mantiene una lista ordenada de servidores proxy.

El servidor proxy con el tiempo de respuesta más rápido se sitúa en la parte superior de la lista. El software actualiza la lista de vez en cuando.

Por ejemplo, la lista se actualiza cuando el usuario inicia el equipo o cuando cambia la directiva de Client Proxy. También se actualiza si se interrumpe la conexión de VPN o si un servidor de proxy no responde. En estos momentos, el software prueba las conexiones a todos los servidores proxy y reordena la lista en función de los tiempos de respuesta.

Si el redireccionamiento al servidor proxy de la parte superior de la lista falla, el software intenta redirigir al segundo servidor proxy de la lista. Al mismo tiempo, el software prueba de nuevo las conexiones del servidor proxy y actualiza la lista.

Al configurar cómo el software de Client Proxy selecciona el siguiente servidor proxy de la lista, dispone de estas opciones:

- **conectar al primer servidor proxy accesible en función de su orden en la lista siguiente**: el software selecciona el siguiente servidor proxy de la lista que se configura.
- **conectar al servidor proxy que tiene el tiempo de respuesta más rápido**: el software selecciona el siguiente servidor proxy de la lista que mantiene, que se basa en el tiempo de respuesta.

Conmutación de proxy automática

Cuando esta opción está activada, el software comprueba la lista de servidores proxy en el intervalo especificado. Si hay disponible un servidor proxy de prioridad superior, el software cambiará automáticamente a él.

La opción de cambio de proxy automático solo está diposnible cuando está seleccionada la opción **conectar al primer servidor proxy accesible en función de su orden en la lista siguiente**.

Configurar la lista de servidores proxy

Para redirigir el tráfico web a un servidor proxy, configure la lista de servidores proxy y las reglas.

Antes de empezar

Debe haber iniciado sesión en el servidor de McAfee ePO, McAfee ePO Cloud o MVISION ePO como administrador.

Cuando configure la lista de servidores proxy, tenga en cuenta si Client Proxy se despliega con McAfee ePO, McAfee ePO Cloud o MVISION ePO.

- **Local**: configure al menos uno de los appliances de Web Gateway instalados en la red como servidor proxy.

- **En la nube**: configure McAfee WGCS como servidor proxy, utilizando este formato para el nombre de host: c<customer_id>.saasprotection.com.

Ejemplo: c12345678.saasprotection.com

Note

Para poder guardar la directiva, debe proporcionar la dirección IP o el nombre de host de al menos un servidor proxy y un número de puerto.

Note

Cuando habilita el ajuste de **canal seguro** con al menos un proxy en la nube configurado en la lista de servidores proxy, Client Proxy ignora los servidores proxy locales y solo tiene en cuenta los servidores proxy en la nube de la lista. En función de la disponibilidad del servidor proxy y el puerto en la nube, Client Proxy aplica la opción de redirección, bloqueo o respaldo (Permitir la conexión sin el canal seguro). Los servidores proxy con dominios como c*******.wgcs.mcafee-cloud.com y c*******.saasprotection.com se consideran servidores en la nube.

Procedimiento

1. En el menú principal, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista **Productos**, seleccione la versión actual de Client Proxy.
3. Haga clic en la **directiva de MCP** para ver la lista de directivas.
4. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.
5. En el menú **Configuración de Client Proxy**, seleccione **Servidores proxy**.
6. Para especificar cómo el software selecciona un servidor proxy de la lista, elija una opción:
   - **conectar al primer servidor proxy accesible en función de su orden en la lista siguiente**: el software selecciona el siguiente servidor proxy de la lista que se configura.
   - **conectar al servidor proxy que tiene el tiempo de respuesta más rápido**: el software selecciona el siguiente servidor proxy de la lista que mantiene, que se basa en el tiempo de respuesta.
7. Para agregar servidores proxy a la **Lista de servidores proxy**, configure estas opciones y, a continuación, haga clic en **Agregar**.
   - **Dirección del servidor proxy**: especifica la dirección IP o el nombre de host del servidor proxy.
   - **Puerto proxy**: especifica el número de puerto del servidor proxy.
   - **HTTP/HTTPS**: seleccione esta casilla de verificación para redirigir el tráfico enviado a los puertos 80 y 443 a un servidor proxy.
   - **Puertos redireccionados no HTTP/HTTPS**: especifica los números de puerto de los protocolos que no sean HTTP/HTTPS cuyo tráfico desee redirigir. Verifique que el servidor proxy admite estos protocolos. Puede introducir hasta 1024 caracteres en este campo.

8. Seleccione **Activar conmutación automática de proxy** y, a continuación, especifique un valor para el **Intervalo de sondeo** en este intervalo: 10 – 3600 segundos. El valor recomendado es 60 segundos.

   La opción de cambio de proxy automático solo está diposnible cuando está seleccionada la opción **conectar al primer servidor proxy accesible en función de su orden en la lista siguiente**.

   Note

   Cuando se utiliza la función **canal seguro**, el ajuste **Habilitar el cambio automático de proxy** no es aplicable a una lista de servidores proxy.

9. En el campo **Especificar puertos adicionales que desee redirigir como tráfico HTTP/HTTPS**, especifique los números de otros puertos cuyo tráfico desee redirigir como tráfico HTTP/HTTPS. Por ejemplo, puede redirigir el tráfico enviado a una aplicación. Puede introducir hasta 1024 caracteres en este campo.
10. Opcionalmente, seleccione **Bloquear el tráfico en los puertos configurados si no se puede acceder a ninguno de los servidores proxy primarios**.
    Cuando no se puede acceder a ninguno de los servidores proxy configurados, se bloquea todo el tráfico de los puertos configurados y los puertos predeterminados 80 y 443.
11. Seleccione **Bloquear el tráfico en los puertos configurados hasta que MCP esté listo** para proteger el endpoint mientras se está iniciando Client Proxy.
    Todo el tráfico a los puertos configurados y los puertos predeterminados 80 y 443 se bloquea desde el momento en el que el usuario tiene acceso a Internet hasta que Client Proxy sale del modo de omisión y empieza a redirigir el tráfico.
12. Seleccione **Bloquear el tráfico IPv6 en los puertos configurados** para requerir que los navegadores web retrocedan a IPv4.
13. Seleccione **Bloquear el tráfico cuando no se ha podido realizar la autenticación mutua con proxy principal** para asegurarse de que Client Proxy solo redirige las solicitudes web cuando puede autenticar el servidor proxy.
14. Anule la selección de **Omitir el servidor proxy para las direcciones locales** para redirigir todo el tráfico, incluido el tráfico enviado a direcciones locales dentro de la red de subred de su organización, a un servidor proxy. Puede configurar una dirección IP, un intervalo de direcciones IP, una subred o un CIDR. Por ejemplo, 192.168.1.1, 172.31.255.10-172.31.255.20, 10.50.0.0/255.255.128.0 o 10.50.0.0/17.
15. Seleccione **Bloquear tráfico UDP en los puertos 80/443 para IPv4 e IPv6** para bloquear este tráfico.
16. Haga clic en **Guardar**.

Resultados

La lista de servidores proxy se guarda con la directiva.

Configurar la lista de servidores proxy alternativos

Puede configurar servidores proxy alternativos y dividir el tráfico web seleccionado en varios servidores proxy. Cuando el servidor proxy alternativo está inactivo y el principal está disponible, Client Proxy redirige todo el tráfico al servidor proxy principal. Cuando un servidor proxy principal está inactivo, Client Proxy redirige el tráfico marcado como redireccionamiento alternativo al servidor proxy alternativo.

Antes de empezar

Debe haber iniciado sesión en el servidor de McAfee ePO, McAfee ePO Cloud o MVISION ePO como administrador.

Cuando configure la lista de servidores proxy, tenga en cuenta si Client Proxy se despliega con McAfee ePO, McAfee ePO Cloud o MVISION ePO.

- **Local**: configure al menos uno de los appliances de Web Gateway instalados en la red como servidor proxy.
- **En la nube**: configure McAfee WGCS como servidor proxy utilizando este formato para el nombre de host: c<customer_id>.saasprotection.com.

Ejemplo: c12345678.saasprotection.com

Note

Para poder guardar la directiva, debe proporcionar la dirección IP o el nombre de host de al menos un servidor proxy y un número de puerto.

Procedimiento

1. En el menú principal, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista **Productos**, seleccione la versión actual de Client Proxy.
3. Haga clic en la **directiva de MCP** para ver la lista de directivas.
4. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.
5. En el menú **Configuración de Client Proxy**, seleccione **Servidores proxy**.
6. Haga clic en la pestaña **Lista de servidores proxy alternativos**.
7. Para especificar cómo el software selecciona un servidor proxy de la lista, elija una opción:
   - **conectar al primer servidor proxy accesible en función de su orden en la lista siguiente**: el software selecciona el siguiente servidor proxy de la lista que se configura.
   - **conectar al servidor proxy que tiene el tiempo de respuesta más rápido**: el software selecciona el siguiente servidor proxy de la lista que mantiene, que se basa en el tiempo de respuesta.
8. Para agregar servidores proxy a la **Lista de servidores proxy**, configure estas opciones y, a continuación, haga clic en **Agregar**.
   - **Dirección del servidor proxy**: especifica la dirección IP o el nombre de host del servidor proxy.
   - **Puerto proxy**: especifica el número de puerto del servidor proxy.
   - **HTTP/HTTPS**: seleccione esta casilla de verificación para redirigir el tráfico enviado a los puertos 80 y 443 a un servidor proxy.

- **Puertos redireccionados no HTTP/HTTPS**: especifica los números de puerto de los protocolos que no sean HTTP/HTTPS cuyo tráfico desee redirigir. Verifique que el servidor proxy admite estos protocolos. Puede introducir hasta 1024 caracteres en este campo.

9. Seleccione **Activar el cambio automático de proxy para el proxy alternativo**, y, a continuación, especifique un valor para **Intervalo de sondeo (en segundos)** en este rango: 10–3600 segundos. El valor recomendado es 60 segundos.

   La opción de cambio de proxy automático solo está diposnible cuando está seleccionada la opción **conectar al primer servidor proxy accesible en función de su orden en la lista siguiente**.

10. Haga clic en **Guardar**.

Resultados

La lista de servidores proxy alternativos se guarda con la directiva.

Configurar los ajustes de cliente

Configure los ajustes que utiliza Client Proxy para determinar la ubicación del endpoint y cuándo redirigir el tráfico web. El software cliente prueba la conectividad al utilizar un protocolo de enlace de tres vías TCP para conectarse y, a continuación, cierra la conexión. El endpoint se puede ubicar dentro de la red, fuera de la red o conectado a la red mediante VPN.

Antes de empezar

Debe haber iniciado sesión en el servidor de McAfee ePO, McAfee ePO Cloud o MVISION ePO como administrador.

Note

Para poder guardar la directiva, debe proporcionar valores para el ID de cliente y la contraseña compartida.

Procedimiento

1. En el menú principal, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista **Productos**, seleccione la versión actual de Client Proxy.
3. Haga clic en la **directiva de MCP** para ver la lista de directivas.
4. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.
5. En la lista **Ajustes de Client Proxy**, seleccione **Configuración de cliente**.
6. Seleccione una opción en función de su plataforma de administración:
   - McAfee ePO: en la sección **Identificador de cliente**, haga clic en **Examinar** para localizar y, a continuación, abrir el archivo .xml del ID de cliente proporcionado por el administrador de Web Gateway o McAfee WGCS. Los valores de este archivo rellenan automáticamente los campos **ID de cliente exclusivo** y **Contraseña compartida**.
   - McAfee ePO Cloud: en la sección **Configurar contraseña compartida**, introduzca y confirme la contraseña que Client Proxy comparte con McAfee WGCS. También dispone de opciones para restablecer o exportar la contraseña.

- MVISION ePO: antes de crear directivas de Client Proxy en MVISION ePO o migrar directivas a MVISION ePO, importe el ID de cliente y la contraseña compartida en la página **Administración de MCP**. Después de haberlos importado correctamente, todas las directivas existentes y nuevas de Client Proxy se actualizan con el ID de cliente y la contraseña compartida importados.

Note

La migración de directivas de Client Proxy del entorno local a MVISION ePO se admite desde Client Proxy 3.0.0 local y versiones posteriores. Para obtener información sobre cómo migrar McAfee ePO local a MVISION ePO, consulte *Migración a MVISION ePO: guía de inicio rápido* en el portal de documentación de productos de McAfee *(docs.mcafee.com)*.

7. Seleccione un ajuste de **Canal seguro para proxy en la nube**:

Note

Esta opción solo es aplicable a McAfee WGCS.

- **Habilitar el canal seguro**: seleccione esta casilla para establecer una conexión segura entre Client Proxy y McAfee WGCS. Cuando selecciona esta casilla, el software valida el certificado de proxy en la nube con la tienda de certificados de dispositivos y establece una conexión segura.

Note

Cuando habilita el **Canal seguro**, Client Proxy utiliza el puerto 8081 para comprobar la conexión de proxy en la nube. Sin embargo, puede continuar configurando el puerto 8080 y el nombre del host del servidor proxy cuando añada un servidor proxy en la nube.

- **Bloquear si falla la validación**: seleccione esta casilla para bloquear el tráfico al servidor proxy en la nube cuando falle la validación del certificado.

Note

Cuando la validación del certificado de un servidor proxy falla, se bloquea el tráfico a ese servidor (principal o alternativo).

- Cuando experimente problemas de conexión con el puerto 8081 (puerto del canal seguro), puede decidir si permitir o bloquear la conexión. Seleccione una de las opciones siguientes:
  - **Bloquear conexión**: seleccione esta opción para bloquear la conexión.

Note

Cuando la validación del certificado de un servidor proxy falla, se bloquea el tráfico a ese servidor (principal o alternativo).

- **Permitir la conexión sin el canal seguro**: seleccione esta opción para permitir la conexión a través del puerto proxy configurado (8080) sin establecer una conexión segura entre Client Proxy y McAfee WGCS.

Note

Cuando seleccione esta opción, todos los servidores configurados (tanto los locales como los que están en la nube) se tendrán en cuenta para filtrar el tráfico. El orden para seleccionar un servidor proxy depende de la opción que haya seleccionado (**conectar con el primer servidor proxy accesible en función de su orden en la lista siguiente** o **conectar con el servidor proxy que tenga el tiempo de respuesta más rápido**) al configurar la lista de servidores proxy.

8. Seleccione el ajuste **Redireccionamiento de tráfico**:
   - **Redirigir el tráfico de red cuando el equipo no está conectado a la red corporativa y no funciona a través de VPN**: redirige las solicitudes web a un servidor proxy cuando los usuarios trabajan fuera de la red de su organización y no están conectados por VPN.
   - **Redirigir siempre el tráfico de red a los servidores proxy**: redirige todas las solicitudes web a un servidor proxy, incluidas las solicitudes de los usuarios que trabajan dentro de la red, fuera de la red o que trabajan conectados a la red mediante VPN.
9. Seleccione el ajuste **Detección de red corporativa**:
   - **al probar la conectividad con ePO**: si el software cliente puede conectarse al servidor de McAfee ePO, el endpoint se ubica dentro de la red.
   - **al probar la conectividad a cualquiera de los siguientes servidores corporativos**: si el software cliente puede conectarse a los servidores de red configurados, el endpoint se encuentra dentro de la red.
10. Para configurar **Detección de VPN corporativa**, especifique las direcciones y los números de puerto de uno o varios servidores de VPN. Si el software cliente puede conectarse a una VPN configurada, el endpoint está conectado a la red mediante VPN.
11. Mediante expresiones regulares, configure el **Filtro de grupos de Active Directory** para limitar los grupos del encabezado que el software cliente añade a las solicitudes web antes de redirigirlos al servidor proxy. La información de pertenencia a grupos no debe exceder los 4096 caracteres.
    Formato: <nombre_dominio>\\<nombre_grupo>
12. (macOS) Seleccione el ajuste **Archivo de registro**:
    - **Registrar mensajes con prioridad de error y crítica**
    - **Registrar mensajes con prioridad de error, crítica, información y advertencia**
    - **Registrar todos los mensajes (recomendado para la solución de problemas y la depuración)**
    - **No registrar ningún mensaje**

    Note

    En los endpoints con Windows, los archivos de registro se encuentran en esta carpeta: C:\Program Data\McAfee\MCP\Logs. Los mensajes de error críticos se guardan en un archivo denominado Mcp.log.

13. (Windows) Configure los ajustes de **Protección de acceso**:

- **Habilitar protección de acceso**: cuando se selecciona, los usuarios pueden deshabilitar el software cliente mediante el gestor de tareas de Windows, editar o eliminar archivos y cambiar los valores de registro.
- **Solicitar clave de versión para la desinstalación manual**: cuando se selecciona, los usuarios pueden solicitar un código de versión de un administrador y usarlo para desinstalar el software cliente. Cuando no se selecciona, los usuarios deben utilizar la función de desinstalación de Windows para desinstalar el software. El procedimiento recomendado es utilizar un código de versión para desinstalar el software.

14. Haga clic en **Guardar**.

Resultados

La configuración del cliente se guarda con la directiva de Client Proxy.

Configurar la lista de omisión (McAfee ePO o McAfee ePO Cloud)

La directiva de Client Proxy permite el tráfico web que coincide con los elementos de la lista de omisión para omitir el servidor proxy e ir directamente a Internet.

Antes de empezar

Debe iniciar sesión en el servidor de McAfee ePO o McAfee ePO Cloud como administrador.

Si la instancia de Common Catalog que desea asociar con esta directiva no existe, debe crearla antes de configurar la lista de omisión.

Procedimiento

1. En el menú de McAfee ePO o McAfee ePO Cloud, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista **Productos**, seleccione la versión actual de Client Proxy.
3. Haga clic en la **directiva de MCP** para ver la lista de directivas.
4. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.
5. En el menú **Configuración de Client Proxy**, seleccione **Lista de omisión**.
6. En la lista desplegable de **Common Catalog** en el panel **Lista de omisión**, seleccione una instancia de Common Catalog.
7. Añada elementos de lista desde el catálogo a la lista de omisión:
   a. En la lista desplegable **Acciones**, seleccione **Agregar elemento de lista de omisión** y, a continuación, seleccione una categoría.
   b. En el cuadro de diálogo **Elegir entre los valores existentes**, seleccione los elementos de la lista que desee agregar a la lista de omisión.
   c. (Opcional) Edite un elemento de la lista existente o agregue uno nuevo.

Caution

Los cambios realizados en este paso se aplican a todas las directivas que comparten esta instancia de Common Catalog.

d. Haga clic en **Aceptar**.

El cuadro de diálogo se cierra y se agregan los elementos de la lista seleccionados a la lista de omisión.

8. (Opcional) Edite o elimine los elementos de la lista de omisión.
9. Haga clic en **Guardar**.

Resultados

La lista de omisión y la instancia de Common Catalog se guardan con la directiva.

Configuración de la lista de redirecciones alternativas (McAfee ePO o McAfee ePO Cloud)

Puede configurar nombres de dominio, direcciones IP, puertos de red y nombres de procesos en una lista de redirecciones alternativas para redirigir tráfico web al servidor proxy de redirección alternativa. Puede ver las listas de los elementos añadidos a la lista de redirecciones alternativas y añadir, editar o eliminar elementos de las listas según sea necesario.

Antes de empezar

Debe iniciar sesión en el servidor de McAfee ePO o McAfee ePO Cloud como administrador.

Si la instancia de Common Catalog que desea asociar con esta directiva no existe, debe crearla antes de configurar la lista de redirecciones alternativas.

Procedimiento

1. En el menú de McAfee ePO o McAfee ePO Cloud, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista **Productos**, seleccione la versión actual de Client Proxy.
3. Haga clic en la **directiva de MCP** para ver la lista de directivas.
4. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.
5. En el menú **Configuración de Client Proxy**, seleccione **Lista de redirecciones alternativas**.
6. En la lista desplegable de **Common Catalog** del panel **Lista de redirecciones alternativas**, seleccione una instancia de Common Catalog.
7. Añada elementos del catálogo a la lista de redirecciones alternativas:
   a. En la lista desplegable **Acciones**, seleccione **Add Alternate Redirection** (Añadir redirección alternativa) y, después, seleccione una categoría.
   b. En el cuadro de diálogo **Elegir entre los valores existentes**, seleccione los elementos de la lista que quiere añadir a la lista de redirecciones alternativas.
   c. (Opcional) Edite un elemento de la lista existente o añada uno nuevo.

Caution

Los cambios realizados en este paso se aplican a todas las directivas que comparten esta instancia de Common Catalog.

d. Haga clic en **Aceptar**.

El cuadro de diálogo se cierra y los elementos de la lista seleccionados se añaden a la lista de redirecciones alternativas.

8. (Opcional) Puede editar o eliminar los elementos de la lista de redirecciones alternativas.
9. Haga clic en **Guardar**.

   La lista de redirecciones alternativas y la instancia de Common Catalog se guardan con la directiva.
10. (Opcional) Haga clic en **Duplicar** para duplicar la directiva Client Proxy seleccionada.

Configurar la lista de omisión (MVISION ePO)

Puede configurar nombres de dominio, direcciones de red, puertos de red y nombres de procesos en la lista de omisión. Puede ver las listas de elementos agregados a la lista de omisión y agregar, editar o eliminar elementos de las listas según sea necesario.

Antes de empezar

Debe iniciar sesión en el servidor de MVISION ePO como administrador.

Procedimiento

1. En el menú de MVISION ePO, seleccione **Directiva** → **Catálogo de directivas** → **McAfee Client Proxy**.
2. Haga clic en la **Directiva de MCP** para ver la lista de directivas.
3. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.
4. En **Configuración de Client Proxy**, haga clic en **Lista de omisión**.
5. En el panel **Lista de omisión**, seleccione una categoría:

   - **Nombre de dominio**: escriba el nombre de dominio y haga clic en **Agregar**. El tráfico web enviado a los dominios de esta lista omite el servidor proxy. Ejemplo: google.com
   - **Dirección de red (IP)**: especifique la dirección IP de la red y haga clic en **Agregar**. El tráfico web enviado a las direcciones IP de esta lista omite el servidor proxy. Las direcciones se pueden configurar individualmente, como un intervalo, mediante una subred o mediante CIDR.

     Entre los ejemplos se incluyen:

     - 192.168.1.1
     - 172.31.255.10–172.31.255.20
     - 10.50.0.0/255.255.128.0
     - 10.50.0.0/17
   - **Puerto de red**: especifique el número de puerto, su descripción y haga clic en **Agregar**. El tráfico web enviado a los puertos de esta lista omite el servidor proxy. Ejemplos: 40, 80, 400–500

- **Lista de procesos**: introduzca el nombre del proceso y haga clic en **Agregar**. El tráfico web procedente de los procesos de esta lista omite el servidor proxy. Se ejecuta un proceso en los endpoints. Los nombres de proceso de Windows deben terminar con la extensión .exe. Los nombres de procesos de macOS no requieren una extensión de nombre de archivo. Agregue McAfee y otros procesos de confianza a esta lista.

6. Haga clic en **Guardar**.
7. Opcionalmente, haga clic en **Duplicar** para duplicar una directiva.

Configuración de la lista de redirecciones alternativas (MVISION ePO)

Puede configurar nombres de dominio, direcciones IP, puertos de red y nombres de procesos en una lista de redirecciones alternativas para redirigir tráfico web al servidor proxy de redirección alternativa. Puede ver las listas de los elementos añadidos a la lista de redirecciones alternativas y añadir, editar o eliminar elementos de las listas según sea necesario.

Antes de empezar

Debe iniciar sesión en el servidor de MVISION ePO como administrador.

Procedimiento

1. En el menú de MVISION ePO, seleccione **Directiva** → **Catálogo de directivas** → **McAfee Client Proxy**.
2. Haga clic en la **Directiva de MCP** para ver la lista de directivas.
3. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.
4. En **Ajustes de Client Proxy**, haga clic en **Lista de redirecciones alternativas**.
5. En el panel **Lista de redirecciones alternativas**, seleccione una categoría:

   - **Nombre de dominio**: escriba el nombre de dominio y haga clic en **Añadir**. El tráfico web enviado a los dominios se redirige al servidor proxy alternativo. Ejemplo: google.com
   - **Dirección de red (IP)**: especifique la dirección IP de la red y haga clic en **Añadir**. El tráfico web enviado a las direcciones IP se redirige al servidor proxy alternativo. Las direcciones se pueden configurar individualmente, como un intervalo, mediante una subred o mediante CIDR.
     Entre los ejemplos se incluyen:

     - 192.168.1.1
     - 172.31.255.10–172.31.255.20
     - 10.50.0.0/255.255.128.0
     - 10.50.0.0/17

   - **Puerto de red**: especifique el número de puerto, su descripción y haga clic en **Añadir**. El tráfico web enviado a los puertos se redirige al servidor proxy alternativo. Ejemplos: 40, 80, 400–500
   - **Lista de procesos**: introduzca el nombre del proceso y haga clic en **Añadir**. El tráfico web procedente de los procesos se redirige al servidor proxy alternativo. Se ejecuta un proceso en los endpoints. Los nombres de proceso de

Windows deben terminar con la extensión .exe. Los nombres de procesos de macOS no requieren una extensión de nombre de archivo. Añada McAfee y otros procesos de confianza a esta lista.

6. Haga clic en **Guardar**.
7. Opcionalmente, haga clic en **Duplicar** para duplicar una directiva.

Importación o exportación de la lista de omisión (MVISION ePO)

Puede utilizar las opciones de importación y exportación para copiar las listas de omisión. Una vez que haya importado o exportado la lista de omisión, puede agregar, editar y eliminar los elementos de la lista de omisión. Es un buen método exportar la lista de omisión existente, modificarla e importar el archivo de nuevo. La importación de una lista de omisión sobrescribe todas las entradas de omisión existentes. Solo se admite el formato de archivo .txt para importar o exportar opciones.

A continuación, se muestra una lista de ejemplo de elementos de la lista de omisión:

```
tipo = DOMAIN google.com
intel.com tipo = NETWORKADDRESS 192.168.1.1
172.31.255.10 - 172.31.255.20
10.50.0.0/255.255.128.0
10.50.0.0/17 tipo = NETWORKPORT Descripción Número Puerto
80,443 Http/Https 21-47 Puerto con rango
22
31,78,100-500 tipo = PROCESSNAME chrome.exe
firefox.exe
xcode
```

Note

Puede agregar números de puerto sin descripciones, y el nombre del proceso es el nombre del proceso de Windows o macOS.

Procedimiento

1. En el menú de MVISION ePO, seleccione **Directiva** → **Catálogo de directivas** → **McAfee Client Proxy**.
2. Haga clic en la **Directiva de MCP** para ver la lista de directivas.
3. Haga clic en **Editar** en la misma fila que la directiva para la que desea importar o exportar la lista de omisión.
4. En **Configuración de Client Proxy**, haga clic en **Lista de omisión**.
5. En el panel **Lista de omisión**, haga lo siguiente:
   - Para exportar una lista de omisión, haga clic en **Exportar lista de omisión**. El navegador descarga la lista de omisión como un archivo .txt.
   - Para importar una lista de omisión, haga clic en **Importar lista de omisión**.
     - En el cuadro de diálogo, haga clic en **Elegir archivo** para navegar a la carpeta que contiene el archivo de la lista de omisión. Seleccione el archivo y, a continuación, haga clic en **Abrir**. Aparece un mensaje de confirmación después de importar la lista de omisión.

Note

Asegúrese de que la lista de elementos de la lista de omisión tenga el formato correcto. Si se produce un error en la importación, el cuadro de diálogo **Importar lista de omisión** devuelve el número de línea en el que se ha producido el error. Después de corregir los errores, puede importar el archivo de nuevo.

6. Haga clic en **Guardar**.

Importación o exportación de la lista de redirecciones alternativas (MVISION ePO)

Puede utilizar las opciones de importación y exportación para copiar las listas de redirecciones alternativas. Tras importar o exportar la lista de redirecciones alternativas, podrá añadir, editar y eliminar los nombres de dominios configurados en la lista de redirecciones alternativas. Es recomendable exportar la lista de redirecciones alternativas existente, modificarla e importar el archivo de nuevo. Importar una lista de redirecciones alternativas sobrescribe todas las entradas de redirección alternativas existentes. Solo se admite el formato de archivo .txt para importar o exportar opciones.

A continuación se enumera una lista de redirecciones alternativas de ejemplo:

```
tipo = DOMAIN google.com
intel.com
```

Procedimiento

1. En el menú de MVISION ePO, seleccione **Directiva** → **Catálogo de directivas** → **McAfee Client Proxy**.
2. Haga clic en la **Directiva de MCP** para ver la lista de directivas.
3. Haga clic en **Editar** en la misma fila que la directiva para la que desea importar o exportar la lista de redirecciones alternativas.
4. En **Configuración de Client Proxy**, haga clic en **Lista de redirecciones alternativas**.
5. En el panel **Lista de redirecciones alternativas**, realice una de las siguientes acciones:
   - Para exportar la lista de redirecciones alternativas, haga clic en **Exportar lista de redirecciones alternativas**. El navegador descarga la lista de redirecciones alternativas como un archivo .txt.
   - Para importar la lista de redirecciones alternativas, haga clic en **Importar lista de redirecciones alternativas**.
     - En el cuadro de diálogo, haga clic en **Elegir archivo** para navegar a la carpeta que contiene el archivo de la lista de redirecciones alternativas. Seleccione el archivo y, a continuación, haga clic en **Abrir**. Aparece un mensaje de confirmación después de importar la lista de redirecciones alternativas.

     Note

     Compruebe que la lista de nombres de dominios en la lista de redirecciones alternativas tenga el formato correcto. Si se produce un error en la importación, el cuadro de diálogo **Importar lista de redirecciones alternativas** devuelve el número de línea en el que se ha producido el error. Después de corregir los errores, puede importar el archivo de nuevo.

6. Haga clic en **Guardar**.

Configuración de la lista de bloqueos

Cada una de las directivas de Client Proxy está asociada a una lista de procesos bloqueados.

Antes de empezar

Debe haber iniciado sesión en el servidor de McAfee ePO, McAfee ePO Cloud o MVISION ePO como administrador.

Una lista de proceso es una lista de procesos que se ejecutan en los endpoints. Los nombres de proceso de Windows deben terminar con la extensión .exe. Los nombres de procesos de macOS no requieren una extensión de nombre de archivo.

Para reducir la cantidad de tráfico que se redirige al servidor proxy para el filtrado, configure una lista de los procesos de endpoint que están bloqueados para acceder a la red.

Procedimiento

1. En el menú principal, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista **Productos**, seleccione la versión actual de Client Proxy.
3. Haga clic en la **directiva de MCP** para ver la lista de directivas.
4. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.
5. En el menú de **Configuración de Client Proxy**, seleccione **Lista de bloqueos**.
6. Seleccione una opción:
   - **Permitir que el tráfico se dirija directamente al destino**: se permite que todos los procesos accedan a Internet sin pasar por un servidor proxy.
   - **Bloquear tráfico para todos los procesos (excepto los procesos de omisión listados)**: todos los procesos están bloqueados para acceder a Internet excepto los procesos de la lista de omisión.
   - **Bloquear el tráfico solo para los siguientes procesos**: se permite que todos los procesos accedan a Internet sin pasar por un servidor proxy excepto los que aparecen en esta lista. Configure la lista mediante las funciones **Agregar**, **Editar** y **Eliminar**.
7. Haga clic en **Guardar**.

Resultados

La lista de bloqueos se guarda con la directiva de Client Proxy.

Asignar una directiva a los endpoints

Puede asignar una directiva de Client Proxy a los endpoints mediante McAfee ePO, McAfee ePO Cloud o MVISION ePO.

Antes de empezar

Debe haber iniciado sesión en el servidor de McAfee ePO, McAfee ePO Cloud o MVISION ePO como administrador.

Procedimiento

1. En el menú principal, seleccione **Directiva** → **Catálogo de directivas**.
2. Seleccione el nivel organizativo en el que desea asignar la directiva.

   Para seleccionar todos los endpoints administrados por la plataforma, seleccione **Mi organización**.

3. Haga clic en **Directivas asignadas**.
4. En la lista desplegable **Producto**, seleccione la versión actual de McAfee Client Proxy.
5. En la columna **Acciones**, haga clic en **Editar asignación** en la misma línea que la directiva que desea asignar.
6. En **Heredar de**, seleccione **Interrumpir la herencia y asignar la directiva y los ajustes siguientes**.
7. En la lista desplegable **Directiva asignada**, seleccione la directiva.
8. Seleccione una opción para **Bloquear herencia de directivas**:
   - **Desbloqueada**: se puede asignar una directiva distinta a uno o varios subgrupos.
   - **Bloqueada**: esta directiva debe asignarse a todos los subgrupos.
9. Haga clic en **Guardar**.

Resultados

La directiva se asigna a los endpoints.

Exportar una directiva a un archivo .xml u .opg

Exporte una directiva de Client Proxy de McAfee ePO, McAfee ePO Cloud, o MVISION ePO a un archivo .xml o .opg.

Antes de empezar

Debe haber iniciado sesión en el servidor de McAfee ePO, McAfee ePO Cloud o MVISION ePO como administrador.

Para equipos independientes que no se gestionan con McAfee ePO o McAfee ePO Cloud, debe exportar la directiva a un archivo .opg y guardar el archivo de forma local en los equipos.

Procedimiento

1. En el menú principal, seleccione **Directiva** → **Catálogo de directivas**.
2. En la lista **Productos**, seleccione la versión actual de Client Proxy.
3. Haga clic en la **directiva de MCP** para ver la lista de directivas.
4. Haga clic en **Editar** en la misma fila que la directiva que desea configurar.

5. En la lista desplegable **Acciones**, seleccione **Exportar directiva a archivo**.
6. Haga clic con el botón derecho en el archivo de directiva que desee descargar y, a continuación, haga clic en **Guardar** → **Aceptar**.
   - **Archivo del servidor de directivas de McAfee Client Proxy**: exporta la directiva de Client Proxy a un archivo .xml que se puede utilizar para la solución de problemas.
   - **Archivo de cliente de la directiva de McAfee Client Proxy**: exporta la directiva de Client Proxy a un archivo .opg que se puede guardar en equipos autónomos o de endpoints.
7. Cambie el nombre del archivo .opg a MCPPolicy.opg y, a continuación, cópielo a esta ubicación en los equipos cliente:
   - Equipos basados en Windows: C:\ProgramData\McAfee\MCP\Policy\Temp
   - Equipos macOS: /usr/local/mcafee/mcp/policy

Resultados

Cuando Client Proxy comienza a ejecutarse en los equipos independientes o de endpoints, carga la directiva y empieza a redirigir el tráfico.

Suspenda la implementación de directivas en un equipo basado en Windows o macOS

Si un usuario necesita acceder a la información confidencial o transferirla por un motivo empresarial aprobado, puede suspender la implementación de directivas en un equipo independiente o de endpoints en el que se esté utilizando Windows o macOS.

Para suspender la implementación de directivas, siga el protocolo desafío-respuesta proporcionado por el software de Help Desk.

Procedimiento

1. **Usuario**: abre el cuadro de diálogo **Introducir el código de la versión**:
   - Windows: en el menú **Inicio**, haga clic en **McAfee** → **Omitir McAfee Client Proxy**.
   - macOS: en el menulet de McAfee en la barra de estado, seleccione **Consola** y, a continuación, **Client Proxy**.

   Caution

   Mientras espera el código de la versión, el usuario debe dejar abierto el cuadro de diálogo. Si el cuadro de diálogo está cerrado, el procedimiento se debe iniciar de nuevo.

2. **Usuario**: le envía un correo electrónico que incluye:
   - Nombre de usuario y dirección de correo electrónico
   - Número de la **Revisión de directiva y Nombre de la directiva** (copiado del cuadro de diálogo **Introducir el código de la versión**)

- Código de **Identificación** (copiado del cuadro de diálogo **Introducir el código de la versión**)

3. **Administrador**: mediante el software de Help Desk y los valores proporcionados por el usuario, genera el código de la versión y lo envía al usuario. En MVISION ePO, puede generar el código de la versión en la página **Administración de MCP**.
4. **Usuario**: introduce el código de la versión en el campo **Versión** y, a continuación, hace clic en **Aceptar** (Windows) o **Versión** (macOS).

Resultados

La implementación de directivas se suspende durante el periodo de tiempo especificado cuando se generó el código de la versión.

Consultas e informes

Crear y ejecutar una consulta de base de datos (McAfee ePO)

Cree y ejecute una consulta de base de datos para devolver información sobre las directivas y las tareas cliente.

Antes de empezar

Debe iniciar sesión en el servidor de McAfee ePO como administrador.

Note

Un administrador de McAfee ePO Cloud puede realizar consultas, pero no crearlas.

Procedimiento

1. En el menú de McAfee ePO, seleccione **Informes** → **Consultas e informes**.
2. En el menú **Grupos**, seleccione **Grupos de McAfee** → **McAfee Client Proxy** y, a continuación, haga clic en **Nueva consulta**.
3. En el **Generador de consultas**: en la lista **Grupo de funciones**, seleccione **Administración de directivas**.
4. Seleccione un **Tipo de resultado** y, a continuación, haga clic en **Siguiente**:
   - **Tareas cliente aplicadas**: devuelve los nombres de las tareas cliente y los niveles organizativos donde se aplicaron.
   - **Directivas aplicadas**: devuelve los nombres de las directivas y los niveles organizativos donde se aplicaron.
   - **Herencia interrumpida de la asignación de tareas cliente**: devuelve los nombres de las tareas cliente y los niveles organizativos donde se han interrumpido las asignaciones de tareas.
   - **Herencia interrumpida de la asignación de directivas**: devuelve los nombres de las directivas y los niveles organizativos donde se ha interrumpido la asignación de directivas.

   Se abre la página **Gráfico**.
5. Configure cómo desea que se muestren los resultados de la consulta en formato de gráfico:
   a. Seleccione un tipo de gráfico.
   b. Especifique las etiquetas, las unidades, los pedidos de clasificación y otros valores según proceda.
   c. Haga clic en **Siguiente**.

   Se abre la página **Columnas**.
6. Configure cómo desea que se muestren los resultados de la consulta en formato de tabla y, a continuación, haga clic en **Siguiente**:
   - En el menú **Columnas disponibles**, haga clic en los nombres de columna para seleccionarlos.
   - En el panel **Columnas seleccionadas**, cierre las columnas para eliminarlas.
   - Para reordenar las columnas seleccionadas, arrástrelas y suéltelas o utilice las teclas de flecha.

   Se abre la página **Filtro**.
7. Configure cómo desea que se filtren los resultados de la consulta:

   a. En el menú **Propiedades disponibles**, haga clic en los nombres de propiedad para seleccionarlos.
   b. En la lista desplegable **Comparación**, seleccione un operador para cada propiedad.
   c. Para cada operador, seleccione un valor.
8. Haga clic en **Ejecutar** para ver los resultados de la consulta y, a continuación, haga clic en **Editar consulta** para realizar cambios según sea necesario.
9. Haga clic en **Guardar** y, a continuación, en la página **Guardar consulta**:
   a. Especifique un nombre y una descripción opcional para la consulta.
   b. Seleccione un grupo existente o especifique un grupo nuevo.
   c. Haga clic en **Guardar**.

Resultados

La consulta de base de datos se guarda para su uso posterior.

Crear un informe de Client Proxy (McAfee ePO o MVISION ePO)

Salida en formato .pdf del número de endpoints en los que la instalación de Client Proxy se ha realizado correctamente o ha fallado durante el último mes.

Antes de empezar

Debe iniciar sesión en el servidor de McAfee ePO o MVISION ePO como administrador.

Procedimiento

1. En el menú de McAfee ePO o MVISION ePO, seleccione **Informes** → **Consultas e informes**.
2. En la lista **Grupos**, seleccione **Grupos de McAfee** → **McAfee Client Proxy**.
3. Haga clic en la ficha **Informes** y, a continuación, haga clic en **Nuevo informe**.
4. En el **Cuadro de herramientas**, arrastre una o varias plantillas al área **Diseño de informe** y, a continuación, configúrelas y colóquelas:
   - **Imagen**
   - **Salto de página**
   - **Gráfico de consulta**
   - **Tabla de consultas**
   - **Texto**

   Note

   Cuando agregue un gráfico o una tabla de consultas, seleccione **MCP: eventos correctos o fallidos de la instalación de endpoint en el último mes** de la lista desplegable **Consulta**.

5. Para personalizar el informe, haga clic en estas opciones:
    - **Encabezado y pie de página**
    - **Configuración de página**
    - **Parámetros en tiempo de ejecución**
6. Haga clic en **Ejecutar** para ver el informe en formato .pdf.
7. Haga clic en **Guardar** y, a continuación, en el cuadro de diálogo **Nombre, descripción y grupo**:
    a. Especifique un nombre y una descripción opcional para el informe.
    b. Seleccione un grupo existente o especifique un grupo nuevo.
    c. Haga clic en **Aceptar**.

Resultados

El informe de Client Proxy se ha guardado y se puede volver a utilizar.

COPYRIGHT

Copyright © 2022 Musarubra US LLC.

McAfee y el logotipo de McAfee son marcas comerciales o marcas registradas de McAfee, LLC o sus filiales en EE. UU. y otros países. Otros nombres y marcas pueden ser reclamados como propiedad de terceros.

Trellix