McAfee®

VirusScan USB

Guía del usuario

Contenido

CAPÍTULO 1

McAfee VirusScan USB

VirusScan USB ofrece protección total, fiable y actualizada para su unidad USB. Protege el contenido de la unidad USB frente a virus, troyanos, software espía, software publicitario y otros programas potencialmente no deseados (PUP).

En este capítulo

Funciones

VirusScan USB ofrece las funciones siguientes:

Análisis en tiempo real

Cuando está habilitado, el análisis en tiempo real de VirusScan USB controla constantemente la unidad USB para localizar cambios en los archivos (por ejemplo, un nuevo archivo agregado a la unidad o una modificación realizada en un archivo que ya estuviera en la unidad). Si el análisis en tiempo real detecta un cambio en un archivo, VirusScan USB analiza el archivo afectado para descubrir la actividad de los virus. Si se detecta un virus o un troyano, VirusScan USB intenta limpiarlo; si no puede limpiarse, VirusScan USB intenta cambiarle el nombre. Si se detecta software espía, software publicitario y otros programas potencialmente no deseados, puede definirlos como fiables o bien eliminarlos.

Análisis bajo demanda

La exploración bajo demanda le permite analizar su unidad USB en busca de virus, Troyanos, software espía y publicitario, y otros programas potencialmente no deseados en cualquier momento.

Opciones de exploración

Puede personalizar el comportamiento de VirusScan USB mediante la configuración de las opciones de análisis. Por ejemplo, puede especificar los tipos de archivo objeto de análisis (archivos, subcarpetas y procesos activos) y las ubicaciones que se vayan a analizar. También puede habilitar o deshabilitar el análisis en tiempo real.

Análisis automático

Cuando se instala VirusScan USB, se agrega a la lista de programas de la plataforma U3 Launchpad y se configura para que se inicie en el momento de la inserción. Esto significa que se inicia un análisis bajo demanda de VirusScan USB cada vez que se introduce una unidad USB en el equipo.

Resumen de análisis

Mientras se ejecuta un análisis, VirusScan USB muestra el número de elementos analizados, infectados o a los que se ha cambiado el nombre por encima de la barra de progreso del análisis. Cuando se detecta una infección y finaliza un análisis, puede ver un resumen de los resultados, lo que incluye la ruta y el nombre de cada archivo infectado, así como la operación realizada en ese archivo (por ejemplo, limpiado o cambiado el nombre). También puede ver información detallada acerca de cada archivo infectado, incluido el tipo de objeto, el nombre, el estado y el nombre del archivo.

CAPÍTULO 2

Instalación y actualización de VirusScan USB

Instale VirusScan USB en su unidad USB de la misma forma en la que instala la mayoría de los programas U3 USB; la única diferencia es que debe registrarse con McAfee. Al registrarse, podrá recibir actualizaciones del programa VirusScan USB y de archivos de definición de virus cuando aparezcan. Si se va a registrar con McAfee por primera vez, deberá indicar su nombre, una dirección de correo electrónico válida y una contraseña. Si ya está registrado con McAfee, deberá iniciar sesión con la dirección de correo electrónico y la contraseña que haya indicado en el registro anterior.

Tras instalar y registrar VirusScan USB, puede actualizarlo con los últimos archivos de protección de virus (DAT) en cualquier momento. Las actualizaciones se ejecutan en segundo plano; puede incluso ejecutar un análisis o cerrar un programa mientras una actualización está en curso. Si está habilitado el análisis en tiempo real, VirusScan USB ejecuta una actualización automática cada cuatro horas. Para obtener más información acerca del análisis en tiempo real, consulte Configuración de opciones de análisis (página 11).

Nota: si la unidad USB se suministra con un programa antivirus ya instalado, McAfee le recomienda que elimine ese programa antes de instalar VirusScan USB.

En este capítulo

Instalar VirusScan USB

Instale VirusScan USB en su unidad USB de la misma forma en la que instala la mayoría de los programas U3 USB; la única diferencia es que debe registrarse con McAfee. Al registrarse, podrá recibir actualizaciones del programa VirusScan USB y de archivos de definición de virus cuando aparezcan.

1. Introduzca la unidad USB en el equipo.
2. En la plataforma U3 Launchpad, haga clic en **Agregar programas** y, a continuación, en **Instalar desde mi equipo**.
3. En el cuadro de diálogo Abrir, acceda a la carpeta donde esté almacenado el archivo de instalación, seleccione el archivo y, a continuación, haga clic en **Abrir**.
4. En el Asistente para agregar programas, haga clic en **Siguiente**.
5. En el cuadro de diálogo Seleccione su país, haga clic en la combinación de país e idioma que mejor represente su ubicación actual y, a continuación, haga clic en **Siguiente**.
6. En el cuadro de diálogo Configuración del programa, revise la política de privacidad y después haga clic en **Siguiente**.
7. En el cuadro de diálogo de Acuerdo de licencia del usuario de McAfee, seleccione un país, revise el acuerdo de licencia de usuario y, a continuación, haga clic en **Aceptar**.
8. Siga uno de estos procedimientos:
   - Si se va a registrar por primera vez, escriba su nombre, primer apellido, dirección de correo electrónico, contraseña y confirmación de contraseña en las casillas apropiadas y, a continuación, haga clic en **Enviar**.
   - Si ya ha registrado previamente un programa con McAfee, haga clic **Iniciar sesión**, escriba la dirección de correo electrónico y la contraseña asociadas a su cuenta de McAfee y, a continuación, haga clic en **Iniciar sesión**.
9. En el cuadro de diálogo Instalación del programa finalizada, grabe su información de registro y después haga clic en **Finalizar**.

Sugerencia: también puede ejecutar el archivo de instalación de VirusScan USB directamente desde un sitio Web. En el sitio Web, inicie la descarga y haga clic en **Sí** ante cualquier advertencia de seguridad que aparezca y que le pregunte si quiere descargar el archivo. A continuación, ejecute el archivo de instalación y siga las instrucciones indicadas en el asistente de instalación.

Actualizar VirusScan USB

Una vez instalado VirusScan USB en su unidad USB, cada vez que conecte la unidad en su equipo se ejecutará una actualización. Asimismo, puede actualizar VirusScan USB manualmente con las últimas actualizaciones del programa o de archivos de definición de virus en cualquier momento. Las actualizaciones se ejecutan en segundo plano; puede incluso ejecutar un análisis o cerrar un programa mientras una actualización está en curso.

1. En el panel principal de VirusScan USB, haga clic en **Actualizar**.
2. Haga clic en **Aceptar**.

Nota: para actualizar VirusScan USB, deberá estar conectado a Internet.

CAPÍTULO 3

Configuración de las opciones de análisis

Puede personalizar el comportamiento de VirusScan USB mediante la configuración de las opciones de análisis. Por ejemplo, puede especificar los tipos de archivo objeto de análisis (archivos, subcarpetas y procesos activos) y las ubicaciones que se vayan a analizar. También puede habilitar o deshabilitar el análisis en tiempo real. Cuando está habilitado, el análisis en tiempo real controla constantemente la unidad USB para localizar cambios en los archivos (por ejemplo, un nuevo archivo agregado a la unidad o una modificación realizada en un archivo que ya estuviera en la unidad). Si el análisis en tiempo real detecta un cambio en un archivo, VirusScan USB analiza el archivo afectado para descubrir la actividad de los virus. Si se detecta un virus o un troyano, VirusScan USB intenta limpiarlo; si no puede limpiarse, VirusScan USB intenta cambiarle el nombre. Si se detecta software espía, software publicitario y otros programas potencialmente no deseados, puede definirlos como fiables o bien eliminarlos.

De forma predeterminada, el análisis en tiempo real está habilitado y McAfee recomienda que no se deshabilite. Cuando está habilitado el análisis en tiempo real, se analizan todos los tipos de archivos; cuando se ejecuta un análisis bajo demanda, VirusScan USB analiza los tipos y ubicaciones de archivos especificados en las opciones de análisis. Para obtener más información acerca de la ejecución de un análisis bajo demanda, consulte Análisis de la unidad USB (página 19).

Cuando se instala VirusScan USB, se agrega a la lista de programas de la plataforma U3 Launchpad y se configura para que se inicie en el momento de la inserción. Esto significa que se inicia un análisis bajo demanda de VirusScan USB cada vez que se introduce una unidad USB en el equipo. Si deshabilita la opción de inicio en el momento de la inserción en la plataforma U3 Launchpad, sólo se iniciará un análisis bajo demanda de VirusScan USB la primera vez que introduzca una unidad USB en el equipo. A continuación, puede configurar VirusScan USB para iniciar o no iniciar el análisis en el momento de la inserción. Si configura VirusScan USB para que no inicie un análisis en el momento de la inserción, VirusScan USB no se iniciará hasta que el análisis en tiempo real detecte una infección, o si lo inicia manualmente. McAfee recomienda no deshabilitar la opción de iniciar análisis en el momento de la inserción en VirusScan USB.

En la tabla siguiente se describen las opciones de análisis en VirusScan USB:

Opción	Descripción
Analizar todos los archivos	Se analizan todos los tipos de archivos.
Analizar subcarpetas	Se analizan subcarpetas (carpetas incluidas en otras carpetas).
Buscar virus nuevos desconocidos con la opción de heurística	Los archivos se comparan con las firmas de virus conocidas para detectar indicios de virus no identificados. Esta opción proporciona el análisis más completo, pero suele resultar más lenta que un análisis normal.
Buscar en archivos .zip y otros archivos de almacenamiento	Se analizan archivos de almacenamiento, incluidos los archivos .zip:
Buscar software espía y programas potencialmente no deseados	Los archivos se escanean en busca de software espía, software publicitario y otros programas potencialmente no deseados.
Analizar procesos activos	Se analizan los programas que se ejecutan en el equipo.
Analizar análisis al abrir VirusScan USB	El análisis empieza al abrir VirusScan USB.

En este capítulo

Configurar tipos de archivo analizados

Puede especificar los tipos de archivo que se han analizado en su unidad USB durante un análisis bajo demanda. Por ejemplo, puede determinar si se han analizado subcarpetas y archivos, y si desea analizar si hay software espía, software publicitario y otros programas potencialmente no deseados. También puede determinar si desea que VirusScan USB empiece el análisis cuando lo abra.

1. En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
2. En el panel Opciones de análisis, en **Opciones**, seleccione o anule la selección de las casillas de verificación correspondientes:
3. Haga clic en **Aceptar**.

Configurar las ubicaciones que se van a analizar

Puede especificar las ubicaciones (unidades USB) que quiera analizar en un análisis bajo demanda. Debido a que VirusScan USB sólo analiza unidades asociadas a su unidad USB, las unidades de disco que no estén asociadas a ella no aparecen en **Unidades para analizar en esta unidad USB**. Aquí se incluyen unidades extraíbles en el equipo y unidades asociadas a otras unidades USB.

1. En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
2. En el panel Opciones de análisis, en **Unidades para analizar en esta unidad USB**, marque o desactive las casillas de verificación adecuadas.
3. Haga clic en **Aceptar**.

En la tabla siguiente se describen las unidades USB que puede analizar:

Unidad	Descripción
Sistema U3	(El nombre de la unidad que se muestra puede ser diferente.) Se analiza la partición del CD-ROM en la unidad. Esta es la ubicación en la que se almacenan los archivos del sistema U3.
Mi unidad U3	(El nombre de la unidad que se muestra puede ser diferente.) Se analiza la partición de datos en la unidad. Esta es la letra de la unidad asignada a la unidad USB.

Deshabilitar el análisis en tiempo real

Cuando está habilitado, el análisis en tiempo real de VirusScan USB controla constantemente la unidad USB para localizar cambios en los archivos (por ejemplo, un nuevo archivo agregado a la unidad o una modificación realizada en un archivo que ya estuviera en la unidad). Si el análisis en tiempo real detecta un cambio en un archivo, VirusScan USB analiza el archivo afectado para descubrir la actividad de los virus. Si se detecta un virus o un troyano, VirusScan USB intenta limpiarlo; si no puede limpiarse, VirusScan USB intenta cambiarle el nombre. Si se detecta software espía, software publicitario y otros programas potencialmente no deseados, puede definirlos como fiables o bien eliminarlos.

El análisis en tiempo real controla todos los tipos de archivo (independientemente de la configuración del análisis bajo demanda). McAfee recomienda no deshabilitar el análisis en tiempo real.

1. En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
2. En el panel Opciones de análisis, en **Análisis en tiempo real**, desactive la casilla de verificación **Habilitar análisis en tiempo real de unidad USB**.
3. Haga clic en **Aceptar**.

Nota: si se habilita el control en tiempo real, podría detectarse un archivo infectado mientras el análisis bajo demanda está en curso. Para garantizar que se informe de la infección al menos una vez, el análisis en tiempo real muestra una alerta como de costumbre.

Iniciar un análisis en el momento de la inserción

Cuando se instala VirusScan USB, se agrega a la lista de programas de la plataforma U3 Launchpad y se configura para que se inicie en el momento de la inserción. Esto significa que se inicia un análisis bajo demanda de VirusScan USB cada vez que se introduce una unidad USB en el equipo. Si deshabilita la opción de inicio en el momento de la inserción en la plataforma U3 Launchpad, se iniciará un análisis bajo demanda de VirusScan USB la primera vez que introduzca una unidad USB en su equipo. A continuación, puede configurar VirusScan USB para iniciar o no iniciar el análisis en el momento de la inserción. Si configura VirusScan USB para que no inicie un análisis en el momento de la inserción, VirusScan USB no se inicia hasta que el control en tiempo real detecta una infección o se inicia manualmente. McAfee recomienda no deshabilitar la opción de iniciar análisis en el momento de la inserción en VirusScan USB.

1. En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
2. En el panel Opciones de análisis, en **Opciones**, asegúrese de que esté marcada la casilla de verificación **Iniciar análisis en el momento de la inserción**.
3. Haga clic en **Aceptar**.

Sugerencia: también puede marcar la casilla **Iniciar análisis en el momento de la inserción** en el panel Progreso del análisis cuando finalice o se cancele un análisis.

Mostrar mensajes informativos

Si decide que quiere mostrar algunas alertas y cuadros de diálogo de VirusScan USB que había decidido ocultar, puede hacerlo.

1. En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Configurar**.
2. En el panel Opciones de análisis, en **Análisis en tiempo real**, marque la casilla de verificación **Mostrar mensajes informativos**.
3. Haga clic en **Aceptar**.

CAPÍTULO 4

Trabajar con alertas

McAfee utiliza alertas para ayudarle a gestionar la seguridad. Las alertas se agrupan en tres tipos básicos:

- Alerta roja
- Alerta amarilla
- Alerta verde

A continuación, puede elegir la forma de gestionar los archivos detectados, conforme a las recomendaciones de las alertas.

En este capítulo

Acerca de las alertas

El control en tiempo real de VirusScan USB tiene tres tipos de alerta básicas: roja, amarilla y verde.

Alerta roja

Las alertas rojas indican que se ha detectado un archivo infectado, pero no se ha podido limpiar ni cambiar de nombre. Estas alertas le permiten eliminar el archivo infectado de la unidad USB u omitir la infección.

Alerta amarilla

Las alertas amarillas indican que se ha detectado un archivo infectado y que no ha podido limpiarse, pero al que se le ha cambiado el nombre por la extensión .vir. Estas alertas le permiten eliminar el archivo infectado de la unidad USB u omitir la infección.

Alerta verde

Las alertas verdes indican que se ha detectado y limpiado un archivo infectado. Dado que estas alertas son principalmente informativas, puede decidir no mostrarlas de nuevo.

CAPÍTULO 5

Análisis de la unidad USB

Cuando se instala VirusScan USB, se agrega a la lista de programas de la plataforma U3 Launchpad y se configura para que se inicie en el momento de la inserción. Esto significa que se inicia un análisis bajo demanda de VirusScan USB cada vez que se introduce una unidad USB en el equipo. Si deshabilita la opción de inicio en el momento de la inserción en la plataforma U3 Launchpad, sólo se iniciará un análisis bajo demanda de VirusScan USB la primera vez que introduzca una unidad USB en el equipo. A continuación, puede configurar VirusScan USB para iniciar o no iniciar el análisis en el momento de la inserción. Si configura VirusScan para que no inicie el análisis en el momento de la inserción, VirusScan USB no se inicia hasta que el análisis en tiempo real detecta una infección o puede ejecutar un análisis bajo demanda. Cuando se ejecuta un análisis bajo demanda, VirusScan USB analiza los tipos de archivo y las ubicaciones en sus opciones de análisis. Para obtener más información sobre la configuración de las opciones de análisis bajo demanda, consulte Configuración de las opciones de análisis (página 11).

Nota: McAfee recomienda no deshabilitar la opción de iniciar el análisis en el momento de la inserción en VirusScan USB.

Cuando VirusScan USB detecta un virus o troyano en uno de los archivos de una unidad USB, realiza una de las siguientes operaciones:

- Limpiar: el virus o troyano se elimina del archivo.
- Cambiar el nombre: se cambia de nombre el archivo por la extensión .vir (si las operaciones de limpieza han fallado).

Si fallan tanto las operaciones de limpieza como de cambio de nombre, puede eliminar el archivo infectado. Para obtener más información, consulte Eliminar un archivo infectado (página 24).

Si se detecta software espía, software publicitario y otros programas potencialmente no deseados, puede definirlos como fiables o bien eliminarlos.

- Definir como fiable: el programa potencialmente no deseado se define como fiable y no se elimina, incluso durante futuros análisis.
- Eliminar: el programa potencialmente no deseado se elimina de forma permanente.

Tras iniciar el análisis de la unidad USB, puede realizar una pausa y reanudarlo después desde ese punto en un momento más apropiado. Por ejemplo, si está realizando una tarea que consume muchos recursos cuando VirusScan USB esté analizando, puede pausar el análisis y reanudarlo después cuando finalice la otra tarea. Asimismo, puede cancelar un análisis en cualquier momento.

En este capítulo

Analizar la unidad USB

Puede analizar la unidad USB en cualquier momento. Por ejemplo, si acaba de instalar VirusScan USB, puede realizar un análisis para comprobar que su unidad USB no tiene virus ni otras amenazas.

- En el panel izquierdo de VirusScan USB, haga clic en **Analizar**.

Pausar el análisis

Puede pausar un análisis en curso. De este modo, se detiene el análisis en un punto específico y puede reanudar el análisis desde ese punto cuando lo crea conveniente.

- En el panel Progreso del análisis, en **Progreso del análisis**, haga clic en **Pausar**.

Sugerencia: para reanudar el análisis desde el punto en que lo pausó, haga clic en el botón **Reanudar** .

Reanudar el análisis

Cuando se pausa un análisis, se detiene temporalmente. Puede reanudar el análisis desde el punto en el que lo pausó. Para obtener más información acerca de pausar un análisis, consulte Pausar el análisis (página 20).

- En el panel Progreso del análisis, en **Progreso del análisis**, haga clic en **Reanudar**.

Cancelar el análisis

Puede cancelar (terminar) un análisis en todo momento. A diferencia de pausar, no se puede reanudar un análisis cancelado.

- En el panel Progreso del análisis, en **Progreso del análisis**, haga clic en **Cancelar** y luego en **Finalizar**.

CAPÍTULO 6

Trabajar con los resultados de análisis

Mientras se ejecuta un análisis, VirusScan USB muestra el número de elementos analizados, infectados o a los que se ha cambiado el nombre por encima de la barra de progreso del análisis. Cuando se detecta una infección y finaliza un análisis, puede ver un resumen de los resultados, lo que incluye la ruta y el nombre de cada archivo infectado, así como la operación realizada en ese archivo (por ejemplo, limpiado o cambiado el nombre). También puede ver información detallada acerca de cada archivo infectado, incluido el tipo de objeto, el nombre, el estado y el nombre del archivo.

Si VirusScan USB detecta un virus o troyano en uno de los archivos de su unidad USB, intenta limpiar el archivo infectado. Si la operación de limpieza falla, VirusScan USB intenta cambiar el nombre del archivo. Si fallan tanto la operación de limpieza como la de cambio de nombre, puede eliminar el archivo de la unidad USB.

Si se detecta software espía, software publicitario y otros programas potencialmente no deseados, puede definirlos como fiables o bien eliminarlos. Si define como fiables programas potencialmente no deseados, se agregarán a una lista de programas de confianza para que ya no vuelvan a detectarse. Si definió como fiable un programa por error, o bien desea que se detecte, debe eliminarlo de dicha lista bloqueándolo de nuevo.

VirusScan USB también muestra un resumen del último análisis en el panel de inicio para que pueda revisar los procesos analizados, los procesos infectados, los archivos analizados, los archivos infectados y la fecha del último análisis.

En este capítulo

Ver los resultados de un análisis

Cuando finaliza un análisis, puede consultar los resultados para ver una lista de elementos infectados.

1. En el panel Progreso del análisis, haga clic en **Ver resultados**.
2. En el panel Resultados del análisis, haga clic en el nombre de un archivo infectado o de un programa potencialmente no deseado.
3. En **Detalles**, consulte la información más específica sobre el archivo infectado o el programa potencialmente no deseado.
4. Haga clic en **Finalizar**.

Nota: el botón **Ver resultados** sólo aparece cuando se detectan archivos infectados.

Eliminar un archivo infectado

Si VirusScan USB detecta un virus o troyano en uno de los archivos de su unidad USB, intenta limpiar el archivo infectado. Si la operación de limpieza falla, VirusScan USB intenta cambiar el nombre del archivo. Si fallan tanto la operación de limpieza como la de cambio de nombre, puede eliminar el archivo de la unidad USB.

1. En el panel Progreso del análisis, haga clic en **Ver resultados**.
2. En el panel Resultados del análisis, haga clic en el nombre del archivo infectado.
3. En **Deseo**, haga clic en **Eliminar**.
4. Haga clic en **Finalizar**.

Eliminar un programa potencialmente no deseado

Una vez que VirusScan USB ha detectado software espía, software publicitario y otros programas potencialmente no deseados, puede eliminarlos. Al eliminar estos programas, se eliminan de la unidad.

1. En el panel Progreso del análisis, haga clic en **Ver resultados**.
2. En el panel Resultados del análisis, haga clic en un programa potencialmente no deseado.
3. En **Deseo**, haga clic en **Eliminar**.
4. Haga clic en **Finalizar**.

Definir como fiable un programa potencialmente no deseado

Una vez que VirusScan USB ha detectado software espía, software publicitario y otros programas potencialmente no deseados, puede definirlos como fiables. Si define como fiables estos programas, pero más tarde desea bloquearlos, consulte Bloquear un programa fiable (página 26).

1. En el panel Progreso del análisis, haga clic en **Ver resultados**.
2. En el panel Resultados del análisis, haga clic en un programa potencialmente no deseado.
3. En **Deseo**, haga clic en **Definir como fiable**.
4. Haga clic en **Finalizar**.

Bloquear un programa fiable

Si define como fiable un programa por error, o bien desea que se detecte, debe eliminarlo de la lista de la lista de confianza.

1. En el panel de inicio de VirusScan USB, en **Opciones de análisis actuales**, haga clic en **Listas de confianza**.
2. En la lista **Programas de confianza**, seleccione un programa.
3. En **Deseo**, haga clic en **Bloquear**.
4. Haga clic en **Aceptar**.

Ver el último resumen de análisis

Para su comodidad, VirusScan USB muestra un resumen del último análisis en el panel de inicio.

- En el panel de inicio de VirusScan USB, consulte los detalles en **Resumen del último análisis**.

Ver el resumen de programa VirusScan USB

En el panel de inicio, VirusScan USB muestra cuándo caduca, la fecha en la que se produjo la comprobación de la última actualización y la versión actual de los archivos de definición de virus (DAT).

- En el panel de inicio de VirusScan USB, consulte los detalles en **Resumen de programa**.

CAPÍTULO 7

Protección del equipo

VirusScan USB no controla ni analiza los archivos almacenados en el equipo. Esta protección la proporciona McAfee VirusScan. Puede descargar una versión completa o de prueba de VirusScan desde el sitio de descarga de McAfee.

En este capítulo

Descargar software antivirus para su equipo

Puede descargar una versión completa o de prueba de McAfee VirusScan.

1. En **Información** en el panel izquierdo, haga clic en **Descargar**.
2. Siga las instrucciones que aparecen en pantalla para descargar VirusScan.

Sugerencia: también puede descargar VirusScan haciendo clic en el vínculo **Unidades para analizar este dispositivo USB** del panel Opciones de análisis.

CAPÍTULO 8

Renovación de la suscripción de VirusScan USB

Cuando caduque su suscripción de VirusScan USB, VirusScan USB ya no funcionará y no podrá recibir actualizaciones del programa ni archivos de definición de virus (DAT). Sin embargo, podrá seguir accediendo al panel de inicio principal de VirusScan USB, que le pedirá que renueve su suscripción.

Sugerencia: si renueva una suscripción antes de que caduque, el tiempo restante se agregará a la nueva suscripción.

En este capítulo

Renovar la suscripción de VirusScan USB

Cuando caduque su suscripción de VirusScan USB, se le pedirá que adquiera una suscripción cada vez que conecte la unidad USB o cada vez que intente ejecutar el programa. Aunque VirusScan USB no analice su unidad USB ni reciba actualizaciones una vez caducada la suscripción, le permite renovar su suscripción.

- En el panel de inicio de VirusScan USB, en **Resumen de programa**, haga clic en **Renovar**.

Referencia

El glosario de términos lista y define la terminología de seguridad más comúnmente utilizada en los productos de McAfee.

Glosario

A

Análisis bajo demanda

Análisis que se inicia bajo demanda (es decir, cuando ejecuta la operación). A diferencia del análisis en tiempo real, los análisis bajo demanda no se inician automáticamente.

Análisis en tiempo real

Analizar archivos y carpetas en busca de virus y otra actividad cuando usted o el equipo acceden a ellos.

D

DAT

(Archivos de firma de datos) Archivos que contienen las definiciones utilizadas al detectar virus, troyanos, software espía, software publicitario y otros programas potencialmente no deseados en el equipo o la unidad USB.

L

Launchpad

Componente de interfaz U3 que actúa como punto de inicio para abrir y gestionar programas USB U3.

P

Programa potencialmente no deseado (PUP)

Programa que recopila y transmite información personal sin su permiso (por ejemplo, software espía y software publicitario).

T

Troyano

Programa que aparece como legítimo pero que puede dañar archivos importantes, alterar el rendimiento y permitir accesos no autorizados al equipo.

U

U3

(Usuario: simplificado, más inteligente, móvil) Plataforma para ejecutar programas de Windows 2000 o XP directamente desde una unidad USB. La iniciativa U3 fue fundada en 2004 por M-Systems y SanDisk y permite a los usuarios ejecutar programas U3 en un equipo Windows sin instalar ni almacenar datos u opciones en el equipo.

Unidad inteligente

Consulte unidad USB.

Unidad USB

Pequeña unidad de memoria que se conecta al puerto USB del equipo. Una unidad USB actúa como un pequeño disco duro que facilita la transferencia de archivos de un equipo a otro.

USB

(Universal Serial Bus) Interfaz informática serie estandarizada que le permite conectar dispositivos periféricos como teclados, joysticks e impresoras al equipo.

V

Virus

Programas que se reproducen automáticamente para alterar otros archivos o datos. A menudo parecen proceder de un remitente de confianza, o parecen ser de contenido inofensivo.

Acerca de McAfee

McAfee, Inc., con sede central en Santa Clara, California, y líder mundial en prevención de intrusiones y gestión de riesgos de seguridad, proporciona servicios y soluciones proactivas y probadas que protegen sistemas y redes en todo el mundo. Su experiencia y su compromiso inigualable con la innovación permiten a McAfee dotar a usuarios particulares, empresas, sector público y proveedores de servicios de la capacidad de bloquear ataques, evitar problemas y controlar y mejorar de manera continua su seguridad.

Copyright

Licencia

AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL CONTRATO LEGAL CORRESPONDIENTE A LA LICENCIA ADQUIRIDA, QUE ESTIPULA LOS TÉRMINOS GENERALES Y CONDICIONES DE USO DEL SOFTWARE CON LICENCIA. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS DE VENTA Y OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑAN AL PAQUETE DE SOFTWARE O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (POR EJEMPLO, UN MANUAL, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DEL SITIO WEB DESDE EL QUE DESCARGÓ EL PAQUETE DE SOFTWARE). SI NO ESTÁ DE ACUERDO CON TODOS LOS TÉRMINOS DESCRITOS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SEGÚN CORRESPONDA, PUEDE DEVOLVER EL PRODUCTO A MCAFEE, INC. O AL ESTABLECIMIENTO DE COMPRA PARA QUE SE LE REEMBOLSE EL IMPORTE COMPLETO.

Índice