McAfee®

VirusScan® Plus

AntiVirus, Firewall & AntiSpyware

Guía del usuario

Contenido

Introducción 3

McAfee SecurityCenter 5
Funciones de SecurityCenter 6
Uso de SecurityCenter....7
Solucionar u omitir problemas de protección....17
Trabajar con alertas....21
Visualización de eventos....27
McAfee VirusScan....29
Funciones de VirusScan....30
Exploración del equipo 31
Trabajar con los resultados de análisis....37
Tipos de análisis....40
Utilización de protección adicional....43
Configurar la protección frente a virus 47
McAfee Personal Firewall 67
Personal Firewall incluye....68
Iniciar el cortafuegos....71
Trabajar con alertas....73
Gestionar las alertas informativas....77
Configurar la protección del cortafuegos....79
Gestionar programas y permisos 91
Gestionar conexiones de equipo....101
Gestionar los servicios del sistema 109
Registro, supervisión y análisis 115
Obtener más información sobre la seguridad en Internet 125
McAfee QuickClean....127
Características de QuickClean 128
Limpiando el equipo 129
Desfragmentación del equipo 133
Planificación de una tarea 135
McAfee Shredder 141
Características de Shredder....142
Purga de archivos, carpetas y discos....142
McAfee Network Manager 145
Funciones de Network Manager 146
Descripción de los iconos de Network Manager....147
Configuración de una red gestionada 149
Gestión remota de la red....155
Supervisión de sus redes....161
McAfee EasyNetwork 165
Funciones de EasyNetwork 166
Configuración de EasyNetwork....167
Compartir y enviar archivos 173
Compartir impresoras....179

Referencia....181

Glosario 182

Acerca de McAfee 197

Licencia....197
Copyright....198
Servicio al cliente y soporte técnico....199
Utilización de McAfee Virtual Technician....200

Índice 210

CAPÍTULO 1

Introducción

Dote a su equipo con la seguridad combinada de las tecnologías de protección contra software espía, análisis de virus y cortafuegos de McAfee. Puede utilizar VirusScan Plus para proteger su equipo de virus, controlar la actividad sospechosa del tráfico de Internet y bloquear software espía que ponga en peligro la integridad de su información personal.

En este capítulo

McAfee SecurityCenter 5
McAfee VirusScan 29
McAfee Personal Firewall 67
McAfee QuickClean 127
McAfee Shredder 141
McAfee Network Manager 145
McAfee EasyNetwork 165
Referencia 181
Acerca de McAfee 197
Servicio al cliente y soporte técnico 199

CAPÍTULO 2

McAfee SecurityCenter

McAfee SecurityCenter le permite supervisar el estado de la configuración de seguridad de su equipo, saber al instante si los servicios de protección de virus, programas espía, correo electrónico y cortafuegos de su equipo están actualizados y actuar en vulnerabilidades potenciales de la seguridad. Ofrece las herramientas y controles de navegación necesarios para coordinar y gestionar todas las áreas de protección de su equipo.

Antes de comenzar a configurar y gestionar la protección de su equipo, revise la interfaz de SecurityCenter y asegúrese de que comprende la diferencia entre estado de protección, categorías de protección y servicios de protección. A continuación, actualice SecurityCenter para asegurarse de que dispone de la protección más reciente disponible de McAfee.

Después de finalizar las tareas de configuración iniciales, puede utilizar SecurityCenter para supervisar el estado de protección de su equipo. Si SecurityCenter detecta un problema de protección, le avisará, de modo que pueda solucionar u omitir el problema (según su gravedad). Además, en el registro de eventos puede revisar los eventos de SecurityCenter, como cambios de configuración en el análisis de virus.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de SecurityCenter 6
Uso de SecurityCenter 7
Solucionar u omitir problemas de protección 17
Trabajar con alertas 21
Visualización de eventos 27

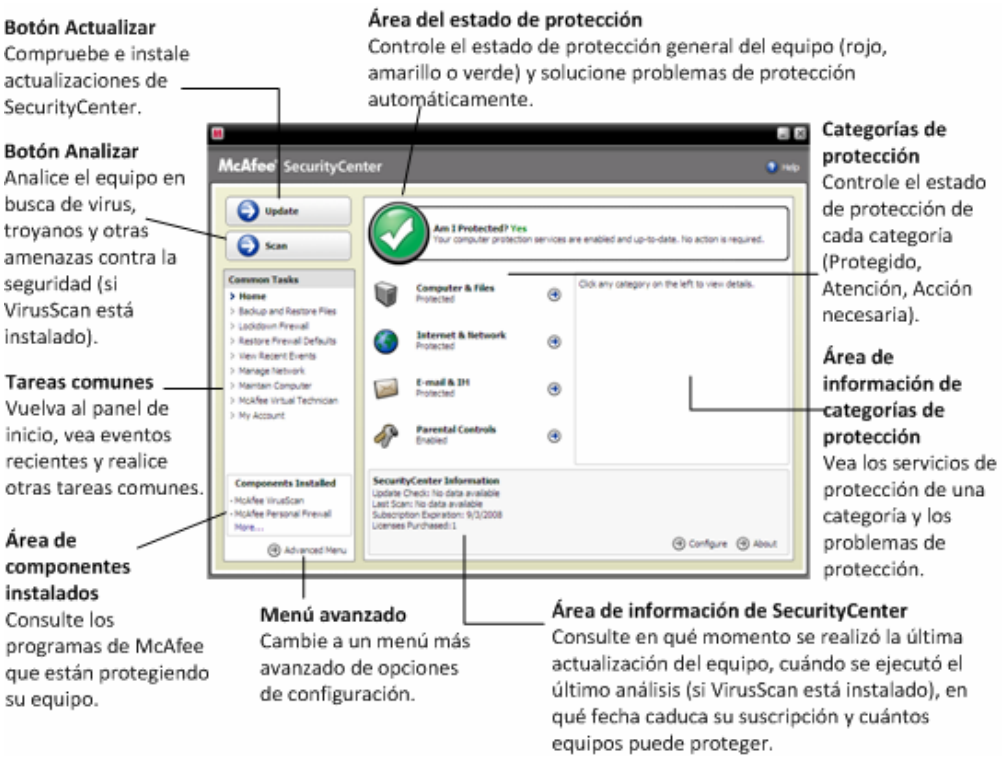
Funciones de SecurityCenter

Estado de protección simplificado	Facilita la comprobación del estado de protección de su equipo, la verificación de actualizaciones y la solución de problemas de protección.
Actualizaciones y mejoras automáticas	SecurityCenter descarga e instala automáticamente actualizaciones de sus programas. Cuando una nueva versión de un programa de McAfee está disponible, se obtiene automáticamente para su equipo siempre y cuando la suscripción tenga validez, garantizando así que siempre tenga una protección actualizada.
Alertas en tiempo real	Las alertas de seguridad indican la aparición de emergencias de virus y amenazas de seguridad.

CAPÍTULO 3

Uso de SecurityCenter

Antes de comenzar a utilizar SecurityCenter, revise los componentes y las áreas de configuración que se utilizarán para gestionar el estado de protección de su equipo. Si desea obtener más información sobre la terminología utilizada en esta imagen, consulte Descripción del estado de protección (página 8) y Descripción de las categorías de protección (página 9). A continuación, puede revisar la información de su cuenta de McAfee y verificar la validez de su suscripción.



En este capítulo

Descripción del estado de protección 8
Descripción de las categorías de protección.....9
Descripción de los servicios de protección 10
Gestión de suscripciones.....11
Actualización de SecurityCenter 13

Descripción del estado de protección

El estado de protección de su equipo se muestra en la zona de estado de protección en el panel Inicio de SecurityCenter. Indica si su equipo está totalmente protegido contra las últimas amenazas de seguridad y puede verse influido por ataques externos contra la seguridad, otros programas de seguridad y los programas que tienen acceso a Internet.

El estado de protección de su equipo puede ser de color rojo, amarillo o verde.

Estado de protección	Descripción
Roja	Su equipo no está protegido. La zona de estado de protección del panel Inicio de SecurityCenter tiene color rojo e indica que no está protegido. SecurityCenter informa sobre, al menos, un problema de seguridad crítico. Para contar con una protección completa, debe solucionar todos los problemas de seguridad críticos de cada categoría de protección (en el estado de la categoría de problema se indica **Acción necesaria**, también en rojo). Para obtener más información sobre cómo solucionar problemas de protección, consulte Solución de problemas de protección (página 18).
Amarilla	Su equipo está parcialmente protegido. La zona de estado de protección del panel Inicio de SecurityCenter tiene color amarillo e indica que no está protegido. SecurityCenter informa sobre, al menos, un problema de seguridad no crítico. Para contar con una protección completa, debe solucionar u omitir los problemas de seguridad no críticos asociados con cada categoría de protección. Para obtener más información sobre cómo solucionar u omitir problemas de protección, consulte Solucionar u omitir problemas de protección (página 17).
Verde	Su equipo está totalmente protegido. La zona de estado de protección del panel Inicio de SecurityCenter tiene color verde e indica que está protegido. SecurityCenter no informa sobre problemas de seguridad críticos o no críticos. Cada categoría de protección muestra los servicios que protegen su equipo.

Descripción de las categorías de protección

Los servicios de protección de SecurityCenter se dividen en cuatro categorías: Equipo y archivos, Internet y redes, correo electrónico y MI y control parental. Estas categorías le ayudan a explorar y configurar los servicios de seguridad que protegen su equipo.

Haga clic en un nombre de categoría para configurar sus servicios de protección y visualizar cualquier problema de seguridad detectado en esos servicios. Si el estado de protección de su equipo es de color rojo o amarillo, una o varias categorías muestran un mensaje de *Acción necesaria* o *Atención*, quiere decir que SecurityCenter ha detectado un problema en la categoría. Si desea obtener más información sobre estados de protección, consulte Descripción del estado de protección (página 8).

Categoría de protección	Descripción
Equipo y archivos	La categoría Equipo y archivos le permite configurar los siguientes servicios de protección: ▪ Protección antivirus ▪ Protección antisoftware espía ▪ SystemGuards ▪ Protección de Windows ▪ PC Health
Internet y red	La categoría Internet y red le permite configurar los siguientes servicios de protección: ▪ Protección por cortafuegos ▪ Protección antiphishing ▪ Protección de la identidad
Correo electrónico y MI	La categoría Correo electrónico y MI le permite configurar los siguientes servicios de protección: ▪ Protección antivirus de correo electrónico ▪ Protección antivirus IM ▪ Protección contra software espía por correo electrónico ▪ Protección contra software espía IM ▪ Protección contra spam
Control parental	La categoría Control parental le permite configurar los siguientes servicios de protección: ▪ Bloqueo de contenido

Descripción de los servicios de protección

Los servicios de protección son los diversos componentes de seguridad que se configuran para proteger el equipo y los archivos. Los servicios de protección se corresponden directamente con los programas de McAfee. Por ejemplo, cuando se instala VirusScan, están disponibles los siguientes servicios de protección: protección antivirus, protección contra software espía, SystemGuards y análisis de secuencias de comandos. Si desea obtener información más detallada acerca de estos servicios de protección en particular, consulte la ayuda de VirusScan.

De manera predeterminada, todos los servicios de protección asociados con un programa se activan al instalarlo; sin embargo, los servicios de protección se pueden desactivar en cualquier momento. Por ejemplo, si se instala el Control parental, se activan los servicios Bloqueo de contenido y Protección de la identidad. Si no tiene intención de utilizar el servicio de protección Bloqueo de contenido, puede desactivarlo por completo. También es posible desactivar un servicio de protección de manera temporal, mientras se realizan tareas de mantenimiento o configuración.

Gestión de suscripciones

Cada producto de protección McAfee que adquiera incluye una suscripción que le permite utilizar el producto en un determinado número de equipos durante un período de tiempo determinado. La duración de la suscripción varía en función de su adquisición, pero normalmente comienza al activar el producto. La activación es sencilla y gratuita (todo lo que necesita es una conexión a Internet) pero es muy importante porque le autoriza a recibir actualizaciones de productos periódicas y automáticas que mantendrán su equipo protegido de las últimas amenazas.

La activación normalmente se produce cuando se instala el producto, pero si decide esperar (por ejemplo, si no dispone de conexión a Internet), tiene 15 días para activarlo. Si no lo activa en un plazo de 15 días, sus productos ya no recibirán actualizaciones críticas ni efectuarán análisis. Asimismo, realizaremos notificaciones periódicas (mediante mensajes en pantalla) antes de que su suscripción esté a punto de caducar. De este modo, podrá evitar interrupciones en su protección renovándolo cuanto antes o configurando la renovación automática en nuestro sitio Web.

Si observa un vínculo en SecurityCenter que le solicita que active el producto, significa que su suscripción no se ha activado. Para ver la fecha de caducidad de su suscripción, puede consultar la página de su cuenta.

Acceso a su cuenta de McAfee

Desde SecurityServer puede acceder fácilmente a la información de su cuenta de McAfee (la página de su cuenta).

1. En **Tareas comunes**, haga clic en **Mi cuenta**.
2. Inicie sesión en su cuenta de McAfee.

Activar productos

Por lo general, la activación tiene lugar al instalar el producto. Pero si todavía no se ha activado, observará un vínculo en SecurityCenter que le solicita la activación. También se le notificará periódicamente.

- En el panel Inicio de SecurityCenter, en **Información de SecurityCenter**, haga clic en **Active la suscripción**.

Sugerencia: también puede activarla desde la alerta que aparece periódicamente.

Comprobación de su suscripción

Ha de comprobar su suscripción para asegurarse de que aún no ha caducado.

- Haga clic con el botón derecho del ratón en el icono de SecurityCenter que aparece en el área de notificación de Windows en el extremo derecho de la barra de tareas y, a continuación, haga clic en **Verificar suscripción**.

Renovar la suscripción

Poco antes de que caduque su suscripción, verá un vínculo en SecurityCenter solicitándole que la renueve. También se le notificará periódicamente la fecha de caducidad pendiente con alertas.

- En el panel Inicio de SecurityCenter, en **Información de SecurityCenter**, haga clic en **Renovar**.

Sugerencia: también puede renovar el producto desde el mensaje de notificación que aparece periódicamente. O bien, puede ir a la página de su cuenta, donde podrá renovarlo o configurar la renovación automática.

CAPÍTULO 4

Actualización de SecurityCenter

SecurityCenter garantiza que sus programas registrados de McAfee están actualizados buscando e instalando actualizaciones en línea cada cuatro horas. En función de los programas que tenga instalados y activados, las actualizaciones en línea pueden incluir las definiciones de virus más recientes y actualizaciones para la protección contra piratas informáticos, spam, programas espía o para la privacidad. Si desea buscar actualizaciones antes del período predeterminado de cuatro horas, puede hacerlo en cualquier momento. Mientras SecurityCenter comprueba si hay actualizaciones, puede seguir realizando otras tareas.

Aunque no es recomendable, puede modificar la forma en la que SecurityCenter busca e instala actualizaciones. Por ejemplo, puede configurar SecurityCenter para descargar las actualizaciones pero no para instalarlas o para notificarle antes de descargar o instalar las actualizaciones. También es posible desactivar las actualizaciones automáticas.

Nota: si ha instalado su producto McAfee desde un CD, deberá activarlo en un plazo de 15 días o sus productos no recibirán actualizaciones críticas ni efectuarán análisis.

En este capítulo

Comprobar actualizaciones 13
Configurar actualizaciones automáticas 14
Desactivar las actualizaciones automáticas 15

Comprobar actualizaciones

De manera predeterminada, SecurityCenter comprueba automáticamente si hay actualizaciones cada cuatro horas si su equipo está conectado a Internet; sin embargo, si desea buscar actualizaciones antes del período predeterminado de cuatro horas, puede hacerlo. Si ha desactivado las actualizaciones automáticas, es su responsabilidad comprobar las actualizaciones de manera periódica.

- En el panel Inicio de SecurityCenter, haga clic en **Actualizar**.

Sugerencia: también puede comprobar si hay actualizaciones sin ejecutar SecurityCenter haciendo clic con el botón derecho en el icono de SecurityCenter en el área de notificación, situada en el extremo derecho de la barra de tareas y haciendo clic a continuación en **Actualizaciones**.

Configurar actualizaciones automáticas

De forma predeterminada, SecurityCenter comprueba e instala cada cuatro horas cuando su equipo está conectado a Internet. Si desea modificar este hábito predeterminado, puede configurar SecurityCenter para descargar las actualizaciones de manera automática y notificarle cuando las notificaciones estén listas para ser instaladas o notificarle antes de descargarlas.

Nota: SecurityCenter le notifica mediante alertas cuando hay actualizaciones listas para ser descargadas o instaladas. Desde las alertas puede descargar o instalar las actualizaciones o posponerlas. Cuando se actualiza un programa desde una alerta, es posible que se le solicite verificar su suscripción antes de descargarla e instalarla. Para obtener más información, consulte Trabajar con alertas (página 21).

1. Abrir el panel de Configuración de SecurityCenter.

   ¿Cómo?

   1. En **Tareas comunes**, haga clic en **Inicio**.
   2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.

2. En el panel Configuración de SecurityCenter, bajo **Actualizaciones automáticas desactivadas**, haga clic en **Activar** y, a continuación, haga clic en **Opciones avanzadas**.
3. Haga clic en uno de los botones siguientes:
   - **Instalar actualizaciones automáticamente y notificarme cuando mis servicios estén actualizados (recomendado)**
   - **Descargar actualizaciones automáticamente y notificarme cuando estén listas para su instalación**
   - **Notificarme antes de descargar cualquier actualización**
4. Haga clic en **Aceptar**.

Desactivar las actualizaciones automáticas

Si desactiva las actualizaciones automáticas, es su responsabilidad comprobar las actualizaciones de manera periódica; de lo contrario, su equipo no dispondrá de la protección de seguridad más actualizada. Para obtener información sobre cómo buscar actualizaciones de manera manual, consulte Comprobar actualizaciones (página 13).

1. Abrir el panel de Configuración de SecurityCenter.

   ¿Cómo?

   1. En **Tareas comunes**, haga clic en **Inicio**.
   2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.

2. En el panel Configuración de SecurityCenter, bajo **Actualizaciones automáticas activadas**, haga clic en **Desactivar**.
3. En el cuadro de diálogo de confirmación, haga clic en **Sí**.

Sugerencia: las actualizaciones automáticas se activan haciendo clic en el botón **Activar** o desactivando la opción **Desactivar la actualización automática y permitirme comprobar manualmente las actualizaciones** del panel Opciones de actualización.

CAPÍTULO 5

Solucionar u omitir problemas de protección

SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Los problemas de protección críticos requieren una acción inmediata y ponen en peligro su estado de protección (el color cambia a rojo). Los problemas de protección no críticos no requieren acciones inmediatas y pueden poner en peligro o no su estado de protección (dependiendo del tipo de problema). Para conseguir un estado de protección de color verde, debe solucionar todos los problemas críticos y solucionar u omitir todos los problemas que no sean críticos. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician. Si desea obtener más información sobre McAfee Virtual Technician, consulte la ayuda de McAfee Virtual Technician.

En este capítulo

Solución de problemas de protección 18
Omitir problemas de protección 19

Solución de problemas de protección

La mayoría de problemas de seguridad pueden solucionarse de manera automática; sin embargo, algunos problemas requieren que tome medidas. Por ejemplo, si la Protección del cortafuegos está desactivada, SecurityCenter puede activarla de manera automática; sin embargo, si la Protección del cortafuegos no está instalada, debe instalarla. La siguiente tabla indica algunas de las acciones posibles que puede tener que realizar a la hora de solucionar problemas de protección de manera manual:

Problema	Acción
No se ha realizado un análisis completo del equipo en los últimos 30 días.	Analizar el equipo manualmente. Para obtener más información, consulte la ayuda de VirusScan.
Los archivos de definiciones (DAT) no están actualizados.	Actualice la protección de manera manual. Para obtener más información, consulte la ayuda de VirusScan.
No está instalado un programa.	Instale el programa desde el sitio Web o el CD de McAfee.
Le faltan componentes a un programa.	Reinstale el programa desde el sitio Web o el CD de McAfee.
Un programa no está activado y no puede recibir protección total.	Active el programa en el sitio Web de McAfee.
Su suscripción ha caducado.	Compruebe el estado de su cuenta en el sitio Web de McAfee. Para obtener más información al respecto, consulte el apartado Gestión de suscripciones (página 11).

Nota: a menudo, un único problema de protección afecta a más de una categoría de protección. En este caso, solucionar el problema en una categoría lo borra del resto de categorías de protección.

Solucionar problemas de protección automáticamente

SecurityCenter puede solucionar la mayoría de problemas de protección automáticamente. Los cambios de configuración que SecurityCenter realiza al solucionar de manera automática los problemas de protección no se guardan en el registro de eventos. Si desea obtener más información sobre los eventos, consulte Visualización de eventos (página 27).

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, en la zona de estado de protección, haga clic en **Solucionar**.

Solucionar problemas de protección manualmente

Si uno o más problemas persisten después de haber intentado solucionarlos de manera automática, puede solucionarlos manualmente.

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en la categoría de protección en la que SecurityCenter ha clasificado el problema.
3. Haga clic en el enlace que sigue a la descripción del problema.

Omitir problemas de protección

Si SecurityCenter detecta un problema no crítico, puede solucionarlo u omitirlo. Otros problemas no críticos (por ejemplo, si los servicios Anti-Spam o Control parental no están instalados) se omiten de manera automática. Los problemas omitidos no se muestran en la zona de información de la categoría de protección del panel Inicio de SecurityCenter a menos que el estado de protección del equipo tenga color verde. Si un problema se omite, pero más tarde desea que aparezca en la zona de información de la categoría de protección incluso si el estado de protección de su equipo no tiene color verde, puede mostrar el problema omitido.

Omitir un problema de protección

Si SecurityCenter detecta un problema no crítico que no tiene intención de solucionar, puede omitirlo. Al omitirlo, el problema desaparece de la zona de información de la categoría de protección de SecurityCenter.

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en la categoría de protección en la que el problema ha sido clasificado.
3. Haga clic en el enlace **Omitir** que se encuentra junto al problema de protección.

Mostrar u ocultar problemas omitidos

Dependiendo de su gravedad, los problemas de protección omitidos pueden mostrarse u ocultarse.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Configuración de SecurityCenter, haga clic en **Problemas omitidos**.

3 En el panel Problemas omitidos, haga lo siguiente:

- Para ignorar un problema, marque su casilla de verificación.
- Para notificar sobre la existencia de un problema en la zona de información de la categoría de protección, desactive esta casilla de verificación.

4 Haga clic en **Aceptar**.

Sugerencia: además, también puede omitir un problema haciendo clic en el enlace **Omitir** que se encuentra junto al problema notificado en la zona de información de la categoría de protección.

CAPÍTULO 6

Trabajar con alertas

Las alertas son pequeños cuadros de diálogo emergentes que aparecen en la esquina inferior derecha de la pantalla cuando se producen determinados eventos de SecurityCenter. Una alerta proporciona información detallada acerca de un evento así como recomendaciones y opciones para resolver problemas que pueden estar asociados al evento. Algunas alertas también contienen enlaces a información adicional sobre el evento. Estos enlaces le permiten abrir el sitio Web global de McAfee o enviar información a McAfee para resolver problemas.

Hay tres tipos de alertas: roja, amarilla y verde.

Tipo de alerta	Descripción
Roja	Una alerta roja es una notificación crítica que requiere una respuesta del usuario. Las alertas rojas se producen cuando SecurityCenter no puede determinar automáticamente cómo solucionar un problema de protección.
Amarilla	Una alerta amarilla es una notificación no crítica que normalmente requiere una respuesta del usuario.
Verde	Una alerta verde es una notificación no crítica que no requiere una respuesta del usuario. Las alertas verdes proporcionan información básica sobre un evento.

Debido a que las alertas juegan un papel muy importante en la supervisión y gestión de su estado de protección, no es posible desactivarlas. Sin embargo, puede controlar cuando pueden aparecer determinados tipos de alertas informativas y configurar otras opciones de alerta (como, por ejemplo, si SecurityCenter debe emitir un sonido cuando emite una alerta o si se debe mostrar la pantalla de bienvenida de McAfee al iniciar).

En este capítulo

Mostrar y ocultar alertas informativas.....22
Configuración de las opciones de alerta.....23

Mostrar y ocultar alertas informativas

Las alertas informativas le indican cuando se producen eventos que no suponen amenazas para la seguridad de su equipo. Por ejemplo, si ha configurado la Protección del cortafuegos, aparecerá una alerta informativa de manera predeterminada cuando a un programa de su equipo se le haya permitido acceder a Internet. Si no desea que aparezca un determinado tipo de alerta informativa, puede ocultarla. Si no desea que aparezca ninguna alerta informativa, puede ocultarlas todas. También puede ocultar todas las alertas informativas cuando está jugando a pantalla completa en su equipo. Al finalizar el juego y salir del modo de pantalla completa, SecurityCenter comienza a mostrar de nuevo las alertas informativas.

Si por error oculta una alerta informativa, puede mostrarla de nuevo en cualquier momento. De manera predeterminada, SecurityCenter muestra todas las alertas informativas.

Muestre u oculte alertas informativas

Puede configurar SecurityCenter para que muestre algunas alertas informativas y que oculte otras o para ocultar todas las alertas informativas.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Configuración de SecurityCenter, haga clic en **Alertas informativas**.

3 En el panel Alertas informativas, haga lo siguiente:

- Para mostrar una alerta informativa, desactive su casilla de verificación.
- Para ocultar una alerta informativa, marque su casilla de verificación.
- Para ocultar todas las alertas informativas, seleccione la casilla de verificación **No mostrar alertas informativas**.

4 Haga clic en **Aceptar**.

Sugerencia: también puede ocultar una alerta informativa al seleccionar la casilla de verificación **No volver a mostrar esta alerta** en la misma alerta. Si lo hace, puede mostrar de nuevo la alerta informativa desactivando la casilla de verificación apropiada en el panel Alertas informativas.

Muestre u oculte alertas informativas al jugar

También puede ocultar las alertas informativas cuando está jugando a pantalla completa en su equipo. Al finalizar el juego y salir del modo de pantalla completa, SecurityCenter comienza a mostrar de nuevo las alertas informativas.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, seleccione o desactive la casilla de verificación **Mostrar alertas informativas cuando se detecte el modo de juegos**.

3 Haga clic en **Aceptar**.

Configuración de las opciones de alerta

SecurityCenter configura la apariencia y la frecuencia de las alertas; sin embargo, puede ajustar algunas opciones de alerta básicas. Por ejemplo, se puede emitir un sonido junto con las alertas u ocultar la pantalla de bienvenida cuando se inicia Windows. También puede ocultar las alertas que le informan sobre nuevos virus y otras amenazas de seguridad de la comunidad en línea.

Emitir un sonido junto con las alertas

Si desea recibir una indicación audible que le indique que ha aparecido una alerta, SecurityCenter puede configurarse para que emita un sonido con cada alerta.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, bajo **Sonido**, seleccione la casilla de verificación **Reproducir un sonido cuando se produzca una alerta**.

Ocultar la pantalla de bienvenida al iniciar

De manera predeterminada, la pantalla de bienvenida de McAfee aparece brevemente cuando Windows se inicia, indicándole que SecurityCenter está protegiendo su equipo. Sin embargo, puede ocultar la pantalla de bienvenida si no desea que aparezca.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, bajo **Pantalla de bienvenida**, desactive la casilla de verificación **Mostrar la pantalla de bienvenida de McAfee al iniciar Windows**.

Sugerencia: en cualquier momento puede mostrar la pantalla de bienvenida de nuevo seleccionando la casilla de verificación **Mostrar la pantalla de bienvenida de McAfee al iniciar Windows**.

Ocultar alertas de nuevos virus

Puede ocultar las alertas que le informan sobre nuevos virus y otras amenazas de seguridad de la comunidad en línea.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, desactive la casilla de verificación **Avisarme cuando se produzca un brote de virus o una amenaza para la seguridad**.

Sugerencia: puede mostrar las alertas de brotes de virus en cualquier momento seleccionando la casilla de verificación **Avisarme cuando se produzca un brote de virus o una amenaza para la seguridad**.

Ocultar mensajes de seguridad

Puede ocultar notificaciones de seguridad sobre la protección de más equipos en su red doméstica. Estos mensajes proporcionan información sobre su suscripción, el número de equipos que puede proteger con la misma y cómo ampliar su suscripción para proteger todavía más equipos.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Opciones de alerta, desactive la casilla **Mostrar avisos de virus u otros mensajes de seguridad**.

Sugerencia: puede mostrar estos mensajes de seguridad en cualquier momento seleccionando la casilla **Mostrar avisos de virus u otros mensajes de seguridad**.

CAPÍTULO 7

Visualización de eventos

Un evento es una acción o un cambio de configuración que se produce en una categoría de protección y en sus servicios de protección relacionados. Los diferentes servicios de protección registran diferentes tipos de eventos. Por ejemplo, SecurityCenter registra un evento si un servicio de protección está activado o desactivado; la Protección antivirus registra un evento cada vez que se detecta y elimina un virus; y la Protección del cortafuegos registra un evento cada vez que se bloquea un intento de conexión a Internet. Si desea obtener más información sobre categorías de protección, consulte Descripción de las categorías de protección (página 9).

Puede visualizar los eventos al resolver problemas de configuración y al revisar operaciones realizadas por otros usuarios. Muchos padres utilizan el registro de eventos para supervisar los hábitos de sus hijos en Internet. Puede visualizar los eventos recientes si desea examinar únicamente los últimos 30 eventos ocurridos. Puede visualizar todos los eventos si desea examinar una lista detallada de todos los eventos ocurridos. Al visualizar todos los eventos, SecurityCenter abre el registro de eventos, que muestra los eventos según la categoría de protección en la que se produjeron.

En este capítulo

Ver eventos recientes 27
Visualizar todos los eventos 27

Ver eventos recientes

Puede visualizar los eventos recientes si desea examinar únicamente los últimos 30 eventos ocurridos.

- Bajo **Tareas comunes,** haga clic en **Ver eventos recientes**.

Visualizar todos los eventos

Puede visualizar todos los eventos si desea examinar una lista detallada de todos los eventos ocurridos.

1. Bajo **Tareas comunes,** haga clic en **Ver eventos recientes**.
2. En el panel Eventos recientes, haga clic en **Ver registro**.
3. En el panel de la izquierda del registro de eventos, haga clic en el tipo de eventos que desea visualizar.

CAPÍTULO 8

McAfee VirusScan

Los servicios avanzados de detección y protección de VirusScan le defienden a usted y a su equipo de las últimas amenazas para la seguridad, tales como virus, troyanos, cookies de rastreo, software espía, software publicitario y otros programas potencialmente no deseados. La protección se amplía más allá de los archivos y carpetas de su equipo de sobremesa, centrándose en las amenazas desde diferentes puntos de entrada, tales como el correo electrónico, los mensajes instantáneos e Internet.

Con VirusScan, la protección de su equipo es inmediata y constante (no es necesario realizar tareas de administración tediosas). Al trabajar, jugar, navegar por Internet o comprobar su correo electrónico, se ejecuta en segundo plano, supervisando, analizando y detectando daños potenciales en tiempo real. Los análisis exhaustivos se realizan de manera programada y comprueban su equipo periódicamente utilizando un conjunto de opciones más sofisticado. VirusScan le ofrece la flexibilidad de personalizar este hábito si así lo desea; pero, en caso contrario, su equipo continúa protegido.

Con el uso normal del equipo, virus, gusanos y otras amenazas potenciales pueden infiltrarse en su equipo. Si esto ocurre, VirusScan le notifica la amenaza, pero normalmente la gestiona por usted: limpiando o poniendo en cuarentena los elementos infectados antes de que se produzca cualquier daño. Aunque no es muy común, en ocasiones puede ser necesario realizar acciones adicionales. En estos casos, VirusScan le permite decidir qué hacer (volver a analizar el equipo la próxima vez que se reinicie, guardar el elemento detectado o eliminarlo).

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de VirusScan 30
Exploración del equipo.....31
Trabajar con los resultados de análisis 37
Tipos de análisis 40
Utilización de protección adicional 43
Configurar la protección frente a virus 47

Funciones de VirusScan

Protección integral contra virus	Protege su equipo de las últimas amenazas contra la seguridad, tales como virus, troyanos, cookies de rastreo, software espía, software publicitario y otros programas potencialmente no deseados. La protección se amplía más allá de los archivos y carpetas y de su equipo de sobremesa, centrándose en las amenazas desde diferentes puntos de entrada, tales como el correo electrónico, los mensajes instantáneos e Internet. No es necesario realizar tareas de administración tediosas.
Opciones de análisis sensibles a los recursos	Permite personalizar las opciones de análisis si lo desea; en caso contrario, su equipo permanecerá protegido. Si experimenta unas velocidades de análisis muy lentas, puede desactivar la opción que utiliza menos recursos del equipo, pero tenga en cuenta que se le asignará una mayor prioridad a la protección antivirus que a otras tareas.
Reparaciones automáticas	Si VirusScan detecta una amenaza para la seguridad al ejecutar un análisis, intentará gestionar la amenaza de manera automática según el tipo de amenaza. De esta manera, es posible detectar y neutralizar la mayoría de amenazas sin la necesidad de su intervención. Aunque no es muy frecuente, es posible que VirusScan no pueda neutralizar una amenaza por su cuenta. En estos casos, VirusScan le permite decidir qué hacer (volver a analizar el equipo la próxima vez que se reinicie, guardar el elemento detectado o eliminarlo).
Detener tareas en modo de pantalla completa	Al realizar actividades lúdicas como ver películas, jugar en el equipo o cualquier otra actividad que ocupe toda la pantalla, VirusScan detiene varias tareas, como los análisis manuales.

CAPÍTULO 9

Exploración del equipo

Incluso antes de iniciar SecurityCenter por primera vez, la protección frente a virus en tiempo real de VirusScan comienza a proteger su equipo de virus, troyanos y otras amenazas a la seguridad potencialmente peligrosas. A menos que desactive la protección frente a virus en tiempo real, VirusScan supervisa su equipo de manera constante en busca de virus, analizando archivos cada vez que usted o su equipo accede a ellos, utilizando las opciones de análisis en tiempo real definidas por usted. Para asegurarse de que su equipo permanece protegido contra las amenazas de seguridad más recientes, active la protección contra virus en tiempo real y programe análisis manuales periódicos más exhaustivos. Para obtener más información acerca de definir las opciones del análisis, consulte Configurar la protección frente a virus (página 47).

VirusScan ofrece un conjunto más detallado de opciones de análisis para la protección frente a virus, lo que le permite ejecutar de manera periódica análisis más amplios. Puede realizar un análisis completo, rápido, personalizado o programado desde SecurityCenter. También puede realizar análisis manuales en el Explorador de Windows mientras trabaja. El análisis en SecurityCenter tiene la ventaja de poder cambiar las opciones de análisis sin detener el análisis. Sin embargo, realizar un análisis desde el Explorador de Windows aporta un enfoque muy adecuado vinculado con la seguridad informática.

Ya realice un análisis desde SecurityCenter o desde el Explorador de Windows, puede visualizar los resultados del análisis cuando éste finalice. Los resultados de un análisis se visualizan para determinar si VirusScan ha detectado, reparado o puesto en cuarentena a virus, troyanos, programas espía, software publicitario, cookies y otros programas potencialmente no deseados. Los resultados de un análisis se pueden mostrar de diferentes formas. Por ejemplo, puede ver un resumen sencillo de los resultados de los análisis o información detallada, como el estado de la infección y el tipo. También puede ver estadísticas generales sobre el análisis y las detecciones.

En este capítulo

Análisis de su PC 32
Ver resultados del análisis 35

Análisis de su PC

VirusScan proporciona un conjunto completo de opciones de análisis para la protección frente a virus, entre ellas, el análisis en tiempo real (que supervisa constantemente su PC en busca de amenazas), el análisis manual desde el Explorador de Windows, y el análisis completo, rápido, personalizado o programado desde SecurityCenter.

Para...	Hacer esto...
Iniciar el análisis en tiempo real para supervisar constantemente el equipo en busca de virus y analizar los archivos cada vez que usted o su equipo accedan a ellos.	1. Abra el panel de Configuración de Equipo y archivos. ¿Cómo? 1. En el panel izquierdo, haga clic en **Menú Avanzado**. 2. Haga clic en **Configurar**. 3. En el panel Configurar, haga clic en **Equipo y Archivos**. 2. En **Protección antivirus**, haga clic en **Activado**. **Nota:** el análisis en tiempo real está activado de forma predeterminada.
Inicie un Análisis rápido para analizar rápidamente el equipo en busca de amenazas	1. Haga clic en **Analizar** en el menú Básico. 2. En el panel Opciones de análisis, en Análisis rápido, haga clic en **Inicio**.
Inicie un Análisis completo para analizar a fondo el equipo en busca de amenazas	1. Haga clic en **Analizar** en el menú Básico. 2. En el panel Opciones de análisis, en Análisis completo, haga clic en **Inicio**.

Para...	Hacer esto...
Inicie un análisis personalizado basado en su configuración	1. Haga clic en **Analizar** en el menú Básico. 2. En el panel Opciones de análisis, en Mi elección, haga clic en **Inicio**. 3. Personalice un análisis desactivando o activando: **Todas las amenazas de todos los archivos** **Virus desconocidos** **Archivos de almacenamiento** **Software espía y amenazas potenciales** **Cookies de rastreo** **Programas invisibles** 4. Haga clic en **Iniciar**.
Inicie un análisis manual para comprobar si existen amenazas en los archivos, las carpetas o las unidades	1. Abra el Explorador de Windows. 2. Haga clic con el botón derecho en un archivo, carpeta o unidad y, a continuación, haga clic en **Analizar**.

Para...	Hacer esto...
Inicie un análisis programado que analizará periódicamente el equipo en búsqueda de amenazas	1. Abra el panel Análisis programado. ¿Cómo? 1. En **Tareas comunes**, haga clic en **Inicio**. 2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**. 3. En la zona información Equipo y archivos, haga clic en **Configurar**. 4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y haga clic en **Avanzada**. 5. Haga clic en **Análisis programado** en el panel Protección antivirus. 2. Seleccione **Activar análisis programado**. 3. Para reducir la cantidad de potencia del procesador que se utiliza normalmente para los análisis, seleccione **Análisis utilizando mínimos recursos del equipo**. 4. Seleccione uno o más días. 5. Especifique una hora de inicio. 6. Haga clic en **Aceptar**.

Los resultados del análisis aparecen en la alerta de Análisis finalizado. Los resultados incluyen el número de elementos escaneados, detectados, reparados, puestos en cuarentena y eliminados. Haga clic en **Ver detalles del análisis** para saber más sobre los resultados del análisis o sobre cómo trabajar con elementos infectados.

Nota: para conocer más detalles sobre las opciones, consulte Tipos de análisis (página 40).

Ver resultados del análisis

Cuando finaliza un análisis, debe ver los resultados para determinar qué se encontró y para analizar el estado de protección actual de su equipo. Los resultados de un análisis le indican si VirusScan ha detectado, reparado o puesto en cuarentena a virus, troyanos, programas espía, software publicitario, cookies y otros programas potencialmente no deseados.

En el menú Básico o Avanzado, haga clic en **Analizar** y siga uno de los siguientes pasos:

Para...	Hacer esto...
Ver los resultados del análisis en la alerta	Vea los resultados del análisis en la alerta de Análisis finalizado.
Ver más información sobre resultados de análisis	Haga clic en **Ver detalles de análisis** en la alerta Análisis finalizado.
Ver un resumen rápido de los resultados de los análisis	Remítase al icono **Análisis finalizado** que se encuentra en el área de notificación de la barra de tareas.
Ver las estadísticas sobre análisis y detección	Haga doble clic en el icono **Análisis finalizado** que se encuentra en el área de notificación de la barra de tareas.
Ver detalles sobre los elementos detectados, el estado y el tipo de infección.	1. Haga doble clic en el icono **Análisis finalizado** que se encuentra en el área de notificación de la barra de tareas. 2. Haga clic en **Detalles** en el panel Análisis completo, Análisis rápido, Análisis personalizado o Análisis manual.
Consultar los detalles sobre el análisis más reciente	Haga doble clic en el icono **Análisis finalizado** del área de notificaciones de la barra de tareas y consulte los detalles de análisis más reciente en el panel Análisis completo, Análisis rápido, Análisis personalizado o Análisis manual.

CAPÍTULO 10

Trabajar con los resultados de análisis

Si VirusScan detecta una amenaza para la seguridad al ejecutar un análisis, intentará gestionar la amenaza de manera automática según el tipo de amenaza. Por ejemplo, VirusScan intenta limpiar los archivos infectados si detecta un virus, troyano o cookie de rastreo en su equipo. VirusScan siempre pone en cuarentena un archivo antes de intentar limpiarlo. Si no está limpio, el archivo se pone en cuarentena.

Cuando se enfrente a determinadas amenazas de seguridad, VirusScan no podrá limpiar ni poner en cuarentena satisfactoriamente el archivo infectado. En este caso, VirusScan le pedirá que gestione la amenaza. Puede realizar diferentes acciones según el tipo de amenaza. Por ejemplo, si se detecta un virus en un archivo pero VirusScan no puede limpiar o ponerlo en cuarentena con éxito, también se denegará el acceso a dicho archivo. Si se detectan cookies de rastreo pero VirusScan no puede limpiarlas o ponerlas en cuarentena, puede decidir si eliminarlas o aceptarlas como elemento de confianza. Si se detectan programas potencialmente no deseados, VirusScan no realiza ninguna acción automática; en cambio, le permite decidir si poner el programa en cuarentena o clasificarlo como programa de confianza.

Cuando VirusScan pone elementos en cuarentena, los cifra y aísla en una carpeta para evitar que los archivos, programas o cookies dañen su equipo. Puede restaurar o eliminar los elementos en cuarentena. En la mayoría de los casos puede eliminar una cookie en cuarentena sin que eso le afecte a su equipo, sin embargo, si VirusScan ha puesto en cuarentena un programa que usted reconoce y utiliza, considere la posibilidad de restaurarlo.

En este capítulo

Trabajo con virus y troyanos.....38
Trabaje con programas potencialmente no deseados.....38
Trabaje con archivos en cuarentena.....39
Trabaje con programas y cookies en cuarentena.....39

Trabajo con virus y troyanos

VirusScan intenta limpiar los archivos infectados si detecta un virus o un troyano en un archivo de su equipo. Si no puede limpiar el archivo, VirusScan intenta ponerlo en cuarentena. Si tampoco es posible realizar esta acción, se deniega el acceso al archivo (sólo en análisis en tiempo real).

1 Abra el panel Resultados del análisis.

¿Cómo?

1. Haga doble clic en el icono **Análisis finalizado** que se encuentra en el área de notificación que se encuentra en la zona más a la derecha de la barra de tareas.
2. En el panel Progreso del análisis: Análisis manual, haga clic en **Ver resultados**.

2 En la lista de resultados del análisis, haga clic en **Virus y troyanos**.

Nota: para trabajar con los archivos que VirusScan ha puesto en cuarentena, consulte Trabajar con archivos en cuarentena (página 39).

Trabaje con programas potencialmente no deseados

Si VirusScan detecta un programa potencialmente no deseado en su equipo, le da la opción de eliminarlo o confiar en el programa. Si el programa no le resulta familiar, le recomendamos que considere su eliminación. Eliminar el programa potencialmente no deseado no lo borra realmente del equipo. En cambio, al eliminarlo el programa se coloca en cuarentena para evitar que dañe su equipo o sus archivos.

1 Abra el panel Resultados del análisis.

¿Cómo?

1. Haga doble clic en el icono **Análisis finalizado** que se encuentra en el área de notificación que se encuentra en la zona más a la derecha de la barra de tareas.
2. En el panel Progreso del análisis: Análisis manual, haga clic en **Ver resultados**.

2 En la lista de resultados del análisis, haga clic en **Programas potencialmente no deseados**.

3 Seleccione un programa potencialmente no deseado.

4 En **Deseo**, haga clic en **Eliminar** o **Confiar**.

5 Confirme su opción seleccionada.

Trabaje con archivos en cuarentena

Cuando VirusScan pone los archivos infectados en cuarentena, los cifra y los coloca en una carpeta para evitar que dañen su equipo. A continuación, puede restaurar o eliminar los archivos en cuarentena.

1 Abra el panel Archivos en cuarentena.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Restaurar**.
3. Haga clic en **Archivos**.

2 Seleccione un archivo en cuarentena.

3 Siga uno de estos procedimientos:

- Para reparar el archivo infectado y devolverlo a su ubicación original en su equipo, haga clic en **Restaurar**.
- Para eliminar el archivo infectado del equipo, haga clic en **Eliminar**.

4 Haga clic en **Sí** para confirmar su opción seleccionada.

Sugerencia: puede restaurar o eliminar varios archivos al mismo tiempo.

Trabaje con programas y cookies en cuarentena

Cuando VirusScan pone en cuarentena programas potencialmente no deseados o cookies de rastreo, los cifra y después los coloca en una carpeta protegida para evitar que los programas o las cookies dañen el equipo. A continuación, puede restaurar o eliminar los elementos en cuarentena. En la mayoría de los casos puede eliminar un elemento en cuarentena sin que su equipo se vea afectado por ello.

1 Abra el panel Programas en cuarentena y cookies de rastreo.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Restaurar**.
3. Haga clic en **Programas y cookies**.

2 Seleccione un programa o cookie en cuarentena.

3 Siga uno de estos procedimientos:

- Para reparar el archivo infectado y devolverlo a su ubicación original en su equipo, haga clic en **Restaurar**.
- Para eliminar el archivo infectado del equipo, haga clic en **Eliminar**.

4 Haga clic en **Sí** para confirmar la operación.

Sugerencia: puede restaurar o eliminar varios programas y cookies al mismo tiempo.

Tipos de análisis

VirusScan proporciona un conjunto completo de opciones de análisis para la protección frente a virus, entre ellas, el análisis en tiempo real (que supervisa constantemente su PC en busca de amenazas), el análisis manual desde el Explorador de Windows, y la posibilidad de ejecutar el análisis completo, rápido o personalizado desde SecurityCenter, o de personalizar el momento en que se llevarán a cabo análisis programados. El análisis en SecurityCenter tiene la ventaja de poder cambiar las opciones de análisis sin detener el análisis.

Análisis en tiempo real

La protección contra virus en tiempo real supervisa constantemente el equipo en busca de virus y analiza los archivos cada vez que usted o su equipo acceden a ellos. Para asegurarse de que su equipo permanece protegido contra las amenazas de seguridad más recientes, active la protección contra virus en tiempo real y programe análisis manuales periódicos más exhaustivos.

Puede establecer opciones predeterminadas para el análisis en tiempo real, que incluyen el análisis en búsqueda de virus y en busca de amenazas en cookies de rastreo y unidades de red. También puede aprovechar la protección contra desbordamiento de búfer, que está activada de forma predeterminada (excepto si utiliza un sistema operativo Windows Vista de 64 bits). Para conocer más detalles, consulte Configuración de opciones de análisis en tiempo real (página 48).

Análisis rápido

El análisis rápido le permite analizar el equipo en busca de amenazas en procesos, archivos críticos de Windows y otras áreas susceptibles de su equipo.

Análisis completo

El Análisis completo le permite analizar el equipo a fondo en busca de virus, software espía y otras amenazas de seguridad que exista en cualquier ubicación del PC.

Análisis personalizado

El análisis personalizado le permite elegir su propia configuración para comprobar si existen amenazas en su PC. Entre las opciones del análisis personalizado se incluye la comprobación de amenazas en todos los archivos, en los archivos almacenados y en las cookies además del análisis en busca de virus desconocidos, software espía y programas invisibles.

Puede establecer opciones predeterminadas para los análisis personalizados, lo que incluye el análisis en busca de virus desconocidos, archivos archivados, software espía y amenazas potenciales, cookies de rastreo y programas invisibles. También puede realizar análisis utilizando recursos informáticos mínimos. Para conocer más detalles, consulte Configuración de opciones de análisis personalizado (página 51).

Análisis manual

El análisis manual le permite comprobar rápidamente la existencia de amenazas en los archivos, las carpetas y las unidades de manera improvisada desde el Explorador de Windows.

Análisis programado

Los Análisis programados analizan a fondo su equipo en busca de virus y otras amenazas en cualquier momento de cualquier día de la semana. Los análisis programados siempre comprueban el equipo al completo mediante sus opciones predeterminadas de análisis. De manera predeterminada, VirusScan realiza un análisis programado una vez a la semana. Si cree que está experimentando unas velocidades de análisis muy lentas, considere la posibilidad de desactivar la opción que utiliza menos recursos del equipo, pero tenga en cuenta que se le asignará una mayor prioridad a la protección antivirus que a otras tareas. Para conocer más detalles, consulte Programación de análisis (página 54).

Nota: para conocer cómo iniciar la mejor opción de análisis para sus necesidades, consulte Análisis de su PC (página 32)

CAPÍTULO 11

Utilización de protección adicional

Además de la protección contra virus en tiempo real, VirusScan ofrece protección avanzada contra secuencias de comandos, programas espía y adjuntos de correos electrónicos y mensajes instantáneos potencialmente peligrosos. De manera predeterminada, están activados y protegen su equipo el análisis de secuencias de comandos y la protección contra programas espía, correo electrónico y mensajería instantánea.

Protección de análisis de secuencias de comandos

La protección de análisis de secuencias de comandos detecta las secuencias de comandos potencialmente peligrosas y evita que se ejecuten en su equipo o el navegador Web. Supervisa su equipo en busca de actividades sospechosas en las secuencias de comandos, tales como una secuencia de comandos que crea, copia o elimina archivos o que abre el registro de Windows y, posteriormente, le informa de ello antes de que se produzca cualquier daño.

Protección contra software espía

La protección contra software espía detecta software espía, software publicitario y otros programas potencialmente no deseados. Los programas espías son aplicaciones que se pueden instalar en su equipo de forma encubierta para supervisar sus hábitos, recopilar información personal e incluso interferir en el control de su equipo instalando programas adicionales o redirigiendo la actividad de los navegadores.

Protección de correo electrónico

La protección de correo electrónico detecta las actividades sospechosas en el correo electrónico y los archivos adjuntos enviados.

Protección de mensajería instantánea

La protección de mensajería instantánea detecta potenciales amenazas contra la seguridad provenientes de adjuntos a mensajes instantáneos que se han recibido. Además, evita que los programas de mensajería instantánea compartan información personal.

En este capítulo

Inicie la protección de análisis de secuencias de comandos 44
Inicie la protección contra software espía.....45
Inicie la protección de correo electrónico.....45
Inicie la protección de mensajería instantánea.....46

Inicie la protección de análisis de secuencias de comandos

Active la protección de análisis de secuencias de comandos para detectar las secuencias de comandos potencialmente peligrosas y evitar que se ejecuten en su equipo. La protección de análisis de secuencias de comandos le indica cuando una secuencia de comandos intenta crear archivos en su equipo, copiarlos o eliminarlos o cuando realiza cambios en el registro de Windows.

1 Abra el panel de Configuración de Equipo y archivos.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2 En **Protección de análisis de secuencias de comandos**, haga clic en **Activado**.

Nota: aunque en cualquier momento es posible desactivar la protección de análisis de secuencias de comandos, si lo hace deja a su equipo en una posición vulnerable ante secuencias de comandos dañinas.

Inicie la protección contra software espía

Active la protección contra software espía para detectar y eliminar software espía, software publicitario y otros programas potencialmente no deseados que recopilan y transmiten información sin su conocimiento o permiso.

1 Abra el panel de Configuración de Equipo y archivos.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2 En **Protección de análisis de secuencias de comandos**, haga clic en **Activado**.

Nota: aunque en cualquier momento es posible desactivar la protección contra software espía, si lo hace deja a su equipo en una posición vulnerable ante programas potencialmente no deseados.

Inicie la protección de correo electrónico

Active la protección de correo electrónico para detectar gusanos, así como otras amenazas peligrosas en los mensajes y adjuntos de correo electrónico salientes (SMTP) y entrantes (POP3).

1 Abrir el panel de configuración de Correo electrónico y MI.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Correo electrónico y MI**.

2 En **Protección de correo electrónico**, haga clic en **Activado**.

Nota: aunque en cualquier momento es posible desactivar la protección de correo electrónico, si lo hace deja a su equipo en una posición vulnerable ante amenazas de correo electrónico.

Inicie la protección de mensajería instantánea

Active la protección de mensajería instantánea para detectar amenazas contra la seguridad que puedan incluirse como adjuntos en los mensajes instantáneos entrantes.

1 Abrir el panel de configuración de Correo electrónico y MI.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Correo electrónico y MI**.

2 En **Protección de mensajería instantánea**, haga clic en **Activado**.

Nota: aunque en cualquier momento es posible desactivar la protección de mensajería instantánea, si lo hace deja a su equipo en una posición vulnerable ante los adjuntos dañinos de los mensajes instantáneos.

CAPÍTULO 12

Configurar la protección frente a virus

Puede establecer diferentes opciones para el análisis programado, personalizado y en tiempo real. Por ejemplo, debido a que la protección en tiempo real supervisa constantemente su equipo, puede seleccionar un grupo determinado de opciones de análisis básico, reservar un conjunto más exhaustivo de opciones de análisis para la protección manual, bajo demanda.

También puede decidir el modo en que desea que VirusScan supervise y gestione los cambios potencialmente no autorizados o no deseados en su PC mediante SystemGuards y las listas de confianza. Guardianes del sistema supervisan, registran y gestionan los cambios potencialmente no autorizados realizados en el registro de Windows o en archivos de sistema importantes en su equipo e informa sobre ellos. Los cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema. Puede utilizar las listas de confianza para decidir si desea eliminar o confiar en reglas que detectan cambios en archivos o registros, programas o desbordamientos del búfer. Si confía en el elemento e indica que en el futuro no desea recibir ninguna notificación sobre esta actividad, el elemento se añade a una lista de confianza y VirusScan no lo detectará nunca más ni nos notificará sobre su actividad.

En este capítulo

Configuración de opciones de análisis en tiempo real 48
Configuración de las opciones de análisis personalizado 51
Programación de análisis 54
Utilización de las opciones de Guardianes del sistema 55
Uso de listas de confianza 62

Configuración de opciones de análisis en tiempo real

Al iniciar la protección contra virus en tiempo real, para analizar los archivos VirusScan utiliza un conjunto de opciones predeterminado; sin embargo, usted puede cambiar las opciones predeterminadas para ajustarlas a sus necesidades.

Para cambiar las opciones de análisis en tiempo real, debe decidir qué es lo que debe comprobar VirusScan durante un análisis, así como las ubicaciones y los tipos de archivo que debe analizar. Por ejemplo, puede determinar si VirusScan ha de buscar virus desconocidos o las cookies que los sitios Web pueden utilizar para realizar un seguimiento de tus hábitos y si analiza las unidades de red que están asignadas a su equipo o únicamente las unidades locales. También puede determinar qué tipo de archivos analiza (todos los archivos o únicamente los documentos y los archivos de programa, dado que es donde más virus se detectan).

Al cambiar las opciones de análisis en tiempo real, también debe decidir si es importante que su equipo cuente con protección contra desbordamiento de búfer. Un búfer es una porción de memoria utilizado para guardar datos informáticos de manera temporal. Los desbordamientos del búfer se pueden producir cuando la cantidad de programas o de procesos de información sospechosos almacenada en un búfer supera su capacidad. Cuando esto ocurre, su equipo se vuelve más vulnerable a los ataques contra la seguridad.

Configure las opciones de análisis en tiempo real

Debe configurar las opciones de análisis en tiempo real para personalizar lo que busca VirusScan durante un análisis en tiempo real, así como las ubicaciones y los tipos de archivo analizados. Las opciones incluyen el análisis en busca de virus desconocidos y cookies de rastreo, así como ofrecer protección contra desbordamiento de búfer. Además, también puede configurar el análisis en tiempo real para comprobar las unidades de red que están asignadas a su equipo.

1 Abra el panel de análisis en tiempo real.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y luego haga clic en **Avanzada**.

2 Especifique sus opciones de análisis en tiempo real y, a continuación, haga clic en **Aceptar**.

Para...	Hacer esto...
Detectar virus desconocidos y nuevas variantes de virus conocidos	Seleccione **Análisis para detectar virus desconocidos**.
Detectar las cookies	Seleccione **Analizar y eliminar las cookies de rastreo**.
Detectar virus y otras amenazas potenciales en las unidades que están conectadas en su red	Seleccione **Analizar unidades de red**.
Proteger su equipo de los desbordamientos del búfer	Seleccione **Activar protección contra desbordamiento de búfer**.
Especificar qué tipo de archivos desea analizar	Haga clic en **Todos los archivos (recomendado)** o en **Solamente archivos de programas y documentos**.

Detener la protección contra virus en tiempo real

Aunque no es habitual, en ocasiones es posible que desee detener el análisis en tiempo real (por ejemplo, para cambiar algunas opciones del análisis o para resolver un problema de rendimiento). Cuando la protección contra virus en tiempo real está desactivada, su equipo no está protegido y su estado de protección en SecurityCenter es de color rojo. Para obtener más información sobre el estado de protección, consulte "Descripción del estado de protección" en la ayuda de SecurityCenter.

Es posible desactivar temporalmente la protección contra virus en tiempo real y, a continuación, indicar cuando se debe reanudar. Puede reanudar la protección de manera automática pasados 15, 30, 45 ó 60 minutos, cuando se reinicie el equipo o nunca.

1. Abra el panel de Configuración de Equipo y archivos.

   ¿Cómo?

   1. En el panel izquierdo, haga clic en **Menú Avanzado**.
   2. Haga clic en **Configurar**.
   3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2. En **Protección antivirus**, haga clic en **Desactivado**.
3. En el cuadro de diálogo, seleccione cuando se debe reanudar el análisis en tiempo real.
4. Haga clic en **Aceptar**.

Configuración de las opciones de análisis personalizado

La protección personalizada contra virus le permite analizar los archivos libremente. Cuando se inicia un análisis personalizado, VirusScan comprueba su equipo en busca de virus y otros elementos potencialmente peligrosos utilizando un conjunto de opciones más exhaustivo. Para modificar las opciones de análisis personalizado, debe decidir qué es lo que debe comprobar VirusScan durante un análisis. Por ejemplo, puede determinar si VirusScan busca virus desconocidos, programas potencialmente no deseados, tales como programas espía o software publicitario, programas invisibles y kits de raíz (que pueden ofrecer acceso no autorizado a su equipo) y las cookies utilizadas por los sitios Web para realizar un seguimiento de sus hábitos. Además, debe decidir qué tipo de archivos se van a comprobar. Por ejemplo, puede determinar si VirusScan ha de comprobar todos los archivos o únicamente archivos y documentos (dado que es ahí donde se detecta la mayoría de virus). También puede determinar qué archivos de almacenamiento (por ejemplo, archivos .zip) se incluirán en el análisis.

De manera predeterminada, VirusScan comprueba todas las unidades y carpetas de su equipo o todas las unidades de red cada vez que ejecuta un análisis personalizado; sin embargo, puede ajustar las ubicaciones predeterminadas a sus necesidades. Por ejemplo, puede analizar únicamente archivos importantes del PC, elementos del escritorio o elementos de la carpeta Archivos de programa. A menos que se responsabilice usted mismo de iniciar cada análisis personalizado, puede establecer una programación periódica para realizar análisis. Los análisis programados siempre comprueban el equipo al completo mediante las opciones predeterminadas de análisis. De manera predeterminada, VirusScan realiza un análisis programado una vez a la semana.

Si cree que está experimentando unas velocidades de análisis muy lentas, considere la posibilidad de desactivar la opción que utiliza menos recursos del equipo, pero tenga en cuenta que se le asignará una mayor prioridad a la protección antivirus que a otras tareas.

Nota: al realizar actividades lúdicas como ver películas, jugar en el equipo o cualquier otra actividad que ocupe toda la pantalla, VirusScan detiene varias tareas, como las actualizaciones automáticas y los análisis personalizados.

Configurar opciones de análisis personalizado

Debe configurar las opciones de análisis personalizado para personalizar lo que VirusScan busca durante un análisis personalizado, así como las ubicaciones y los tipos de archivo analizados. Las opciones incluyen el análisis en busca de virus desconocidos, archivos, programas espía y programas potencialmente no deseados, cookies de rastreo, kits de raíz y programas invisibles. También puede configurar la ubicación del análisis personalizado para determinar dónde va a realizar la búsqueda VirusScan de virus y otros elementos peligrosos durante un análisis manual. Es posible analizar todos los archivos, carpetas y unidades de su ordenador o puede restringir el análisis a determinadas carpetas y unidades.

1 Abra el panel Análisis personalizado.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y haga clic en **Avanzada**.
5. Haga clic en **Análisis manual** en el panel Protección antivirus.

2 Especifique sus opciones de análisis personalizado y, a continuación, haga clic en **Aceptar**.

Para...	Hacer esto...
Detectar virus desconocidos y nuevas variantes de virus conocidos	Seleccione **Análisis para detectar virus desconocidos.**
Detectar y eliminar los virus de los archivos .zip y otros archivos de almacenamiento	Seleccione **Analizar archivos de almacenamiento.**
Detectar software espía, software publicitario y otros programas potencialmente no deseados	Seleccione **Buscar software espía y amenazas potenciales.**
Detectar las cookies	Seleccione **Analizar y eliminar las cookies de rastreo.**
Detectar los kits de raíz y los programas invisibles que pueden alterar y obtener archivos de sistema de Windows	Seleccione **Buscar programas invisibles.**

Para...	Hacer esto...
Utilizar menos potencia del procesador durante el análisis y dar más prioridad a otras tareas (tales como navegar en Internet o abrir documentos)	Seleccione **Análisis utilizando mínimos recursos del equipo**.
Especificar qué tipo de archivos desea analizar	Haga clic en **Todos los archivos (recomendado)** o en **Solamente archivos de programas y documentos**.

3 Haga clic en **Ubicación predeterminada para el análisis** y, a continuación, seleccione o desactive las ubicaciones que desee analizar u omitir y, a continuación, haga clic en **Aceptar**:

Para...	Hacer esto...
Analizar todos los archivos y carpetas de su equipo	Seleccione **(Mi) Equipo**.
Analizar archivos, carpetas y unidades determinadas de su equipo	Desactive la casilla de verificación **(Mi) Equipo** y seleccione una o más unidades o carpetas.
Analizar archivos de sistema importantes	Desactive la casilla de verificación **(Mi) Equipo** y, a continuación, seleccione la casilla de verificación **Archivos de sistema importantes**.

Programación de análisis

Planifique análisis para comprobar a fondo su equipo en busca de virus y otras amenazas en cualquier momento de cualquier día de la semana. Los análisis programados siempre comprueban el equipo al completo mediante las opciones predeterminadas de análisis. De manera predeterminada, VirusScan realiza un análisis programado una vez a la semana. Si cree que está experimentando unas velocidades de análisis muy lentas, considere la posibilidad de desactivar la opción que utiliza menos recursos del equipo, pero tenga en cuenta que se le asignará una mayor prioridad a la protección antivirus que a otras tareas.

Programe análisis que analizan a fondo todo el equipo en busca de virus y otras amenazas mediante sus opciones de análisis predeterminadas. De manera predeterminada, VirusScan realiza un análisis programado una vez a la semana.

1 Abra el panel Análisis programado.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y haga clic en **Avanzada**.
5. Haga clic en **Análisis programado** en el panel Protección antivirus.

2 Seleccione **Activar análisis programado**.

3 Para reducir la cantidad de potencia del procesador que se utiliza normalmente para los análisis, seleccione **Análisis utilizando mínimos recursos del equipo**.

4 Seleccione uno o más días.

5 Especifique una hora de inicio.

6 Haga clic en **Aceptar**.

Sugerencia: puede restablecer la programación predeterminada haciendo clic en **Restablecer**.

Utilización de las opciones de Guardianes del sistema

Guardianes del sistema supervisa, registra y gestiona los cambios potencialmente no autorizados realizados en el registro de Windows o en archivos de sistema importantes en su equipo e informa sobre ellos. Los cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema.

Los cambios en el registro y en los archivos son comunes y normalmente se producen en su equipo. Debido a que muchos son inofensivos, los ajustes predeterminados de Guardianes del sistema están configurados para ofrecer una protección fiable, inteligente y real contra los cambios no autorizados que supongan un gran potencial de peligrosidad. Por ejemplo, cuando Guardianes del sistema detecta los cambios no comunes y que presentan una amenaza potencialmente significativa, se informa sobre la actividad de manera inmediata y se añade al registro. Los cambios que sean más comunes, pero que aún impliquen algún potencial peligroso, sólo se incluyen en el registro. Sin embargo, la supervisión de los cambios estándar y de bajo riesgo está, de manera predeterminada, desactivada. La tecnología Guardianes del sistema puede configurarse para ampliar su protección a cualquier entorno que desee.

Hay tres tipos de Guardianes del sistema: Guardianes del sistema de programas, Guardianes del sistema de Windows y Guardianes del sistema de navegadores.

Guardianes del sistema de programas

Los Guardianes del sistema de programas detectan los cambios no autorizados potencialmente en el registro de su equipo y en otros archivos importantes esenciales para Windows. Estos importantes elementos y archivos del registro incluyen instalaciones de ActiveX, elementos de inicio, hooks de ejecución en shell de Windows y las cargas retrasadas de objeto de servicio de Shell. Al supervisarlos, la tecnología Guardianes del sistema de programas detiene los programas sospechosos con ActiveX (descargados de Internet), además de los programas espía y los programas potencialmente no deseados que se ejecutan de manera automática cuando Windows se inicia.

Guardianes del sistema de Windows

Los Guardianes del sistema de Windows también detectan los cambios no autorizados potencialmente en el registro de su equipo y en otros archivos importantes esenciales para Windows. Estos importantes elementos y archivos del registro incluyen identificadores de menús contextuales, applnit DLLs y el archivo hosts de Windows. Al supervisar estos elementos, la tecnología Guardianes del sistema ayuda a evitar que su equipo envíe y reciba información personal o no autorizada a través de Internet. También contribuye a detener los programas sospechosos que pueden traer cambios no deseados en relación con la apariencia y los hábitos de los programas que son importantes para usted y su familia.

Guardianes del sistema de navegadores

Al igual que los Guardianes del sistema de programa y de Windows, los Guardianes del sistema de navegadores detectan los cambios no autorizados potencialmente en el registro de su equipo y en otros archivos importantes esenciales para Windows. Sin embargo, los Guardianes del sistema de navegadores supervisan los cambios de elementos importantes del registro y de archivos como los complementos de Internet Explorer, las URL de Internet Explorar y las zonas de seguridad de Internet Explorer. Al supervisar este sistema, la tecnología de los Guardianes del sistema de navegadores ayuda a evitar la actividad no autorizada en los navegadores como la redirección a sitios Web sospechosos, cambios en los ajustes y en las opciones del navegador sin la formación adecuada y la confianza no autorizada en sitios Web sospechosos.

Active la protección Guardianes del sistema

Activa la protección de Guardianes del sistema para detectar los cambios potencialmente no autorizados en el registro de Windows y en los archivos de su equipo e informarle de ellos. Los cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema.

1 Abra el panel de Configuración de Equipo y archivos.

¿Cómo?

1. En el panel izquierdo, haga clic en **Menú Avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configurar, haga clic en **Equipo y Archivos**.

2 En **Protección del guardián del sistema**, haga clic en **Activado**.

Nota: es posible desactivar la protección de los Guardianes del sistema haciendo clic en **Desactivar**.

Configure las opciones de Guardianes del sistema

Utilice el panel Guardianes del sistema para configurar las opciones de protección, registro y alertas de los cambios de registro y de archivo no autorizados asociados con los archivos y programas de Windows e Internet Explorer. Los cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema.

1 Abra el panel Guardianes del sistema.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección del Guardián del sistema está activada y haga clic en **Avanzada**.

2 Seleccione un tipo de Guardián del sistema de la lista.

- **Guardianes del sistema de programas**
- **Guardianes del sistema de Windows**
- **Guardianes del sistema de navegadores**

3 En **Deseo**, elija una de las siguientes opciones:

- Para detectar y registrar cambios no autorizados en el registro y archivos asociados con los Guardianes del sistema de programa, de Windows y de navegadores e informar sobre ellos, haga clic en **Mostrar alertas.**
- Para detectar y registrar cambios no autorizados en el registro y archivos asociados con los Guardianes del sistema de programa, de Windows y de navegadores, haga clic en **Sólo cambios de registro.**
- Para desactivar la detección de cambios no autorizados en el registro y archivos asociados con los Guardianes del sistema de programa, de Windows y de navegador, haga clic en **Desactivar el Guardián del sistema.**

Nota: para obtener más información sobre los tipos de Guardianes del sistema, consulte Acerca de los tipos de Guardianes del sistema (página 58).

Acerca de los tipos de Guardianes del sistema

Los Guardianes del sistema detectan los cambios no autorizados potencialmente en el registro de su equipo y en otros archivos importantes esenciales para Windows. Hay tres tipos de Guardianes del sistema: Guardianes del sistema de programas, Guardianes del sistema de Windows y Guardianes del sistema de navegadores

Guardianes del sistema de programas

La tecnología Guardianes del sistema de programas detiene los programas sospechosos con ActiveX (descargados de Internet), además de los programas espía y los programas potencialmente no deseados que se ejecutan de manera automática cuando Windows se inicia.

guardián del sistema	Detecta...
Instalaciones de ActiveX	Los cambios no autorizados en las instalaciones de ActiveX que pueden causar daños en el equipo, ponen en riesgo su seguridad y dañar archivos importantes del sistema.
Elementos de inicio	El software espía, el software publicitario y los programas potencialmente no deseados que pueden instalar cambios en archivos de los elementos de inicio, lo que permite que se ejecuten programas sospechosos al iniciar el equipo.
Hooks de ejecución en Shell de Windows	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden instalar hooks de ejecución en shell de Windows para impedir que se inicien los programas de seguridad.

guardián del sistema	Detecta...
Carga retrasada de objeto de servicio de Shell	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro para la carga retrasada de objeto de servicio de shell, lo que permite que se ejecuten archivos dañinos al iniciar el equipo.

Guardianes del sistema de Windows

La tecnología Guardianes del sistema ayuda a evitar que su equipo envíe y reciba información personal o no autorizada a través de Internet. También contribuye a detener los programas sospechosos que pueden traer cambios no deseados en relación con la apariencia y los hábitos de los programas que son importantes para usted y su familia.

guardián del sistema	Detecta...
Identificadores de menús contextuales	Los cambios no autorizados en el registro para identificadores de menús contextuales de Windows que pueden afectar a la apariencia y comportamiento de los menús de Windows. Los menús contextuales permiten realizar acciones en el equipo, tales como hacer clic con el botón derecho en los archivos.
AppInit DLLs	Los cambios no autorizados en el registro para appInit DLLs de Windows que pueden permitir en principio que se ejecuten archivos dañinos al iniciar el equipo.
Archivo Hosts de Windows	El software espía, el software publicitario y los programas potencialmente no deseados que pueden realizar cambios no autorizados en el archivo hosts de Windows, lo que permite redireccionar el navegador a sitios Web sospechosos y bloquear actualizaciones de software.
Shell Winlogon	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de shell de Winlogon, lo que permite que otros programas sustituyan a Windows Explorer.
Winlogon User Init	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de Winlogon user init, lo que permite que se ejecuten programas sospechosos al iniciar la sesión en Windows.

guardián del sistema	Detecta...
Protocolos Windows	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de protocolos de Windows, lo que afecta a la forma en la que el equipo envía y recibe información a través de Internet.
Proveedores de servicios por niveles de Winsock	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden instalar cambios en el registro de proveedores de servicios por niveles (LSP) Winsock para interceptar y modificar la información que se envía y se recibe a través de Internet.
Comandos de apertura de Shell de Windows	Los cambios no autorizados a comandos de apertura de shell de Windows que pueden permitir que se ejecuten gusanos y otros programas dañinos en el equipo.
Planificador de tareas compartidas	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en los archivos y el registro del planificador de tareas compartidas, lo que permite que se ejecuten archivos potencialmente dañinos al iniciar el equipo.
Windows Messenger Service	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de Windows messenger service, lo que permite que haya anuncios no solicitados y programas de ejecución remota en el equipo.
Archivo Win.ini de Windows	El software espía, el software publicitario y los programas potencialmente no deseados que pueden realizar cambios en el archivo Win.ini, lo que permite que se ejecuten programas sospechosos al iniciar el equipo.

Guardianes del sistema de navegadores

La tecnología de los Guardianes del sistema de navegadores ayuda a evitar la actividad no autorizada en los navegadores como la redirección a sitios Web sospechosos, cambios en los ajustes y en las opciones del navegador sin la formación adecuada y la confianza no autorizada en sitios Web sospechosos.

guardián del sistema	Detecta...
Objetos de ayuda del navegador	El software espía, el software publicitario y los programas potencialmente no deseados que pueden utilizar objetos del ayudante del navegador para rastrear navegaciones en la Web y mostrar anuncios no solicitados.

guardián del sistema	Detecta...
Barras de Internet Explorer	Los cambios no autorizados en el registro para programas de la barra de Internet Explorar tales como Buscar y Favoritos que pueden afectar a la apariencia y comportamiento de Internet Explorer.
Complementos de Internet Explorer	El software espía, el software publicitario y los programas potencialmente no deseados que pueden instalar complementos de Internet Explorer para rastrear navegaciones en la Web y mostrar anuncios no solicitados.
ShellBrowser de Internet Explorer	Los cambios no autorizados en el registro para el shell browser de Internet Explorer que pueden afectar a la apariencia y comportamiento del navegador Web.
WebBrowser de Internet Explorer	Los cambios no autorizados en el registro para el navegador Web de Internet Explorer que pueden afectar a la apariencia y comportamiento del navegador.
Hook de búsqueda de direcciones URL de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios no autorizados en el registro de los hooks de búsqueda de direcciones URL de Internet Explorer, lo que permite enviar el navegador a sitios Web sospechosos cuando se hacen búsquedas en Internet.
Direcciones URL de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de las URL de Internet Explorer, lo que afecta a la configuración del navegador.
Restricciones de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de las restricciones de Internet Explorer, lo que afecta a la configuración y a las opciones del navegador.
Zonas de seguridad de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el archivo de zonas de seguridad de Internet Explorer, lo que permite que se ejecuten archivos potencialmente dañinos al iniciar el equipo.
Sitios de confianza de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de sitios de confianza de Internet Explorer, lo que permite que el equipo confíe en sitios Web sospechosos.

guardián del sistema	Detecta...
Directiva de Internet Explorer	El software espía, el software publicitario y otros programas potencialmente no deseados que pueden realizar cambios en el registro de directivas de Internet Explorer, lo que afecta a la apariencia y comportamiento del navegador.

Uso de listas de confianza

Si VirusScan detecta un cambio en un archivo o en registro (Guardián del sistema), programa o desbordamiento de búfer, le pedirá que lo añada a una lista de confianza o lo elimine. Si confía en el elemento e indica que en el futuro no desea recibir ninguna notificación sobre esta actividad, el elemento se añade a una lista de confianza y VirusScan no lo detectará nunca más ni nos notificará sobre su actividad. Si se ha añadido un elemento a una lista de confianza pero decide bloquear esta actividad, puede hacerlo. El bloqueo evita que el elemento se ejecute y realice cambios en el ordenador sin notificarle cada vez que lo intenta. También puede quitar un elemento de una lista de confianza. Al quitarlo de la lista, VirusScan podrá detectar de nuevo la actividad del elemento.

Gestión de listas de confianza

Utilice el panel Listas de confianza para confiar en elementos que han sido detectados y en los que se ha confiado anteriormente o para bloquearlos. También puede quitar un elemento de una lista predeterminada para que VirusScan lo detecte de nuevo.

1 Abra el panel Listas de confianza.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Equipo y archivos**.
3. En la zona información Equipo y archivos, haga clic en **Configurar**.
4. En el panel Configuración de Equipo y archivos, asegúrese de que la protección contra virus está activada y haga clic en **Avanzada**.
5. Haga clic en **Listas de confianza** en el panel Protección antivirus.

2 Seleccione uno de los siguientes tipos de listas de confianza:
   - **Guardianes del sistema de programas**
   - **Guardianes del sistema de Windows**
   - **Guardianes del sistema de navegadores**
   - **Programas definidos como fiables**
   - **Desbordamiento de búfer de confianza**
3 En **Deseo**, elija una de las siguientes opciones:
   - Para que el objeto detectado pueda realizar cambios en el registro de Windows o en archivos de sistema importantes de su ordenador sin tener que notificárselo a usted, haga clic en **Confiar**.
   - Para evitar que el objeto detectado pueda realizar cambios en el registro de Windows o en archivos de sistema importantes de su ordenador sin tener que notificárselo a usted, haga clic en **Bloquear**.
   - Para eliminar el elemento detectado de las listas de confianza, haga clic en **Eliminar**.
4 Haga clic en **Aceptar**.

Nota: para obtener más información sobre los tipos de listas de confianza, consulte Acerca de los tipos de listas de confianza (página 64).

Acerca de los tipos de listas de confianza

Los Guardianes del sistema del panel Listas de confianza representan los cambios no autorizados en el registro y en archivos que VirusScan ha detectado, pero a los que ha decidido asignar desde una alerta o desde el panel de Resultados del análisis. Hay cinco tipos de listas de confianza que pueden gestionarse desde el panel Listas de confianza: Guardianes del sistema de programas, Guardianes del sistema de Windows, Guardianes del sistema de navegadores, Programas fiables y Desbordamientos del búfer de confianza.

Opción	Descripción
Guardianes del sistema de programas	Los Guardianes del sistema de programas del panel Listas de confianza representan los cambios no autorizados en el registro y en archivos que VirusScan ha detectado, pero a los que ha decidido asignar desde una alerta o desde el panel de Resultados del análisis. Los Guardianes del sistema de programas detectan cambios no autorizados en el registro y en archivos asociados con instalaciones de ActiveX, elementos de inicio, hooks de ejecución en shell de Windows y con la actividad de carga retrasada de objeto de servicio de shell. Estos tipos de cambios no autorizados en el registro y en archivos pueden causar daños en el equipo, poner en riesgo la seguridad y dañar archivos importantes del sistema.
Guardianes del sistema de Windows	Los Guardianes del sistema de Windows del panel Listas de confianza representan los cambios no autorizados en el registro y en archivos que VirusScan ha detectado, pero a los que ha decidido asignar desde una alerta o desde el panel de Resultados del análisis. Los Guardianes del sistema de Windows detectan cambios no autorizados en el registro y en archivos asociados con identificadores de menús contextuales, applnit DLLs, el archivo hosts de Windows, Shell Winlogon, proveedores de servicios por niveles (LSP) Winsock, etc. Estos tipos de cambios no autorizados en el registro o en los archivos pueden afectar al modo en que su ordenador envía y recibe la información en Internet, cambiar la apariencia y los hábitos de los programas y permitir la ejecución de programas sospechosos en su equipo.

Opción	Descripción
Guardianes del sistema de navegadores	Los Guardianes del sistema de navegadores del panel Listas de confianza representan los cambios no autorizados en el registro y en archivos que VirusScan ha detectado, pero a los que ha decidido asignar desde una alerta o desde el panel de Resultados del análisis. Los Guardianes del sistema de navegadores detectan los cambios no autorizados en el registro y otros hábitos no autorizados asociados con objetos de ayuda del navegador, complementos de Internet Explorer, complementos de Internet Explorer, URL de Internet Explorer, zonas de seguridad de Internet Explorer, etc. Estos tipos de cambios no autorizados en el registro pueden producir una actividad no autorizada en los navegadores como la redirección a sitios Web sospechosos, cambios en los ajustes y en las opciones del navegador y la confianza en sitios Web sospechosos.
Programas definidos como fiables	Los programas fiables son programas no deseados potencialmente, detectados previamente por VirusScan, pero en los que ha decidido confiar a través de una alerta o a través del panel Resultados del análisis.
Desbordamiento de búfer de confianza	Los desbordamientos del búfer representan una actividad no deseada anteriormente, detectada por VirusScan, pero en los que ha decidido confiar a través de una alerta o a través del panel Resultados del análisis. Los desbordamientos del búfer pueden causar daños en el equipo y dañar archivos. Los desbordamientos del búfer se producen cuando la cantidad de programas o de procesos de información sospechosos almacenada en un búfer supera su capacidad.

CAPÍTULO 13

McAfee Personal Firewall

Personal Firewall ofrece protección avanzada para su equipo y sus datos personales. Personal Firewall establece una barrera entre su equipo e Internet y supervisa en segundo plano si se realizan operaciones de tráfico de Internet que resulten sospechosas.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Personal Firewall incluye 68
Iniciar el cortafuegos 71
Trabajar con alertas 73
Gestionar las alertas informativas 77
Configurar la protección del cortafuegos 79
Gestionar programas y permisos 91
Gestionar conexiones de equipo 101
Gestionar los servicios del sistema 109
Registro, supervisión y análisis 115
Obtener más información sobre la seguridad en Internet 125

Personal Firewall incluye

Niveles de protección estándar y personalizada	Protéjase contra intrusiones y actividades sospechosas mediante la configuración de protección predeterminada o personalizable del cortafuegos.
Recomendaciones en tiempo real	Reciba recomendaciones de forma dinámica para ayudarle a decidir si debe permitirse el acceso a Internet a los programas o si el tráfico de red es fiable.
Gestión de acceso inteligente para los programas	Gestione el acceso a Internet de los programas mediante alertas y registros de eventos, y configure los permisos de acceso de programas específicos.
Protección para juegos	Evite que las alertas de intentos de intrusión y de actividades sospechosas lo distraigan cuando juegue en pantalla completa.
Protección al iniciar el equipo	Proteja su equipo contra intentos de intrusión y programas no deseados, así como el tráfico de red, en cuanto Windows® se inicia.
Control de puertos de servicio del sistema	Gestione los puertos de servicio del sistema abiertos o cerrados necesarios para algunos programas.
Gestión de conexiones de equipo	Permita o bloquee conexiones remotas entre otros equipos y su propio equipo.
Integración de la información de HackerWatch	Rastree patrones globales de intrusión y piratería informática a través del sitio Web de HackerWatch, que también proporciona información de seguridad actual acerca de los programas de su equipo, así como de eventos de seguridad globales y de estadísticas de puertos de Internet.
Firewall bloqueado	Bloquee instantáneamente todo el tráfico de red entrante y saliente entre el equipo e Internet.
Restaurar Firewall	Restaure al instante la configuración de protección original del cortafuegos.
Detección avanzada de troyanos	Detecte y bloquee aplicaciones potencialmente malintencionadas como, por ejemplo, troyanos, y evite que se envíen sus datos personales a Internet.
Registro de eventos	Rastree los eventos de intrusión, entrantes y salientes.
Control del tráfico de Internet	Revise mapas de todo el mundo que muestran el origen de los ataques hostiles y el tráfico. También localiza información detallada de propiedad y datos geográficos correspondientes a las direcciones IP de origen. Además, analice el tráfico entrante y saliente, controle el ancho de banda del programa y la actividad del programa.
Prevención de intrusiones	Proteja su privacidad contra las posibles amenazas de Internet. Gracias a la función heurística, proporcionamos un tercer nivel de protección mediante el bloqueo de los elementos que muestren indicios de ataque o intentos de piratería.

Análisis de tráfico sofisticados

Firewall revisa el tráfico entrante y saliente de Internet, así como las conexiones de programas, incluidas aquéllas que están "a la escucha" de conexiones abiertas. Esto permite a los usuarios ver los programas que pueden ser susceptibles de intrusión y actuar en consecuencia.

CAPÍTULO 14

Iniciar el cortafuegos

Desde el mismo momento en que instala el cortafuegos, su equipo queda protegido contra las intrusiones y el tráfico de red no deseado. Por otra parte, ya puede responder a las alertas y gestionar el acceso entrante y saliente a Internet, tanto para programas conocidos como desconocidos. Las recomendaciones inteligentes y el nivel de seguridad automático (con la opción para permitir programas de acceso saliente a Internet seleccionada) se activan automáticamente.

Si bien puede deshabilitar el cortafuegos desde el panel Configuración de Internet y redes, su equipo ya no estará protegido contra intrusiones y tráfico de red no deseado; tampoco podrá gestionar de manera eficiente las conexiones de Internet entrantes y salientes. Si tiene que deshabilitar la protección del cortafuegos, hágalo de manera temporal y sólo cuando sea realmente necesario. También puede habilitar el cortafuegos desde el panel Configuración de Internet y redes.

El cortafuegos desactiva automáticamente el servidor de seguridad de Windows y se establece como cortafuegos predeterminado.

Nota: Para configurar el cortafuegos, abra el panel Configuración de Internet y redes.

En este capítulo

Iniciar la protección de Firewall 71
Detener la protección de Firewall 72

Iniciar la protección de Firewall

Puede activar el cortafuegos para proteger su equipo contra intrusiones y tráfico de red no deseado, así como gestionar las conexiones a Internet entrantes y salientes.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está desactivada**, haga clic en **Activado**.

Detener la protección de Firewall

Puede desactivar el cortafuegos si no desea proteger su equipo contra intrusiones y tráfico de red no deseado. Cuando el cortafuegos está desactivado, no se pueden gestionar las conexiones entrantes y salientes de Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Desactivado**.

CAPÍTULO 15

Trabajar con alertas

El cortafuegos emplea todo un abanico de alertas para que gestione su seguridad con mayor facilidad. Las alertas se agrupan en tres tipos básicos:

- Alerta roja
- Alerta amarilla
- Alerta verde

Las alertas también pueden contener información de ayuda para que el usuario pueda decidir mejor cómo ordenar las alertas o bien obtener información relativa a los programas que se ejecutan en su equipo.

En este capítulo

Acerca de las alertas 74

Acerca de las alertas

El cortafuegos dispone de tres tipos de alerta básicos. A su vez, algunas alertas incluyen información relativa a los programas que se ejecutan en su equipo o sobre cómo obtener información.

Alerta roja

Una alerta roja que aparece cuando el cortafuegos detecta, y luego bloquea, un troyano en su equipo, y recomienda que analice el equipo en busca de más amenazas. Los troyanos tienen el aspecto de programas válidos, pero pueden trastornar o dañar los equipos, así como proporcionar acceso no autorizado a ellos. Esta alerta se produce en todos los niveles de seguridad.

Alerta amarilla

El tipo de alerta más habitual es la alerta amarilla, que información activa de la actividad de un programa o un evento de red detectado por cortafuegos. Cuando esto se produce, la alerta describe la actividad del programa o el evento de red y, a continuación, proporciona una o varias opciones que necesitan respuesta. Por ejemplo, la alerta **Nueva conexión de red** aparece cuando un equipo con cortafuegos instalado se conecta a una red nueva. Puede especificar el nivel de confianza que desea asignar a esta nueva red y, a continuación, ésta aparece en la lista Redes. Si Recomendaciones inteligentes está habilitada, los programas conocidos se agregan automáticamente al panel Permisos de programas.

Alerta verde

En la mayoría de los casos, una alerta verde proporciona información básica acerca de un evento y no requiere ningún tipo de respuesta. Las alertas verdes están desactivadas de manera predeterminada.

Ayuda al usuario

Muchas alertas del cortafuegos contienen información adicional para facilitarle la gestión de la seguridad de su equipo y consisten en lo siguiente:

- **Obtener más información sobre este programa**: inicie el sitio Web de seguridad global de McAfee para obtener información acerca de un programa que el cortafuegos ha detectado en su equipo.
- **Notifique a McAfee la existencia de este programa**: envíe información a McAfee acerca de un archivo desconocido que el cortafuegos ha detectado en su equipo.
- **Recomendaciones de McAfee**: consejos sobre cómo gestionar las alertas. Por ejemplo, una alerta le puede recomendar que permita acceso a un programa.

CAPÍTULO 16

Gestionar las alertas informativas

El cortafuegos permite visualizar u ocultar alertas de información cuando detecta intentos de intrusión o actividad sospechosa durante determinados eventos; por ejemplo, cuando se juega en pantalla completa.

En este capítulo

Mostrar las alertas mientras se juega 77
Ocultar alertas informativas 78

Mostrar las alertas mientras se juega

Puede permitir que las alertas de cortafuego informativas se visualicen cuando detecta intentos de intrusión o actividad sospechosa cuando se juega en pantalla completa.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configuración de SecurityCenter, en **Acerca de las alertas** haga clic en **Avanzado**.
4. En el panel Opciones de alerta, seleccione **Mostrar alertas informativas cuando se detecte el modo de juegos**.
5. Haga clic en **Aceptar**.

Ocultar alertas informativas

Puede evitar que las alertas de cortafuego informativas se visualicen cuando detecte intentos de intrusión o una actividad sospechosa.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Configurar**.
3. En el panel Configuración de SecurityCenter, en **Acerca de las alertas** haga clic en **Avanzado**.
4. En el panel Configuración de SecurityCenter, haga clic en **Alertas informativas**.
5. En el panel Alertas informativas, realice una de las siguientes operaciones:
   - Seleccione **No mostrar alertas informativas** para que se oculten todas las alertas informativas.
   - Despeje una alerta para ocultarla.
6. Haga clic en **Aceptar**.

CAPÍTULO 17

Configurar la protección del cortafuegos

El cortafuegos le ofrece varios métodos para gestionar su seguridad y personalizar su respuesta a las alertas y los eventos relacionados con la seguridad.

Después de instalar el cortafuegos por primera vez, el nivel de seguridad de la protección de su equipo se establecerá en Automático y se permitirá un acceso a Internet únicamente saliente. A pesar de ello, el cortafuegos proporciona otros niveles, desde el más restrictivo al más permisivo.

El cortafuegos también le ofrece la posibilidad de recibir recomendaciones sobre alertas y acceso a Internet para programas.

En este capítulo

Gestionar los niveles de seguridad del cortafuegos.....80
Configurar Recomendaciones inteligentes para alertas 83
Optimizar la seguridad del cortafuegos.....85
Bloquear y restaurar el cortafuegos.....88

Gestionar los niveles de seguridad del cortafuegos

Los niveles de seguridad del cortafuegos controlan el grado de gestión y respuesta a las alertas. Estas alertas aparecen cuando se detecta tráfico de red no deseado y conexiones de Internet entrantes y salientes. De forma predeterminada, el nivel de seguridad del cortafuegos se establece en Automático, con acceso únicamente saliente.

Cuando se establece el nivel de seguridad Automático y las recomendaciones inteligentes están activadas, las alertas amarillas dan la opción de permitir o bloquear el acceso a programas desconocidos que necesitan un acceso entrante. Aunque las alertas verdes están desactivadas de manera predeterminada, aparecen cuando se detectan programas conocidos y se permite el acceso automáticamente. Permitir el acceso a un programa significa permitirle establecer conexiones salientes y escuchar conexiones entrantes no solicitadas.

Por lo general, cuanto más restrictivo es un nivel de seguridad (Invisible y Estándar), mayor es el número de opciones y alertas que se muestran y que, por consiguiente, deberá gestionar.

En la tabla siguiente se describen los tres niveles de seguridad del cortafuegos, empezando por el más estricto y acabando por el menos:

Nivel	Descripción
Invisible	Bloquea todas las conexiones de Internet entrantes, salvo los puertos abiertos, y oculta la presencia del equipo en Internet. El cortafuegos le alertará cuando un nuevo programa intente una conexión saliente a Internet o si recibe solicitudes de conexión entrantes. Los programas bloqueados y agregados aparecen en el panel Permisos de programas.
Estándar	Controla las conexiones entrantes y salientes y le avisa cuando un nuevo programa intente acceder a Internet. Los programas bloqueados y agregados aparecen en el panel Permisos de programas.

Nivel	Descripción
Automático	Permite que los programas tengan acceso entrante y saliente (completo) o sólo saliente. El nivel de seguridad predeterminado es Automático con la opción para permitir que los programas tengan acceso únicamente saliente seleccionada. Si se permite acceso completo a un programa, el cortafuegos confiará automáticamente en él y lo agregará a la lista de programas permitidos en el panel Permisos de programa. Si se permite acceso únicamente saliente a un programa, el cortafuegos confiará automáticamente en él cuando efectúan únicamente una conexión a Internet saliente. No se confía automáticamente en una conexión entrante.

El cortafuegos también le permite restablecer de inmediato su nivel de seguridad en Automático (y permitir acceso únicamente saliente) desde el panel Restaurar valores predeterminados del cortafuegos.

Definir el nivel de seguridad como Invisible

Puede establecer el nivel de seguridad del cortafuegos en Invisible para bloquear todas las conexiones de red entrantes, salvo los puertos abiertos, y ocultar la presencia del equipo en Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Invisible** como el nivel actual.
4. Haga clic en **Aceptar**.

Nota: en el modo invisible, el cortafuegos le alerta cuando nuevos programas solicitan una conexión de Internet saliente o reciben solicitudes de conexión entrantes.

Definir el nivel de seguridad como Estándar

Puede establecer el nivel de seguridad en Estándar para controlar las conexiones entrantes o salientes y que le alerte cuando nuevos programas intenten acceder a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Estándar** como el nivel actual.
4. Haga clic en **Aceptar**.

Definir el nivel de seguridad como Automático

Puede establecer el nivel de seguridad del cortafuegos en Automático para permitir un acceso completo o sólo un acceso saliente.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, mueva el control deslizante de manera que aparezca **Automático** como el nivel actual.
4. Siga uno de estos procedimientos:
   - Para permitir un acceso de red entrante y saliente completo, seleccione **Permitir acceso pleno**.
   - Para permitir sólo el acceso saliente de la red, seleccione **Permitir sólo acceso saliente**.
5. Haga clic en **Aceptar**.

Nota: la opción predeterminada es **Permitir sólo acceso saliente**.

Configurar Recomendaciones inteligentes para alertas

Puede configurar el cortafuegos para incluir, excluir o mostrar recomendaciones en alertas cuando algún programa intenta acceder a Internet. Al habilitar Recomendaciones inteligentes obtendrá ayuda para decidir la manera cómo ordenar las alertas.

Cuando se ha aplicado Recomendaciones inteligentes (y el nivel de seguridad está establecido en Automático con acceso únicamente saliente activado), el cortafuegos permite automáticamente programas conocidos y bloquea aquellos potencialmente peligrosos.

Por el contrario, cuando Recomendaciones inteligentes no está aplicado, el cortafuegos ni permite ni bloquea el acceso a Internet, ni proporciona ninguna recomendación en la alerta.

Cuando Recomendaciones inteligentes está establecido en Mostrar, una alerta solicita al usuario que permita o bloquee el acceso, y el cortafuegos proporciona una recomendación en la alerta.

Habilitar Recomendaciones inteligentes

Puede activar Recomendaciones inteligentes para que el cortafuegos permita o bloquee automáticamente programas y le alerte sobre programas no reconocidos y potencialmente peligrosos.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **Aplicar Recomendaciones inteligentes**.
4. Haga clic en **Aceptar**.

Deshabilitar Recomendaciones inteligentes

Puede desactivar Recomendaciones inteligentes para que el cortafuegos permita o bloquee programas y le alerte sobre programas no reconocidos y potencialmente peligrosos. No obstante, las alertas no incluirán ninguna recomendación acerca de cómo tratar el acceso de los programas. Si el cortafuegos detecta un programa nuevo que parece sospechoso o que se sabe que puede ser una amenaza, bloqueará automáticamente el acceso a Internet a este programa.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **No aplicar Recomendaciones inteligentes**.
4. Haga clic en **Aceptar**.

Mostrar Recomendaciones inteligentes

Puede mostrar Recomendaciones inteligentes para mostrar únicamente una recomendación en las alertas para decidir si desea permitir o bloquear programas no reconocidos o potencialmente peligrosos.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Recomendaciones inteligentes**, seleccione **Mostrar Recomendaciones inteligentes**.
4. Haga clic en **Aceptar**.

Optimizar la seguridad del cortafuegos

La seguridad de su equipo puede estar en peligro de muchas maneras. Por ejemplo, algunos programas pueden intentar conectarse a Internet al iniciarse Windows®. Asimismo, otros usuarios informáticos pueden lograr una solicitud de ping en su equipo que les permita saber si está conectado a una red. Además, pueden enviar información a su equipo, mediante el protocolo UDP, en la forma de unidades de mensajes (datagramas). El cortafuegos protege su equipo frente a estos tipos de intrusión permitiéndole bloquear programas de manera que no puedan acceder a Internet al iniciarse Windows, lo que le permite bloquear solicitudes de ping que ayudan a otros usuarios a detectar su equipo en una red, y le permite impedir a otros usuarios que envíen información a su equipo en forma de unidades de mensajes (datagramas).

La configuración de instalación estándar incluye una detección automática para los intentos de intrusión más comunes, como los ataques de denegación de servicio o vulnerabilidades. Al utilizar esta configuración se garantiza su protección contra estos ataques y análisis. No obstante, puede deshabilitar la detección automática de uno o varios ataques y análisis en el panel Detección de intrusiones.

Proteger su equipo durante el inicio

Puede proteger su equipo cuando Windows se inicia, para bloquear los programas nuevos que no tenían acceso a Internet durante el arranque y ahora lo necesitan. El cortafuegos muestra las alertas pertinentes para los programas que han solicitado acceso a Internet, que el usuario puede permitir o bloquear.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Configuración de seguridad**, seleccione **Habilitar la protección durante el inicio de Windows**.
4. Haga clic en **Aceptar**.

Nota: las conexiones e intrusiones bloqueadas no quedan registradas mientras la protección al iniciar está habilitada.

Configurar solicitudes de ping

Puede permitir o evitar que otros usuarios de equipos detecten su equipo en la red.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Configuración de seguridad**, realice una de las siguientes acciones:
   - Seleccione **Permitir solicitudes de ping ICMP** para permitir que se detecte su equipo en la red mediante solicitudes de ping.
   - Borre **Permitir solicitudes de ping ICMP** para impedir que se detecte su equipo en la red mediante solicitudes de ping.
4. Haga clic en **Aceptar**.

Configurar opciones de UDP

Puede permitir a los usuarios de otras redes que envíen unidades de mensajes (datagramas) a su equipo mediante el protocolo UDP. Sin embargo, puede hacerlo únicamente si ha cerrado un puerto de servicio del sistema para bloquear este protocolo.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Nivel de seguridad, en **Configuración de seguridad**, realice una de las siguientes acciones:
   - Seleccione **Activar rastreo de puertos UDP** para permitir a los usuarios de otros equipos enviar unidades de mensajes (datagramas) a su equipo.
   - Desactive **Activar rastreo de puertos UDP** para impedir que los usuarios de otros equipos envíen unidades de mensajes (datagramas) a su equipo.
4. Haga clic en **Aceptar**.

Configurar la detección de intrusiones

Puede detectar los intentos de intrusión para proteger su equipo contra los ataques y los análisis no autorizados. La configuración estándar el cortafuegos incluye la detección automática de los intentos de intrusión más habituales como, por ejemplo, los ataques de denegación de servicio o vulnerabilidades; no obstante, puede desactivar la detección automática de uno o varios ataques o análisis.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Detección de intrusiones**.
4. En **Detectar intentos de intrusión**, realice una de las siguientes opciones:
   - Seleccione un nombre para detectar el ataque o el análisis de manera automática.
   - Borre un nombre para deshabilitar la detección automática del ataque o el análisis.
5. Haga clic en **Aceptar**.

Configurar los estados de protección del cortafuegos

Puede configurar el cortafuegos para que no tenga en cuenta que problemas específicos de su equipo no se notifican a SecurityCenter.

1. En el panel McAfee SecurityCenter, en **Información de SecurityCenter**, haga clic en **Configurar**.
2. En el panel Configuración de SecurityCenter, en **Estado de protección** haga clic en **Avanzado**.
3. En el panel Problemas omitidos, seleccione una o más de las opciones siguientes:
   - **La protección del cortafuegos está desactivada.**
   - **El servicio de cortafuegos no está en funcionamiento.**
   - **La protección del cortafuegos no está instalada en su equipo.**
   - **Su cortafuegos de Windows está desactivado.**
   - **El cortafuegos saliente no está instalado en este equipo.**
4. Haga clic en **Aceptar**.

Bloquear y restaurar el cortafuegos

Bloquear tráfico bloquea todas las conexiones de red entrantes y salientes, incluido el acceso a los sitios Web, al correo electrónico y a las actualizaciones de seguridad. Bloquear tráfico tiene el mismo resultado que desconectar los cables de red de su equipo. Puede utilizar esta opción para bloquear puertos abiertos en el panel Servicios del sistema y para ayudarle a aislar y solucionar problemas en su equipo.

Bloquear el cortafuegos al instante

Puede bloquear el cortafuegos para que bloquee al instante todo el tráfico de red entre el equipo y cualquier red, incluida Internet.

1. En el panel McAfee SecurityCenter, en **Tareas comunes**, haga clic en **Firewall bloqueado**.
2. En el panel Bloquear cortafuegos haga clic en **Habilitar bloqueo de cortafuegos**.
3. Haga clic en **Sí** para confirmar.

Sugerencia: también puede bloquear el cortafuegos pulsando con el botón derecho del ratón en el icono de SecurityCenter en el área de notificación ubicada en el extremo derecho de la barra de tareas y, a continuación, haciendo clic en **Vínculos rápidos** y en **Firewall bloqueado**.

Desbloquear el cortafuegos de manera instantánea

Puede desbloquear el cortafuegos para que permita al instante todo el tráfico de red entre el equipo y cualquier red, incluida Internet.

1. En el panel McAfee SecurityCenter, en **Tareas comunes**, haga clic en **Firewall bloqueado**.
2. En el panel Bloqueo activado haga clic en **Deshabilitar bloqueo de cortafuegos**.
3. Haga clic en **Sí** para confirmar.

Restaurar la configuración del cortafuegos

Puede restaurar el cortafuegos con su configuración de protección original rápidamente. Esta opción restablece el nivel de seguridad en Automático y permite sólo el acceso saliente de red, activa las recomendaciones inteligentes, restaura la lista de programas predeterminados y sus permisos en el panel Permisos de programa, elimina las direcciones IP fiables y no permitidas y restaura los servicios del sistema, la configuración del registro de eventos y la detección de intrusiones.

1. En el panel McAfee SecurityCenter, haga clic en **Restaurar valores predeterminados del cortafuegos**.
2. En el panel Restaurar valores predeterminados de protección del cortafuegos, haga clic en **Restaurar valores predeterminados**.
3. Haga clic en **Sí** para confirmar.
4. Haga clic en **Aceptar**.

CAPÍTULO 18

Gestionar programas y permisos

El cortafuegos le permite gestionar y crear permisos de acceso tanto para programas ya existentes como para programas nuevos que soliciten acceso a Internet entrante y saliente. El cortafuegos le permite controlar el acceso pleno o sólo saliente a estos programas. Aunque también puede bloquearles el acceso.

En este capítulo

Permiso de acceso a Internet para los programas 92
Permiso para programas de sólo acceso saliente 94
Bloquear el acceso a Internet a los programas 96
Eliminar los permisos de acceso de los programas 97
Obtener información sobre los programas 98

Permiso de acceso a Internet para los programas

Algunos programas, como los navegadores de Internet, necesitan acceder a Internet para funcionar correctamente.

El cortafuegos le permite utilizar el panel Permisos de programas para:

- Permite el acceso a los programas
- Permite a los programas sólo acceso saliente
- Bloquear el acceso a los programas

También puede permitir que un programa tenga acceso pleno o sólo saliente desde el registro Eventos salientes y eventos recientes.

Conceder acceso pleno a un programa

Puede permitir que un programa bloqueado de su equipo tenga acceso pleno entrante y saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa con **Bloqueado** o **Acceso sólo saliente**.
5. En **Acción**, haga clic en **Permitir acceso**.
6. Haga clic en **Aceptar**.

Conceder acceso pleno a un programa nuevo

Puede permitir que un programa nuevo de su equipo tenga acceso pleno entrante y saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, haga clic en **Agregar programa con permiso**.
5. En el cuadro de diálogo **Agregar programa**, navegue hasta el programa que desee agregar y selecciónelo; a continuación, haga clic en **Abrir**.

Nota: Puede modificar los permisos de un programa recién agregado como lo haría con un programa ya existente, es decir, seleccionando el programa y haciendo clic en **Permitir sólo acceso saliente** o bien **Bloquear acceso** en **Acción**.

Permitir acceso pleno desde el registro Eventos recientes

Puede permitir que un programa bloqueado existente que aparece en el registro de eventos recientes tenga acceso pleno entrante y saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, seleccione la descripción del evento y luego haga clic en **Permitir acceso**.
4. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Temas relacionados

- Ver eventos salientes (página 117)

Permitir acceso pleno desde el registro Eventos salientes

Puede permitir que un programa bloqueado existente que aparece en el registro de eventos salientes tenga acceso pleno entrante y saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos salientes**.
5. Seleccione un programa y en **Deseo**, haga clic en **Permitir acceso**.
6. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Permiso para programas de sólo acceso saliente

Algunos programas de su equipo necesitan un acceso a Internet saliente. El cortafuegos le permite configurar permisos para que sea posible el acceso sólo saliente a Internet.

Permitir a un programa sólo acceso saliente

Puede permitir que un programa tenga un acceso a Internet sólo saliente.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa con **Bloqueado** o **Acceso pleno**.
5. En **Acción**, haga clic en **Permitir sólo acceso saliente**.
6. Haga clic en **Aceptar**.

Permitir sólo acceso saliente desde el registro Eventos recientes

Puede permitir que un programa bloqueado existente que aparece en el registro de eventos recientes tenga sólo acceso saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, seleccione la descripción del evento y luego haga clic en **Permitir sólo acceso saliente**.
4. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Permitir sólo acceso saliente desde el registro Eventos salientes

Puede permitir que un programa bloqueado existente que aparece en el registro de eventos salientes tenga sólo acceso saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos salientes**.
5. Seleccione un programa y en **Deseo**, haga clic en **Permitir sólo acceso saliente**.
6. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Bloquear el acceso a Internet a los programas

El cortafuegos le permite bloquear los programas para que no accedan a Internet. Asegúrese de que al bloquear un programa no se va a interrumpir su conexión a Internet o la de otro programa que necesite acceso a Internet para funcionar correctamente.

Bloquear el acceso a los programas

Puede bloquear un programa para que no tenga acceso entrante ni saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa con **Acceso pleno** o **Sólo acceso saliente**.
5. En **Acción**, haga clic en **Bloquear acceso**.
6. Haga clic en **Aceptar**.

Bloquear el acceso a un nuevo programa

Puede bloquear un programa nuevo para que no tenga acceso entrante ni saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, haga clic en **Agregar programa bloqueado**.
5. En el cuadro de diálogo Agregar programa, navegue hasta el programa que desee agregar y selecciónelo; a continuación, haga clic en **Abrir**.

Nota: Puede modificar los permisos de un programa recién agregado seleccionando el programa y haciendo clic en **Permitir sólo acceso saliente** o bien **Permitir acceso** en **Acción**.

Bloquear el acceso desde el registro Eventos recientes

Puede bloquear un programa que aparezca en el registro Eventos recientes para que no tenga acceso entrante ni saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En **Eventos recientes**, seleccione la descripción del evento y luego haga clic en **Bloquear acceso**.
4. En el cuadro de diálogo Permisos de programa, haga clic en **Sí** para confirmar.

Eliminar los permisos de acceso de los programas

Antes de eliminar un permiso de un programa, asegúrese de que su ausencia no afectará a la funcionalidad de su equipo o de su conexión a Internet.

Eliminar un permiso de programa

Puede hacer que un programa no tenga acceso entrante ni saliente a Internet.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa.
5. En **Acción**, haga clic en **Eliminar permiso de programa**.
6. Haga clic en **Aceptar**.

Nota: El cortafuegos le impide modificar algunos programas mediante la atenuación y la desactivación de determinadas acciones.

Obtener información sobre los programas

Si no está seguro de qué permiso de programa debe aplicar, puede obtener información acerca del programa en el sitio Web HackerWatch de McAfee.

Obtener información sobre un programa

Puede obtener información del programa en el sitio Web HackerWatch de McAfee para decidir si permitirá o bloqueará el acceso entrante y saliente a Internet.

Nota: asegúrese de que está conectado a Internet para que su navegador pueda lanzar correctamente el sitio Web HackerWatch de McAfee; allí encontrará información actualizada sobre los programas, los requisitos de acceso a Internet y las amenazas de seguridad.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Permisos de programas**.
4. En **Permisos de programas**, seleccione un programa.
5. En **Acción**, haga clic en **Más información**.

Obtener información sobre el programa desde el registro Eventos salientes

En el registro de eventos salientes, puede obtener información del programa en el sitio Web HackerWatch de McAfee para decidir a qué programas permitirá o bloqueará el acceso entrante y saliente a Internet.

Nota: asegúrese de que está conectado a Internet para que su navegador pueda lanzar correctamente el sitio Web HackerWatch de McAfee; allí encontrará información actualizada sobre los programas, los requisitos de acceso a Internet y las amenazas de seguridad.

1. En el panel McAfee SecurityCenter, haga clic en **Menú avanzado**.
2. Haga clic en **Informes & registros**.
3. En Eventos recientes, seleccione un evento y haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos salientes**.
5. Seleccione una dirección IP y haga clic en **Más información**.

CAPÍTULO 19

Gestionar conexiones de equipo

Puede configurar el cortafuegos para gestionar conexiones remotas específicas a su equipo mediante la creación de reglas, basadas en direcciones del protocolo de Internet (IP), que están asociadas a los equipos remotos. Los equipos que están asociados a direcciones IP fiables se pueden conectar a su equipo con confianza, mientras que a las IP que sean desconocidas, sospechosas o no sean fiables, se les puede prohibir que se conecten a su equipo.

Al permitir una conexión, asegúrese de que el equipo en el que confía sea seguro. Si un equipo fiable resulta infectado por un gusano u otro mecanismo, su equipo podría ser infectado. Además, McAfee recomienda que el equipo en el que confía esté protegidos por un cortafuegos y un programa antivirus actualizado. El cortafuegos no registra el tráfico ni genera alertas de los eventos procedentes de las direcciones IP fiables que están en la lista **Redes**.

Puede prohibir equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables de modo que no puedan conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP.

En este capítulo

Acerca de las conexiones de equipo.....102
Prohibir conexiones de equipo.....106

Acerca de las conexiones de equipo

Las conexiones de equipo son las conexiones que usted crea entre otros equipos de cualquier red y el suyo. Puede agregar, editar y eliminar direcciones IP en la lista **Redes**. Estas direcciones IP están asociadas a redes a las que desee asignar un nivel de confianza al conectarse a su equipo: Fiable, Estándar y Pública.

Nivel	Descripción
Fiable	El cortafuegos permite que el tráfico de una IP llegue a su equipo a través de cualquier puerto. El cortafuegos no filtra ni analiza la actividad que pueda haber entre el equipo asociado a un dirección IP fiable y su equipo. De manera predeterminada, la primera red privada que encuentra el cortafuegos aparece como Fiable en la lista **Redes**. Un ejemplo de red Fiable es un equipo o varios equipos de su red local o doméstica.
Estándar	El cortafuegos controla el tráfico de una IP (pero no de otro equipo de la misma red) cuando se conecta a su equipo, y lo permite o lo bloquea según las reglas de la lista **Servicios del sistema**. El cortafuegos registra el tráfico y genera alertas de eventos a partir de IP estándar. Un ejemplo de una red estándar es un equipo o varios equipos de una red corporativa.
Pública	El cortafuegos controla el tráfico de una red pública según las reglas de la lista **Servicios del sistema**. Un ejemplo de red pública es una red de Internet en una cafetería, un hotel o un aeropuerto.

Al permitir una conexión, asegúrese de que el equipo en el que confía sea seguro. Si un equipo fiable resulta infectado por un gusano u otro mecanismo, su equipo podría ser infectado. Además, McAfee recomienda que el equipo en el que confía esté protegidos por un cortafuegos y un programa antivirus actualizado.

Agregar una conexión de equipo

Puede agregar una conexión de equipo fiable, estándar o pública y su dirección IP asociada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Redes**.
4. En el panel Redes, haga clic en **Agregar**.
5. Si la conexión del equipo se encuentra en una red IPv6, seleccione la casilla **IPv6**.
6. En **Agregar regla**, realice una de las acciones siguientes:
   - Seleccione **Único** y luego introduzca la dirección IP en el cuadro **Dirección IP**.
   - Seleccione **Intervalo** y luego introduzca las direcciones IP inicial y final en los cuadros **Dirección IP inicial** y **Dirección IP final**. Si la conexión de su equipo se encuentra en una red IPv6, introduzca la dirección IP inicial y la longitud del prefijo en los cuadros **Dirección IP inicial** y **Longitud del prefijo**.
7. En **Tipo**, realice una de las acciones siguientes:
   - Seleccione **Fiable** para especificar que la conexión de este equipo es fiable (por ejemplo, un equipo de una red doméstica).
   - Seleccione **Estándar** para especificar que la conexión de este equipo (y no la de otros equipos de la misma red) es fiable (por ejemplo, un equipo de una red corporativa).
   - Seleccione **Pública** para especificar que la conexión de este equipo es pública (por ejemplo, un equipo de un cibercafé, un hotel o un aeropuerto).
8. Si un servicio del sistema utiliza Conexión compartida a Internet (ICS), podrá agregar el rango de direcciones IP siguiente: de 192.168.0.1 a 192.168.0.255.
9. También tiene la opción de seleccionar **Regla caduca en** e introducir el número de días para aplicar la regla.
10. O también puede escribir una descripción para la regla.
11. Haga clic en **Aceptar**.

Nota: para obtener más información acerca de la Conexión compartida a Internet (ICS), consulte Configurar un servicio del sistema nuevo.

Agregar un equipo desde el registro Eventos entrantes

Puede agregar una conexión de equipo fiable o estándar y su dirección IP asociada desde el registro Eventos entrantes.

1. En el panel McAfee SecurityCenter, en el panel Tareas comunes, haga clic en **Menú avanzado**.
2. Haga clic en **Informes y registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos entrantes**.
5. Seleccione una dirección IP de origen y en **Deseo**, realice una de las acciones siguientes:
   - Haga clic en **Agregar esta IP como Fiable** para agregar este equipo como Fiable en su lista **Redes**.
   - Haga clic en **Agregar esta IP como Estándar** para agregar la conexión de este equipo como Estándar en su lista **Redes**.
6. Haga clic en **Sí** para confirmar.

Editar una conexión de equipo

Puede editar una conexión de equipo fiable, estándar o pública y su dirección IP asociada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Redes**.
4. En el panel Redes, seleccione una dirección IP y haga clic en **Editar**.
5. Si la conexión del equipo se encuentra en una red IPv6, seleccione la casilla **IPv6**.
6. En **Editar regla**, realice una de las acciones siguientes:
   - Seleccione **Único** y luego introduzca la dirección IP en el cuadro **Dirección IP**.
   - Seleccione **Intervalo** y luego introduzca las direcciones IP inicial y final en los cuadros **Dirección IP inicial** y **Dirección IP final**. Si la conexión de su equipo se encuentra en una red IPv6, introduzca la dirección IP inicial y la longitud del prefijo en los cuadros **Dirección IP inicial** y **Longitud del prefijo**.

7 En **Tipo**, realice una de las acciones siguientes:
   - Seleccione **Fiable** para especificar que la conexión de este equipo es fiable (por ejemplo, un equipo de una red doméstica).
   - Seleccione **Estándar** para especificar que la conexión de este equipo (y no la de otros equipos de la misma red) es fiable (por ejemplo, un equipo de una red corporativa).
   - Seleccione **Pública** para especificar que la conexión de este equipo es pública (por ejemplo, un equipo de un cibercafé, un hotel o un aeropuerto).
8 También tiene la opción de verificar **Regla caduca en** e introducir el número de días para aplicar la regla.
9 O también puede escribir una descripción para la regla.
10 Haga clic en **Aceptar**.

Nota: no puede editar la conexión predeterminada del equipo que el cortafuegos ha agregado automáticamente a partir de una red privada fiable.

Eliminar una conexión de equipo

Puede eliminar una conexión de equipo fiable, estándar o pública y su dirección IP asociada.

1 En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2 En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3 En el panel Cortafuegos haga clic en **Redes**.
4 En el panel Redes, seleccione una dirección IP y haga clic en **Eliminar**.
5 Haga clic en **Sí** para confirmar.

Prohibir conexiones de equipo

Puede agregar, editar y eliminar direcciones IP prohibidas en el panel IP prohibidas.

Puede prohibir equipos asociados a direcciones IP desconocidas, sospechosas o que no son fiables de modo que no puedan conectarse a su equipo.

El cortafuegos bloquea todo el tráfico no deseado, por lo que no suele ser necesario prohibir una dirección IP. Se debe definir una dirección IP como no permitida sólo cuando se esté seguro de que una conexión de Internet determinada supone una amenaza. Asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP.

Agregar una conexión de equipo no permitida

Puede agregar una conexión de equipo prohibida y su dirección IP asociada.

Nota: asegúrese de no bloquear direcciones IP importantes, como el servidor DNS o DHCP, u otros servidores pertenecientes al ISP.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **IP prohibidas**.
4. En el panel IP prohibidas, haga clic en **Agregar**.
5. Si la conexión del equipo se encuentra en una red IPv6, seleccione la casilla **IPv6**.
6. En **Agregar regla**, realice una de las acciones siguientes:
   - Seleccione **Único** y luego introduzca la dirección IP en el cuadro **Dirección IP**.
   - Seleccione **Intervalo** y luego introduzca las direcciones IP inicial y final en los cuadros **Dirección IP inicial** y **Dirección IP final**. Si la conexión de su equipo se encuentra en una red IPv6, introduzca la dirección IP inicial y la longitud del prefijo en los cuadros **Dirección IP inicial** y **Longitud del prefijo**.
7. También tiene la opción de seleccionar **Regla caduca en** e introducir el número de días para aplicar la regla.
8. O también puede escribir una descripción para la regla.
9. Haga clic en **Aceptar**.
10. Haga clic en **Sí** para confirmar.

Editar una conexión de equipo no permitida

Puede editar una conexión de equipo prohibida y su dirección IP asociada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **IP prohibidas**.
4. En el panel IP prohibidas, haga clic en **Editar**.
5. Si la conexión del equipo se encuentra en una red IPv6, seleccione la casilla **IPv6**.
6. En **Editar regla**, realice una de las acciones siguientes:
   - Seleccione **Único** y luego introduzca la dirección IP en el cuadro **Dirección IP**.
   - Seleccione **Intervalo** y luego introduzca las direcciones IP inicial y final en los cuadros **Dirección IP inicial** y **Dirección IP final**. Si la conexión de su equipo se encuentra en una red IPv6, introduzca la dirección IP inicial y la longitud del prefijo en los cuadros **Dirección IP inicial** y **Longitud del prefijo**.
7. También tiene la opción de seleccionar **Regla caduca en** e introducir el número de días para aplicar la regla.
8. O también puede escribir una descripción para la regla.
9. Haga clic en **Aceptar**.

Eliminar una conexión de equipo no permitida

Puede eliminar una conexión de equipo prohibida y su dirección IP asociada.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **IP prohibidas**.
4. En el panel IP prohibidas, seleccione una dirección IP y haga clic en **Eliminar**.
5. Haga clic en **Sí** para confirmar.

Prohibir un equipo desde el registro Eventos entrantes

Puede prohibir una conexión de equipo y su dirección IP asociada desde el registro Eventos entrantes. Utilice este registro, que muestra las direcciones IP de todo el tráfico de Internet entrante, para prohibir una dirección IP que crea que es el origen de actividad de Internet no deseada o sospechosa.

Agregue una dirección IP a su lista de **IP prohibidas** si desea bloquear todo el tráfico de Internet que entre desde esa dirección IP, independientemente de si los puertos de sus servicios de sistema están abiertos o cerrados.

1. En el panel McAfee SecurityCenter, en **Tareas comunes**, haga clic en **Menú avanzado**.
2. Haga clic en **Informes y registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y, a continuación, en **Eventos entrantes**.
5. Seleccione una dirección IP de origen y en **Deseo**, haga clic en **Prohibir esta IP**.
6. Haga clic en **Sí** para confirmar.

Prohibir un equipo desde el registro Eventos de detección de intrusiones

Puede prohibir una conexión de equipo y su dirección IP asociada desde el registro Eventos de detección de intrusiones.

1. En el panel McAfee SecurityCenter, en **Tareas comunes**, haga clic en **Menú avanzado**.
2. Haga clic en **Informes y registros**.
3. En **Eventos recientes**, haga clic en **Ver registro**.
4. Haga clic en **Internet y redes** y luego haga clic en **Eventos de detección de intrusiones**.
5. Seleccione una dirección IP de origen y en **Deseo**, haga clic en **Prohibir esta IP**.
6. Haga clic en **Sí** para confirmar.

CAPÍTULO 20

Gestionar los servicios del sistema

Para funcionar correctamente, algunos programas (incluidos los servidores Web o programas servidores de intercambio de archivos), deben aceptar conexiones no solicitadas procedentes de otros equipos a través de puertos de servicio de sistema designados. El cortafuegos suele cerrar estos puertos de servicio de sistema porque constituyen el origen más probable de las inseguridades en su sistema. Sin embargo, para aceptar conexiones procedentes de equipos remotos, los puertos de servicio de sistema deben estar abiertos.

En este capítulo

Configurar puertos de servicio del sistema 110

Configurar puertos de servicio del sistema

Los puertos de servicio del sistema pueden configurarse para permitir o bloquear el acceso en red remoto a un servicio de su equipo. Estos puertos del servicio del sistema pueden abrirse o cerrarse para los equipos que aparecen como Fiable, Estándar o Pública en su lista **Redes**.

La lista que mostramos a continuación muestra los servicios del sistema habituales, así como sus puertos asociados:

- Puerto de sistema operativo generalizado 5357
- Protocolo de transferencia de archivos (FTP): puertos 20-21
- Servidor de correo (IMAP): puerto 143
- Servidor de correo (POP3): puerto 110
- Servidor de correo (SMTP): puerto 25
- Servidor de directorio de Microsoft (MSFT DS): puerto 445
- Microsoft SQL Server (MSFT SQL): puerto 1433
- Network Time Protocol: puerto 123
- Puerto de Remote Desktop/Asistencia remota/Terminal Server (RDP): 3389
- Llamadas a procedimientos remotos (RPC): puerto 135
- Servidor Web seguro (HTTPS): puerto 443
- Plug and Play universal (UPNP): puerto 5000
- Servidor Web (HTTP): puerto 80
- Archivos compartidos en Windows (NETBIOS): puertos 137-139

Los puertos del servicio de sistema también se pueden configurar para que un equipo pueda compartir su conexión a Internet con otros equipos conectados a él a través de la misma red. Esta conexión, conocida como Conexión compartida a Internet (ICS), permite al equipo que comparte la conexión actuar como puerta de enlace a Internet para el otro equipo de la red.

Nota: si el equipo tiene una aplicación que acepta conexiones de servidor a Web o FTP, es posible que el equipo que comparta la conexión necesite abrir el puerto del servicio del sistema asociado y permitir el reenvío de las conexiones entrantes para dichos puertos.

Permitir el acceso a un puerto de servicio del sistema existente

Puede abrir un puerto existente para permitir el acceso remoto de una red a un servicio del sistema del equipo.

Nota: un puerto de servicio del sistema abierto puede dejar a su equipo totalmente vulnerable ante las amenazas de seguridad de Internet, por lo que es mejor que sólo abra un puerto cuando sea necesario.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. En **Abrir puerto de servicio del sistema**, seleccione un servicio del sistema para que abra su puerto.
5. Haga clic en **Editar**.
6. Siga uno de estos procedimientos:
   - Para abrir el puerto a cualquier equipo en una red fiable, estándar o pública (por ejemplo, una red doméstica, una red corporativa o Internet), seleccione **Fiable, Estándar y Pública**.
   - Para abrir el puerto a cualquier equipo en una red estándar (por ejemplo, una red corporativa), seleccione **Estándar (incluye Fiable)**.
7. Haga clic en **Aceptar**.

Bloquear el acceso a un puerto de servicio del sistema existente

Puede cerrar un puerto existente para bloquear el acceso remoto de una red a un servicio del sistema del equipo.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. En **Abrir puerto de servicio del sistema**, desactive la casilla situada junto al puerto del servicio del sistema que desee cerrar.
5. Haga clic en **Aceptar**.

Configurar un puerto de servicio del sistema

Puede configurar un puerto de servicio de red nuevo en su equipo, que pueda abrir o cerrar para permitir o bloquear el acceso remoto en su equipo.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. Haga clic en **Agregar**.
5. En el panel Servicios del sistema, en **Agregar regla de servicio del sistema**, introduzca lo siguiente:
   - Nombre del servicio del sistema
   - Categoría del servicio del sistema
   - Puertos TCP/IP locales
   - Puertos UPD locales
6. Siga uno de estos procedimientos:
   - Para abrir el puerto a cualquier equipo en una red fiable, estándar o pública (por ejemplo, una red doméstica, una red corporativa o Internet), seleccione **Fiable, Estándar y Pública**.
   - Para abrir el puerto a cualquier equipo en una red estándar (por ejemplo, una red corporativa), seleccione **Estándar (incluye Fiable)**.
7. Si desea enviar la información de actividad de este puerto a otro equipo de red de Windows que comparta la conexión a Internet, seleccione **Reenvíe la actividad de la red de este puerto a los equipos de la red que utilicen la función de conexión compartida a Internet**.
8. También puede introducir una descripción opcional para la nueva configuración.
9. Haga clic en **Aceptar**.

Nota: si el equipo tiene un programa que acepta conexiones de servidor a Web o FTP, es posible que el equipo que comparta la conexión necesite abrir el puerto del servicio del sistema asociado y permitir el reenvío de las conexiones entrantes para dichos puertos. Si utiliza Conexión compartida a Internet (ICS), también deberá agregar una conexión de equipo fiable en la lista **Redes**. Para obtener más información, consulte Agregar una conexión de equipo.

Modificar un puerto de servicio del sistema

Puede modificar la información de acceso entrante y saliente a la red de un puerto de servicio del sistema existente.

Nota: si la información del puerto está escrita de manera incorrecta, el servicio del sistema no funciona.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. Haga clic en la casilla situada junto al servicio del sistema y haga clic en **Editar**.
5. En el panel Servicios del sistema, en **Agregar regla de servicio del sistema**, modifique lo siguiente:
   - Nombre del servicio del sistema
   - Puertos TCP/IP locales
   - Puertos UPD locales
6. Siga uno de estos procedimientos:
   - Para abrir el puerto a cualquier equipo en una red fiable, estándar o pública (por ejemplo, una red doméstica, una red corporativa o Internet), seleccione **Fiable, Estándar y Pública**.
   - Para abrir el puerto a cualquier equipo en una red estándar (por ejemplo, una red corporativa), seleccione **Estándar (incluye Fiable)**.
7. Si desea enviar la información de actividad de este puerto a otro equipo de red de Windows que comparta la conexión a Internet, seleccione **Reenvíe la actividad de la red de este puerto a los equipos de la red que utilicen la función de conexión compartida a Internet**.
8. También puede introducir una descripción opcional para la configuración modificada.
9. Haga clic en **Aceptar**.

Eliminar un puerto de servicio del sistema

Puede eliminar un puerto de servicio del sistema existente de su equipo. Después de su eliminación, los equipos remotos ya no podrán acceder al servicio de red de su equipo.

1. En el panel McAfee SecurityCenter, haga clic en **Internet y redes** y, a continuación en **Configurar**.
2. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
3. En el panel Cortafuegos haga clic en **Servicios del sistema**.
4. Seleccione un servicio del sistema y haga clic en **Eliminar**.
5. En el indicador, haga clic en **Sí** para confirmar.

CAPÍTULO 21

Registro, supervisión y análisis

El cortafuegos proporciona el registro, supervisión y análisis de los eventos y el tráfico de Internet, los cuales resultan muy completos y de fácil lectura. El hecho de comprender mejor el tráfico y los eventos de Internet facilita la gestión de sus conexiones de Internet.

En este capítulo

Registro de eventos 116
Trabajar con estadísticas 118
Rastrear el tráfico de Internet 119
Supervisar el tráfico de Internet 122

Registro de eventos

El cortafuegos permite activar o desactivar el registro de eventos y, en el caso de que lo active, qué tipos de evento desea registrar. El registro de eventos le permite ver los eventos entrantes, salientes y de intrusión.

Configurar un registro de eventos

Puede especificar y configurar los tipos de eventos de cortafuegos que se registrarán. De forma predeterminada, el registro de eventos está activado para todos los eventos y actividades.

1. En el panel Configuración de Internet y redes, en **La protección por cortafuegos está activada**, haga clic en **Avanzadas**.
2. En el panel Cortafuegos, haga clic en **Configuración de registro de eventos**.
3. Si todavía no la ha seleccionado, seleccione la opción **Activar el Registro de eventos**.
4. En **Activar el Registro de eventos**, seleccione o despeje los tipos de eventos que desee o no desee registrar. Existen los tipos de evento siguientes:
   - Programas bloqueados
   - Pings ICMP
   - Tráfico de direcciones IP no permitidas
   - Eventos en puertos de servicio del sistema
   - Eventos en puertos desconocidos
   - Eventos de detección de intrusiones (IDS)
5. Para evitar el registro en algunos puertos específicos, seleccione **No registrar eventos en los puertos siguientes** e introduzca los números de puerto individuales separados por comas o series de puertos separados por guiones. Por ejemplo, `137-139, 445, 400-5000`.
6. Haga clic en **Aceptar**.

Ver eventos recientes

Si el registro está habilitado, podrá ver los eventos recientes. El panel Eventos recientes muestra la fecha y la descripción del evento. Muestra la actividad de programas a los que se ha bloqueado explícitamente el acceso a Internet.

- En el **Menú avanzado**, en el panel Tareas comunes, haga clic en **Informes & Registros** o **Ver eventos recientes**. Como alternativa, haga clic en **Ver eventos recientes** en el panel Tareas comunes desde el Menú básico.

Ver eventos entrantes

Si el registro está habilitado, podrá ver los eventos entrantes. Los eventos entrantes incluyen la fecha y la hora, la dirección IP de origen, el nombre de host y la información y tipo de evento.

1. Asegúrese de que el Menú avanzado esté activado. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y, a continuación, en **Eventos entrantes**.

Nota: Puede definir una dirección IP como fiable o permitida, o bien rastrearla desde el registro Eventos entrantes.

Ver eventos salientes

Si el registro está habilitado, podrá ver los eventos salientes. Eventos salientes incluye el nombre del programa que intenta obtener acceso saliente, la fecha y la hora del evento, y la ubicación del programa en su equipo.

1. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y, a continuación, en **Eventos salientes**.

Nota: Puede permitir acceso pleno y sólo saliente a un programa desde el registro Eventos salientes. También puede localizar información adicional sobre el programa.

Ver eventos de detección de intrusiones

Si el registro está activado, podrá ver los eventos de intrusiones entrantes. Los eventos de detección de intrusiones muestran la fecha y la hora, la dirección IP de origen, el nombre de host del evento y el tipo de evento.

1. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y luego haga clic en **Eventos de detección de intrusiones**.

Nota: Puede prohibir y rastrear una dirección IP desde el registro Eventos de detección de intrusiones.

Trabajar con estadísticas

El cortafuegos aprovecha el sitio Web de seguridad McAfee's HackerWatch para proporcionarle estadísticas sobre los eventos de seguridad de Internet y la actividad de puertos en todo el mundo.

Visualizar las estadísticas globales de los eventos de seguridad

HackerWatch rastrea los eventos de seguridad de Internet a nivel mundial, los cuales se pueden visualizar desde SecurityCenter. La información rastreada enumera los incidentes que ha recibido HackerWatch en las últimas 24 horas, 7 días y 30 días.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. En Seguimiento de eventos, vea las estadísticas de los eventos de seguridad.

Visualizar la actividad global de los puertos de Internet

HackerWatch rastrea los eventos de seguridad de Internet a nivel mundial, los cuales se pueden visualizar desde SecurityCenter. La información que se muestra incluye los puertos de eventos principales que HackerWatch ha registrado durante los últimos siete días. La información que se muestra suele ser de puertos HTTP, TCP y UDP.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. Visualice los eventos de los puertos principales en **Actividad de puertos reciente**.

Rastrear el tráfico de Internet

El cortafuegos ofrece varias opciones para rastrear el tráfico de Internet. Dichas opciones le permiten rastrear geográficamente un equipo de red, obtener información acerca del dominio y la red, y rastrear equipos desde los registros Eventos entrantes y Eventos de detección de intrusiones.

Rastrear un equipo de red geográficamente

Con Visual Tracer puede localizar geográficamente un equipo que esté conectado o esté intentado conectarse a su equipo, mediante su nombre o dirección IP. También puede acceder a información relativa a la red y al registro mediante Visual Tracer. Al ejecutar Visual Tracer aparece un mapamundi que muestra la ruta más probable que toman los datos entre el equipo de origen y el suyo.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de mapa**.

Nota: No se pueden rastrear eventos de direcciones IP de bucle de retorno, privadas o no válidas.

Obtenga información de registro de los equipos

Mediante Visual Trace puede obtener información de registro de un equipo desde SecurityCenter. Dicha información incluye el nombre de dominio, el nombre y la dirección de la persona registrada, y el contacto administrativo.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de personas registradas**.

Obtenga información de red de los equipos

Mediante Visual Trace puede obtener información de red de un equipo desde SecurityCenter. La información de red incluye detalles relativos a la red en la que reside el dominio.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Visual Tracer**.
3. Escriba la dirección IP del equipo y haga clic en **Rastrear**.
4. En **Visual Tracer**, seleccione **Vista de red**.

Rastrear un equipo desde el registro Eventos entrantes

Desde el panel Eventos entrantes, se puede rastrear una dirección IP que aparezca en el registro Eventos entrantes.

1. Asegúrese de que el Menú avanzado esté activado. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y, a continuación, en **Eventos entrantes**.
4. En el panel Eventos entrantes, seleccione una dirección IP de origen y luego haga clic en **Rastrear esta IP**.
5. En el panel Visual Tracer, realice una de las siguientes acciones:
   - **Vista de mapa**: Localiza un equipo geográficamente mediante la dirección IP seleccionada.
   - **Vista de personas registradas**: Localiza información relativa al dominio mediante la dirección IP seleccionada.
   - **Vista de red**: Localiza información relativa a la red mediante la dirección IP seleccionada.
6. Haga clic en **Listo**.

Rastrear un equipo desde el registro Eventos de detección de intrusiones

Desde el panel Eventos de detección de intrusiones, se puede rastrear una dirección IP que aparezca en el registro Eventos de detección de intrusiones.

1. En el panel Tareas comunes haga clic en **Informes y Registros**.
2. En **Eventos recientes**, haga clic en **Ver registro**.
3. Haga clic en **Internet y redes** y luego haga clic en **Eventos de detección de intrusiones**. En el panel Eventos de detección de intrusiones, seleccione una dirección IP de origen y luego haga clic en **Rastrear esta IP**.
4. En el panel Visual Tracer, realice una de las siguientes acciones:
   - **Vista de mapa**: Localiza un equipo geográficamente mediante la dirección IP seleccionada.
   - **Vista de personas registradas**: Localiza información relativa al dominio mediante la dirección IP seleccionada.
   - **Vista de red**: Localiza información relativa a la red mediante la dirección IP seleccionada.
5. Haga clic en **Listo**.

Rastrear una dirección IP supervisada

Puede rastrear una dirección IP supervisada para obtener una vista geográfica que muestre la ruta más probable que han seguido los datos desde el equipo de origen hasta el suyo. También puede obtener información de red y de registro sobre la dirección IP.

1. Asegúrese de que el Menú avanzado está habilitado y haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Programas activos**.
4. Seleccione un programa y luego la dirección IP que aparece debajo del nombre del programa.
5. En **Actividad del programa**, haga clic en **Rastrear esta IP**.
6. En **Visual Trace** aparece un mapa que muestra la ruta más probable que toman los datos entre el equipo de origen y el suyo. También puede obtener información de red y de registro sobre la dirección IP.

Nota: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Visual Trace**.

Supervisar el tráfico de Internet

El cortafuegos proporciona varios métodos para supervisar su tráfico de Internet, incluido lo siguiente:

- **Gráfico Análisis de tráfico**: Muestra el tráfico de Internet entrante y saliente más reciente.
- **Gráfico Uso del tráfico**: Muestra el porcentaje aproximado de ancho de banda que las aplicaciones más activas han utilizado durante las últimas 24 horas.
- **Programas activos**: Muestra aquellos programas que utilizan actualmente la mayoría de conexiones de Internet en su equipo, así como las direcciones IP a las que acceden dichos programas.

Acerca del gráfico Análisis del tráfico

El gráfico Análisis de tráfico es una representación numérica y gráfica del tráfico entrante y saliente de Internet. Además, el Monitor de tráfico muestra aquellos programas que utilizan la mayoría de conexiones de Internet en su equipo, así como las direcciones IP a las que acceden dichos programas.

Desde el panel Análisis de tráfico, se puede visualizar el tráfico de Internet entrante y saliente más reciente, así como las velocidades de transferencia actual, media y máxima. También puede visualizar el volumen de tráfico, incluida la cantidad de tráfico acumulada desde que inició el cortafuegos, y el tráfico total del mes actual o de los meses anteriores.

El panel Análisis de tráfico muestra la actividad de Internet en su equipo a tiempo real, incluidos el volumen y la velocidad del tráfico de Internet entrante y saliente más reciente de su equipo, la velocidad de conexión y el total de bytes transferidos a través de Internet.

La línea continua de color verde representa la velocidad actual de transferencia del tráfico entrante. La línea punteada de color verde representa la velocidad media de transferencia del tráfico entrante. Si la velocidad actual de transferencia y la velocidad media de transferencia coinciden, la línea de puntos no se muestra en el gráfico. La línea continua representa tanto la velocidad de transferencia media como la actual.

La línea continua de color rojo representa la velocidad actual de transferencia del tráfico saliente. La línea punteada de color rojo representa la velocidad media de transferencia del tráfico saliente. Si la velocidad actual de transferencia y la velocidad media de transferencia coinciden, la línea de puntos no se muestra en el gráfico. La línea continua representa tanto la velocidad de transferencia media como la actual.

Analizar el tráfico entrante y saliente

El gráfico Análisis de tráfico es una representación numérica y gráfica del tráfico entrante y saliente de Internet. Además, el Monitor de tráfico muestra aquellos programas que utilizan la mayoría de conexiones de Internet en su equipo, así como las direcciones IP a las que acceden dichos programas.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Análisis del tráfico**.

Sugerencia: Para ver las estadísticas más actualizadas, haga clic en **Actualizar** en **Análisis del tráfico**.

Supervisar el ancho de banda de un programa

Puede visualizar el gráfico de sectores, que muestra el porcentaje aproximado del ancho de banda utilizado por los programas que han estado más activos en su equipo durante las últimas veinticuatro horas. El gráfico de sectores ofrece una representación visual de las cantidades relativas del ancho de banda utilizado por los programas.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Uso del tráfico**.

Sugerencia: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Uso del tráfico**.

Supervisar la actividad de un programa

Puede ver la actividad entrante y saliente del programa, que le muestra las conexiones y puertos del equipo.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **Control del tráfico**.
3. En **Control del tráfico**, haga clic en **Programas activos**.
4. Puede ver la información siguiente:
   - Gráfico de actividad del programa: Seleccione un programa para que muestre un gráfico de su actividad.
   - Conexión en escucha: Seleccione un elemento en escucha bajo el nombre del programa.
   - Conexión del equipo: Seleccione una dirección IP con el nombre del programa, proceso del sistema o servicio.

Nota: Para visualizar las estadísticas más actualizadas, haga clic en **Actualizar** en **Programas activos**.

CAPÍTULO 22

Obtener más información sobre la seguridad en Internet

El cortafuegos aprovecha el sitio Web de seguridad de McAfee, HackerWatch, para proporcionarle información acerca de los programas y la actividad de Internet en todo el mundo. HackerWatch también pone a su disposición un tutorial HTML sobre el cortafuegos.

En este capítulo

Iniciar el tutorial de HackerWatch 126

Iniciar el tutorial de HackerWatch

Para obtener información sobre el cortafuegos, puede acceder al tutorial de HackerWatch desde SecurityCenter.

1. Asegúrese de que el Menú avanzado está habilitado y luego haga clic en **Herramientas**.
2. En el panel Herramientas haga clic en **HackerWatch**.
3. En **Recursos de HackerWatch**, haga clic en **Ver tutorial**.

CAPÍTULO 23

McAfee QuickClean

QuickClean mejora el rendimiento de su equipo mediante la eliminación de archivos que pueden crear desorden en el equipo. Vacía la Papelera de reciclaje y elimina los archivos temporales, accesos directos, fragmentos de archivos perdidos, archivos de registro, archivos en la caché, cookies, archivos del historial de navegación, correos electrónicos enviados y eliminados, archivos usados recientemente, archivos de Active-X y archivos de puntos de restauración del sistema. QuickClean también protege su privacidad mediante el uso del componente McAfee Shredder para eliminar de manera segura y permanente elementos que puedan contener información personal y delicada, como su nombre y dirección. Si desea información sobre la purga de archivos, consulte McAfee Shredder.

El Desfragmentador de disco organiza los archivos y las carpetas de su equipo para asegurar que no se esparzan (es decir, que no se fragmenten) cuando se guardan en el disco duro de su equipo. Mediante la desfragmentación de su disco duro de manera periódica, se garantiza que estos archivos y carpetas fragmentados se consoliden para poder recuperarlos rápidamente más adelante.

Si no desea mantener su equipo manualmente, puede programar QuickClean y el Desfragmentador de disco para que se ejecuten de manera automática, como tareas independientes con cualquier frecuencia que desee.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Características de QuickClean 128
Limpiando el equipo 129
Desfragmentación del equipo 133
Planificación de una tarea 135

Características de QuickClean

Limpiador de archivos	Permite eliminar archivos innecesarios de forma segura y eficaz utilizando diversos limpiadores. Mediante la eliminación de estos archivos, aumenta el espacio de su disco duro y mejora su rendimiento.

CAPÍTULO 24

Limpiando el equipo

QuickClean elimina los archivos que pueden colapsar su equipo. Vacía la Papelera de reciclaje y elimina los archivos temporales, accesos directos, fragmentos de archivos perdidos, archivos de registro, archivos en la caché, cookies, archivos del historial de navegación, correos electrónicos enviados y eliminados, archivos usados recientemente, archivos de Active-X y archivos de puntos de restauración del sistema. QuickClean elimina estos elementos sin que eso afecte a otra información esencial.

Puede utilizar cualquiera de los limpiadores de QuickClean para eliminar archivos innecesarios de su equipo. La siguiente tabla describe los limpiadores de QuickClean:

Nombre	Función
Limpiador de Papelera de reciclaje	Elimina los archivos de la Papelera de reciclaje.
Limpiador de archivos temporales	Elimina los archivos almacenados en las carpetas temporales.
Limpiador de accesos directos	Elimina los accesos directos deshabilitados y aquellos que no tienen un programa asociado.
Limpiador de fragmentos de archivos perdidos	Elimina del equipo los fragmentos de archivos perdidos.
Limpiador del Registro	Elimina la información de los programas que ya no están en el equipo del Registro de Windows®. El registro es una base de datos en la que Windows almacena su información de configuración. El registro contiene perfiles para cada usuario del equipo e información acerca del hardware, los programas instalados y los ajustes de propiedades del sistema. Windows consulta continuamente esta información durante su funcionamiento.

Nombre	Función
Limpiador de caché	Elimina los archivos de la caché que se almacenan mientras navega por páginas Web. Estos archivos se almacenan, por lo general, como archivos temporales en una carpeta de la caché. Una carpeta de la caché es un área de almacenamiento temporal de su equipo. Para aumentar la eficacia y velocidad de navegación de páginas Web, su explorador puede recuperar una página Web desde la caché la siguiente vez que desee verla, en lugar de tener que hacerlo desde un servidor remoto.
Limpiador de cookies	Elimina las cookies. Estos archivos se almacenan, por lo general, como archivos temporales. Una cookie es un pequeño archivo que contiene información y que, por lo general, incluye un nombre de usuario y la fecha y hora actual, que se almacena en el equipo de una persona que navega por Internet. Las cookies son utilizadas principalmente por los sitios Web para identificar a los usuarios que se han registrado previamente o que han visitado el sitio; sin embargo, también pueden ser una fuente de información para los piratas informáticos.
Limpiador del historial del navegador	Elimina el historial del navegador Web.
Limpiador de correo de Outlook Express y Outlook (para elementos eliminados y enviados)	Elimina los correos electrónicos enviados y eliminados de Outlook® y Outlook Express.
Limpiador utilizado recientemente	Elimina archivos usados recientemente que se hayan creado con cualquiera de estos programas: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®

Nombre	Función
Limpiador de ActiveX	Elimina los controles ActiveX. ActiveX es un componente de software que utilizan los programas o páginas Web para añadir funciones que se integran y aparecen como parte normal de esos programas o páginas Web. La mayor parte de los controles ActiveX son inofensivos; sin embargo, algunos pueden capturar información de su equipo.
Limpiador de punto de restauración del sistema	Elimina puntos antiguos de restauración del sistema de su equipo (excepto los más recientes). Windows crea los puntos de restauración del sistema para marcar cualquier cambio realizado en el equipo con el fin de que usted pueda volver a un estado anterior si tuviese lugar cualquier problema.

En este capítulo

Limpieza del equipo 132

Limpieza del equipo

Puede utilizar cualquiera de los limpiadores de QuickClean para eliminar archivos innecesarios de su equipo. Al finalizar, bajo **Resumen de QuickClean**, puede ver la cantidad de espacio en disco recuperada tras la limpieza, el número de archivos eliminados y la fecha y hora en la que se ejecutó la última operación de QuickClean de su equipo.

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **McAfee QuickClean**, haga clic en **Inicio**.
3. Siga uno de estos procedimientos:
   - Haga clic en **Siguiente** para aceptar los limpiadores predeterminados de la lista.
   - Active o desactive los limpiadores correspondientes y haga clic en **Siguiente.** Si selecciona el Limpiador utilizado recientemente, puede hacer clic en **Propiedades** para seleccionar o borrar los archivos que se han creado recientemente con los programas de la lista y, a continuación, haga clic en **Aceptar**.
   - Haga clic en **Restaurar valores predeterminados** para restaurar los limpiadores predeterminados y, a continuación, haga clic en **Siguiente.**
4. Una vez realizado el informe, haga clic en **Siguiente**.
5. Haga clic en **Siguiente** para confirmar la eliminación de los archivos.
6. Siga uno de estos procedimientos:
   - Haga clic en **Siguiente** para aceptar la opción predeterminada **No, deseo borrar los archivos con el método de eliminación estándar de Windows**.
   - Haga clic en **Sí, deseo usar Shredder para borrar de modo seguro los archivos** y especifique el número de veces que se ejecutará el proceso, hasta un máximo de 10 y, a continuación, haga clic en **Siguiente**. La purga de archivos puede ser un proceso largo si la cantidad de información que se ha de borrar es grande.
7. Si se bloquearon archivos o elementos durante la limpieza, puede que se le solicite que reinicie el equipo. Haga clic en **Aceptar** para cerrar la solicitud.
8. Haga clic en **Finalizar**.

Nota: Los archivos eliminados con Shredder no se pueden recuperar. Si desea información sobre la purga de archivos, consulte McAfee Shredder.

CAPÍTULO 25

Desfragmentación del equipo

El Desfragmentador de disco organiza los archivos y las carpetas de su equipo para que no se esparzan (es decir, que no se fragmenten) cuando se guardan en el disco duro de su equipo. Mediante la desfragmentación de su disco duro de manera periódica, se garantiza que estos archivos y carpetas fragmentados se consoliden para poder recuperarlos rápidamente más adelante.

Desfragmentación del equipo

Puede desfragmentar su equipo para mejorar el acceso y recuperación a sus archivos y carpetas.

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Desfragmentador de disco**, haga clic en **Analizar**.
3. Siga las instrucciones que aparecen en pantalla.

Nota: Si desea obtener más información acerca del Desfragmentador de disco, consulte la ayuda de Windows.

CAPÍTULO 26

Planificación de una tarea

El Planificador de tareas automatiza la frecuencia a la que QuickClean o el Desfragmentador de disco se ejecutan en su equipo. Por ejemplo, puede programar una tarea de QuickClean para vaciar su Papelera de reciclaje cada domingo a las 9:00 P.M. o una tarea del Desfragmentador de disco para desfragmentar el disco duro de su equipo el último día de cada mes. Puede crear, modificar o eliminar una tarea en cualquier momento. Debe haber iniciado sesión en su equipo para que se ejecute una tarea programada. Si, por cualquier motivo, no se ejecutase una tarea, se volverá a programar cinco minutos después de que se inicie sesión de nuevo.

Programación de una tarea de QuickClean

Puede programar una tarea de QuickClean para limpiar de manera automática su equipo usando uno o más limpiadores. Cuando acabe, bajo **Resumen de QuickClean**, puede ver la fecha y hora a la que su tarea está programada para ejecutarse de nuevo.

1. Abra el panel del Planificador de tareas.

   ¿Cómo?

   1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
   2. En **Planificador de tareas**, haga clic en **Inicio**.

2. En la lista **Seleccione la operación que desee programar**, haga clic en **McAfee QuickClean**.
3. Escriba un nombre para la tarea en el cuadro **Nombre de la tarea** y, a continuación, haga clic en **Crear.**
4. Siga uno de estos procedimientos:
   - Haga clic en **Siguiente** para aceptar los limpiadores de la lista.
   - Active o desactive los limpiadores correspondientes y haga clic en **Siguiente**. Si selecciona el Limpiador utilizado recientemente, puede hacer clic en **Propiedades** para seleccionar o borrar los archivos que se han creado recientemente con los programas de la lista y, a continuación, haga clic en **Aceptar**.
   - Haga clic en **Restaurar valores predeterminados** para restaurar los limpiadores predeterminados y, a continuación, haga clic en **Siguiente**.

5 Siga uno de estos procedimientos:

- Haga clic en **Calendario** para aceptar la opción predeterminada **No, deseo borrar los archivos con el método de eliminación estándar de Windows**.
- Haga clic en **Sí, deseo usar Shredder para borrar de modo seguro los archivos** y especifique el número de veces que se ejecutará el proceso, hasta un máximo de 10 y, a continuación, haga clic en **Calendario**.

6 Seleccione la frecuencia a la que desea que se ejecute la tarea en el cuadro de diálogo **Calendario** y, a continuación, haga clic en **Aceptar**.

7 Si realizó cambios en las propiedades del Limpiador utilizado recientemente, puede que se le solicite que reinicie el equipo. Haga clic en **Aceptar** para cerrar la solicitud.

8 Haga clic en **Finalizar**.

Nota: Los archivos eliminados con Shredder no se pueden recuperar. Si desea información sobre la purga de archivos, consulte McAfee Shredder.

Modificación de una tarea de QuickClean

Puede modificar una tarea planificada de QuickClean para cambiar los limpiadores que utiliza o la frecuencia a la que se ejecutará de manera automática en su equipo. Cuando acabe, bajo **Resumen de QuickClean**, puede ver la fecha y hora a la que su tarea está programada para ejecutarse de nuevo.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **McAfee QuickClean**.

3 Seleccione la tarea en la lista **Seleccione una tarea existente** y, a continuación, haga clic en **Modificar**.

4 Siga uno de estos procedimientos:

- Haga clic en **Siguiente** para aceptar los limpiadores para la tarea.
- Active o desactive los limpiadores correspondientes y haga clic en **Siguiente**. Si selecciona el Limpiador utilizado recientemente, puede hacer clic en **Propiedades** para seleccionar o borrar los archivos que se han creado recientemente con los programas de la lista y, a continuación, haga clic en **Aceptar**.

- Haga clic en **Restaurar valores predeterminados** para restaurar los limpiadores predeterminados y, a continuación, haga clic en **Siguiente.**

5 Siga uno de estos procedimientos:

- Haga clic en **Calendario** para aceptar la opción predeterminada **No, deseo borrar los archivos con el método de eliminación estándar de Windows**.
- Haga clic en **Sí, deseo usar Shredder para borrar de modo seguro los archivos**, especifique el número de veces que se ejecutará el proceso, hasta un máximo de 10 y, a continuación, haga clic en **Calendario**.

6 Seleccione la frecuencia a la que desea que se ejecute la tarea en el cuadro de diálogo **Calendario** y, a continuación, haga clic en **Aceptar**.

7 Si realizó cambios en las propiedades del Limpiador utilizado recientemente, puede que se le solicite que reinicie el equipo. Haga clic en **Aceptar** para cerrar la solicitud.

8 Haga clic en **Finalizar**.

Nota: Los archivos eliminados con Shredder no se pueden recuperar. Si desea información sobre la purga de archivos, consulte McAfee Shredder.

Eliminación de una tarea de QuickClean

Puede eliminar una tarea planificada de QuickClean si ya no desea que se ejecute automáticamente.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **McAfee QuickClean**.

3 Seleccione la tarea de la lista **Seleccione una tarea existente**.

4 Haga clic en **Eliminar** y, a continuación, haga clic en **Sí** para confirmar la eliminación.

5 Haga clic en **Finalizar**.

Planificación de una tarea del Desfragmentador de disco

Puede planificar una tarea del Desfragmentador de disco para planificar la frecuencia a la que se desfragmenta automáticamente el disco duro de su equipo. Cuando acabe, bajo **Desfragmentador de disco**, puede ver la fecha y hora a la que su tarea está programada para ejecutarse de nuevo.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **Desfragmentador de disco**.

3 Escriba un nombre para la tarea en el cuadro **Nombre de la tarea** y, a continuación, haga clic en **Crear**.

4 Siga uno de estos procedimientos:

- Haga clic en **Calendario** para aceptar la opción predeterminada **Realizar la desfragmentación aunque haya poco espacio libre**.
- Desactive la opción **Realizar la desfragmentación aunque haya poco espacio libre** y, a continuación, haga clic en **Calendario**.

5 Seleccione la frecuencia a la que desea que se ejecute la tarea en el cuadro de diálogo **Calendario** y, a continuación, haga clic en **Aceptar**.

6 Haga clic en **Finalizar**.

Modificación de una tarea del Desfragmentador de disco

Puede modificar una tarea planificada del Desfragmentador de disco para cambiar la frecuencia a la que se ejecuta automáticamente en su equipo. Cuando acabe, bajo **Desfragmentador de disco**, puede ver la fecha y hora a la que su tarea está programada para ejecutarse de nuevo.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **Desfragmentador de disco**.

3 Seleccione la tarea en la lista **Seleccione una tarea existente** y, a continuación, haga clic en **Modificar**.

4 Siga uno de estos procedimientos:

- Haga clic en **Calendario** para aceptar la opción predeterminada **Realizar la desfragmentación aunque haya poco espacio libre**.
- Desactive la opción **Realizar la desfragmentación aunque haya poco espacio libre** y, a continuación, haga clic en **Calendario**.

5 Seleccione la frecuencia a la que desea que se ejecute la tarea en el cuadro de diálogo **Calendario** y, a continuación, haga clic en **Aceptar**.

6 Haga clic en **Finalizar**.

Eliminación de una tarea del Desfragmentador de disco

Puede eliminar una tarea planificada del Desfragmentador de disco si ya no desea que se ejecute automáticamente.

1 Abra el panel del Planificador de tareas.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Mantener equipo**.
2. En **Planificador de tareas**, haga clic en **Inicio**.

2 En la lista **Seleccione la operación que desee programar**, haga clic en **Desfragmentador de disco**.

3 Seleccione la tarea de la lista **Seleccione una tarea existente**.

4 Haga clic en **Eliminar** y, a continuación, haga clic en **Sí** para confirmar la eliminación.

5 Haga clic en **Finalizar**.

CAPÍTULO 27

McAfee Shredder

McAfee Shredder elimina (o purga) permanentemente elementos de la unidad de disco duro de su equipo. Incluso si elimina archivos y carpetas manualmente, vacía la Papelera de reciclaje o elimina su carpeta de Archivos temporales de Internet, puede recuperar esta información utilizando herramientas forenses informáticas. Del mismo modo, un archivo eliminado se puede recuperar debido a que algunos programas crean copias ocultas y temporales de los archivos abiertos. Shredder protege su privacidad al eliminar de forma eficaz y definitiva estos archivos no deseados. Recuerde que los archivos purgados no se pueden restaurar.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Características de Shredder 142
Purga de archivos, carpetas y discos 142

Características de Shredder

Eliminar archivos y carpetas de forma permanente

Permite eliminar elementos del disco duro para que la información asociada a ellos no se pueda recuperar. Protege su privacidad eliminando de manera segura y permanente archivos y carpetas, elementos de la Papelera de reciclaje y de la carpeta de Archivos temporales de Internet y el contenido entero de los discos del equipo, como CD regrabables, discos duros externos y unidades de disquete.

Purga de archivos, carpetas y discos

Shredder garantiza que la información contenida en los archivos y carpetas eliminados de su Papelera de reciclaje y de la carpeta de Archivos temporales de Internet no se pueda recuperar, ni siquiera con herramientas especiales. Con Shredder, puede especificar cuántas veces (hasta un máximo de 10) desea que se purgue un elemento. Cuanto mayor sea al número de veces que se realiza esta operación, más eficaz será la eliminación del archivo.

Purgar archivos y carpetas

Puede purgar archivos y carpetas del disco duro de su equipo, incluidos los elementos de la Papelera de reciclaje y de la carpeta de Archivos temporales de Internet.

1 Abrir **Shredder**.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Menú avanzado**.
2. En el panel izquierdo, haga clic en **Herramientas**.
3. Haga clic en **Shredder**.

2 En el panel Purgar archivos y carpetas, bajo **Deseo**, haga clic en **Borrar archivos y carpetas**.

3 En **Nivel de purga**, haga clic en uno de los siguientes niveles de purga:

- **Rápido**: Purga una vez los elementos seleccionados.
- **Exhaustivo**: Purga siete veces los elementos seleccionados.
- **Personalizado**: Purga los elementos seleccionados un máximo de diez veces.

4 Haga clic en **Siguiente**.

5 Siga uno de estos procedimientos:

- En la lista **Seleccione los archivos que desee purgar**, haga clic en **Contenido de la Papelera de reciclaje** o **Archivos temporales de Internet**.
- Haga clic en **Examinar**, acceda a los archivos que desee purgar, selecciónelos y, a continuación, haga clic en **Abrir**.

6 Haga clic en **Siguiente**.

7 Haga clic en **Iniciar**.

8 Cuando Shredder acabe, haga clic en **Listo**.

Nota: No trabaje con estos archivos hasta que Shredder complete esta tarea.

Purgar un disco completo

Puede purgar el contenido entero de un disco de una sola vez. Sólo se pueden purgar las unidades extraíbles, como los discos duros externos, los CD grabables y los disquetes.

1 Abrir **Shredder**.

¿Cómo?

1. En el panel McAfee SecurityCenter, bajo **Tareas comunes**, haga clic en **Menú avanzado**.
2. En el panel izquierdo, haga clic en **Herramientas**.
3. Haga clic en **Shredder**.

2 En el panel Purgar archivos y carpetas, bajo **Deseo**, haga clic en **Borrar un disco entero**.

3 En **Nivel de purga**, haga clic en uno de los siguientes niveles de purga:

- **Rápido**: Purga la unidad seleccionada una vez.
- **Exhaustivo**: Purga siete veces la unidad seleccionada.
- **Personalizado**: Purga la unidad seleccionada un máximo de diez veces.

4 Haga clic en **Siguiente**.

5 En la lista **Seleccione el disco**, haga clic en la unidad que desee purgar.

6 Haga clic en **Siguiente** y, a continuación, en **Sí** para confirmar.

7 Haga clic en **Iniciar**.

8 Cuando Shredder acabe, haga clic en **Listo**.

Nota: No trabaje con estos archivos hasta que Shredder complete esta tarea.

CAPÍTULO 28

McAfee Network Manager

Network Manager ofrece una representación gráfica de los equipos y otros dispositivos que forman una red doméstica. Con Network Manager podrá gestionar de forma remota el estado de protección de cada uno de los equipos gestionados en la red, así como reparar también de forma remota todas las vulnerabilidades de seguridad que se hayan registrado en cualquiera de esos equipos. Si ha instalado McAfee Total Protection, Network Manager también puede supervisar su red frente a intrusos (equipos o dispositivos no reconocidos o que no son de confianza) que intenten conectarse a la misma.

Antes de comenzar a usar Network Manager, puede familiarizarse con algunas de las funciones más conocidas. En la ayuda de Network Manager hallará toda la información acerca de cómo configurar y utilizar dichas funciones.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de Network Manager 146
Descripción de los iconos de Network Manager 147
Configuración de una red gestionada.....149
Gestión remota de la red 155
Supervisión de sus redes 161

Funciones de Network Manager

Mapa de la red gráfica

Visualice una visión gráfica del estado de protección de los equipos y dispositivos que forman su red doméstica. Cuando realice cambios en su red (por ejemplo, al agregar un equipo), el mapa de la red reconoce estos cambios. Puede actualizar el mapa de la red, cambiar el nombre de la red y mostrar u ocultar componentes del mapa de la red para personalizar su vista. También puede ver los detalles asociados con cualquiera de los dispositivos mostrados en el mapa de la red.

Gestión remota

Permite gestionar el estado de protección de los equipos que conforman su red doméstica. Puede invitar a un equipo a conectarse a la red gestionada, controlar el estado de protección del equipo gestionado y solucionar vulnerabilidades de seguridad conocidas en un equipo remoto de la red.

Supervisión de la red

Si está disponible, Network Manager puede supervisar sus redes y notificarle en el momento en que se conecten amigos o intrusos. La supervisión de la red sólo está disponible si ha adquirido McAfee Total Protection.

Descripción de los iconos de Network Manager

La siguiente tabla describe los iconos que más se utilizan en el mapa de la red de Network Manager.

Icono	Descripción
	Representa un equipo gestionado, en línea
	Representa un equipo gestionado, sin conexión
	Representa un equipo no gestionado que tiene instalado SecurityCenter
	Representa un equipo no gestionado y sin conexión
	Representa un equipo en línea que no tiene instalado el SecurityCenter, o un dispositivo de red desconocido
	Representa un equipo sin conexión que no tiene instalado SecurityCenter o un dispositivo de red desconocido sin conexión
	Indica que el elemento correspondiente está protegido y conectado
	Indica que el elemento correspondiente requiere su atención
	Indica que el elemento correspondiente requiere su atención inmediata
	Representa un enrutador doméstico inalámbrico
	Representa un enrutador doméstico estándar
	Representa Internet cuando está conectado
	Representa Internet cuando está desconectado

CAPÍTULO 29

Configuración de una red gestionada

Para configurar una red gestionada, debe confiar en la red (si todavía no lo ha hecho) y agregar miembros (equipos) a la red. Es preciso que un equipo se convierta primero en miembro de confianza de la red antes de poder gestionarlo de forma remota o antes de concederle el permiso para que gestione otros equipos de la red de forma remota. Los miembros (equipos) ya existentes en la red que poseen permisos de administración son los que conceden el título de miembro de la red a los equipos nuevos.

Puede consultar la información relacionada con cualquiera de los elementos que aparecen en el mapa de la red incluso después de modificar la red (cuando, por ejemplo, agrega un equipo).

En este capítulo

Trabajar con el mapa de la red 150
Incorporación a la red gestionada.....152

Trabajar con el mapa de la red

Cada vez que conecte un equipo a la red, Network Manager analizará la red para determinar si existen miembros gestionados o no, los atributos del enrutador y el estado de Internet. Si no encuentra a ningún miembro, Network Manager supone que el equipo conectado actualmente es el primer equipo de la red y lo trata como a un miembro gestionado con permisos de administración. De forma predeterminada, el nombre de la red incluye el nombre del primer equipo que se conecta a la red con SecurityCenter instalado; de todos modos, puede cambiar el nombre de la red en cualquier momento.

Siempre que realice cambios en la red (por ejemplo, cuando agregue un equipo), puede personalizar el mapa de la red. Por ejemplo, puede actualizar el mapa de la red, cambiar el nombre de la red y mostrar u ocultar elementos del mapa de la red para personalizar su vista. También puede ver los detalles asociados a cualquiera de los elementos que se muestran en el mapa de la red.

Acceder al mapa de la red

El mapa de la red le ofrece una representación gráfica de los equipos y dispositivos que forman su red doméstica.

- En el menú básico o avanzado, haga clic en **Gestionar red**.

Nota: si todavía no confía en la red (con McAfee Personal Firewall), se le solicitará que lo haga la primera vez que acceda al mapa de la red.

Actualizar el mapa de la red

El mapa de la red se puede actualizar en cualquier momento; por ejemplo, después de que se haya incorporado otro equipo a la red gestionada.

1. En el menú básico o avanzado, haga clic en **Gestionar red**.
2. Haga clic en **Actualizar el mapa de la red** en **Deseo**.

Nota: el vínculo **Actualizar el mapa de la red** sólo está disponible cuando no hay ningún elemento seleccionado en el mapa de la red. Para desactivar un elemento, haga clic en el elemento seleccionado o en cualquier espacio en blanco del mapa de la red.

Cambiar el nombre de la red

De forma predeterminada, el nombre de la red incluye el nombre del primer equipo que se conecta a la red con SecurityCenter instalado. Si prefiere utilizar otro nombre, puede cambiarlo.

1 En el menú básico o avanzado, haga clic en **Gestionar red**.

2 Haga clic en **Cambiar nombre de red** en **Deseo**.

3 Escriba el nombre de la red en el cuadro **Nombre de red**.

4 Haga clic en **Aceptar**.

Nota: el enlace **Cambiar el nombre de la red** sólo está disponible cuando no hay ningún elemento seleccionado en el mapa de la red. Para desactivar un elemento, haga clic en el elemento seleccionado o en cualquier espacio en blanco del mapa de la red.

Mostrar u ocultar un elemento en el mapa de la red

De forma predeterminada, el mapa de la red muestra todos los equipos y dispositivos de su red doméstica. Si tiene elementos ocultos, puede volver a mostrarlos en cualquier momento. Sólo se pueden ocultar los elementos no gestionados, los equipos gestionados no se pueden ocultar.

Para...	En el menú Básico o Avanzado, haga clic en Gestionar red y luego haga lo siguiente:
Ocultar un elemento en el mapa de la red	Haga clic en un elemento del mapa de la red y otro clic en **Ocultar este elemento** en **Deseo**. En el cuadro de diálogo de confirmación, haga clic en **Sí**.
Mostrar elementos ocultos en el mapa de la red	En **Deseo**, haga clic en **Mostrar elementos ocultos**.

Ver detalles de un elemento

Para visualizar información detallada acerca de un elemento de la red, seleccione el componente en cuestión en el mapa de la red. Dicha información incluye el nombre del elemento, su estado de protección y demás información necesaria para gestionar el elemento.

1 Haga clic en el icono del elemento en el mapa de la red.

2 En **Detalles**, visualice la información sobre el elemento.

Incorporación a la red gestionada

Es preciso que un equipo se convierta primero en miembro de confianza de la red antes de poder gestionarlo de forma remota o antes de concederle el permiso para que gestione otros equipos de la red de forma remota. Los miembros (equipos) ya existentes en la red que poseen permisos de administración son los que conceden el título de miembro de la red a los equipos nuevos. Para asegurar que sólo los equipos de confianza se incorporan a la red, tanto los usuarios de los equipos que conceden el permiso como los de los equipos que se incorporan tienen que autenticarse.

Cuando un equipo se incorpora a la red, se le pide que exponga su estado de protección McAfee a los demás equipos de la red. Si el equipo accede a exponer su estado de protección, se convierte en miembro gestionado de la red. Si el equipo se niega a exponer su estado de protección, se convierte en miembro no gestionado de la red. Los miembros no gestionados de la red suelen ser equipos invitados que desean acceder a otras funciones de la red (por ejemplo, enviar archivos o compartir impresoras).

Nota: tras incorporarse a la red, y en el caso de que tenga instalados otros programas de redes McAfee (por ejemplo, EasyNetwork), esos programas también reconocerán al equipo como equipo gestionado. El nivel de permisos que se asigna a un equipo en Network Manager es aplicable al resto de programas de redes McAfee. Para más información acerca del significado de los distintos permisos (invitado, pleno o administrador) en otros programas de red McAfee, consulte la documentación correspondiente a cada programa.

Incorporarse a una red gestionada

Cuando reciba una invitación para incorporarse a una red gestionada, podrá aceptarla o rechazarla. También puede determinar si desea que los otros equipos de la red gestionen la configuración de seguridad de este equipo.

1. Asegúrese de que está seleccionada la casilla de verificación **Permitir que todos los equipos de esta red gestionen la configuración de seguridad** en el cuadro de diálogo Red gestionada.
2. Haga clic en **Incorporar**.
   Al aceptar la invitación, se muestran dos tarjetas.
3. Confirme que se trata de las mismas tarjetas que se mostraron en el equipo que le invitó a incorporarse a la red gestionada.
4. Haga clic en **Aceptar**.

Nota: si el equipo que le invitó a incorporarse a la red gestionada no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación, significa que ha habido un ataque a la seguridad en la red gestionada. En ese caso, la incorporación a la red puede poner en peligro a su equipo; por consiguiente, haga clic en **Cancelar** en el cuadro de diálogo Red gestionada.

Invitar a un equipo a que se incorpore a la red gestionada

Si un equipo se agrega a la red gestionada, o bien, existe un equipo no gestionado en la red, puede invitar a ese equipo a incorporarse a la red gestionada. Sólo los equipos con permisos administrativos en la red pueden invitar a otros equipos a que se incorporen a ella. Al enviar la invitación, se especifica también el nivel de permisos que se desea asignar al equipo que se incorpora.

1. Haga clic en el icono del equipo no gestionado en el mapa de la red.
2. Haga clic en **Gestionar este equipo** en **Deseo**.
3. En el cuadro de diálogo Invitar a un equipo a incorporarse a la red gestionada, realice una de las siguientes opciones:
   - Haga clic en **Permitir acceso de invitado a programas de redes gestionadas** para que el equipo pueda acceder a la red (puede utilizar esta opción para usuarios temporales de su equipo doméstico).
   - Haga clic en **Permitir acceso completo a programas de redes gestionadas** para que el equipo pueda acceder a la red.

- Haga clic en **Permitir acceso administrativo a programas de redes gestionadas** para que el equipo pueda acceder a la red con permisos de administrador. Asimismo, permite que el equipo conceda acceso, a su vez, a otros equipos que desean incorporarse a la red gestionada.

4 Haga clic en **Aceptar**.
El equipo recibe una invitación para incorporarse a la red gestionada. Cuando el equipo acepta la invitación, se muestran dos tarjetas.

5 Confirme que se trata de las mismas tarjetas que se muestran en el equipo que ha invitado a incorporarse a la red gestionada.

6 Haga clic en **Conceder acceso**.

Nota: si el equipo que ha invitado a incorporarse a la red gestionada no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación, significa que se ha producido un ataque a la seguridad en la red gestionada. Si permite que el equipo se incorpore a la red, puede poner en peligro a otros equipos; por consiguiente, haga clic en **Denegar acceso** en el cuadro de diálogo de confirmación de seguridad.

Dejar de confiar en los equipos de la red

Si ha confiado en otros equipos de la red por error, puede dejar de hacerlo.

- Haga clic en **Dejar de confiar en los equipos de esta red**, en **Deseo**.

Nota: el enlace **Dejar de confiar en los equipos de esta red** no está disponible si tiene permisos administrativos y existen otros equipos gestionados en la red.

CAPÍTULO 30

Gestión remota de la red

Después de configurar su red gestionada, puede gestionar de forma remota los equipos y dispositivos que forman la red. Puede gestionar el estado y los niveles de permiso de los equipos y dispositivos, así como solucionar problemas de seguridad de forma remota.

En este capítulo

Gestión de estado y permisos 156
Solución de vulnerabilidades de seguridad 158

Gestión de estado y permisos

Una red gestionada dispone de miembros gestionados y no gestionados. Los miembros gestionados permiten que otros equipos de la red gestionen su estado de protección de McAfee; los miembros no gestionados no lo permiten. Los miembros no gestionados suelen ser equipos invitados que desean acceder a otras funciones de la red (por ejemplo, enviar archivos o compartir impresoras). Un equipo gestionado de la red puede invitar en cualquier momento a un equipo no gestionado a que se convierta en equipo gestionado con permisos administrativos en la red. Del mismo modo, un equipo gestionado con permisos administrativos puede hacer que otro equipo gestionado deje de gestionarse en cualquier momento.

Los equipos gestionados tienen permisos administrativos, completos o de invitado. Los permisos administrativos permiten al equipo gestionado gestionar el estado de protección de todos los demás equipos gestionados de la red y conceder el título de miembro de la red a otros equipos. Los permisos pleno y de invitado sólo permiten al equipo acceder a la red. El nivel de permisos de un equipo se puede modificar en cualquier momento.

Dado que una red gestionada también puede tener dispositivos como, por ejemplo, enrutadores, puede utilizar Network Manager para gestionarlos. Asimismo, es posible configurar y modificar las propiedades de visualización de un dispositivo en el mapa de la red.

Gestionar el estado de protección de un equipo

Si no se está gestionando el estado de protección de un equipo en la red (en el caso, por ejemplo, de que el equipo no sea un miembro o sea un miembro no gestionado), puede solicitar su gestión.

1. Haga clic en el icono del equipo no gestionado en el mapa de la red.
2. Haga clic en **Gestionar este equipo** en **Deseo**.

Interrumpir la gestión del estado de protección de un equipo

Puede dejar de gestionar el estado de protección de un equipo gestionado de la red; sin embargo, este equipo dejará de estar gestionado, por lo que no podrá gestionar su estado de protección de forma remota.

1. Haga clic en el icono de un equipo gestionado en el mapa de la red.
2. Haga clic en **Detener la gestión de este equipo** en **Deseo**.
3. En el cuadro de diálogo de confirmación, haga clic en **Sí**.

Modificar los permisos de un equipo gestionado

Se pueden modificar los permisos de un equipo gestionado en cualquier momento. Esto permite modificar los equipos que pueden gestionar el estado de protección de otros equipos de la red.

1. Haga clic en el icono de un equipo gestionado en el mapa de la red.
2. Haga clic en **Modificar los permisos para este equipo** en **Deseo**.
3. En el cuadro de diálogo de modificación de permisos, active o desactive la casilla para determinar si este y otros equipos de la red gestionada pueden gestionarse mutuamente el estado de protección.
4. Haga clic en **Aceptar**.

Gestionar un dispositivo

Puede gestionar un dispositivo accediendo a su página Web de administración desde el mapa de redes.

1. Haga clic en el icono de un dispositivo en el mapa de la red.
2. Haga clic en **Gestionar este dispositivo**, en **Deseo**.
   Se abrirá un navegador Web que mostrará la página Web de administración del dispositivo.
3. En su navegador Web, introduzca sus datos de inicio de sesión y configure la seguridad del dispositivo.

Nota: si el dispositivo es un enrutador inalámbrico o un punto de acceso protegido por Wireless Network Security, deberá utilizar McAfee Wireless Network Security para configurar la seguridad del dispositivo.

Modificar las propiedades de visualización de un dispositivo

Al modificar las propiedades de visualización de un dispositivo, puede cambiar el nombre de visualización del mismo en el mapa de la red y especificar si se trata de un enrutador inalámbrico.

1. Haga clic en el icono de un dispositivo en el mapa de la red.
2. Haga clic en **Modificar propiedades de dispositivos** en **Deseo**.
3. Para especificar el nombre de visualización de un dispositivo, escriba el nombre en el cuadro **Nombre**.
4. Para especificar el tipo de dispositivo, haga clic en **Enrutador estándar** si no es un enrutador inalámbrico o **Enrutador inalámbrico** si lo es.
5. Haga clic en **Aceptar**.

Solución de vulnerabilidades de seguridad

Los equipos gestionados con permisos administrativos pueden gestionar el estado de protección McAfee de otros equipos gestionados de la red, así como solucionar de forma remota cualquier tipo de vulnerabilidad de seguridad que se registre. Por ejemplo, si el estado de protección McAfee de un equipo gestionado indica que VirusScan está desactivado, otro equipo gestionado que posea permisos administrativos puede activar VirusScan de forma remota.

Al solucionar vulnerabilidades de seguridad de forma remota, Network Manager repara los problemas más habituales. No obstante, algunas vulnerabilidades de seguridad pueden precisar la intervención manual en el equipo local. En tal caso, Network Manager soluciona aquellos problemas que se pueden resolver de forma remota y luego le solicita que solucione los temas restantes iniciando la sesión en SecurityCenter desde el equipo vulnerable y siguiendo las recomendaciones propuestas. En algunos casos, la solución sugerida consiste en instalar la versión más reciente de SecurityCenter en el equipo o equipos remotos de la red.

Solucionar vulnerabilidades de seguridad

Puede utilizar Network Manager para solucionar la mayoría de las vulnerabilidades de seguridad en equipos gestionados remotos. Por ejemplo, si VirusScan está desactivado en un equipo remoto, podrá activarlo.

1. Haga clic en el icono del elemento en el mapa de la red.
2. Visualice el estado de protección de un elemento en **Detalles**.
3. Haga clic en **Solucionar vulnerabilidades de seguridad** en **Deseo**.
4. Una vez solucionados los problemas de seguridad, haga clic en **Aceptar**.

Nota: si bien Network Manager soluciona automáticamente la mayoría de las vulnerabilidades de seguridad, algunas reparaciones pueden requerir que inicie SecurityCenter en el equipo vulnerable y siga las instrucciones que aparecen en pantalla.

Instalar el software de seguridad McAfee en equipos remotos

Si uno o más equipos de su red no tienen instalada la versión más reciente de SecurityCenter, su estado de protección no se podrá gestionar de forma remota. Si desea gestionar estos equipos de forma remota, deberá ir a cada uno de ellos e instalar la versión más reciente de SecurityCenter.

1. Asegúrese de seguir estas instrucciones en el equipo que desea gestionar de forma remota.
2. Tenga a mano su información de inicio de sesión de McAfee (se trata de la dirección de correo electrónico y contraseña que utilizó por vez primera cuando activó el software de McAfee).
3. En un navegador, vaya al sitio Web de McAfee, inicie sesión y haga clic en **Mi cuenta**.
4. Busque el producto que desee instalar, haga clic en el botón **Descargar** y, a continuación, siga las instrucciones que aparecerán en pantalla.

Sugerencia: también puede obtener información sobre cómo instalar el software de seguridad McAfee en equipos remotos abriendo el mapa de redes y haciendo clic en **Proteger mis PC** en **Deseo**.

CAPÍTULO 31

Supervisión de sus redes

Si tiene McAfee Total Protection instalado, Network Manager también supervisa que no haya intrusos en sus redes. Cada vez que un equipo o dispositivo desconocido se conecta a su red, se le notificará para que pueda decidir si dicho equipo o dispositivo es un Amigo o un Intruso. Un Amigo es un equipo o dispositivo reconocido y de confianza, y un Intruso es un equipo o dispositivo no reconocido o que no es de confianza. Si marca un equipo o dispositivo como Amigo, puede decidir si desea que se le notifique cada vez que dicho Amigo se conecte a la red. Si marca un equipo o dispositivo como Intruso, le avisaremos automáticamente cada vez que se conecte.

La primera vez que se conecte a una red tras instalar esta versión de Total Protection o actualizar a esta versión, marcaremos automáticamente cada equipo o dispositivo como Amigo y no le avisaremos cuando éste se conecte a la red en el futuro. Después de tres días, empezaremos a notificarle sobre cada equipo o dispositivo desconocido que se conecte de modo que pueda marcarlos usted mismo.

Nota: la supervisión de redes es una característica de Network Manager que sólo está disponible con McAfee Total Protection. Para obtener más información sobre Total Protection, visite nuestro sitio Web.

En este capítulo

Detener la supervisión de redes 162
Volver a activar las notificaciones de supervisión de redes.....162
Marcar como Intruso.....163
Marcar como Amigo 163
Dejar de detectar nuevos Amigos.....163

Detener la supervisión de redes

Si desactiva la supervisión de redes, ya no podremos avisarle si se conectan intrusos a su red doméstica o a cualquier otra red a la que usted se conecte.

1 Abrir el panel de Configuración de Internet y redes

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel Inicio de SecurityCenter, haga clic en **Internet y redes**.
3. En la sección de información de Internet y redes, haga clic en **Configurar**.

2 En **Supervisión de la red**, haga clic en **Desactivado**.

Volver a activar las notificaciones de supervisión de redes

Aunque puede desactivar las notificaciones de supervisión de redes, no se lo recomendamos. Si lo hace, es posible que ya no podamos comunicarle cuándo se conectan a su red equipos desconocidos o Intrusos. Si por un descuido desactiva estas notificaciones (por ejemplo, si selecciona la casilla **No volver a mostrar esta alerta** en una alerta), puede volver a activarlas en cualquier momento.

1 Abra el panel Opciones de alerta.

¿Cómo?

1. En **Tareas comunes**, haga clic en **Inicio**.
2. En el panel de la derecha, en **Información de SecurityCenter**, haga clic en **Configurar**.
3. En **Alertas**, haga clic en **Opciones avanzadas**.

2 En el panel Configuración de SecurityCenter, haga clic en **Alertas informativas**.

3 En el panel Alertas informativas, asegúrese de que las siguientes casillas estén desactivadas:

- **No mostrar alertas cuando se conecten nuevos equipos o dispositivos a la red**
- **No mostrar alertas cuando se conecten Intrusos a la red**
- **No mostrar alertas para Amigos sobre los que normalmente deseo que se me notifique**
- **No recordármelo cuando se detecten equipos o dispositivos desconocidos**

- **No avisarme cuando McAfee haya terminado de detectar nuevos Amigos**

4 Haga clic en **Aceptar**.

Marcar como Intruso

Marque un equipo o dispositivo de su red como Intruso si no lo reconoce o no confía en él. Le avisaremos automáticamente cada vez que éste se conecte a la red.

1 En el menú básico o avanzado, haga clic en **Gestionar red**.

2 En el mapa de redes, haga clic en un elemento.

3 En **Deseo**, haga clic en **Marcar como Amigo o Intruso**.

4 En el cuadro de diálogo, haga clic en **Un intruso**.

Marcar como Amigo

Marque un equipo o dispositivo de su red como Amigo únicamente si lo reconoce y confía en él. Al marcar un equipo o dispositivo como Amigo, también puede decidir si desea o no que se le notifique cada vez que éste se conecte a la red.

1 En el menú básico o avanzado, haga clic en **Gestionar red**.

2 En el mapa de redes, haga clic en un elemento.

3 En **Deseo**, haga clic en **Marcar como Amigo o Intruso**.

4 En el cuadro de diálogo, haga clic en **Un amigo**.

5 Para que se le notifique cada vez que este Amigo se conecte a la red, seleccione la casilla **Notificarme cuando este equipo o dispositivo se conecte a la red**.

Dejar de detectar nuevos Amigos

Durante los tres primeros días tras haberse conectado a una red con esta versión de Total Protection instalada, marcaremos automáticamente como Amigo cada equipo o dispositivo sobre el que no desea que se le notifique. Puede detener este marcado automático en cualquier momento durante esos tres días, pero no puede reiniciarlo más tarde.

1 En el menú básico o avanzado, haga clic en **Gestionar red**.

2 En **Deseo**, haga clic en **Dejar de detectar nuevos Amigos**.

CAPÍTULO 32

McAfee EasyNetwork

EasyNetwork permite compartir archivos de forma segura, simplificar la transferencia de archivos y compartir impresoras entre los equipos de su red doméstica. No obstante, todos los equipos de su red doméstica deben tener instalado EasyNetwork para poder acceder a sus funciones.

Antes de usar EasyNetwork, puede familiarizarse con algunas de sus funciones. Encontrará información mas detallada sobre la configuración y uso de estas funciones en la ayuda de EasyNetwork.

Nota: SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician.

En este capítulo

Funciones de EasyNetwork....166
Configuración de EasyNetwork....167
Compartir y enviar archivos....173
Compartir impresoras....179

Funciones de EasyNetwork

EasyNetwork ofrece las funciones siguientes.

Uso compartido de archivos

EasyNetwork hace que compartir archivos con otros equipos de la red sea muy fácil. Cuando comparte archivos, proporciona acceso de sólo lectura a otros equipos a estos archivos. Sólo los equipos con acceso completo o de administrador a su red gestionada (miembros) pueden compartir archivos o acceder a archivos compartidos por otros miembros.

Transferencia de archivos

Puede enviar archivos a otros equipos con acceso completo o de administrador a su red gestionada (miembros). Cuando reciba un archivo, aparecerá en su buzón de entrada de EasyNetwork. El buzón de entrada es una ubicación de almacenamiento temporal para todos aquellos archivos que le envíen otros equipos de la red.

Uso compartido de la impresora automatizado

Después de conectarse a una red gestionada, puede compartir con otros miembros cualquier impresora local que esté conectada con su equipo, utilizando el nombre actual de la impresora como nombre de impresora compartida. También detecta impresoras compartidas por otros equipos de la red y le permite configurar y utilizar estas impresoras.

CAPÍTULO 33

Configuración de EasyNetwork

Antes de poder utilizar EasyNetwork, deberá iniciarlo e incorporarse a una red gestionada. Tras incorporarse a una red gestionada, podrá compartir, buscar y enviar archivos a otros equipos de la red. También puede compartir impresoras. Puede decidir salir de la red en cualquier momento.

En este capítulo

Abrir EasyNetwork 167
Incorporarse a una red gestionada 168
Abandonar una red gestionada 170

Abrir EasyNetwork

Puede abrir EasyNetwork desde el menú Inicio de Windows o haciendo clic en el icono del escritorio correspondiente.

- En el menú **Inicio**, seleccione **Programas**, **McAfee** y, a continuación, haga clic en **McAfee EasyNetwork**.

Sugerencia: también puede abrir EasyNetwork haciendo doble clic en el icono McAfee EasyNetwork del escritorio.

Incorporarse a una red gestionada

Si ningún equipo de la red a la que está conectado dispone de SecurityCenter, se convertirá en miembro de la red y se le pedirá que identifique si la red es de confianza. Cuando el primer equipo se une a la red, el nombre de su equipo está incluido en el nombre de la red; sin embargo, puede cambiar el nombre de la red en cualquier momento.

Cuando un equipo se conecta a la red, envía una solicitud de incorporación a los equipos que están en la red. Cualquier equipo con permisos administrativos en la red puede conceder la solicitud. El equipo que la admita puede determinar también el nivel de permiso para el equipo que se une a la red; por ejemplo, como invitado (solamente transferencia de archivos) o completo/administrador (transferir y compartir archivos). En EasyNetwork, los equipos con acceso de administrador pueden conceder el acceso a otros equipos y administrar permisos (promover o degradar equipos); los equipos con un acceso completo realizan estas tareas administrativas.

Nota: tras incorporarse a la red, y en el caso de que tenga instalados otros programas de redes McAfee (por ejemplo, Network Manager), esos programas también reconocerán al equipo como equipo gestionado. El nivel de permisos que se asigna a un equipo en EasyNetwork se aplica a todos los programas de conexión a redes de McAfee. Para más información acerca del significado de los distintos permisos (invitado, pleno o administrador) en otros programas de red McAfee, consulte la documentación correspondiente a cada programa.

Incorporación a la red

Cuando un equipo se conecta a una red de confianza por primera vez tras instalar EasyNetwork, aparece un mensaje preguntándole si desea incorporarse a la red gestionada. Si el equipo está de acuerdo con la incorporación, se envía una solicitud a todos los demás equipos de la red que tengan derechos de administrador. Esta solicitud debe admitirse antes de que el equipo pueda compartir impresoras o archivos, o enviar y copiar archivos en la red. El primer equipo de la red obtiene permisos de administrador automáticamente.

1. En la ventana Archivos compartidos, haga clic en **Incorporarse a esta red**.
   Cuando un equipo de administrador de la red admite su solicitud, aparece un mensaje preguntándole si desea permitir que este equipo y otros equipos de la red gestionen la configuración de seguridad de los demás.
2. Para permitir que este y otros equipos de la red gestionen la configuración de seguridad de los demás, haga clic en **Aceptar**; de lo contrario, haga clic en **Cancelar**.
3. Compruebe que el equipo que concede el permiso muestre las tarjetas que aparecen en el cuadro de diálogo de confirmación de la seguridad y, a continuación, haga clic en **Aceptar**.

Nota: si el equipo que le invitó a incorporarse a la red gestionada no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación, significa que ha habido un ataque a la seguridad en la red gestionada. En ese caso, la incorporación a la red puede poner en peligro a su equipo; por consiguiente, haga clic en **Cancelar**en el cuadro de diálogo de confirmación.

Concesión de acceso a la red

Cuando un equipo solicita incorporarse a una red gestionada, se envía un mensaje a todos los demás equipos de la red que tengan derechos de administrador. El primer equipo que responde se convierte en el equipo que realiza la concesión. Como tal, usted es responsable de decidir qué tipo de acceso desea conceder al equipo: invitado, completo o administrador.

1. En la alerta, haga clic en el nivel de acceso adecuado.
2. En el cuadro de diálogo Invitar a un equipo a incorporarse a la red gestionada, realice una de las siguientes opciones:
   - Haga clic en **Permitir acceso de invitado a programas de redes gestionadas** para permitir que el equipo acceda a la red (puede utilizar esta opción para usuarios temporales de su equipo doméstico).
   - Haga clic en **Permitir acceso completo a programas de redes gestionadas** para permitir que el equipo acceda a la red.

- Haga clic en **Permitir acceso administrativo a programas de redes gestionadas** para permitir que el equipo acceda a la red con permisos de administrador. Asimismo, permite que el equipo conceda acceso, a su vez, a otros equipos que desean incorporarse a la red gestionada.

3 Haga clic en **Aceptar**.

4 Compruebe que el equipo muestre las tarjetas que aparecen en el cuadro de diálogo de confirmación de la seguridad y, a continuación, haga clic en **Conceder acceso**.

Nota: si el equipo no muestra las mismas tarjetas que aparecen en el cuadro de diálogo de confirmación de la seguridad, se ha producido una brecha de seguridad en la red gestionada. La concesión de acceso a este equipo puede poner su equipo en peligro; por lo tanto, haga clic en **Rechazar acceso** en el cuadro de diálogo de confirmación de la seguridad.

Cambiar el nombre de la red

De forma predeterminada, el nombre de la red incluye el nombre del primer equipo que se incorporó a ella; sin embargo, puede cambiar el nombre de la red en cualquier momento. Cuando cambie el nombre de la red, cambie la descripción de la red mostrada en EasyNetwork.

1 En el menú **Opciones**, haga clic en **Configurar**.

2 En el cuadro de diálogo Configurar, escriba el nombre de la red en el cuadro **Nombre de red**.

3 Haga clic en **Aceptar**.

Abandonar una red gestionada

Si se incorpora a una red gestionada y después decide que no quiere seguir siendo miembro de ella, puede abandonarla. Tras abandonar la red gestionada podrá reincorporase a ella siempre que lo desea; sin embargo, deberá obtener el permiso nuevamente. Para obtener más información acerca de la incorporación, consulte Incorporación a una red gestionada (página 168).

Abandonar una red gestionada

Puede abandonar una red gestionada a la que se haya incorporado previamente.

1. Desconectar el equipo de la red.
2. En EasyNetwork, en el menú **Herramientas**, haga clic en **Abandonar red**.
3. En el cuadro de diálogo Abandonar red, seleccione el nombre de la red que desea abandonar.
4. Haga clic en **Abandonar red**.

CAPÍTULO 34

Compartir y enviar archivos

EasyNetwork hace que compartir y enviar archivos con los otros equipos de la red sea muy fácil. Cuando comparte archivos, proporciona acceso de sólo lectura a estos archivos a otros equipos. Sólo los equipos que sean miembros de la red gestionada (con acceso completo o de administrador) pueden compartir archivos o acceder a archivos compartidos por otros equipos miembros.

Nota: si está compartiendo un número de archivos elevado, los recursos de su equipo pueden verse afectados.

En este capítulo

Cómo compartir archivos 174
Envío de archivos a otros equipos.....177

Cómo compartir archivos

Sólo los equipos que sean miembros de la red gestionada (con acceso completo o de administrador) pueden compartir archivos o acceder a archivos compartidos por otros equipos miembros. Si comparte una carpeta, se comparten todos los archivos incluidos en esa carpeta y sus subcarpetas; sin embargo, los archivos que se agreguen posteriormente a la carpeta no se compartirán automáticamente. Si se elimina un archivo o carpeta, se elimina de la ventana Archivos compartidos. Puede dejar de compartir un archivo en cualquier momento.

Para acceder a un archivo compartido, ábralo directamente desde EasyNetwork o cópielo en su equipo para abrirlo desde ahí. Si la lista de archivos compartidos es demasiado larga para ver dónde está el archivo, puede buscarlo.

Nota: no se puede acceder a los archivos compartidos con EasyNetwork desde otros equipos con el Explorador de Windows porque los archivos EasyNetwork deben compartirse a través de conexiones seguras.

Compartir un archivo

Cuando se comparte un archivo, todos los miembros pueden acceder a él con acceso completo o derechos de administrador a la red gestionada.

1. En el Explorador de Windows, localice el archivo que desea compartir.
2. Arrastre el archivo desde su ubicación en el Explorador de Windows hasta la ventana Archivos compartidos de EasyNetwork.

Sugerencia: también puede compartir un archivo haciendo clic en **Compartir archivos** del menú **Herramientas**. En el cuadro de diálogo Compartir, acceda a la carpeta donde esté almacenado el archivo que desee compartir, seleccione el archivo y, a continuación, haga clic en **Compartir**.

Detener el uso compartido de un archivo

Si comparte un archivo en la red gestionada, puede detener el uso compartido en cualquier momento. Cuando deja de compartir un archivo, otros miembros de la red gestionada ya no pueden acceder a él.

1. En el menú **Herramientas**, haga clic en **Detener el uso compartido de archivos**.
2. En el cuadro de diálogo Detener el uso compartido de archivos, seleccione el archivo que ya no desea compartir.
3. Haga clic en **Aceptar**.

Copiar un archivo compartido

Copie un archivo compartido si desea tenerlo después de que deje de compartirse. Puede copiar un archivo compartido desde cualquier equipo de la red gestionada.

- Arrastre un archivo desde la ventana Archivos compartidos en EasyNetwork hasta una ubicación del Explorador de Windows o al escritorio de Windows.

Sugerencia: también puede copiar un archivo compartido seleccionando el archivo en EasyNetwork y haciendo clic en **Copiar a** del menú **Herramientas**. En el cuadro de diálogo Copiar a carpeta, acceda a la carpeta en la que quiera copiar el archivo, selecciónela y haga clic en **Guardar**.

Buscar un archivo compartido

Puede buscar un archivo que no lo haya compartido usted ni ningún otro miembro de la red. Mientras escribe sus criterios de búsqueda, EasyNetwork muestra los resultados correspondientes en la ventana Archivos compartidos.

1. En la ventana Archivos compartidos, haga clic en **Buscar**.
2. Haga clic en la opción adecuada (página 176) de la lista **Contiene**.
3. Escriba parte o todo el nombre del archivo en la lista **Nombre de archivo o ruta**.
4. Haga clic en el tipo de archivo (página 176) adecuado de la lista **Tipo**.
5. En las listas **De** y **A**, haga clic en las fechas que representan el intervalo de fechas en las que se haya creado el archivo.

Criterios de búsqueda

Las siguientes tablas describen los criterios de búsqueda que puede especificar al buscar archivos compartidos.

Nombre del archivo o ruta

Contiene	Descripción
Contiene todas las palabras	Busca un nombre de archivo o una ruta que contenga todas las palabras que especifique en la lista **Nombre de archivo o ruta**, en cualquier orden.
Contiene alguna de las palabras	Busca un nombre de archivo o una ruta que contenga alguna de las palabras que especifique en la lista **Nombre de archivo o ruta**.
Contiene la cadena de texto exacta	Busca un nombre de archivo o una ruta que contenga la frase exacta que especifique en la lista **Nombre de archivo o ruta**.

Tipo de archivo

Tipo	Descripción
Cualquiera	Busca todos los tipos de archivos compartidos.
Documento	Busca todos los archivos compartidos.
Imagen	Busca todos los archivos de imagen compartidos.
Vídeo	Busca todos los archivos de vídeo compartidos.
Audio	Busca todos los archivos de audio compartidos.
Comprimido	Busca todos los archivos comprimidos (por ejemplo, archivos .zip).

Envío de archivos a otros equipos

Puede enviar archivos a otros equipos que sean miembros de la red gestionada. Antes de enviar un archivo, EasyNetwork comprueba que el equipo que recibe el archivo tiene suficiente espacio disponible en el disco.

Cuando reciba un archivo, aparecerá en su buzón de entrada de EasyNetwork. El buzón de entrada es una ubicación de almacenamiento temporal para todos aquellos archivos que le envíen otros equipos de la red. Si tiene abierto EasyNetwork al recibir un archivo, este archivo aparece al instante en su buzón de entrada; de lo contrario, aparece un mensaje en el área de notificación, situada en el extremo derecho de la barra de herramientas de Windows. Si no quiere recibir mensajes de notificación (por ejemplo, porque interrumpen las tareas que está realizando), puede desactivar esta opción. Si ya existe un archivo con el mismo nombre en el buzón de entrada, el nuevo archivo cambia de nombre por un sufijo numérico. Los archivos se mantienen en el buzón de entrada hasta que los acepte (deberá copiarlos en su equipo).

Enviar un archivo a otro equipo

Puede enviar un archivo a otro equipo de la red gestionada sin compartirlo. Antes de que el usuario del equipo receptor pueda ver el archivo, deberá guardarlo en una ubicación local. Para obtener más información, consulte Aceptar un archivo de otro equipo (página 178).

1. En el Explorador de Windows, localice el archivo que desea enviar.
2. Arrastre el archivo desde su ubicación en el Explorador de Windows hasta el icono de un equipo activo de EasyNetwork.

Sugerencia: para enviar múltiples archivos a un equipo presione CTRL al seleccionar los archivos. También puede enviar archivos haciendo clic en **Enviar** del menú **Herramientas**, seleccionando los archivos y después haciendo clic en **Enviar**.

Aceptar un archivo de otro equipo

Si otro equipo de la red gestionada le envía un archivo, deberá aceptarlo guardándolo en su equipo. Si EasyNetwork no se está ejecutando cuando se envía un archivo a su equipo, recibirá un mensaje de notificación en el área de notificación, situada en el extremo derecho de la barra de tareas. Haga clic en el mensaje de notificación para abrir EasyNetwork y acceder al archivo.

- Haga clic en **Recibido** y arrastre el archivo desde el buzón de entrada de EasyNetwork a una carpeta del Explorador de Windows.

Sugerencia: también puede recibir un archivo desde otro equipo seleccionando el archivo en su buzón de entrada de EasyNetwork y, a continuación, haciendo clic en **Aceptar** del menú **Herramientas**. En el cuadro de diálogo Aceptar en la carpeta, acceda a la carpeta en la que quiera guardar los archivos que esté recibiendo, selecciónela y, a continuación, haga clic en **Guardar**.

Recibir una notificación cuando se envíe el archivo

Puede recibir un mensaje de notificación cuando otro equipo de la red gestionada le envíe un archivo. Si EasyNetwork no se está ejecutando, el mensaje de notificación aparece en el área de notificación, situada en el extremo derecho de la barra de herramientas.

1. En el menú **Opciones**, haga clic en **Configurar**.
2. En el cuadro de diálogo Configurar, marque la casilla de verificación **Notificarme cuando otro equipo me envíe archivos**.
3. Haga clic en **Aceptar**.

CAPÍTULO 35

Compartir impresoras

Después de conectarse a una red gestionada, EasyNetwork comparte las impresoras locales que estén conectadas con su equipo y utiliza el nombre de la impresora como nombre de impresora compartida. EasyNetwork también detecta impresoras compartidas por otros equipos de la red y le permite configurarlas y utilizarlas.

Si ha configurado un controlador de impresora para imprimir a través de un servidor de impresión en red (por ejemplo, un servidor de impresión USB inalámbrico), EasyNetwork considera que la impresora es una impresora local y la comparte en la red. También puede dejar de compartir una impresora en cualquier momento.

En este capítulo

Trabajar con impresoras compartidas.....180

Trabajar con impresoras compartidas

EasyNetwork detecta las impresoras compartidas por los equipos de la red. Si EasyNetwork detecta una impresora remota que no esté conectada a su equipo, el vínculo **Impresoras de red disponibles** de la ventana Archivos compartidos aparece al abrir EasyNetwork por primera vez. Entonces puede instalar impresoras disponibles o desinstalar impresoras que ya estén conectadas a su equipo. Asimismo, puede actualizar la lista de impresoras para asegurarse de estar visualizando la información actualizada.

Si aún no se ha incorporado a una red gestionada pero está conectada a ella, puede acceder a las impresoras compartidas desde el panel de control de impresoras de Windows.

Detener el uso compartido de una impresora

Cuando deja de compartir una impresora, los miembros ya no pueden usarla.

1. En el menú **Herramientas**, haga clic en **Impresoras**.
2. En el cuadro de diálogo Gestionar impresoras de red, haga clic en el nombre de la impresora que ya no desea compartir.
3. Haga clic en **No compartir**.

Instalar una impresora de red disponible

Si es miembro de una red gestionada, puede acceder a las impresoras que estén compartidas; sin embargo, debe instalar el controlador de la impresora utilizado por dicha impresora. Si el propietario de la impresora deja de compartirla, no podrá utilizarla.

1. En el menú **Herramientas**, haga clic en **Impresoras**.
2. En el cuadro de diálogo Impresoras de red disponibles, haga clic en un nombre de impresora.
3. Haga clic en **Instalar**.

Referencia

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

Glosario

8

802.11

Conjunto de estándares para transmitir datos a través de una red inalámbrica. 802.11 se conoce comúnmente como Wi-Fi.

802.11a

Extensión de 802.11 que transmite datos a una velocidad de hasta 54 Mbps en la banda de 5 GHz. Aunque la velocidad de transmisión es mayor que en el caso de 802.11b, la distancia de cobertura es mucho menor.

802.11b

Extensión de 802.11 que transmite datos a una velocidad de hasta 11 Mbps en la banda de 2.4 GHz. Aunque la velocidad de transmisión es menor que en el caso de 802.11a, la distancia de cobertura es mucho mayor.

802.1x

Un estándar para la autenticación de redes con cable e inalámbricas. 802.1x se utiliza normalmente con redes inalámbricas 802.11. Consulte también autenticación (página 183).

A

acceso directo

Archivo que contiene únicamente la ubicación de otro archivo en el equipo.

adaptador inalámbrico

Dispositivo que agrega la capacidad inalámbrica a un equipo o PDA. Se conecta mediante un puerto USB, una ranura de PC Card (CardBus), una ranura de tarjeta de memoria o internamente en el bus PCI.

análisis bajo demanda

Exploración planificada de los archivos, aplicaciones o dispositivos de red seleccionados para determinar si existe un virus o código no deseado. Se puede realizar inmediatamente, en el futuro de forma planificada o a intervalos regulares planificados. Compárese con análisis en tiempo real. Véase también vulnerabilidad.

Análisis en tiempo real

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

ancho de banda

Cantidad de datos que pueden transmitirse en un período de tiempo fijo.

archivar

Crear una copia de archivos importantes en un CD, un DVD, una unidad USB, un disco duro externo o una unidad de red. Compárese con realizar copia de seguridad (página 185).

archivo temporal

Un archivo, creado en la memoria o en un disco mediante el sistema operativo o algún otro programa, que se utiliza durante una sesión para desecharlo posteriormente.

ataque de denegación de servicio (DOS)

Tipo de ataque contra un equipo, servidor o red que ralentiza o detiene el tráfico de una red. Se produce cuando se desborda una red con tantas solicitudes adicionales que el tráfico habitual se ralentiza o se detiene por completo. Un ataque de denegación de servicio sobrecarga a su objetivo con solicitudes de conexión falsas, de forma que el objetivo ignora las solicitudes legítimas.

ataque de diccionario

Tipo de ataque de fuerza bruta que utiliza palabras habituales para intentar descubrir una contraseña.

ataque de fuerza bruta

Un método de piratería informática usado para descubrir contraseñas o claves de cifrado mediante la entrada de todas las combinaciones posibles de caracteres hasta que se rompe el cifrado.

ataque de intermediario

Método para interceptar y, posiblemente, modificar mensajes entre dos partes sin que ninguna de ellas sepa que su vínculo de comunicación ha sido interceptado.

autenticación

El proceso de verificar la identidad digital del remitente de una comunicación electrónica.

B

browser

Programa utilizado para ver páginas Web en Internet. Entre los navegadores Web más habituales figuran Microsoft Internet Explorer y Mozilla Firefox.

C

caché

Área de almacenamiento temporal del equipo para los datos a los que se tiene acceso reciente o frecuentemente. Por ejemplo, para aumentar la eficacia y velocidad de navegación en Web, su explorador puede recuperar una página Web desde la caché la siguiente vez que desee verla, en lugar de tener que hacerlo desde un servidor remoto.

caja fuerte de contraseñas

Área de almacenamiento segura de las contraseñas personales. Le permite almacenar sus contraseñas con la seguridad de que ningún otro usuario (incluso un administrador) pueda acceder a ellas.

cifrado

Método para codificar información de manera que las partes no autorizadas no puedan tener acceso a ella. Cuando los datos se codifican, el proceso emplea una "clave" y algoritmos matemáticos. La información cifrada no se puede descifrar sin la clave adecuada. Los virus utilizan a veces el cifrado para intentar burlar los sistemas de detección.

clave

Serie de letras y números utilizados por dos dispositivos con objeto de autenticar sus comunicaciones. Ambos dispositivos deben disponer de la clave. Véase también WEP (página 194), WPA (página 195), WPA2 (página 195), WPA2-PSK (página 195), WPA-PSK (página 195).

cliente

Programa que se ejecuta en un equipo personal o estación de trabajo y que depende de un servidor para realizar algunas operaciones. Por ejemplo, un cliente de correo electrónico es una aplicación que permite enviar y recibir mensajes de correo electrónico.

cliente de correo electrónico

Programa que se ejecuta en el equipo para enviar y recibir correo electrónico (por ejemplo, Microsoft Outlook).

código de autenticación de mensajes (MAC)

Código de seguridad utilizado para cifrar mensajes que se transmiten entre equipos. El mensaje se acepta si el equipo reconoce el código descifrado como válido.

compartir

Permitir a los destinatarios de mensajes de correo electrónico acceder a los archivos copiados seleccionados durante un período de tiempo limitado. Cuando se comparte un archivo, el usuario manda una copia del archivo a los destinatarios de correo electrónico especificados. Los destinatarios reciben un mensaje de correo electrónico procedente de Copia de seguridad y restauración en el que se indica que se han compartido archivos con ellos. Este mensaje contiene también un vínculo a los archivos compartidos.

complemento

Programa de software que añade funciones que mejora un producto de software mayor. Por ejemplo, los complementos permiten que un navegador Web acceda a archivos que están incorporados en documentos HTML y que tienen formatos que normalmente no podría reconocer, por ejemplo, archivos de animación, vídeo y audio, y le permite ejecutarlos.

compresión

Proceso que comprime archivos en un formato que minimiza el espacio necesario para su almacenamiento o transmisión.

contraseña

Código (por lo general formado por letras y números) utilizado para acceder al equipo, a un programa o a un sitio Web.

Control ActiveX

Componente de software que utilizan los programas o páginas Web para añadir funciones que aparecen como parte normal de esos programas o páginas. La mayor parte de los controles ActiveX son inofensivos; sin embargo, algunos pueden capturar información de su equipo.

cookie

Pequeño archivo de texto usado en muchos sitios Web para almacenar información sobre las páginas visitadas, almacenadas en el equipo de una persona que navega por la Web. Puede contener información de registro o de inicio de sesión, de carros de compra o preferencias de usuario. Las cookies las utilizan principalmente los sitios Web para identificar a los usuarios que se han registrado previamente o que han visitado el sitio; sin embargo, también pueden ser una fuente de información para los piratas informáticos.

correo electrónico

Correo electrónico: mensajes enviados y recibidos electrónicamente a través de una red informática. Véase también webmail (página 194).

cortafuegos

Sistema (hardware, software o ambos) diseñado para impedir el acceso no autorizado de entrada o salida de una red privada. Se utilizan con frecuencia para impedir que usuarios de Internet no autorizados accedan a redes privadas conectadas a Internet y, en particular, a una intranet. Todos los mensajes que entran o salen de la intranet pasan por el cortafuegos, que examina cada uno de ellos y bloquea aquellos que no cumplen los criterios de seguridad especificados.

crear copia de seguridad

Crear una copia de los archivos importantes, por lo general en un servidor en línea seguro. Compárese con archivar (página 182).

cuarentena

Aislamiento obligado de un archivo o carpeta sospechoso de contener virus, spam, contenido sospechoso o programas potencialmente no deseados, de manera que los archivos o carpetas no se pueden abrir ni ejecutar.

cuenta de correo electrónico estándar

Véase POP3 (página 189).

D

DAT

Los archivos de definición de detección, también llamados archivos de firma, contienen definiciones que identifican, detectan y reparan virus, troyanos, software espía, software publicitario y otros programas potencialmente no deseados (PUP).

desbordamiento del búfer

Condición que se produce en un sistema operativo o aplicación cuando procesos o programas sospechosos intentan almacenar en un búfer (área de almacenamiento temporal) más datos de los que realmente puede contener. Los desbordamientos de búfer dañan la memoria o sobrescriben los datos de los búferes adyacentes.

Dirección IP

Dirección de Protocolo de Internet (IP) Una dirección usada para identificar un equipo o dispositivo de una red TCP/IP. El formato de una dirección IP es una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar comprendido entre 0 y 255 (por ejemplo, 192.168.1.100).

Dirección MAC

dirección Media Access Control. Número de serie único asignado a un dispositivo físico (NIC, tarjeta de interfaz de red) que accede a la red.

disco duro externo

Disco duro que se encuentra fuera del equipo.

DNS

Sistema de nombres de dominio. Sistema de bases de datos que traduce un dirección IP, como 11.2.3.44, en un nombre de dominio, como www.mcafee.com.

dominio

Subred local o descriptor de sitios de Internet. En una red de área local (LAN), un dominio es una subred formada por equipos servidor y cliente controlados mediante una base de datos de seguridad. En Internet, un dominio es parte de la dirección Web. Por ejemplo, en www.mcafee.com, mcafee es el dominio.

E

enrutador o router

Dispositivo de red que reenvía paquetes de datos de una red a otra. Los enrutadores leen cada paquete que entra y deciden cómo reenviarlo según las direcciones de origen y destino, y las condiciones de tráfico. En ocasiones, se denomina a los enrutadores puntos de acceso (AP).

ESS

Extended Service Set. Grupo de dos o más redes que forman una subred única.

evento

En un programa o sistema de equipos, un incidente que puede detectarse mediante software de seguridad, de acuerdo con criterios predefinidos. Por lo general, un evento desencadena una acción, por ejemplo, enviar una notificación o agregar una entrada a un registro de eventos.

F

falsificación de IP

Como su propio nombre indica, se trata de la falsificación de la dirección IP de un paquete IP. Se utiliza en muchos tipos de ataques, incluidos los secuestros de sesiones. También se utiliza con frecuencia en la falsificación de encabezados de mensajes spam, para complicar su seguimiento.

fragmentos de archivos

Restos de un archivo dispersos por un disco. La fragmentación de archivos se produce a medida que se agregan o eliminan archivos y puede ralentizar el rendimiento del equipo.

G

grupo de clasificación de contenido

En Control parental, grupo de edad al que pertenece el usuario. El contenido se bloquea o bien está disponible según el grupo de clasificación de contenido al que pertenezca el usuario. Los grupos de clasificación de contenido incluyen: Niños de corta edad, niños, adolescentes, jóvenes y adultos.

guardián del sistema

Alertas de McAfee que detectan cambios no autorizados en el equipo y lo notifican al usuario cuando esto ocurre.

gusano

Virus que se propaga creando duplicados de sí mismo en las unidades, sistemas o redes. Un gusano de correo masivo es el que requiere la intervención del usuario para propagarse, por ejemplo, abrir un archivo adjunto o ejecutar un archivo descargado. La mayoría de los virus de correo electrónico actuales son gusanos. Un gusano que se autopropaga no necesita la intervención del usuario. Ejemplos de gusanos que se autopropagan son Blaster y Sasser.

H

hotspot o zona de cobertura inalámbrica

Zona geográfica cubierta por un punto de acceso (AP) Wi-Fi (802.11). Los usuarios que entran en un hotspot con un portátil inalámbrico se pueden conectar a Internet, siempre y cuando el hotspot emita señales (anuncie su presencia) y no sea preciso efectuar una autenticación. A menudo, los hotspots se encuentran con frecuencia en zonas con gran afluencia de público como aeropuertos.

I

intranet

Red informática privada, a menudo en el interior de una organización, a la que sólo pueden acceder los usuarios autorizados.

itinerancia

Moverse de una zona de cobertura de un punto de acceso (AP) a otra sin que se produzca una interrupción del servicio ni una pérdida de conectividad.

K

kit de raíz

Recopilación de herramientas (programa) que garantizan a un usuario, acceso de nivel de administrador a un equipo o una red de equipos. Los kits de raíz pueden estar formados por software espía y otros programas potencialmente no deseados que pueden poner en riesgo la seguridad o la privacidad de los datos de su equipo o de su información personal.

L

LAN

Red de área local. Red de equipos que se distribuye por una zona relativamente pequeña (por ejemplo, un único edificio). Los equipos de una LAN pueden comunicarse entre si y compartir recursos como impresoras y archivos.

Launchpad

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

lista blanca

Lista de direcciones de correo electrónico o sitios Web considerados seguros. Los sitios de una lista blanca son aquellos a los que los usuarios tienen acceso. Las direcciones de correo electrónico de una lista blanca son de fuentes de confianza cuyos mensajes se desean recibir. Compárese con lista negra (página 188).

lista de confianza

Una lista de elementos en los que tiene confianza y que no se detectan. Si por error indica que tiene confianza en un elemento (como un programa potencialmente no deseado o un cambio del Registro) o desea que se vuelva a detectar el elemento, deberá suprimirlo de la lista.

lista negra

En Anti-Spam, una lista de direcciones de correo electrónico de los que no desea recibir mensajes porque cree que los mensajes serán spam. En antiphishing, una lista de sitios Web considerados fraudulentos. Compárese con lista blanca (página 188).

M

mapa de la red

Representación gráfica de los equipos y componentes que forman una red doméstica.

MAPI

Interfaz de programación de aplicaciones de mensajería. Especificación de la interfaz de Microsoft que permite que diferentes programaciones de mensajería y grupos de trabajo (incluido el correo electrónico, el correo de voz y el fax) funcionen a través de un único cliente, como el cliente de Exchange.

marcadores

Software que redirige las conexiones de Internet a una parte distinta del ISP (proveedor de servicios de Internet) predeterminado del usuario para ejecutar cargos de conexión adicionales de un proveedor de servicios, distribuidor u otra tercera parte.

MSN

Microsoft Network. Grupo de servicios basados en Web ofrecidos por Microsoft Corporation, formados por un motor de búsqueda, correo electrónico, mensajería instantánea y un portal.

N

NIC

Tarjeta de interfaz de red. Acrónimo del inglés Network Interface Card. Tarjeta que se inserta en un portátil u otro dispositivo y que conecta el dispositivo a la red LAN.

nodo

Un solo equipo conectado a una red.

P

Papelera de reciclaje

Papelera simulada para almacenar los archivos y carpetas eliminados en Windows.

phishing

Método fraudulento para obtener información personal, como contraseñas, números de seguridad social y detalles de tarjetas de crédito, enviando correos electrónicos trucados que parecen proceder de fuentes de confianza, como bancos o empresas legítimas. Por lo general, los correos electrónicos de phishing solicitan a los destinatarios que hagan clic en un vínculo para verificar o actualizar los detalles de contacto o la información de la tarjeta de crédito.

POP3

Protocolo de oficina postal 3. Interfaz entre un programa cliente de correo electrónico y el servidor de correo electrónico. La mayoría de los usuarios domésticos tienen una cuenta de correo electrónico POP3, también conocida como cuenta de correo electrónico estándar.

popups

Pequeñas ventanas que aparecen en la parte superior de otras ventanas en la pantalla del equipo. Las ventanas emergentes se utilizan con frecuencia en los navegadores Web para mostrar anuncios.

PPPoE

Acrónimo del inglés Point-to-Point Protocol Over Ethernet, Protocolo punto a punto en Ethernet. Método para utilizar el protocolo de acceso telefónico PPP (protocolo punto a punto) con Ethernet como transporte.

Programa potencialmente no deseado (PUP)

Programa de software que no se quiere, a pesar de que los usuarios hayan dado su consentimiento para descargarlo. Puede modificar la configuración de seguridad o privacidad del equipo en el que se instala. Estos programas pueden incluir, aunque no necesariamente, software espía, software publicitario y marcadores, y pueden descargarse con un programa que el usuario desee.

protocolo

Conjunto de reglas que habilitan el intercambio de datos entre equipos y dispositivos. En una arquitectura de red por niveles (modelo de interconexión de sistemas abiertos), cada nivel tiene su protocolo concreto que especifica cómo transcurre la comunicación en ese nivel. El equipo o dispositivo debe ser compatible con el protocolo correcto para comunicarse con otros equipos. Véase también Interconexión abierta de sistemas

proxy

Un equipo (o el software que lo ejecuta) que actúa como barrera entre una red e Internet presentando únicamente una sola dirección de red a los sitios externos. Al representar a todos los equipos internos, el proxy protege las identidades de la red y, al mismo tiempo, proporciona acceso a Internet. Véase también servidor proxy (página 191).

publicar

Proceso de hacer pública la copia de seguridad de un archivo en Internet. Se puede acceder a los archivos publicados buscando en la biblioteca de Backup and Restore.

puerta de enlace integrada

Dispositivo que combina las funciones de un punto de acceso, un enrutador y un cortafuegos. Algunos dispositivos también pueden incluir funciones de mejora de la seguridad y enlace inalámbrico.

puerto

Ubicación de hardware por la que entran y salen datos de un dispositivo informático. Los equipos personales incluyen varios tipos de puertos: puertos internos para conectar los controladores de disco, el monitor y el teclado, y puertos externos para conectar un módem, una impresora, un ratón y otros periféricos.

punto de acceso (AP)

Un dispositivo de red (conocido comúnmente como enrutador inalámbrico) que se conecta a un hub Ethernet o conmutador para ampliar el rango físico del servicio para un usuario inalámbrico. Cuando los usuarios inalámbricos se encuentran en itinerancia con sus dispositivos móviles, la transmisión pasa de un punto de acceso (AP) al otro para mantener la conectividad.

punto de acceso no autorizado

Tal como su nombre indica, se trata de un punto de acceso no autorizado. Los puntos de acceso no autorizados se instalan en una red de empresa fiable, a fin de garantizar acceso a la red a partes no autorizadas. También se pueden crear para que un atacante pueda llevar a cabo un ataque de intermediario.

punto de restauración del sistema

Instantánea (imagen) del contenido de la memoria del equipo o de una base de datos. Windows crea periódicamente puntos de restauración y en el momento de eventos significativos del sistema, como cuando se instala un programa o un controlador. También se puede crear y nombrar puntos de restauración propios en cualquier momento.

R

RADIUS

Remote Access Dial-In User Service. Protocolo que permite autenticación para usuarios, normalmente en el contexto del acceso remoto. Originalmente definido para el uso con servidores de acceso telefónico remoto, se utiliza en la actualidad en varios entornos de autenticación, entre ellos, en la autenticación 802.1x de un secreto compartido de usuario WLAN. Véase también Cadena o clave (por lo general una contraseña) que se ha compartido entre las dos partes de la comunicación antes de iniciar ésta. Se utiliza para proteger las partes importantes de los mensajes RADIUS. Véase también RADIUS (página 190).

red

Conjunto de sistemas basados en IP (como enrutadores, conmutadores, servidores y cortafuegos) agrupados como una unidad lógica. Por ejemplo, un "Red de finanzas" puede incluir todos los servidores, enrutadores y sistemas que prestan servicio en un departamento de finanzas. Véase también red doméstica (página 191).

red doméstica

Dos o varios equipos que están conectados en un hogar de modo que puedan compartir archivos y acceder a Internet. Véase también LAN (página 187).

Registro

Base de datos que utiliza Windows para almacenar la configuración de cada usuario del equipo de hardware del sistema, los programas instalados y los ajustes de propiedades del sistema. La base de datos se descompone en claves para las que se establecen valores. Los programas no deseados pueden cambiar el valor de la clave del Registro o crear nuevas para ejecutar código malintencionado.

S

secreto compartido

Cadena o clave (por lo general una contraseña) que se ha compartido entre las dos partes de la comunicación antes de iniciar ésta. Se utiliza para proteger las partes importantes de los mensajes RADIUS. Véase también RADIUS (página 190).

secuencia de comandos

Lista de comandos que se pueden ejecutar automáticamente (es decir, sin interacción con el usuario). A diferencia de los programas, las secuencias de comandos se almacenan normalmente en forma de texto normal y se compilan cada vez que se ejecutan. Las macros y los archivos por lotes también se denominan secuencias de comandos o scripts.

servidor

Equipo o programa que acepta conexiones de otros equipos o programas y devuelve las respuestas apropiadas. Por ejemplo, el programa de correo electrónico se conecta a un servidor de correo electrónico cada vez que se envían o reciben mensajes.

servidor proxy

Un cortafuegos que gestiona el tráfico de Internet desde y hacia una red de área local (LAN). Un servidor proxy puede mejorar el rendimiento suministrando datos que se solicitan con frecuencia, como una página Web muy visitada, y puede filtrar y desechar solicitudes que el titular no considere convenientes, como el acceso no autorizado a archivos de propiedad.

sincronizar

Resolver inconsistencias entre los archivos copiados y los archivos almacenados en el equipo local. Los archivos se sincronizan cuando la versión del archivo que se encuentra en el repositorio de la copia de seguridad en línea es más reciente que la versión de otros equipos.

SMTP

Protocolo simple de transferencia de correo. Protocolo TCP/IP para el envío de mensajes de un equipo a otro en una red. Este protocolo se utiliza en Internet para enrutar los correos electrónicos.

SSID

Service Set Identifier. Un token (clave secreta) que identifica a una red Wi-Fi (802.11). El administrador de red configura el SSID que los usuarios que desean unirse a la red deben suministrar.

SSL

Secure Sockets Layer. Protocolo desarrollado por Netscape para transmitir documentos privados a través de Internet. SSL utiliza una clave pública para cifrar datos que se transfieren a través de la conexión SSL. Las direcciones URL que requieren una conexión SSL empiezan por HTTPS en lugar de por HTTP.

T

tarjeta adaptadora inalámbrica PCI

Interconexión de componentes periféricos. Tarjeta adaptadora inalámbrica que se conecta en una ranura de expansión PCI del equipo.

tarjeta adaptadora inalámbrica USB

Tarjeta adaptadora inalámbrica que se conecta en un puerto USB del equipo.

texto cifrado

Texto codificado. El texto cifrado es ilegible hasta que se convierte en texto normal (es decir, se descifra). Véase también cifrado (página 183).

texto normal

Texto sin cifrar. Véase también cifrado (página 183).

tipos de archivos observados

Tipos de archivos (por ejemplo, .doc, .xls, etc.) que Copia de seguridad y restauración copia o archiva en las ubicaciones de observación.

TKIP

Temporal Key Integrity Protocol Parte del estándar de cifrado 802.11i para LAN inalámbricas. TKIP es la siguiente generación de WEP, que se usa para asegurar LAN inalámbricas de 802.11. TPKI ofrece combinación de claves por paquete, comprobación de integridad de los mensajes y un mecanismo para volver a asignar claves, lo que subsana los errores de WEP.

Troyanos, caballos de Troya.

Programa que no replica pero causa daño o pon en peligro la seguridad del equipo. Por lo general, una personal le envía un troyano por correo electrónico, no se envía a sí mismo. También se puede descargar un troyano inadvertidamente de un sitio Web o a través de una red punto-a-punto.

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.

ubicaciones de observación

Carpetas del equipo supervisadas por Copia de seguridad y restauración.

unidad de red

Disco o unidad magnética que se conecta a un servidor de una red que comparten varios usuarios. Las unidades de red se denominan a veces "unidades remotas".

unidad inteligente

Véase unidad USB (página 193).

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.

URL

Siglas en inglés de Uniform Resource Locator (localizador universal de recursos). Formato estándar de las direcciones de Internet.

USB

Bus de serie universal. Un conector estándar de la mayoría de equipos modernos que sirve para conectar dispositivos varios, desde un teclado y un ratón hasta cámaras Web, escáneres e impresoras.

V

Virus

Programa informático que puede copiarse a sí mismo e infectar un equipo sin permiso o sin conocimiento del usuario.

VPN

Red privada virtual. Red de comunicaciones privada que está configurada a través de una red host como Internet. Los datos que viajan a través de una conexión VPN están cifrados y contienen fuertes funciones de seguridad.

W

wardriver

Persona que busca redes Wi-Fi (802.11) conduciendo por las ciudades con un equipo Wi-Fi y algún hardware o software especial.

Web bugs

Pequeños archivos de gráficos que pueden incorporarse a las páginas HTML y permitir que un origen no autorizado introduzca cookies en el equipo. Estos cookies pueden transmitir información a la fuente no autorizada. Los Web bugs también se denominan microespías, señales o balizas Web, pixel tags o GIF invisibles.

Webmail

Correo electrónico basado en web Servicio de correo electrónico al que se accede principalmente a través de un navegador de Web en lugar de a través de un cliente de correo electrónico como Microsoft Outlook. Véase también correo electrónico (página 185).

WEP

Wired Equivalent Privacy. Protocolo de cifrado y autenticación definido como parte del estándar Wi-Fi (802.11). Las versiones iniciales se basan en algoritmos de cifrado RC4 y presentan fallos importantes. WEP tiene como objetivo proporcionar seguridad mediante el cifrado de los datos a través de ondas de radio para protegerlos cuando se transmiten de un punto a otro. Sin embargo, se ha demostrado que el protocolo WEP no es tan seguro como se pensaba al principio.

Wi-Fi

Fidelidad inalámbrica. Término utilizado por la Wi-Fi Alliance al referirse a cualquier tipo de red 802.11.

Wi-Fi Alliance

Organización formada por los principales proveedores de hardware y software inalámbrico. Wi-Fi Alliance lucha para que todos los productos basados en 802.11 puedan certificarse como interoperables y para promocionar el uso del término Wi-Fi como nombre de marca global en todos los mercados de las LAN inalámbricas basadas en 802.11. La organización actúa como consorcio, laboratorio de pruebas y centro de intercambio de información para proveedores que deseen promocionar el crecimiento de la industria.

Wi-Fi Certified

Probado y aprobado por la Wi-Fi Alliance. Se considera que los productos Wi-Fi Certified son interoperables aunque puedan provenir de diferentes fabricantes. Un usuario que disponga de un producto Wi-Fi Certified puede utilizar cualquier marca de punto de acceso con otra marca de hardware cliente que también esté certificada.

WLAN

Red de área local inalámbrica. Red de área local que utiliza una conexión inalámbrica. Una WLAN utiliza ondas de radio de alta frecuencia en vez de cables para permitir a los equipos comunicarse entre si.

WPA

Wi-Fi Protected Access. Especificación estándar que aumenta de manera significativa el nivel de protección de los datos y el control de acceso de los sistemas LAN inalámbricos actuales y futuros. Diseñada para ejecutarse en hardware existente como ampliación de software, WPA procede del estándar 802.11i y es compatible con él. Cuando se instala adecuadamente, ofrece a los usuarios de una LAN inalámbrica amplias garantías de que sus datos permanecen protegidos y de que sólo los usuarios autorizados pueden acceder a la red.

WPA-PSK

Modo WPA especial para usuarios domésticos que no necesitan seguridad de tipo empresarial y que no tienen acceso a servidores de autenticación. En este modo, el usuario introduce la contraseña inicial para activar el modo Wi-Fi Protected Access con clave precompartida y debe cambiar regularmente la contraseña larga en cada equipo inalámbrico y punto de acceso. Véase también WPA2-PSK (página 195), TKIP (página 192).

WPA2

Actualización del estándar de seguridad WPA en el estándar 802.11i.

WPA2-PSK

Modo WPA especial similar a WPA-PSK basado en el estándar WPA2. Una característica común de WPA2-PSK es que los dispositivos normalmente admiten varios modos de cifrado (p. ej. AES, TKIP) simultáneamente, mientras que otros dispositivos sólo admiten por lo general un único modo de cifrado a la vez (es decir, todos los clientes tendrían que utilizar el mismo modo de cifrado).

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.

Licencia

Copyright

CAPÍTULO 36

Servicio al cliente y soporte técnico

SecurityCenter informa de los problemas de protección críticos y no críticos tan pronto como los detecta. Los problemas de protección críticos requieren una acción inmediata y ponen en peligro su estado de protección (el color cambia a rojo). Los problemas de protección no críticos no requieren acciones inmediatas y pueden poner en peligro o no su estado de protección (dependiendo del tipo de problema). Para conseguir un estado de protección de color verde, debe solucionar todos los problemas críticos y solucionar u omitir todos los problemas que no sean críticos. Si necesita ayuda para diagnosticar sus problemas de protección, puede ejecutar McAfee Virtual Technician. Si desea obtener más información sobre McAfee Virtual Technician, consulte la ayuda de McAfee Virtual Technician.

Si adquirió su software de seguridad a través de un distribuidor o proveedor distinto de McAfee, abra un navegador Web y visite www.mcafeeayuda.com. Una vez allí, en enlaces de proveedores, seleccione su proveedor para acceder a McAfee Virtual Technician.

Nota: para instalar y ejecutar McAfee Virtual Technician, debe iniciar sesión en su equipo como Administrador de Windows. En caso contrario, Virtual Technician no podrá resolver sus problemas. Si desea obtener información sobre cómo iniciar sesión como Administrador de Windows, consulte la Ayuda de Windows. En Windows Vista™, se le solicita al ejecutar Virtual Technician. Cuando esto ocurra, haga clic en **Aceptar**. Virtual Technician no funciona con Mozilla® Firefox.

En este capítulo

Utilización de McAfee Virtual Technician.....200

Utilización de McAfee Virtual Technician

Al igual que un representante personal de soporte técnico, Virtual Technician recopila información sobre sus programas de SecurityCenter para poder resolver los problemas de protección de su equipo. Al ejecutar Virtual Technician, realiza una comprobación para asegurarse de que sus programas de SecurityCenter funcionan correctamente. Si detecta algún problema, Virtual Technician se ofrece a solucionarlo por usted o le facilita información más detallada sobre dicho problema. Al finalizar, Virtual Technician muestra los resultados de su análisis y, en caso necesario, le permite buscar soporte técnico adicional de McAfee.

Para mantener la seguridad y la integridad de su equipo y archivos, Virtual Technician no recopila información personal e identificable.

Nota: para obtener más información sobre Virtual Technician, haga clic en el icono **Ayuda** de Virtual Technician.

Iniciar Virtual Technician

Virtual Technician recopila información sobre sus programas de SecurityCenter para poder resolver sus problemas de protección. Para proteger su privacidad, esta información no incluye información personal e identificable.

1. En **Tareas comunes**, haga clic en **McAfee Virtual Technician**.
2. Siga las instrucciones que aparecen en pantalla para descargar y ejecutar Virtual Technician.

Consulte las siguientes tablas para conocer los sitios de Soporte técnico y Descargas de McAfee de su región, incluidas las Guías de usuario.

Soporte técnico y Descargas

País o región	Soporte de McAfee	Descargas de McAfee
Alemania	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canadá (francés)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
Canadá (inglés)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp

China (chino simplificado)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Corea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Dinamarca	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Eslovaquia	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
España	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Estados Unidos	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp
Finlandia	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Francia	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Grecia	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
Hungría	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp
Italia	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japón	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
México	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Noruega	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polonia	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Reino Unido	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
República Checa	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Rusia	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Suecia	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Taiwán	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Turquía	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp

Guías de usuario de McAfee Total Protection

País o región	Guías de usuario de McAfee
Alemania	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canadá (francés)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Canadá (inglés)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
China (chino simplificado)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Eslovaquia	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
España	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Grecia	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Hungría	http://download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japón	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Países Bajos	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf

Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Reino Unido	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Rusia	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Suecia	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Taiwán	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Turquía	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf

Guías de usuario de McAfee Internet Security

País o región	Guías de usuario de McAfee
Alemania	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canadá (francés)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Canadá (inglés)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
China (chino simplificado)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Eslovaquia	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
España	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf

Grecia	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Hungría	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japón	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Países Bajos	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Reino Unido	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Rusia	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Suecia	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Taiwán	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Turquía	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf

Guías de usuario de McAfee VirusScan Plus

País o región	Guías de usuario de McAfee
Alemania	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canadá (francés)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Canadá (inglés)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf

China (chino simplificado)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Eslovaquia	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
España	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Grecia	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Hungría	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japón	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Países Bajos	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Reino Unido	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Rusia	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Suecia	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Taiwán	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf

Turquía	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf

Guías de usuario de McAfee VirusScan

País o región	Guías de usuario de McAfee
Alemania	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canadá (francés)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Canadá (inglés)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
China (chino simplificado)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Dinamarca	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Eslovaquia	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
España	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Estados Unidos	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Grecia	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Hungría	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
Italia	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japón	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
México	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Noruega	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf

Países Bajos	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Reino Unido	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
República Checa	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Rusia	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Suecia	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Taiwán	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Turquía	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf

Consulte la siguiente tabla para conocer los sitios del Centro de amenazas e Información sobre virus de McAfee en su país o región.

País o región	Centros de seguridad	Información de virus
Alemania	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canadá (francés)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canadá (inglés)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
China (chino simplificado)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Corea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Dinamarca	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Eslovaquia	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo

España	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Estados Unidos	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo
Finlandia	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Francia	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Grecia	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Hungría	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
Italia	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japón	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
México	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Noruega	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Países Bajos	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Polonia	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Reino Unido	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
República Checa	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Rusia	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Suecia	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Taiwán	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Turquía	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo

Consulte la siguiente tabla para conocer los sitios de HackerWatch en su país o región.

País o región	HackerWatch
Alemania	www.hackerwatch.org/?lang=de
Australia	www.hackerwatch.org

Brasil	www.hackerwatch.org/?lang=pt-br
Canadá (francés)	www.hackerwatch.org/?lang=fr-ca
Canadá (inglés)	www.hackerwatch.org
China (chino simplificado)	www.hackerwatch.org/?lang=zh-cn
Corea	www.hackerwatch.org/?lang=ko
Dinamarca	www.hackerwatch.org/?lang=da
Eslovaquia	www.hackerwatch.org/?lang=sk
España	www.hackerwatch.org/?lang=es
Estados Unidos	www.hackerwatch.org
Finlandia	www.hackerwatch.org/?lang=fi
Francia	www.hackerwatch.org/?lang=fr
Grecia	www.hackerwatch.org/?lang=el
Hungría	www.hackerwatch.org/?lang=hu
Italia	www.hackerwatch.org/?lang=it
Japón	www.hackerwatch.org/?lang=jp
México	www.hackerwatch.org/?lang=es-mx
Noruega	www.hackerwatch.org/?lang=no
Países Bajos	www.hackerwatch.org/?lang=nl
Polonia	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Reino Unido	www.hackerwatch.org
República Checa	www.hackerwatch.org/?lang=cs
Rusia	www.hackerwatch.org/?lang=ru
Suecia	www.hackerwatch.org/?lang=sv
Taiwán	www.hackerwatch.org/?lang=zh-tw
Turquía	www.hackerwatch.org/?lang=tr

Índice

8

802.11 182
802.11a 182
802.11b 182
802.1x 182

A

Abandonar una red gestionada 170, 171
Abrir EasyNetwork 167
Acceder al mapa de la red 150
Acceso a su cuenta de McAfee 11
acceso directo 182
Aceptar un archivo de otro equipo 177, 178
Acerca de las alertas 74
Acerca de las conexiones de equipo 102
Acerca de los tipos de Guardianes del sistema 58
Acerca de los tipos de listas de confianza 63, 64
Acerca de McAfee 197
Acerca del gráfico Análisis del tráfico .. 122
Activar productos 11
Active la protección Guardianes del sistema 57
Actualización de SecurityCenter 13
Actualizar el mapa de la red 150
adaptador inalámbrico 182
Agregar un equipo desde el registro Eventos entrantes 104
Agregar una conexión de equipo 103
Agregar una conexión de equipo no permitida 106
análisis bajo demanda 182
Análisis de su PC 32, 42
Análisis en tiempo real 182
Analizar el tráfico entrante y saliente .. 123
ancho de banda 182
archivar 183, 185
archivo temporal 183
ataque de denegación de servicio (DOS) 183
ataque de diccionario 183
ataque de fuerza bruta 183
ataque de intermediario 183
autenticación 182, 183

B

Bloquear el acceso a Internet a los programas 96
Bloquear el acceso a los programas 96
Bloquear el acceso a un nuevo programa 96
Bloquear el acceso a un puerto de servicio del sistema existente 111
Bloquear el acceso desde el registro Eventos recientes 97
Bloquear el cortafuegos al instante 88
Bloquear y restaurar el cortafuegos 88
browser 183
Buscar un archivo compartido 175

C

caché 183
caja fuerte de contraseñas 183
Cambiar el nombre de la red 151, 170
Características de QuickClean 128
Características de Shredder 142
cifrado 184, 192
clave 184
cliente 184
cliente de correo electrónico 184
código de autenticación de mensajes (MAC) 184
Cómo compartir archivos 174
compartir 184
Compartir impresoras 179
Compartir un archivo 174
Compartir y enviar archivos 173
complemento 184
compresión 184
Comprobación de su suscripción 12
Comprobar actualizaciones 13, 15
Conceder acceso pleno a un programa. 92
Conceder acceso pleno a un programa nuevo 93
Concesión de acceso a la red 169
Configuración de EasyNetwork 167
Configuración de las opciones de alerta 23
Configuración de las opciones de análisis personalizado 41, 51
Configuración de opciones de análisis en tiempo real 40, 48

Configuración de una red gestionada . 149
Configurar actualizaciones automáticas 14
Configurar la detección de intrusiones . 87
Configurar la protección del cortafuegos 79
Configurar la protección frente a virus 31, 47
Configurar los estados de protección del cortafuegos 87
Configurar opciones de análisis personalizado 52
Configurar opciones de UDP 86
Configurar puertos de servicio del sistema 110
Configurar Recomendaciones inteligentes para alertas 83
Configurar solicitudes de ping 86
Configurar un puerto de servicio del sistema 112
Configurar un registro de eventos 116
Configure las opciones de análisis en tiempo real 49
Configure las opciones de Guardianes del sistema 57
contraseña 184
Control ActiveX 185
cookie 185
Copiar un archivo compartido 175
Copyright 198
correo electrónico 185, 194
cortafuegos 185
crear copia de seguridad 183, 185
Criterios de búsqueda 175, 176
cuarentena 185
cuenta de correo electrónico estándar 185

D

DAT 185
Definir el nivel de seguridad como Automático 82
Definir el nivel de seguridad como Estándar 82
Definir el nivel de seguridad como Invisible 81
Dejar de confiar en los equipos de la red 154
Dejar de detectar nuevos Amigos 163
Desactivar las actualizaciones automáticas 15
Desbloquear el cortafuegos de manera instantánea 88
desbordamiento del búfer 185
Descripción de las categorías de protección 7, 9, 27
Descripción de los iconos de Network Manager 147
Descripción de los servicios de protección 10
Descripción del estado de protección . 7, 8, 9
Desfragmentación del equipo 133
Deshabilitar Recomendaciones inteligentes 84
Detener el uso compartido de un archivo 174
Detener el uso compartido de una impresora 180
Detener la protección contra virus en tiempo real 50
Detener la protección de Firewall 72
Detener la supervisión de redes 162
Dirección IP 186
Dirección MAC 186
disco duro externo 186
DNS 186
dominio 186

E

Editar una conexión de equipo 104
Editar una conexión de equipo no permitida 107
Eliminación de una tarea de QuickClean 137
Eliminación de una tarea del Desfragmentador de disco 139
Eliminar los permisos de acceso de los programas 97
Eliminar un permiso de programa 97
Eliminar un puerto de servicio del sistema 114
Eliminar una conexión de equipo 105
Eliminar una conexión de equipo no permitida 107
Emitir un sonido junto con las alertas .. 23
enrutador o router 186
Enviar un archivo a otro equipo 177
Envío de archivos a otros equipos 177
ESS 186
evento 186
Exploración del equipo 31

F

falsificación de IP 186
fragmentos de archivos 187
Funciones de EasyNetwork 166
Funciones de Network Manager 146

Funciones de SecurityCenter 6
Funciones de VirusScan..... 30

G

Gestión de estado y permisos 156
Gestión de listas de confianza..... 62
Gestión de suscripciones.....11, 18
Gestión remota de la red..... 155
Gestionar conexiones de equipo 101
Gestionar el estado de protección de un equipo 156
Gestionar las alertas informativas 77
Gestionar los niveles de seguridad del cortafuegos 80
Gestionar los servicios del sistema 109
Gestionar programas y permisos..... 91
Gestionar un dispositivo..... 157
grupo de clasificación de contenido ... 187
guardián del sistema 187
gusano 187

H

Habilitar Recomendaciones inteligentes 83
hotspot o zona de cobertura inalámbrica 187

I

Incorporación a la red..... 169
Incorporación a la red gestionada..... 152
Incorporarse a una red gestionada..... 153, 168, 170
Iniciar el cortafuegos..... 71
Iniciar el tutorial de HackerWatch..... 126
Iniciar la protección de Firewall 71
Iniciar Virtual Technician..... 200
Inicie la protección contra software espía 45
Inicie la protección de análisis de secuencias de comandos..... 44
Inicie la protección de correo electrónico 45
Inicie la protección de mensajería instantánea..... 46
Instalar el software de seguridad McAfee en equipos remotos 159
Instalar una impresora de red disponible 180
Interrumpir la gestión del estado de protección de un equipo 156
intranet 187
Introducción 3
Invitar a un equipo a que se incorpore a la red gestionada..... 153
itinerancia 187

K

kit de raíz 187

L

LAN 188, 191
Launchpad 188
Licencia 197
Limpiando el equipo..... 129
Limpieza del equipo..... 132
lista blanca 188
lista de confianza..... 188
lista negra 188

M

mapa de la red 188
MAPI 188
marcadores 188
Marcar como Amigo..... 163
Marcar como Intruso 163
McAfee EasyNetwork 165
McAfee Network Manager..... 145
McAfee Personal Firewall 67
McAfee QuickClean..... 127
McAfee SecurityCenter 5
McAfee Shredder 141
McAfee VirusScan..... 29
Modificación de una tarea de QuickClean 136
Modificación de una tarea del Desfragmentador de disco..... 138
Modificar las propiedades de visualización de un dispositivo 157
Modificar los permisos de un equipo gestionado 157
Modificar un puerto de servicio del sistema 113
Mostrar las alertas mientras se juega 77
Mostrar Recomendaciones inteligentes 84
Mostrar u ocultar problemas omitidos . 20
Mostrar u ocultar un elemento en el mapa de la red..... 151
Mostrar y ocultar alertas informativas .. 22
MSN 188
Muestre u oculte alertas informativas... 22
Muestre u oculte alertas informativas al jugar..... 23

N

NIC..... 189
nodo..... 189

O

Obtener información sobre el programa desde el registro Eventos salientes..... 99
Obtener información sobre los programas 98
Obtener información sobre un programa 98
Obtener más información sobre la seguridad en Internet 125
Obtenga información de red de los equipos..... 120
Obtenga información de registro de los equipos..... 119
Ocultar alertas de nuevos virus..... 24
Ocultar alertas informativas..... 78
Ocultar la pantalla de bienvenida al iniciar 24
Ocultar mensajes de seguridad..... 25
Omitir problemas de protección 19
Omitir un problema de protección 19
Optimizar la seguridad del cortafuegos 85

P

Papelera de reciclaje 189
Permiso de acceso a Internet para los programas..... 92
Permiso para programas de sólo acceso saliente..... 94
Permitir a un programa sólo acceso saliente..... 94
Permitir acceso pleno desde el registro Eventos recientes 93
Permitir acceso pleno desde el registro Eventos salientes..... 94
Permitir el acceso a un puerto de servicio del sistema existente..... 111
Permitir sólo acceso saliente desde el registro Eventos recientes 95
Permitir sólo acceso saliente desde el registro Eventos salientes..... 95
Personal Firewall incluye..... 68
phishing..... 189
Planificación de una tarea..... 135
Planificación de una tarea del Desfragmentador de disco..... 138
POP3 ..... 185, 189
popups..... 189
PPPoE 189
Programa potencialmente no deseado (PUP) 189
Programación de análisis 42, 54
Programación de una tarea de QuickClean 135
Prohibir conexiones de equipo 106
Prohibir un equipo desde el registro Eventos de detección de intrusiones 108
Prohibir un equipo desde el registro Eventos entrantes 108
Proteger su equipo durante el inicio 85
protocolo 189
proxy 190
publicar 190
puerta de enlace integrada..... 190
puerto 190
punto de acceso (AP)..... 190
punto de acceso no autorizado..... 190
punto de restauración del sistema 190
Purga de archivos, carpetas y discos ... 142
Purgar archivos y carpetas..... 142
Purgar un disco completo 143

R

RADIUS..... 191
Rastrear el tráfico de Internet 119
Rastrear un equipo de red geográficamente 119
Rastrear un equipo desde el registro Eventos de detección de intrusiones 121
Rastrear un equipo desde el registro Eventos entrantes 120
Rastrear una dirección IP supervisada 121
Recibir una notificación cuando se envíe el archivo..... 178
red 191
red doméstica 191
Referencia 181
Registro..... 191
Registro de eventos 116
Registro, supervisión y análisis 115
Renovar la suscripción..... 12
Restaurar la configuración del cortafuegos 89

S

secreto compartido 191
secuencia de comandos..... 191
Servicio al cliente y soporte técnico 199
servidor..... 191
servidor proxy 190, 192
sincronizar 192
SMTP..... 192
Solución de problemas de protección8, 18
Solución de vulnerabilidades de seguridad 158
Solucionar problemas de protección automáticamente..... 18

Solucionar problemas de protección manualmente 19
Solucionar u omitir problemas de protección.....8, 17
Solucionar vulnerabilidades de seguridad 158
SSID 192
SSL..... 192
Supervisar el ancho de banda de un programa 123
Supervisar el tráfico de Internet..... 122
Supervisar la actividad de un programa 124
Supervisión de sus redes..... 161

T

tarjeta adaptadora inalámbrica PCI 192
tarjeta adaptadora inalámbrica USB... 192
texto cifrado 192
texto normal..... 192
Tipos de análisis 34, 40
tipos de archivos observados 192
TKIP 193, 195
Trabajar con alertas.....14, 21, 73
Trabajar con el mapa de la red..... 150
Trabajar con estadísticas 118
Trabajar con impresoras compartidas 180
Trabajar con los resultados de análisis . 37
Trabaje con archivos en cuarentena 38, 39
Trabaje con programas potencialmente no deseados 38
Trabaje con programas y cookies en cuarentena..... 39
Trabajo con virus y troyanos..... 38
Troyanos, caballos de Troya..... 193

U

U3..... 193
ubicaciones de observación..... 193
unidad de red..... 193
unidad inteligente 193
Unidad USB 193
URL 193
USB 193
Uso de listas de confianza 62
Uso de SecurityCenter 7
Utilización de las opciones de Guardianes del sistema 55
Utilización de McAfee Virtual Technician 200
Utilización de protección adicional 43

V

Ver detalles de un elemento..... 151
Ver eventos de detección de intrusiones 117
Ver eventos entrantes 117
Ver eventos recientes 27, 116
Ver eventos salientes..... 93, 117
Ver resultados del análisis 35
Virus..... 193
Visualización de eventos 18, 27
Visualizar la actividad global de los puertos de Internet 118
Visualizar las estadísticas globales de los eventos de seguridad 118
Visualizar todos los eventos 27
Volver a activar las notificaciones de supervisión de redes 162
VPN 194

W

wardriver 194
Web bugs..... 194
Webmail 185, 194
WEP..... 184, 194
Wi-Fi 194
Wi-Fi Alliance..... 194
Wi-Fi Certified 194
WLAN..... 195
WPA..... 184, 195
WPA2..... 184, 195
WPA2-PSK 184, 195
WPA-PSK 184, 195