Configuración de una exploración

Seleccione una de las siguientes opciones:

{button ,JI(`scan32.HLP',`Configuring_a_scan_Classic')} Exploración clásica

{button ,JI(`scan32.HLP',`Configuring_a_scan_Advanced')} Exploración avanzada

Configuración de una exploración: Clásico

1 Inicie VirusScan.
2 Escoja Clásico en el menú Herramientas. Si no encuentra en dicho menú, quiere decir que este modo ya está activado.
3 Elija las ubicaciones y tipos de archivo que desee explorar en la página Parámetros.
4 Seleccione el modo en que VirusScan responderá a una infección de virus en la página Acciones.
5 Escoja las opciones de informe en la página Informes.
6 Para ejecutar la exploración en este momento, haga clic en **Explorar ahora**. Para guardar esta configuración como un archivo de configuración de VirusScan, seleccione Guardar configuración en el menú Archivo.

{button ,AL(`CFG',0,`',`')} Temas relacionados

Configuración de una exploración: Avanzado

1 Inicie VirusScan.
2 Seleccione Avanzado en el menú Herramientas. Si no se encuentra en dicho menú, quiere decir que este modo ya está activado.
3 Elija las ubicaciones y tipos de archivo que desee explorar en la página Detección.
4 Seleccione el modo en que VirusScan responderá a una infección de virus en la página Acciones.
5 Seleccione el modo en que VirusScan le alerta a usted o a los administradores de red de la actividad de virus en la página Alerta.
6 Escoja las opciones de informe en la página Informes.
7 Elija los archivos que desee excluir de la exploración en la página Exclusiones.
8 Para ejecutar la exploración en este momento, haga clic en **Explorar ahora**. Para guardar esta configuración como un archivo de configuración de VirusScan, seleccione Guardar configuración en el menú Archivo.

Sugerencia

- Para restituir todas las configuraciones a los valores predeterminados, haga clic en **Nueva exploración**.

{button ,AL(`CFG',0,`',`')} Temas relacionados

Página Acciones

VirusScan puede alternar entre los modos Clásico y Avanzado. Para cambiar de uno a otro, limítese a seleccionar Clásico o Avanzado en el menú Herramientas.

Seleccione una de las siguientes opciones:

{button ,JI(`scan32.HLP>(w95sec)',`Actions_page_Classic')} Página Acciones: Clásico

{button ,JI(`scan32.HLP>(w95sec)',`Actions_page_Advanced')} Página Acciones: Avanzado

Página Informes

VirusScan puede alternar entre los modos Clásico y Avanzado. Para cambiar de uno a otro, limítese a seleccionar Clásico o Avanzado en el menú Herramientas.

Seleccione una de las siguientes opciones:

{button ,JI(`scan32.HLP>(w95sec)',`Reports_page_Classic')} Página Informes: Clásico

{button ,JI(`scan32.HLP>(w95sec)',`Reports_page_Advanced')} Página Informes: Avanzado

Página Parámetros: Clásico

La página Parámetros se utiliza para configurar las ubicaciones y tipos de archivo que se van a explorar. Para configurar la página Parámetros, siga el procedimiento que se describe a continuación:

1 Inicie VirusScan. Se abre la ventana principal de VirusScan mostrando la página Parámetros. Si no aparece la página Parámetros, seleccione Clásico en el menú Herramientas.
2 Ingrese la unidad o carpeta que desee explorar o haga clic en **Examinar** para localizarla.
3 Para explorar todas las subcarpetas, seleccione la casilla Incluir subcarpetas.
4 Para explorar todos los tipos de virus, seleccione la casilla Todos los archivos. Si desea explorar exclusivamente los archivos que sean más susceptibles a los virus, seleccione la casilla Sólo archivos de programa.
5 Para explorar archivos comprimidos, seleccione la casilla Archivos comprimidos.
6 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAGB',0,`',`')} Temas relacionados

Página Acciones: Clásico

La página Acciones se utiliza para configurar el modo en que VirusScan responde a la existencia de archivos infectados. Para configurar la página Acciones, siga el procedimiento que se describe a continuación:

1 Inicie VirusScan. Se abre la ventana principal de VirusScan mostrando la página Parámetros. Si no aparece la página Parámetros, seleccione Clásico en el menú Herramientas.

2 Haga clic en la ficha Acciones.

3 A continuación, seleccione el método de respuesta de VirusScan ante la existencia de archivos infectados.
Consultar antes de actuar
Trasladar los archivos infectados automáticamente
Limpiar los archivos infectados automáticamente
Borrar los archivos infectados automáticamente
Continuar la exploración

4 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAGB',0,`',`')} Temas relacionados

Página Informes: Clásico

La página Informes se utiliza para configurar cómo VirusScan notifica la actividad de virus. Las opciones de informe incluyen mantener un archivo de registro, emitir señales audibles y mostrar mensajes. Para configurar la página Informes, siga el procedimiento que se describe a continuación:

1 Inicie VirusScan. Se abre la ventana principal de VirusScan mostrando la página Parámetros. Si no aparece la página Parámetros, seleccione Clásico en el menú Herramientas.
2 Haga clic en la ficha Informes.
3 Para que VirusScan muestre un mensaje cada vez que encuentre un virus, seleccione la casilla Mostrar mensaje y escriba un mensaje.
4 Si desea que VirusScan emita una señal sonora, seleccione la casilla Señal audible.
5 Para que VirusScan mantenga un archivo de registro, seleccione la casilla Registrar en el archivo. Ingrese una ruta y un nombre para el archivo de registro (predeterminada: C:\Archivos de programa\McAfee\VirusScan\VSCLOG.TXT).
6 A fin de limitar el tamaño del archivo de registro, seleccione la casilla Limitar el tamaño del archivo de registro a e ingrese el tamaño máximo de dicho archivo.
7 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAGB',0,`',`')} Temas relacionados

Página Detección: Avanzado

La página Detección se utiliza para configurar las ubicaciones y tipos de archivos que se van a explorar. Para configurar la página Detección, siga el procedimiento que se describe a continuación:

1 Inicie VirusScan. Se abre la ventana principal de VirusScan mostrando la página Detección. Si no aparece la página Detección, seleccione Avanzado en el menú Herramientas.

2 Para agregar un elemento a la exploración, haga clic en **Agregar**. Se abre el cuadro de diálogo Agregar elemento de exploración.

3 Para explorar todas las unidades adjuntadas a su PC, haga clic en el botón de opción Seleccionar elemento a explorar y seleccione Mi PC.
Para explorar todos los medios extraíbles, discos flexibles incluidos, haga clic en el botón de opción Seleccionar elemento a explorar y escoja Todos los medios extraíbles.
Para explorar todas las unidades de disco duro adjuntadas a su PC, haga clic en el botón de opción Seleccionar elemento a explorar y elija Todos los discos duros.
Para explorar todas las unidades de red instaladas, haga clic en el botón de opción Seleccionar elemento a explorar y seleccione Todas las unidades de red.
Para explorar una unidad o carpeta individual, haga clic en el botón de opción Seleccionar unidad o carpeta a explorar e ingrese la ruta del elemento que vaya a explorar o haga clic en **Examinar** para localizarla.
Haga clic en **Aceptar**.

4 Repita los pasos 3 y 4 con cada elemento que desee explorar.

5 Para explorar todas las subcarpetas, seleccione la casilla Incluir subcarpetas.

6 Para explorar todos los tipos de virus, seleccione la casilla Todos los archivos. Si desea explorar exclusivamente los archivos que sean más susceptibles a los virus, seleccione la casilla Sólo archivos de programa.

7 Para explorar archivos comprimidos, seleccione la casilla Archivos comprimidos.

8 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

Sugerencias

Para editar un elemento de exploración, selecciónelo y haga clic en **Editar**.

Para borrar un elemento de exploración, selecciónelo y haga clic en **Borrar**.

{button ,AL(`SPAG',0,`',`')} Temas relacionados

Página Acciones: Avanzado

La página Acciones se utiliza para configurar el modo en que VirusScan responde a la existencia de archivos infectados. Para configurarla, siga el procedimiento que se describe a continuación:

1 Inicie VirusScan. Se abre la ventana principal de VirusScan mostrando la página Detección. Si no aparece la página Detección, seleccione Avanzado en el menú Herramientas.

2 Haga clic en la ficha Acciones.

3 A continuación, seleccione el método de respuesta de VirusScan ante la existencia de archivos infectados.
Consultar antes de actuar
Trasladar los archivos infectados automáticamente
Limpiar los archivos infectados automáticamente
Borrar los archivos infectados automáticamente
Continuar la exploración

4 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAG',0,`',`')} Temas relacionados

Página Alerta: Avanzado

Para seleccionar opciones de alerta, siga el procedimiento que se describe a continuación.

1 Inicie VirusScan. Se abre la ventana principal de VirusScan mostrando la página Detección. Si no aparece la página Detección, seleccione Avanzado en el menú Herramientas.
2 Escoja la ficha Alerta.
3 Para configurar VShield de modo que envíe notificaciones a los servidores que ejecuten NetShield, seleccione la casilla Enviar alerta de red. Ingrese la ruta de la carpeta Alerta centralizada del servidor o haga clic en **Examinar** para localizarla.
4 Para configurar VirusScan para que emita una señal sonora, seleccione la casilla Emitir señal audible.
5 Si desea configurar VirusScan para que envíe un mensaje, seleccione la casilla Mostrar mensaje personalizado y escriba un mensaje personalizado (máximo de 256 caracteres).
6 Para continuar configurando esta exploración, escoja otra página de propiedades. Para comenzar la exploración, haga clic en **Explorar ahora**. Para salir sin realizarla, seleccione Cerrar en el menú Archivo.

{button ,AL(`SPAG',0,`',`')} Temas relacionados

Página Informes: Avanzado

La página Informes se utiliza para configurar cómo VirusScan notifica la actividad de virus. Las opciones de informe incluyen mantener un archivo de registro, emitir señales audibles y mostrar mensajes. Para configurarla, siga el procedimiento que se describe a continuación:

1 Inicie VirusScan. Se abre la ventana principal de VirusScan mostrando la página Detección. Si no aparece la página Detección, seleccione Avanzado en el menú Herramientas.

2 Haga clic en la ficha Informes.

3 Para que VirusScan muestre un mensaje personalizado cada vez que encuentre un virus, seleccione la casilla Mostrar mensaje y escriba un mensaje.

4 Si desea que VirusScan emita una señal sonora, seleccione la casilla Señal audible.

5 Para que VirusScan mantenga un archivo de registro, seleccione la casilla Registrar en el archivo. Ingrese una ruta y un nombre para el archivo de registro (predeterminada: C:\Archivos de programa\McAfee\VirusScan\VSCLOG.TXT).

6 A fin de limitar el tamaño del archivo de registro, seleccione la casilla Limitar el tamaño del archivo de registro a e ingrese el tamaño máximo de dicho archivo.

7 Escoja los elementos que desee que VShield registre en la sección Elementos a registrar.
Detección de virus
Limpieza de virus
Eliminación de archivos infectados
Traslado de archivos infectados
Configuración de sesión
Resumen de sesión
Fecha y hora
Nombre de usuario

8 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAG',0,`',`')} Temas relacionados

Página Exclusiones: Avanzado

Para excluir archivos, directorios o unidades de la exploración, siga el procedimiento que se describe a continuación:

1 Inicie VirusScan. Se abre la ventana principal de VirusScan mostrando la página Detección. Si no aparece la página Detección, seleccione Avanzado en el menú Herramientas.
2 Escoja la ficha Exclusiones.
3 Para agregar un elemento y excluirlo de la exploración, haga clic en Agregar. Aparece el cuadro de diálogo Excluir elemento.

   Ingrese la ruta completa de un archivo, unidad o carpeta, o bien haga clic en **Examinar** para localizarla.

   Para excluir las subcarpetas de la exploración, seleccione la casilla Incluir subcarpetas.

   Para excluir el elemento de la exploración de archivos, seleccione la casilla Exploración de archivos. Para excluirlo de la exploración del sector de arranque, seleccione la casilla Exploración del sector de arranque.

   Haga clic en **Aceptar**.
4 Repita el paso 3 con cada elemento que desee excluir.
5 Para editar un elemento de exploración, selecciónelo y haga clic en **Editar**.
6 Para eliminar un elemento de exploración, selecciónelo y haga clic en **Eliminar**.
7 Para continuar configurando esta exploración, escoja otra página de propiedades. Para comenzar la exploración, haga clic en Explorar ahora. Para salir sin realizarla, seleccione Cerrar en el menú Archivo.

{button ,AL(`SPAG',0,`',`')} Temas relacionados

Planificación de una tarea

Para planificar una tarea, utilice la Consola VirusScan.

1 Inicie VirusScan. Se abre la ventana principal de VirusScan.
2 Escoja Avanzado en el menú Herramientas. Si no ve Avanzado en dicho menú, quiere decir que ya se encuentra en el modo Avanzado.
3 Seleccione AVConsole en el menú Herramientas. Se abre la Consola VirusScan.

Sugerencias

- Para iniciar la Consola VirusScan desde el escritorio, haga clic en Inicio, Programas, McAfee VirusScan y haga clic en la Consola VirusScan.
- Para abrirla la Consola VirusScan ahora, haga clic aquí  .
- Para acceder a la ayuda de la Consola VirusScan, escoja Temas de Ayuda en el menú Ayuda.
- Para abrir el archivo de ayuda de la Consola VirusScan ahora, haga clic aquí  .

Creación de un archivo de configuración de VirusScan (.VSC)

Seleccione una de las siguientes opciones:

{button ,JI(`scan32.HLP',`Creating_a_VirusScan_settings_file_.VSC_Classic')} Exploración clásica

{button ,JI(`scan32.HLP',`Creating_a_VirusScan_settings_file_.VSC_Advanced')} Exploración avanzada

Creación de un archivo de configuración de VirusScan (.VSC): Clásico

1 Inicie VirusScan.
2 Escoja Clásico en el menú Herramientas. Si no ve Clásico en dicho menú, quiere decir que se encuentra en el modo Clásico.
3 Elija las ubicaciones y tipos de archivo que desee explorar en la página Parámetros.
4 Seleccione el modo en que VirusScan responderá a una infección de virus en la página Acciones.
5 Escoja las opciones de informe en la página Informes.
6 Seleccione Guardar configuración en el menú Archivo. Aparece el cuadro de diálogo Guardar configuración de exploración como.
7 Escoja una ruta y un nombre de archivo para la nueva configuración. Haga clic en **Guardar**.

Sugerencia

- Para configurar este archivo de modo que se ejecute automáticamente cada vez que lo abra, consulte Configuración de un archivo VSC para que se inicie al abrirlo.

Creación de un archivo de configuración de VirusScan (.VSC): Avanzado

1 Inicie VirusScan.
2 Escoja Avanzado en el menú Herramientas. Si no ve Avanzado en dicho menú, quiere decir que ya se encuentra en el modo Avanzado.
3 Elija las ubicaciones y tipos de archivo que desee explorar en la página Detección.
4 Seleccione el modo en que VirusScan responderá a una infección de virus en la página Acciones.
5 Seleccione el modo en que VirusScan le alerta a usted o a los administradores de red de la actividad de virus en la página Alerta.
6 Escoja las opciones de informe en la página Informes.
7 Elija los archivos que desee excluir de la exploración en la página Exclusiones.
8 Seleccione Guardar configuración en el menú Archivo. Aparece el cuadro de diálogo Guardar configuración de exploración como.
9 Escoja una ruta y un nombre de archivo para la nueva configuración. Haga clic en **Guardar**.

Sugerencia

- Para configurar este archivo de modo que se ejecute automáticamente cada vez que lo abra, consulte Configuración de un archivo VSC para que se inicie al abrirlo.

Exploración desde la ventana principal

1 Inicie VirusScan.
2 Configure la exploración.
3 Haga clic en **Explorar ahora**. VirusScan inicia la exploración en busca de virus.

{button ,AL(`SCAN',0,`',`')} Temas relacionados

Exploración utilizando un archivo de configuración de VirusScan (.VSC)

1 Localice y haga doble clic en un archivo de configuración de VirusScan guardado.
2 Haga clic en **Explorar ahora**. VirusScan inicia la exploración en busca de virus utilizando la configuración guardada.

{button ,AL(`SCAN',0,`',`')} Temas relacionados

Exploración de un archivo, carpeta o unidad en el Explorador de Windows o Mi PC

Seleccione una de las siguientes opciones:

{button ,JI(`scan32.HLP',`Scanning_a_file_folder_or_drive_in_Windows_Explorer')} Explorador de Windows

{button ,JI(`scan32.HLP',`Scanning_a_file_folder_or_drive_in_My_Computer')} Mi PC

{button ,AL(`SCAN',0,`',`')} Temas relacionados

Exploración de un archivo, carpeta o unidad en el Explorador de Windows

1 Abra el Explorador de Windows. Para ello, haga clic aquí  .

2 Localice una unidad, carpeta o archivo que desee explorar.

3 Haga clic con el botón derecho del mouse en la unidad, carpeta o archivo y escoja Explorar en busca de virus del menú de método abreviado. VirusScan comienza con el elemento seleccionado para ser explorado.

4 Haga clic en **Explorar ahora**. VirusScan empieza a explorar los archivos.

Nota

- Esta función sólo admite unidades, carpetas, archivos ejecutables (.EXE), archivos COM (.COM), archivos de Word (.DO?), de Excel (.XL?) y de PKZIP (.ZIP).

Exploración de un archivo, carpeta o unidad en Mi PC

1 Abra Mi PC.
2 Localice una unidad, carpeta o archivo que desee explorar.
3 Haga clic con el botón derecho del mouse en la unidad, carpeta o archivo y escoja Explorar en busca de virus del menú de método abreviado. VirusScan comienza con el elemento seleccionado para ser explorado.
4 Haga clic en **Explorar ahora**. VirusScan empieza a explorar los archivos.

Nota

- Esta función sólo admite unidades, carpetas, archivos ejecutables (.EXE), archivos COM (.COM), archivos de Word (.DO?), de Excel (.XL?) y de PKZIP (.ZIP).

Exploración automática al iniciarse el sistema

1 Cree un archivo de configuración de VirusScan (.VSC) y guárdelo en C:\Windows\Menú Inicio\Programas\Inicio.

2 Abra el Explorador de Windows o Mi PC y diríjase a C:\Windows\Menú Inicio\Programas\Inicio, o bien haga clic aquí  .

3 Haga clic con el botón derecho del mouse en el archivo de configuración de VirusScan y escoja Propiedades del menú de método abreviado. Aparece la hoja de propiedades del archivo VSC.

4 Haga clic en la ficha Opciones. Aparece la página de propiedades Opciones.

5 Seleccione la casilla Iniciar automáticamente.

6 Haga clic en **Aceptar**.

Se ejecutará VirusScan automáticamente utilizando los parámetros especificados en el archivo VSC especificado cada vez que se inicie el sistema.

Nota

- Todos los archivos que se encuentren la carpeta Inicio se ejecutan automáticamente cuando se inicia el sistema.

{button ,AL(`SCAN',0,`',`')} Temas relacionados

No se encuentra la carpeta Inicio

Si Windows se encuentra en la carpeta Win95, haga clic aquí  . De lo contrario, diríjase a la carpeta \Menú Inicio\Programas\Inicio ubicada en la carpeta Windows.

Configuración de un archivo VSC para que se inicie al abrirlo

1 Vaya a la carpeta donde se encuentra el archivo de configuración de VirusScan (.VSC) mediante el Explorador de Windows o Mi PC.

2 Haga clic con el botón derecho del mouse en el archivo de configuración de VirusScan y seleccione Propiedades del menú de método abreviado. Aparece la hoja de propiedades del archivo VSC.

3 Haga clic en la ficha Opciones. Aparece la página de propiedades Opciones.

4 Seleccione la casilla Iniciar automáticamente.

5 Haga clic en **Aceptar**.

Se ejecutará VirusScan automáticamente utilizando los parámetros especificados en el archivo VSC cada vez que éste se abra.

Protección mediante contraseña con VirusScan

Para optimizar la seguridad y la protección antivirus, VirusScan ofrece la protección mediante contraseñas en páginas, es decir, puede escoger las páginas de propiedades de VirusScan individuales que desee proteger. Esto le permite evitar la realización de cambios accidentales a la configuración de VirusScan que pudieran comprometer su sistema de seguridad. Seleccione una de las siguientes opciones:

{button ,JI(`scan32.HLP>(w95sec)',`Enabling_Password_Protection')} Activación de la protección mediante contraseña

{button ,JI(`scan32.HLP>(w95sec)',`Editing_Password_Protection')} Edición de la protección mediante contraseña

{button ,JI(`scan32.HLP>(w95sec)',`Disabling_Password_Protection')} Desactivación de la protección mediante contraseña

Activación de la protección mediante contraseña

1 Inicie VirusScan.
2 Escoja Proteger mediante contraseña en el menú Herramientas. Aparece el cuadro de diálogo Protección mediante contraseña.
3 Seleccione las páginas de propiedades que desee proteger. Las páginas protegidas van precedidas de un símbolo  y las que no, de un símbolo

 .

4 Haga clic en **Contraseña**. Aparece el cuadro de diálogo Especificar contraseña.
5 Escriba una contraseña, confírmela y haga clic en **Aceptar**. Volverá al cuadro de diálogo Protección mediante contraseña.
6 Haga clic en **Aceptar**. Cuando alguien intente acceder a una de las páginas protegidas, se le solicitará la contraseña.

Notas

- Para acceder a las páginas de propiedades de VirusScan, escoja ##Unlock Password en el menú Herramientas y escriba la contraseña.
- Las contraseñas no distinguen entre mayúsculas y minúsculas. Por ejemplo, si VirusScan es la contraseña, tanto “VirusScan” como “virusscan” son aceptables.
- La contraseña se solicita una vez por sesión.

{button ,AL(`PWD',0,`',`')} Temas relacionados

Edición de la protección mediante contraseña

1 Inicie VirusScan.

2 Escoja Proteger mediante contraseña en el menú Herramientas. Aparece el cuadro de diálogo ##Password.

3 Escriba la contraseña y haga clic en **Aceptar**. Aparece el cuadro de diálogo Protección mediante contraseña.

4 Seleccione las páginas de propiedades que desee proteger. Las páginas protegidas van precedidas de un símbolo  y las que no, de un símbolo

 .

5 Para cambiar la contraseña, haga clic en **Contraseña**. Aparece el cuadro de diálogo Especificar contraseña. Escriba una contraseña, confírmela y haga clic en **Aceptar**. Volverá al cuadro de diálogo Protección mediante contraseña.

6 Haga clic en **Aceptar**. Cuando alguien intente acceder a una de las páginas protegidas, se le solicitará la contraseña.

Notas

- Para acceder a las páginas de propiedades de VirusScan, escoja ##Unlock Password en el menú Herramientas y escriba la contraseña.
- Las contraseñas no distinguen entre mayúsculas y minúsculas. Por ejemplo, si VirusScan es la contraseña, tanto “VirusScan” como “virusscan” son aceptables.
- La contraseña se solicita una vez por sesión.

{button ,AL(`PWD',0,`',`')} Temas relacionados

Desactivación de la protección mediante contraseña

1 Inicie VirusScan.
2 Escoja Proteger mediante contraseña en el menú Herramientas. Aparece el cuadro de diálogo ##Password.
3 Escriba la contraseña y haga clic en **Aceptar**. Aparece el cuadro de diálogo Protección mediante contraseña.
4 Desbloquee todas las páginas de propiedades. Las páginas protegidas van precedidas de un símbolo  y las que no, de un símbolo
 .
5 Haga clic en **Aceptar**. Ha desactivado la protección mediante contraseña.

Notas

- Para acceder a las páginas de propiedades de VirusScan sin desactivar la protección mediante contraseña, seleccione ##Unlock Password en el menú Herramientas y escriba la contraseña.
- Las contraseñas no distinguen entre mayúsculas y minúsculas. Por ejemplo, si VirusScan es la contraseña, tanto “VirusScan” como “virusscan” son aceptables.
- La contraseña se solicita una vez por sesión.

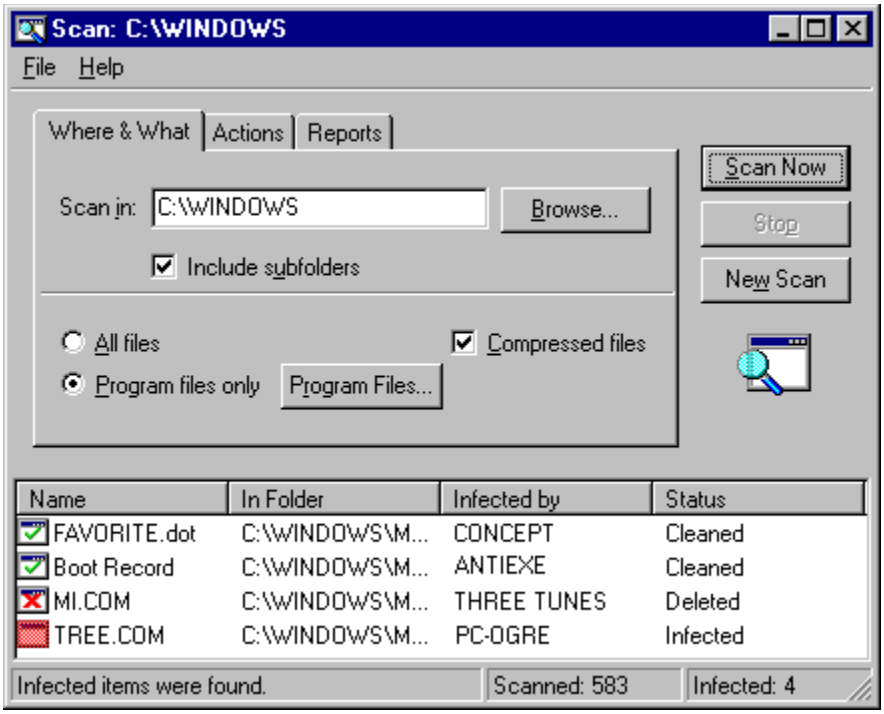
{button ,AL(`PWD',0,`',`')} Temas relacionados

Inicio de VirusScan

Haga clic en Inicio, Programas, McAfee VirusScan y después en VirusScan.

Ventana principal de VirusScan: Se ha encontrado un virus

Cuando VirusScan encuentre un virus, el archivo infectado aparece en la parte inferior de la ventana principal de VirusScan.



Desde esta ventana puede ofrecer respuesta manual a los archivos infectados. Si ha seleccionado una acción automática, compruebe cada uno de los archivos para cerciorarse de que el virus se haya limpiado, borrado o desplazado. Si ha intentado limpiar el archivo y no se ha eliminado el virus, haga clic con el botón derecho del mouse en el archivo, escoja Borrar y restituya el archivo desde la copia de respaldo.

Haga clic con el botón derecho del mouse en un archivo infectado y seleccione una de las siguientes opciones:

{button ,JI(`scan32.HLP>more',`Continue_Scanning_Clean')} Limpiar
{button ,JI(`scan32.HLP>more',`Continue_Scanning_Delete')} Borrar
{button ,JI(`scan32.HLP>more',`Continue_Scanning_Move')} Trasladar a
{button ,JI(`scan32.HLP>more',`Continue_Scanning_File_Info')} Información acerca del archivo
{button ,JI(`scan32.HLP>more',`Continue_Scanning_Virus_Info')} Información acerca del virus

Respuesta al virus

Los virus atacan a los sistemas de computación infectando los archivos, normalmente archivos de programa ejecutables o documentos y plantillas de Microsoft Word y Excel. VirusScan elimina con seguridad la mayoría de los virus de los archivos infectados y repara los daños que se puedan haber producido. Sin embargo, algunos virus se diseñan de forma que los daños producidos a los archivos sean irreparables. Éstos, denominados archivos “dañados”, se desplazan a una carpeta de cuarentena o se eliminan para evitar que el sistema vuelva a sufrir una infección.

Si VirusScan encuentra un virus, realice uno de los siguientes procedimientos:

{button ,JI(`scan32.HLP',`Responding_to_a_virus_found_in_a_file')} Respuesta a un virus encontrado en un archivo

{button ,JI(`scan32.HLP',`Responding_to_a_virus_found_in_memory')} Reacción frente al descubrimiento de un virus

Respuesta a un virus encontrado en un archivo

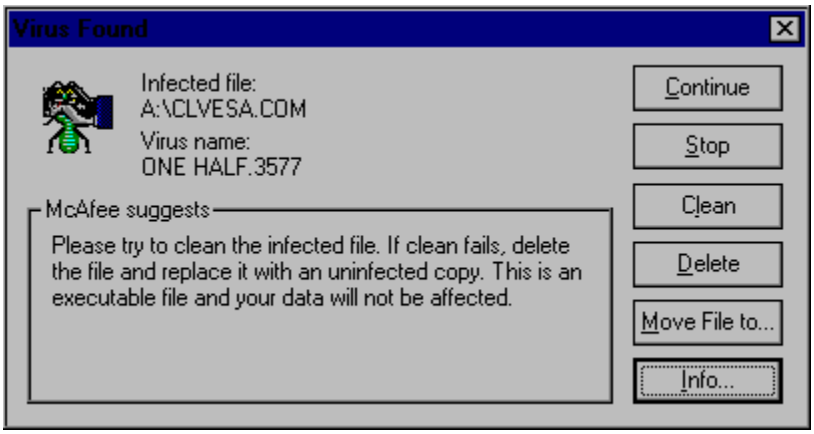
Si VirusScan detecta virus en un archivo, emprenderá la acción que haya especificado durante la configuración. Consulte la página de propiedades Acciones.

{button ,JI(`scan32.HLP',`Removing_a_Virus_Prompt_for_Action')} Consultar antes de actuar
{button ,JI(`scan32.HLP',`Removing_a_Virus_Move_Infected_Files_to_a_Folder')} Trasladar los archivos infectados automáticamente
{button ,JI(`scan32.HLP',`Removing_a_Virus_Clean_Infected_Files')} Limpiar los archivos infectados automáticamente
{button ,JI(`scan32.HLP',`Removing_a_Virus_Delete_Infected_Files')} Borrar los archivos infectados automáticamente
{button ,JI(`scan32.HLP',`Removing_a_Virus_Continue_Scanning')} Continuar la exploración

{button ,AL(`VIRFOUND',0,`',`')} Temas relacionados

Consultar antes de actuar

Si seleccionó Consultar antes de actuar en la página de propiedades Acciones y VirusScan encuentra un virus, aparecerá el cuadro de diálogo Se ha encontrado un virus.



Escoja una de las siguientes opciones:

{button ,JI(`scan32.HLP>more',`Prompt_for_Action_Continue')} Continuar
{button ,JI(`scan32.HLP>more',`Prompt_for_Action_Stop')} Detener
{button ,JI(`scan32.HLP>more',`Prompt_for_Action_Clean')} Limpiar
{button ,JI(`scan32.HLP>more',`Prompt_for_Action_Delete')} Borrar
{button ,JI(`scan32.HLP>more',`Prompt_for_Action_Move_File_to...')} Trasladar el archivo a
{button ,JI(`scan32.HLP>more',`Prompt_for_Action_Exclude')} Excluir
{button ,JI(`scan32.HLP>more',`Prompt_for_Action_Info')} Info

Trasladar los archivos infectados automáticamente

Si seleccionó esta opción en la página de propiedades Acciones y se encuentra un virus, el archivo infectado se desplaza automáticamente a la carpeta especificada.

Una vez el archivo se encuentre en la carpeta de cuarentena, puede limpiarlo o restituirlo desde las copias de respaldo y devolverlo a su ubicación original. Para volver a situarlo en la carpeta original, consulte el archivo de registro de VirusScan (VSCLOG.TXT). Si desea más información sobre cómo activar el registro de informes, consulte la página Informes. Para abrir el archivo de registro, haga clic aquí  .

Limpiar los archivos infectados automáticamente

Si seleccionó esta opción en la página de propiedades Acciones y se encuentra un virus, VirusScan intentará automáticamente limpiar el archivo.

Para confirmar que se haya limpiado el virus, compruebe la ventana principal de VirusScan. Si no se ha eliminado con éxito el virus, haga clic con el botón derecho del mouse en el archivo infectado y seleccione Borrar. A continuación, restituya el archivo desde las copias de respaldo.

Borrar los archivos infectados automáticamente

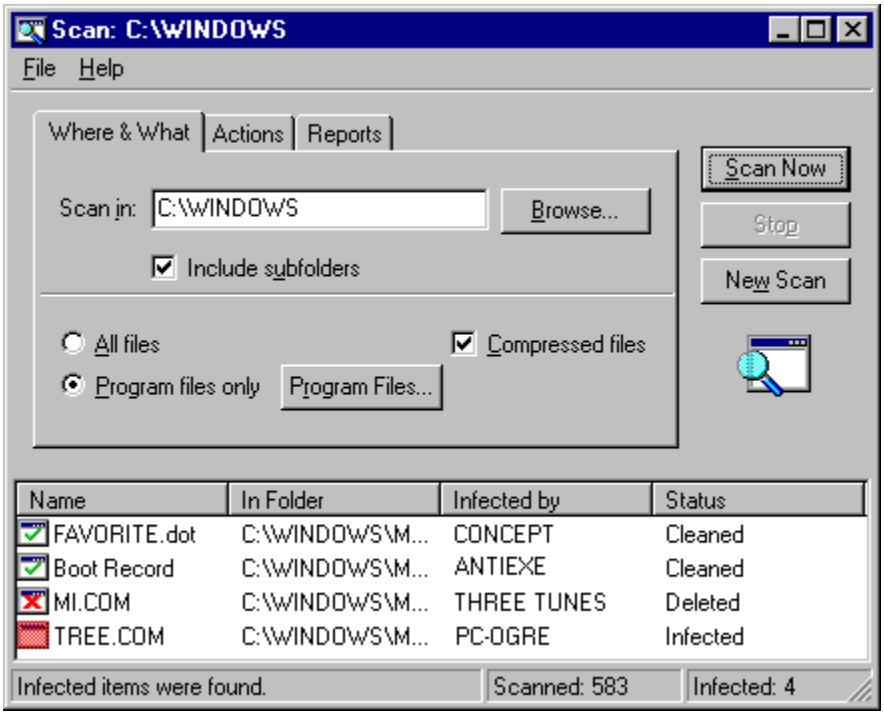
Si seleccionó esta opción en la página de propiedades Acciones y se encuentra un virus, VirusScan borrará automáticamente el archivo infectado.

Si ha seleccionado esta opción, confirme que el registro de informes esté activado. Así se cerciorará de que se guarde un registro de los archivos eliminados, de modo que pueda restituirlos desde las copias de respaldo. Consulte la página Informes.

Continuar la exploración

Si seleccionó Continuar la exploración en la página de propiedades Acciones y se encuentra un virus, VirusScan continúa la exploración sin emprender ninguna acción.

Cuando finalice la exploración, puede ofrecer respuesta manual a cada uno de los archivos infectados.



Haga clic con el botón derecho del mouse en un archivo infectado y escoja una de las siguientes opciones:

{button ,JI(`scan32.HLP>more',`Continue_Scanning_Clean')} Limpiar
{button ,JI(`scan32.HLP>more',`Continue_Scanning_Delete')} Borrar
{button ,JI(`scan32.HLP>more',`Continue_Scanning_Move')} Trasladar a
{button ,JI(`scan32.HLP>more',`Continue_Scanning_Exclude')} Excluir
{button ,JI(`scan32.HLP>more',`Continue_Scanning_File_Info')} Información acerca del archivo
{button ,JI(`scan32.HLP>more',`Continue_Scanning_Virus_Info')} Información acerca del virus

Consultar antes de actuar: Continuar

VirusScan continúa la exploración sin emprender ninguna acción. Cuando finalice la exploración, puede ofrecer respuesta manual a cada uno de los archivos infectados.

Si desea más información, consulte Continuar la exploración.

Consultar antes de actuar: Detener

Detiene la exploración y vuelve a la ventana principal.

Consultar antes de actuar: Limpiar

VirusScan intenta limpiar el archivo.

Para confirmar que se haya limpiado el virus, compruebe la ventana principal de VirusScan. Si no se ha eliminado con éxito el virus, haga clic con el botón derecho del mouse en el archivo infectado y seleccione Borrar. A continuación, restituya el archivo desde las copias de respaldo.

Consultar antes de actuar: Borrar

VirusScan borra el archivo infectado.

Si ha seleccionado esta opción, confirme que el registro de informes esté activado. Así se cerciorará de que se guarde un registro de los archivos eliminados, de modo que pueda restituirlos desde las copias de respaldo. Consulte la página Informes.

Consultar antes de actuar: Trasladar el archivo a...

Abre un cuadro de diálogo **Examinar** desde el cual puede desplazar el archivo infectado a una carpeta de cuarentena.

Consultar antes de actuar: Excluir

Excluye el archivo de futuras exploraciones.

Nota

- Ya que no se ha emprendido ninguna acción contra el archivo infectado y se le ha excluido de futuras exploraciones, esta opción no es recomendable a no ser que el archivo esté generando una falsa alarma.

Consultar antes de actuar: Info

VirusScan ofrece información detallada sobre virus y archivos.

Limpiar

VirusScan intenta eliminar el virus del archivo infectado.

Borrar

VirusScan borra el archivo infectado.

Nota

Antes de utilizar esta opción, confirme que el registro de informes esté activado. Así se cerciorará de que se guarde un registro de los archivos eliminados, de modo que pueda restituirlos desde las copias de respaldo. Consulte la página de propiedades Informes.

Trasladar a

VirusScan le solicita que seleccione una ubicación para la cuarentena.

Una vez el archivo se encuentre en la carpeta de cuarentena, puede limpiar el archivo o restituirlo desde las copias de respaldo y devuélvalo a su ubicación original.

Continuar la exploración: Excluir

Excluye el archivo de futuras exploraciones.

Nota

- Dado que no se ha emprendido ninguna acción contra el archivo infectado y se le ha excluido de futuras exploraciones, está opción no es recomendable a no ser que el archivo esté generando una falsa alarma.

Información acerca del archivo

Muestra la información de archivo, la cual incluye: tipo, ubicación y tamaño, las fechas de modificación y creación, así como los atributos del archivo.

Información acerca del virus

Muestra el nombre y los atributos del virus.

Visualización de la lista de virus

Proporciona información vital acerca de los virus. Para conocer mejor un virus, siga el procedimiento que se describe a continuación:

1 Abra la lista seleccionado Lista de virus en el menú Herramientas o haciendo clic aquí  . Se cargará la lista de virus.
2 Localice un virus desplazándose por Lista de virus o haciendo clic en **Buscar virus** e ingresando el nombre del virus.
3 Resalte el virus y haga clic en **Información acerca del virus**. Aparecerá la página Información acerca del virus.
4 Esta información incluye:

Información sobre el virus, que incluye:
Nombre del virus
Infecta
Tamaño del virus

Características del virus, que incluyen:
Residente en memoria
Codificado
Polimórfico
Reparable
Virus de macro

Nota

- Lista de virus consta de más de 250 páginas, por lo que es posible que tarde en abrirse.
- Para averiguar información detallada acerca de un virus, utilice la biblioteca de información acerca del virus.

Visualización del registro de actividades de VirusScan

El registro de actividades contiene información acerca de la detección de virus, la acción tomada y las configuraciones de sesión. Para ver el registro de actividades, seleccione Ver registro de actividades en el menú Archivo o haga clic aquí  .

Nota

- Si el registro de actividades no se abre, es posible que la opción Registrar en el archivo no esté activada (consulte la página Informes) o que no esté utilizando el nombre de archivo de registro predeterminado.
-

Relativa al contexto, a continuación

Página Parámetros

La página Parámetros se utiliza para configurar las ubicaciones y tipos de archivo que se van a explorar. Para configurar la página Parámetros, siga el procedimiento que se describe a continuación:

1 Ingrese la unidad o carpeta que desee explorar o haga clic en **Examinar** para localizarla.

2 Para explorar todas las subcarpetas, seleccione la casilla Incluir subcarpetas.

3 Para explorar todos los tipos de virus, seleccione la casilla Todos los archivos. Si desea explorar exclusivamente los archivos que sean más susceptibles a los virus, seleccione la casilla Sólo archivos de programa.

4 Para explorar archivos comprimidos, seleccione la casilla Archivos comprimidos.

5 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAGC',0,`',`')} Temas relacionados

Página Acciones

La página Acciones se utiliza para configurar el modo en que VirusScan responde a la existencia de archivos infectados. Para configurar la página Acciones, siga el procedimiento que se describe a continuación:

1 A continuación, seleccione el método de respuesta de VirusScan ante la existencia de archivos infectados.
   Consultar antes de actuar
   Trasladar los archivos infectados automáticamente
   Limpiar los archivos infectados automáticamente
   Borrar los archivos infectados automáticamente
   Continuar la exploración
2 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAGC',0,`',`')} Temas relacionados

Página Informes

La página Informes se utiliza para configurar cómo VirusScan notifica la actividad de virus. Las opciones de informe incluyen mantener un archivo de registro, emitir señales audibles y mostrar mensajes. Para configurar la página Informes, siga el procedimiento que se describe a continuación:

1 Para que VirusScan muestre un mensaje cada vez que encuentre un virus, seleccione la casilla Mostrar mensaje y escriba un mensaje.

2 Si desea que VirusScan emita una señal sonora, seleccione la casilla Señal audible.

3 Para que VirusScan mantenga un archivo de registro, seleccione la casilla Registrar en el archivo. Ingrese una ruta y un nombre para el archivo de registro (predeterminada: C:\Archivos de programa\McAfee\VirusScan\VSCLOG.TXT).

4 A fin de limitar el tamaño del archivo de registro, seleccione la casilla Limitar el tamaño del archivo de registro a e ingrese el tamaño máximo de dicho archivo.

5 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAGC',0,`',`')} Temas relacionados

Página Detección

Esta página se utiliza para configurar las ubicaciones y tipos de archivos que se van a explorar. Para configurar la página Detección, siga el procedimiento que se describe a continuación:

1 Para agregar un elemento a la exploración, haga clic en **Agregar**. Se abre el cuadro de diálogo Agregar elemento de exploración.

2 Para explorar todas las unidades adjuntadas a su PC, haga clic en el botón de opción Seleccionar elemento a explorar y seleccione Mi PC.
Para explorar todos los medios extraíbles, discos flexibles incluidos, haga clic en el botón de opción Seleccionar elemento a explorar y escoja Todos los medios extraíbles.
Para explorar todas las unidades de disco duro adjuntadas a su PC, haga clic en el botón de opción Seleccionar elemento a explorar y elija Todos los discos duros.
Para explorar todas las unidades de red instaladas, haga clic en el botón de opción Seleccionar elemento a explorar y seleccione Todas las unidades de red.
Para explorar una unidad o carpeta individual, haga clic en el botón de opción Seleccionar unidad o carpeta a explorar e ingrese la ruta del elemento a explorar, o bien haga clic en **Examinar** para localizarla.

3 Repita los pasos 1 y 2 con cada elemento que desee explorar.

4 Para explorar todas las subcarpetas, seleccione la casilla Incluir subcarpetas.

5 Para explorar todos los tipos de virus, seleccione la casilla Todos los archivos. Si desea explorar exclusivamente los archivos que sean más susceptibles a los virus, seleccione la casilla Sólo archivos de programa.

6 Para explorar archivos comprimidos, seleccione la casilla Archivos comprimidos.

7 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

Sugerencias

Para editar un elemento de exploración, selecciónelo y haga clic en **Editar**.

Para borrar un elemento de exploración, selecciónelo y haga clic en **Borrar**.

{button ,AL(`SPAGC2',0,`',`')} Temas relacionados

Página Acciones

Esta página se utiliza para configurar el modo en que VirusScan responde a la existencia de archivos infectados. Para configurar la página Acciones, siga el procedimiento que se describe a continuación:

1 A continuación, seleccione el método de respuesta de VirusScan ante la existencia de archivos infectados.
   Consultar antes de actuar
   Trasladar los archivos infectados automáticamente
   Limpiar los archivos infectados automáticamente
   Borrar los archivos infectados automáticamente
   Continuar la exploración
2 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAGC2',0,`',`')} Temas relacionados

Página Alerta

Para seleccionar opciones de alerta, siga el procedimiento que se describe a continuación.

1 Escoja la ficha Alerta.

2 Para configurar VShield de modo que envíe notificaciones a los servidores que ejecuten NetShield, seleccione la casilla Enviar alerta de red. Ingrese la ruta de la carpeta Alerta centralizada del servidor o haga clic en **Examinar** para localizarla.

3 Para configurar VirusScan para que emita una señal sonora, seleccione la casilla Emitir señal audible.

4 Si desea configurar VirusScan para que envíe un mensaje, seleccione la casilla Mostrar mensaje personalizado y escriba un mensaje personalizado (máximo de 256 caracteres).

5 Para guardar los cambios realizados al perfil de exploración predeterminado, escoja Predeterminado.

6 Para continuar configurando esta exploración, escoja otra página de propiedades. Para comenzar la exploración, haga clic en **Explorar ahora**. Para salir sin realizarla, seleccione Cerrar en el menú Archivo.

{button ,AL(`SPAGC2',0,`',`')} Temas relacionados

Página Informes

La página Informes se utiliza para configurar cómo VirusScan notifica la actividad de virus. Las opciones de informe incluyen mantener un archivo de registro, emitir señales audibles y mostrar mensajes. Para configurarla, siga el procedimiento que se describe a continuación:

1 Para que VirusScan muestre un mensaje cada vez que encuentre un virus, seleccione la casilla Mostrar mensaje y escriba un mensaje.

2 Si desea que VirusScan emita una señal sonora, seleccione la casilla Señal audible.

3 Para que VirusScan mantenga un archivo de registro, seleccione la casilla Registrar en el archivo. Ingrese una ruta y un nombre para el archivo de registro (predeterminada: C:\Archivos de programa\McAfee\VirusScan\VSCLOG.TXT).

4 A fin de limitar el tamaño del archivo de registro, seleccione la casilla Limitar el tamaño del archivo de registro a e ingrese el tamaño máximo de dicho archivo.

5 Escoja los elementos que desee que VShield registre en la sección Elementos a registrar.
Detección de virus
Limpieza de virus
Eliminación de archivos infectados
Traslado de archivos infectados
Configuración de sesión
Resumen de sesión
Fecha y hora
Nombre de usuario

6 Si desea continuar configurando la exploración, escoja otra página de propiedades. Para salir sin guardar los cambios ni realizar la exploración, seleccione Cerrar en el menú Archivo. Escoja Guardar configuración en el menú Archivo si prefiere guardar esta configuración como un archivo Configuración de VirusScan (.VSC). Para comenzar la exploración, seleccione **Explorar ahora**.

{button ,AL(`SPAGC2',0,`',`')} Temas relacionados

Página Exclusiones

Para excluir archivos, directorios o unidades de la exploración, siga el procedimiento que se describe a continuación:

1 Para agregar un elemento y excluirlo de la exploración, haga clic en Agregar. Aparece el cuadro de diálogo Excluir elemento.

   Ingrese la ruta completa de un archivo, unidad o carpeta o haga clic en **Examinar** para localizarla.

   Para excluir las subcarpetas de la exploración, seleccione la casilla Incluir subcarpetas.

   Para excluir el elemento de la exploración de archivos, seleccione la casilla Exploración de archivos. Para excluirlo de la exploración del sector de arranque, seleccione la casilla Exploración del sector de arranque.

   Haga clic en **Aceptar**.

2 Repita el paso 1 con cada elemento que desee excluir.

3 Para editar un elemento de exploración, selecciónelo y haga clic en **Editar**.

4 Para eliminar un elemento de exploración, selecciónelo y haga clic en **Eliminar**.

5 Para guardar los cambios realizados al perfil de exploración predeterminado, escoja Predeterminado.

6 Para continuar configurando esta exploración, escoja otra página de propiedades. Para comenzar la exploración, haga clic en Explorar ahora. Para salir sin realizarla, seleccione Cerrar en el menú Archivo.

{button ,AL(`SPAGC2',0,`',`')} Temas relacionados

Protección mediante contraseña

1 Seleccione las páginas de propiedades que desee proteger. Las páginas protegidas van precedidas de un símbolo  y las que no, de un símbolo

 .

2 Haga clic en **Contraseña**. Aparece el cuadro de diálogo Especificar contraseña.

3 Escriba una contraseña, confírmela y haga clic en **Aceptar**. Volverá al cuadro de diálogo Protección mediante contraseña.

4 Haga clic en **Aceptar**. Cuando alguien intente acceder a una de las páginas protegidas, se le solicitará la contraseña.

Notas

- Las contraseñas no distinguen entre mayúsculas y minúsculas. Por ejemplo, si VirusScan es la contraseña, tanto “VirusScan” como “virusscan” son aceptables.
- La contraseña se solicita una vez por sesión.

Sugerencia

- Para desactivar la protección mediante contraseña, limítese a desbloquear todas las páginas de propiedades y haga clic en **Aceptar**.

Acerca de los virus

Los virus informáticos, como la mayoría de usuarios sabe, pueden tener efectos devastadores en la productividad. Lo que estos usuarios no saben es que existe información básica que podría ayudarles a protegerse de infecciones, como, por ejemplo, el origen y el comportamiento de los virus.

El origen

Los conceptos fundamentales de virus informáticos son anteriores a la propia existencia real de los mismos. Los expertos no logran ponerse de acuerdo acerca de los cuándos y los dóndes, pero generalmente se acepta que la idea surgió cuando las computadoras eran todavía máquinas enormes y caras que pertenecían a grandes corporaciones y organizaciones gubernamentales, y no al gran público. Aunque la mayoría de los virus que están en circulación hoy en día son nocivos, la destrucción de datos no era su propósito original.

La idea era que si podía crearse un programa informático que pudiera hacer copias de sí mismo, o autoduplicarse, ello conduciría a una evolución del programa. Si el error ocurría en el proceso de réplica, el código resultante (los bits de información que forman el programa) sería mutante. De la misma forma que el código genético mutante es lo que permite a un virus biológico poder sobrevivir y propagarse, el mismo código digital mutante podría permitir a un virus informático sobrevivir en un entorno informático. Después de cierto tiempo, la continuación lógica de la teoría es que los virus informático podrían evolucionar en algo que se aproximaría a la inteligencia artificial. La ciencia ficción se convirtió de pronto en más ciencia y menos ficción.

Lo que los virus son realmente

Básicamente, un virus es simplemente un programa con un objetivo: autoduplicación. Parte de ese objetivo es pasar desapercibidos. Si un usuario encuentra un virus, lo más probable es que lo borre, con lo cual los planes de autoduplicación quedan imposibilitados. Como cualquier otro programa, para saber cómo funciona un virus, hay que ejecutarlo. Y como el usuario no va a ejecutar ningún virus intencionadamente, éste tiene que incorporarse a archivos que el usuario sí ejecutará. Ello incluye archivos ejecutables y archivos de documento con macros, tal como analizaremos más adelante. Para un virus, infectar cualquier otro tipo de archivo —por ejemplo, un archivo de texto— sería contraproducente, porque no debemos olvidar que la replicación es su principal objetivo.

¿Computadoras resfriadas?

Analice las similitudes entre los virus informáticos y los biológicos. Los virus informáticos afectan a los programas, de la misma forma que los virus biológicos infectan las células. El virus escribe su propio código entre los códigos que forman el programa. De la misma forma que los virus biológicos utilizan los propios recursos del organismo para reproducirse, el virus informático se ejecuta cada vez que el programa se ejecuta y hace copias de sí mismo. Dichas copias pueden afectar a otros programas y el ciclo vuelve a comenzar.

Los efectos de los virus informáticos son tan nocivos como los de los biológicos. Los primeros virus informáticos eran simples experimentos por parte de investigadores para probar la teoría, es decir, para ver si funcionaba. Efectivamente probaron la teoría, pero también descubrieron que los virus tenían efectos secundarios nocivos. Los virus interceptaban algunos de los procesos normales de las computadoras y causaban un comportamiento errático. Muchos virus se programan ahora específicamente para llevar a cabo alguna función a parte de la autoduplicación. Esta función, denominada la carga, puede ser tan inocua como mostrar un mensaje en el monitor de la computadora o tan nociva como destruir datos del disco duro de la computadora. Se transfiere cuando ocurre el desencadenador, que puede ser una combinación de pulsaciones de tecla específica, una cierta fecha o un número de acciones predeterminadas.

¿Quién crea estos virus?

La razón de este cambio en el comportamiento de los virus —de un experimento inocente a un ataque malicioso por la espalda — es el resultado de un cambio en el perfil de las personas que los crean. Muchas de las personas que desarrollan códigos de virus están menos interesadas en estudiar la posibilidad de inteligencia artificial que en causar daño. Algunos lo hacen con mala fe, otros porque aspiran a convertirse en los “piratas locos” clandestinos que la cultura pop tanto ha ensalzado como los libertadores de era digital. Las razones por las que la gente crea virus son probablemente tan diferentes y extrañas como las razones por las que las personas cometen otros actos destructivos.

Algunos creadores de virus se deciden a identificarse, como los hermanos paquistaníes que escribieron el virus Brain. Dichos hermanos incluían el nombre, la dirección y el número de teléfono de la compañía de software en el código vírico. Cuando se transfería la carga, el usuario podía ver esta información. Aparentemente, los hermanos crearon el virus para demostrar lo extendida que estaba la piratería informática. Lo colocaron en el software que salía de su oficina con la idea de que el virus se extendería allí donde llegara el software. Por supuesto, lo que no tuvieron en cuenta fue el hecho de que el virus se extendió infectando otros programas a parte del programa original.

Otros creadores de virus son empleados despechados buscando venganza o estudiantes que lo intentan para probarse a sí mismos. Se dice que el famoso virus Stoned lo escribió un adolescente. Cuando lo hubo escrito, y al darse cuenta de las consecuencias que tendría, destruyó todas las copias del virus excepto una, que guardó en su casa. Su hermano menor, junto con un par de amigos, consiguieron hacerse con el virus e infectaron algunos discos para gastar una broma. Pero la infección se extendió rápidamente y pronto fue imposible de detener.

Cualquiera que sea su motivación, el número de personas capaces de crear un virus está aumentando junto con la industria informática. Todos quienes corran el riesgo de una infección —todos los usuarios informáticos— deberían estar preparados y alerta.

Sólo va a peor

En parte, el hecho de que seamos tantos los que debemos estar alerta hoy en día es lo que realmente propicia la proliferación

de virus. Cuando el mundo informático estaba compuesto básicamente de máquinas enormes y caras, los virus no podían ir muy lejos una vez ejecutados. Pero con el advenimiento de las computadoras personales, de pronto los virus tenían muchos lugares a donde ir. El rápido crecimiento de la Internet, la capacidad de atacar archivos de correo electrónico y el grado creciente de dependencia del mundo respecto a las computadoras, todo ello hace que las condiciones sean aún mejores para que los virus informáticos se extiendan.

Nuevos desarrollos

Hay otras razones por las que debería estarse especialmente alerta en la actualidad. Los virus se están volviendo cada vez más complejos y avanzados, como las computadoras. Sólo en los últimos años han aparecido nuevas familias de virus peligrosas y sofisticadas, como los virus polimórficos y los virus de macro. Los virus polimórficos son especialmente complicados porque cambian cada vez que infectan un nuevo archivo. Anteriormente los programas antivirus buscaban los virus por las “firmas” (códigos únicos en cada virus), ahora dichos programas deben poder detectar los virus polimórficos que cambian la firma cada vez que infectan un archivo.

Los virus de macro infectan documentos y plantillas de documentos, un nuevo territorio para los virus. Los documentos solían estar a salvo de ataques víricos porque hasta hace pocos años no contenían ningún código ejecutable. Ahora que programas como Microsoft Word y Microsoft Excel contienen macros, los virus pueden infectar los documentos creados con dicho software a través del lenguaje de macro.

Y todo esto ha sucedido en los últimos años. Los virus que representan la mayor amenaza sólo tienen diez años. Sólo imaginar lo que nos depara a medida que las computadoras se vuelven más complicadas y más parte de nuestra vida diaria impresiona. Afortunadamente, ha adquirido la mejor protección contra infección disponible en el mercado. Junto con el excelente soporte técnico de McAfee y los equipos de investigación de antivirus en todo el mundo, puede estar seguro de que su protección va a ir evolucionando junto con el mundo de la informática.

Características de VirusScan

- El escáner con certificado NCSA asegura una detección del 100% de los virus que se encuentran “en circulación”. Consulte el sitio web NCSA, www.NCSA.com, para obtener el estado de certificación o haga clic aquí  .
- VShield, el escáner automático de VirusScan, proporciona identificación en tiempo real de virus conocidos y desconocidos en acceso, creación, copia, cambio de nombre y ejecución de archivos; acceso a discos; inicio del sistema y cierre del sistema.
- Scan, el escáner manual de VirusScan, permite la detección de virus conocidos de arranque, de archivo, mutantes, de macro, furtivos, y codificados, que se encuentran en archivos, unidades de disco y disquetes.
- La nueva interfaz del usuario de VirusScan ofrece opciones de exploración básicas o avanzadas.
- Las exploraciones de Trace™, Code Poly™ y Code Matrix™ emplean la tecnología de McAfee para conseguir máxima precisión en la identificación de virus.
- VirusScan puede configurarse para ofrecer una respuesta automatizada al detectar virus, incluidos notificación, registro, eliminación, aislamiento o limpieza.
- La ventana de exploración, el registro de actividades y la lista de virus de VirusScan proporcionan los resultados de la exploración de forma detallada, así como información acerca de los virus detectados.
- Las actualizaciones mensuales de las firmas de virus están incluidas en la compra de una licencia de suscripción McAfee para asegurar los mejores resultados en detección y eliminación de virus. Consulte Actualizaciones de VirusScan.

Tipos de virus

Un virus es un programa de software que se incorpora a otro programa ubicado en un disco o que se introduce en la memoria la computadora y propaga el virus de un programa a otro.

Además de la autoduplicación, los virus pueden dañar información, causar fallos en la computadora y mostrar mensajes ofensivos o molestos.

{button ,JI(`>more',`Boot_virus')} Virus de arranque

{button ,JI(`>more',`File_virus')} Virus de archivo

{button ,JI(`>more',`Stealth_virus')} Virus furtivos

{button ,JI(`>more',`Multi_partite_virus')} Virus multipartitos

{button ,JI(`>more',`Mutating_virus')} Virus mutantes

{button ,JI(`>more',`Encrypted_virus')} Virus codificados

Virus de arranque

El virus de arranque efectúa copias de sí mismo desde el sector de arranque de una unidad de disco a otra (por ejemplo, de una unidad de disco flexible a una unidad de disco duro).

Virus de archivo

El virus de archivo se incorpora a un programa. Cuando éste se ejecuta, el virus se incorpora a otros programas.

Virus furtivos

El virus furtivo se esconde para no ser detectado. Puede tratarse de un virus de arranque o de un virus de archivo.

Virus multipartitos

Un virus multipartito se comporta como un virus de arranque y un archivo de virus y se extiende por sectores de arranque y archivos.

Virus mutantes

Los virus mutantes cambian de forma para evitar ser detectados. Muchos virus mutantes son también virus codificados.

Virus codificados

Los virus codificados codifican parte del código para evitar ser detectados. Muchos virus codificados son también virus mutantes.

Virus de macro

Los virus de macro infectan los archivos de Microsoft Word y Excel aprovechando su funcionalidad de macro. Microsoft introdujo la funcionalidad de macro en sus productos de Word y Excel para automatizar tareas repetitivas y combinar múltiples comandos. Aunque las intenciones eran buenas, más tarde se descubrió que las macros podían usarse para propósitos maliciosos.

¿Por qué hay que explorar en busca de virus?

En el mundo de hoy, es necesario tomar medidas de seguridad informática.

Los virus atacan su computadora a través de todos los entornos informáticos con los que tiene algún contacto, ya sea mediante disquetes, redes, módems o los archivos que comparte con sus compañeros de trabajo.

Valore por un momento la información que guarda en su computadora. Es posiblemente irremplazable, y remplazarla costaría mucho tiempo y dinero. A continuación, valore las información en todas las computadoras con las que tiene contacto, las computadoras con las que éstas a su vez tienen contacto, etc.

Las soluciones de exploración en busca de virus de McAfee debería encabezar su propia lista de medidas de seguridad informática. Las exploraciones periódicas programadas de su computadora ofrecen la seguridad añadida de que está tomando precauciones contra la infección de virus.

Acerca de McAfee

Fundada in 1989, McAfee Inc. es la proveedora líder de herramientas informáticas productivas para entornos DOS, OS/2, UNIX y Windows. Nuestros productos antivirus se utilizan en más de 16.000 corporaciones en todo el mundo. Nuestros productos de utilidades ofrecen seguridad para la información, actualización de versiones automatizada y edición e inspección del sistema. McAfee es también la proveedora líder y pionera en distribución electrónica de software. Todos los productos de McAfee pueden adquirirse en distribuidores o pueden transferirse desde sistemas de tablón de anuncios y servicios en línea en todo el mundo.

McAfee no se conforma con desarrollar los mejores antivirus y utilidades del mercado mundial, sino que ofrece el mejor servicio y soporte técnico de la industria. Un equipo dedicado de investigadores, programadores y otros profesionales hacen posible el soporte técnico del producto, que McAfee o uno de nuestros agentes autorizados en más de 50 países en todo el mundo se encargan de repartir directamente.

Reacción frente al descubrimiento de un virus en la memoria

Si VirusScan descubre un virus en la memoria, complete el siguiente procedimiento:

1 Apague la computadora.
2 No reinicie mediante el botón de reinicio o Ctrl+Alt+Suprimir, ya que entonces es posible que algunos virus permanezcan intactos o suelten sus cargas destructivas.
3 Introduzca el disco de emergencia de McAfee en la unidad de disco flexible. Consulte Creación del disco de emergencia.
4 Encienda la computadora.
5 Siga las instrucciones en pantalla y elimine los virus encontrados.

Si los virus se eliminan

Si VirusScan consigue eliminar todos los virus, cierre el sistema y retire el disco.

Para encontrar y eliminar la fuente de infección, explore los disquetes inmediatamente después de la instalación.

Si los virus no se eliminan

Si VirusScan no puede eliminar todos los virus, aparecerá un mensaje informándole de ello.

Si el virus se encontró en un archivo y VirusScan no pudo eliminarlo, debería borrar el archivo y repetir los pasos descritos arriba. Si el virus se encontró en el registro de arranque maestro, consulte la documentación en el sitio web de McAfee relacionada con la eliminación manual de virus. Para obtener más información, consulte Puesta en contacto con McAfee.

{button ,AL(`VIRFOUND',0,`',`')} Temas relacionados

Análisis de falsas alarmas

Una falsa alarma es un informe de la existencia de un virus en un archivo o en la memoria cuando en realidad dicho virus no existe. Es más probable que se produzcan falsas alarmas si utiliza más de un antivirus, ya que algunos de estos programas almacenan las cadenas de firmas de virus desprotegidas en la memoria.

Tenga siempre la seguridad que cualquier virus que VirusScan encuentre es real y peligroso, por lo que debe seguir los pasos necesarios para eliminarlo del sistema. Si, por el contrario, tiene motivos para creer que VirusScan está generando falsas alarmas (por ejemplo, si detectó un virus en un único archivo que ha estado utilizando de forma segura durante años), consulte la siguiente lista de posibles causas:

- Si se está ejecutando más de un programa antivirus, es posible que VirusScan dé una falsa alarma. Configure la computadora de forma que sólo se ejecute un solo antivirus a un tiempo. Borre las líneas del archivo AUTOEXEC.BAT que se refieren a otros antivirus. Apague la computadora, espere unos segundos y enciéndala de nuevo para asegurarse de que todos los códigos de otros antivirus han desaparecido de la memoria.
- Algunos chips del BIOS incluyen una característica antivirus que podría ser la causa de falsas alarmas. Consulte el manual de referencia de su computadora para obtener más detalles.
- Si configura los códigos de validación/recuperación, es posible que las exploraciones posteriores detecten cambios en los archivos validados. Esto puede desencadenar falsas alarmas si los archivos ejecutables se automodifican o se autocomprueban. Cuando se utilizan códigos de validación, especifique una lista de excepciones para excluir dichos archivos de la comprobación.
- Algunas PC Hewlett-Packard y Zenith antiguas modifican el sector de arranque cada vez que se inicia el sistema. Es posible que VirusScan interprete estas modificaciones como una posible infección, aunque no exista ningún virus. Consulte el manual de referencia de la PC para determinar si ésta ha tiene un código de arranque que se automodifica. Para solucionar este problema, guarde la información de validación/recuperación en los propios archivos ejecutables. Este método no guarda la información acerca del sector de arranque o del registro de arranque maestro.
- Puede que VirusScan informe de virus en el sector de arranque o del registro de arranque maestro de algunos disquetes protegidos contra copia.

Mantenimiento de un entorno seguro

VirusScan es una herramienta efectiva para la prevención, detección y recuperación de una infección vírica. Es todavía más efectiva cuando se utiliza junto con un programa de seguridad informática completo que incluya una serie de medidas, como copias de respaldo a intervalos regulares, protección de contraseña eficaz, cursos de aprendizaje para el usuario y estado de alerta.

Actualizaciones de VirusScan

Para ofrecer la mejor protección antivirus posible, McAfee realiza continuas actualizaciones en los archivos que VirusScan utiliza para la detección de virus. Después de un cierto período de tiempo, VirusScan le notificará cuándo es conveniente actualizar la base de datos de definición de virus. Para una máxima protección, es importante que actualice estos archivos de forma regular.

¿Qué es un archivo de datos?

Los archivos CLEAN.DAT, NAMES.DAT, MCALYZE.DAT y SCAN.DAT proporcionan información a VirusScan y organizan los archivos de datos a los que nos referimos en esta sección.

¿Para qué se necesita un nuevo archivo de datos?

Se descubren más de 200 nuevos virus al mes. A menudo, estos virus no pueden detectarse mediante el uso de archivos de datos más antiguos. Es posible que los archivos de datos que venían originalmente con VirusScan no detecten los virus descubiertos después de la adquisición del producto.

Los investigadores de McAfee trabajan constantemente para actualizar los archivos de datos con más definiciones de virus y más actuales. Los nuevos archivos de datos se distribuyen cada cuatro o seis semanas.

Para actualizar VirusScan, haga la selección adecuada:

{button ,JI(`>(w95sec)',`Updating_VirusScan_using_Electronic_Update')} Actualización electrónica

{button ,JI(`>(w95sec)',`Updating_VirusScan_manually')} Actualización manual

Nota

- McAfee no puede garantizar que no exista compatibilidad con archivos de firmas de virus de una versión anterior. Si se suscribe a un plan de mantenimiento y actualiza el software de VirusScan, se asegurará una protección antivirus total durante la duración íntegra de dicho plan.

Actualización de VirusScan mediante Actualización electrónica

La nueva característica de McAfee, Actualización Electrónica, le informará cuándo debe actualizar urgentemente sus archivos o cuando la copia de evaluación de VirusScan haya expirado. Con esta característica, puede actualizar sus archivos de datos de una forma muy fácil o registrar el software electrónicamente. Cuando se le solicite, haga clic en Actualizar o Adquirir y siga las instrucciones en pantalla.

Para iniciar la Actualización electrónica desde la ventana principal de VirusScan, seleccione Actualizar VirusScan del menú Archivo y siga las instrucciones en pantalla.

Actualización manual de VirusScan

1 Transfiera el archivo de datos (por ejemplo, DAT-3006.ZIP) desde uno de los servicios electrónicos de McAfee. En la mayoría de los servicios, está ubicado en el área de antivirus.
2 Copie el archivo a una nueva carpeta.
3 El archivo está en formato comprimido. Descomprímalo desde cualquier programa compatible con PKUNZIP. Si no dispone de software de descompresión, puede transferir PKUNZIP (shareware) desde los sitios electrónicos de McAfee.
4 Copie el nuevo archivo de datos a la carpeta VirusScan predeterminada, cuya ruta es C:\Archivos de programa\McAfee\VirusScan.

Consejo

- Para acceder al sitio web de McAfee, haga clic aquí  .

Nota

- No olvide que su capacidad de acceso a estas actualizaciones está legalmente restringida por los términos de mantenimiento especificados en el archivo README.1ST que acompaña al software y detallados en el acuerdo de licencia del software.

Creación del disco de emergencia

El disco de emergencia es una parte muy importante de una prevención antivirus adecuada. Si el sistema se infecta, el disco de emergencia le permitirá iniciar su computadora desde un entorno limpio.

Para crear un disco de emergencia, complete el siguiente procedimiento:

1. Formatee un disco flexible de 3,5” y 1,44MB mediante DOS o el Explorador de Windows con la opción de archivos del sistema.
2. Haga clic en Inicio, ponga el puntero en Programas, luego en McAfee VirusScan y haga clic en Crear disco de emergencia, o haga clic aquí  . Aparece la pantalla de bienvenida de la Utilidad de creación del disco de emergencia McAfee.
3. Haga clic en **Aceptar**. La utilidad comienza a crear el disco de emergencia.
4. Cuando la utilidad haya terminado, retire el disco, protéjalo contra escritura, póngale una etiqueta donde se lea "Disco de emergencia VirusScan" y guárdelo en un lugar seguro.

Nota

- Si utiliza una utilidad de compresión de discos o una de codificación de contraseñas, asegúrese de que copia los controladores requeridos para tener acceso a las unidades de disco al disco de emergencia. Para obtener más información, consulte la documentación que acompaña a las utilidades.

Inserte un disco flexible e inténtelo de nuevo.

Formato de un disquete mediante DOS

Haga clic aquí  .o ingrese el siguiente comando desde el indicador del DOS:

format a: /s

Formato de un disquete mediante el Explorador de Windows

1 Inserte un disco flexible en la unidad A:\.

2 Abra el Explorador de Windows o haga clic aquí  .

3 Haga clic con el botón derecho del mouse en el icono Disco de 3½ y seleccione Formatear del menú contextual. Aparece el cuadro de diálogo Formatear - Disco de 3½ (A).

4 Seleccione la opción Total en Tipo de formateo.

5 Seleccione Copiar sólo archivos de sistema en Otras opciones.

6 Haga clic en Inicio. El Explorador de Windows comienza a dar formato al disquete.

Protección de los disquetes contra escritura

Los discos flexibles son dispositivos portátiles que sirven para guardar y recuperar datos de la computadora. Los disquetes se utilizan para guardar archivos (escritura) y recuperar archivos (lectura). Son el vehículo más común que los virus utilizan para invadir el sistema de su computadora.

Una manera de ayudar a evitar infecciones a través de discos flexibles que utilice sólo para leer información es protegerlos contra escritura . Si el sistema queda infectado por un virus, la característica de protección contra escritura evita que los disquetes se infecten, evitando a su vez que el sistema vuelva a infectarse una vez limpio.

Para proteger un disco flexible de 3,5" contra escritura:

1 Coloque el disquete boca abajo con el deslizador metálico mirando hacia usted.
2 Examine el pequeño orificio rectangular en la parte superior izquierda. Hay una lengüeta cuadrada de plástico que puede deslizar hacia arriba y hacia abajo a través del orificio.
3 Para proteger el disquete contra escritura, deslice la lengüeta de plástico hacia arriba hasta el extremo del disquete para que el orificio quede abierto.

Notas

- Los disquetes que no estén protegidos contra escritura deberían explorarse y limpiarse antes seguir con este procedimiento.
- Si no existen ninguna lengüeta y el orificio está abierto, significa que el disquete está protegido contra escritura.

Puesta en contacto con McAfee

Seleccione una de las siguientes opciones:

{button ,JI(`',`Customer_Service')} Servicio al cliente

{button ,JI(`',`Technical_Support')} Soporte técnico

{button ,JI(`',`McAfee_Training')} Cursos de aprendizaje

Servicio al cliente

Para encargar productos u obtener información acerca de cualquier producto, póngase en contacto con nuestro departamento de atención al cliente al (972) 278-6100 para clientes individuales o (408) 988-3832 para compañías clientes. Alternativamente, puede escribirnos a la siguiente dirección:

McAfee Associates, Inc.
2805 Bowers Avenue
Santa Clara, CA 95051-0963
EE.UU.

Soporte técnico

En McAfee nos dedicamos a satisfacer al cliente. McAfee ha continuado esta tradición invirtiendo tiempo y esfuerzo para hacer de nuestro sitio web un recurso útil para las actualizaciones del software de McAfee y tener acceso a las últimas noticias e información. Para obtener información acerca de los temas relacionados con el soporte técnico, le invitamos primero a visitar nuestro sitio web.

World Wide Web	http://www.mcafee.com

Haga clic aquí  para acceder al sitio web de McAfee.

Si no encuentra lo que necesita o no dispone de acceso a la Web, intente ponerse en contacto con los servicios automáticos de McAfee.

Sistema automático de contestador de voz y de fax	(408) 988-3034
Internet	support@mcafee.com
BBS de McAfee	(408) 988-4004 de 1.200 bps a 28.800 bps 8 bits, sin paridad, 1 bit de parada 24 horas, 365 días al año
CompuServe	GO MCAFEE
America Online	Keyword MCAFEE
Microsoft Network (MSN)	MCAFEE

Si los servicios automáticos no solucionan su problema, puede ponerse en contacto con McAfee de lunes a viernes entre las 6:00 h. y las 18:00 h (hora del Pacífico).

Clientes individuales	(972) 278-6100
Compañías clientes	(408) 988-3832
Fax	(408) 970-9727

Para acelerar el proceso de ayuda en la utilización de nuestros productos, anote lo siguiente antes de llamar:

- Nombre y versión del producto
- Marca y modelo de la computadora y de cualquier software adicional
- Tipo y versión de sistema operativo
- Tipo y versión de red
- Contenido de los archivos AUTOEXEC.BAT y CONFIG.SYS y del script LOGIN del sistema
- Los pasos específicos para reproducir el problema, si procede

Cursos de aprendizaje de McAfee

Para obtener información acerca de cursos de aprendizaje programados de cualquier producto McAfee en sus propias instalaciones, llame al (800) 338-8754.

Niveles de error en VirusScan para DOS

Cuando ejecute VirusScan en el entorno DOS (mediante SCAN.EXE), se establece un nivel de error de DOS. Puede utilizar ERRORLEVEL en archivos por lotes para llevar a cabo diferentes acciones según los resultados de la exploración. Para obtener más información, consulte la documentación de su sistema operativo DOS.

VirusScan puede responder con los siguientes niveles de error:

NIVEL DE ERROR	Descripción
0	No ocurrió ningún error y no se encontró ningún virus.
1	Ocurrió un error al acceder a un archivo (lectura o escritura).
2	Uno de los archivos de datos de VirusScan está corrupto.
3	Ocurrió un error al acceder a un disco (lectura o escritura).
4	Ocurrió un error al acceder al archivo creado con la opción /AF; el archivo se ha dañado.
5	No hay memoria suficiente para cargar el programa o completar la operación.
6	Ocurrió un error de programa interno (error de falta de memoria).
7	Ocurrió un error al acceder a un archivo de mensajes internacional (MCAFEE.MSG).
8	Falta un archivo necesario para ejecutar VirusScan, como SCAN.DAT.
9	Las opciones o argumentos de opción especificados en la línea de comando son incompatibles o no se reconocen.
10	Se encontró un virus en la memoria.
11	Ocurrió un error de programa interno.
12	Ocurrió un error al intentar eliminar un virus, como, por ejemplo, no se encontró CLEAN.DAT o VirusScan no pudo eliminar el virus.
13	Se encontró uno o más virus en el registro de arranque maestro, el sector de arranque o los archivos.
14	El archivo SCAN.DAT no está actualizado; actualice los archivos de datos de VirusScan.
15	Falló la autocomprobación de VirusScan; es posible que esté infectado o dañado.
16	Ocurrió un error al acceder a la unidad de disco o al archivo especificados.
17	No se especificó ninguna unidad, carpeta o archivo; no hay nada a explorar.
18	Se ha modificado un archivo validado (opciones /CF o /CV).
19-99	Reservado.
100+	Error del sistema operativo; VirusScan agrega 100 al número original.
102	Se utilizó CTRL+C o CTRL+BREAK para interrumpir la exploración. (Puede desactivar CTRL+C o CTRL+BREAK con la opción de línea de comando /NOBREAK.)

Medidas de seguridad informática

Las medidas de seguridad informática incluyen:

Protección contra virus
Copias de respaldo a intervalos regulares
Protección de contraseña eficaz
Cursos de aprendizaje y estado de alerta

Trasladar los archivos infectados automáticamente

Cuando esta opción está seleccionada, los archivos infectados se trasladan automáticamente a la carpeta especificada. Para seleccionar un área de cuarentena, ingrese la ruta de acceso a la carpeta o haga clic en **Examinar** para ubicar una.

Limpiar los archivos infectados automáticamente

Cuando esta opción está seleccionada, los virus se eliminan automáticamente de los archivos. Si no pudo eliminarse algún virus, ejecute VirusScan con la opción de eliminación y restaure el archivo infectado a partir de las copias de respaldo.

Borrar los archivos infectados automáticamente

Cuando esta opción está seleccionada, los archivos infectados se borran automáticamente. Después de que VirusScan haya borrado los archivos infectados, puede restaurarlos a partir de las copias de respaldo.

Si selecciona esta opción, asegúrese de activar el registro de informes. Ello le permitirá disponer de un registro de los archivos eliminados, de modo que podrá restaurarlos a partir de las copias de respaldo.

Continuar la exploración

Cuando esta opción está seleccionada, la exploración continúa y no se lleva a cabo ninguna acción. Cuando la exploración haya terminado, puede realizar acciones manuales sobre cada archivo infectado en la ventana principal de VirusScan.

Nota

- Esta opción no es recomendable en máquinas que estén desatendidas.

Consultar antes de actuar

Cuando esta opción está seleccionada, se realiza una consulta antes de actuar en cada archivo infectado. Para convertir una acción en disponible o no disponible para la detección de virus, seleccione o cancele la selección de la casilla de verificación.

Consejo

- Para evitar el acceso a acciones específicas, como Continuar la exploración (sin llevar a cabo ninguna acción), cancele la selección de las casillas de verificación y active la Protección mediante contraseña.

Nombre del virus

Indica el nombre del virus.

Infecta

Indica los tipos de archivo infectados por el virus, que incluyen:

Ejecutables (.EXE)
Archivos COM (.COM)
Archivos de Word (.DO?)
Archivos de Excel (.XL?)

Tamaño del virus

Indica el tamaño del virus en bytes.

Residente en memoria

Indica si el virus reside en la memoria.

Codificado

Indica si se trata de un virus codificado.

Polimórfico

Indica si se trata de un virus polimórfico. Los virus polimórficos modifican su código para evitar ser detectados.

Reparable

Indica si los archivos infectados por este virus son reparables.

Virus de macro

Indica si se trata de un virus de macro. Los virus de macro infectan archivos de Microsoft Word y de Excel.

Archivos de programa

Los archivos de programa son los más expuestos a las infecciones de virus. Éstos incluyen los archivos .COM, .EXE, .DO?, .XL?. Para cambiar los tipos de archivo a explorar en busca de virus, siga este procedimiento:

1 Haga clic en **Extensiones**. Aparece el cuadro de diálogo Extensiones de archivos de programa.

2 Para agregar una extensión de archivo a explorar, haga clic en Agregar. Ingrese una nueva extensión de archivo y haga clic en **Aceptar**. Repita este paso hasta haber ingresado todas las extensiones de archivo deseadas.

3 Para borrar una extensión, selecciónela y haga clic en Borrar.

4 Para volver a las extensiones predeterminadas, haga clic en Predeterminadas.

5 Para salir de la lista de archivos de programa sin guardar cambios, haga clic en Cancelar. Para guardar los cambios y salir, haga clic en **Aceptar**.

Archivos comprimidos

Cuando esta opción está activada, VirusScan explora los archivos comprimidos PKZIP, PKLITE, WInZip, LZH y LZEXE.

Archivos comprimidos

Cuando esta opción está activada, VShield explora los archivos comprimidos PKLITE y LZEXE.

Para abrir el Explorador de Windows

Haga clic en Inicio, coloque el puntero en Programas y haga clic en Explorador de Windows.

Para abrir Mi PC

Ubique y haga doble clic en el icono Mi PC situado en el extremo superior izquierdo del escritorio.

Alerta centralizada

La Alerta centralizada es la solución de McAfee para avisar a toda una compañía de la existencia de un virus. Una vez configuradas, las estaciones de trabajo que ejecuten VirusScan envían notificaciones sobre virus a los servidores que ejecutan NetShield. Esto ayuda a los administradores a localizar la fuente de las infecciones víricas y evitar que se extiendan.

Para configurar la Alerta centralizada, haga lo siguiente:

1 Solicite al administrador del sistema el nombre de un servidor que ejecute NetShield y la carpeta Alerta centralizada.
2 Asegúrese de que tiene derechos de escritura para esta carpeta.
3 Configure las tareas VShield y VirusScan para enviar mensajes de red a esta carpeta.

Notas

- Para configurar las tareas VShield y VirusScan para enviar mensajes de Alerta centralizada a un servidor, seleccione Enviar alerta de red en la página Acciones y haga clic en **Examinar** para ubicar la carpeta Alerta centralizada del servidor.
- El archivo denominado CENTALRT.TXT debe estar ubicado en la carpeta Alerta centralizada del servidor.

Biblioteca de información acerca de virus de McAfee

La biblioteca de información acerca de virus de McAfee contiene información que incluye el nombre del virus, sus características, su método de infección, cómo saber si se está infectado y cómo eliminarlo.

Hay varias formas de acceder a la biblioteca de información acerca de virus de McAfee:

- Para acceder automáticamente a la versión más actual de la biblioteca de información acerca de virus de McAfee, haga clic aquí  .
- Para acceder manualmente a la versión más actual de la biblioteca de información acerca de virus de McAfee, navegue a http://www.mcafee.com/support/techdocs/vinfo/index.html.
- Si copió la versión del archivo de ayuda de la biblioteca de información acerca de virus a la carpeta de archivos de programa VirusScan, haga clic aquí  .
- Si no copió la versión del archivo de ayuda de la biblioteca de información acerca de virus a la carpeta de archivos de programa VirusScan, abra el Explorador de Windows o Mi PC, navegue al CD-ROM de VirusScan y haga doble clic en MCAFEE.HLP.

Notas

- Para acceder a esta versión de Internet de la biblioteca de información acerca de virus, debe disponer de una conexión activa a la Internet y de una copia de Netscape Navigator o Microsoft Internet Explorer. Si no dispone de ninguno de estos exploradores pero tiene acceso a la World Wide Web, acceda al sitio web de forma manual.
- Si la versión del archivo de ayuda de la biblioteca tarda más de 10-15 segundos en cargarse, puede que no esté instalada en el sistema. Para ver la biblioteca de información acerca de los virus, puede copiar el archivo MCAFEE.HLP en la carpeta VirusScan (predeterminado en C:\Archivos de programa\McAfee\VirusScan) o navegar al CD-ROM de VirusScan y hacer doble clic en MCAFEE.HLP.

Comprobación de la instalación

El archivo de comprobación de antivirus estándar Eicar Standard AntiVirus Test File es fruto del esfuerzo combinado de fabricantes de antivirus en todo el mundo para establecer un estándar para que los clientes puedan verificar las instalaciones de antivirus. Para comprobar la instalación, copie la línea siguiente en el archivo correspondiente y denomínelo EICAR.COM:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Cuando termine, tendrá un archivo de 69 o 70 bytes.

Cuando se explore el archivo, VirusScan informará de la existencia del virus EICAR-STANDARD-AV-TEST-FILE.

¡ESTE ARCHIVO NO ES UN VIRUS! Borre el archivo cuando la comprobación de la instalación haya terminado para que no alarmar innecesariamente a los usuarios que lo desconozcan.

Nota

- Dado que Eicar Standard AntiVirus Test File no es en realidad ninguna infección vírica, no podrá limpiar o reparar el archivo infectado.

Formato de archivo VSH

El archivo VSH es un archivo de texto de configuración, con el mismo formato que el archivo INI de Windows, que describe la configuración de Vshield. Cada una de las variables en el archivo tiene un nombre seguido por un signo (=) igual y una cifra. Las cifran definen los parámetros seleccionados para la configuración de VShield. Las variables se dividen en cinco grupos: DetectionOptions, ActionOptions, ReportOptions, General y ExcludedItems. Para editar el archivo VSH, haga clic con el botón derecho del mouse en el nombre de archivo correspondiente y seleccione Editar.

En las variable booleanas, las cifras posibles son 0 y 1. La cifra 0 indica a VShield que desactive el parámetro, mientras que 1 indica que el parámetro está activado.

General

Variable	Descripción
bCanBeDisabled	Tipo: Booleana (1/0) Define si VShield puede desactivarse Valor predeterminado: 1
bShowTaskbarIcon	Tipo: Booleana (1/0) Define si se muestra el icono de la barra de tareas de VShield Valor predeterminado: 1

DetectionOptions

Variable	Descripción
bScanOnExecute	Tipo: Booleana (1/0) Indica a Vshield que explore al ejecutar los archivos Valor predeterminado: 1
bScanOnOpen	Tipo: Booleana (1/0) Indica a VShield que explore al abrir los archivos Valor predeterminado: 1
bScanOnCreate	Tipo: Booleana (1/0) Indica a VShield que explore al crear los archivos Valor predeterminado: 1
bScanOnRename	Tipo: Booleana (1/0) Indica a VShield que explore al cambiar el nombre de los archivos Valor predeterminado: 1
bScanOnShutdown	Tipo: Booleana (1/0) Indica a VShield que explore el registro de arranque de la unidad A: cuando se cierra el sistema Valor predeterminado: 1
bScanOnBootAccess	Tipo: Booleana (1/0) Indica a VShield que explore el registro de arranque de una unidad de disco la primera vez que se accede a él Valor predeterminado: 1
bScanAllFiles	Tipo: Booleana (1/0) Indica al programa que explore en todos los archivos Valor predeterminado: 0
bScanCompressed	Tipo: Booleana (1/0)

	Indica al programa que explore los archivos comprimidos .
	Valor predeterminado: 0
szProgramExtensions	Tipo: Cadena
	Define las extensiones a explorar
	Valor predeterminado: EXE COM DO? XL?
szDefaultProgramExtensions -	Tipo: Cadena
	Define las extensiones a utilizar como extensiones de programa predeterminadas durante la configuración de la exploración
	Valor predeterminado: EXE COM DO? XL?

AlertOptions

Variable	**Descripción**
bNetworkAlert	Tipo: Booleana (1/0)
	Activa la Alerta centralizada
	Valor predeterminado: 0
szNetworkAlertPath	Tipo: Cadena
	Especifica la carpeta Alerta centralizada de un servidor.
	Valor predeterminado: ninguno

ActionOptions

Variable	Descripción
bDisplayMessage	Tipo: Booleana (1/0)
	Define si debería aparecer un mensaje personalizado en el cuadro de diálogo Consultar antes de actuar si se detecta un virus
	Valor predeterminado: 0
uVshieldAction	Tipo: Entera (1-5)
	Indica a VShield que inicie una acción especificada cuando se detecta un virus
	Valores posibles:
	1 - Consultar antes de actuar
	2 - Mover los archivos infectados a una carpeta
	3 - Limpiar los archivos infectados automáticamente (Negar el acceso si los archivos no pueden limpiarse)
	4 - Borrar los archivos infectados automáticamente
	5 - Negar el acceso a los archivos infectados
	Valor predeterminado: 1
bButtonClean	Tipo: Booleana (1/0)
	Indica a Vshield que ofrezca al usuario la opción de limpiar un archivo si Consultar antes de actuar está seleccionada y se detecta un virus
	Valor predeterminado: 1
bButtonDelete	Tipo: Booleana (1/0)

	Indica a Vshield que ofrezca al usuario la opción de borrar un archivo si Consultar antes de actuar está seleccionada y se detecta un virus
	Valor predeterminado: 1
bButtonExclude	Tipo: Booleana (1/0)
	Indica a Vshield que ofrezca al usuario la opción de excluir un archivo si Consultar antes de actuar está seleccionada y se detecta un virus
	Valor predeterminado: 1
bButtonContinue	Tipo: Booleana (1/0)
	Indica a VShield que ofrezca al usuario la opción de continuar el evento interceptado si Consultar antes de actuar está seleccionada y se detecta un virus
	Valor predeterminado: 1
bButtonStop	Tipo: Booleana (1/0)
	Indica a VShield que ofrezca al usuario la opción de negar el acceso al archivo infectado si Consultar antes de actuar está seleccionada y se detecta un virus
	Valor predeterminado: 1
szMoveToFolder	Tipo: Cadena
	Define la carpeta a donde trasladar los archivos infectados
	Valor predeterminado: \Infectados
szCustomMessage	Tipo: Cadena
	Define el mensaje personalizado a mostrar cuando se detecta un virus si la acción está configurada en Consultar antes de actuar
	Valor predeterminado: Se ha encontrado un posible virus

ReportOptions

Variable	**Descripción**
bLogToFile	Tipo: Booleana (1/0)
	Define si los resultados de la exploración deberían registrarse en un archivo de registro
	Valor predeterminado: 0
bLimitSize	Tipo: Booleana (1/0)
	Define si debería limitarse el tamaño del archivo de registro
	Valor predeterminado: 1
uMaxKilobytes	Tipo: Entera (10-999)
	Define el tamaño máximo del archivo de registro en kilobytes
	Valor predeterminado: 100
bLogDetection	Tipo: Booleana (1/0)
	Define si deberían registrarse los resultados de la exploración

	Valor predeterminado: 1
bLogClean	Tipo: Booleana (1/0) Define si deberían registrarse las operaciones de limpieza de archivos infectados Valor predeterminado: 1
bLogDelete	Tipo: Booleana (1/0) Define si deberían registrarse las operaciones de eliminación de archivos infectados Valor predeterminado: 1
bLogMove	Tipo: Booleana (1/0) Define si deberían registrarse las operaciones de traslado de archivos infectados Valor predeterminado: 1
bLogSettings	Tipo: Booleana (1/0) Define si debería registrarse la configuración de sesión al cerrar el sistema Valor predeterminado: 1
bLogSummary	Tipo: Booleana (1/0) Define si debería registrarse el resumen de la sesión al cerrar el sistema Valor predeterminado: 1
bLogDateTime	Tipo: Booleana (1/0) Define si debería registrarse la fecha y la hora de un evento Valor predeterminado: 1
bLogUserName	Tipo: Booleana (1/0) Define si debería registrarse el nombre del usuario Valor predeterminado: 1
szLogFileName	Tipo: Cadena Define el nombre del archivo de registro Valor predeterminado: C:\Archivos de programa\McAfee\VirusScan\VSHLOG.TXT

SecurityOptions

Variable	**Descripción**
szPasswordProtect	Tipo: Booleana (1/0) Define si la protección de contraseña está activada. Valor predeterminado: 0

ExclusionOptions

Variable	**Descripción**
szExclusionsFileName	Tipo: Cadena Valor predeterminado: VSHLOG.TXT

AVCONFILE

Variable	Descripción
AVCONFILE	Tipo: Cadena Especifica la ruta de acceso a AVCONSOLE Predeterminado: C:\Archivos de programa\McAfee\VirusScan\ avconsole.ini
SECTION	Tipo:Cadena Especifica la ubicación de los reportes dentro AVCONSOL.INI Predeterminado: Item_0

ExcludedItems

Variable	Descripción
NumExcludedItems	Tipo: Entera (0-n) Define el número de elementos excluidos de la exploración automática Valor predeterminado: 1
ExcludedItem_x, donde x es un índice basado en cero	Tipo: Cadena Instruye a VShield que excluya un elemento de la exploración automática Valor predeterminado: \Papelera de reciclaje|*.*|1|1 * * La cadena está separada en campos mediante el carácter (|): Campo 1 - Sección de carpeta del elemento a excluir. Déjelo en blanco para un archivo único en cualquier parte del sistema. Campo 2 - Sección de archivo del elemento a excluir. Déjelo en blanco si se excluye una carpeta sin nombre de archivo. Campo 3 - Entera (1-3) Valores posibles: 1 - Excluir de la exploración de acceso a archivos 2 - Excluir de exploración del registro de arranque 3 - Excluir de la exploración del registro de arranque y de la de acceso a archivos Campo 4 - Booleana (1/0) Valores posibles: 1 - Indica a VShield que excluya las subcarpetas del elemento excluido 0 - Indica a VShield que no excluya las subcarpetas

Formato de archivo VSC

El archivo VSC es un archivo de texto de configuración, formateado de una forma parecida al archivo INI de Windows, que define la configuración VirusScan. Cada variable en el archivo tiene un nombre seguido del signo (=) igual y una cifra. Las cifras definen los parámetros seleccionados para la configuración de VirusScan. Las variables se dividen en tres grupos: ScanOptions, AlertOptions y ActivityLogOptions. Para editar el archivo VSC, haga clic con el botón derecho del mouse en el nombre de archivo y seleccione Editar.

Nota

- En las variables booleanas, los valores posibles son 0 y 1. El valor 0 indica a VirusScan que desactive la configuración, mientras que el 1 indica que la configuración está activada.

ScanOptions

Variable	Descripción
bAutoStart	Tipo: Booleana (1/0) Indica a VirusScan que inicie la exploración inmediatamente después de ejecutarse Valor predeterminado: 0
bAutoExit	Tipo: Booleana (1/0) Instruye a VirusScan que se cierre al terminar la exploración si no se han encontrado virus Valor predeterminado: 0
bAlwaysExit	Tipo: Booleana (1/0) Indica a VirusScan que se cierre al terminar la exploración Valor predeterminado: 0
bSkipMemoryScan	Tipo: Booleana (1/0) Indica a VirusScan que ignore la exploración de la memoria Valor predeterminado: 0
bSkipBootScan	Tipo: Booleana (1/0) Indica a VirusScan que ignore la exploración del sector de arranque Valor predeterminado: 0
bSkipSplash	Tipo: Booleana (1/0) Indica a VirusScan que no muestre la pantalla inicial de presentación cuando se inicie la aplicación Valor predeterminado: 0
nPriority	Tipo: Entera (0-5) Especifica la prioridad de los enlaces de exploración. Valores: 0 - Prioridad de enlace normal (predeterminado) 1 - Prioridad de enlace baja 2 - Prioridad de enlace más baja de lo normal 3 - Prioridad de enlace normal 4 - Prioridad de enlace más alta de lo normal 5 - Prioridad de enlace más alta Valor predeterminado: 0
nChecksum	Reservado
bConfigurableGuiMode	Tipo: Booleana (1/0) Indica a VirusScan que utilice la

	interfaz del usuario en modo Avanzado Valor predeterminado: 0
szTaskName	Reservado

DetectionOptions

Variable	Descripción
bScanAllFiles	Tipo: Booleana (1/0) Instruye a VirusScan que explore en todos los archivos. Valor predeterminado: 0
bScanCompressed	Tipo: Booleana (1/0) Indica a VirusScan que explore los archivos comprimidos Valor predeterminado: 1
szProgramExtensions	Tipo: Cadena Define las extensiones a explorar. Valor predeterminado: COM DO? EXE XL?
SzDefaultProgramExtensions	Tipo: Cadena Define las extensiones a utilizar las extensiones de programa predeterminadas durante la configuración de la exploración Valor predeterminado: COM DO? EXE XL?

AlertOptions

Variable	Descripción
bNetworkAlert	Tipo: Booleana (1/0) Activa la Alerta centralizada Valor predeterminado: 0
bSoundAlert	Tipo: Booleana (1/0) Indica a VirusScan que emita una señal audible cuando detecte un virus Valor predeterminado: 1
szNetworkAlertPath	Tipo: Cadena Especifica la carpeta Alerta centralizada de un servidor. Valor predeterminado: ninguno

ActionOptions

Variable	Descripción
bDisplayMessage	Tipo: Booleana (1/0) Define si debería aparecer un mensaje personalizado si se detecta un virus Valor predeterminado: 0
uScanAction	Tipo: Entera (1-5) Indica a VirusScan que inicie una acción especificada cuando se detecta un virus Valores posibles:

	0 - Consultar antes de actuar 1 - Mover los archivos infectados a una carpeta 2 - Limpiar los archivos infectados automáticamente 3 - Borrar los archivos infectados automáticamente 4 - Continuar explorando Valor predeterminado: 0
bButtonClean	Tipo: Booleana (1/0) Indica a VirusScan que ofrezca al usuario la opción de limpiar un archivo si Consultar antes de actuar está seleccionada y se detecta un virus Valor predeterminado: 1
bButtonDelete	Tipo: Booleana (1/0) Indica a VirusScan que ofrezca al usuario la opción de borrar un archivo si Consultar antes de actuar está seleccionada y se detecta un virus Valor predeterminado: 1
bButtonExclude	Tipo: Booleana (1/0) Indica a VirusScan que ofrezca al usuario la opción de excluir un archivo si Consultar antes de actuar está seleccionada y se detecta un virus Valor predeterminado: 0
bButtonMove	Tipo: Booleana (1/0) Indica a VirusScan que ofrezca al usuario la opción de trasladar el archivo infectado si Consultar antes de actuar está seleccionada y se detecta un virus Valor predeterminado: 1
bButtonContinue	Tipo: Booleana (1/0) Indica a VirusScan que ofrezca al usuario la opción de continuar el evento interceptado si Consultar antes de actuar está seleccionada y se detecta un virus Valor predeterminado: 1
bButtonStop	Tipo: Booleana (1/0) Indica a VirusScan que ofrezca al usuario la opción de negar el acceso al archivo infectado si Consultar antes de actuar está seleccionada y se detecta un virus Valor predeterminado: 1
szMoveToFolder	Tipo: Cadena Define la carpeta a donde trasladar los archivos infectados Valor predeterminado: \Infectados
szCustomMessage	Tipo: Cadena Define el mensaje personalizado a mostrar a mostrar si se detecta un virus Valor predeterminado: Se ha encontrado un posible virus

ReportOptions

Variable	Descripción
bLogToFile	Tipo: Booleana (1/0) Define si los resultados de la exploración deberían registrarse en un archivo de registro Valor predeterminado: 1
bLimitSize	Tipo: Booleana (1/0) Define si debería limitarse el tamaño del archivo de registro Valor predeterminado: 1
uMaxKilobytes	Tipo: Entera Define el tamaño máximo del archivo de registro en kilobytes Valor predeterminado: 100
bLogDetection	Tipo: Booleana (1/0) Define si deberían registrarse los resultados de la exploración Valor predeterminado: 1
bLogClean	Tipo: Booleana (1/0) Define si deberían registrarse los resultados de limpieza Valor predeterminado: 1
bLogDelete	Tipo: Booleana (1/0) Define si deberían registrarse las operaciones de eliminación Valor predeterminado: 1
bLogMove	Tipo: Booleana (1/0) Define si deberían registrarse las operaciones de traslado de archivos infectados Valor predeterminado: 1
bLogSettings	Tipo: Booleana (1/0) Define si debería registrarse la configuración de sesión al cerrar el sistema Valor predeterminado: 1
bLogSummary	Tipo: Booleana (1/0) Define si debería registrarse el resumen de la sesión al cerrar el sistema Valor predeterminado: 1
bLogDateTime	Tipo: Booleana (1/0) Define si debería registrarse la fecha y la hora de un evento Valor predeterminado: 1
bLogUserName	Tipo: Booleana (1/0) Define si debería registrase el nombre del usuario Valor predeterminado: 1
szLogFileName	Tipo: Cadena Define el nombre del archivo de registro Valor predeterminado: VSCLOG.TXT

ScanItems

Variable	Descripción

NumScanItems	Tipo: Entera (0-n) Define el número de elementos a explorar Valor predeterminado: 1
szScanItem_x	Tipo: Cadena Valor predeterminado: C:\ Indica a Vshield que explore el elemento * La cadena está separada en campos mediante el carácter (|): Campo 1 - Sección de carpeta del elemento a excluir. Déjelo en blanco para un archivo único en cualquier parte del sistema. Campo 2 - Sección de archivo del elemento a excluir. Déjelo en blanco si se excluye una carpeta sin nombre de archivo. Campo 3 - Entera (1-3) Valores posibles: 1 - Explora el archivo 2 - Explora el registro de arranque 3 - Explora el archivo y el registro de arranque Campo 4 - Booleana (1/0) Valores posibles: 1 - Indica a VShield que explore las subcarpetas del elemento 0 - Indica a VShield que no explore las subcarpetas del elemento

SecurityOptions

Variable	**Descripción**
szPasswordProtect	Tipo: Booleana (1/0) Define si la protección de contraseña está activada Valor predeterminado: 0
szPasswordCRC	Reservado. No modificar.
bInheritSecurity	Tipo: Booleana (1/0) Define si la característica de herencia de seguridad está activada. Cuando lo está, las copias de la tarea permanecen protegidas por contraseña Valor predeterminado: 0

ExcludedItems

Variable	**Descripción**
NumExcludeItems	Tipo: Entera (0-n) Define el número de elementos excluidos de la exploración automática Valor predeterminado: 1
ExcludedItem_x,	Tipo: Cadena

donde x es un índice basado en cero	Instruye a VShield que excluya un elemento de la exploración automática Valor predeterminado: \Papelera de reciclaje|*.*|1|1 * * La cadena está separada en campos mediante el carácter (|): Campo 1 - Sección de carpeta del elemento a excluir. Déjelo en blanco para un archivo único en cualquier parte del sistema. Campo 2 - Sección de archivo del elemento a excluir. Déjelo en blanco si se excluye una carpeta sin nombre de archivo. Campo 3 - Entera (1-3) Valores posibles: 1 - Excluir de la exploración de acceso a archivos 2 - Excluir de exploración del registro de arranque 3 - Excluir de la exploración del registro de arranque y de la de acceso a archivos Campo 4 - Booleana (1/0) Valores posibles: 1 - Indica a VShield que excluya las subcarpetas del elemento excluido 0 - Indica a VShield que no excluya las subcarpetas

Formato de archivo ALR de Alerta centralizada

El archivo ALR es el texto de Alerta centralizada que contiene variables de evento de virus. Cada variable en el archivo tiene un nombre seguido por el signo (=) igual. A continuación viene una descripción línea a línea del formato de archivo ALR de Alerta centralizada:

[CentralAlert]	Identificador de Alerta centralizada
uFileVersion	Tipo: Entera
	Número de versión de Alerta centralizada
uStatus	Reservado
szVirusName	Tipo: Cadena
	El nombre del virus.
szItemName	Tipo: Cadena
	El nombre y la ruta de acceso del archivo infectado.
szUserName	Tipo: Cadena
	El nombre del usuario.
szSoftware	Tipo: Cadena
	El nombre del antivirus de McAfee instalado en la máquina de informes.
szSoftwareVersion	Tipo: Cadena
	La versión del antivirus.
szComputerName	Tipo: Cadena
	El nombre de la máquina que informa de los eventos.
uYear	Tipo: Entera (0000-9999)
	El año del evento.
uMonth	Tipo: Entera (1-12)
	El mes del evento.
uDay	Tipo: Entera (1-31)
	El día del evento.
uHour	Tipo: Entera (0-23)
	La hora del evento.
uMinute	Tipo: Entera (0-59)
	El minuto del evento.
uSecond	Tipo: Entera (0-59)
	El segundo del evento.

Opciones de línea de comando de VirusScan para DOS

La siguiente tabla ofrece una lista de todas las opciones que puede utilizar si ejecuta el programa de línea de comando de DOS, SCAN.EXE. Para ejecutar SCAN.EXE, utilice el comando cd para cambiar los directorios a la carpeta donde se instaló VirusScan. Luego, escriba scan /? para mostrar una lista de opciones y descripciones de cómo pueden utilizarse.

Notas

- Al especificar un nombre de archivo como parte de una opción de línea de comando, debe incluir la ruta de acceso completa del archivo si está ubicado en la carpeta donde VirusScan está instalado.
- Estas opciones sólo están disponibles para SCAN.EXE y sólo pueden utilizarse en el indicador de la línea de comando de DOS.

Consejo

- Para explorar todas las unidades del sistema (incluidas las unidades comprimidas y las unidades de CD-ROM y PCMCIA asignadas localmente, excepto disquetes) en busca de virus, ingrese el siguiente comando:

  scan /adl

Opción de la línea de comando	Descripción
`/?` o `/HELP`	No explora, sino que muestra una lista de opciones de línea de comando de VirusScan con una breve descripción de cada una. Utilice sólo una de estas opciones en la línea de comando (y no junto con otras opciones).
/ADL	Explora todas las unidades locales (incluidas las comprimidas y las de CD-ROM y PCMCIA, excepto disquetes), así como las especificadas en la línea de comando. Para explorar las unidades locales y de red, use /ADL y /ADN conjuntamente en la misma línea de comando.
/ADN	Explora todas las unidades de red en busca de virus, así como las especificadas en la línea de comando. Para explorar las unidades locales y de red, utilice /ADL y /ADN en la misma línea de comando.
/nombre de archivo AF	Almacena códigos de validación/recuperación en el *nombre de archivo*. Le ayuda a detectar virus nuevos o desconocidos. /AF registra información de validación/recuperación para archivos ejecutables, el sector de arranque y el registro de arranque maestro en la unidad de disco duro o de disquete del archivo especificado. El archivo de registro está validado en cerca de 89 bytes por archivo. Debe especificar un *nombre de archivo*, que puede incluir una ruta de acceso. Si la ruta es una unidad de red, debe disponer de derechos para poder crear y borrar archivos en dicha unidad. Si el *nombre de archivo* ya existe, VirusScan lo actualiza. /AF agrega cerca de 300% de tiempo adicional a la exploración. */AF lleva a cabo la misma función que /AV, pero almacena la información en un archivo diferente en lugar de cambiar los archivos ejecutables.* La opción /AF no almacena ninguna

	información acerca del registro de arranque maestro o del sector de arranque de la unidad que está siendo explorada.
carpeta /ALERTPATH	Especifica la carpeta de red Alerta centralizada controlada por NetShield. Véase Alerta centralizada.
/ALL	Sobrescribe la configuración predeterminada explorando todos los archivos. Esta opción aumenta substancialmente el tiempo de exploración requerido. Utilícela si ha encontrado un virus o sospecha que pueda haber uno. *La lista de extensiones para archivos ejecutables estándar ha cambiado respecto a las versiones anteriores de VirusScan.*
/APPEND	Utilizada junto con /REPORT, adjunta el texto de mensaje del informe al archivo de informe específico, si existe. De lo contrario, la opción /REPORT lo sobrescribe.
/AV	Para ayudarle a detectar y recuperar datos dañados por virus nuevos o desconocidos, /AV agrega información de recuperación y validación a cada archivo ejecutable estándar (.EXE, .COM, .SYS, .BIN, .OVL y .DLL), aumentando el tamaño de cada archivo en 98 bytes. Para actualizar los archivos en una unidad de red compartida, debe actualizar primero los derechos de acceso. Para excluir los archivos que se automodifican o autocomprueban, así como los archivos dañados que podrían provocar falsas alarmas, utilice la opción /EXCLUDE. Al utilizar las opciones /AV, /CV o /RV conjuntamente en la misma línea de comando aparece un mensaje de error. *La opción /AV no almacena ninguna información acerca del registro de arranque maestro o del sector de arranque de la unidad que está siendo explorada.*
/BOOT	Sólo explora el sector de arranque y el registro de arranque maestro en la unidad especificada.
nombre de archivo /CF	Le ayuda a detectar virus nuevos o desconocidos. Comprueba la información de validación almacenada por la opción /AF en el *nombre de archivo*. Si un área de archivo o sistema ha cambiado, VirusScan informará que es posible que se haya producido una infección vírica. La opción /CF agrega cerca de 250% de tiempo adicional a la exploración. Al utilizar las opciones /AV, /CV o /RV conjuntamente en la misma línea de comando aparece un mensaje de error. *Algunas PC Hewlett-Packard y Zenith más antiguas modifican el sector de arranque cada vez que se arranca el sistema. Si utiliza /CF, VirusScan*

	informa continuamente que el sector de arranque se modificó aunque no exista ningún virus. Consulte el manual de referencia de la computadora para determinar si su PC tiene un código de arranque que se automodifica.
/CLEANDOC	Sólo limpia virus de archivos infectados de Microsoft Word.
/CLEANDOCALL	Elimina todas las macros de archivos infectados de Microsoft Word.
nombre de archivo/ CONTACTFILE	Identifica un archivo que contiene una cadena de mensaje que aparece si se encuentra un virus. Esta opción es especialmente útil en entornos de red, porque puede mantener el texto del mensaje de una forma fácil en un archivo central en lugar de en cada estación de trabajo. Todos los caracteres son válidos excepto la barra invertida (\). Los mensajes que empiezan con una barra inclinada (/) o un guión (-) deberían estar entre comillas.
/CV	Le ayudan a detectar virus nuevos o desconocidos. Comprueba la información de validación agregada por la opción /AV. Si se modifica un archivo, VirusScan le informa de que es posible que se haya producido una infección vírica. La opción /CV agrega cerca de un 50% de tiempo adicional a la exploración. Al utilizar las opciones /AV, /CV o /RV conjuntamente en la misma línea de comando aparece un mensaje de error. *La opción /CV no comprueba los cambios en el sector de arranque.*
/DEL	Borra los archivos infectados. Una vez eliminados, los restaura a partir de la copia de respaldo.
nombre de archivo /EXCLUDE	Excluye todos los archivos de la lista *nombre de archivo* de la exploración. Esta opción le permite excluir los archivos de la validación /AF y /AV y de la comprobación /CF y /CV. Los archivos que se automodifican o autocomprueban pueden provocar falsas alarmas durante una exploración.
/FAST	Acelera la exploración. Reduce el tiempo de exploración cerca de un 15%. Mediante la opción /FAST, VirusScan examina una sección pequeña de cada archivo en busca de virus. Con /FAST es posible que no se detecten algunas infecciones que podrían encontrarse con una exploración más completa (pero más lenta). No utilice esta opción si ha encontrado un virus o sospecha de la existencia de uno.
/FORCE	Utiliza el registro de virus genérico al limpiar virus de tabla de partición.
horas /FREQUENCY	El número de horas que debe pasar entre exploraciones (Ejemplo:

	/FREQUENCY 1). En entornos donde el riesgo de una infección vírica es muy bajo, utilice esta opción para evitar exploraciones innecesarias o demasiado frecuentes. Cuanto más bajo sea el número de *horas* especificado, más altas serán las frecuencias de exploración y la protección contra infección.
nombre de archivo/LOAD	Lleva a cabo una exploración mediante la información guardada en el *nombre de archivo*. Puede almacenar todas las configuraciones personalizadas en un archivo de configuración diferente (un archivo de texto ASCII), utilice /LOAD para cargar dichas configuraciones desde este archivo.
/LOCK	Bloquea el sistema para prevenir cualquier otra infección si VirusScan encuentra un virus. /LOCK es adecuado en entornos de red especialmente vulnerables, como salas de computadoras abiertas al público. Si usa /LOCK, recomendamos que utilice /CONTACTFILE para comunicar a los usuarios qué hacer o a quién contactar si se encuentra un virus y el sistema se bloquea.
/LOG	Almacena la fecha y la hora en que se ejecuta VirusScan mediante la actualización o creación de un archivo denominado SCAN.LOG en la raíz de la unidad actual.
/MANY	Explora múltiples disquetes en una sola unidad de forma consecutiva. VirusScan le va solicitando cada disquete. Una vez haya comprobado que el sistema está libre de virus, utilice esta opción para comprobar múltiples disquetes de una manera rápida. El programa VirusScan debe estar en un disco que no se retire durante la exploración. Por ejemplo, si está explorando discos en la unidad A: de la computadora y está ejecutando el programa desde un disco en la unidad A:, el programa no estará disponible tan pronto como retire el disquete para introducir otro. El siguiente comando provoca un error durante la ejecución: a:\scan a: /many
/MAXFILESIZE xxx.x	Especifica el tamaño máximo de archivos explorados en busca de virus.
/MEMEXCL	Excluye el área de memoria de la exploración. (El comando predeterminado es A000-FFFF, 0000=Scan all.) Esta opción de línea de comando se ha agregado para evitar que VirusScan explore áreas en la memoria alta que podrían contener hardware con memoria asignada, lo cual podría provocar falsas alarmas.

directorio /MOVE	Traslada todos los archivos infectados que se hayan encontrado durante la exploración al directorio especificado. Para preservar la estructura de la unidad y del directorio, esta opción no surte efecto si el registro de arranque maestro o el sector de arranque está infectado, ya que éstos no son archivos realmente .
/NOBEEP	Desactiva la señal que suena cada vez que VirusScan encuentra un virus.
/NOBREAK	Desactiva ctrl-c y ctrl-break durante las exploraciones. Los usuarios no podrán detener las exploraciones que se estén efectuando mediante ctrl-c o ctrl-break. Utilice esta opción juntamente con /LOG para crear una forma de control eficaz mediante exploraciones programadas a intervalos regulares.
/NOCOMP	No comprueba los archivos ejecutables comprimidos creados con los programas de compresión LZEXE o PKLITE. Reduce el tiempo de exploración cuando no se necesita una exploración completa. De lo contrario, VirusScan comprueba por defecto todos los archivos ejecutables o que se autodescomprimen que se hayan creado mediante programas como LZEXE o PKLITE. VirusScan descomprime cada archivo en la memoria y busca firmas de virus, que es un proceso lento pero ofrece resultados más fiables. Si utiliza /NOCOMP, VirusScan no busca virus en los archivos comprimidos, aunque puede comprobar si se han realizado modificaciones en dichos archivos mediante códigos de validación/recuperación.
/NODDA	No hay acceso directo al disco. Impide a VirusScan acceder al registro de arranque. Esta característica se ha agregado para que VirusScan pueda ejecutarse a Windows NT. Puede que tenga que utilizar esta opción en algunos controladores de dispositivo.
/NODOC	Ignora la exploración de archivos Microsoft Word.
/NOEMS	Impide a VirusScan utilizar memoria ampliada (LIM EMS 3.2) de modo que EMS esté disponible para otros programas.
/NOEXPIRE	Desactiva el mensaje de “fecha de expiración” si los archivos de datos de VirusScan no están actualizados.
/NOMEM	Reduce el tiempo de exploración ignorando todas las búsquedas de virus en memoria. Use /NOMEM sólo cuando esté absolutamente seguro de que la memoria está limpia de virus. VirusScan puede buscar los virus informáticos conocidos más importantes en la memoria del sistema. Además de explorar la memoria del sistema de 0kb

	a 640kb, VirusScan también puede realizar búsquedas de 640kb a 1088kb, en sistemas 286 y posteriores. Actualmente, la memoria superior a 1088kb no es vulnerable a los virus, ya que el procesador no tiene acceso directo a la misma.
/PAUSE	Activa una pausa en la pantalla. Si especifica /PAUSE, aparece el mensaje “Presione cualquier tecla para continuar” cuando VirusScan llena una pantalla de mensajes (por ejemplo, al utilizar las opciones /SHOWLOG o /VIRLIST). De lo contrario, VirusScan llenará y desplazará por defecto la pantalla sin parar, lo cual permite ejecutar este programa en PC que tengan muchos controladores o que padecen infecciones graves, sin tener que asistir al proceso. Es recomendable no usar /PAUSE al guardar un registro de los mensajes de VirusScan mediante las opciones de informe (/REPORT, /RPTCOR, /RPTMOD y /RPTERR).
/PLAD	Guarda las últimas fechas de acceso (sólo en controladores propietarios). Impide que la última fecha de acceso almacenada en la unidad de red en una red propietaria. Normalmente, las unidades de red propietarias actualizan la última fecha de acceso cuando VirusScan abre y examina un archivo. Sin embargo, algunos sistemas de copia de respaldo de cinta utilizan esta última fecha de acceso para decidir si van a realizar una copia del archivo. Utilice /PLAD para asegurarse que la última fecha de acceso no cambia como resultado de la exploración.
nombre de archivo /REPORT	Crea un informe de archivos infectados y errores del sistema. Guarda el resultado de VirusScan en *nombre de archivo* en formato de archivo de texto ASCII. Si el *nombre de archivo* existe, /REPORT lo borra y lo sustituye (o, si utiliza /APPEND, agrega la información del informe al final del archivo existente). Puede incluir la unidad y el directorio de destino (como D:\VSREPRT\ALL.TXT), pero si la unidad de destino es una unidad de red, debe tener derechos de acceso para crear y borrar archivos en ella. También puede usar /RPTALL, /RPTCOR, /RPTMOD, y /RPTERR para agregar archivos explorados, dañados, modificados y errores del sistema al informe.
nombre de archivo /RF	Elimina la información de recuperación y validación del *nombre de archivo* creado por la opción /AF. Si el *nombre de archivo* reside en una unidad de red compartida, podrá borrar archivos en ella. Si utiliza las opciones /AF, /CF y /RF conjuntamente en la misma línea de comando,

	aparecerá un mensaje de error.
/RPTALL	Agrega un lista de archivos explorados al archivos de informe (utilizado mediante /REPORT).
/RPTCOR	Cuando se utiliza junto con /REPORT, agrega los nombres de los archivos dañados al informe. Un archivo dañado puede haber sido atacado por un virus. Puede utilizar /RPTCOR con /RPTMOD y /RPTERR en la misma línea de comando. *Es posible que se den falsas lecturas en algunos archivos que requieren un recubrimiento u otro ejecutable para ejecutarse adecuadamente (es decir, un archivo que no puede ejecutarse en solitario).*
/RPTERR	Agrega una lista de errores del sistema al archivo de informe. Esta opción se utiliza junto con /REPORT. Los errores del sistema incluyen problemas de lectura o escritura en un disquete o disco duro, de sistema de archivo, de red, de creación de informes y otros problemas relacionados con el sistema. Puede usar /RPTERR con /RPTCOR y /RPTMOD en la misma línea de comando.
/RPTMOD	Agrega una lista de los archivos modificados en el archivo de informe. Esta opción se utiliza junto con /REPORT. VirusScan identifica los archivos modificados cuando los códigos de validación/recuperación no coinciden (mediante las opciones /CF o /CV). Puedes utilizar /RPTMOD con /RPTCOR y /RPTERR en la misma línea de comando.
/RV	Elimina la información de validación y recuperación de los archivos validados con la opción /AV. Para actualizar los archivos en una unidad de red compartida, debe disponer de derechos de acceso. Si utiliza las opciones /AV, /CV y /RV conjuntamente en la misma línea de comando, aparecerá un mensaje de error.
/SHOWLOG	Muestra el contenido de SCAN.LOG. SCAN.LOG almacena la fecha y la hora en que VirusScan se ejecuta mediante la actualización o creación de un archivo denominado SCAN.LOG en el directorio actual, mientras la fecha y la hora de las exploraciones previas registradas en SCAN.LOG se almacenan mediante el conmutador /LOG. El archivo SCAN.LOG contiene texto y otros formatos especiales. Si desea que se efectúe una pausa cuando la pantalla se llena de mensajes, especifique la opción /PAUSE.
/SUB	Explora los subdirectorios de un directorio. Por defecto, cuando se especifica una

	exploración en un directorio en lugar de una unidad, VirusScan examinará sólo los archivos que contiene e ignorará los subdirectorios. Mediante /SUB podrá explorar todos los subdirectorios de los directorios especificados. No utilice /SUB si está explorando toda una unidad.
/VIRLIST	Muestra el nombre y una breve descripción de todos los virus detectados por VirusScan. Si desea que se efectúe una pausa cuando la pantalla se llena de mensajes, especifique la opción /PAUSE. Utilice la opción /VIRLIST sola o junto con /PAUSE en la línea de comando. Puede guardar la lista de nombres y descripciones de virus en un archivo si redirige la acción de un comando. Por ejemplo, en DOS, ingrese: scan /virlist > nombredearchivo.txt *Dado que VirusScan puede detectar muchos virus, este archivo tiene más de 250 páginas.*

Tipo

Especifica el tipo de archivo infectado (por ejemplo, ejecutable, Word, Excel).

Ubicación

Especifica la ubicación del directorio donde se encuentra el archivo infectado.

Tamaño

Especifica el tamaño del archivo infectado.

Nombre en MS-DOS

Especifica el nombre del archivo infectado.

Creado

Especifica la fecha en que se creó el archivo infectado.

Modificado

Especifica la fecha en que se modificó el archivo infectado por última vez.

Con acceso

Especifica la fecha en que el archivo infectado se accedió por última vez.

Sólo lectura

Especifica si el archivo es de sólo lectura.

Oculto

Especifica si el archivo está oculto.

Modificado

Especifica si el archivo está modificado.

Sistema

Especifica si se trata de un archivo del sistema.

Relativo al contexto, a continuación

Archivos de programa

Los archivos de programa son los tipos de archivo más vulnerables a las infecciones víricas. Éstos incluyen los archivos .COM, .EXE, .DO?, .XL?. Para cambiar los tipos de archivo en los que efectuar búsquedas de virus, complete el siguiente procedimiento:

1 Haga clic en **Extensiones**. Aparece el cuadro de diálogo Extensiones de archivos de programa.

2 Para agregar una extensión de archivo a la exploración, haga clic en Agregar. Ingrese una nueva extensión de archivo y haga clic en **Aceptar**. Repita esta acción hasta haber ingresado todas las extensiones de archivo deseadas.

3 Para borrar una extensión, selecciónela y haga clic en Eliminar.

4 Para volver a las extensiones predeterminadas, haga clic Predeterminadas.

5 Para salir sin guardar cambios en la lista de archivos de programa, haga clic en Cancelar. Para guardar los cambios y salir, haga clic en **Aceptar**.

Agregar un elemento de exclusión

1 Ingrese la ruta de acceso completa al archivo, unidad o carpeta en cuestión o haga clic en **Examinar** para ubicarla.
2 Para excluir subcarpetas de la exploración, seleccione la casilla de verificación Incluir subcarpetas.
3 Para excluir el elemento de la exploración de archivos, seleccione la casilla de verificación Exploración de archivos.
4 Para excluir el elemento de la exploración del sector de arranque, seleccione la casilla de verificación Exploración del sector de arranque.
5 Para agregar un elemento de exclusión, haga clic **Aceptar**. Para salir sin agregar el elemento de exclusión, haga clic en **Cancelar**.

Notas

- Para editar un elemento de exploración, selecciónelo y haga clic en **Editar**.
- Para eliminar un elemento de exploración, selecciónelo y haga clic en **Eliminar**.

Agregar un elemento de exploración

Seleccione una de las opciones siguientes:

- Para explorar todas las unidades conectadas a esta computadora, haga clic en Seleccionar elemento a explorar y escoja Mi PC.
- Para explorar todos los medios extraíbles, incluidas las unidades de disquete, haga clic en Seleccionar elemento a explorar y escoja Todos los medios extraíbles.
- Para explorar todas las unidades de disco duro conectadas a esta computadora, haga clic en Seleccionar elemento a explorar y escoja Todos los discos duros.
- Para explorar todas las unidades de red asignadas, haga clic en Seleccionar elemento a explorar y seleccione Todas las unidades de red.
- Para explorar una unidad o carpeta individual, haga clic en Seleccionar elemento a explorar e ingrese la ruta de acceso del elemento o bien haga clic en **Examinar** para ubicar una.

Después de seleccionar un elemento de exploración, haga clic en **Aceptar**. Para salir sin agregar un elemento de exploración, haga clic en **Cancelar**.

Para cambiar la contraseña

1 Ingrese una nueva contraseña.
2 Vuelva a ingresar la contraseña.

Lista de virus

La lista de virus le proporciona información básica aunque vital acerca de sus virus. Para obtener dicha información, complete el siguiente procedimiento:

Desplácese por la lista para encontrar los virus o haga clic en **Buscar virus** e ingrese el nombre del virus.

Resalte el virus y haga clic en **Información acerca del virus**. Aparece la página Información acerca del virus.

Esta información comprende:

Información acerca del virus, incluidos:
Nombre del virus
Infecta
Tamaño del virus

Características, incluidos:
Residente en memoria
Codificado
Polimórfico
Reparable
Virus de macro

Información acerca del virus

Este cuadro de diálogo contiene la siguiente información:

Información acerca del virus

Nombre del virus
Infecta
Tamaño del virus

Características

Residente en memoria
Codificado
Polimórfico
Reparable
Virus de macro

Información acerca del elemento

Este cuadro de diálogo contiene la siguiente información:

Nombre del virus

Información acerca del archivo
Tipo
Ubicación
Tamaño

Nombre en MS-DOS y fechas
Nombre en MS-DOS
Creado
Modificado
Con acceso

Atributos del archivo
Sólo lectura
Oculto
Modificado
Sistema

Abre el cuadro de diálogo Agregar elemento de exploración, donde puede agregar un elemento a explorar.

Cuando está activada, la tarea VShield puede desactivarse desde la barra de tareas o la Consola.

Cierra la biblioteca de información acerca de virus.

Cierra la lista de virus.

Abre la hoja de propiedades de configuración donde puede configurar la tarea.

Indica la fecha en que se creó el archivo.

Al activarse, aparecerá un mensaje personalizado si se detecta algún virus.

Abre el cuadro de diálogo Editar elemento de exploración, donde puede editar el elemento de exploración seleccionado.

Activa la planificación.

Indica si se trata de un virus codificado.

Abre el cuadro de diálogo Agregar elemento de exclusión, donde puede agregar un elemento de exclusión.

Enumera los elementos excluidos de la exploración.

Abre el cuadro de diálogo Editar elemento de exclusión, donde puede editar el elemento de exclusión seleccionado.

Borra el elemento de exclusión seleccionado.

Abre el cuadro de diálogo Encontrar virus, donde puede encontrar un virus si ingresa el nombre del mismo.

Indica los tipos de archivos infectados por este virus. Éstos pueden ser:
Ejecutables (.EXE)
Archivos COM (.COM)
Archivos de Word (.DO?)
Archivos de Excel (.XL?)

Al activarse, todas las copias de esta tarea quedarán automáticamente protegidas con contraseña.

Al activarse, se limita el tamaño del archivo de registro.

Al activarse, VShield se cargará automáticamente al arrancar.

Al activarse, se registra la actividad de limpieza de archivos infectados.

Al seleccionarse, se registran las horas de inicio de la exploración.

Al seleccionarse, se registra la actividad de eliminación de archivos infectados.

Al seleccionarse, se registra la actividad de detección de archivos infectados.

Abre el cuadro de diálogo Examinar, donde puede seleccionar la ubicación de un archivo de registro.

Al seleccionarse, se registra la actividad de traslado de archivos infectados.

Al seleccionarse, se registra la configuración de la sesión.

Al seleccionarse, se registran los resúmenes de la actividad de exploración.

Al seleccionarse, se mantiene un archivo de registro de actividad de los virus.

Al seleccionarse, se registra el nombre del usuario.

Indica si se trata de un virus de macro. Los virus de macro infectan archivos de Microsoft Word y de Excel.

Indica si el virus reside en la memoria.

Abre el cuadro de diálogo Examinar, donde puede seleccionar un área de cuarentena.

Le permite ingresar la ubicación de un área de cuarentena.

Abre el cuadro de diálogo Examinar, donde puede seleccionar un servidor para que éste reciba los mensajes de Alerta centralizada.

Muestra el virus siguiente.

Le permite ingresar los parámetros necesarios para el archivo ejecutable.

Indica si se trata de un virus polimórfico. Los virus polimórficos modifican el código para evitar ser detectados.

Muestra el virus anterior.

Muestra la ruta de acceso al archivo ejecutable del programa.

Abre el cuadro de diálogo Examinar, donde puede ubicar el archivo ejecutable del programa.

Al activarse, la opción Limpiar los archivos infectados automáticamente estará disponible si se detecta un virus.

Al activarse, la opción Continuar la exploración (sin llevar a cabo ninguna acción) estará disponible si se detecta un virus.

Al activarse, la opción Borrar los archivos infectados automáticamente estará disponible si se detecta un virus.

Al activarse, la opción Excluir estará disponible si se detecta un virus.

Al activarse, la opción Trasladar los archivos infectados automáticamente estará disponible si se detecta un virus.

Al activarse, la opción Detener exploración estará disponible si se detecta un virus.

Enumera las páginas de propiedades que están protegidas. Las páginas de propiedades protegidas van precedidas de  , mientras que las no protegidas van precedidas de
 .

Abre el cuadro de diálogo Contraseña, donde puede seleccionar una contraseña.

Borra el elemento de exploración seleccionado.

Indica si el archivo infectado puede limpiarse.

Selecciona si la tarea se ejecutará de forma minimizada, maximizada o en una ventana normal.

Ejecuta la tarea inmediatamente.

Selecciona el tipo de respuesta que ofrece VirusScan o VShield ante un archivo infectado.

Al seleccionarse, se exploran todos los tipos de archivo. Aunque de este modo se consigue una exploración exhaustiva, el tiempo de exploración aumentará significativamente.

Al seleccionarse, esta tarea explorará en busca de virus de sector de arranque.

Al seleccionarse, se exploran los archivos comprimidos.

Nota

- El escáner manual de VirusScan explora los archivos PKZIP, PKLITE, WinZip, LZH y LZEXE.
- VShield explora los archivos PKLITE y LZEXE.

No existe ningún tema de ayuda relacionado con este elemento.

Abre el cuadro de diálogo Extensiones de archivos de programa, donde pueden seleccionarse los tipos de archivo que deben explorarse en busca de virus. Por defecto, se explorarán los archivos COM (.COM), los ejecutables (.EXE), los de Word (.DO?) y los de Excel (.XL?).

Seleccione un elemento a explorar.

Abre el cuadro de diálogo Examinar, donde puede seleccionar la unidad de disco o la carpeta a explorar.

Enumera los elementos de exploración actualmente configurados.

Abre el cuadro de diálogo Examinar, donde puede seleccionar una ubicación a explorar.

Al seleccionarse, se explorará la memoria del sistema antes de que VirusScan comience a explorar unidades de disco.

Al seleccionarse, VShield explora en busca de virus de sector de arranque en los discos flexibles.

Al seleccionarse, VShield explora en busca de virus cuando se copia un archivo.

Al seleccionarse, VShield explora en busca de virus cuando se crea un archivo.

Al seleccionarse, VShield explora en busca de virus cuando se cambia el nombre a un archivo.

Al seleccionarse, VShield explora en busca de virus de sector de arranque cuando se ejecuta un archivo.

Al seleccionarse, VShield explora en busca de virus de sector de arranque al cerrar el sistema.

Al seleccionarse, sólo se exploran los tipos de archivo que son vulnerables a las infecciones víricas. Para cambiar los tipos de archivos a explorar, haga clic en **Extensiones**.

No existe ningún tema de ayuda relacionado con este elemento.

Seleccione una unidad o carpeta a explorar o haga clic en Examinar para ubicar una de ellas.

Indica que la tarea se ejecutará en las fechas seleccionadas a la hora especificada.

Seleccione en qué día de la semana debe ejecutarse la tarea.

Indica que la tarea se ejecutará todos los viernes a la hora especificada.

Indica que la tarea se ejecutará una vez cada hora.

Indica que la tarea se ejecutará todos los lunes a la hora especificada.

Seleccione en qué mes debe ejecutarse la tarea.

Indica que la tarea se ejecutará una vez al mes en el día y la hora especificados.

Indica que la tarea se ejecutará una vez en la fecha y la hora especificados.

Indica que la tarea se ejecutará todos los sábados a la hora especificada.

Indica que la tarea se ejecutará todos los domingos a la hora especificada.

Indica que la tarea se ejecutará todos los jueves a la hora especificada.

Indica que la tarea se ejecutará todos los martes a la hora especificada.

Indica que la tarea se ejecutará todos los miércoles a la hora especificada.

Indica que la tarea se ejecutará todas las semanas en el día y la hora especificados.

Activa la Alerta centralizada, que es la solución ideada por McAfee para avisar a toda una compañía la existencia de un virus. Una vez configuradas, las estaciones de trabajo que ejecuten VirusScan envían notificaciones sobre virus a los servidores que ejecutan NetShield. Esto permite a los administradores localizar la fuente de las infecciones víricas y evitar que se extiendan.

Al activarse, el icono VShield aparece en la barra de tareas.

Al activarse, se emitirá una señal audible cuando se detecte un virus.

Al activarse, esta tarea se iniciará automáticamente al abrirse.

Muestra el directorio de trabajo del archivo ejecutable.

Abre el cuadro de diálogo Examinar, donde puede seleccionar el directorio de trabajo del archivo ejecutable.

Activa y desactiva la barra de estado.

Indica el número de archivos infectados que se han limpiado.

Indica el número de archivos infectados que se han borrado.

Indica el número de archivos infectados que se han encontrado.

Indica cúando se inició la tarea por última vez.

Indica el número de archivos infectados que se han trasladado a la carpeta de cuarentena.

Especifica cúando se ejecutará la tarea por próxima vez.

Indica el número total de archivos explorados.

Al seleccionarse, se exploran todas las subcarpetas del elemento.

Muestra el nombre de la tarea. Para seleccionar un nuevo nombre, ingrese uno y haga clic en Aplicar.

Activa y desactiva la barra de título.

Activa y desactiva la barra de herramientas.

No existe ningún tema de ayuda relacionado con este elemento.

Enumera los virus. Para encontrar un virus específico, haga clic Encontrar virus e ingrese el nombre del virus o utilice la barra de desplazamiento.

Abre el cuadro de diálogo Información acerca del virus, que describe las características del virus.

Indica el nombre del virus.

Indica el tamaño del virus.

Abre el cuadro de diálogo Examinar, donde puede seleccionar el elemento a excluir.

Ingresa la ruta de acceso a la unidad de disco, carpeta o archivo a excluir.

Al seleccionarse, no se explora el sector de arranque del elemento.

Al seleccionarse, no se exploran los archivos del elemento.

Al seleccionarse, no se exploran las subcarpetas del elemento.

Indica cuándo se accedió al archivo por última vez.

Especifica si el archivo está modificado.

Especifica las características de los archivos. Estas características indican si el archivo está oculto, es de sólo lectura, está modificado o es un archivo del sistema.

Especifica la fecha de creación del archivo.

Indica si el archivo está oculto.

Especifica la ubicación del archivo.

Especifica cuándo se modificó el archivo por última vez.

Especifica el nombre del archivo.

Indica si el archivo es de sólo lectura.

Especifica el tamaño del archivo.

Indica si el archivo es un archivo de sistema.

Indica el tipo de archivo. Los tipos más comunes de archivos infectados son: archivos COM, ejecutables, archivos de Word o archivos de Excel.

Enumera las características del virus.

Limpia el archivo infectado.

Borra el archivo infectado.

Especifica los tipos de archivos que este virus infecta.

Abre el cuadro de diálogo Examinar de modo que puede trasladar el archivo infectado a una carpeta de cuarentena.

Especifica el estado del archivo infectado.

Especifica el nombre del virus.

Especifica el tamaño del virus.

Le permite ingresar una extensión de archivo de programa de tres letras (por ejemplo, .EXE, .COM).

Cierra esta página sin aplicar ningún cambio.

Cierra esta página.

Abre un tema de ayuda relacionado con el contexto para esta página.

Aplica los cambios y sale de esta página.

Le permite ingresar una contraseña.

Le permite volver a ingresar la contraseña.

Le permite ingresar la contraseña de la tarea.

Abre la página de propiedades de configuración, donde puede configurar la tarea.

Inicia la tarea.

Selecciona el tamaño máximo de un archivo de registro (en kilobytes).

Devuelve todos los parámetros de exploración a la configuración predeterminada.

Comienza la exploración de acuerdo con los parámetros elegidos.

Detiene la exploración.

Le permite seleccionar en qué minuto después de cada hora desea que se ejecute esta tarea.

Le permite seleccionar en qué día de la semana desea que se ejecute esta tarea.

Le permite seleccionar en qué día del mes desea que se ejecute la tarea.

Le permite seleccionar en qué mes desea que se ejecute la tarea.

Seleccione en qué día de la semana desea que se ejecute la tarea.

Enumera los tipos de archivos de programa que se han comprobado en busca de virus.

Carga la lista predeterminada de extensiones de archivos de programa.

Abre el cuadro de diálogo Agregar extensión de archivo de programa, donde puede agregar una nueva extensión de archivo.

Elimina la extensión seleccionada.

Muestra el nombre del archivo infectado.

Muestra el nombre del virus.

Aplica los cambios sin salir de esta página.

Detiene esta tarea.

Activa VShield.

Desactiva VShield.

Abre la página de propiedades de información, que contiene datos acerca del virus y del archivo infectado.

Limpia el archivo infectado.

Continúa la exploración sin llevar a cabo ninguna acción. Cuando la exploración se ha completado, pueden realizarse acciones manualmente en cada archivo infectado.

Borra el archivo infectado.

Continúa la exploración sin llevar a cabo ninguna acción y excluye este archivo de futuras exploraciones.

Nota

- No se recomienda esta acción a menos que el archivo esté generando una falsa alarma.

Traslada el archivo infectado a una carpeta de cuarentena.

Detiene la exploración y le devuelve a la ventana principal.

Muestra las características del virus. Estas características indican si el virus es residente en memoria, codificado, polimórfico y si los archivos infectados pueden repararse.

Parámetros de la línea de comando de VirusScan para Windows

Las siguientes opciones deben utilizarse con VirusScan para Windows95 y no con VirusScan para DOS. Dichas opciones pueden usarse como parámetros de línea de comando con funciones rápidas e iconos para controlar el estado de VirusScan al ejecutarlo:

- **/NoSplash:** Suprime la pantalla inicial de VirusScan
- **/AutoScan:** Inicia la exploración de forma automática