

Avira AntiVir Professional

Manual para usuarios

Marcas comerciales y Copyright

Marcas comerciales

AntiVir es una marca registrada de Avira GmbH.

Windows es una marca registrada de Microsoft Corporation in the EEUU y otros países.

Todas las marcas y productos mencionados son propiedad de sus respectivos propietarios.

Las marcas protegidas no se utilizan como tales en este manual. Esto no significa, de todas formas, que pueden usarse libremente.

Información de Copyright

Para Avira AntiVir Professional, se ha utilizado código de otros proveedores. Agradecemos a los titulares de los derechos de autor que hayan puesto su código a nuestra disposición. Encontrará más información sobre los derechos de autor Licencias de terceros de la ayuda de Avira AntiVir Professional, en Licencias de terceros.

Contenido

1	Introducción	1
2	Símbolos y resaltados	2
3	Información de producto	3
3.1	Gama de prestaciones	3
3.2	Requisitos del sistema	4
3.3	Concesión de licencia y actualización a nuevas versiones	5
3.3.1	Administración de licencias	5
4	Instalación y desinstalación	7
4.1	Instalación.....	7
4.2	Instalación diferencial	11
4.3	Módulos de instalación.....	12
4.4	Desinstalación.....	13
4.5	Instalación y desinstalación en la red	13
4.5.1	Instalación en la red.....	14
4.5.2	Desinstalación en la red.....	14
4.5.3	Parámetros de línea de comandos para el programa de instalación.....	15
4.5.4	Parámetros del fichero setup.inf	16
5	Información general	20
5.1	Interfaz de usuario y uso	20
5.1.1	Centro de control	20
5.1.2	Configuración.....	23
5.1.3	Icono de bandeja	27
5.2	Procedimientos	28
5.2.1	Activar licencia	28
5.2.2	Ejecutar actualizaciones automáticas	28
5.2.3	Iniciar una actualización manualmente.....	30
5.2.4	Análisis directo: analizar la existencia de virus y malware con un perfil de análisis	30
5.2.5	Análisis directo: Analizar la existencia de virus y malware mediante Arrastrar y soltar	32
5.2.6	Análisis directo: analizar la existencia de virus y malware mediante el menú contextual	32
5.2.7	Análisis directo: analizar la existencia de virus y malware de forma automática.....	33
5.2.8	Análisis directo: analizar directamente la existencia de rootkits activos.....	34
5.2.9	Reaccionar a virus y malware detectados.....	34
5.2.10	Cuarentena: tratar con ficheros (*.qua) en cuarentena.....	39
5.2.11	Cuarentena: restaurar los ficheros de cuarentena.....	40
5.2.12	Cuarentena: mover fichero sospechoso a cuarentena.....	42
5.2.13	Perfil de análisis: añadir o eliminar un tipo de fichero de un perfil de análisis ..	42
5.2.14	Perfil de análisis: crear acceso directo en el escritorio para el perfil de análisis ..	43
5.2.15	Eventos: Filtrar eventos.....	43
5.2.16	MailGuard: Excluir direcciones de email del análisis	44
5.2.17	FireWall: Seleccionar nivel de seguridad para FireWall	44

6	Escáner	47
7	Actualizaciones	49
8	Avira FireWall:: Información general	52
9	Solución de problemas, sugerencias	54
9.1	Ayuda en caso de problemas	54
9.2	Atajos.....	58
9.2.1	En los cuadros de diálogo.....	58
9.2.2	En la Ayuda.....	59
9.2.3	En el Centro de control.....	59
9.3	Centro de Seguridad de Windows.....	61
9.3.1	General	61
9.3.2	El Centro de seguridad de Windows y su programa Antivir	61
10	Virus y más	64
10.1	Categorías de riesgos	64
10.2	Virus y otro tipo de Malware.....	67
11	Información y servicio.....	70
11.1	Dirección de contacto	70
11.2	SopORTE Técnico	70
11.3	Archivos sospechosos	70
11.4	Informe falso positivo	71
11.5	Sus observaciones para más seguridad.....	71
12	Referencia: opciones de configuración	72
12.1	Escáner	72
12.1.1	Análisis	72
12.1.1.1.	Acción en caso de detección	75
12.1.1.2.	Acciones adicionales	78
12.1.1.3.	Excepciones	79
12.1.1.4.	Heurística	80
12.1.2	Informe.....	81
12.2	Guard.....	81
12.2.1	Análisis	82
12.2.1.1.	Acción en caso de detección	84
12.2.1.2.	Acciones adicionales	86
12.2.1.3.	Excepciones	87
12.2.1.4.	Heurística	91
12.2.2	ProActiv	92
12.2.2.1.	Filtro de aplicación: Aplicaciones a bloquear	93
12.2.2.2.	Filtro de aplicación: Aplicaciones permitidas	94
12.2.3	Informe.....	95
12.3	MailGuard	96
12.3.1	Análisis	96
12.3.1.1.	Acción en caso de detección	97
12.3.1.2.	Otras acciones	99
12.3.1.3.	Heurística	99
12.3.2	General	100
12.3.2.1.	Excepciones	100
12.3.2.2.	Memoria caché	101
12.3.2.3.	Pie de página	102
12.3.3	Informe.....	102

12.4	Firewall.....	103
12.4.1	Reglas del adaptador	103
12.4.1.1.	Reglas de Entrada.....	106
12.4.1.2.	Reglas de salida	114
12.4.2	Reglas de aplicación	115
12.4.3	Proveedores de confianza.....	117
12.4.4	Configuración.....	118
12.4.5	Configuración de ventanas emergentes.....	119
12.5	FireWall bajo SMC	121
12.5.1	Opciones generales	121
12.5.2	Reglas generales del adaptador	122
12.5.2.1.	Reglas de Entrada.....	125
12.5.2.2.	Reglas de salida	133
12.5.3	Lista de aplicaciones	133
12.5.4	Proveedores de confianza.....	134
12.5.5	Configuración adicional.....	135
12.5.6	Configuración de visualización.....	136
12.6	WebGuard	137
12.6.1	Análisis	138
12.6.1.1.	Acción en caso de detección	138
12.6.1.2.	Accesos bloqueados.....	140
12.6.1.3.	Excepciones	141
12.6.1.4.	Heurística	144
12.6.2	Informe.....	145
12.7	Actualización.....	146
12.7.1	Actualización de producto	147
12.7.2	Configuración del reinicio	148
12.7.3	Servidor de ficheros	149
12.7.4	Servidor Web	149
12.7.4.1.	Proxy.....	150
12.8	General	151
12.8.1	Email.....	151
12.8.2	Categorías de riesgos.....	152
12.8.3	Contraseña	153
12.8.4	Seguridad.....	155
12.8.5	WMI.....	156
12.8.6	Directorios.....	156
12.8.7	Advertencias.....	157
12.8.7.1.	Red.....	157
12.8.7.2.	Email.....	159
12.8.7.3.	Advertencias acústicas.....	166
12.8.7.4.	Advertencias.....	167
12.8.8	Eventos	167
12.8.9	Limitar informes	168

1 Introducción

Con su programa AntiVir protege su equipo frente a virus, gusanos, troyanos, adware y spyware, así como frente a otros riesgos. Para abreviar, en este manual se habla de virus o malware (software malintencionado) y programas no deseados.

El manual describe la instalación y el uso del programa.

En nuestro sitio Web puede utilizar múltiples opciones y otras posibilidades de información:

<http://www.avira.es>

En el sitio Web de Avira puede...

- acceder a información sobre otros programas de escritorio AntiVir
- descargar los programas de escritorio AntiVir más actuales
- descargar los manuales de producto más actuales en formato PDF
- descargar herramientas gratuitas de soporte y reparación
- utilizar la completa base de datos de conocimientos y los artículos de FAQ para solucionar problemas
- acceder a las direcciones de soporte específicas de cada país.

Su equipo Avira

2 Símbolos y resaltados

Se usan los siguientes iconos:

Icono / Denominación	Explicación
✓	Consta delante de una condición que debe cumplirse antes de ejecutar una acción.
▶	Consta delante de un paso de acción que se ejecuta.
→	Consta delante de un resultado que se deduce de la acción precedente.
Advertencia	Consta delante de una advertencia en caso de riesgo de pérdida grave de datos.
Nota	Consta delante de una nota con información especialmente importante o delante de una sugerencia que facilita el entendimiento y uso de su programa AntiVir.

Se usan los siguientes resaltados:

Resaltado	Explicación
<i>Cursiva</i>	Nombre de fichero o indicación de ruta.
	Elementos que se muestran de la interfaz de software (p. ej., título de la ventana, área de la ventana o botones de opción).
Negrita	Elementos en los que se hace clic de la interfaz de software (p. ej., opción de menú, sección o botón).

3 Información de producto

Este capítulo proporciona toda la información relevante para la adquisición y el uso de su programa AntiVir:

- consulte el capítulo: Gama de prestaciones
- consulte el capítulo: Requisitos del sistema
- consulte el capítulo: Concesión de licencia

Los programas AntiVir ofrecen herramientas completas y flexibles para proteger su equipo de forma fiable frente a virus, malware, programas no deseados y otros peligros.

► Tenga en cuenta las siguientes indicaciones:

Nota

La pérdida de datos valiosos suele tener consecuencias dramáticas. Incluso el mejor programa antivirus no puede protegerle totalmente contra la pérdida de datos. Haga regularmente copias de seguridad (backups) de sus datos.

Nota

Un programa que protege frente a virus, malware, programas no deseados y otros peligros sólo es fiable y eficaz si está actualizado. Asegúrese de disponer de la versión más reciente de su programa AntiVir mediante las actualizaciones automáticas. Configure el programa correspondientemente.

3.1 Gama de prestaciones

Su programa AntiVir dispone de las siguientes funciones:

- Centro de control para la supervisión, la administración y el control de todo el programa
- Configuración centralizada con configuración estándar y avanzada fáciles de usar, así como ayuda sensible al contexto
- Escáner (análisis a petición) con análisis controlado por perfil y configurable de todos los tipos conocidos de virus y malware
- Integración en el control de cuentas de usuario (User Account Control) de Windows Vista para poder realizar tareas para las que se requieren derechos de administrador.
- Guard (análisis en acceso) para la supervisión constante de cualquier acceso a los ficheros
- Componente ProActiv para la monitorización permanente de acciones de programas (solamente para sistemas de 32 bits, no disponible bajo Windows 2000)
- MailGuard (escáner de POP3, escáner IMAP y escáner SMTP) para el control permanente de la existencia de virus y malware en los emails. Incluye el análisis de los datos adjuntos a los emails

- WebGuard para la supervisión de los datos y ficheros transmitidos desde Internet mediante el protocolo HTTP (supervisión de los puertos 80, 8080, 3128)
- Administración integrada de cuarentena para aislar y tratar los ficheros sospechosos
- Protección contra rootkits para detectar malware instalado de forma oculta en el sistema del ordenador (denominado rootkit)
(No está disponible en Windows XP 64 Bit)
- Acceso directo a información detallada en Internet acerca de los virus y el malware detectado
- Actualización sencilla y rápida del programa, de las firmas de virus (VDF) y del motor de análisis mediante actualización con un único fichero y actualización incremental del VDF a través de un servidor Web en Internet o en la Intranet
- Concesión de licencias fácil de usar en la administración de licencias
- Programador integrado para programar tareas únicas o periódicas, como actualizaciones o análisis
- Grado de detección muy alto de virus y malware mediante tecnologías de análisis innovadoras (motor de análisis) que incluyen procedimientos de análisis heurísticos
- Detección de todos los tipos de archivo convencionales, incluido la detección de archivos anidados y el reconocimiento de extensiones inteligentes
- Gran rendimiento por su capacidad de subprocesamiento múltiple (análisis simultáneo de muchos ficheros a gran velocidad)
- Avira FireWall para proteger el equipo de accesos no autorizados desde Internet o desde una red, así como de accesos no autorizados a Internet o la red por usuarios no autorizados.

3.2 Requisitos del sistema

Existen los siguientes requisitos del sistema::

- PC Pentium o superior, de un mínimo de 266 MHz
- Sistema operativo
- Windows XP, SP2 (32 o 64 bits) o
- Windows Vista (32 o 64 bits, SP 1)
- Windows 7 (32 o 64 bits)
- Al menos 150 MB de espacio libre en el disco duro (en caso de usar la cuarentena y para la memoria temporal, más)
- Al menos 256 MB de memoria RAM con Windows XP
- Al menos 1024 MB de memoria RAM con Windows Vista, Windows 7
- Para la instalación del programa: derechos de administrador
- Para todas las instalaciones: Windows Internet Explorer 6.0 o superior
- Si fuera necesario, conexión a Internet (consulte Instalación)

3.3 Concesión de licencia y actualización a nuevas versiones

Para poder utilizar su producto AntiVir, es necesaria una licencia. Se deben aceptar las condiciones de licencia.

La licencia se emite por medio de una clave de licencia digital en forma de archivo hbedv.key. Este código de licencia digital es centro neurálgico de su licencia personal. Contiene detalles de los programas que tienen licencia activa y el periodo de validez. Un código de licencia digital por lo tanto también puede contener la licencia de más de un producto.

La clave de licencia digital se envía en un email si ha adquirido su programa AntiVir en Internet o se encuentra en el CD/DVD del programa. Puede cargar la clave de licencia durante la instalación del programa o instalarla posteriormente en la administración de licencias.

3.3.1 Administración de licencias

El administrador de licencia de Avira AntiVir Professional permite una instalación muy simple de la licencia de Avira AntiVir Professional.

Administrador de licencia de Avira AntiVir Professional



Se puede instalar la licencia seleccionando el fichero de licencia en el administrador de licencias o en el email de activación con un doble clic y siguiendo las instrucciones en la pantalla.

Nota

El administrador de licencia de Avira AntiVir Professional copia automáticamente la correspondiente licencia en la carpeta de producto correspondiente. Si la licencia existe ya, aparecerá una nota para indicar que el fichero de licencia será reemplazado. En ese caso, el fichero existente se sobrescribirá con el fichero de licencia actual.

4 Instalación y desinstalación

Este capítulo proporciona información en torno a la instalación y desinstalación de su programa AntiVir:

- consulte el capítulo Instalación: requisitos, tipos de instalación, ejecutar instalación
- consulte el capítulo Módulos de instalación
- consulte el capítulo Instalación diferencial
- Instalación y desinstalación en la red
- consulte el capítulo Desinstalación: ejecutar desinstalación

4.1 Instalación

Antes de la instalación, compruebe si su equipo cumple los requisitos mínimos del sistema. De ser así, puede instalar el programa AntiVir.

Nota

Tiene la posibilidad de crear un punto de restauración durante el proceso de instalación. Un punto de restauración sirve para restablecer en el sistema operativo el estado anterior a la instalación. Si desea utilizar esta opción, asegúrese de que el sistema operativo permite crear puntos de restauración:

Windows XP: Propiedades del programa -> Restauración del sistema: Desactive la opción **Desactivar Restaurar sistema**.

Windows Vista / Windows 7: Propiedades del programa -> Protección del sistema: Marque en el área **Configuración de protección** la unidad en la que está instalada el sistema y pulse el botón **Configurar**. Active en la ventana **Protección del sistema** la opción **Configuración del sistema y restaurar versiones anteriores de fichero**.

Tipos de instalación

Durante la instalación, puede seleccionar un tipo de instalación en el asistente de instalación:

Exprés

- No se instalan todos los componentes de programa disponibles. Los siguientes componentes no se instalan:

Avira AntiVir ProActiv

Avira FireWall

- Los ficheros de programa se instalan en un directorio estándar predefinido en C:\Archivos de programa.
- Su programa AntiVir se instala con la configuración estándar. No dispondrá de la posibilidad de establecer valores predefinidos en el asistente de configuración.

Definido por el usuario

- Tiene la posibilidad de seleccionar determinados componentes del programa para su instalación (consulte el capítulo Instalación y desinstalación::Módulos de instalación).
- Puede seleccionar una carpeta de destino para ubicar los ficheros de programa que se instalarán.
- Puede desactivar la creación de un icono de escritorio y un grupo de programas en el menú Inicio.
- En el asistente podrá establecer valores predefinidos de su programa AntiVir e iniciar un breve análisis del sistema que se ejecutará automáticamente después de la instalación.

Antes de la instalación

- ▶ Cierre su programa de correo. También se recomienda cerrar todas las aplicaciones.
- ▶ Asegúrese de que no existen otras soluciones de protección Antivirus. Si existen diferentes soluciones, podrían interferir entre ellas.
- ▶ Establezca una conexión de Internet. La conexión de Internet es necesaria para ejecutar los siguientes pasos de la instalación
- ▶ Descarga de los ficheros de programa actuales y del motor de análisis, así como de los ficheros de firmas de virus actuales del día mediante el programa de instalación (en instalaciones basadas en Internet)
- ▶ Si fuera necesario, ejecución de una actualización tras finalizar la instalación
- ▶ Guarde el fichero de licencia hbedv.key en su sistema informático si desea activar su programa AntiVir.

Nota

Instalación basada en Internet:

Para la instalación basada en Internet del programa dispone de un programa de instalación que descarga los ficheros de programa actuales de los servidores Web de Avira GmbH antes de ejecutar la instalación. Este procedimiento garantiza que su programa AntiVir se instale con un fichero de firmas de virus actual del día.

Instalación con un paquete de instalación:

El paquete de instalación contiene el programa de instalación y todos los ficheros de programa necesarios. Sin embargo, al instalar con un paquete de instalación no se puede seleccionar el idioma de su programa AntiVir. Se recomienda ejecutar una actualización al acabar la instalación para actualizar el fichero de firmas de virus.

Ejecutar instalación

El programa de instalación te guía durante la misma. Las ventanas contienen diferentes opciones para controlar la instalación.

Los botones más importantes, tienen asignadas las siguientes funciones:

- **Aceptar:** Confirmar acción.
- **Cancelar:** Cancelar acción.
- **Siguiente:** Continuar con el siguiente paso.
- **Anterior:** Volver al paso anterior.

Así se instala su programa AntiVir:

Nota

Las acciones que se describen a continuación para desactivar el Firewall de Windows sólo se refieren al sistema operativo Windows XP.

- ▶ Inicie el programa de instalación con un doble clic en el fichero de instalación descargado de Internet o bien coloque el CD del programa en la unidad.

Instalación basada en Internet

- Aparece el cuadro de diálogo *Bienvenido...*
- ▶ Haga clic en **Continuar** para continuar con la instalación.
- Aparece el cuadro de diálogo *Selección de idioma*.
- ▶ Seleccione el idioma con el que desea instalar su programa AntiVir y confirme la selección con **Continuar**.
- Aparece el cuadro de diálogo *Descarga*. Se descargan todos los ficheros necesarios para la instalación de los servidores Web de Avira GmbH. Tras finalizar la descarga se cierra la ventana *Descarga*.

Instalación con un paquete de instalación

- El asistente de instalación se abre y muestra el cuadro de diálogo *Avira AntiVir Professional*.
- ▶ Haga clic en *Aceptar* para iniciar la instalación.
- Se descomprime el fichero de instalación. Se inicia la rutina de instalación.
- Aparece el cuadro de diálogo *Bienvenido...*
- ▶ Haga clic en **Continuar**.

Continuación de Instalación basada en Internet e instalación con un paquete de instalación

- Aparece el cuadro de diálogo con el contrato de licencia.
- ▶ Confirme que acepta el contrato de licencia y pulse **Continuar**.
- Aparece el cuadro de diálogo *Generar número de serie*.
- ▶ Confirme, dado el caso, que se generará un número de serie aleatorio y se transferirá durante la actualización, y pulse **Continuar**.
- Aparece el cuadro de diálogo *Seleccionar tipo de instalación*.
- ▶ Active la opción **Exprés** o **Personalizada**. Si desea crear un punto de restauración, active la opción **Crear punto de restauración del sistema**. Confirme sus datos con **Continuar**.

Instalación personalizada

- Aparece el cuadro de diálogo *Seleccionar directorio de destino*.
- ▶ Confirme el directorio de destino indicado pulsando **Continuar**.
- O BIEN -
Mediante **Examinar** seleccione otro directorio de destino y confirme pulsando **Continuar**.
- Aparece el cuadro de diálogo *Instalar componentes*:
- ▶ Active o desactive los componentes pertinentes y confirme pulsando **Continuar**.
- Si ha seleccionado el componente ProActiv para su instalación, aparecerá la ventana *Comunidad de AntiVir ProActiv*. Tiene la posibilidad de confirmar la participación en la comunidad de AntiVir ProActiv: con esta opción activada, Avira AntiVir ProActiv envía datos a programas sospechosos notificados por el componente ProActiv al Avira Malware Research Center. Los datos se utilizan únicamente para un análisis online

ampliado y para la ampliación y depuración de la tecnología de detección. A través del enlace **más información** puede acceder a los detalles del análisis online ampliado.

- ▶ Active o desactive la participación en la comunidad de AntiVir ProActiv y confirme con **Continuar**.

→ En el siguiente cuadro de diálogo puede establecer si debe crearse un acceso directo en el escritorio y/o un grupo de programas en el menú Inicio.

- ▶ Haga clic en **Continuar**.

Continuación: Instalación exprés e instalación personalizada

→ Aparece el cuadro de diálogo *Instalar licencia*:

- ▶ Elija el directorio en el que haya guardado el fichero de licencia, siga las indicaciones del cuadro de diálogo y confirme pulsando **Continuar**.

→ Se copia el fichero de licencia, los componentes se instalan e inician.

→ En el siguiente cuadro de diálogo puede seleccionar si debe abrirse el fichero Léame (Readme) y reiniciarse el equipo una vez finalizada la instalación.

- ▶ En caso necesario, confírmelo y concluya la instalación con *Finalizar*.

→ Se cierra el asistente de instalación.

Continuación: Instalación personalizada

Asistente de configuración

→ En caso de una instalación personalizada, en el siguiente paso se abre el asistente de configuración. En el asistente de configuración puede establecer importantes valores predefinidos para su programa AntiVir.

- ▶ En la ventana de bienvenida del asistente de configuración, haga clic en **Continuar** para iniciar la configuración del programa.

→ El cuadro de diálogo *Configurar AHeAD* permite seleccionar un nivel de detección para la tecnología AHeAD. El nivel de detección seleccionado se aplica en la configuración de la tecnología AHead del escáner (análisis directo) y del Guard (análisis en tiempo real)

- ▶ Seleccione un nivel de detección y continúe con la configuración pulsando **Continuar**.

→ En la siguiente ventana de diálogo *Seleccionar categorías de riesgos avanzadas* podrá adaptar las funciones de protección de su programa AntiVir con la selección de categorías de riesgos.

- ▶ Si fuera necesario, active más categorías de riesgos y prosiga con la configuración pulsando *Continuar*.

→ En caso de que haya seleccionado el módulo de instalación Avira FireWall para su instalación, aparece la ventana de diálogo *FireWall-Nivel de seguridad*. Puede especificar si Avira FireWall permitirá accesos externos a recursos compartidos, así como accesos a la red por parte de las aplicaciones de empresas de confianza.

- ▶ Active las opciones pertinentes y prosiga con la configuración pulsando *Continuar*.

→ En caso de que haya seleccionado el módulo de instalación AntiVir Guard para su instalación, aparece el cuadro de diálogo *Modo de inicio del Guard*. Podrá definir el momento de inicio del Guard. El Guard se iniciará con el modo de inicio indicado cada vez que se reinicie el equipo.

Nota

El modo de inicio especificado del Guard se guarda en el registro y no puede modificarse a través de la configuración.

- ▶ Active la opción pertinente y prosiga con la configuración pulsando *Continuar*.
- En la siguiente ventana de diálogo *Seleccionar configuración de email*, puede introducir la configuración del servidor para el envío de emails. Su programa AntiVir utiliza el envío de emails por SMTP para enviar alertas de email.
- ▶ Si fuera necesario, aporte la información necesaria para la configuración del servidor y prosiga con la configuración pulsando *Continuar*.
- En el siguiente cuadro de diálogo, *Análisis del sistema*, puede activar o desactivar un breve análisis del sistema. El breve análisis del sistema se ejecuta una vez concluida la configuración y antes de reiniciar el equipo, y se analizan los programas iniciados, así como los ficheros del sistema más importantes para detectar virus y malware.
- ▶ Active o desactive la opción *Análisis breve del sistema* y prosiga con la configuración pulsando *Continuar*.
- En el siguiente cuadro de diálogo puede concluir la configuración con *Finalizar*.
- ▶ Haga clic en *Finalizar* para concluir la configuración.
- Se aplican los parámetros de configuración indicados y seleccionados.
- Si ha activado la opción *Análisis breve del sistema*, aparece la ventana Luke Filewalker. El escáner lleva a cabo un breve análisis del sistema.

Continuación: Instalación exprés e instalación personalizada

- Si en el último asistente de instalación ha seleccionado la opción **Reiniciar equipo**, se produce un reinicio del equipo.
- Después del reinicio del equipo se muestra el fichero Léame si en el asistente de instalación ha seleccionado la opción **Mostrar Léame.txt**.

Tras la instalación correcta se recomienda comprobar en el Centro de control en *Información general:: Estado* comprobar la actualidad del programa.

- ▶ Si fuera necesario, lleve a cabo una actualización para actualizar el fichero de firmas de virus.
- ▶ A continuación, lleve a cabo un análisis completo del sistema.

4.2 Instalación diferencial

Puede añadir o quitar determinados componentes del programa en la instalación actual del programa AntiVir (consulte el capítulo Instalación y desinstalación::Módulos de instalación)

Si desea añadir o quitar módulos de programa a la instalación actual, puede usar la opción **Añadir o quitar programas** para **Cambiar/Eliminar** programas en el **Panel de control de Windows**.

Seleccione su programa AntiVir y haga clic en **Modificar**. En el cuadro de diálogo de bienvenida del programa, seleccione la opción **Modificar programa**. Será guiado/a a través de la instalación diferencial.

4.3 Módulos de instalación

En caso de instalación personalizada o de instalación diferencial, puede seleccionar los siguientes módulos para añadir a la instalación o bien quitarlos de ella:

- **AntiVir Professional**
Este módulo contiene todos los componentes necesarios para la instalación correcta de su programa AntiVir.
- **AntiVir Guard**
El AntiVir Guard se ejecuta en segundo plano. Supervisa y repara, si fuera posible, los ficheros en operaciones como abrir, escribir y copiar en tiempo real (en acceso). Si un usuario realiza una operación con un fichero (cargar, ejecutar, copiar el fichero), el programa AntiVir analiza automáticamente el fichero. En el caso de la operación de fichero Cambiar nombre, AntiVir Guard no realiza análisis alguno.
- **AntiVir ProActiv**
El componente ProActiv supervisa acciones de aplicaciones y avisa sobre un comportamiento sospechoso. Mediante este reconocimiento basado en el comportamiento podrá protegerse ante malware desconocido. El componente ProActiv está integrado en el AntiVir Guard.
- **AntiVir MailGuard**
MailGuard es el interfaz entre su equipo y el servidor de correo del cual su programa de correo (cliente de correo) descarga los emails. MailGuard se intercala como Proxy entre el programa de correo y el servidor de correo. Todos los emails entrantes se dirigen a través de este proxy, que analiza la existencia de virus o programas no deseados en los emails y los entrega al programa de correo. Según la configuración, el programa trata los emails infectados automáticamente o pregunta al usuario antes de realizar una determinada acción.
- **AntiVir WebGuard**
Mientras se "navega" por Internet, el explorador Web solicita datos a un servidor Web. Los datos transmitidos por el servidor Web (ficheros HTML, ficheros de script y de imagen, ficheros Flash, secuencias de audio y de vídeo, etc.) pasan por regla general de la memoria caché del explorador directamente a la ejecución en el explorador Web, de modo que un análisis en tiempo real, como el que ofrece el AntiVir Guard, no es posible en este caso. Ésta es una vía de acceso de virus y programas no deseados a su sistema informático. El WebGuard es un proxy HTTP que supervisa los puertos utilizados para la transmisión de datos (80, 8080, 3128) y analiza los datos transmitidos para detectar la existencia de virus y programas no deseados. Según la configuración, el programa trata los ficheros infectados automáticamente o pregunta al usuario antes de realizar una determinada acción.
- **Avira FireWall**
El Avira FireWall controla las vías de comunicación hacia y desde el equipo. Permite o deniega la comunicación basándose en directrices de seguridad.
- *AntiVir Protección contra rootkits*
La protección contra rootkits de AntiVir analiza si ya hay software instalado en el equipo que, una vez ha irrumpido en el sistema informático, ya no puede detectarse con los métodos convencionales de detección de malware.
- **Extensión del shell**
La extensión del shell crea en el menú contextual del Windows Explorer (botón derecho del ratón) la entrada Analizar ficheros seleccionados con AntiVir. Esta entrada permite analizar directamente determinados ficheros o directorios.

4.4 Desinstalación

Si desea desinstalar el programa AntiVir del equipo, puede utilizar la opción **Agregar o Quitar Programas** para **Cambiar/Quitar** programas en el Panel de Control de Windows.

Procedimiento para desinstalar su programa AntiVir (descrito con el ejemplo de Windows XP y Windows Vista):

- ▶ Por medio del menú **Inicio**, abra el **Panel de control**.
- ▶ Haga doble clic en **Programas** (Windows XP: **Software**).
- ▶ Seleccione su programa AntiVir en la lista y haga clic en **Eliminar**.
- Se le pregunta si confirma que desea quitar el programa.
- ▶ Confirme con **Sí**.
- Se le pregunta si debe activarse de nuevo el Firewall de Windows (puesto que se va a desactivar el Avira FireWall).
- ▶ Confirme con **Sí**.
- Se quitan todos los componentes del programa.
- ▶ Pulse **Finalizar** para completar la desinstalación.
- Es posible que aparezca un cuadro de diálogo recomendando el reinicio del equipo.
- ▶ Confirme con **Sí**.
- El programa AntiVir se ha desinstalado, si fuera necesario, el equipo se reiniciará. Al hacerlo, se eliminan todos los directorios, ficheros y entradas del registro del programa.

4.5 Instalación y desinstalación en la red

Para facilitar al administrador del sistema la instalación de programas AntiVir en una red con varios equipos cliente, su programa AntiVir ofrece un procedimiento especial para la primera instalación y la instalación diferencial.

Para la instalación automática, el programa de instalación utiliza el fichero de control setup.inf. EL programa de instalación (presetup.exe) está incluido en el paquete de instalación del programa. La instalación se inicia con un script o un fichero por lotes y contiene toda la información necesaria del fichero de control. Los comandos del script sustituyen las habituales entradas manuales que se hacen durante la instalación.

Nota

Tenga en cuenta que para la primera instalación en la red es imprescindible un fichero de licencia.

Nota

Tenga en cuenta que para la instalación a través de la red necesitará un paquete de instalación para el programa AntiVir. No se puede usar un fichero de instalación para la instalación basada en Internet.

Con un script de inicio de sesión del servidor o mediante SMS se pueden distribuir cómodamente programas AntiVir en la red.

Aquí encontrará información sobre la instalación y desinstalación en la red:

- consulte el capítulo: Parámetros de línea de comandos para el programa de instalación
- consulte el capítulo: Parámetros del fichero setup.inf
- consulte el capítulo: Instalación en la red
- consulte el capítulo: Desinstalación en la red

Nota

Otra posibilidad cómoda de instalar y desinstalar programas AntiVir en red la ofrece el AntiVir Security Management Center. El AntiVir Security Management Center permite la instalación y el mantenimiento remotos de los productos AntiVir en red. Encontrará más información en nuestra página Web:

<http://www.avira.es>

4.5.1 Instalación en la red

La instalación puede ejecutarse controlada por el script en el modo por lotes.

Esta configuración es adecuada para las siguientes instalaciones:

- primera instalación a través de la red (instalación desatendida)
- Instalación de equipos independientes

► Instalación diferencial o actualización

Nota

Recomendamos probar la instalación automática antes de ejecutar la rutina de instalación en la red.

Procedimiento para instalar programas AntiVir automáticamente en la red:

- ✓ Dispone de derechos de administrador (también es necesario en el modo por lotes)
- Configure los parámetros del fichero *setup.inf* y guarde el fichero.
- Inicie la instalación con el parámetro */inf* o integre el parámetro en el script de inicio de sesión del servidor.
 - Ejemplos: `presetup.exe /inf="c:\temp\setup.inf"`
- La instalación transcurre automáticamente.

4.5.2 Desinstalación en la red

Procedimiento para desinstalar programas AntiVir automáticamente en la red:

- ✓ Dispone de derechos de administrador (también es necesario en el modo por lotes)
- ▶ Inicie la desinstalación con el parámetro `/remsilent` o `/remsilentaskreboot` o bien integre el parámetro en el script de inicio de sesión del servidor.
Adicionalmente, puede indicar el parámetro para el registro de la desinstalación.
 - Ejemplos: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`
- La desinstalación transcurre automáticamente.

Nota

No inicie el programa de instalación para la desinstalación en una unidad de red compartida, sino de forma local en el equipo en el que deba desinstalarse el programa AntiVir.

4.5.3 Parámetros de línea de comandos para el programa de instalación

Todos los datos sobre rutas o ficheros deben indicarse entre comillas.

Para la instalación, puede usar el siguiente parámetro:

- `/inf`

El programa de instalación se inicia con el script indicado y toma de él todos los parámetros necesarios.

Ejemplo: `presetup.exe /inf="c:\temp\setup.inf"`

Para la desinstalación, puede usar los siguientes parámetros:

- `/remove`

El programa de instalación desinstala el programa AntiVir.

Ejemplo: `presetup.exe /remove`

- `/remsilent`

El programa de instalación desinstala el programa AntiVir sin mostrar cuadros de diálogo. El equipo se reinicia después de la desinstalación.

Ejemplo: `presetup.exe /remsilent`

- `/remsilentaskreboot`

El programa de instalación desinstala el programa AntiVir sin mostrar cuadros de diálogo y, después de la desinstalación, pregunta si debe reiniciarse el equipo.

Ejemplo: `presetup.exe /remsilentaskreboot`

Para el registro de la desinstalación, dispone además del siguiente parámetro opcional:

- `/unsetuplog`

Se registran todas las acciones durante la desinstalación.

```
Ejemplo: presetup.exe /remsilent  
/unsetuplog="c:\logfiles\unsetup.log"
```

4.5.4 Parámetros del fichero setup.inf

En el fichero de control setup.inf, puede establecer, para la instalación del programa AntiVir, los siguientes parámetros en el área [DATA]. El orden de los parámetros no tiene importancia. Si un parámetro falta o se ha establecido erróneamente, la rutina de instalación se cancela con un mensaje de error.

– DestinationPath

Ruta de destino en la que se instalará el programa. Debe indicarse en el script. Tenga en cuenta que el programa de instalación añade al final automáticamente nombres de empresa y de producto. Pueden utilizarse variables de entorno.

Ejemplo: DestinationPath=%PROGRAMFILES%
da como resultado, por ejemplo, C:\Archivos de
programa\Avira\AntiVir Desktop

– ProgramGroup

Creación de un grupo de programas para todos los usuarios del equipo en el menú Inicio de Windows.

1: Crear grupo de programas

0: No crear grupo de programas

Ejemplo: ProgramGroup=1

– DesktopIcon

Creación de un icono de acceso directo para todos los usuarios del equipo en el escritorio.

1: Crear icono de escritorio

0: No crear icono de escritorio

Ejemplo: DesktopIcon=1

– ShellExtension

Registro de la extensión del shell en el registro. La extensión del shell permite analizar ficheros o directorios con el menú contextual del botón derecho del ratón para detectar la existencia de virus y malware.

1: Registrar extensión del shell

0: No registrar extensión del shell

Ejemplo: ShellExtension=1

– Guard

Instala el AntiVir Guard (escáner en acceso).

1: Instalar AntiVir Guard

0: No instalar AntiVir Guard

Ejemplo: Guard=1

– MailScanner

Instala el AntiVir MailGuard.

1: Instalar AntiVir MailGuard

0: No instalar AntiVir MailGuard

Ejemplo: MailScanner=1

– KeyFile

Indica la ruta del fichero de licencia que se copia durante la instalación. En la primera instalación: requisito imprescindible. El nombre de fichero debe indicarse completo. (En instalación diferencial: opcional.)

Ejemplo: KeyFile=D:\inst\license\hbedv.key

– ShowReadMe

Muestra el fichero léame.txt tras la instalación.

1: Mostrar fichero

0: No mostrar fichero

Ejemplo: ShowReadMe=1

– RestartWindows

Reinicia el equipo tras la instalación. Esta entrada tiene una prioridad más alta que ShowRestartMessage.

1: Reiniciar equipo

0: No reiniciar equipo

Ejemplo: RestartWindows=1

– ShowRestartMessage

Durante la instalación, muestra un mensaje antes de un reinicio automático.

0: No mostrara información

1: Mostrar información

Ejemplo: ShowRestartMessage=1

– SetupMode

No es necesario en la primera instalación. El programa de instalación detecta si se ejecuta una primera instalación. Determina el tipo de instalación. Cuando ya existe una instalación, sin embargo, debe indicarse con SetupMode si para esa instalación sólo se va a ejecutar una actualización o una modificación (nueva configuración) o bien se va a ejecutar una desinstalación.

Actualizar: ejecuta una actualización de una instalación existente. Los parámetros de configuración, p. ej., Guard, se omiten.

Modificar: ejecuta una modificación (nueva configuración) de una instalación existente. No se copia ningún fichero en la ruta de destino.

Quitar: Desinstala su programa AntiVir del sistema.

Ejemplo: SetupMode=Update

- AVWinIni (opcional)

Indica la ruta de destino del fichero de configuración que puede copiarse durante la instalación. El nombre de fichero debe indicarse completo.

Ejemplo: AVWinIni=d:\inst\config\avwin.ini

- Password

Esta opción pasa a la rutina de instalación la contraseña establecida para la instalación (diferencial) y la desinstalación. La rutina de instalación sólo comprueba esta entrada si se estableció una contraseña. Si se estableció una contraseña y el parámetro de contraseña falta o se ha establecido erróneamente, la rutina de instalación se cancela.

Ejemplo: Password=Contraseña123

- WebGuard

Instala el AntiVir WebGuard.

1: Instalar AntiVir WebGuard

0: No instalar AntiVir WebGuard

Ejemplo: WebGuard=1

- RootKit

Instala el módulo AntiVir Protección contra rootkits. Sin AntiVir Protección contra rootkits el escáner no puede analizar la existencia de rootkits en el sistema.

1: Instalar AntiVir Protección contra rootkits

0: No instalar AntiVir Protección contra rootkits

Ejemplo: RootKit=1

- HIPS

Instala el componente AntiVir ProActiv. AntiVir ProActiv es una tecnología de reconocimiento basada en el comportamiento con la que se puede reconocer malware todavía desconocido.

1: Instalar ProActiv

0: No instalar ProActiv

Ejemplo: HIPS=1

– Firewall

Instala el componente Avira FireWall. Avira FireWall monitoriza y regula el tráfico de datos entrante y saliente en su sistema informático y protege así su equipo contra las amenazas procedentes de Internet o de otros entornos de red.

1: Instalar Firewall

0: No instalar Firewall

Ejemplo: FireWall=1

5 Información general

En este capítulo dispone de una descripción general de las funciones y el uso de su programa AntiVir.

- consulte el capítulo Interfaz y uso
- consulte el capítulo Procedimientos

5.1 Interfaz de usuario y uso

Su programa AntiVir se utiliza por medio de tres elementos de la interfaz del programa:

- Centro de control: Monitorización y control del programa AntiVir
- Configuración: Configuración del programa AntiVir
- Icono de bandeja en la bandeja del sistema de la barra de tareas: apertura del Centro de control y otras funciones

5.1.1 Centro de control

El Centro de control sirve para supervisar el estado de protección de su sistema informático y para controlar y operar con los componentes de protección y las funciones de su programa AntiVir.



La ventana del Centro de control se divide en tres áreas: la **barra de menús**, la **barra de exploración** y la ventana de detalles **Vista**:

- **Barra de menús:** en los menús del Centro de control puede activar funciones de programa generales y consultar información sobre el programa.

- **Área de exploración:** en el área de exploración puede cambiar fácilmente entre las diversas secciones del Centro de control. Las secciones contienen información y funciones de los componentes de programa y están dispuestas en la barra de exploración por áreas de actividades. Ejemplo: área de actividades *Descripción general* - sección **Estado**.
- **Vista:** en esta ventana se muestra la sección seleccionada en el área de exploración. En función de cada sección, en la barra superior de la ventana de detalles encontrará botones para ejecutar funciones o acciones. En algunas secciones, aparecen datos u objetos de datos en listas. Puede ordenar las listas pulsando en el campo según el cual quiera ordenar la lista.

Inicio y finalización del Centro de control

Puede iniciar el Centro de control de las siguientes maneras:

- Con un doble clic en el icono del programa de su escritorio
- Por medio de la entrada de programa en el menú Inicio | Programas.
- A través del icono de bandeja de su programa AntiVir.

Para finalizar el Centro de control, use la opción de menú **Salir** del menú **Fichero** o bien pulse el aspa de cierre en el Centro de control.

Usar el Centro de control

Así se navega por el Centro de control

- ▶ Seleccione un área de actividades en la barra de exploración.
- Se abre el área de actividades y aparecen otras secciones. Está seleccionada la primera sección del área de actividades y se muestra en la vista.
- ▶ Si lo desea, pulse en otra sección para mostrarla en la ventana de detalles.
 - O BIEN -
- ▶ Elija una sección por medio del menú *Ver*.

Nota

La exploración usando el teclado de la barra de menús se activa con la tecla [Alt]. Si está activada la exploración, puede desplazarse por el menú usando las teclas de flecha. Con la tecla Intro se activa la opción de menú seleccionada en ese momento.

Para abrir y cerrar los menús en el Centro de control o para explorarlos, podrá usar las siguientes combinaciones de teclas: [Alt] + letra subrayada del menú o comando de menú. Mantenga pulsada la tecla [Alt] si desea abrir un comando de menú de un menú o un submenú

Para editar los datos u objetos que se muestran en la ventana de detalles:

- ▶ Seleccione los datos u objetos que va a editar.
 - Para seleccionar varios elementos, mantenga pulsada la tecla Ctrl o la tecla Mayús (selección de elementos consecutivos) mientras selecciona los elementos.
- ▶ Pulse el botón que desee en la barra superior de la ventana de detalles para editar el objeto

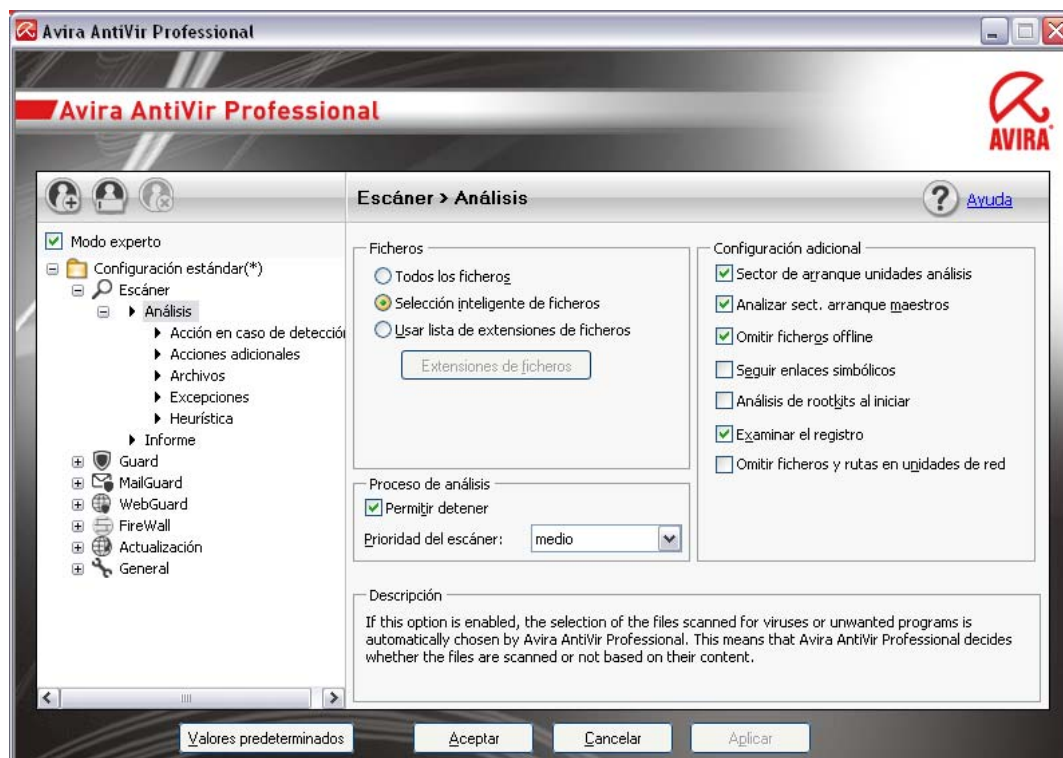
Descripción general del Centro de control

- **Descripción general:** en **Información general** encontrará todas las secciones con las que puede supervisar la funcionalidad de su programa AntiVir.

- La sección **Estado** ofrece la posibilidad de ver de una sola mirada qué módulos del programa están activos y aporta información sobre la última actualización realizada. Además, se ve si dispone de una licencia válida.
- La sección Eventos ofrece la posibilidad de informarse sobre los eventos que generan los módulos de programa.
- La sección Informes ofrece la posibilidad de consultar los resultados de las acciones realizadas.
- **Protección local:** en **Protección local** constan los componentes con los que se analizan los ficheros del sistema informático para detectar la existencia de virus o software malintencionado (malware).
- La sección Analizar permite configurar o iniciar fácilmente el análisis directo. Los perfiles predefinidos permiten llevar a cabo un análisis con opciones predeterminadas ya adaptadas. Del mismo modo, puede adaptar a sus propias necesidades el análisis de detección de virus y programas no deseados por medio de la selección manual (no se guarda) o bien mediante la creación de perfiles definidos por el usuario.
- La sección Guard muestra información sobre los ficheros analizados, así como otros datos estadísticos que puede restablecer en cualquier momento y permite abrir el fichero de informe. Dispondrá de información detallada acerca de la última detección de virus o programas no deseados " prácticamente con sólo pulsar un botón".
- **Protección online :** en **Protección online** encontrará los componentes con los que se protege el sistema informático frente a virus y malware de Internet, así como frente a los accesos no deseados a la red.
- La sección MailGuard muestra los emails analizados por el MailGuard, sus propiedades y otros datos estadísticos.
- La sección WebGuard muestra información sobre las URL analizadas y los virus detectados, así como otros datos estadísticos que puede restablecer en cualquier momento y permite abrir el fichero de informe. Dispondrá de información detallada acerca de la última detección de virus o programas no deseados " prácticamente con sólo pulsar un botón".
- La sección FireWall permite configurar los parámetros básicos del cortafuegos Avira. Además, se muestran la velocidad de transmisión de datos actual y todas las aplicaciones activas que utilizan una conexión de red.
- **Administración:** en **Administración** encontrará herramientas con las que aislar y administrar ficheros sospechosos o infectados por virus, así como programar tareas periódicas.
- La sección Cuarentena contiene lo que se denomina Gestor de cuarentena. Es el elemento central para ficheros ya puestos en cuarentena o para ficheros sospechosos que se quieren poner en cuarentena. Además, existe la posibilidad de enviar un determinado fichero por email al Avira Malware Research Center.
- La sección Programador permite crear tareas de análisis y actualización, así como programadas, y adaptar o eliminar tareas existentes.

5.1.2 Configuración

En la configuración puede establecer los parámetros de su programa Antivir . Tras la instalación, su programa AntiVir está configurado con parámetros predeterminados que garantizan que el sistema informático esté óptimamente protegido. No obstante, su sistema informático o los requisitos que usted tiene respecto a su programa AntiVir pueden presentar particularidades, de modo que querrá adaptar los componentes de protección del programa.



La configuración tiene estructura de cuadro de diálogo: Con los botones Aceptar o Aplicar se guardan los parámetros establecidos en la configuración, con Cancelar se descartan los parámetros y con el botón Valores predeterminados puede restablecer los parámetros de la configuración en los valores predeterminados. En la barra de exploración de la izquierda, puede seleccionar las distintas secciones de configuración.

Abrir la configuración

Hay varias maneras de activar la configuración:

- A través del Panel de control de Windows.
- Por medio del Centro de seguridad de Windows: a partir de Windows XP Service Pack 2.
- A través del icono de bandeja de su programa AntiVir.
- En el Centro de control a través de la opción de menú Herramientas | Configuración.
- En el Centro de control pulsando el botón Configuración.

Nota

Si activa la configuración pulsando el botón **Configuración** en el Centro de control, accederá a la ficha de configuración de la sección que esté activa en el Centro de control. Para seleccionar cada una de las fichas de configuración, debe estar activado el modo experto de la configuración. En ese caso, aparece un cuadro de diálogo que solicita activar el modo experto.

Usar la configuración

En la ventana de configuración, puede desplazarse como en el Explorador de Windows:

- ▶ Pulse en una entrada de la estructura de árbol para mostrar esa sección de configuración en la ventana de detalles.
- ▶ Pulse en el signo más delante de una entrada para expandir la sección de configuración y mostrar otras secciones de configuración subordinadas en la estructura de árbol.
- ▶ Para ocultar las secciones de configuración subordinadas, pulse en el signo menos delante de la sección de configuración expandida.

Nota

Para activar o desactivar opciones en la configuración y pulsar los botones, también puede usar combinaciones de teclas: [Alt] + letra subrayada en el nombre de opción o en la denominación del botón.

Nota

Sólo en el modo experto se muestran todas las secciones de configuración. Active el modo experto para ver todas las secciones de configuración. Puede asignar una contraseña al modo experto y, al activarlo, tendrá que indicarla.

Si quiere aceptar los parámetros establecidos en la configuración:

- ▶ Haga clic en el botón **Aceptar**.
- La ventana de configuración se cierra y los parámetros establecidos se aplican.
- O BIEN -
- ▶ Haga clic en el botón **Aplicar**.
- Se aplica la configuración. La ventana de configuración permanece abierta.

Si quiere finalizar la configuración sin aceptar los parámetros establecidos:

- ▶ Pulse el botón **Cancelar**.
- La ventana de configuración se cierra y los parámetros establecidos se descartan.

Si desea restablecer todos los parámetros de la configuración en sus valores predeterminados:

- ▶ Haga clic en **Valores predeterminados**.
- Todos los parámetros de la configuración se restablecen con los valores predeterminados. Al restablecer los valores predeterminados, se pierde cualquier cambio efectuado y todas las entradas propias.

Perfiles de configuración

Tiene la posibilidad de guardar los parámetros en la configuración como perfiles de configuración. En el perfil de configuración, es decir, en una configuración, constan todas las opciones de configuración resumidas en un grupo. La configuración se representa en la barra de exploración como un nodo. Puede añadir más configuraciones a la configuración predeterminada. Existe la posibilidad de definir reglas para cambiar a una configuración en concreto:

El cambio de configuración basado en reglas permite acoplar configuraciones al uso de una conexión LAN o de Internet (identificación por medio de la puerta de enlace predeterminada): Puede crear así, por ejemplo, perfiles de configuración para los distintos escenarios de uso de un equipo portátil:

- Uso en la red de la empresa: Actualización a través del servidor de la Intranet, WebGuard desactivado
- Uso en casa: Actualización a través de los servidores Web predeterminados de Avira GmbH, WebGuard activado

Si no se han definido reglas para cambiar a otra configuración, puede cambiarla manualmente en el menú contextual del icono de bandeja. Con los botones de la barra de exploración o los comandos del menú contextual de las secciones de configuración puede añadir configuraciones, cambiarles el nombre, eliminarlas, copiarlas, restablecerlas y definir reglas para el cambio a una configuración determinada.

Nota

Windows 2000 no admite el cambio automático a otra configuración. Windows 2000 no permite definir reglas para cambiar a otra configuración.

Descripción general de las opciones de configuración

Dispone de las siguientes opciones de configuración:

- **Escáner:** Configuración del análisis directo

Opciones de análisis

Acciones en caso de detección

Opciones al analizar archivos

Excepciones del análisis directo

Heurística del análisis directo

Configuración de la función de informe

- **Guard:** Configuración del análisis en tiempo real

Opciones de análisis

Acciones en caso de detección

Excepciones del análisis en tiempo real

Heurística del análisis en tiempo real

Configuración de la función de informe

- **MailGuard:** Configuración del MailGuard

Opciones de análisis: Activación de la supervisión de cuentas POP3, cuentas IMAP, emails salientes (SMTP)

Acciones en caso de malware



Heurística del análisis del MailGuard

- Excepciones del análisis del MailGuard
- Configuración de la memoria caché, vaciar memoria caché
- Configuración de un pie de página en emails enviados
- Configuración de la función de informe
 - **WebGuard:** Configuración del WebGuard
- Opciones de análisis, activación y desactivación del WebGuard
- Acciones en caso de detección
- Accesos bloqueados: Tipos de fichero y tipos MIME no deseados, filtro Web para direcciones URL conocidas no deseadas (malware, suplantación de identidad (phishing), etc.)
- Excepciones del análisis del WebGuard: direcciones URL, tipos de fichero, tipos MIME
- Heurística del WebGuard
- Configuración de la función de informe
 - **FireWall** Configuración del FireWall
- Configuración de reglas de adaptador
- Configuración definida por el usuario de reglas de aplicación
- Lista de productores de confianza (excepciones durante el acceso a la red de las aplicaciones)
- Configuración avanzada: tiempo de espera para reglas, bloquear fichero host de Windows, detener FireWall de Windows, notificaciones
- Configuración de ventanas emergentes (mensajes de advertencia durante el acceso a la red de las aplicaciones)
 - **General:**
- Configuración del envío de email vía SMTP
- Categorías de riesgos avanzadas para análisis directo y análisis en tiempo real
- Protección con contraseña para el acceso al Centro de control y a la configuración
- Seguridad: indicador de estado de actualización, indicador de estado de análisis completo del sistema, protección del producto
- WMI: Activar compatibilidad con WMI
- Configuración del registro de eventos
- Configuración de las funciones de informe
- Configuración de los directorios usados
- Actualización: configuración de la conexión con el servidor de descarga, descarga vía servidor Web o servidor de ficheros), configuración de la actualización del producto
- Advertencias: Configuración de advertencias por email de los componentes:
 - Escáner
 - Guard
 - Updater
- Configuración de advertencias de red de los componentes Escáner, Guard

Configuración de advertencias acústicas al detectar malware

5.1.3 Icono de bandeja

Tras la instalación verá el icono de bandeja de su programa AntiVir en la bandeja del sistema de la barra de tareas:

Icono	Descripción
	AntiVir Guard está activado y el FireWall está activado
	AntiVir Guard está desactivado o el FireWall está desactivado

El icono de bandeja muestra el estado del servicio de Guard y FireWall.

Por medio del menú contextual del icono de bandeja puede acceder rápidamente a las funciones principales de su programa AntiVir. Para activar el menú contextual, pulse con el botón derecho del ratón en el icono de bandeja.

Entradas en el menú contextual

- **Activar AntiVir Guard** Activa o desactiva el AntiVir Guard.
- **Activar AntiVir MailGuard:** Activa o desactiva el AntiVir MailGuard.
- **Activar AntiVir WebGuard:** Activa o desactiva el AntiVir WebGuard.
- **FireWall**
- Activar FireWall: Activa o desactiva el FireWall
- Bloquear todo el tráfico: Activado: bloquea cualquier transmisión de datos a excepción de las transmisiones al sistema informático propio (host local / IP 127.0.0.1).
- Activar el modo de juego: Activa o desactiva el modo:
Activado: Cuando está activado, se aplican todas las reglas definidas del adaptador. Las aplicaciones para las que no se ha definido una regla, pueden acceder a la red y no se abre ninguna ventana emergente.
- **Iniciar AntiVir:** Abre el Centro de control.
- **Configurar AntiVir:** Abre la Configuración.
- **Iniciar actualización:** Inicia una Actualización.
- **Seleccionar configuración:** abre un submenú con los perfiles de configuración disponibles. Haga clic en una configuración para activarla. El comando de menú está desactivado si ya ha definido reglas para cambiar automáticamente a una configuración.
- **Ayuda:** Abre la ayuda online.
- **Acerca de AntiVir Professional:** Abre un cuadro de diálogo con información sobre su programa AntiVir: Información del producto, información sobre la versión, información sobre la licencia.
- **Avira en Internet:** Abre el portal Web de Avira en Internet. Debe de existir una conexión activa a Internet

5.2 Procedimientos

5.2.1 Activar licencia

Así se activa la licencia de su programa AntiVir:

Con el fichero de licencia hbedv.key se activa la licencia para su producto AntiVir. Recibirá el fichero de licencia por email de Avira GmbH. El fichero de licencia contiene la licencia para todos los productos que haya pedido.

Si todavía no ha instalado su programa AntiVir:

- ▶ Guarde el fichero de licencia en un directorio local de su equipo.
- ▶ Instale su programa AntiVir.
- ▶ Durante la instalación, indique dónde guardó el fichero de licencia.

Si ya ha instalado su programa AntiVir:

- ▶ En el administrador de ficheros o en el email de activación, haga doble clic en el fichero de licencia y siga las instrucciones en pantalla de la administración de licencias que aparece.

- O BIEN -

- ▶ En el Centro de control de su programa AntiVir seleccione la opción de menú Ayuda / Cargar fichero de licencia...

Nota

En Windows Vista aparece el cuadro de diálogo control de cuentas de usuario. En caso necesario, inicie sesión como administrador. Haga clic en **Continuar**.

- ▶ Seleccione el fichero de licencia y haga clic en **Abrir**.

→ Aparece un mensaje.

- ▶ Confirme con **Aceptar**.

→ La licencia está activada.

- ▶ Si fuera necesario, reinicie el sistema.

5.2.2 Ejecutar actualizaciones automáticas

Así se crea una tarea con el programador AntiVir con la que actualizar automáticamente su programa AntiVir:

- ▶ En el Centro de control seleccione la sección **Administración :: Programador**.

- ▶ Haga clic sobre el icono  *Crear tarea nueva con el asistente*.

→ Aparece el cuadro de diálogo *Nombre y descripción de la tarea*.

- ▶ Asigne nombre a la tarea y descríbalas si fuera el caso.

- ▶ Haga clic en **Continuar**.

→ Aparece el cuadro de diálogo *Tipo de tarea*.

- ▶ Seleccione **Tarea de actualización** en la lista de selección.






- ▶ Haga clic en **Continuar**.
- Aparece el cuadro de diálogo *Momento de inicio de la tarea*.
- ▶ Seleccione cuándo se ejecutará la actualización:
 - **Inmediatamente**
 - **Diariamente**
 - **Semanalmente**
 - **Intervalo**
 - **Una vez**
 - **Inicio de sesión**

Nota

Recomendamos llevar a cabo actualizaciones frecuentes y periódicas. El intervalo de actualización recomendado es de: 60 minutos.

- ▶ Según lo que seleccione, indique la fecha si fuera necesario.
- ▶ En caso necesario, seleccione opciones adicionales (sólo disponible en algunos tipos de tarea):
 - **Iniciar tarea adicionalmente al conectarse a Internet**
Además de la frecuencia definida, la tarea se lanza al iniciarse la conexión a Internet.
 - **Repetir la tarea si el tiempo ya transcurrió**
Las tareas del pasado se relanzan si no pudieron realizarse en su momento, por ejemplo, porque el equipo estaba apagado.
- ▶ Haga clic en **Continuar**.
- Aparece el cuadro de diálogo *Selección del modo de visualización*.
- ▶ Seleccione el modo de visualización de la ventana de tareas:
 - **Minimizado**: sólo barra de progreso
 - **Maximizado**: toda la ventana de tarea
 - **Invisible**: ninguna ventana de tarea
- ▶ Haga clic en **Finalizar**.
- La tarea recién creada aparece en la página de inicio de la sección **Administración :: Analizar** como activada (marca de verificación).
- ▶ Si es el caso, desactive las tareas que no deban ejecutarse.

Los siguientes iconos permiten continuar con la edición de las tareas:

-  Ver las propiedades de una tarea
-  Modificar tarea
-  Eliminar tarea
-  Iniciar tarea
-  Detener tarea

5.2.3 Iniciar una actualización manualmente

Dispone de varias posibilidades de iniciar manualmente una actualización: En las actualizaciones iniciadas manualmente también se ejecuta siempre una actualización del fichero de firmas de virus y el motor de análisis. La actualización del producto sólo tiene lugar si, en General:: Actualización, ha activado la opción **Descargar actualizaciones de producto e instalar automáticamente**.

Así se inicia manualmente una actualización de su programa AntiVir:

- ▶ Haga clic con el botón derecho del ratón en el icono de bandeja de AntiVir en la barra de tareas.
- Aparece un menú contextual.
- ▶ Seleccione **Iniciar actualización**.
- Aparece el cuadro de diálogo *Updater*.
- O BIEN -
- ▶ En el Centro de control seleccione la sección **Información general:: Estado**.
- ▶ En el área *Ultima actualización* haga clic en el enlace **Iniciar actualización**.
- Aparece el cuadro de diálogo *Updater*.
- O BIEN -
- ▶ En el Centro de control, en el menú **Actualización**, seleccione el comando de menú *Iniciar actualización*.
- Aparece el cuadro de diálogo *Updater*.

Nota

Recomendamos llevar a cabo actualizaciones automáticas periódicamente. El intervalo de actualización recomendado es de: 60 minutos.

Nota

También puede ejecutar la actualización automática directamente en el Centro de seguridad de Windows.

5.2.4 Análisis directo: analizar la existencia de virus y malware con un perfil de análisis

El perfil de análisis es una agrupación de unidades y directorios que deben analizarse.

Dispone de las siguientes maneras de analizar mediante un perfil de análisis:

- Usar perfil de análisis predefinido

Cuando los perfiles de análisis predefinidos satisfacen sus necesidades.

- Adaptar y usar perfil de análisis (selección manual)

Cuando desea analizar con un perfil de análisis personalizado.

- Crear y usar nuevo perfil de análisis

Cuando desea crear su propio perfil de análisis.

Según el sistema operativo que use, dispondrá de distintos iconos para iniciar un perfil de análisis:

- En Windows XP y 2000:



Este icono permite iniciar el análisis por medio de un perfil de análisis.

- En Windows Vista:

En Microsoft Windows Vista, de momento el Centro de control sólo tiene derechos limitados, p. ej., de acceso a directorios y ficheros. El Centro de control sólo puede ejecutar determinadas acciones y accesos a ficheros con derechos de administrador ampliados. Estos derechos de administrador ampliados deben concederse al iniciar cualquier análisis mediante un perfil de análisis.



Este icono permite iniciar un análisis limitado por medio de un perfil de análisis. Sólo se analizan los directorios y ficheros para los que Windows Vista ha concedido derechos de acceso.



Este icono permite iniciar el análisis con derechos de administrador ampliados. Tras una confirmación, se analizan todos los directorios y ficheros del perfil de análisis seleccionado.

Así se analiza la existencia de virus y malware con un perfil de análisis:

- ▶ En el Centro de control seleccione **Protección local :: Analizar**.
- Aparecen perfiles de análisis predefinidos.
- ▶ Seleccione uno de los perfiles de análisis predefinidos.
 - O BIEN -
- ▶ Adapte el perfil de análisis *Selección manual*.
 - O BIEN -
- ▶ Cree un perfil de análisis nuevo
- ▶ Haga clic en el icono (Windows XP: o Windows Vista:).
- ▶ Aparece la ventana *Luke Filewalker* y el análisis directo comienza.
- Una vez transcurrido el proceso de análisis, se muestran los resultados.



Si desea adaptar un perfil de análisis:

- ▶ Despliegue el árbol de ficheros del perfil de análisis **Selección manual** de manera que estén abiertos todos los directorios y las unidades que deben analizarse.
 - Si hace clic en el carácter +: aparece el siguiente nivel de directorios.
 - Si hace clic en el carácter -: se oculta el siguiente nivel de directorios.
- ▶ Seleccione los nodos y directorios que desea analizar mediante un clic en la casilla correspondiente de cada uno de los niveles de directorios.

Dispone de las siguientes posibilidades de seleccionar directorios:

- Directorio con subdirectorios incluidos (marca de verificación negra)
- Directorio sin subdirectorios (marca de verificación verde)
- Sólo los subdirectorios de un directorio (marca de verificación gris, los subdirectorios tienen marcas de verificación negras)
- Ningún directorio (ninguna marca de verificación)

Si desea crear un perfil de análisis nuevo:

- ▶ Haga clic sobre el icono  **Crear nuevo perfil.**
- Aparece el perfil *Nuevo perfil* debajo de los perfiles existentes.
- ▶ Si fuera necesario, cambie el nombre del perfil de análisis haciendo clic en el icono .
- ▶ Seleccione los nodos y directorios que desea analizar mediante un clic en la casilla del nivel de directorios correspondiente:
Dispone de las siguientes posibilidades de seleccionar directorios:
 - Directorio con subdirectorios incluidos (marca de verificación negra)
 - Directorio sin subdirectorios (marca de verificación verde)
 - Sólo los subdirectorios de un directorio (marca de verificación gris, los subdirectorios tienen marcas de verificación negras)
 - Ningún directorio (ninguna marca de verificación)

5.2.5 Análisis directo: Analizar la existencia de virus y malware mediante Arrastrar y soltar

Así se analiza la existencia de virus y malware mediante Arrastrar y soltar de forma precisa:

- ✓ Esta abierto el Centro de control de su programa AntiVir.
- ▶ Seleccione el fichero o directorio que desea analizar.
- ▶ Arrastre con el botón izquierdo del ratón el fichero seleccionado o el directorio seleccionado al *Centro de control*.
- Aparece la ventana *Luke Filewalker* y el análisis directo comienza.
- Una vez transcurrido el proceso de análisis, se muestran los resultados.

5.2.6 Análisis directo: analizar la existencia de virus y malware mediante el menú contextual

Así se analiza la existencia de virus y malware a través del menú contextual de forma precisa:


- ▶ Haga clic (p. ej., en el Explorador de Windows, en el escritorio o en un directorio de Windows abierto) con el botón derecho del ratón en el fichero o directorio que desea analizar.
- Aparece el menú contextual del Explorador de Windows.
- ▶ Seleccione en el menú contextual **Analizar los ficheros seleccionados con AntiVir.**
- Aparece la ventana *Luke Filewalker* y el análisis directo comienza.
- Una vez transcurrido el proceso de análisis, se muestran los resultados.

5.2.7 Análisis directo: analizar la existencia de virus y malware de forma automática

Nota






Después de la instalación la tarea de análisis *Análisis completo del sistema* queda creada en el planificador: Se ejecuta un análisis completo del sistema en un intervalo recomendado.

Así se crea una tarea con la que analizar automáticamente la existencia de virus y malware:

- ▶ En el Centro de control seleccione la sección **Administración :: Programador**.
- ▶ Haga clic en el icono .
- Aparece el cuadro de diálogo *Nombre y descripción de la tarea*.
- ▶ Asigne nombre a la tarea y descríbalas si fuera el caso.
- ▶ Haga clic en **Continuar**.
- Aparece el cuadro de diálogo *Tipo de tarea*.
- ▶ Seleccione la **Tarea de análisis**.
- ▶ Haga clic en **Continuar**.
- Aparece el cuadro de diálogo *Selección del perfil*.
- ▶ Seleccione el perfil que debe analizarse.
- ▶ Haga clic en **Continuar**.
- Aparece el cuadro de diálogo *Momento de inicio de la tarea*.
- ▶ Seleccione cuándo se ejecutará el análisis:
 - **Inmediatamente**
 - **Diariamente**
 - **Semanalmente**
 - **Intervalo**
 - **Una vez**
 - **Inicio de sesión**
- ▶ Según lo que seleccione, indique la fecha si fuera necesario.
- ▶ En caso necesario, seleccione la siguiente opción adicional (sólo disponible en algunos tipos de tarea):
 - **Repetir la tarea si el tiempo ya transcurrió**
Las tareas del pasado se relanzan si no pudieron realizarse en su momento, por ejemplo, porque el equipo estaba apagado.
- ▶ Haga clic en **Continuar**.
- Aparece el cuadro de diálogo *Selección del modo de visualización*.
- ▶ Seleccione el modo de visualización de la ventana de tareas:
 - **Minimizado**: sólo barra de progreso
 - **Maximizado**: toda la ventana de tarea
 - **Invisible**: ninguna ventana de tarea

- ▶ Seleccione la opción *Apagar equipo* si desea que el equipo de apague en cuanto la tarea haya sido ejecutada y finalizada. La opción solamente está disponible en el modo de representación minimizado o maximizado.
- ▶ Haga clic en **Finalizar**.
- La tarea recién creada aparece en la página de inicio de la sección *Administración :: Planificador* como activado (marca de verificación).
- ▶ Si es el caso, desactive las tareas que no deban ejecutarse.



Los siguientes iconos permiten continuar con la edición de las tareas:

-  Ver las propiedades de una tarea
-  Modificar tarea
-  Eliminar tarea
-  Iniciar tarea
-  Detener tarea

5.2.8 Análisis directo: analizar directamente la existencia de rootkits activos

Para analizar la existencia de rootkits activos, use el perfil de análisis predefinido *Análisis de rootkits y malware activo*.

Así se analiza directamente la existencia de rootkits activos:

- ▶ En el Centro de control seleccione **Protección local :: Analizar**.
- Aparecen perfiles de análisis predefinidos.
- ▶ Seleccione el perfil de análisis predefinido **Análisis de rootkits y malware activo**.
- ▶ Seleccione si fuera el caso más nodos y directorios para analizar mediante un clic en la casilla del nivel de directorios.
- ▶ Haga clic en el icono (Windows XP:  o Windows Vista: ).
- Aparece la ventana *Luke Filewalker* y el análisis directo comienza.
- Una vez transcurrido el proceso de análisis, se muestran los resultados.

5.2.9 Reaccionar a virus y malware detectados

Para cada uno de los componentes de protección de su programa AntiVir puede establecer, en la sección de la configuración *Acción en caso de detección*, la manera en que su programa AntiVir reaccionará al detectar un virus o programa no deseado.

En el componente ProActiv de Guard no existen opciones de acción configurables. Una detección siempre se indica en la ventana *Guard: Comportamiento sospechoso de una aplicación*.

Opciones de acción del escáner:

– **Interactivo**

En el modo de acción interactivo, las detecciones del análisis del escáner se notifican en un cuadro de diálogo. Este ajuste está activado de forma estándar.

En el **Análisis del escáner** recibirá un mensaje de advertencia con una lista de los ficheros afectados encontrados al finalizar el análisis. Tiene la posibilidad de seleccionar mediante el menú contextual la acción que se ejecutará para cada uno de los ficheros afectados. Puede ejecutar las acciones seleccionadas para todos los ficheros afectados o finalizar el escáner.

– **Automático**

Al detectar un virus o programa no deseado en el modo de acción automático se ejecuta automáticamente la acción seleccionada en esta área. Si activa la opción *Mostrar mensaje de advertencia*, al detectar un virus recibirá un mensaje de advertencia en el que se muestra la acción ejecutada.

Opciones de acción del Guard:

– **Interactivo**

En el modo de acción interactivo se impide el acceso a los datos y se muestra una notificación en el escritorio. En la notificación de escritorio puede eliminar el malware detectado o pasar el malware para el consiguiente tratamiento de virus al componente de escáner a través del botón Detalles. El escáner avisa la detección en una ventana, en la que dispondrá de distintas opciones para el tratamiento del fichero afectado a través de un menú (ver Detección::Escáner).

– **Automático**

Si se detecta un virus o programa no deseado en el modo de acción automático, se ejecuta automáticamente la acción seleccionada en este área. Si activa la opción *Mostrar mensaje de advertencia*, recibirá una notificación de escritorio en caso de detección de virus.

Opciones de acción para MailGuard, WebGuard:

– **Interactivo**

Al detectar un virus o programa no deseado en el modo de acción interactivo aparece un cuadro de diálogo en el que puede seleccionar lo que debe hacerse con el objeto afectado. Este ajuste está activado de forma estándar.

– **Automático**

Al detectar un virus o programa no deseado en el modo de acción automático se ejecuta automáticamente la acción seleccionada en esta área. Si activa la opción *Mostrar mensaje de advertencia*, si se detecta un virus recibirá un mensaje de advertencia en el que podrá confirmar la acción a ejecutar.

Al detectar virus y programas no deseados en el modo de acción interactivo la reacción es que, en el mensaje de advertencia que recibe, debe seleccionar una acción para los objetos afectados y ejecutarla mediante confirmación.

Dispone de las siguientes acciones de tratamiento de los objetos afectados entre las que elegir:

Nota

Las acciones que se pueden seleccionar dependen del sistema operativo, del componente de protección (AntiVir Guard, AntiVir Scanner, AntiVir MailGuard, AntiVir WebGuard) que notifica la detección y del malware detectado.

Acciones del escáner y del Guard (sin detecciones de ProActiv):

- **Reparar**

El fichero se repara.

Sólo puede activar esta opción si el fichero detectado se puede reparar.

- **Mover a cuarentena**

El fichero se comprime con un formato especial (*.qua) y se mueve al directorio de cuarentena *INFECTED* del disco duro, de manera que ya no se puede tener acceso a él. Los ficheros de este directorio pueden repararse posteriormente en la cuarentena o, si fuera necesario, enviarse a Avira GmbH.

- **Eliminar**

El fichero se elimina. Este proceso es considerablemente más rápido que *Sobrescribir y eliminar*. Si la detección corresponde a un virus del sector de arranque, su eliminación elimina también el sector de arranque. Se escribe un sector de arranque nuevo.

- **Sobrescribir y eliminar**

El fichero se sobrescribe con un patrón predeterminado y, a continuación, se elimina. No puede restaurarse.

- **Cambiar nombre**

Se cambia el nombre del fichero añadiéndole la extensión *.vir. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. Posteriormente, los ficheros se pueden reparar y su nombre se puede cambiar de nuevo.

- **Omitir**

No se ejecuta ninguna acción más. El fichero afectado permanece activo en el equipo.

Advertencia

Existe el riesgo de pérdida de datos y de daños del sistema operativo. Use la opción *Omitir* sólo en casos excepcionales justificados.

- **Ignorar siempre**

Opción de acción en las detecciones de Guard: El Guard no ejecuta ninguna acción más. Se permite el acceso al fichero. Todos los demás accesos a ese fichero se admiten y no se notifican hasta que se reinicie el equipo o tenga lugar una actualización del fichero de firmas de virus.

- **Copiar a cuarentena**

Opción de acción al detectar un rootkit: la detección se copia a la cuarentena.

- **Reparar sector de arranque | Descargar Repairtool**

Opciones de acción en caso de detección de sectores de arranque infectados: Para disqueteras infectadas se dispone de opciones para la reparación. Si una reparación con su programa AntiVir no fuera posible, podrá descargar una herramienta especial para la detección y eliminación de virus del sector de arranque.

Nota

Si aplica acciones a procesos activos, los procesos afectados se terminarán antes de ejecutar la acción.

Acciones del Guard en caso de detecciones del componente ProActiv (aviso de acciones sospechosas de una aplicación):

– **Programa de confianza**

Se continua la ejecución de la aplicación. El programa se añade a la lista de las aplicaciones autorizadas y se excluye de la monitorización por el componente ProActiv. Al añadir la aplicación autorizada a la lista, se establece el tipo de monitorización *Contenido*. Esto significa que la aplicación solamente se excluye de una monitorización por el componente ProActiv si su contenido permanece invariable (ver Configuración::Guard::ProActiv::Filtro de aplicación: Aplicaciones permitidas).

– **Bloquear programa una vez**

La aplicación se bloquea, es decir, la ejecución de la aplicación finaliza. Las acciones de la aplicación se seguirán monitorizando por el componente ProActiv.

– **Bloquear siempre este programa**

La aplicación se bloquea, es decir, la ejecución de la aplicación finaliza. El programa se añade a la lista de las aplicaciones a bloquear y ya no podrá ejecutarse (ver Configuración::Guard::ProActiv::Filtro de aplicación: Aplicaciones a bloquear).

– **Omitir**

Se continua la ejecución de la aplicación. Las acciones de la aplicación se seguirán monitorizando por el componente ProActiv.

Acciones de MailGuard: Emails entrantes

– **Mover a cuarentena**

El email con todos sus datos adjuntos se mueve a la cuarentena. El email afectado se elimina. Un texto predeterminado sustituye el cuerpo de texto y, si fuera el caso, los datos adjuntos del email.

– **Eliminar**

El email afectado se elimina. Un texto predeterminado sustituye el cuerpo de texto y, si fuera el caso, los datos adjuntos del email.

– **Eliminar datos adjuntos**

Los datos adjuntos afectados se reemplazan por un texto predeterminado. Si está afectado el cuerpo del mensaje, se borra y se reemplaza por un texto estándar. El email en sí, se entrega.

– **Mover datos adjuntos a cuarentena**

Los datos adjuntos afectados se envían a cuarentena y después se eliminan (se reemplazan con un texto predeterminado). El cuerpo del mensaje se entrega. El adjunto puede enviarse más tarde mediante el Gestor de Cuarentena

– **Omitir**

El email afectado se entrega.

Advertencia

Hay posibilidad de que un virus o programa no deseado pueda acceder a su equipo. Seleccione la opción **Omitir** sólo en casos excepcionales justificados. Desactive la vista previa en su cliente de correo y ¡nunca abra un fichero adjunto con un doble clic!

Acciones de MailGuard: Emails salientes

– Mover correo a cuarentena (no enviar)

El email con todos sus datos adjuntos se copia a la cuarentena y no se envía. El email permanece en la bandeja de salida del cliente de correo. El programa de correo emite un mensaje de error. En cada proceso de envío posterior de la cuenta de correo se analiza este email para detectar si contiene malware.

– Bloquear envío de correo (no enviar)

El email no se envía y permanece en la bandeja de salida del cliente de correo. El programa de correo emite un mensaje de error. En cada proceso de envío posterior de la cuenta de correo se analiza este email para detectar si contiene malware.

– Omitir

El email afectado se envía.

Advertencia

De este modo, es posible que los virus o programas no deseados tengan acceso al sistema informático del destinatario del email.

Acciones del WebGuard:

– denegar acceso

El sitio Web requerido por el servidor Web y los datos solicitados no son transferidos a su navegador. Un error sobre acceso denegado ha sido mostrado en su navegador Web.

– Mover a cuarentena

La página Web solicitada por el servidor Web o los datos y ficheros transmitidos se mueven a la cuarentena. El fichero infectado puede ser restaurado a través de la cuarentena si es de vital importancia, o si es necesario, o enviarse al Avira Malware Research Center.

– Omitir

La página Web solicitada por el servidor Web o los datos y archivos transmitidos son pasados por el WebGuard a su navegador.

Advertencia

Hay posibilidad de que un virus o programa no deseado pueda acceder a su equipo. Seleccione la opción **Omitir** sólo en casos excepcionales justificados.

Nota

Se recomienda mover a la cuarentena cualquier fichero sospechoso que no se pueda reparar.

Nota

Envíenos los ficheros notificados por la heurística para analizarlos.

Esos ficheros se pueden cargar a través de nuestra página web, por ejemplo: <http://www.avira.es/file-upload>


Los ficheros notificados por la heurística pueden reconocerse por la denominación *HEUR/* o *HEURISTIC/* antepuesta al nombre de fichero, p. ej.: *HEUR/prueba.**.

5.2.10 Cuarentena: tratar con ficheros (*.qua) en cuarentena

Así puede tratar los ficheros que están en la cuarentena:

- ▶ En el Centro de control seleccione la sección **Administración :: Cuarentena**.
- ▶ Compruebe de qué ficheros se trata, de modo que pueda cargar los originales desde otro lugar a su equipo si fuera necesario.


Si desea ver información más detallada de un fichero:

- ▶ Seleccione el fichero y haga clic en .

→ Aparece el cuadro de diálogo *Propiedades* con más información sobre el fichero.

Si desea analizar de nuevo un fichero:


Se recomienda analizar un fichero cuando se ha actualizado el fichero de firmas de virus de su programa AntiVir y se sospecha de que exista una falsa alarma. Así puede confirmar tras un nuevo análisis de que se trataba de una falsa alarma y puede restablecer el fichero.

- ▶ Seleccione el fichero y haga clic en .

→ El fichero se analiza con la configuración del análisis directo para detectar virus y malware.


→ Tras el análisis, aparece el cuadro de diálogo *Estadística del análisis*, que muestra una estadística sobre el estado del fichero antes y después del nuevo análisis.

Si desea eliminar un fichero:

- ▶ Seleccione el fichero y haga clic en .

Si desea cargar el fichero en un servidor Web del Avira Malware Research Center para analizarlo:

- ▶ Seleccione el fichero que desea cargar.

- ▶ Haga clic en .

→ Aparece un cuadro de diálogo con un formulario para indicar sus datos de contacto

- ▶ Indique los datos completos.

- ▶ Seleccione un tipo: **Fichero sospechoso** o **Falsa alarma**.

- ▶ Pulse **Aceptar**.

→ El fichero se carga comprimido en un servidor Web del Avira Malware Research Center.

Nota

En los siguientes casos se recomienda un análisis por el Avira Malware Research Center: **Detección mediante heurística (fichero sospechoso):** Durante un análisis, su programa AntiVir ha clasificado un fichero como sospechoso y lo ha movido a la cuarentena; en el cuadro de diálogo de detección de virus o en el fichero de informe del análisis se recomienda el análisis del fichero por parte del Avira Malware Research Center.

Fichero sospechoso: Considera que un fichero es sospechoso por lo que lo ha añadido a la cuarentena; sin embargo, el análisis del fichero en cuanto a virus y malware da un resultado negativo.

Falsa alarma: Supone que la detección de un virus es una falsa alarma: Su programa AntiVir notifica la detección en un fichero que con toda probabilidad no está afectado por malware.


Nota

El tamaño de los ficheros que se cargan está limitado a 20 MB sin comprimir o 8 MB comprimido.

Nota

Para cargar varios ficheros simultáneamente, debe seleccionar todos los ficheros que desea cargar y pulsar el botón **Enviar objeto**.


Si desea copiar un objeto en cuarentena de la cuarentena a otro directorio:

- ▶ Seleccione el objeto en cuarentena y haga clic en .
- El botón abre un cuadro de diálogo de búsqueda en el que puede seleccionar un directorio.
- ▶ Seleccione un directorio donde desea guardar una copia del objeto en cuarentena y confirme su selección.
- El objeto de cuarentena seleccionado se guardará en el directorio elegido.

Nota

El objeto de cuarentena no es idéntico con el fichero restaurado. El objeto de cuarentena está cifrado y no puede ejecutarse ni leerse en su formato original.

Si desea exportar las propiedades de un objeto en cuarentena a un fichero de texto:

- ▶ Seleccione el objeto en cuarentena y haga clic en .
- Se abre un fichero de texto con los datos sobre el objeto en cuarentena seleccionado.
- ▶ Guarde el fichero de texto.

Los ficheros que están en la cuarentena se pueden restaurar:

- consulte el capítulo: Cuarentena: restaurar los ficheros de cuarentena

5.2.11 Cuarentena: restaurar los ficheros de cuarentena

Según el sistema operativo que use, dispondrá de distintos iconos para la restauración:

- En Windows XP y 2000:



Este icono permite restaurar los ficheros en su directorio original.



Este icono permite restaurar los ficheros en el directorio que elija.

- En Windows Vista:

En Microsoft Windows Vista, de momento el Centro de control sólo tiene derechos limitados, p. ej., de acceso a directorios y ficheros. El Centro de control sólo puede ejecutar determinadas acciones y accesos a ficheros con derechos de administrador ampliados. Estos derechos de administrador ampliados deben concederse al iniciar cualquier análisis mediante un perfil de análisis.



Este icono permite restaurar los ficheros en el directorio que elija.



Este icono permite restaurar los ficheros en su directorio original. Si para acceder a este directorio se necesitan derechos de administrador ampliados, aparece la consulta correspondiente.

Así puede restaurar los ficheros que están en la cuarentena:


Advertencia

Existe el riesgo de pérdida de datos y de daños del sistema operativo del equipo. Utilice la función *Restaurar objeto seleccionado* solamente en casos excepcionales. Restaure únicamente aquellos ficheros que pudieron repararse mediante un nuevo análisis.



- ✓ Fichero analizado y reparado con nuevo análisis.

- ▶ En el Centro de control seleccione la sección **Administración :: Cuarentena**.

Nota


Los emails y los adjuntos de emails sólo se pueden restaurar con la opción  y con la extensión *.eml.

Si desea restaurar un fichero en su ubicación original:

- ▶ Seleccione el fichero y haga clic en el icono (Windows 2000/XP: , Windows Vista ).

Esta opción no está disponible para emails.

Nota


Los emails y los adjuntos de emails sólo se pueden restaurar con la opción  y con la extensión *.eml.

- Aparece la petición de si desea restaurar el fichero.

- ▶ Haga clic en **Sí**.

- El fichero se restaura en el directorio desde el que se movió a la cuarentena.

Si desea restaurar un fichero en un determinado directorio:

- ▶ Seleccione el fichero y haga clic en .

- Aparece la petición de si desea restaurar el fichero.

- ▶ Haga clic en **Sí**.


- Aparece la ventana predeterminada de Windows para seleccionar directorios.

- ▶ Seleccione el directorio en el que va a restaurar el fichero y confirme.

- El fichero se restaura en el directorio seleccionado.

5.2.12 Cuarentena: mover fichero sospechoso a cuarentena

Así puede mover un fichero sospechoso a la cuarentena:

- ▶ En el Centro de control seleccione la sección **Administración :: Cuarentena**.
- ▶ Haga clic en .
- Aparece la ventana predeterminada de Windows para seleccionar ficheros.
- ▶ Seleccione el fichero y confirme.
- El fichero se mueve a la cuarentena.

Los ficheros que están en la cuarentena se pueden analizar con el escáner AntiVir:

- consulte el capítulo: Cuarentena: tratar con ficheros (*.qua) en cuarentena

5.2.13 Perfil de análisis: añadir o eliminar un tipo de fichero de un perfil de análisis

De esta manera, se especifica para un perfil de análisis que se analizarán adicionalmente ciertos tipos de fichero o que determinados tipos de fichero quedarán excluidos del análisis (sólo posible con la selección manual y perfiles de análisis definidos por el usuario):

- ✓ Se encuentra en el Centro de control, en la sección **Protección local :: Analizar**.
- ▶ Haga clic con el botón derecho del ratón en el perfil de análisis que desea editar.
- Aparece un menú contextual.
- ▶ Seleccione la entrada **Filtro de ficheros**.
- ▶ Despliegue más el menú contextual haciendo clic en el pequeño triángulo de la parte derecha del menú contextual.
- Aparecen las entradas *Predeterminado*, *Analizar todos los ficheros* y *Definido por el usuario*.
- ▶ Seleccione la entrada **Definido por el usuario**.
- Aparece el cuadro de diálogo *Extensiones de fichero* con una lista de todos los tipos de fichero que se analizarán con el perfil de análisis.

Si desea excluir un tipo de fichero del análisis:

- ▶ Seleccione el tipo de fichero y haga clic en **Eliminar**.

Si desea añadir un tipo de fichero al análisis:


- ▶ Seleccione el tipo de fichero.
- ▶ Haga clic en **Insertar** e introduzca la extensión de fichero del tipo de fichero en el campo de entrada

Use un máximo de 10 caracteres y no indique el punto inicial. Se admiten comodines (* e ?) como caracteres comodín.

5.2.14 Perfil de análisis: crear acceso directo en el escritorio para el perfil de análisis

Puede iniciar un análisis directo directamente desde el escritorio por medio de un acceso directo a un perfil de análisis sin tener que activar el Centro de control de su programa AntiVir.

Así se crea un acceso directo al perfil de análisis en el escritorio:

- ✓ Se encuentra en el Centro de control, en la sección **Protección local :: Analizar**.
- ▶ Seleccione el perfil de análisis para el que desea crear un enlace o acceso directo.
- ▶ Haga clic en el icono .
- Se crea el acceso directo en el escritorio.

5.2.15 Eventos: Filtrar eventos

En el Centro de control en **Información general :: Eventos** se muestran eventos generados por los componentes de su programa AntiVir (de forma parecida a como lo hace el visor de eventos del sistema operativo Windows). Los componentes del programa son:

- Updater
- Guard
- MailGuard
- Escáner
- Programador
- FireWall
- WebGuard
- Servicio de ayuda
- ProActiv

Se muestran los siguientes tipos de evento:

- Información
- Advertencia
- Error
- Detección

Así se filtran los eventos mostrados:

- ▶ En el Centro de control seleccione la sección **Información general:: Eventos**.
- ▶ Active las casillas de verificación de los componentes de programa para mostrar los eventos de los componentes activados.
 - O BIEN -
 - Desactive las casillas de verificación de los componentes de programa para ocultar los eventos de los componentes desactivados.
- ▶ Active las casillas de verificación de los tipos de evento para mostrar esos eventos.
 - O BIEN -

Desactive las casillas de verificación de los tipos de evento para ocultar esos eventos.

5.2.16 MailGuard: Excluir direcciones de email del análisis

Así se establecen las direcciones de email (remitente) que deben excluirse del análisis del MailGuard (crear listas blancas):

- ▶ En el Centro de control seleccione **Protección online :: MailGuard**.
- En la lista verá los emails recibidos.
- ▶ Seleccione el email que desea excluir del análisis del MailGuard.
- ▶ Haga clic en el icono pertinente para excluir el email del análisis del MailGuard:



La dirección de email seleccionada ya no se analizará en el futuro en cuanto a virus y programas no deseados.

- La dirección del remitente de email se incluye en la lista de exclusiones y ya no se analizará en cuanto a virus y programas no deseados .

Advertencia

Excluya únicamente direcciones de email de remitentes de total confianza del análisis del MailGuard.

Nota

En la configuración, en MailGuard:: General :: Excepciones puede introducir más direcciones de email en la lista de exclusiones o excluir direcciones de ella.

5.2.17 FireWall: Seleccionar nivel de seguridad para FireWall

Puede seleccionar entre distintos niveles de seguridad. En función de ello, dispondrá de diferentes posibilidades de configuración para las reglas del adaptador.

Dispone de los siguientes niveles de seguridad:

- **Bajo**
 - Se detecta el desbordamiento y el escaneo de puertos.
- **Medio**
 - Se descartan los paquetes TCP y UDP sospechosos.
 - Se impide el desbordamiento y el escaneo de puertos.
- **Alto**
 - El equipo es invisible en la red.
 - Se bloquean las conexiones desde el exterior.
 - Se impide el desbordamiento y el escaneo de puertos.
- **Usuario**
 - Reglas definidas por el usuario: el programa cambia automáticamente a este nivel de seguridad si se cambiaron reglas del adaptador.

Nota

La configuración estándar del nivel de seguridad para todas las reglas predefinidas de Avira FireWall es **Alto**.

Así se establece el nivel de seguridad para el FireWall:

- ▶ En el Centro de control seleccione **Protección:: FireWall**.
- ▶ Sitúe el control deslizante en el nivel de seguridad que desee.
- El nivel de seguridad seleccionado se activa de inmediato.

6 Escáner

El componente escáner permite ejecutar con precisión análisis para detectar virus y programas no deseados (análisis directo). Dispone de las siguientes posibilidades de analizar ficheros afectados:

- **Análisis directo mediante menú contextual**
El análisis directo a través del menú contextual (botón derecho del ratón - entrada **Analizar ficheros seleccionados con AntiVir**) se recomienda, por ejemplo, cuando se desee analizar ficheros y directorios individuales en Windows Explorer. Otra ventaja es que no es necesario arrancar primero el Centro de control mediante el menú contextual para realizar un análisis directo.
- **Análisis directo con Arrastrar y soltar**
Si se arrastra un fichero o directorio a la ventana del Centro de control, el escáner analiza el fichero o el directorio y todos los subdirectorios que contenga. Esto es recomendable si desea analizar ficheros o directorios individualmente, por ejemplo, aquéllos que se encuentran en el escritorio.
- **Análisis mediante perfiles**
Esto es lo recomendado si, con frecuencia hace un análisis de determinados ficheros o carpetas (por ejemplo en algún directorio de trabajo o unidad extraíble). No necesita seleccionar estas carpetas y unidades otra vez en cada nuevo análisis, use simplemente el perfil deseado.
- **Análisis directo mediante el programador**
El programador le permite programar la ejecución de tareas de análisis en el tiempo.

Al analizar la existencia de rootkits, virus del sector de arranque y al analizar procesos activos se requieren procedimientos especiales. Dispone de las siguientes opciones:

- Análisis de rootkits mediante el perfil de análisis *Análisis de malware activo*
- Análisis de procesos activos mediante el perfil de análisis **Procesos activos**
- Análisis de virus del sector de arranque mediante el comando de menú **Analizar virus del sector de arranque** en el menú **Herramientas**

7 Actualizaciones

La eficacia de un software antivirus crece y disminuye con la actualidad del programa, sobre todo la del fichero de firmas de virus y la del motor de análisis. Para la ejecución de actualizaciones, se ha integrado el componente Updater en su AntiVir . El Updater se encarga de que su programa AntiVir funcione siempre con la vigencia más reciente y pueda así detectar los virus que aparecen a diario. Updater actualiza los siguientes componentes:

- Fichero de firmas de virus:

El fichero de firmas de virus contiene los patrones de detección de los programas malintencionados que utiliza su programa AntiVir en los análisis de virus y malware, así como en la reparación de objetos infectados.

- Motor de análisis:

El motor de análisis contiene los métodos que usa su programa AntiVir para analizar la existencia de virus y malware.

- Ficheros de programa (actualización de producto):

Los paquetes de actualización para actualizar los productos proporcionan más funciones para cada uno de los componentes del programa.

Al ejecutar una actualización, se comprueba el grado de vigencia o actualidad del fichero de firmas de virus y del motor de análisis y, si fuera necesario, se actualizan. Según los parámetros establecidos en la configuración, Updater ejecuta, además, una actualización de producto o bien le informa sobre la disponibilidad de actualizaciones de producto. Después de una actualización de producto puede ser preciso un reinicio de su equipo. Si sólo se lleva a cabo una actualización del fichero de firmas de virus y del motor de análisis, no se requiere el reinicio del equipo.

Nota

Por razones de seguridad, Updater comprueba si el fichero host de Windows del equipo se ha modificado en lo que se refiere, por ejemplo, a una manipulación por parte de malware de la URL de actualización con el fin de que Updater se dirija a páginas de descarga no deseadas. Si se manipuló el fichero host de Windows, queda constancia en el fichero de informe de Updater.

Una actualización se ejecuta automáticamente con el siguiente intervalo: 60 minutos. Puede modificar o desactivar la actualización automática a través de la configuración (Configuración::Actualización).

En el Centro de control en el programador puede configurar las tareas de actualización que Updater ejecutará con los intervalos indicados. También puede iniciar la actualización manualmente:

- En el Centro de control: en el menú Actualizar y en la sección Estado
- Por medio del menú contextual del icono de bandeja

Las actualizaciones se reciben de Internet a través de un servidor Web del productor o bien a través de un servidor Web o servidor de ficheros de Intranet, que descarga los ficheros de actualización de Internet y los pone a disposición de los demás equipos de la red. Ello es útil si desea actualizar programas AntiVir en varios equipos de la red. Mediante la instalación de un servidor de descarga en Intranet puede garantizarse la vigencia de programas AntiVir en los equipos que requieran protección al tiempo que se ahorran recursos. Para establecer un servidor de descargas funcional en Intranet se requiere un servidor que ofrezca la estructura de actualización de su programa AntiVir.

Nota

Puede utilizar AntiVir Internet Update Manager (servidor de ficheros o servidor Web bajo Windows) como servidor Web o servidor de ficheros en Intranet. El AntiVir Internet Update Manager refleja el servidor de descargas de los productos Avira AntiVir y se puede obtener en Internet en el sitio Web de Avira:

<http://www.avira.es>

Si se usa un servidor Web, la descarga tiene lugar mediante el protocolo HTTP. Si se usa un servidor de ficheros, se produce un acceso a los ficheros de actualización a través de la red. La conexión con el servidor Web o el servidor de ficheros se configura en la configuración en General :: Actualización. En el caso de la configuración predeterminada, se utiliza la conexión de Internet existente como conexión a los servidores Web de Avira GmbH.

8 Avira FireWall:: Información general

Avira FireWall supervisa y regula el tráfico de datos entrante y saliente de su sistema informático y le protege frente a distintos ataques y amenazas procedentes de Internet: sobre la base de directrices de seguridad se permite o rechaza el tráfico de datos entrante y saliente o la escucha de puertos. Recibirá una notificación en el escritorio si Avira FireWall rechaza las actividades de la red y, por lo tanto, bloquea las conexiones de red. Dispone de las siguientes posibilidades para configurar Avira FireWall:

- estableciendo el nivel de seguridad en el Centro de control

En el Centro de control puede configurar el nivel de seguridad. Los niveles de seguridad *Bajo*, *Medio* y *Alto* contienen varias reglas de seguridad cada uno que se complementan y están basadas en filtros de paquete. Estas reglas de seguridad están guardadas como reglas de adaptador predefinidas en la configuración en FireWall::Reglas del adaptador.

- guardando acciones en la ventana Evento de red

Cuando una aplicación intenta establecer por primera vez una conexión de red o de Internet, se abre la ventana emergente *Evento de red*. En la ventana *Evento de red* el usuario puede seleccionar si la actividad de red de la aplicación se permitirá o se rechazará. Si está activada la opción **Guardar acción para esta aplicación**, la acción se crea como regla de aplicación y se guarda en la configuración, en FireWall::Reglas de aplicación. Al guardar las acciones en la ventana Evento de red se obtiene un conjunto de reglas para las actividades de red de las aplicaciones.

Nota

En el caso de aplicaciones de proveedores de confianza, el acceso a la red se permite de forma estándar, a no ser que una regla del adaptador prohíba el acceso a la red. Tiene la posibilidad de quitar proveedores de la lista de proveedores de confianza.

- creando reglas de adaptador y de aplicación en la configuración

En la configuración puede modificar las reglas predefinidas del adaptador o crear nuevas reglas del adaptador. El nivel de seguridad del FireWall se establece automáticamente en el valor *Usuario* cuando se añaden o modifican reglas del adaptador.

Las reglas de aplicación permiten definir reglas de supervisión específicas de aplicaciones:

Unas sencillas reglas de aplicación permiten establecer si se permitirán o rechazarán todas las actividades de red de una aplicación de software, o si se tratarán de manera interactiva por medio de la ventana emergente *Evento de red*.

En la sección *Reglas de aplicación* de la configuración avanzada puede definir distintos filtros de paquete para una aplicación que se ejecutarán como reglas específicas de la aplicación.

Nota

Se distingue entre dos modos en el caso de las reglas de aplicación: *con privilegios* y *filtrado*. En las reglas de aplicación del modo *filtrado* se da prioridad a las reglas del adaptador coincidentes, es decir, la regla del adaptador coincidente se ejecuta después de la regla de aplicación. Así, puede darse el caso de que el acceso a la red de aplicaciones permitidas se rechace debido a un nivel de seguridad alto o a la existencia de reglas del adaptador. En las reglas de aplicación del modo *con privilegios* se omiten las reglas del adaptador. Si se permiten aplicaciones en el modo *con privilegios*, el acceso a la red de la aplicación se permite en todos los casos.

9 Solución de problemas, sugerencias

En este capítulo encontrará indicaciones importantes sobre la solución de problemas y otras sugerencias para el uso de su programa AntiVir.

consulte el capítulo Ayuda en caso de problemas

consulte el capítulo Comandos de teclado

consulte el capítulo Centro de seguridad de Windows

9.1 Ayuda en caso de problemas

Aquí encontrarás información sobre las causas y las soluciones a los posibles problemas

- Aparece el mensaje de error *No puede abrirse el fichero de licencia*.
- AntiVir MailGuard no funciona.
- No hay conexión de red en una máquina virtual si se instala Avira FireWall en el sistema operativo host y el nivel de seguridad de Avira FireWall se ha configurado en el nivel medio o alto.
- La conexión Virtual Private Network (VPN) se bloquea si el nivel de seguridad de Avira FireWall es medio o alto.
- Un email enviado a través de una conexión TSL ha sido bloqueado por MailGuard.
- El chat en Web no funciona: no se muestran los mensajes de chat

Aparece el mensaje de error *no puede abrirse el fichero de licencia*.

Causa: El fichero está encriptado.

- ▶ Para activar la licencia, simplemente hay que copiarla en la carpeta del programa. Consulte también Administración de licencias.

Aparece el mensaje de error *Error de establecimiento de conexión al descargar el fichero...* cuando se intenta iniciar una actualización.

Causa: Su conexión está inactiva. Por ello no se puede establecer una conexión con el servidor Web en Internet.

- ▶ Compruebe que los servicios de Internet como la navegación o el correo funcionan. Si no, restablece la conexión.

Causa: El servidor proxy no se puede alcanzar.

- ▶ Compruebe si la información de inicio de sesión para el servidor proxy ha cambiado y cambie su configuración si es necesario.

Causa: El fichero update.exe no está totalmente aprobado por su Firewall .

- ▶ Asegúrese de que el fichero update.exe está totalmente aprobado por su Firewall .

Si no:

- ▶ Compruebe los parámetros en la configuración (Modo experto) en General :: Actualización.

Los virus y el malware no se pueden mover ni borrar.

Causa: El fichero ha sido cargado por Windows y está activo

- ▶ Actualice su producto AntiVir.
- ▶ Si usa el sistema operativo Windows XP, desactive la Restauración del Sistema.
- ▶ Arranque el equipo en modo seguro
- ▶ Inicie el programa AntiVir y la configuración (modo experto).
- ▶ Seleccione Escáner:: Análisis :: Ficheros :: Todos los ficheros y pulse **Aceptar**.
- ▶ Inicie un análisis de todos los discos locales
- ▶ Arranque el equipo en modo normal
- ▶ Inicie un análisis en modo normal
- ▶ Si no se ha encontrado virus o malware, active la Restauración del Sistema.

El icono de bandeja muestra un estado desactivado.

Causa: AntiVir Guard está desactivado.

- ▶ Pulse en el Centro de control en la sección Descripción general :: Estado, en el área AntiVir Guard en el enlace **Activar**.

Causa: AntiVir Guard está siendo bloqueado por un Firewall.

- ▶ Habilite una autorización general para AntiVir Guard en la configuración de su Firewall . AntiVir Guard sólo trabaja con la dirección 127.0.0.1 (host local). No se ha establecido conexión con Internet. Lo mismo es aplicable para AntiVir MailGuard.

Si no:

- ▶ Compruebe el tipo de inicio del servicio AntiVir Guard. Si fuera el caso, active el servicio: En la barra de inicio seleccione "Inicio | Configuración | Panel de control". Inicie, en el Panel de Control, los "Servicios" con un doble clic (en Windows 2000 y Windows XP los servicios se encuentran en la subcarpeta "Herramientas Administrativas"). Busque la entrada *Avira AntiVir Guard*. El inicio debe ser "Automático" y el estado, "Iniciado". Si es necesario, inicie el servicio manualmente, seleccionando la línea y pulsando sobre "Iniciar". Si aparece un error, compruebe los eventos que aparecen.

El equipo se vuelve extremadamente lento cuando realizo una copia de seguridad.

Causa: Durante el proceso de backup, AntiVir Guard analiza todos los ficheros usados en el procedimiento de ejecución de copias de seguridad de datos.

- ▶ En la configuración (modo experto) seleccione Guard:: Análisis :: Excepciones e introduzca el nombre de proceso del software de backup.

Mi Firewall notifica la existencia de AntiVir Guard y AntiVir MailGuard en cuanto estos se activan.

Causa: La comunicación de AntiVir Guard y AntiVir MailGuard se realiza mediante el protocolo de Internet TCP/IP. Un Firewall monitoriza todas las conexiones con este protocolo.

- ▶ Habilite una autorización general para AntiVir Guard y AntiVir MailGuard. AntiVir Guard sólo trabaja con la dirección 127.0.0.1 (host local). No se ha establecido conexión con Internet. Lo mismo es aplicable para AntiVir MailGuard.

AntiVir MailGuard no funciona.

Asegúrese de que AntiVir MailGuard funciona comprobando los siguientes puntos en caso de que se presenten problemas con AntiVir MailGuard.

Lista de Comprobación

- ▶ Compruebe que su cliente de correo entra en el servidor vía Kerberos, APOP o RPA. Actualmente estos métodos no se soportan.
- ▶ Compruebe si su cliente de correo se registra mediante SSL (también denominado TSL – Transport Layer Security) en el servidor. AntiVir MailGuard no es compatible con SSL y por tanto finaliza las conexiones cifradas mediante SSL. Si desea utilizar conexiones cifradas mediante SSL sin la protección de MailGuard, deberá utilizar para la conexión un puerto distinto que los puertos monitorizados por MailGuard. Los puertos monitorizados por MailGuard pueden configurarse en la configuración en MailGuard::Análisis.
- ▶ ¿Está activo el servicio AntiVir MailGuard? Si fuera el caso, active el servicio: En la barra de inicio seleccione "Inicio | Configuración | Panel de control". Inicie, en el Panel de Control, los "Servicios" con un doble clic (en Windows 2000 y Windows XP los servicios se encuentran en la subcarpeta "Herramientas Administrativas"). Busque la entrada *Avira AntiVir MailGuard*. El inicio debe ser "Automático" y el estado, "Iniciado". Si es necesario, inicie el servicio manualmente, seleccionando la línea y pulsando sobre "Iniciar". Si aparece un error, compruebe los eventos que aparecen. Si esto no funciona, desinstale por completo el programa AntiVir a través de "Inicio | Panel de Control | Agregar o quitar programas", reinicie el sistema y vuelva a instalar el programa AntiVir.

General

- ▶ Las conexiones POP3 encriptadas vía SSL (también conocidas como TLS), no se protegen en la actualidad y son ignoradas.
- ▶ La verificación del servidor de correo sólo se soporta vía "Contraseña". "Kerberos" y "RPA" no son soportados actualmente.
- ▶ Su programa AntiVir no comprueba los emails salientes en busca de virus y programas no deseados.

Nota

Recomendamos que se instalen regularmente las actualizaciones de Microsoft para evitar posibles agujeros de seguridad.

No hay conexión de red en una máquina virtual si se instala Avira FireWall en el sistema operativo host y el nivel de seguridad de Avira FireWall se ha configurado en el nivel medio o alto.

Cuando se instala Avira FireWall en un equipo en el que funciona adicionalmente una máquina virtual (por ejemplo, VMWARE, Virtual PC...), este bloquea todas las conexiones de red de la máquina virtual si el nivel de seguridad de Avira FireWall está puesto a nivel medio o alto. Con el nivel de seguridad Bajo, FireWall reacciona según lo previsto.

Causa: La máquina virtual tiene una tarjeta de red virtual, simulada por software. Por medio de esta emulación, los paquetes de datos del sistema invitado se encapsulan en paquetes especiales (denominados UDP) y se dirigen a través de la puerta de enlace externa de vuelta al sistema host. Avira FireWall rechaza estos paquetes que vienen desde el exterior a partir del nivel de seguridad Medio.

Para evitar esta característica, siga los siguientes pasos :

- ▶ En el Centro de control seleccione **Protección online :: FireWall**.

- ▶ Haga clic en **Configuración**.
- ▶ Aparece el cuadro de diálogo *Configuración*. Se encuentra en la sección de configuración *Reglas de aplicación*.
- ▶ Active el **Modo Experto**.
- ▶ Seleccione la sección de configuración **Reglas del adaptador**.
- ▶ Haga clic en **Añadir regla**.
- ▶ En *Reglas entrantes* seleccione **UDP**.
- ▶ Escriba el **Nombre** de la regla en la Sección Nombre de la Regla.
- ▶ Haga clic en **Aceptar**.
- ▶ Compruebe que la regla está por encima de **Bloquear todos los paquetes IP**.

Advertencia

Esta regla es potencialmente peligrosa ya que permite todo el tráfico UDP sin ningún filtrado! Después de trabajar con la máquina virtual, cambie a su nivel de seguridad previo.

La conexión Virtual Private Network (VPN) se bloquea si el nivel de seguridad de Avira FireWall es medio o alto.

Causa: Este problema es causado por la última regla **Bloquear todos los paquetes IP** que descarta todos los paquetes que no cumplen las reglas por encima de ella. Esta regla filtra los paquetes enviados por el software de VPN, ya que debido a su tipo (los llamados paquetes GRE) no pertenecen a ninguna de las otras categorías.

Reemplace la regla **Denegar todos los paquetes IP** por dos reglas nuevas que bloqueen los paquetes TCP y UPD. De esta forma, se permiten paquetes de otros protocolos.

Un email enviado a través de una conexión TSL ha sido bloqueado por MailGuard.

Causa: El protocolo de seguridad del nivel de transporte (TLS, Transport Layer Security: protocolo de cifrado para transmisiones de datos en Internet) no es compatible actualmente con MailGuard. Dispone de las siguientes posibilidades para enviar el email:

- ▶ Utilice un puerto distinto del puerto 25 que utiliza SMTP. De este modo evita la supervisión por parte de MailGuard
- ▶ Renuncie a la conexión TSL cifrada y desactive la compatibilidad con TSL en su cliente de correo.
- ▶ Desactive (temporalmente) la supervisión de los emails salientes por parte de MailGuard en la configuración, en MailGuard:Análisis.

El chat en Web no funciona: no se muestran los mensajes de chat, en el explorador se cargan datos.

Este fenómeno puede aparecer en chats basados en el protocolo HTTP con "transfer-encoding= chunked".

Causa: WebGuard analiza por completo los datos enviados para detectar virus y programas no deseados antes de cargarlos en el explorador Web. En las transferencias de datos con "r;r;transfer-encoding= chunked" el WebGuard no puede detectar la longitud del mensaje o la cantidad de datos.

- Indique en la configuración la URL del chat en Web como excepción (consulte configuración: WebGuard::Excepciones).

9.2 Atajos

Los comandos de teclado -conocidos como accesos directos - ofrecen una rápida posibilidad de encontrar módulos individuales, ejecutar acciones y navegar por el programa .

A continuación hacemos un repaso de los comando de teclado disponibles. Consulte las indicaciones adicionales sobre la funcionalidad en el capítulo correspondiente de la ayuda.

9.2.1 En los cuadros de diálogo

Comando de teclado	Descripción
Ctrl + Tab Ctrl + Avanzar Página	Navegación en el Centro de control Cambiar a la sección siguiente.
Ctrl + May+ Tab Ctrl + Retroceder Página	Navegación en el Centro de control Cambiar a la sección anterior.
← ↑ → ↓	Navegación en las secciones de configuración En primer lugar, seleccione una sección de configuración mediante el ratón.
Tab	Cambiar a la siguiente acción u opciones de grupo.
May+ Tab	Cambiar a la opción previa u opciones de grupo
← ↑ → ↓	Cambiar entre las opciones en una lista desplegable o entre varias opciones en un grupo de opciones.
Espacio	Activar o desactiva una marca. si la opción activa es una de marcar.
Alt + letra subrayada	Selecciona opción o lanzar comando
Alt + ↓ F4	Abre la lista desplegable seleccionada
Esc	Cerrar el campo de lista desplegable seleccionado. Cancelar el comando y cerrar el cuadro de diálogo.
Intro	Ejecutar comando de la opción o botón activos

9.2.2 En la Ayuda

Comando de teclado	Descripción
Alt + Espacio	Mostrar el menú del sistema
Alt + Tab	Conmuta entre la ayuda y otras posibles ventanas abiertas.
Alt + F4	Cerrar ayuda
May+ F10	Mostrar el menú de contexto de la ayuda.
Ctrl + Tab	Cambiar a la sección siguiente en la ventana de exploración.
Ctrl + May+ Tab	Cambiar a la sección anterior en la ventana de exploración.
Retr. Pág.	Cambia al asunto. el cual se muestra sobre los contenidos, en el índice o en la lista de los resultados encontrados.
Av. Pág.	Cambiar al tema que se muestra debajo del tema actual en el índice de materias, el índice o en la lista de resultados encontrados.
Retr. Pág. Av. Pág.	Avanzar y retroceder por un tema.

9.2.3 En el Centro de control

General

Comando de teclado	Descripción
F1	Mostrar la Ayuda
Alt + F4	Cerrar Centro de control
F5	Refrescar la pantalla
F8	Abrir la configuración
F9	Iniciar actualización

Sección Analizar

Comando de teclado	Descripción
F2	Cambiar nombre del perfil seleccionado
F3	Iniciar análisis con el perfil seleccionado
F4	Crear un acceso directo en el escritorio para el perfil seleccionado
Insertar	Crear nuevo perfil
Suprimir	Eliminar el perfil seleccionado

Sección FireWall

Comando de teclado	Descripción
Enter	Propiedades

Sección Cuarentena

Comando de teclado	Descripción
F2	Volver a analizar objeto
F3	Restaurar objeto
F4	Enviar objeto
F6	Restaurar objeto en...
Enter	Propiedades
Insertar	Añadir fichero
Suprimir	Eliminar objeto

Sección Programador

Comando de teclado	Descripción
F2	Modificar tarea
Enter	Propiedades
Insertar	Insertar nueva tarea
Suprimir	Eliminar tarea

Sección Informes

Comando de teclado	Descripción
F3	Mostrar fichero de informe
F4	Imprimir fichero de informe
Enter	Mostrar informe
Suprimir	Borrar informes

Sección Eventos

Comando de teclado	Descripción
F3	Exportar eventos
Enter	Mostrar evento
Suprimir	Eliminar eventos

9.3 Centro de Seguridad de Windows

- Windows XP Service Pack 2 o posterior -

9.3.1 General

El Centro de Seguridad de Windows comprueba el estado del equipo en aspectos importantes de seguridad.

Si se detecta un problema en algunos de estos puntos (por ejemplo por tener un antivirus que ha caducado), el Centro de Seguridad crea una alerta y da recomendaciones para proteger al equipo.

9.3.2 El Centro de seguridad de Windows y su programa Antivir

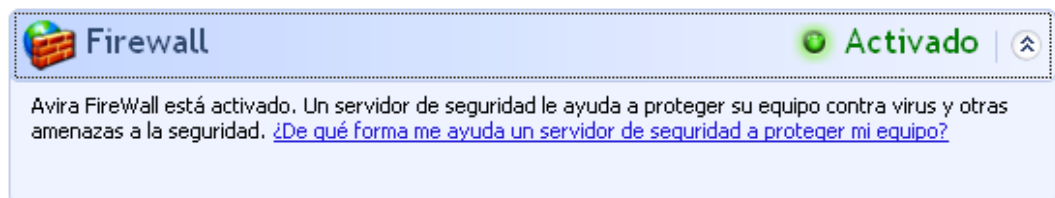
Firewall

Puede recibir la siguiente información del Centro de Seguridad con respecto a su Firewall:

- Firewall ACTIVADO / Firewall encendido
- Firewall DESACTIVADO / Apagado

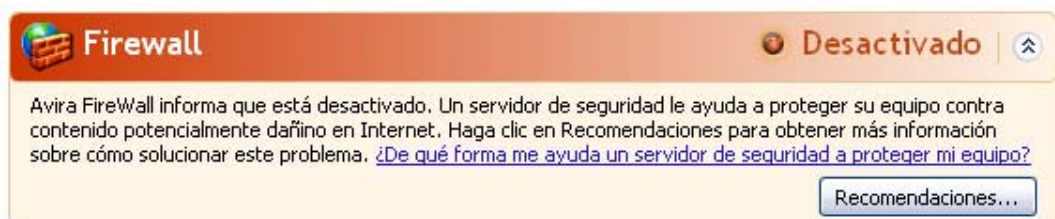
Firewall ACTIVO / Firewall desactivado

Tras la instalación de su programa AntiVir y apagar el cortafuegos de Windows, se recibe el siguiente mensaje:



Firewall INACTIVO / Firewall desactivado

Recibirá el siguiente mensaje si desactiva Avira FireWall:



Nota

Puede activar o desactivar el Avira FireWall a través de Estado en el Centro de control.

Advertencia

Si desactiva el Avira FireWall, su equipo ya no queda protegido del acceso por parte de usuarios no autorizados a través de la red o de Internet.

Software de protección / Protección contra software malicioso

Puede recibir la siguiente información del Centro de Seguridad con respecto a su protección Antivirus.

Sin protección antivirus

Protección Antivirus Caducada

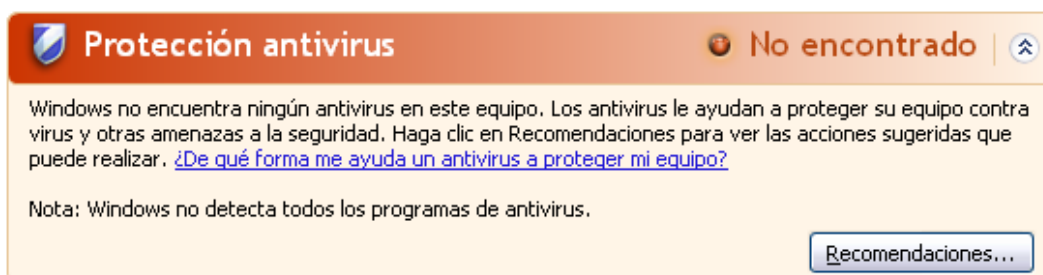
Protección Antivirus ACTIVA

Protección Antivirus INACTIVA

Protección antivirus NO MONITORIZADA

Protección Antivirus NO ENCONTRADA

Esta información aparece cuando el Centro de Seguridad de Windows no ha encontrado ningún software antivirus en su equipo.



Protección antivirus No encontrado

Windows no encuentra ningún antivirus en este equipo. Los antivirus le ayudan a proteger su equipo contra virus y otras amenazas a la seguridad. Haga clic en Recomendaciones para ver las acciones sugeridas que puede realizar. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)

Nota: Windows no detecta todos los programas de antivirus.

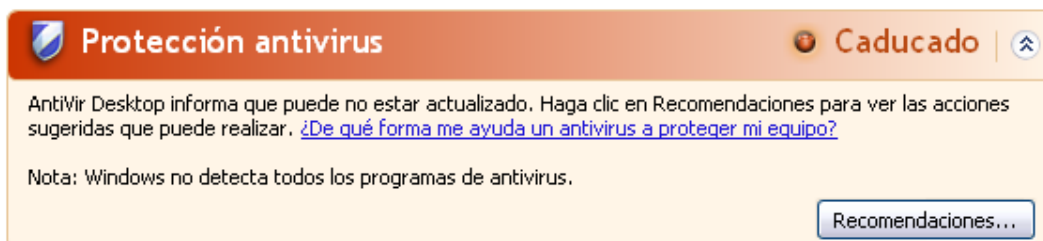
Recomendaciones...

Nota

Instale su programa AntiVir en su equipo para protegerlo contra virus y otros programas no deseados.

Protección Antivirus NO ACTUAL

Si ya ha instalado Windows XP Service Pack 2 o Windows Vista e instala después su programa AntiVir, o si instala Windows XP Service Pack 2 o Windows Vista en un sistema que ya tenga instalado su programa AntiVir, recibirá el siguiente mensaje:



Protección antivirus Caducado

AntiVir Desktop informa que puede no estar actualizado. Haga clic en Recomendaciones para ver las acciones sugeridas que puede realizar. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)

Nota: Windows no detecta todos los programas de antivirus.

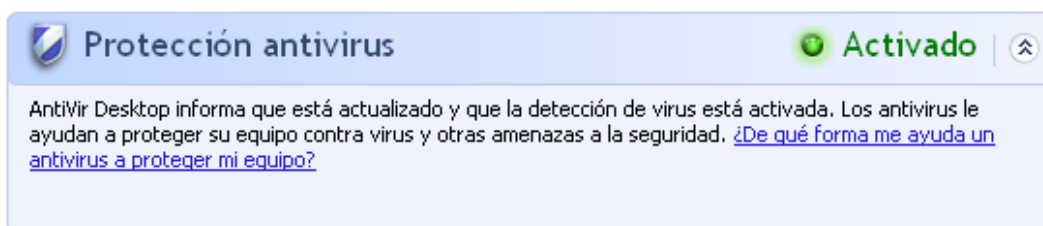
Recomendaciones...

Nota

Para que el Centro de seguridad de Windows reconozca a su programa AntiVir como un producto actualizado, debe de llevarse a cabo una actualización forzosamente tras la instalación. Actualice su sistema mediante una Actualización.

Protección Antivirus ACTIVA

Tras la instalación de su programa AntiVir y la actualización subsecuente, se recibe la siguiente indicación:



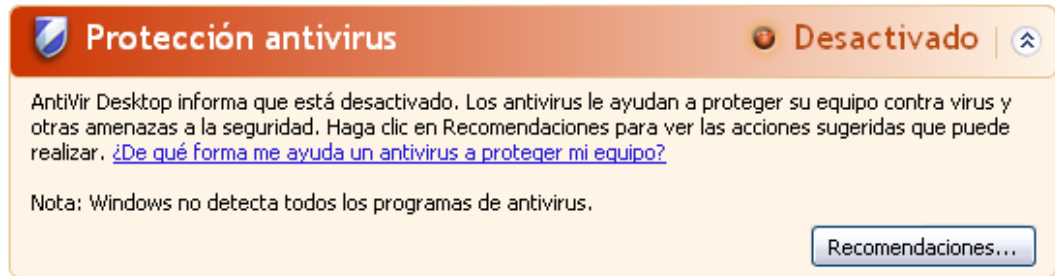
Protección antivirus Activado

AntiVir Desktop informa que está actualizado y que la detección de virus está activada. Los antivirus le ayudan a proteger su equipo contra virus y otras amenazas a la seguridad. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)

Su programa Anti Vir está actualizado y AntiVir Guard está activo.

Protección Antivirus INACTIVA

Recibirá el siguiente mensaje si desactiva AntiVir Guard o detiene el servicio Guard.



The screenshot shows a Windows Security notification titled "Protección antivirus" with a status of "Desactivado". The text inside the notification reads: "AntiVir Desktop informa que está desactivado. Los antivirus le ayudan a proteger su equipo contra virus y otras amenazas a la seguridad. Haga clic en Recomendaciones para ver las acciones sugeridas que puede realizar. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)" Below this text is a note: "Nota: Windows no detecta todos los programas de antivirus." and a button labeled "Recomendaciones...".

Notas

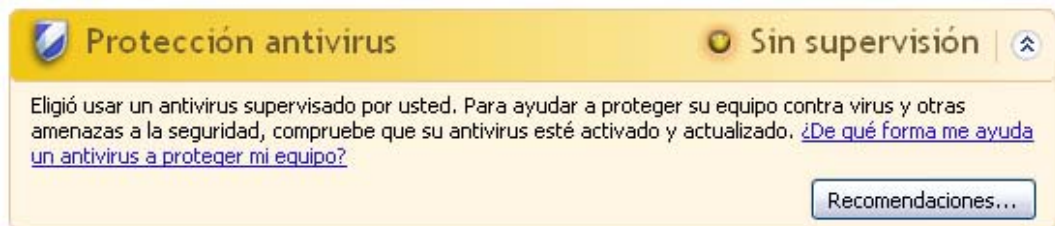
Puede activar o desactivar el AntiVir Guard en la sección Descripción general :: Activar o desactivar el estado del Centro de Control. Además, puede ver que está activado el AntiVir Guard si el paraguas rojo en la barra de tareas está abierto.

Protección Antivirus NO MONITORIZADA

Si recibe el siguiente mensaje del Centro de Seguridad de Windows, ha decidido que quiere monitorizar su software de antivirus por si mismo.

Nota

Windows Vista no admite esta función.



The screenshot shows a Windows Security notification titled "Protección antivirus" with a status of "Sin supervisión". The text inside the notification reads: "Elegió usar un antivirus supervisado por usted. Para ayudar a proteger su equipo contra virus y otras amenazas a la seguridad, compruebe que su antivirus esté activado y actualizado. [¿De qué forma me ayuda un antivirus a proteger mi equipo?](#)" Below this text is a button labeled "Recomendaciones...".

Nota

Su programa AntiVir es compatible con el Centro de seguridad de Windows. Puede activar esta opción siempre que lo desee con el botón "Recomendaciones...".

Nota

Incluso si ha instalado Windows XP Service Pack 2 o Windows Vista, necesita una solución antivirus. Aunque Windows XP Service Pack 2 monitoriza el software de Antivirus, no contiene ninguna función antivirus en si mismo. Por lo tanto ¡necesita una solución Antivirus adicional para estar protegido!

10 Virus y más

10.1 Categorías de riesgos

Programa de marcación telefónica con coste (DIALER)

Algunos servicios en Internet son de pago. A éstos pueden accederse mediante dialers (marcadores) que pudieran estar conectados a la línea telefónica (normalmente los 9XX). Instalados en el equipo, estos programas (denominados dialer) se encargan de establecer conexiones a través de números de tarifa de cobro adicional, cuya configuración puede abarcar un espectro muy amplio.

La comercialización de contenidos en línea a través de la factura telefónica es legal y puede tener ventajas para el usuario. Los dialers serios no permiten que surjan dudas acerca del uso consciente y moderado por parte del cliente. Únicamente se instalan en la máquina del usuario si éste da su conformidad al respecto. Esta conformidad debe darse a raíz de un etiquetado o una petición unívocos y claramente reconocibles. El establecimiento de la conexión de los programas tipo dialer serios se muestra de forma inequívoca. Además, los dialer serios informan con exactitud y de forma llamativa sobre el importe de los costes que implican.

Lamentablemente, existen dialers que se instalan en los equipos disimuladamente, de manera cuestionable o incluso con intenciones fraudulentas. Por ejemplo, reemplazan la conexión de acceso telefónico a redes predeterminada del usuario de Internet con su ISP (proveedor de servicios de Internet) y llaman en cada conexión a un número 0190/0900 que genera gastos y presenta tarifas exorbitantes. Además, es posible que, hasta no recibir la próxima factura telefónica, el usuario afectado no se dé cuenta de que un programa no deseado tipo dialer ha estado marcando cada vez que se establecía una conexión a Internet un número con tarifa de cobro adicional, por lo que sus gastos han crecido drásticamente.

Para protegerse en general frente a programas no deseados de marcación telefónica con coste (dialers de 0190/0900), recomendamos contactar con la compañía que le ofrece el servicio de telefonía para que bloquee ese rango de números.

Su programa AntiVir detecta los programas de marcación telefónica con coste conocidos.

Si en la configuración de Categorías de riesgos se activa con una marca la opción **Programas de marcación telefónica con coste (DIALER)**, si se detecta un programa de este tipo se emite el correspondiente mensaje de advertencia. Así puede eliminar el potencial peligro de los dialers no deseados. De todas formas si hay algún dialer que desee utilizar, puede declararlo como archivo excepcional y excluirlo del análisis en el futuro.

Juegos (GAMES)

Los juegos pueden ser evitados a la hora de trabajar. La cantidad de juegos accesibles desde Internet puede ser una amenaza a la productividad. La selección de posibles juegos en Internet es inmensa. Incluso el juego por email se está haciendo popular: existen numerosas variantes de juegos de este tipo desde los de ajedrez hasta los especializados en "estrategias navales" (batallas con torpedos incluidas). Las rondas de juego se envían a través de programas de correo a los contrincantes y éstos las contestan.

Las investigaciones demuestran que el tiempo dedicado a jugar con el equipo en horario laboral alcanza ya magnitudes económicamente importantes. Así que no sorprende que las empresas se tomen en serio este tipo de posibles problemas.

Su programa AntiVir reconoce los juegos de ordenador. Activando en la configuración de Categorías de riesgos la opción **Juegos (GAMES)** con una marca, recibirá la correspondiente advertencia en caso de que su programa AntiVir realice una detección. El juego ha terminado en el sentido literal, porque tiene la posibilidad de eliminarlo fácilmente.

Programas broma (JOKES)

Los programas de broma sólo deberían estar destinados a poner un toque de humor sin llegar a ocasionar perjuicios ni multiplicarse a sí mismos. El equipo suele empezar a emitir una melodía o a mostrar algo inusual en pantalla tras haber activado el programa de broma. Ejemplos clásicos son: DRAIN.COM (lavadora en la disquetera) o BUGSRES.COM (come pantallas).

Pero... ¡cuidado! Los síntomas de los programas de broma pueden ser también el resultado de virus o troyanos. Cuanto menos, intentan llamar la atención y entonces el usuario por desconocimiento puede provocar aún más daño.

Su programa AntiVir puede detectar los programas de broma ampliando sus rutinas de análisis e identificación y eliminarlos, tratándolos como programas no deseados, si fuera necesario. Activando en la configuración Categorías de riesgos la opción **Programas broma (JOKES)** con una marca se informa en caso de realizarse una detección.

Riesgo de seguridad-confidencialidad (Security privacy risk - SPR)

Software que puede comprometer la seguridad del sistema, iniciar actividades de programas no deseadas, violar su privacidad o espiar datos y/o comportamientos, lo que probablemente no sea deseado.

Su programa AntiVir detecta el software de "Riesgo de seguridad-confidencialidad". Si se activa la opción **Riesgo de seguridad-confidencialidad (SPR)** en Categorías de riesgos avanzadas con una marca, se recibirán alertas si su programa AntiVir detecta software de este tipo.

Software de control de puerta trasera (backdoor - BDC)

Para el robo de datos o la manipulación del equipo, se introduce un programa backdoor "por la puerta trasera" sin que el usuario lo detecte. Este programa puede ser controlado por terceras personas vía Internet o en un entorno de red.

Su programa AntiVir reconoce el "software de control de puerta trasera". Activando en la configuración de Categorías de riesgos la opción **Software de control de puerta trasera (BDC)** con una marca, recibirá la correspondiente advertencia en caso de que su programa AntiVir realice una detección.

Adware/Spyware (ADSPY)

Software que muestra anuncios publicitarios, mensajes o envía datos del usuario a terceras personas a menudo sin el consentimiento ni el conocimiento de éste.

Su programa AntiVir reconoce el "adware/spyware". Activando en la configuración de Categorías de riesgos la opción **Adware/Spyware (ADSPY)** con una marca, recibirá la correspondiente advertencia en caso de que su programa AntiVir realice una detección.

Utilidades de compresión poco habituales (PCK)

Ficheros que se han comprimido con un formato de compresión atípico y que, por lo tanto, son posiblemente sospechosos.

Su programa AntiVir reconoce "utilidades de compresión poco habituales". Si se configura **Utilidades de compresión poco habituales (PCK)** en Categorías de riesgos, recibirá una advertencia si su programa AntiVir realiza una detección.

Ficheros de doble extensión (HEUR-DBLEXT)

Estos ficheros enmascaran su extensión de una forma sospechosa. A menudo se considera como malware.

Su programa AntiVir detecta "ficheros de doble extensión". Si en la configuración de Categorías de riesgos avanzadas se activa la opción **Ficheros de doble extensión (HEUR-DBLEXT)** con una marca, recibirá la alerta correspondiente si su programa AntiVir realiza una detección.

Suplantación de identidad (phishing)

El Phishing, también conocido como *Suplantación de marca* pretende sustraer datos de clientes que acceden a servicios bancarios, oficiales, proveedores de servicios, etc. en Internet.

La divulgación de la dirección de email en Internet, rellenar formularios en línea, darse de alta en grupos de noticias o páginas Web puede provocar que los denominados "Internet crawling spiders" puedan robar sus datos y utilizarlos sin su consentimiento en estafas u otros delitos.

Su programa AntiVir detecta la "suplantación de identidad (phishing)". Si se activa la opción **Phishing** en Categorías de riesgos, se recibirán alertas cuando su programa AntiVir detecte un comportamiento de este tipo.

Aplicación (APPL)

EL término APPL se refiere a una aplicación que implica riesgo al ser utilizada o tiene un origen dudoso.

Su programa AntiVir reconoce una "aplicación (APPL)". Si se activa la opción **Aplicación (APPL)** en Categorías de riesgos, se recibirá la alerta correspondiente cuando su programa AntiVir detecte un comportamiento de este tipo.

10.2 Virus y otro tipo de Malware

Adware

Adware es software que muestra banners (mensajes o anuncios) en ventanas emergentes que aparecen en la pantalla. Estos anuncios normalmente no pueden quitarse y por lo tanto siempre están visibles. Estos programas pueden ofrecer muchos datos del usuario y son problemáticos en términos de seguridad.

Backdoors (software de control de puerta trasera)

Los backdoors (castellano: puerta trasera) intentan coger el control del equipo, saltándose los mecanismos habituales de seguridad.

Un programa que se ejecute de manera oculta (una tarea invisible concurrente) en general concede al atacante derechos casi ilimitados. Con los backdoor se puede espiar, pero se utilizan normalmente para instalar otro tipo de virus o gusanos, creando un peligro adicional. Estos programas pueden ofrecer muchos datos del usuario y son problemáticos en términos de seguridad.

Virus del sector de arranque

El sector de arranque maestro de los discos duros se infecta mayormente con estos tipos de virus. Los cuales sobrescriben información importante necesaria para la ejecución del sistema. Una de las posibles consecuencias: que el equipo no se pueda reiniciar más...

Bot-Net (red de robots)

Una Bot-Net se define como una red remota de PC, la cual se compone de bots (robots de software) en comunicación entre sí. La red de robots se compone de una serie de equipo atacados que ejecutan programas (normalmente troyanos o gusanos) bajo una infraestructura de control común. Estas redes pueden usarse para propagar spam, realizar ataques DDoS (denegación de servicio distribuido), etc., en parte sin que el usuario del PC afectado lo descubra. El peligro principal de las redes de robots es que pueden componerse de miles de equipo y la suma de su tráfico generado puede agotar el ancho de banda de los accesos convencionales a Internet.

Exploit (vulnerabilidades)

Un exploit (agujero de seguridad) es un programa que aprovecha algún fallo o vulnerabilidad que permita controlar el sistema o crear una denegación de servicio en un equipo. Una caso de exploit, por ejemplo, son ataques desde Internet con las ayuda de paquetes de datos manipulados. Los programas pueden infiltrarse para obtener un acceso con mayores permisos.

Hoaxes (del inglés: hoax - bulo, engaño, broma de mal gusto)

Los usuarios reciben alertas de virus en Internet y en otras redes que se supone se han extendido vía email. Estas alertas se extienden por email de forma exponencial, ya que a los usuarios se les urge a que expandan la alerta para evitar el "peligro" sin ningún tipo de comprobación real.

Honeypot (foco de atracción, equipo trampa)

Un honeypot es un servicio (en forma de programa o para servidores) que se instala en una red. Tiene la función de monitorizar una red y desarrollar los protocolos de ataques. Este servicio está oculto al usuario legítimo, ya que nunca se hace notar. Si un atacante examina una red en busca de puntos débiles y usa los servicios ofrecidos por el honeypot, se protocoliza y se crea una alerta.

Macrovirus

Los macrovirus son programas que se escriben en lenguajes de macros de la aplicación (por ejemplo Word) y que normalmente sólo pueden propagarse dentro de los documentos de esa aplicación. Por ello, también se conocen como virus de documento. Para ser activos, necesitan de las aplicaciones correspondientes y que sean ejecutados en las mismas. A diferencia de los virus "normales", los macrovirus no atacan a archivos ejecutables sino a documentos de la aplicación anfitriona correspondiente.

Pharming (redirección de nombres de dominio)

El pharming es la manipulación del fichero host o los navegadores para que se hagan peticiones a sitios Web con pretensiones maliciosas. Es un desarrollo del clásico phishing. Los practicantes de pharming manipulan su conjunto de equipo infectados para almacenar datos con pretensiones maliciosas. El pharming se ha establecido como un término que abarca varios tipos de ataques DNS. En el caso de la manipulación del fichero host, un virus o troyano manipula de forma específica el sistema. El resultado es que el sistema sólo puede acceder a sitios Web predeterminados, incluso si se introducen direcciones correctas en el navegador.

Suplantación de identidad (phishing)

Se conoce como phishing la búsqueda no autorizada de datos personales del usuario en Internet. Los atacantes que utilizan phishing normalmente envían a sus víctimas emails aparentemente oficiales en los que inducen a desvelar datos personales tales como números de tarjeta o claves para acceder a servicios bancarios o comerciales. Con los datos sustraídos, los atacantes podrían asumir la identidad de sus víctimas y realizar transacciones en su nombre. Una cosa está clara: los bancos y las compañías de seguros nunca solicitan el envío de número de tarjetas de crédito, PIN, TAN u otros datos de acceso por email, SMS teléfono.

Virus polimórficos

Los virus polimórficos son auténticos maestros del disfraz. Cambian su propio código, por lo que son muy difíciles de detectar.

Virus de programas

Un virus de equipo es un programa que es capaz de anexarse a otro programa tras ejecutarse, creando así una infección. Los virus se multiplican a si mismos, a diferencia de las bombas lógicas y los troyanos. En contraste con un gusano (worm), un virus siempre requiere de un programa portador, en el cual el virus deposita su código. La ejecución normal del programa anfitrión original, en apariencia no cambia.

Rootkit

Un rootkit es una colección de herramientas de software que, tras penetrar en un sistema informático, se instalan para ocultar los inicios de sesión del intruso, ocultar procesos y espiar la información, es decir, actuar de forma invisible. Intentan actualizar programas espía ya instalados y volver a instalar el spyware eliminado.

Virus de script y gusanos

Tales virus son fáciles de programar y se pueden extender -con la tecnología adecuada- en sólo unas horas, vía email, por todo el globo.

Los virus de script y gusanos utilizan un lenguaje de script, como Javascript, VBScript etc., para infiltrarse en otros scripts nuevos o propagarse mediante la ejecución de funciones del sistema operativo. Este ocurre frecuentemente por email o mediante el intercambio de ficheros (documentos).

Un gusano es un programa que se multiplica por si mismo, sin infectar a otros. Los gusanos consecuentemente no forman parte de otros programas. Los gusanos son, a menudo, la única posibilidad de infiltrarse en sistemas con medidas de seguridad restrictivas.

Spyware

Se conoce por spyware a programas espías que interceptan o toman control parcial de un equipo, sin que el usuario se dé cuenta de ello. El spyware está diseñado para explotar los equipos en busca de un algún beneficio, normalmente fraudulento.

Troyanos

Los troyanos son muy comunes actualmente. Son programas que pretenden tener alguna función en particular pero que, al ejecutarse, desarrollan otra función, en el mayor de los casos, destructiva. Los troyanos no se multiplican ellos mismos, lo que los diferencia de los virus y gusanos. La mayoría de ellos tienen un nombre llamativo (SEX.EXE o leeme.EXE), con la intención de que el usuario lo ejecute. En cuanto se ejecutan pueden ejecutar cualquier acción, por ejemplo: formatear el disco duro. Un dropper es una forma especial de troyano que crea virus en el equipo atacado.

Zombie

Un PC zombie es un ordenador infectado con malware que permite a los hackers o piratas el abusar de otros ordenadores vía control remoto con propósitos criminales. El equipo infectado, inicia, por ejemplo, ataques por denegación de servicio o envía correo no solicitado (spam) o emails de suplantación de identidad (phishing).

11 Información y servicio

En este capítulo se ofrece información acerca de cómo ponerse en contacto con nosotros.
consulte el capítulo Dirección de contacto
consulte el capítulo Soporte técnico
consulte el capítulo Fichero sospechoso
consulte el capítulo Notificar una falsa alarma
consulte el capítulo Sus comentarios para mayor seguridad

11.1 Dirección de contacto

Si tiene cualquier pregunta o sugerencia acerca de cualquier producto AntiVir, estaremos encantados de ayudarle. Encontrará nuestras direcciones de contacto en el Centro de control en Ayuda :: Acerca de Avira AntiVir Professional.

11.2 Soporte Técnico

El soporte Avira está a su disposición para responder a sus preguntas o solucionar problemas técnicos con toda fiabilidad.

Toda la información necesaria sobre nuestro amplio servicio de soporte se puede obtener en nuestro sitio Web:

<http://www.avira.es/support>

Para que podamos ofrecerte ayuda de forma rápida y eficiente, deberías tener preparada la siguiente información:

- **Información de la licencia.** La encontrará en la interfaz del programa en la opción de menú Ayuda:: Acerca de Avira AntiVir Professional :: Información de licencia.
- **Información de versión.** La encontrará en la interfaz del programa en la opción de menú Ayuda:: Acerca de Avira AntiVir Professional :: Información de versión.
- **Versión de Sistema operativo** y los Service-Packs instalados.
- **Software instalado**, ej. antivirus de otras casas.
- **Mensaje exacto** del programa o del fichero de informe.

11.3 Archivos sospechosos

Los virus que no hayan sido detectados o eliminados por nuestros productos o archivos sospechosos se nos pueden enviar. Le ofrecemos varias vías para hacerlo.

- Seleccione el fichero en el Gestor de cuarentena del Centro de control y seleccione a través del menú contextual o el botón correspondiente el punto Enviar fichero.

- Envíe el fichero deseado comprimido (WinZIP, PKZip, Arj, etc.) adjunto en un email a la siguiente dirección:
virus@avira.es
Como algunos servidores de correo trabajan con programas antivirus, también deberá poner una contraseña al archivo o archivos que desee enviar (por favor recuerde decirnos la contraseña).

También puede enviarnos el archivo sospechoso por medio de nuestro sitio Web:
<http://www.avira.es/file-upload>

11.4 Informe falso positivo

Si cree que su programa AntiVir notifica la detección de un fichero que muy probablemente esté "limpio", envíe ese fichero comprimido (WinZIP, PKZIP, Arj, etc.) adjunto en un email a la siguiente dirección:

- virus@avira.es

Como algunos servidores de correo trabajan con programas antivirus, también deberá poner una contraseña al archivo o archivos que desee enviar (por favor recuerde decirnos la contraseña).

11.5 Sus observaciones para más seguridad

En Avira, la seguridad de nuestros clientes es el principal objetivo. Por esa razón, no solo disponemos de un equipo interno de expertos que comprueban la calidad y la seguridad de cada solución de Avira GmbH y cada actualización antes de distribuir el producto. También damos gran importancia a las indicaciones respecto a grietas relevantes en la seguridad que se hayan podido crear y que trataremos inmediatamente.

Si usted cree que ha detectado una fisura en la seguridad de alguno de nuestros productos, por favor envíenos un email a la siguiente dirección:

vulnerabilities@avira.es

12 Referencia: opciones de configuración

La referencia de la configuración documenta todas las opciones de configuración disponibles.

12.1 Escáner

La sección Escáner de la configuración se encarga de la configuración del análisis directo, es decir del análisis a petición.

12.1.1 Análisis

Aquí se define el comportamiento básico de la rutina de búsqueda en caso de análisis directo. Si selecciona determinadas carpetas en un análisis directo, dependiendo de la configuración, el escáner analiza:

- con una cierta profundidad y prioridad,
- también ciertos sectores y la memoria principal,
- ciertos o todos los sectores y la memoria principal,
- todos o ciertos ficheros seleccionados.

Ficheros

El escáner puede usar un filtro para analizar sólo ficheros con una determinada extensión (tipo).

Todos los ficheros

Con esta opción seleccionada se analizan todos los ficheros sin tener en cuenta su extensión ni contenido en busca de virus o programas no deseados. No se utilizará ningún filtro.

Nota

Si se activa Todos los ficheros, el botón **Extensiones de ficheros** no se puede seleccionar.

Extensiones inteligentes

Con esta opción activada, el programa selecciona de forma completamente automática los ficheros a analizar. Es decir, su programa AntiVir decide, dependiendo del contenido de un fichero, si éste se analizará o no en cuanto a virus y programas no deseados. Este procedimiento es algo más lento que usar la lista de extensiones de ficheros, pero más seguro, ya que no se analiza únicamente en base a la extensión del fichero. Esta configuración está activada de forma estándar y es la recomendada.

Nota

Si se activa las extensiones inteligentes el botón **Extensiones de fichero** no puede seleccionarse.

Usar lista de extensiones de fichero

Con esta opción activada, sólo se analizan ficheros de la extensión especificada. Todos los tipos de ficheros que pueden contener virus o programas no deseados ya están preseleccionados. Esta lista puede editarse manualmente con el botón "**Extensión de fichero**".

Nota

Si está activa esta opción y ha eliminado todas las entradas de la lista con extensiones de fichero, esto se indica con el texto "Sin extensiones" debajo del botón **Extensiones de ficheros**.

Extensiones de fichero

Con la ayuda de este botón se abre una ventana de diálogo en la que aparecen todas las extensiones a analizar en el modo "**Usar lista de extensiones de fichero**". Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

Nota

La lista estándar puede variar entre versiones.

Configuración adicional

Analizar los sectores boot (de arranque) de los discos seleccionados

Con esta opción seleccionada el escáner sólo analiza los sectores de arranque de las unidades seleccionadas para el análisis directo. Este ajuste está activado de forma estándar.

Analizar sect. arranque maestros

Con esta opción activada, el escáner sólo analiza los sectores de arranque maestros de los discos duros usados en el sistema.

Omitir ficheros offline

Si se activa esta opción, el análisis directo omite por completo los llamados ficheros offline durante el análisis. Es decir, que no se analiza los mismos en busca de malware. Los ficheros offline son los que se han trasladado físicamente del disco duro a otro medio, p. ej., una cinta, en un sistema jerárquico de administración de almacenamientos (HSMS - Hierarchical Storage Management System). Este ajuste está activado de forma estándar.

Compr. integridad ficheros del sistema

Si está activada la opción, en cada análisis directo se analizan de manera especialmente segura los ficheros del sistema Windows más importantes para detectar modificaciones debidas a malware. Si se detecta un fichero modificado, se notifica como detección sospechosa. Esta función requiere mucha capacidad de rendimiento del equipo. Por ello, esta opción está desactivada de forma estándar.

Importante

Esta opción sólo está disponible a partir de Windows Vista. Si administra el programa AntiVir bajo SMC, la opción no está disponible.

Nota

Si utiliza herramientas de otros proveedores que modifican archivos de sistema y adaptan la pantalla arranque o inicio a sus propias necesidades, no debería utilizar esta opción. Ejemplos para este tipo de herramientas son los llamados Skinpacks, TuneUp Utilities o Vista Customization.

Análisis optimizado

Si la opción está activada, durante el análisis del escáner se optimiza la capacidad del procesador. Por motivos de rendimiento, el registro en informes durante el análisis optimizado únicamente se lleva a cabo en un nivel estándar.

Nota

Esta opción sólo está disponible en equipos con multiprocesador. Si administra su programa AntiVir a través de SMC, la opción se muestra en todos los casos y se puede activar: Si el equipo administrado no dispone de varios procesadores, el escáner no usa la opción.

Seguir enlaces simbólicos

Si la opción está activada, el escáner sigue durante el análisis todos los accesos directos simbólicos del perfil de análisis o del directorio seleccionado con el fin de analizar los ficheros vinculados acerca de la existencia de virus y malware. Esta opción no es compatible con Windows 2000 y está desactivada de forma estándar.

Importante

La opción no incluye accesos directos a ficheros (accesos directos), sino que se refiere exclusivamente a vínculos simbólicos (creados con mklink.exe) o puntos de unión (creados con junction.exe) que existen en el sistema de ficheros de forma transparente.

Análisis de rootkits al iniciar

Con esta opción activada, al inicio del análisis el escáner comprueba si hay rootkits activos en el directorio de sistema de Windows con el llamado procedimiento rápido. Este procedimiento no analiza la existencia de rootkits activos en el equipo tan exhaustivamente como lo hace el perfil de análisis "**Búsqueda de rootkits**", pero su ejecución es considerablemente más rápida.

Importante

¡La búsqueda de rootkits no está disponible en Windows XP 64 Bit !

Analizar el registro

Con esta opción activada, se analiza el registro en búsqueda de indicios de software dañino.

No analizar ficheros y rutas en unidades de red

Con esta opción activada se excluyen del análisis directo las unidades de red conectadas al equipo. Esta opción es recomendable si los servidores u otras estaciones de trabajo ya disponen de software de protección antivirus. Esta opción está desactivada de forma estándar.

Proceso de análisis

Permitir detener

Si esta opción está activada, es posible finalizar en cualquier momento el análisis de virus o programas no deseados pulsando el botón "**Detener**" en la ventana del "Luke Filewalker". Si ha desactivado este ajuste, el botón **Detener** de la ventana del "Luke Filewalker" aparece en gris. ¡Debido a ello no se puede detener el análisis de forma prematura! Este ajuste está activado de forma estándar.

Prioridad del escáner

Con el análisis directo, el escáner distingue entre varios niveles de prioridad. Esto es efectivo únicamente si se ejecutan varios procesos simultáneamente en el equipo. La selección afecta a la velocidad de análisis.

Bajo

El sistema operativo únicamente asigna tiempo de procesador al escáner si ningún otro proceso necesita tiempo de procesador, es decir, mientras sólo se esté ejecutando el escáner, la velocidad es la máxima. Por lo general, así se facilita en gran medida el trabajo con otros programas: el equipo reacciona más rápidamente cuando otros programas precisan tiempo de cálculo y en esos casos el escáner continúa ejecutándose en segundo plano. Esta configuración está activada de forma estándar y es la recomendada.

Medio

Al escáner se le asigna una prioridad normal. El sistema operativo asigna a todos los procesos la misma cantidad de tiempo de procesador. En ciertas circunstancias, puede afectarse el rendimiento de otras aplicaciones.

Alto

Al escáner se le asigna una prioridad máxima. El trabajo simultáneo con otras aplicaciones es casi imposible. No obstante, el escáner analiza con la mayor velocidad posible.

12.1.1.1. Acción en caso de detección

Acción en caso de detección

Puede definir las acciones que debe tomar el escáner cuando se detecta un virus o programa no deseado.

Interactiva

Si se activa esta opción, las detecciones del análisis del escáner se notifican en un cuadro de diálogo. Durante la búsqueda del escáner se recibe al finalizar el análisis un mensaje de advertencia con una lista de los ficheros afectados detectados. Tiene la posibilidad de seleccionar mediante el menú contextual la acción que se ejecutará para cada uno de los ficheros afectados. Puede ejecutar las acciones seleccionadas para todos los ficheros afectados o finalizar el escáner.

Nota

En el diálogo del escáner aparece la acción 'Mover a cuarentena' como acción predeterminada.

Acciones permitidas

En esta área de la pantalla, puede seleccionar las acciones que se pueden seleccionar en el cuadro de diálogo si se detecta un virus en el modo de notificación personalizado o experto. Para ello, debe activar las opciones correspondientes.

reparar

El escáner repara el fichero infectado si esto es posible.

cambiar el nombre

El escáner renombra el fichero. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. El fichero puede repararse posteriormente y renombrarse otra vez con su nombre original.

Cuarentena

El escáner mueve el fichero a la cuarentena. Desde el Gestor de cuarentena puede volver a restaurar el fichero si éste tiene valor informativo o, si fuera necesario, puede enviarlo al Avira Malware Research Center. Dependiendo del objeto, hay más posibilidades de selección en el Gestor de Cuarentena.

eliminar

El fichero se elimina. Este proceso es considerablemente más rápido que "sobrescribir y eliminar".

omitir

El fichero se ignorará

sobrescribir y eliminar

El escáner sobrescribe el fichero con un patrón predeterminado y después lo elimina. No puede restaurarse.

Predeterminado

Con este botón se define una acción predeterminada del escáner para el tratamiento de los ficheros afectados. Seleccione una acción y haga clic en el botón "**Predeterminado**". En el modo de notificación combinado sólo se puede ejecutar la acción predeterminada que se ha seleccionado para los ficheros afectados. En el modo de notificación personalizado y experto aparece seleccionada la acción predeterminada que se ha seleccionado para los ficheros afectados.

Nota

No se puede seleccionar la acción **reparar** como acción predeterminada.

Nota

Si ha seleccionado como acción predeterminada *eliminar* o *sobrescribir y eliminar* y desea establecer el modo de notificación combinado, tenga en cuenta lo siguiente: en caso de detección mediante heurística, los ficheros afectados no se eliminan, sino que se mueven a cuarentena.

Encontrará más información aquí.

Automático

Si esta opción está activada, entonces no mostrará la ventana de acciones después de una detección de un virus o programa no deseado. El escáner reacciona de acuerdo a lo que configure en esta sección.

Copiar fichero a cuarentena antes de la acción

Si se activa esta opción, el escáner crea una copia de seguridad (backup) antes de llevar a cabo la acción principal o secundaria pertinente. La copia se guarda en cuarentena desde donde luego puede restaurarse si tienes algún valor informativo. Además puede enviar la copia al Avira Malware Research Center para que sea analizada a fondo.

Mostrar mensajes de advertencia

Con esta opción activada, al detectar un virus o un programa no deseado aparece un mensaje de advertencia indicando las acciones que se ejecutarán.

Acción Primaria

La acción primaria es la que se ejecuta cuando el escáner detecta un virus o programa no deseado. Si seleccionó la opción "**reparar**" pero no es posible reparar el fichero afectado, se ejecuta la acción seleccionada en "**Acción secundaria**".

Nota

La opción **Acción Secundaria** sólo puede seleccionarse si se ha configurado la **Opción primaria** como **Reparar**.

reparar

Con esta opción seleccionada el escáner repara los ficheros automáticamente. Si el escáner no puede reparar el fichero afectado, ejecuta alternativamente la opción seleccionada en Acción secundaria.

Nota

Se recomienda la reparación automática, pero eso significa que el escáner puede modificar los ficheros del equipo.

eliminar

Con esta opción activada, el fichero se borra. Este proceso es considerablemente más rápido que "sobrescribir y eliminar".

sobrescribir y eliminar

Con esta opción activada, el escáner sobrescribe el fichero con un patrón estándar y lo elimina. No puede restaurarse.

cambiar el nombre

Con esta opción activada, el escáner renombra el fichero. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. Los ficheros pueden repararse posteriormente y renombrarse otra vez con su nombre original

omitir

Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

Advertencia

¡El fichero afectado sigue activo en el equipo! ¡Podría causar daños graves a su sistema!

Cuarentena

Con esta opción activada el escáner mueve el fichero a cuarentena. Estos ficheros pueden ser reparados posteriormente o -si fuera necesario- enviarse al Avira Malware Research Center.

Acción secundaria

La opción "**Acción Secundaria**" sólo puede seleccionarse si se ha seleccionado como "**Acción Principal**" el ajuste **Reparar**. Con esta opción se decide qué debe hacerse si el fichero afectado no puede repararse.

eliminar

Con esta opción activada, el fichero se borra. Este proceso es considerablemente más rápido que "sobrescribir y eliminar".

sobrescribir y eliminar

Con esta opción seleccionada el escáner sobrescribe el fichero con un patrón estándar y luego lo elimina. No puede restaurarse.

cambiar el nombre

Con esta opción activada, el escáner renombra el fichero. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. Los ficheros pueden repararse posteriormente y renombrarse otra vez con su nombre original

omitir

Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

Advertencia

¡El fichero afectado sigue activo en el equipo! ¡Podría causar daños graves a su sistema!

Cuarentena

Con esta opción activada el escáner mueve el fichero a cuarentena. Estos ficheros pueden ser reparados posteriormente o -si fuera necesario- enviarse al Avira Malware Research Center.

Nota

Si ha seleccionado como acción principal o secundaria **Eliminar** o **Sobrescribir y eliminar**, tenga en cuenta lo siguiente: en caso de detección mediante heurística, los ficheros afectados no se eliminan, sino que se mueven a cuarentena.

12.1.1.2. Acciones adicionales

Iniciar programa tras detección

Tras el análisis directo, el escáner puede abrir el fichero que usted seleccione (por ejemplo, un programa) si ha detectado al menos un virus o programa no deseado, p. ej., un programa de correo, para que pueda advertir a otros usuarios o al administrador.

Nota

Por razones de seguridad sólo es posible iniciar un programa tras la detección si usuario se ha identificado en el equipo. El fichero se abre con los derechos del usuario que se ha identificado. Si el usuario no está autenticado, esta opción no será realizada.

Nombre del programa

El botón abre una ventana en la que puede introducir el nombre y ruta del programa que el escáner debe iniciar tras una detección.



El botón abre una ventana en la que puede navegar hasta el fichero con la ayuda del explorador de ficheros.

Argumentos

Aquí puede introducir los parámetros en la línea de comandos para el programa a arrancar.

Registro de eventos

Usar registro de eventos

Si está activada la opción, tras el análisis del escáner se transmite un mensaje de evento con los resultados del análisis al registro de eventos de Windows. Los eventos pueden abrirse en el visor de eventos de Windows. La opción está desactivada de forma estándar.

Cuando el escáner analiza archivos comprimidos utiliza un análisis recursivo: también se descomprimen los archivos comprimidos que estén incluidos en otros archivos comprimidos y se analizan en busca de virus y programas no deseados. Los ficheros se analizan, descomprimen y vuelven a analizarse.

Analizar archivos comprimidos

Con esta opción activada, se analizan los archivos comprimidos seleccionados en la lista. Este ajuste está activado de forma estándar.

Todos los tipos de archivo comprimido

Con esta opción se seleccionan y analizan todos los archivos comprimidos en la lista.

Extensiones inteligentes

Con esta opción activa, el escáner detecta si un fichero tiene un formato de archivo comprimido, incluso si su extensión no lo refleja, y analiza el archivo. De todas formas, esto significa que se deben de abrir todos los ficheros, lo que reduce la velocidad de análisis. Ejemplo: si un archivo *.zip tiene la extensión de fichero *.xyz, el escáner descomprime también este archivo y lo analiza. Este ajuste está activado de forma estándar.

Nota

Sólo se soportan aquéllos tipos de archivos comprimidos marcados en la lista de archivos comprimidos.

Limitar la profundidad en la recursividad

El descomprimir y analizar ficheros profundamente entrelazados puede requerir gran cantidad de tiempo y recursos. Si esta opción está activada, se limita la profundidad del análisis en archivos comprimidos múltiples veces (máximo nivel de recursividad). Esto ahorra tiempo y recursos del equipo.

Nota

Para encontrar un virus o programa no deseado dentro de un archivo comprimido, el escáner debe analizar hasta el nivel de recursividad donde se encuentre el virus o programa no deseado.

Nivel máximo de recursividad

Para introducir el máximo nivel de recursividad, se debe activar la opción Límite de profundidad de recursividad.

Puede introducir directamente el nivel de recursividad pertinente o cambiarlo con las teclas de flecha que hay a la derecha del campo de introducción. Los valores permitidos van del 1 al 99. El valor predeterminado es 20 y es el recomendado.

Valores predeterminados

Este botón restableces los valores predefinidos cuando se analizan comprimidos.

Lista de archivos comprimidos

En este apartado puede establecer qué archivos comprimidos debe analizar el escáner. Para ello debe seleccionar las entradas relevantes.

12.1.1.3. Excepciones

Ficheros a excluir por el escáner

La lista en esta ventana contiene los ficheros y rutas que no deben ser incluidas en el análisis en busca de virus o programas no deseados por el escáner.

Introduzca las mínimas excepciones posibles que considere que no deberían incluirse en un análisis de rutina. ¡Le recomendamos analizar antes los ficheros y programas no deseados incluidos en esta lista!

Nota

La suma de las entradas de la lista no puede superar el máximo de 6 000 caracteres.

Advertencia

¡Estos ficheros no se toman en cuenta en el análisis!

Nota

Los ficheros incluidos en esta lista se anotan en el fichero de informe. Compruebe la presencia de estos ficheros no comprobados de vez en cuando en el fichero de informe, ya que quizás la razón por la que ha retirado un fichero de la comprobación ya no existe. En este caso, debería retirarse el nombre de estos ficheros de la lista.

Campo de entrada

En esta ventana, puede introducir el nombre del objeto fichero que no desee incluir en el análisis directo. No hay ningún fichero objeto fichero introducido de forma estándar.



El botón abre una ventana en la que puede seleccionar el fichero o la ruta pertinente. Cuando introduce un fichero con su ruta completa, sólo este fichero se excluye del análisis. Si se introduce un nombre de fichero sin una ruta, todos los ficheros con ese nombre (independientemente de donde se encuentren) se excluyen del análisis.

Añadir

Este botón permite incluir en la ventana de visualización el objeto fichero introducido en el campo de entrada.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

Nota

Si añade toda una partición a la lista de los objetos fichero que deben excluirse, sólo se excluyen del análisis los ficheros guardados directamente debajo de la partición y no los ficheros que estén en directorios en esa partición.

Ejemplo: objeto fichero que se debe excluir: `D:\ = D:\file.txt` se excluye del análisis del escáner, `D:\folder\file.txt` no se excluye del análisis.

Nota

Si administra el programa AntiVir en SMC, puede utilizar variables en las indicaciones de ruta en caso de excepciones de ficheros. Puede encontrar una lista de las variables que se pueden utilizar en Variables: Excepciones de Guard y escáner.

12.1.1.4. Heurística

Esta sección de configuración contiene los parámetros para la heurística del motor de análisis.

Los productos AntiVir disponen de unas heurísticas muy eficaces que permiten detectar malware desconocido de forma proactiva, es decir, antes de que se haya creado una firma de virus específica para ese software malintencionado y se haya enviado la correspondiente actualización del antivirus. La detección de virus se lleva a cabo mediante un minucioso análisis del código en cuestión para encontrar funciones típicas del malware. Si el código analizado se comporta de forma similar, se reporta como sospechoso. Sin embargo, ese código no es necesariamente malware; también pueden producirse falsas alarmas. El usuario debe decidir que hacer con el código encontrado, por ejemplo, basándose en su conocimiento o experiencia previa, puede decidir si la fuente que contiene el código es de confianza.

Heurística de macrovirus

Heurística de macrovirus

Su producto AntiVir incluye una potente herramienta de heurística para macrovirus. Con esta opción activada, se eliminan todas las macros en el caso de una reparación del documento afectado. Otra opción es que sólo se notifique la existencia de documentos sospechosos, es decir, se reciba una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Su programa AntiVir dispone de la tecnología AntiVir AHeAD, de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Si esta opción está activada, puede definir el nivel de "tolerancia" de la heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si está activada la opción, se detecta algo menos de malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es en este caso reducido.

Nivel de detección medio

Esta configuración está activa por defecto si ha seleccionado el uso de esta heurística.

Nivel de detección alto

Si está activada la opción, se detecta bastante más malware desconocido pero hay que contar con falsas alarmas.

12.1.2 Informe

El escáner tiene una completa funcionalidad sacando informes. Así puede obtener información muy precisa del resultado del análisis directo. El fichero de informe contiene todas las entradas del sistema, así como advertencias y mensajes del análisis directo.

Nota

Para que pueda establecer qué acciones ha tomado el escáner al detectar un virus o programa no deseado, debería crearse siempre un fichero de informe.

Protocolización

Desactivado

Si esta opción está activada, el escáner no informa de las acciones o resultados de un análisis directo.

Predeterminado

Si se selecciona esta opción, el escáner informa del nombre y ruta de los ficheros afectados. Además, en el fichero de informe aparece la configuración del análisis, información de la versión y del licenciataro.

Ampliado

Con esta opción activada, el escáner informa de alertas e instrucciones, además de los nombres y rutas de los ficheros afectados.

Completo

Si se selecciona esta opción, el escáner informa de todos los ficheros analizados. Además se incluyen en el informe todos los ficheros, así como alertas y mensajes .

Nota

Si tiene que enviarnos algún fichero de informe para resolver algún problema, hágalo de este modo.

12.2 Guard

La sección Guard es responsable de la configuración del análisis en tiempo real.

12.2.1 Análisis

Normalmente deseará monitorizar su sistema de forma constante. Para ello utiliza el Guard (análisis en tiempo real = escáner en acceso). Así puede, entre otras cosas, analizar todos los ficheros que se copian o abren en el equipo sobre la marcha para detectar la existencia de virus y programas no deseados.

Modo de análisis

Aquí se define el momento en que debe analizarse un fichero.

Analizar al leer

Si esta opción está activada, el Guard analiza los ficheros antes de que sean leídos o ejecutados por la aplicación o el sistema operativo.

Analizar al escribir

Si esta opción está activada, el Guard analiza el fichero al ser escrito. Sólo puede acceder al fichero de nuevo cuando se haya completado el proceso.

Analizar al leer y escribir

Si esta opción está activada, el Guard analiza los ficheros antes de ser abiertos, leídos, ejecutados y después de ser escritos. Este ajuste está activado de forma estándar y es el recomendado.

Ficheros

El Guard puede usar un filtro para analizar sólo ficheros de una cierta extensión (tipo).

Todos los ficheros

Si esta opción está activada, se analizan si hay virus o programas no deseados en todos los ficheros, independientemente de su contenido y su extensión.

Nota

Si se activa Todos los ficheros, el botón **Extensiones de ficheros** no se puede seleccionar.

Extensiones inteligentes

Con esta opción activada, el programa selecciona de forma completamente automática los ficheros a analizar. Esto significa que el programa decide, dependiendo del contenido, si se debe comprobar la existencia de virus y programas no deseados en los ficheros. Este procedimiento es algo más lento que usar la lista de extensiones de ficheros, pero más seguro, ya que no se analiza únicamente en base a la extensión del fichero.

Nota

Si se activa las extensiones inteligentes el botón **Extensiones de fichero** no puede seleccionarse.

Usar lista de extensiones de fichero

Con esta opción activada, sólo se analizan ficheros de la extensión especificada. Todos los tipos de ficheros que pueden contener virus o programas no deseados ya están preseleccionados. Esta lista puede editarse manualmente con el botón "**Extensiones de ficheros**". Esta configuración está activada de forma estándar y es la recomendada.

Nota

Si está activa esta opción y ha eliminado todas las entradas de la lista, esto se indica con el texto "Sin extensiones" debajo del botón **Extensiones de ficheros**.

Extensiones de fichero

Con la ayuda de este botón se abre una ventana de diálogo en la que aparecen todas las extensiones a analizar en el modo "**Usar extensiones de la lista de ficheros**". Las extensiones incluyen entradas predeterminadas, pero puede añadir o eliminar entradas.

Nota

La lista de extensiones de ficheros puede variar entre versiones.

Archivos

Analizar archivos

Si está activa esta opción, se analizarán los archivos comprimidos. Los archivos comprimidos se analizan, se descomprimen y se analizan de nuevo. Esta opción no está activa de forma estándar. Se limita el análisis de archivos mediante el nivel de recursividad, la cantidad de ficheros que se analizan y el tamaño del archivo comprimido. Puede establecer el nivel de recursividad, la cantidad de ficheros que se analizarán y el tamaño máximo del archivo comprimido.

Nota

Esta opción no está activa de forma estándar, ya que sobrecarga mucho al procesador. En general se recomienda que los archivos comprimidos se comprueben con el análisis directo.

Nivel máximo de recursividad

Al realizar análisis de archivos el Guard usa un análisis recursivo: también se descomprimen los archivos comprimidos que estén incluidos en otros archivos comprimidos y se analizan en busca de virus y programas no deseados. Puede definir el nivel de recursividad. El valor predeterminado para el nivel de recursividad es 1 y es el recomendado: se analizan todos los archivos que se encuentren directamente en el archivo principal.

Máximo número de ficheros

Al analizar archivos comprimidos el análisis se limita a una cantidad máxima de ficheros. El valor predeterminado para la cantidad máxima de ficheros que se analizarán es 10 y es el valor recomendado.

Tamaño máximo (KB)

Al analizar archivos el análisis se limita a un tamaño máximo del archivo que se descomprimirá. Se recomienda el valor estándar de 1 000 KB.

Unidades

Unidades de red

Al activar esta opción, se analizan las unidades de red (discos asignados).

Nota

Para no afectar al rendimiento del equipo excesivamente, únicamente debería activarse la opción **Unidades de red** en casos excepcionales.

Advertencia

Si la opción está desactivada, las unidades de red **no** se supervisan. ¡Ya no está protegido contra virus o programas no deseados!

Nota

Al ejecutar ficheros desde unidades de red, el Guard los analiza, independientemente del parámetro configurado en la opción *Unidades de red*. En algunos casos, los ficheros en unidades de red se analizan al abrir aunque esté desactivada la opción *Unidades de red*. El motivo es que a estos ficheros se accede con el permiso 'Ejecutar fichero'. Si desea excluir estos ficheros o también los ficheros que se ejecuten en unidades de red de la supervisión del Guard, debe incluir estos ficheros en la lista de objetos fichero omitidos (consulte: Guard::Análisis::Excepciones).

Activar almacenamiento en caché

Si está activada la opción, los ficheros supervisados en unidades de red se ponen a disposición del caché del Guard. La supervisión de unidades de red sin función de caché ofrece más seguridad, pero es más lenta que la supervisión de unidades de red con caché.

12.2.1.1. Acción en caso de detección

Acción en caso de detección

Puede definir las acciones a tomar por el Guard, cuando se detecta un virus o programa no deseado.

Interactivo

Con esta opción activada, aparece una notificación de escritorio en caso de una detección del Guard. Tiene la posibilidad de eliminar el malware encontrado o tomar otras posibles acciones para el tratamiento de virus a través del botón 'Detalles'. Las acciones se indican en un cuadro de diálogo. Esta opción está activada de forma estándar.

Acciones permitidas

En este área de la pantalla puede seleccionar las acciones que desea que estén disponibles como acciones adicionales en el cuadro de diálogo para el tratamiento de virus. Para ello, debe activar las opciones correspondientes.

reparar

El Guard repara el fichero infectado si es posible.

cambiar el nombre

El Guard renombra el fichero. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. El fichero puede repararse posteriormente y renombrarse otra vez con su nombre original.

Cuarentena

El Guard mueve el fichero a la Cuarentena. Desde el Gestor de cuarentena puede volver a restaurar el fichero si éste tiene valor informativo o, si fuera necesario, puede enviarlo al Avira Malware Research Center. Dependiendo del fichero, hay más posibilidades de selección en el Gestor de Cuarentena.

eliminar

El fichero se elimina. Este proceso es considerablemente más rápido que "sobrescribir y eliminar".

omitir

Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

sobrescribir y eliminar

El Guard sobrescribe el fichero con un patrón estándar y lo elimina. No puede restaurarse.

Predeterminado

Este botón le permite seleccionar la acción que será activada de forma estándar en el cuadro de diálogo que aparece al detectar un virus. Seleccione la acción que será activada de forma estándar y pulse "**Predeterminado**".

Nota

No se puede seleccionar la acción **reparar** como acción predeterminada.

Encontrará más información aquí.

Automático

Si esta opción está activada, entonces no mostrará la ventana de acciones después de una detección de un virus o programa no deseado. El Guard reacciona de acuerdo a lo que configure en esta sección.

Copiar fichero a cuarentena antes de la acción

Con esta opción activada, el Guard crea una copia de seguridad (backup) antes de llevar a cabo la acción principal o secundaria pertinente. La copia se guarda en la cuarentena. Se puede restablecer desde el Gestor de cuarentena si tiene algún valor informativo.

Además puede enviar la copia de seguridad al Avira Malware Research Center.

Dependiendo del objeto, hay más posibilidades de selección en el Gestor de Cuarentena.

Mostrar mensajes de advertencia

Con esta opción activada, aparece un mensaje de advertencia al detectarse algún virus o programa no deseado.

Acción Primaria

La acción principal es la que se ejecuta cuando el Guard detecta un virus o programa no deseado. Si seleccionó la opción "**reparar**" pero no es posible reparar el fichero afectado, se ejecuta la acción seleccionada en "**Acción secundaria**".

Nota

La opción Acción Secundaria sólo puede seleccionarse si se ha configurado la Opción primaria como Reparar.

reparar

Si se selecciona esta opción, el Guard repara los ficheros afectados automáticamente. Si el Guard no puede reparar el fichero afectado, ejecuta alternativamente la acción seleccionada como Acción Secundaria.

Nota

Se recomienda la reparación automática, pero eso significa que el Guard puede modificar los ficheros en el equipo.

eliminar

Con esta opción activada, el fichero se borra. Este proceso es considerablemente más rápido que "sobrescribir y eliminar".

sobrescribir y eliminar

Con esta opción activada, el Guard sobrescribe el fichero con un patrón estándar y lo elimina. No puede restaurarse.

cambiar el nombre

Con esta opción activada, el Guard renombra el fichero. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. Los ficheros pueden repararse posteriormente y renombrarse otra vez con su nombre original

omitir

Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

Advertencia

¡El fichero afectado sigue activo en el equipo! ¡Podría causar daños graves a su sistema!

Denegar acceso

Si la opción está activada, el Guard sólo incluye la detección en el Fichero de informe en caso de haber activado la función de informe. Además el Guard escribe una entrada en el Registro de eventos si está activada esta opción.

Cuarentena

Si esta opción está activada, el Guard mueve el fichero al directorio de cuarentena. Estos ficheros pueden ser reparados posteriormente o -si fuera necesario- ser enviados al Avira Malware Research Center.

Acción secundaria

Sólo puede seleccionar la opción "**Acción secundaria**" si en "**Acción principal**" ha seleccionado la opción "**Reparar**". Con esta opción se decide qué debe hacerse si el fichero afectado no puede repararse.

eliminar

Con esta opción activada, el fichero se borra. Este proceso es considerablemente más rápido que "sobrescribir y eliminar".

sobrescribir y eliminar

Con esta opción activada, el Guard sobrescribe el fichero con un patrón estándar y lo elimina. No puede restaurarse.

cambiar el nombre

Con esta opción activada, el Guard renombra el fichero. El acceso directo a estos ficheros (haciendo doble clic) ya no es posible. Los ficheros pueden repararse posteriormente y renombrarse otra vez con su nombre original

omitir

Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

Advertencia

¡El fichero afectado sigue activo en el equipo! ¡Podría causar daños graves a su sistema!

Denegar acceso

Si la opción está activada, el Guard sólo incluye la detección en el Fichero de informe en caso de haber activado la función de informe. Además el Guard escribe una entrada en el Registro de eventos si está activada esta opción.

Cuarentena

Con esta opción activada el Guard mueve el fichero a Cuarentena. Los ficheros pueden ser reparados posteriormente o -si fuera necesario- enviarse al Avira Malware Research Center.

Nota

Si ha seleccionado como acción principal o secundaria **Eliminar** o **Sobrescribir y eliminar**, tenga en cuenta lo siguiente: en caso de detección mediante heurística, los ficheros afectados no se eliminan, sino que se mueven a cuarentena.

12.2.1.2. Acciones adicionales

Notificaciones

Registro de eventos

Usa el registro de eventos

Si esta opción está activada, se añade una entrada en el registro de eventos de Windows con cada detección. Los eventos pueden abrirse en el visor de eventos de Windows. Este ajuste está activado de forma estándar.

Inicio automático

Bloquear función de inicio automático

Con esta opción activada, se bloquea la ejecución de la función de inicio automático de Windows en todas las unidades conectadas tales como lápices USB, unidades de CD y DVD, unidades de red. Con la función de inicio automático de Windows se leen inmediatamente los ficheros al insertar portadatos o conectar unidades de red, permitiendo así el inicio y ejecución automática de los ficheros. Sin embargo, esta funcionalidad conlleva un elevado riesgo de seguridad ya que el inicio automático de ficheros permite la instalación de malware y programas no deseados. La función de inicio automático es especialmente crítica para lápices USB, ya que los datos de un lápiz pueden cambiar constantemente.

Excluir CD y DVD

Con esta opción activada, se permite la función de inicio automático en las unidades de CD y DVD.

Advertencia

Desactive la función de inicio automático para unidades de CD y DVD sólo si está seguro de utilizar únicamente portadatos de confianza.

12.2.1.3. Excepciones

Estas opciones permiten configurar los objetos de excepción para el Guard (análisis en tiempo real). Los objetos en cuestión no se considerarán en el análisis en tiempo real. Mediante la lista de procesos omitidos, el Guard puede omitir sus accesos a ficheros durante el análisis en tiempo real. Esto resulta útil en el caso de bases de datos o de soluciones de copia de seguridad.

Tenga en cuenta lo siguiente al indicar los procesos y los objetos de fichero que deben omitirse: La lista se procesa de arriba a abajo. Cuanto más larga es la lista, más tiempo de procesador se requiere para procesar la lista en cada acceso. Por lo tanto se recomienda que las listas sean lo más cortas posible.

Procesos omitidos por Guard

Todos los accesos a ficheros de los procesos que constan en esta lista se excluyen de la supervisión por parte del Guard.

Campo de entrada

En este campo se introduce el nombre del proceso que no debe considerarse durante el análisis en tiempo real. De forma estándar no hay ningún proceso indicado.

Nota

Puede introducir un máximo de 128 procesos.

Nota

Al indicar el proceso se aceptan caracteres Unicode. Por ello, puede indicar nombres de procesos o directorios que contienen caracteres especiales.

Nota

Tiene la posibilidad de excluir procesos sin la indicación completa de la ruta de monitorización del Guard:

aplicación.exe

No obstante, esto es válido exclusivamente para procesos cuyos ficheros ejecutables se encuentren en unidades del disco duro.

La indicación completa de la ruta se requiere en procesos cuyos ficheros ejecutables se encuentren en unidades conectadas, p. ej. unidades de red. Tenga en cuenta al respecto las indicaciones generales de anotación de excepciones en unidades de red conectadas.

No indique ninguna excepción en procesos cuyos ficheros ejecutables se encuentren en unidades dinámicas. Las unidades dinámicas se utilizan para soportes de datos extraíbles como CD, DVD o lápiz de memoria USB.

Nota

Las unidades de deben indicar de la siguiente forma: [letra de la unidad]:\

El carácter de dos puntos (:) sólo puede utilizarse para indicar unidades.

Nota

Al indicar el proceso puede utilizar los comodines * (sin límite de caracteres) e ? (un solo carácter):

C:\Archivos de programa\Aplicación\aplicación.exe\

C:\Archivos de programa\Aplicación\aplicaci?.exe

C:\Archivos de programa\Aplicación\aplic*.exe\

C:\Archivos de programa\Aplicación*.exe

Para evitar que los procesos queden excluidos de forma global de la monitorización del Guard, se consideran no válidos los datos formados exclusivamente por los siguientes caracteres: * (asterisco), ? (interrogante), / (barra), \ (barra invertida), . (punto), : (dos puntos).

Nota

La ruta y el nombre de fichero del proceso no deben superar un máximo de 255 caracteres. La suma de las entradas de la lista no puede superar el máximo de 6 000 caracteres.

Advertencia

¡Tenga en cuenta que todos los accesos a ficheros por procesos anotados en la lista son excluidos del análisis en busca de virus y programas no deseados! Windows Explorer y el sistema operativo en sí no pueden excluirse. La entrada correspondiente de la lista se ignorará.



Al pulsar el botón se abre una ventana en la que puede seleccionar un fichero ejecutable.

Procesos

El botón "**Procesos**" abre la ventana "*Selección de proceso*", donde se indican los procesos activos.

Añadir

Con este botón, puede añadir el proceso seleccionado al campo que aparece en la ventana.

Eliminar

Con este botón, puede borrar el proceso seleccionado que aparece en la ventana.

Ficheros a excluir por Guard

Todos los accesos a objetos de esta lista son excluidos del análisis realizado por Guard.

Campo de entrada

En este campo puede introducir el nombre del objeto fichero que no debe incluirse en el análisis en tiempo real. No hay ningún fichero objeto fichero introducido de forma estándar.

Nota

Al indicar los objetos de fichero que deben omitirse, puede utilizar los comodines * (sin límite de caracteres) e ? (un solo carácter). También se pueden excluir distintas extensiones de fichero (incluidos los comodines):

C:\Directorio*.mdb

*.mdb

*.md?

.xls

C:\Directorio*.log

Nota

Los nombres de directorio deben acabar con una barra diagonal inversa \; de no ser así, se supone que se trata de un nombre de fichero.

Nota

La suma de las entradas de la lista no puede superar el máximo de 6 000 caracteres.

Nota

Si se excluye un directorio, todos sus subdirectorios se excluyen automáticamente.

Nota

Por cada unidad puede indicar como máximo 20 excepciones con la ruta completa (empezando por la letra de la unidad).

Ejemplo: C:\Archivos de programa\Aplicación\Nombre.log

El número máximo de excepciones sin ruta completa es de 64.

Ejemplo: *.log

\Equipo1\C\Carpeta1

Nota

En el caso de unidades dinámicas que se integran (montan) como directorio en otra unidad, debe usar el alias del sistema operativo para la unidad integrada en la lista de excepciones:

p. ej., \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\

Si usa el punto de montaje (mount point) propiamente dicho, p. ej., C:\DynDrive, la unidad dinámica se analiza de todos modos. El fichero de informe del Guard permite determinar el nombre de alias del sistema operativo que se debe usar.



El botón abre una ventana en la que puede seleccionar el objeto a excluir.

Añadir

Este botón permite incluir en la ventana de visualización el objeto fichero introducido en el campo de entrada.

Eliminar

Con este botón, puede borrar el objeto seleccionado que aparece en la ventana.

Al indicar excepciones, tenga en cuenta lo siguiente:

Nota

Para excluir objetos a los que se tiene acceso con nombres de fichero DOS cortos (convención de nombres DOS 8.3), el nombre de fichero en cuestión también debe incluirse en la lista.

Nota

Un nombre de fichero que contenga un comodín no puede acabar con una barra diagonal inversa.

Por ejemplo:

```
C:\Archivos de programa\Aplicación\aplic*.exe\
```

¡Esta entrada no es válida y no se trata como una excepción!

Nota

Para las excepciones en unidades de red conectadas debe considerarse lo siguiente: si usa la letra de unidad de la unidad de red conectada, los ficheros y directorios indicados NO se excluirán del análisis del Guard. Si la ruta UNC de la lista de excepciones difiere de la ruta UNC que se usa para la conexión con la unidad de red (indicación de la dirección IP en la lista de excepciones, indicación del nombre del equipo para la conexión con la unidad de red), los directorios indicados NO se excluyen del análisis del Guard. El fichero de informe del Guard permite determinar la ruta UNC que se debe usar:

```
\\<Nombre del equipo>\<Recurso compartido>\ - O BIEN - \\<Dirección IP>\<Recurso compartido>\
```

Nota

Mediante el fichero de informe del Guard puede determinar las rutas que usará el Guard al analizar la existencia de ficheros afectados. Use en principio las mismas rutas en la lista de excepciones. Proceda del modo siguiente: establezca la función de registro del Guard en la configuración, en Guard :: informe, en **Completo**. Con el Guard activado, acceda a los ficheros, directorios, unidades incorporadas o unidades de red conectadas. Ahora puede leer la ruta que debe usarse en el fichero de informe del Guard. El fichero de informe se activa en el Centro de control en Protección local :: Guard.

Nota

Si administra el programa AntiVir en SMC, puede utilizar variables en las indicaciones de ruta en caso de excepciones de procesos y ficheros. Puede encontrar una lista de las variables que se pueden utilizar en Variables: Excepciones de Guard y escáner.

Ejemplos de procesos que deben excluirse:

- aplicación.exe

El proceso de aplicación.exe queda excluido del análisis del Guard, independientemente de en qué unidad del disco duro y en qué directorio se encuentre anwendung.exe.

- C:\Archivos de programa1\aplicación.exe

El proceso del fichero aplicación.exe, que se encuentra en la ruta C:\Archivos de programa1, queda excluido del análisis del Guard.

- C:\Archivos de programa1*.exe

Todos los procesos de ficheros ejecutables que se encuentran en la ruta C:\Archivos de programa1, quedan excluidos del análisis del Guard.

Ejemplos de ficheros que deben excluirse:

- *.mdb

Todos los ficheros con la extensión de fichero "mdb" quedan excluidos del análisis del Guard.

- *.xls*

Todos los ficheros cuya extensión de fichero comience por "xls" quedan excluidos del análisis del Guard, p. ej. ficheros con las extensiones de fichero .xls y .xlsx.

- C:\Directorio*.log

Todos los ficheros log con la extensión de fichero "log" que se encuentran en la ruta C:\Directorio, quedan excluidos del análisis del Guard.

- \\Nombre de equipo1\Recurso compartido1\

Todos los ficheros a los que se accede con una conexión "\\Nombre de equipo1\Recurso compartido1" quedan excluidos del análisis del Guard. Se trata generalmente de una unidad de red conectada que acceden a otro ordenador con directorio compartido con el nombre de equipo "Nombre de equipo1" y el nombre de recurso compartido "Recurso compartido1".

- \\1.0.0.0\Recurso compartido1*.mdb

Todos los ficheros con la extensión de fichero "mdb" a los que se accede con una conexión "\\1.0.0.0\Recurso compartido1" quedan excluidos del análisis del Guard. Se trata generalmente de una unidad de red conectada que accede a otro ordenador con directorio compartido con la dirección IP "1.0.0.0" y el nombre de recurso compartido "Recurso compartido1".

-

12.2.1.4. Heurística

Esta sección de configuración contiene los parámetros para la heurística del motor de análisis.

Los productos AntiVir disponen de unas heurísticas muy eficaces que permiten detectar malware desconocido de forma proactiva, es decir, antes de que se haya creado una firma de virus específica para ese software malintencionado y se haya enviado la correspondiente actualización del antivirus. La detección de virus se lleva a cabo mediante un minucioso análisis del código en cuestión para encontrar funciones típicas del malware. Si el código analizado se comporta de forma similar, se reporta como sospechoso. Sin embargo, ese código no es necesariamente malware; también pueden producirse falsas alarmas. El usuario debe decidir que hacer con el código encontrado, por ejemplo, basándose en su conocimiento o experiencia previa, puede decidir si la fuente que contiene el código es de confianza.

Heurística de macrovirus

Heurística de macrovirus

Su producto AntiVir incluye una potente herramienta de heurística para macrovirus. Con esta opción activada, se eliminan todas las macros en el caso de una reparación del documento afectado. Otra opción es que sólo se notifique la existencia de documentos sospechosos, es decir, se reciba una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Su programa AntiVir dispone de la tecnología AntiVir AHeAD, de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Si esta opción está activada, puede definir el nivel de "tolerancia" de la heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si está activada la opción, detecta algo menos de malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es en este caso reducido.

Nivel de detección medio

Esta configuración está activa por defecto si ha seleccionado el uso de esta heurística.

Nivel de detección alto

Si está activada la opción, detecta bastante más malware desconocido pero hay que contar con falsas alarmas.

12.2.2 ProActiv

Con el uso de Avira AntiVir ProActiv se está protegiendo de nuevas y desconocidas amenazas para las que aún no existen definiciones de virus ni heurísticas. La tecnología ProActiv está integrada en el componente Guard y observa y analiza las acciones ejecutadas por programas. Se analiza si el comportamiento de los programas presenta patrones de actividad típicos de malware: tipo de acción y secuencias de acciones. Si un programa muestra un comportamiento típico de malware, se tratará y notificará como una detección de virus : Tiene la posibilidad de bloquear la ejecución del programa o ignorar el mensaje y continuar ejecutando el programa. Puede clasificar el programa como digno de confianza y añadirlo así al filtro de aplicaciones de los programas permitidos. También puede añadir el programa a través del comando *Bloquear siempre* al filtro de aplicaciones de los programas a bloquear.

Para detectar un comportamiento sospechoso, el componente ProActiv utiliza juegos de reglas desarrollados por el Avira Malware Research Center. Los juegos de reglas son proporcionados por las bases de datos de Avira GmbH. Para recopilar información en las bases de datos de Avira, Avira AntiVir ProActiv envía información sobre programas sospechosos notificados. No obstante, tiene la posibilidad de desactivar la transmisión de datos a las bases de datos de Avira.

Nota

¡La tecnología ProActiv aún no está disponible para los sistemas de 64 bits! Windows 2000 no soporta el componente ProActiv.

General

Activar Avira AntiVir ProActiv

Con la opción activada se supervisan los programas en su sistema informático buscando acciones sospechosas. Si se produce un comportamiento típico de malware, aparecerá un mensaje. Entonces puede bloquear el programa o seguir ejecutando el programa pulsando "Ignorar". Quedan excluidos de la supervisión: programas clasificados como fiables, programas fiables y firmados incluidos de forma estándar en el filtro de aplicaciones permitidas y todos los programas que ha añadido al filtro de aplicaciones permitidas.

Mejorar la seguridad de su equipo participando en la comunidad de AntiVir ProActiv

Con esta opción activada, Avira AntiVir ProActiv envía datos a programas sospechosos, y en algunos casos, ficheros de programa sospechosos (ficheros ejecutables) al Avira Malware Research Center para un análisis online ampliado. Después de su evaluación estos datos se incluyen en los juegos de reglas del análisis de comportamiento de ProActiv. De este modo participa en la comunidad Avira ProActiv y contribuye en la continua mejora y depuración de la tecnología de seguridad ProActiv. Con esta opción desactivada no se envían datos. Esto no afecta a la funcionalidad de ProActiv.

Para obtener más información, haga clic aquí

A través de este enlace se accede a una página Web con más información detallada sobre el análisis online ampliado. Los datos que se transfieren en un análisis online ampliado, se indican por completo en la página Web.

12.2.2.1. Filtro de aplicación: Aplicaciones a bloquear

*Bajo filtro de aplicación: En las aplicaciones a bloquear puede incorporar aplicaciones que considera nocivas y que desea que Avira AntiVir ProActiv bloquee de forma estándar. Las aplicaciones incorporadas no pueden ejecutarse en su sistema informático. También puede añadir programas al filtro de las aplicaciones a bloquear a través del mensaje del Guard acerca de un comportamiento sospechoso de un programa, utilizando la opción *Bloquear siempre este programa* .*

Aplicaciones a bloquear

Aplicaciones

La lista contiene todas las aplicaciones que ha clasificado como nocivas y añadido a través de la configuración o los mensajes del componente ProActiv. Las aplicaciones de la lista son bloqueadas por Avira AntiVir ProActiv y no pueden ejecutarse en su equipo. Al iniciarse un programa bloqueado aparece un mensaje del sistema operativo. Las aplicaciones a bloquear son identificadas por Avira AntiVir ProActiv por la ruta y el nombre de fichero indicados y se bloquean independientemente de su contenido.

Campo de entrada

Indique en este campo la aplicación que desea bloquear. Para la identificación de la aplicación es necesario indicar la ruta completa y el nombre del fichero junto con su extensión. La indicación de la ruta debe incluir la unidad que contiene la aplicación o comenzar con una variable de entorno.



Al pulsar el botón se abre una ventana en la que puede seleccionar la aplicación a bloquear.

Añadir

El botón "**Añadir**" permite incorporar la aplicación que consta en el campo de entrada en la lista de aplicaciones a bloquear.

Nota

No se pueden añadir aplicaciones necesarias para la funcionalidad del sistema operativo.

Eliminar

Con el botón "**Eliminar**" puede borrar la aplicación marcada de la lista de aplicaciones a bloquear.

12.2.2.2. Filtro de aplicación: Aplicaciones permitidas

Bajo *filtro de aplicación*: Bajo *aplicaciones permitidas* figuran aplicaciones excluidas de la supervisión por el componente ProActiv: programas que han sido clasificados como fiables y están en la lista de forma estándar, todas las aplicaciones que usted ha clasificado como fiables y añadido al filtro de aplicación: En la configuración puede añadir aplicaciones a la lista de las aplicaciones permitidas. También tiene la posibilidad añadir aplicaciones a través de los mensajes del Guard acerca de un comportamiento de programa sospechoso, activando en el mensaje Guard la opción **Programa de confianza**.

Aplicaciones a excluir

Aplicaciones

La lista contiene aplicaciones excluidas de la supervisión por el componente ProActiv. Con la configuración predeterminada tras la instalación la lista contiene aplicaciones firmadas de productores de confianza. Tiene la posibilidad de incorporar aplicaciones que considera de confianza a través de la configuración o los mensajes del Guard. El componente ProActiv identifica las aplicaciones por la ruta, el nombre de fichero y el contenido. La comprobación del contenido es útil, ya que a un programa puede añadirse código dañino con posterioridad por ejemplo a través de actualizaciones. Puede determinar a través del tipo indicado, si desea realizar un análisis del contenido: Con el tipo "*Contenido*" las aplicaciones indicadas con ruta y nombre de fichero son comprobadas en cuanto a modificaciones de su contenido, antes de que sean excluidas de la supervisión por el componente ProActiv. Si el contenido del fichero ha variado, el componente ProActiv vuelve a supervisar la aplicación. Con el tipo "*Ruta*" no se analiza el contenido antes de excluir la aplicación de la supervisión por el Guard. Para cambiar el tipo de exclusión haga clic en el tipo indicado.

Advertencia

Utilice el tipo *Ruta* sólo en casos excepcionales. A través de una actualización se puede añadir código dañino a una aplicación. La aplicación antes inofensiva se convierte en malware.

Nota

Algunas aplicaciones de confianza, como p. ej. todos los componentes de aplicación de su programa AntiVir, están excluidas de forma estándar de la supervisión por el componente ProActiv pero no figuran en la lista.

Campo de entrada

Indique en este campo las aplicaciones que desea excluir de la supervisión por el componente ProActiv. Para la identificación de la aplicación es necesario indicar la ruta completa y el nombre del fichero junto con su extensión. La indicación de la ruta debe incluir la unidad que contiene la aplicación o comenzar con una variable de entorno.



Al pulsar el botón se abre una ventana en la que puede seleccionar la aplicación omitida.

Añadir

El botón "**Añadir**" permite incorporar la aplicación que consta en el campo de entrada en la lista de aplicaciones omitidas.

Eliminar

Con el botón "**Eliminar**" puede borrar la aplicación marcada de la lista de aplicaciones omitidas.

12.2.3 Informe

El Guard incluye una completa función de registro que puede ayudar al administrador en la identificación de una detección.

Protocolización

En este grupo se determina el volumen de contenido del fichero de informe.

Desactivado

Con esta opción el Guard no crea ningún protocolo.

Desactive la protocolización sólo en casos excepcionales, p. ej. sólo cuando realice una prueba con muchos virus o programas no deseados.

Predeterminado

Si la opción está activada, el Guard incluye información importante (sobre la detección, advertencias y errores) en el fichero de registro; la información de menor importancia se ignora para mayor claridad. Este ajuste está activado de forma estándar.

Ampliado

Con esta opción activada, el Guard registra también información secundaria.

Completo

Si la opción está activada, el Guard registra toda la información en el fichero de informe, incluso la correspondiente al tamaño de fichero, tipo de fichero, fecha, etc.

Limitar fichero de informe

Limitar tamaño a n MB

Si la opción está activada, el fichero de registro se puede limitar a un determinado tamaño; posibles valores: 1 a 100 MB. En la limitación del fichero de informe se concede un margen de unos 50 kilobytes para mantener reducida la carga del equipo. Si el tamaño del fichero de informe supera la magnitud indicada en 50 kilobytes, se eliminan automáticamente tantas entradas antiguas como sea necesario para alcanzar la magnitud indicada menos 50 kilobytes.

Guardar fichero de informe antes de reducir

Si está activada esta opción, se hace una copia del fichero de informe antes de reducirlo. Ubicación de copia de seguridad, ver Configuración :: General :: Directorios :: Carpeta de Informes.

Escribir configuración en fichero de informe

Al activar esta opción, la configuración del análisis directo se guarda en el fichero de informe.

Nota

Si no ha indicado ninguna limitación del fichero de informe, se creará de forma automática un nuevo fichero de informe cuando el fichero de informe haya alcanzado un tamaño de 100 MB. Se creará una copia de seguridad del antiguo fichero de informe. Se preservarán hasta tres copias de seguridad de los antiguos ficheros de informe. Las copias de seguridad más antiguas son las que primero se borran.

12.3 MailGuard

La sección MailGuard es responsable de la configuración del MailGuard.

12.3.1 Análisis

Esta utilizando el MailGuard para analizar los emails entrantes en cuanto a la existencia de virus, malware . El MailGuard también puede analizar los emails salientes en cuanto a la existencia de virus y malware.

Análisis

Activar MailGuard

Si esta opción está activada, MailGuard supervisa el tráfico de correo electrónico. MailGuard es un servidor proxy que comprueba el tráfico de datos entre el servidor de correo que utiliza y el programa de cliente de correo en su sistema informático. En la configuración predeterminada se analiza la existencia de malware en los emails entrantes. Si la opción está desactivada, se inicia el servicio MailGuard, pero se desactiva la monitorización por parte de MailGuard.

Analizar emails entrantes

Si está activada la opción, los emails salientes se analizan en cuanto a la existencia de virus y malware . MailGuard soporta los protocolos POP3 y IMAP. Active la cuenta de entrada de correo que usa su cliente de correo para recibir emails con el fin de que el MailGuard la supervise.

Supervisar cuentas POP3

Si la opción está activada, se supervisan las cuentas POP3 en los puertos indicados.

Puertos supervisados

En este campo se indica el puerto que usa el protocolo POP3 como entrada de correo. Indique varios puertos separándolos con comas.

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de POP3.

Supervisar cuentas IMAP

Si la opción está activada, se supervisan las cuentas IMAP en los puertos indicados.

Puertos supervisados

En este campo se indica el puerto que usa el protocolo IMAP. Indique varios puertos separándolos con comas.

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de IMAP.

Analizar emails salientes (SMTP)

Si está activada la opción, se analiza la existencia de virus y malware en los emails salientes.

Puertos supervisados

En este campo se indica el puerto que usa el protocolo SMTP como salida de correo. Indique varios puertos separándolos con comas.

Predeterminado

Este botón restablece los puertos indicados con el puerto predeterminado de SMTP.

Nota

Para verificar los protocolos y puertos usados, abra las propiedades de sus cuentas de email en el programa del cliente de correo. Normalmente se usan puertos estándar.

12.3.1.1. Acción en caso de detección

Esta sección de configuración contiene los parámetros que indican la acción que se ejecutará cuando MailGuard detecte un virus o programa no deseado en un email o en los datos adjuntos.

Nota

Las acciones establecidas aquí se llevan a cabo tanto en el caso de detectar virus en emails entrantes como al detectarlos en emails salientes.

Acción en caso de detección

Interactiva

Si esta opción está activada, se abre un cuadro de diálogo cuando se detecta un virus o programa indeseado, en el que se pregunta por la acción a ejecutar con el email o fichero adjunto. Esta opción está activada de forma estándar.

Acciones permitidas

En este cuadro puede especificar aquellas acciones que van a mostrarse en el cuadro de diálogo en el caso de que se descubra un virus o programa no deseado. Para ello, debe activar las opciones correspondientes.

Mover a cuarentena

Si está activada esta opción, el email, incluidos todos los datos adjuntos, se copia a la cuarentena. Puede enviarse posteriormente mediante el gestor de cuarentena. El email afectado se elimina. Un texto predeterminado sustituye el cuerpo de texto y, si fuera el caso, los datos adjuntos del email.

Eliminar

Si esta opción está activada, el email concerniente se elimina si se ha encontrado un virus o programa no deseado. Un texto predeterminado sustituye el cuerpo de texto y, si fuera el caso, los datos adjuntos del email.

Eliminar datos adjuntos

Si está activada esta opción, un texto predeterminado sustituye los datos adjuntos afectados. Si estuviera afectado el cuerpo de texto del email, éste se elimina y también se sustituye por un texto predeterminado. El email en sí, se entrega.

Mover datos adjuntos a cuarentena

Si está activada esta opción, los datos adjuntos afectados se colocan en cuarentena y después se eliminan (sustituyen por un texto predeterminado). El cuerpo del mensaje se entrega. El adjunto puede enviarse más tarde mediante el Gestor de Cuarentena

Omitir

Si esta opción está activada, el email concerniente se entrega independiente de si se ha encontrado un virus o programa no deseado.

Predeterminado

Este botón le permite seleccionar la acción que será activada de forma estándar en el cuadro de diálogo que aparece al detectar un virus. Seleccione la acción que será activada de forma estándar y pulse **Predeterminado**.

Mostrar la barra de progreso

Si esta opción está activada, el MailGuard muestra una barra de progreso durante la descarga de los emails. Sólo se puede activar esta opción si se seleccionó la opción **Interactivo**.

Automático

Con esta opción activada, no se realizarán más notificaciones en caso de encontrar algún virus o programa no deseado. El MailGuard reacciona de acuerdo a lo que configure en esta sección.

Acción principal

La acción principal es la que se ejecuta cuando el MailGuard detecta un virus o programa no deseado en un email. Si la opción "**Ignorar Email**" se ha seleccionado, aún puede seleccionarse en "**Adjuntos afectados**" la acción a tomar cuando se ha detectado un programa o virus no deseado en un adjunto.

Eliminar email

Si esta opción está activada, el email concerniente se elimina automáticamente si se ha encontrado un virus o programa no deseado. El cuerpo del mensaje se reemplaza por el texto estándar siguiente. Lo mismo se aplica a todos los adjuntos incluidos; estos también se reemplazan con un texto estándar.

Aislar email

Si la opción está activada, todo el email, incluidos sus datos adjuntos, se ponen en cuarentena al detectar un virus o un programa no deseado. Si se requiere, puede restaurarse más tarde. El email afectado en si, se elimina. El cuerpo del mensaje se reemplaza por el texto estándar siguiente. Lo mismo se aplica a todos los adjuntos incluidos; estos también se reemplazan con un texto estándar.

Omitir email

Si esta opción está activada, el email concerniente se ignora, independientemente de si se ha encontrado un virus o programa no deseado. De todas formas, puede decidir qué hacer con el fichero adjunto afectado:

Datos adjuntos afectados

La opción "**Adjuntos afectados**" sólo puede seleccionarse si se ha configurado como "**Acción principal**" el ajuste "**Ignorar email**". Con esta opción ahora es posible decidir qué hacer si se encuentra un virus o programa no deseado en un fichero adjunto.

eliminar

Si esta opción está activada, se elimina el fichero adjunto afectado si se encuentra un virus o programa no deseado y es reemplazado por un texto estándar.

aislar

Si la opción está activada, los datos adjuntos afectados se envían a cuarentena y después se eliminan (se reemplazan con un texto predeterminado). Los datos adjuntos afectados pueden restablecerse posteriormente si se desea.

omitir

Si está activada la opción, los datos adjuntos se omiten y se envían aunque se haya detectado un virus o programa no deseado.

Advertencia

Con esta opción seleccionada no tiene protección contra virus o programa no deseado por parte de MailGuard. Seleccione esta opción sólo si está seguro de lo que está haciendo. ¡Desactive la vista previa en su programa de correo y nunca abra un fichero adjunto con un doble clic!

12.3.1.2. Otras acciones

Esta sección de configuración contiene parámetros adicionales para establecer las acciones que se ejecutarán si el MailGuard detecta un virus o programa no deseado en un email o en sus datos adjuntos.

Nota

Las acciones configuradas aquí se llevan a cabo únicamente en caso de detección de virus en emails entrantes.

Texto predeterminado para emails eliminados y movidos

El texto de este campo se inserta como mensaje en el email infectado sustituyéndolo. Puede modificar este mensaje. El texto puede contener un máximo de 500 caracteres.

Puede usar la siguiente combinación de teclas para aplicar formatos:

Strg + **Enter** inserta un salto de línea.

Predeterminado

Este botón inserta un texto estándar predefinido en el campo de edición.

Texto predeterminado para datos adjuntos eliminados y movidos

El texto de este campo se inserta como mensaje en el email infectado sustituyendo los datos adjuntos. Puede modificar este mensaje. El texto puede contener un máximo de 500 caracteres.

Puede usar la siguiente combinación de teclas para aplicar formatos:

Strg + **Enter** inserta un salto de línea.

Predeterminado

Este botón inserta un texto estándar predefinido en el campo de edición.

12.3.1.3. Heurística

Esta sección de configuración contiene los parámetros para la heurística del motor de análisis.

Los productos AntiVir disponen de unas heurísticas muy eficaces que permiten detectar malware desconocido de forma proactiva, es decir, antes de que se haya creado una firma de virus específica para ese software malintencionado y se haya enviado la correspondiente actualización del antivirus. La detección de virus se lleva a cabo mediante un minucioso análisis del código en cuestión para encontrar funciones típicas del malware. Si el código analizado se comporta de forma similar, se reporta como sospechoso. Sin embargo, ese código no es necesariamente malware; también pueden producirse falsas alarmas. El usuario debe decidir que hacer con el código encontrado, por ejemplo, basándose en su conocimiento o experiencia previa, puede decidir si la fuente que contiene el código es de confianza.

Heurística Macrovirus

Activar heurística de macrovirus

Su producto AntiVir incluye una potente herramienta de heurística para macrovirus. Con esta opción activada, se eliminan todas las macros en el caso de una reparación del documento afectado. Otra opción es que sólo se notifique la existencia de documentos sospechosos, es decir, se reciba una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Su programa AntiVir dispone de la tecnología AntiVir AHeAD, de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Si esta opción está activada, puede definir el nivel de "tolerancia" de la heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si está activada la opción, detecta algo menos de malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es en este caso reducido.

Nivel de detección medio

Esta opción está activa de forma estándar si ha seleccionado la aplicación de esta heurística. Este ajuste está activado de forma estándar y es el recomendado.

Nivel de detección alto

Si está activada la opción, se detecta bastante más malware desconocido pero hay que contar con falsas alarmas.

12.3.2 General

12.3.2.1. Excepciones


Direcciones de email no analizadas

Esta tabla muestra la lista de direcciones de email excluidas del análisis por parte del AntiVir MailGuard (lista blanca).

Nota

El MailGuard utiliza la lista de excepciones exclusivamente en el caso de emails entrantes.

Estado

Icono	Descripción
	Esta dirección de email no se analizará más en busca de malware.

Dirección de correo/email

Esta dirección de email no se analizará más.

Malware

Si esta opción está activada, la dirección de email no se analizará más en busca de malware.

arriba

Con este botón la dirección de email marcada se desplaza una posición hacia arriba. Este botón no está activado si no hay ninguna entrada marcada o si la dirección marcada es la primera posición de la lista.

abajo

Con este botón la dirección de email marcada se desplaza una posición hacia abajo. Este botón no está activado si no hay ninguna entrada marcada o si la dirección marcada es la última posición de la lista.

Campo de entrada

Aquí se introduce la dirección de email que desee añadir a la lista de direcciones que no se analizarán. Dependiendo de su configuración, la dirección de correo no será analizada en futuro por el MailGuard.

Añadir

Aquí se introduce la dirección de email que desees añadir a la lista de direcciones que no se analizarán.

Eliminar

El botón elimina la dirección seleccionada de la lista.

12.3.2.2. Memoria caché

Memoria caché

La memoria caché del MailGuard contiene los datos acerca de los emails analizados que se muestran en la estadística del Centro de control bajo MailGuard.

Número máximo de emails para almacenar en la caché

Este campo contiene el máximo número de emails que el MailGuard mantiene en la caché. Los emails más antiguos son los que primero se borran.

Tiempo máximo de almacenamiento de un email en días

Aquí se introduce el número máximo de días durante el cual se guarda un email. Tras este periodo, se elimina el email de la memoria caché.

Vaciar memoria caché

Hacer clic en este botón para eliminar los emails almacenados en la caché.

12.3.2.3. Pie de página

En *Pie de página* puede configurar el pie de página que desea que se muestre en los emails que envía. Esta función requiere la activación de la comprobación de los emails salientes por MailGuard (véase la opción *Analizar emails salientes (SMTP)* en Configuración::MailGuard::Análisis) . Puede utilizar el pie de página predefinido de AntiVir MailGuard con el que confirma que el email enviado ha sido comprobado por un programa antivirus. También tiene la posibilidad de introducir un texto propio para un pie de página personalizado. Si utiliza las dos opciones de pie de página, el texto definido por el usuario antecede al pie de página de AntiVir MailGuard.

Pie de página de los emails a enviar

Anexar pie de página de AntiVir MailGuard

Si la opción está activada, se visualiza debajo del texto del mensaje de los emails enviados el pie de página de AntiVir MailGuard. Con el pie de página de AntiVir MailGuard, usted confirma que el email enviado ha sido comprobado por el AntiVir MailGuard en cuanto a virus y programas no deseados. El pie de página de AntiVir MailGuard contiene el siguiente texto: "Analizado por AntiVir MailGuard [versión del producto] [abreviatura y número de versión del motor de análisis] [abreviatura y número de versión del fichero de firmas de virus]".

Anexar este pie de página

Con la opción activada se visualiza en los emails enviados el texto que indica en el campo de entrada.

Campo de entrada

En este campo de entrada puede introducir un texto que será visualizado como pie de página en los emails enviados.

12.3.3 Informe

El MailGuard incluye una completa función de registro que puede ayudar al administrador en la identificación de una detección.

Protocolización

En este grupo se determina el volumen de contenido del fichero de informe.

Desactivado

Con esta opción el MailGuard no crea ningún registro/informe.

Desactive la protocolización sólo en casos excepcionales, p. ej. sólo cuando realice una prueba con muchos virus o programas no deseados.

Predeterminado

Si la opción está activada, el MailGuard incluye información importante (sobre la detección, advertencias y errores) en el fichero de registro; la información de menor importancia se omite para mayor claridad. Este ajuste está activado de forma estándar.

Ampliado

Con esta opción activada, el MailGuard registra también información secundaria.

Completo

Con esta opción activada, el MailGuard registra toda la información en el fichero de informe.

Limitar fichero de informe

Limitar tamaño a n MB

Si la opción está activada, el fichero de registro se puede limitar a un determinado tamaño; posibles valores: 1 a 100 MB. En la limitación del fichero de informe se concede un margen de unos 50 kilobytes para mantener reducida la carga del equipo. Si el tamaño del fichero de informe supera la magnitud indicada en 50 kilobytes, se eliminan automáticamente tantas entradas antiguas como sea necesario para alcanzar la magnitud indicada menos 50 kilobytes.

Guardar fichero de informe antes de reducir

Si está activada esta opción, se hace una copia del fichero de informe antes de reducirlo. Ubicación de copia de seguridad, ver Configuración :: General :: Directorios :: Carpeta de Informes.

Escribir configuración en fichero de informe

Si esta opción está activada, la configuración utilizada del MailGuard se guarda en el fichero de informe.

Nota

Si no ha indicado ninguna limitación del fichero de informe, se creará de forma automática un nuevo fichero de informe cuando el fichero de informe haya alcanzado un tamaño de 100 MB. Se creará una copia de seguridad del antiguo fichero de informe. Se preservarán hasta tres copias de seguridad de los antiguos ficheros de informe. Las copias de seguridad más antiguas son las que primero se borran.

12.4 Firewall

La sección FireWall de la configuración se encarga de la configuración del componente Avira FireWall.

12.4.1 Reglas del adaptador

Un adaptador representa para Avira FireWall un dispositivo de hardware simulado (p. ej., Miniport, Bridge Connection, etc.) o un dispositivo de hardware real (p. ej., una tarjeta de red).

Avira FireWall muestra las reglas de todos los adaptadores existentes en el equipo para los que se instaló un controlador.

Las reglas predefinidas dependen del nivel de seguridad. Puede modificar el nivel de seguridad en la sección Protección online :: Modificar FireWall del Centro de control o adaptar las reglas del adaptador a sus necesidades. Si ha adaptado las reglas del adaptador a sus necesidades, en la sección FireWall del Centro de control en el área Nivel de seguridad, el regulador se sitúa en Usuario.

Nota

La configuración predeterminada del nivel de seguridad para todas las reglas predefinidas de Avira FireWall es **Medio**.

Protocolo ICMP

El protocolo ICMP (Internet Control Message Protocol) se utiliza para intercambiar mensajes de error e información en las redes. El protocolo también se utiliza para los mensajes de estado con ping o tracert.

Con esta regla puede definir los tipos ICPM de entrada y salida que deben ser bloqueados, los parámetros para desbordamiento y el comportamiento ante paquetes ICMP fragmentados. Esta regla sirve para evitar los ataques conocidos como de desbordamiento ICPM (ICPM Flood) que pueden conllevar una carga o sobrecarga del procesador del equipo atacado al responder a todos los paquetes.

Reglas predefinidas para el protocolo ICMP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
Bloquea tipos entrantes: sin tipo . Bloquea tipos salientes: sin tipo . Asumir desbordamiento si el retraso entre paquetes es inferior a 50ms . Rechazar paquetes ICMP fragmentados.	La misma regla que para el nivel bajo	Bloquea tipos entrantes: varios tipos . Bloquea tipos salientes: varios tipos . Asumir desbordamiento si el retraso entre paquetes es inferior a 50ms . Rechazar paquetes ICMP fragmentados.

Tipos entrantes bloqueados: sin tipo/varios tipos

Haciendo clic en el enlace se abre una lista con los tipos de paquete ICMP. En esta lista puede seleccionar los tipos de mensaje ICMP entrantes que desee bloquear.

Tipos de salida bloqueados: sin tipo/varios tipos

Haciendo clic en el enlace se abre una lista con los tipos de paquete ICMP. En esta lista puede seleccionar los tipos de mensaje ICMP salientes que desee bloquear.

Desbordamiento

Haciendo clic en el enlace se abre un cuadro de diálogo donde puede introducir el valor máximo permitido para el retardo de ICMP.

Paquetes ICMP Fragmentados

Haciendo clic en el enlace tiene la posibilidad de rechazar o no los paquetes ICMP fragmentados.

Escaneo de puertos TCP

Con esta regla se define cuándo el FireWall debe suponer que existe un escaneo de puertos TCP y cómo debe comportarse en este caso. Esta regla sirve para evitar los ataques conocidos como de escaneo de puertos TCP, que pueden detectar puertos abiertos en su equipo. Esta clase de ataque se emplea la mayoría de las veces para detectar los puntos débiles en un equipo y posteriormente lanzar ataques más serios.

Reglas predeterminadas para el escaneo de puertos TCP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
Suponer que existe escaneo de puertos TCP si 50 o más puertos se han escaneado en 5 000 milisegundos. Si se detecta un escaneo de puertos TCP, <code>span style="font-weight: bold;">>escribir</code> en el fichero de informe la dirección IP del atacante y no añadir la regla para bloquear el ataque.	Suponer que existe escaneo de puertos TCP si 50 o más puertos se han escaneado en 5 000 milisegundos. Si se detecta un escaneo de puertos TCP, escribir en el fichero de informe la dirección IP del atacante y añadir la regla para bloquear el ataque.	La misma regla que para el nivel medio.

Puertos

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede indicar la cantidad de puertos que deben haberse escaneado para suponer que se trata de un escaneo de puertos TCP.

Ventana de tiempo de escaneo de puertos

Al hacer clic en el enlace aparece un cuadro de diálogo donde puede introducir el intervalo de tiempo en el que debe haberse escaneado un determinado número de puertos para suponer que se trata de un escaneo de puertos TCP.

Fichero de informe

Al hacer clic en el enlace puede hacer que se registre o no la IP del atacante.

Regla

Al hacer clic en el enlace tiene la opción de decidir si se añadirá o no la regla de bloqueo de ataques por escaneo de puertos TCP.

Escaneo de puertos UDP

Con esta regla se define cuándo el FireWall debe suponer que existe escaneo de puertos UDP y cómo debe comportarse en este caso. Esta regla sirve para evitar los ataques conocidos como de escaneo de puertos UDP, que pueden detectar puertos abiertos en su equipo. Esta clase de ataque se emplea la mayoría de las veces para detectar los puntos débiles en un equipo y posteriormente lanzar ataques más serios.

Reglas predeterminadas para el escaneo de puertos UDP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
Suponer que existe escaneo de puertos UDP si 50 o más puertos se han escaneado en 5 000 milisegundos. Si se detecta un escaneo de puertos UDP, escribir	Suponer que existe escaneo de puertos UDP si 50 o más puertos se han escaneado en 5 000 milisegundos. Si se detecta un escaneo de puertos TCP, escribir	La misma regla que para el nivel medio.

en el fichero de informe la dirección IP del atacante y **no añadir** la regla para bloquear el ataque.

en el fichero de informe la dirección IP del atacante y **añadir** la regla para bloquear el ataque.

Puertos

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede indicar la cantidad de puertos que deben haberse escaneado para suponer que se trata de un escaneo de puertos UDP.

Ventana de tiempo de escaneo de puertos

Al hacer clic en el enlace aparece un cuadro de diálogo donde puede introducir el intervalo de tiempo en el que debe haberse escaneado un determinado número de puertos para suponer que se trata de un escaneo de puertos UDP.

Fichero de informe

Al hacer clic en el enlace puede hacer que se registre o no la IP del atacante.

Regla

Al hacer clic en el enlace tiene la opción de decidir si se añadirá o no la regla de bloqueo de ataques por escaneo de puertos UDP.

12.4.1.1. Reglas de Entrada

Las reglas de entrada sirven para controlar el tráfico de datos entrante por medio de Avira FireWall.

Nota

Cuando se filtra un paquete las reglas correspondientes se aplican sucesivamente, por lo que el orden es muy importante. Cambie el orden de las reglas únicamente cuando tenga la completa seguridad de lo que está haciendo.

Reglas predeterminadas para monitorizar el tráfico de datos TCP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
Avira FireWall no bloquea el tráfico de datos entrante.	<ul style="list-style-type: none"> Permitir conexión TCP establecida en puerto 135 <p>Permitir paquetes TCP desde la dirección 0.0.0.0 con la máscara 0.0.0.0 si el puerto local se encuentra en {135} y el puerto remoto en {0-65535}. Aplicar para paquetes en las conexiones</p>	<ul style="list-style-type: none"> Monitorizar tráfico de datos TCP admitido <p>Permitir paquetes TCP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar para paquetes en las conexiones existentes.</p>

	<p>existentes. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p> <p>– Denegar paquetes TCP en el puerto 135</p> <p>Denegar paquetes TCP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {135} y el puerto remoto en {0-65535}. Aplicar para todos los paquetes. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Denegar paquetes con los siguientes bytes <vacío> con máscara <vacío> en el desplazamiento 0.</p> <p>– Monitorizar el tráfico de datos</p>	<p>No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p>
--	---	--

	<p>conforme a TCP</p> <p>Permitir paquetes TCP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar al inicio del establecimiento de la conexión y a paquetes de conexiones existentes. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p> <p>– Denegar todos los paquetes TCP</p> <p>Denegar paquetes TCP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar para todos los paquetes.</p>	
--	---	--

	<p>No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p>	
--	--	--

Aceptar / denegar paquetes TCP

Haciendo clic en este enlace tiene la opción de decidir si desea permitir o denegar paquetes TCP especialmente definidos.

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Puertos locales

Al hacer clic en este enlace aparece un cuadro de diálogo en el que puede definir el número de puerto(s) local(es) o rango(s).

Puertos remotos

Al hacer clic en este enlace aparece un cuadro de diálogo en el que puede definir el número de puerto(s) local(es) o rango(s) remoto(s).

Método de aplicación

Al hacer clic en este enlace puede decidir si la regla se aplicará en el inicio de las conexiones y en las existente o sólo para las conexiones existentes o para todos los paquetes.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

La opción **Características avanzadas** permite el filtrado basándose en el contenido. Por ejemplo, pueden rechazarse los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico

Filtrado por contenido: máscara

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del filtrado según el contenido. El desplazamiento se calcula desde donde termina el encabezamiento TCP.

Reglas predeterminadas para monitorizar el tráfico de datos UDP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
-	<ul style="list-style-type: none"> <li data-bbox="852 624 1086 723">– Monitorizar el tráfico de datos conforme a UDP <li data-bbox="887 763 1107 1753"> <p>Permitir paquetes UDP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar la regla a puertos abiertos. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p> <li data-bbox="852 1807 1107 2047"> <p>– Denegar todos los paquetes UDP</p> <p>Denegar paquetes UDP de la dirección 0.0.0.0 con</p> 	<p>Monitorizar tráfico de datos UDP admitido</p> <p>Permitir paquetes UDP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {53, 67, 68, 123}. Aplicar la regla a puertos abiertos. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p>

	<p>máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar a todos los puertos. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p>	
--	---	--

Aceptar / denegar paquetes UDP

Haciendo clic en este enlace tiene la opción de decidir si desea permitir o denegar paquetes UDP especialmente definidos.

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Puertos locales

Al hacer clic en este enlace aparece un cuadro de diálogo en el que puede definir el número de puerto(s) local(es) o rango(s).

Puertos remotos

Al hacer clic en este enlace aparece un cuadro de diálogo en el que puede definir el número de puerto(s) local(es) o rango(s) remoto(s).

Método de aplicación

Al hacer clic en este enlace puede elegir la aplicación de esta regla a todos los puertos o sólo a los abiertos.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

La opción **Características avanzadas** permite el filtrado basándose en el contenido. Por ejemplo, pueden rechazarse los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico

Filtrado por contenido: máscara

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del filtrado según el contenido. El desplazamiento se calcula desde donde termina el encabezamiento UDP.

Reglas predeterminadas para monitorizar el tráfico de datos ICMP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
-	- No descartar paquetes ICMP sobre la base de la dirección IP Permitir paquetes ICMP de la dirección 0.0.0.0 con máscara 0.0.0.0 . No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0 .	La misma regla que para el nivel medio.

Aceptar / denegar paquetes ICMP

Haciendo clic en este enlace tiene la opción de decidir si desea permitir o denegar paquetes ICMP especialmente definidos.

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

La opción **Características avanzadas** permite el filtrado basándose en el contenido. Por ejemplo, pueden rechazarse los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico

Filtrado por contenido: máscara

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del filtrado según el contenido. El desplazamiento se calcula desde donde termina el encabezamiento ICMP.

Reglas predeterminadas para los paquetes IP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
-	-	Denegar todos los paquetes IP Denegar paquetes IP de la dirección 0.0.0.0 con máscara 0.0.0.0 . No escribir en el fichero de informe cuando el paquete cumple la regla.

Aceptar / denegar paquetes TCP

Al hacer clic en el enlace puede decidir si permitir o denegar los paquetes IP entrantes definidos especialmente

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

Reglas posibles para la monitorización de paquetes IP basándose en protocolos IP

Paquetes IP

Al hacer clic en el enlace puede decidir si permitir o denegar los paquetes IP entrantes definidos especialmente

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Protocolo

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir el protocolo IP requerido.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

12.4.1.2. Reglas de salida

Las reglas de salida se definen para controlar el tráfico de datos saliente a través de Avira FireWall. Puede definir una regla saliente para los siguientes protocolos: IP, ICMP, UDP y TCP.

Nota

Cuando se filtra un paquete las reglas correspondientes se aplican sucesivamente, por lo que el orden es muy importante. Cambie el orden de las reglas únicamente cuando tenga la completa seguridad de lo que está haciendo.

Botones

Botón	Descripción
Añadir	Permite crear una nueva regla. Pulsando este botón aparece el cuadro de diálogo " Añadir nueva regla ". En este cuadro de diálogo puede seleccionar nuevas reglas.
Quitar	Elimina la regla seleccionada.
Bajar	Mueve la regla seleccionada una línea hacia abajo, es decir reduce la prioridad de la regla.
Subir	La regla seleccionada se desplaza una posición hacia arriba, por lo que aumenta su prioridad.
Cambiar el nombre	Permite renombrar la regla seleccionada.

Nota

Puede añadir nuevas reglas para cada adaptador o para todos los adaptadores del equipo. Para añadir una regla de adaptador para todos los adaptadores, seleccione **Equipo** en la estructura del adaptador que se muestra y haga clic en el botón **Añadir**.

Nota

Para cambiar la posición de una regla, también puede arrastrarla con el ratón a la posición pertinente.

12.4.2 Reglas de aplicación

Reglas de Aplicación para el usuario

En esta lista constan todos los usuarios del sistema. Si ha iniciado sesión como administrador, puede seleccionar un usuario para el que desea crear reglas. Si no es un usuario con privilegios, sólo puede ver el usuario identificado actualmente.

Lista de Aplicaciones

Esta tabla muestra la lista de aplicaciones para las que se han definido reglas. Esta lista de aplicaciones contiene la configuración de cada aplicación que se ha ejecutado y que tenía una regla asociada desde que se instaló Avira FireWall.

Vista Normal

	Descripción
Aplicación	Nombre de la aplicación.
Modo	Muestra el modo establecido de la regla de aplicación : En el modo filtrado , tras ejecutar la regla de aplicación, se comprueban y ejecutan reglas del adaptador. En el modo <i>con privilegios</i> se omiten las reglas del adaptador. Haciendo clic en este enlace tiene la opción de cambiar a otro modo.
Acción	Muestra la acción que Avira FireWall tomará automáticamente cuando la aplicación utiliza la red de cualquier forma. Con un clic en el enlace, puede cambiar a otro tipo de acción. Puede seleccionar entre los tipos de acción Preguntar , Permitir o Denegar . La acción de forma estándar es Preguntar .

Configuración avanzada

Si desea regular de forma personalizada los accesos de red de una aplicación, puede crear reglas de aplicación específicas basadas en los filtros de paquete de manera similar a las reglas de adaptador. Para cambiar a la configuración avanzada de las reglas de aplicación, debe activar primero el modo experto. En la sección FireWall:: Configuración cambie el parámetro para reglas de aplicación: active la opción **Configuración avanzada** y guarde el parámetro con **Aplicar** o **Aceptar**. Dentro de la configuración de FireWall, cambie a la sección **FireWall::Reglas de aplicación**: En la lista de las reglas de aplicación se muestra una columna adicional *Filtrado* con la entrada *Simple*. Ahora dispone de la opción adicional **Filtrado: Avanzado - Acción: Reglas**, con la que puede cambiar a la configuración avanzada.

	Descripción
Aplicación	Nombre de la aplicación.
Modo	Muestra el modo establecido de la regla de aplicación : En el modo filtrado , tras ejecutar la regla de aplicación, se comprueban y ejecutan reglas del adaptador. En el modo <i>con privilegios</i> se omiten

	las reglas del adaptador. Haciendo clic en este enlace tiene la opción de cambiar a otro modo.
Acción	Muestra la acción que Avira FireWall tomará automáticamente cuando la aplicación utiliza la red de cualquier forma. Con la configuración <i>Filtrado - simple</i> puede cambiar a otro tipo de acción mediante clic sobre el enlace. Puede seleccionar entre los tipos de acción Preguntar, Permitir, Denegar o <i>Avanzado</i> . Con la configuración <i>Filtrado - avanzado</i> se muestra el tipo de acción <i>Reglas</i> . El enlace Reglas abre la ventana Reglas de aplicación , donde puede guardar reglas de aplicación específicas.
Filtrado	Muestra el tipo de filtrado. Con un clic en el enlace, puede cambiar a otro tipo de filtrado. <i>Simple</i> : Con filtrado simple la acción indicada se ejecuta en cualquier actividad de red de la aplicación de software. <i>Avanzado</i> : Durante el filtrado se ejecutan las reglas que se hayan guardado en la configuración avanzada.

Si desea crear reglas de aplicación específicas para una aplicación, en *Filtrado* cambie a la entrada **Avanzado**. En la columna **Acción** se muestra la entrada *Reglas*. Haga clic sobre **Reglas** para llegar a la ventana para la creación de reglas de aplicación específicas.

Reglas de aplicación específicas en la configuración avanzada

Con las reglas de aplicación específicas puede permitir o denegar un tráfico de datos específico de la aplicación, así como permitir o denegar la escucha pasiva de determinados puertos. Dispone de las siguientes opciones:

- Permitir o denegar la inyección de código

La inyección de código es una técnica con la que se ejecuta código en el ámbito de direcciones de otro proceso obligando a ese proceso a cargar una biblioteca de vínculos dinámicos (DLL). El software malintencionado o malware, entre otros, utiliza la técnica de inyección de código para ejecutar su propio código de forma encubierta por otro programa. De este modo es posible encubrir accesos a Internet ante el FireWall. De forma estándar se permite la inyección de código a todas las aplicaciones firmadas.

- Permitir o denegar la escucha pasiva de puertos de la aplicación
- Permitir o denegar el tráfico de datos:

Permitir o denegar los paquetes IP entrantes y/o salientes

Permitir o denegar los paquetes TCP entrantes y/o salientes

Permitir o denegar los paquetes UDP entrantes y/o salientes

Para cada aplicación puede crear tantas reglas como lo desee. Las reglas de aplicación se ejecutan en el orden que se muestra .

Nota

Si modifica el filtrado *Avanzado* en una regla de aplicación, las reglas de aplicación ya creadas no se eliminan definitivamente en la configuración avanzada, sino que sólo se desactivan. Si vuelve a cambiar al filtrado *Avanzado*, las reglas de aplicación ya creadas se activan de nuevo y se muestran en la ventana de la configuración avanzada para reglas de aplicación.

Detalles de aplicación

En esta caja puede ver los detalles de la aplicación seleccionada en la lista de aplicaciones.

	Descripción
Nombre	Nombre de la aplicación.
Ruta	Ruta completa al fichero ejecutable

Botones

Botón	Descripción
Añadir aplicación	Permite la creación de una nueva regla. Pulsando este botón, se abre un cuadro de diálogo. Aquí puede seleccionar la aplicación para la que se va a crear una nueva regla.
Quitar regla	Elimina la regla de aplicación seleccionada.
Volver a cargar	Refresca la lista de aplicaciones y simultáneamente descarta los cambios en las reglas que estuviera haciendo.

12.4.3 Proveedores de confianza

En *Proveedores de confianza* se muestra una lista de productores de software de confianza. En la lista puede quitar o añadir productores mediante la opción *Confiar siempre en este proveedor* en la ventana emergente *Evento de red*. Puede permitir de forma estándar el acceso a la red de las aplicaciones firmadas por los proveedores que se enumeran si activa la opción **Permitir automáticamente aplicaciones creadas por proveedores de confianza**.

Proveedores de confianza para usuario

En esta lista constan todos los usuarios del sistema. Si ha iniciado sesión como administrador, puede seleccionar un usuario cuya lista de proveedores de confianza desee ver o actualizar. Si usted no es un usuario con privilegios, la lista sólo muestra el usuario que ha iniciado sesión.

Permitir automáticamente aplicaciones creadas por proveedores de confianza

Si está activada la opción, se permite automáticamente el acceso a la red a las aplicaciones con firma de proveedores conocidos y de confianza. La opción está activada de forma estándar.

Proveedores

La lista muestra todos los proveedores clasificados como de confianza.

Botones

Botón	Descripción
-------	-------------

Quitar	La entrada seleccionada se quita de la lista de proveedores de confianza. Para quitar el proveedor seleccionado definitivamente de la lista, pulse Aplicar o Aceptar en la ventana de configuración.
Volver a cargar	Se deshacen los cambios realizados. Se carga la última lista guardada.

Nota

Si quita proveedores de la lista y, a continuación, pulsa el botón **Aplicar**, los proveedores se eliminan definitivamente de la lista. El cambio no se puede deshacer con *Volver a cargar*. Sin embargo, existe la posibilidad de volver a añadir un proveedor a la lista de proveedores de confianza mediante la opción *Confiar siempre en este proveedor* de la ventana emergente *Evento de red*.

Nota

El FireWall da prioridad a las reglas de aplicación frente a las entradas de la lista de proveedores de confianza: si creó una regla de aplicación y el proveedor de la aplicación consta en la lista de proveedores de confianza, la regla de aplicación se ejecuta.

12.4.4 Configuración

Configuración avanzada

Activar FireWall

Con la opción activada Avira FireWall se encuentra activo y protege su equipo de los peligros procedentes de Internet y de otras redes.

Desactivar firewall de Windows al iniciar

Si la opción está activada, el Firewall de Windows estará desactivado al iniciar el equipo. Esta opción está activada de forma estándar.

El fichero host de Windows está NO BLOQUEADO/BLOQUEADO

Si esta opción aparece como BLOQUEADO, el fichero host de Windows está protegido contra escritura. Ya no es posible manipular el fichero. Por ejemplo, ningún malware podrá redirigirle a sitios Web no deseados. El estado de esta opción es NO BLOQUEADO de forma estándar.

Tiempo de espera excesivo de la regla

Bloquear siempre

Si la opción está activada, se conserva la regla creada automáticamente, por ejemplo, durante un escaneo de puertos.

Quitar la regla tras n segundos

Si esta opción está activada, una regla creada automáticamente, por ejemplo durante un escaneo de puertos, se elimina tras el periodo estipulado. Esta opción está activada de forma estándar.

Notificaciones

En Notificaciones se determina para qué eventos desea recibir una notificación del FireWall en el escritorio.

Escaneado de puertos

Si la opción está activada, recibirá una notificación en el escritorio cuando el FireWall detecte un escaneado de puertos.

Desbordamiento

Si la opción está activada, recibirá una notificación en el escritorio cuando el FireWall detecte un ataque por desbordamiento.

Aplicaciones bloqueadas

Si la opción está activada, recibirá una notificación en el escritorio cuando el FireWall deniegue la actividad de red de una aplicación, es decir, la bloquee.

IP bloqueada

Si la opción está activada, recibirá una notificación en el escritorio cuando el FireWall deniegue el tráfico de datos de una dirección IP.

Reglas de aplicación

Las opciones del área Reglas de aplicación permiten establecer las opciones de configuración para reglas de aplicación en la sección FireWall::Reglas de aplicación.

Configuración avanzada

Si la opción está activada, puede regular de forma personalizada los distintos accesos a la red de una aplicación.

Configuración básica

Si la opción está activada, sólo se puede configurar una única acción para los distintos accesos a la red de la aplicación.

12.4.5 Configuración de ventanas emergentes

Configuración de ventanas emergentes

Comprobar el bloqueo de inicio del proceso

Si la opción está activada, tiene lugar un análisis más preciso de la pila de procesos. El FireWall parte de la base de que cualquier proceso de la pila que no sea de confianza es el proceso a través de cuyo proceso secundario se accede a la red. Por ello, en este caso se abre una ventana emergente propia para cada proceso que no sea de confianza en la pila de procesos. Esta opción está desactivada de forma estándar.

Mostrar varios cuadros de diálogo por proceso

Si esta opción está activada, cada vez que una aplicación intenta establecer una conexión de red, se abre una ventana emergente. Otra opción es que la información sólo aparezca en el primer intento de conexión. Esta opción está desactivada de forma estándar.

Cancelar automáticamente ventana emergente en modo de juego

Si la opción está activada, Avira FireWall cambia automáticamente al modo de juego cuando en el sistema se ejecuta una aplicación a pantalla completa. En el modo de juego se aplican todas las reglas definidas del adaptador y de la aplicación. Las aplicaciones para las que no se definieron reglas con las acciones "Permitir" o "Denegar" disponen de permiso temporal de acceso a la red, por lo que no se abrirán ventanas emergentes con consultas sobre el evento de red.

Guardar acción para esta aplicación

Siempre activado

Si la opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" estará activada de forma predeterminada. Esta opción está activada de forma estándar.

Siempre desactivado

Si la opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" estará desactivada de forma predeterminada.

Permitir aplicaciones firmadas

Si la opción está activada, cuando las aplicaciones firmadas de determinados productores acceden a la red, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" está activada automáticamente. Los productores son: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Recordar último estado

Si la opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" se usa del mismo modo que con el último evento de red. Si en el último evento de red se activó la opción "**Guardar acción para esta aplicación**", la opción estará activa en el siguiente evento de red. Si en el último evento de red se desactivó la opción "**Guardar acción para esta aplicación**", la opción estará desactivada en el siguiente evento de red.

Mostrar detalles

En este grupo de opciones de configuración puede configurar la presentación de información detallada en la ventana **Evento de red**.

Mostrar detalles a petición

Si la opción está activada, la información detallada de la ventana "*Evento de red*" sólo se muestra a petición, es decir, la presentación de la información detallada tiene lugar tras pulsar el botón "**Mostrar detalles**" en la ventana "*Evento de red*".

Mostrar siempre detalles

Si la opción está activada, la información detallada de la ventana "*Evento de red*" se muestra siempre.

Recordar último estado

Si la opción está activada, la presentación de información detallada se usa del mismo modo que en el evento de red anterior. Si en el último evento de red se mostró o solicitó información detallada, en el siguiente evento de red se mostrará dicha información. Si en el último evento de red no se mostró o se ocultó la información detallada, en el siguiente evento de red no se mostrará dicha información.

Permitir con privilegios

En este grupo de opciones de configuración, puede establecer el estado de la opción *Permitir con privilegios* en la ventana **Evento de red**.

Siempre activado

Si la opción está activada, la opción "*Permitir con privilegios*" en la ventana "*Evento de red*" está activada de forma predeterminada.

Siempre desactivado

Si la opción está activada, la opción "*Permitir con privilegios*" en la ventana "*Evento de red*" está desactivada de forma predeterminada.

Recordar último estado

Si la opción está activada, el estado de la opción "*Permitir con privilegios*" en la ventana "*Evento de red*" se gestiona igual que en el evento de red anterior. Si al ejecutar el último evento de red estaba activada la opción "*Permitir con privilegios*", la opción estará activada de forma predeterminada durante el siguiente evento de red. Si al ejecutar el último evento de red estaba desactivada la opción "*Permitir con privilegios*", la opción estará desactivada de forma estándar durante el siguiente evento de red.

12.5 FireWall bajo SMC

La configuración del FireWall está adaptada a las necesidades específicas de una administración a través de Avira Security Management Center. Existen opciones avanzadas y limitaciones de opciones de configuración individuales:

- La configuración del FireWall se aplica para todos los usuarios de las estaciones de trabajo
- Reglas del adaptador: Para adaptadores individuales se pueden configurar los niveles de seguridad a través de menús contextuales
- Reglas de aplicación: El acceso a red de aplicaciones puede permitirse o bloquearse. No existe la posibilidad de crear reglas de aplicación específicas.

Cuando su programa AntiVir se administra a través de Avira Security Management Center, las siguientes opciones de configuración del FireWall en el Centro de control quedan desactivadas en las estaciones de trabajo:

- Configuración de los niveles de seguridad del FireWall
- Configuración de reglas de adaptador y reglas de aplicación

12.5.1 Opciones generales

Configuración avanzada

Bloquear fichero host de Windows

Si la opción está activada, el fichero host de Windows está protegido contra escritura. Ya no es posible manipular el fichero. Por ejemplo, ningún malware podrá redirigirle a sitios Web no deseados.

Activar el modo de juego

Si la opción está activada, Avira FireWall cambia automáticamente al modo de juego cuando en el sistema se ejecuta una aplicación a pantalla completa. En el modo de juego se aplican todas las reglas definidas del adaptador y de la aplicación. Las aplicaciones para las que no se definieron reglas con las acciones "Permitir" o "Denegar" disponen de permiso temporal de acceso a la red, por lo que no se abrirán ventanas emergentes con consultas sobre eventos de red.

Desactivar firewall de Windows al iniciar

Si la opción está activada, el Firewall de Windows estará desactivado al iniciar el equipo. Esta opción está activada de forma estándar.

Activar FireWall

Con la opción activada Avira FireWall se encuentra activo y protege su equipo de los peligros procedentes de Internet y de otras redes.

Tiempo de espera excesivo de la regla

Bloquear siempre

Si la opción está activada, se conserva la regla creada automáticamente, por ejemplo, durante un escaneo de puertos.

Quitar la regla tras n segundos

Si esta opción está activada, una regla creada automáticamente, por ejemplo durante un escaneo de puertos, se elimina tras el periodo estipulado. Esta opción está activada de forma estándar.

12.5.2 Reglas generales del adaptador

Las conexiones de red configuradas se conocen como adaptadores. Se pueden definir reglas del adaptador para las siguientes conexiones de red de cliente:

- Adaptador predeterminado: LAN o Internet de alta velocidad
- Inalámbrico
- Conexión de acceso telefónico a redes

Puede ajustar reglas del adaptador predefinidas para cada adaptador disponible a través del menú contextual del adaptador:

- Nivel de seguridad Alto
- Nivel de seguridad Medio
- Nivel de seguridad Bajo

También existe la posibilidad de adaptar y personalizar reglas del adaptador individuales.

Nota

La configuración predeterminada del nivel de seguridad para todas las reglas predefinidas de Avira FireWall es **Medio**.

Protocolo ICMP

El protocolo ICMP (Internet Control Message Protocol) se utiliza para intercambiar mensajes de error e información en las redes. El protocolo también se utiliza para los mensajes de estado con ping o tracer.

Con esta regla puede definir los tipos ICMP de entrada y salida que deben ser bloqueados, los parámetros para desbordamiento y el comportamiento ante paquetes ICMP fragmentados. Esta regla sirve para evitar los ataques conocidos como de desbordamiento ICMP (ICPM Flood) que pueden conllevar una carga o sobrecarga del procesador del equipo atacado al responder a todos los paquetes.

Reglas predefinidas para el protocolo ICMP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
Bloquea tipos entrantes: sin tipo . Bloquea tipos salientes: sin tipo . Asumir desbordamiento si el retraso entre paquetes es inferior a 50ms . Rechazar paquetes ICMP fragmentados.	La misma regla que para el nivel bajo	Bloquea tipos entrantes: varios tipos . Bloquea tipos salientes: varios tipos . Asumir desbordamiento si el retraso entre paquetes es inferior a 50ms . Rechazar paquetes ICMP fragmentados.

Tipos entrantes bloqueados: sin tipo/varios tipos

Haciendo clic en el enlace se abre una lista con los tipos de paquete ICMP. En esta lista puede seleccionar los tipos de mensaje ICMP entrantes que desee bloquear.

Tipos de salida bloqueados: sin tipo/varios tipos

Haciendo clic en el enlace se abre una lista con los tipos de paquete ICMP. En esta lista puede seleccionar los tipos de mensaje ICMP salientes que desee bloquear.

Desbordamiento

Haciendo clic en el enlace se abre un cuadro de diálogo donde puede introducir el valor máximo permitido para el retardo de ICMP.

Paquetes ICMP Fragmentados

Haciendo clic en el enlace tiene la posibilidad de rechazar o no los paquetes ICMP fragmentados.

Escaneo de puertos TCP

Con esta regla se define cuándo el FireWall debe suponer que existe un escaneo de puertos TCP y cómo debe comportarse en este caso. Esta regla sirve para evitar los ataques conocidos como de escaneo de puertos TCP, que pueden detectar puertos abiertos en su equipo. Esta clase de ataque se emplea la mayoría de las veces para detectar los puntos débiles en un equipo y posteriormente lanzar ataques más serios.

Reglas predeterminadas para el escaneo de puertos TCP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
Suponer que existe escaneo de puertos TCP	Suponer que existe escaneo de puertos TCP	La misma regla que para el nivel medio.

<p>si 50 o más puertos se han escaneado en 5 000 milisegundos. Si se detecta un escaneado de puertos TCP, escribir en el fichero de informe la dirección IP del atacante y no añadir la regla para bloquear el ataque.</p>	<p>si 50 o más puertos se han escaneado en 5 000 milisegundos. Si se detecta un escaneado de puertos TCP, escribir en el fichero de informe la dirección IP del atacante y añadir la regla para bloquear el ataque.</p>
--	---

Puertos

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede indicar la cantidad de puertos que deben haberse escaneado para suponer que se trata de un escaneado de puertos TCP.

Ventana de tiempo de escaneado de puertos

Al hacer clic en el enlace aparece un cuadro de diálogo donde puede introducir el intervalo de tiempo en el que debe haberse escaneado un determinado número de puertos para suponer que se trata de un escaneo de puertos TCP.

Fichero de informe

Al hacer clic en el enlace puede hacer que se registre o no la IP del atacante.

Regla

Al hacer clic en el enlace tiene la opción de decidir si se añadirá o no la regla de bloqueo de ataques por escaneo de puertos TCP.

Escaneado de puertos UDP

Con esta regla se define cuándo el FireWall debe suponer que existe escaneado de puertos UDP y cómo debe comportarse en este caso. Esta regla sirve para evitar los ataques conocidos como de escaneado de puertos UDP, que pueden detectar puertos abiertos en su equipo. Esta clase de ataque se emplea la mayoría de las veces para detectar los puntos débiles en un equipo y posteriormente lanzar ataques más serios.

Reglas predeterminadas para el escaneado de puertos UDP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
<p>Suponer que existe escaneado de puertos UDP si 50 o más puertos se han escaneado en 5 000 milisegundos. Si se detecta un escaneado de puertos UDP, escribir en el fichero de informe la dirección IP del atacante y no añadir la regla para bloquear el ataque.</p>	<p>Suponer que existe escaneado de puertos UDP si 50 o más puertos se han escaneado en 5 000 milisegundos. Si se detecta un escaneado de puertos TCP, escribir en el fichero de informe la dirección IP del atacante y añadir la regla para bloquear el ataque.</p>	<p>La misma regla que para el nivel medio.</p>

Puertos

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede indicar la cantidad de puertos que deben haberse escaneado para suponer que se trata de un escaneo de puertos UDP.

Ventana de tiempo de escaneo de puertos

Al hacer clic en el enlace aparece un cuadro de diálogo donde puede introducir el intervalo de tiempo en el que debe haberse escaneado un determinado número de puertos para suponer que se trata de un escaneo de puertos UDP.

Fichero de informe

Al hacer clic en el enlace puede hacer que se registre o no la IP del atacante.

Regla

Al hacer clic en el enlace tiene la opción de decidir si se añadirá o no la regla de bloqueo de ataques por escaneo de puertos UDP.

12.5.2.1. Reglas de Entrada

Las reglas de entrada sirven para controlar el tráfico de datos entrante por medio de Avira FireWall.

Nota

Cuando se filtra un paquete las reglas correspondientes se aplican sucesivamente, por lo que el orden es muy importante. Cambie el orden de las reglas únicamente cuando tenga la completa seguridad de lo que está haciendo.

Reglas predeterminadas para monitorizar el tráfico de datos TCP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
Avira FireWall no bloquea el tráfico de datos entrante.	<ul style="list-style-type: none"> – Permitir conexión TCP establecida en puerto 135 <p>Permitir paquetes TCP desde la dirección 0.0.0.0 con la máscara 0.0.0.0 si el puerto local se encuentra en {135} y el puerto remoto en {0-65535}. Aplicar para paquetes en las conexiones existentes. No escribir en el fichero de informe cuando el paquete</p>	<ul style="list-style-type: none"> – Monitorizar tráfico de datos TCP admitido <p>Permitir paquetes TCP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar para paquetes en las conexiones existentes. No escribir en el fichero de informe cuando el paquete cumple la regla.</p>

	<p>cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p> <p>– Denegar paquetes TCP en el puerto 135</p> <p>Denegar paquetes TCP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {135} y el puerto remoto en {0-65535} . Aplicar para todos los paquetes. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Denegar paquetes con los siguientes bytes <vacío> con máscara <vacío> en el desplazamiento 0.</p> <p>– Monitorizar el tráfico de datos conforme a TCP</p> <p>Permitir paquetes TCP de la dirección</p>	<p>Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p>
--	---	---

	<p>0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar al inicio del establecimiento de la conexión y a paquetes de conexiones existentes. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p> <p>– Denegar todos los paquetes TCP</p> <p>Denegar paquetes TCP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar para todos los paquetes. No escribir en el fichero de informe cuando el paquete cumple la regla.</p>	
--	---	--

	Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0 .	
--	--	--

Aceptar / denegar paquetes TCP

Haciendo clic en este enlace tiene la opción de decidir si desea permitir o denegar paquetes TCP especialmente definidos.

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Puertos locales

Al hacer clic en este enlace aparece un cuadro de diálogo en el que puede definir el número de puerto(s) local(es) o rango(s).

Puertos remotos

Al hacer clic en este enlace aparece un cuadro de diálogo en el que puede definir el número de puerto(s) local(es) o rango(s) remoto(s).

Método de aplicación

Al hacer clic en este enlace puede decidir si la regla se aplicará en el inicio de las conexiones y en las existente o sólo para las conexiones existentes o para todos los paquetes.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

La opción **Características avanzadas** permite el filtrado basándose en el contenido. Por ejemplo, pueden rechazarse los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico

Filtrado por contenido: máscara

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del filtrado según el contenido. El desplazamiento se calcula desde donde termina el encabezamiento TCP.

Reglas predeterminadas para monitorizar el tráfico de datos UDP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
-	<p>– Monitorizar el tráfico de datos conforme a UDP</p> <p>Permitir paquetes UDP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar la regla a puertos abiertos. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p> <p>– Denegar todos los paquetes UDP</p> <p>Denegar paquetes UDP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {0-65535}. Aplicar a todos los puertos.</p>	<p>Monitorizar tráfico de datos UDP admitido</p> <p>Permitir paquetes UDP de la dirección 0.0.0.0 con máscara 0.0.0.0 si el puerto local se encuentra en {0-65535} y el puerto remoto en {53, 67, 68, 123}. Aplicar la regla a puertos abiertos. No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p>

	<p>No escribir en el fichero de informe cuando el paquete cumple la regla. Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p>	
--	--	--

Aceptar / denegar paquetes UDP

Haciendo clic en este enlace tiene la opción de decidir si desea permitir o denegar paquetes UDP especialmente definidos.

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Puertos locales

Al hacer clic en este enlace aparece un cuadro de diálogo en el que puede definir el número de puerto(s) local(es) o rango(s).

Puertos remotos

Al hacer clic en este enlace aparece un cuadro de diálogo en el que puede definir el número de puerto(s) local(es) o rango(s) remoto(s).

Método de aplicación

Al hacer clic en este enlace puede elegir la aplicación de esta regla a todos los puertos o sólo a los abiertos.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

La opción **Características avanzadas** permite el filtrado basándose en el contenido. Por ejemplo, pueden rechazarse los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico

Filtrado por contenido: máscara

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del filtrado según el contenido. El desplazamiento se calcula desde donde termina el encabezamiento UDP.

Reglas predeterminadas para monitorizar el tráfico de datos ICMP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
-	<ul style="list-style-type: none"> No descartar paquetes ICMP sobre la base de la dirección IP <p>Permitir paquetes ICMP de la dirección 0.0.0.0 con máscara 0.0.0.0.</p> <p>No escribir en el fichero de informe cuando el paquete cumple la regla.</p> <p>Avanzado: Descartar paquetes que tengan los siguientes bytes <vacío> con la máscara <vacío> con desplazamiento 0.</p>	La misma regla que para el nivel medio.

Aceptar / denegar paquetes ICMP

Haciendo clic en este enlace tiene la opción de decidir si desea permitir o denegar paquetes ICMP especialmente definidos.

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

La opción **Características avanzadas** permite el filtrado basándose en el contenido. Por ejemplo, pueden rechazarse los paquetes que contienen datos específicos con un determinado desplazamiento. Si no desea utilizar esta opción no seleccione ningún fichero o seleccione un fichero vacío.

Filtrado por contenido: datos

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar el fichero que contiene el buffer específico

Filtrado por contenido: máscara

Al hacer clic en el enlace, aparece el cuadro de diálogo en el que puede seleccionar la máscara específica.

Filtrado por contenido: desplazamiento

Haciendo clic en el enlace se abre un cuadro de diálogo en el que puede seleccionar el desplazamiento del filtrado según el contenido. El desplazamiento se calcula desde donde termina el encabezamiento ICMP.

Reglas predeterminadas para los paquetes IP

Configuración: Bajo	Configuración: Medio	Configuración: Alto
-	-	Denegar todos los paquetes IP Denegar paquetes IP de la dirección 0.0.0.0 con máscara 0.0.0.0 . No escribir en el fichero de informe cuando el paquete cumple la regla.

Aceptar / denegar paquetes TCP

Al hacer clic en el enlace puede decidir si permitir o denegar los paquetes IP entrantes definidos especialmente

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

Reglas posibles para la monitorización de paquetes IP basándose en protocolos IP

Paquetes IP

Al hacer clic en el enlace puede decidir si permitir o denegar los paquetes IP entrantes definidos especialmente

Dirección IP

Al hacer clic en el enlace aparece un cuadro de diálogo en el que puede definir la IP deseada.

Máscara IP

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir la máscara IP requerida.

Protocolo

Al hacer clic en este enlace, aparece un cuadro de diálogo en el que puede introducir el protocolo IP requerido.

Fichero de informe

Al hacer clic en este enlace puede decidir si se debe generar un fichero de informe cuando el paquete cumple con la regla.

12.5.2.2. Reglas de salida

Las reglas de salida se definen para controlar el tráfico de datos saliente a través de Avira FireWall. Puede definir una regla saliente para los siguientes protocolos: IP, ICMP, UDP y TCP.

Nota

Cuando se filtra un paquete las reglas correspondientes se aplican sucesivamente, por lo que el orden es muy importante. Cambie el orden de las reglas únicamente cuando tenga la completa seguridad de lo que está haciendo.

Botones

Botón	Descripción
Añadir	Permite crear una nueva regla. Pulsando este botón aparece el cuadro de diálogo " Añadir nueva regla ". En este cuadro de diálogo puede seleccionar nuevas reglas.
Quitar	Elimina la regla seleccionada.
Bajar	Mueve la regla seleccionada una línea hacia abajo, es decir reduce la prioridad de la regla.
Subir	La regla seleccionada se desplaza una posición hacia arriba, por lo que aumenta su prioridad.
Cambiar el nombre	Permite renombrar la regla seleccionada.

Nota

Puede añadir nuevas reglas para cada adaptador o para todos los adaptadores del equipo. Para añadir una regla de adaptador para todos los adaptadores, seleccione **Equipo** en la estructura del adaptador que se muestra y haga clic en el botón **Añadir**.

Nota

Para cambiar la posición de una regla, también puede arrastrarla con el ratón a la posición pertinente.

12.5.3 Lista de aplicaciones

Bajo lista de aplicaciones puede crear reglas para los accesos de red de aplicaciones. Puede añadir aplicaciones a la lista y establecer mediante un menú contextual las reglas *Permitir* y **Bloquear** para la aplicación seleccionada:

- Los accesos de red de aplicaciones con la regla *Permitir* se permiten.
- Los accesos de red de aplicaciones con la regla *Bloquear* se rechazan.

Al añadir aplicaciones, se establece la regla *Permitir*.

Lista de Aplicaciones

Esta tabla muestra la lista de aplicaciones para las que se han definido reglas. Los símbolos indican si los accesos de red de las aplicaciones están permitidos o bloqueados. Puede modificar las reglas de las aplicaciones a través de un menú contextual.

Botones

Botón	Descripción
Añadir mediante ruta	El botón abre un cuadro de diálogo en el que puede seleccionar aplicaciones. La aplicación se añade a la lista de aplicaciones con la regla " Permitir acceso a red ". Si utiliza la opción " Añadir mediante ruta ", la aplicación agregada es identificada por el cortafuegos FireWall a través de la ruta y el nombre de archivo. Las reglas para una aplicación conservan su validez y son aplicadas por FireWall, incluso aunque el contenido de un fichero ejecutable incorporado haya sido modificado, por ejemplo, por medio de una actualización.
Añadir mediante md5	El botón abre un cuadro de diálogo en el que puede seleccionar aplicaciones. La aplicación se añade a la lista de aplicaciones con la regla " Permitir acceso a red ". Si utiliza la opción " Añadir mediante md5 ", todas las aplicaciones agregadas se identifican inequívocamente mediante la suma de comprobación MD5. Esto permite que FireWall detecte cambios en los contenidos del fichero. Si se modifica una aplicación, por ejemplo debido a una actualización, la aplicación con la regla establecida se borra automáticamente de la lista de aplicaciones. La aplicación deberá añadirse nuevamente a la lista después de la modificación y la regla deseada deberá establecerse de nuevo.
Añadir grupo	El botón abre un cuadro de diálogo en el que puede seleccionar un directorio. Todas las aplicaciones bajo la ruta seleccionada se añaden a la lista de aplicaciones con la regla " Permitir acceso a red ".
Quitar	La regla de aplicación seleccionada se elimina.
Eliminar todas	Se eliminan todas las reglas de aplicación.

12.5.4 Proveedores de confianza

En *Proveedores de confianza* se muestra una lista de productores de software de confianza. Se permiten los accesos de red de aplicaciones de los productores de software contenidos en la lista. Pueden quitar o añadir productores a la lista.

Proveedores

La lista muestra todos los proveedores clasificados como de confianza.

Botones

Botón	Descripción
Añadir	El botón abre un cuadro de diálogo en el que puede seleccionar aplicaciones. Se determina el productor de la aplicación y se añade a la lista de proveedores de confianza.
Añadir grupo	El botón abre un cuadro de diálogo en el que puede seleccionar un directorio. Se determinan los productores de todas las aplicaciones en la ruta seleccionada y se añaden a la lista de proveedores de confianza.
Quitar	La entrada seleccionada se quita de la lista de proveedores de confianza. Para quitar el proveedor seleccionado definitivamente de la lista, pulse " Aplicar " o " Aceptar " en la ventana de configuración.
Eliminar todas	Se eliminan todas las entradas de la lista de proveedores de confianza.
Volver a cargar	Se deshacen los cambios realizados. Se carga la última lista guardada.

Nota

Si quita proveedores de la lista y, a continuación, pulsa el botón **Aplicar**, los proveedores se eliminan definitivamente de la lista. El cambio no se puede deshacer con *Volver a cargar*.

Nota

El FireWall da prioridad a las reglas de aplicación frente a las entradas de la lista de proveedores de confianza: si creó una regla de aplicación y el proveedor de la aplicación consta en la lista de proveedores de confianza, la regla de aplicación se ejecuta.

12.5.5 Configuración adicional

Notificaciones

En Notificaciones se determina para qué eventos desea recibir una notificación del FireWall en el escritorio.

Escaneado de puertos

Si la opción está activada, recibirá una notificación en el escritorio cuando el FireWall detecte un escaneado de puertos.

Desbordamiento

Si la opción está activada, recibirá una notificación en el escritorio cuando el FireWall detecte un ataque por desbordamiento.

Aplicaciones bloqueadas

Si la opción está activada, recibirá una notificación en el escritorio cuando el FireWall deniegue la actividad de red de una aplicación, es decir, la bloquee.

IP bloqueada

Si la opción está activada, recibirá una notificación en el escritorio cuando el FireWall deniegue el tráfico de datos de una dirección IP.

Configuración de ventanas emergentes

Comprobar el bloqueo de inicio del proceso

Si la opción está activada, tiene lugar un análisis más preciso de la pila de procesos. El FireWall parte de la base de que cualquier proceso de la pila que no sea de confianza es el proceso a través de cuyo proceso secundario se accede a la red. Por ello, en este caso se abre una ventana emergente propia para cada proceso que no sea de confianza en la pila de procesos. Esta opción está desactivada de forma estándar.

Mostrar varios cuadros de diálogo por proceso

Si esta opción está activada, cada vez que una aplicación intenta establecer una conexión de red, se abre una ventana emergente. Otra opción es que la información sólo aparezca en el primer intento de conexión. Esta opción está desactivada de forma estándar.

Cancelar automáticamente ventana emergente en modo de juego

Si la opción está activada, Avira FireWall cambia automáticamente al modo de juego cuando en el sistema se ejecuta una aplicación a pantalla completa. En el modo de juego se aplican todas las reglas definidas del adaptador y de la aplicación. Las aplicaciones para las que no se definieron reglas con las acciones "Permitir" o "Denegar" disponen de permiso temporal de acceso a la red, por lo que no se abrirán ventanas emergentes con consultas sobre el evento de red.

12.5.6 Configuración de visualización

Guardar acción para esta aplicación

Siempre activado

Si la opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" estará activada de forma predeterminada. Esta opción está activada de forma estándar.

Siempre desactivado

Si la opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" estará desactivada de forma predeterminada.

Permitir aplicaciones firmadas

Si la opción está activada, cuando las aplicaciones firmadas de determinados productores acceden a la red, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" está activada automáticamente. Los productores son: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Recordar último estado

Si la opción está activada, la opción "**Guardar acción para esta aplicación**" del cuadro de diálogo "**Evento de red**" se usa del mismo modo que con el último evento de red. Si en el último evento de red se activó la opción "**Guardar acción para esta aplicación**", la opción estará activa en el siguiente evento de red. Si en el último evento de red se desactivó la opción "**Guardar acción para esta aplicación**", la opción estará desactivada en el siguiente evento de red.

Mostrar detalles

En este grupo de opciones de configuración puede configurar la presentación de información detallada en la ventana **Evento de red**.

Mostrar detalles a petición

Si la opción está activada, la información detallada de la ventana "*Evento de red*" sólo se muestra a petición, es decir, la presentación de la información detallada tiene lugar tras pulsar el botón "**Mostrar detalles**" en la ventana "*Evento de red*".

Mostrar siempre detalles

Si la opción está activada, la información detallada de la ventana "*Evento de red*" se muestra siempre.

Recordar último estado

Si la opción está activada, la presentación de información detallada se usa del mismo modo que en el evento de red anterior. Si en el último evento de red se mostró o solicitó información detallada, en el siguiente evento de red se mostrará dicha información. Si en el último evento de red no se mostró o se ocultó la información detallada, en el siguiente evento de red no se mostrará dicha información.

Permitir con privilegios

En este grupo de opciones de configuración, puede establecer el estado de la opción *Permitir con privilegios* en la ventana **Evento de red**.

Siempre activado

Si la opción está activada, la opción "*Permitir con privilegios*" en la ventana "*Evento de red*" está activada de forma predeterminada.

Siempre desactivado

Si la opción está activada, la opción "*Permitir con privilegios*" en la ventana "*Evento de red*" está desactivada de forma predeterminada.

Recordar último estado

Si la opción está activada, el estado de la opción "*Permitir con privilegios*" en la ventana "*Evento de red*" se gestiona igual que en el evento de red anterior. Si al ejecutar el último evento de red estaba activada la opción *Permitir con privilegios*, la opción estará activada de forma estándar durante el siguiente evento de red. Si al ejecutar el último evento de red estaba desactivada la opción *Permitir con privilegios*, la opción estará desactivada de forma estándar durante el siguiente evento de red.

12.6 WebGuard

La sección WebGuard se utiliza para la configuración del WebGuard.

12.6.1 Análisis

Con el WebGuard puede protegerse frente a virus y malware que acceden a su sistema a través de las páginas Web que se cargan desde Internet en el explorador Web. En la sección *Análisis* puede configurar el comportamiento de WebGuard.

Análisis

Activar WebGuard

Si está activada la opción, las páginas Web que se solicitan a través del explorador de Internet se analizan en cuanto a virus y malware. El WebGuard supervisa los datos de Internet transmitidos con el protocolo HTTP en los puertos 80, 8080 y 3128. En caso de detectar páginas Web afectadas, se bloquea su carga. Si la opción está desactivada, el servicio WebGuard sigue ejecutándose pero el análisis de virus y malware se desactiva.

Protección sobre la marcha

Con la protección sobre la marcha dispone de la posibilidad de realizar configuraciones para bloquear I-Frames, también denominados marcos incorporados. I-Frames son elementos HTML, es decir elementos de páginas de Internet que limitan un área de una página Web. Los I-Frames permiten cargar y mostrar otros contenidos Web (normalmente, otras direcciones URL) como documentos independientes en una subventana del explorador. La mayoría de las veces los I-Frames se usan para banners, un formato publicitario en Internet. En algunos casos los I-Frames sirven para ocultar malware, es decir, software malintencionado. El área del I-Frame es, en esos casos, apenas visible en el explorador. La opción *Bloquear I-Frames sospechosos* permite controlar y bloquear la carga de I-Frames sospechosos.

Bloquear I-Frames sospechosos

Si la opción está activada, los I-Frames de las páginas Web solicitadas se analizan según determinados criterios. En caso de que existan I-Frames sospechosos en una página Web solicitada, éstos se bloquean. En la ventana del I-Frame aparece un mensaje de error.

Predeterminado

Si está activada esta opción, se bloquean los I-Frames de contenido sospechoso.

Ampliado

Con esta opción activada, los I-Frames de contenido sospechoso y los que se usan de forma sospechosa se bloquean. Se habla de uso sospechoso de I-Frames si el I-Frame es muy pequeño por lo que apenas o ni tan siquiera se ve, o si el I-Frame está colocado en una posición poco habitual en la página Web.

12.6.1.1. Acción en caso de detección

Acción en caso de detección

Puede definir las acciones que tomar el WebGuard cuando se detecta un virus o programa no deseado.

Interactiva

Con esta opción activada, durante un análisis directo aparece una ventana con opciones sobre qué hacer con el fichero concerniente. Este ajuste está activado de forma estándar.

Acciones permitidas

En este cuadro puede especificar aquellas acciones que van a mostrarse en el cuadro de diálogo en el caso de que se descubra un virus o programa no deseado. Para ello, debe activar las opciones correspondientes.

denegar acceso

El sitio Web requerido por el servidor Web y los datos solicitados no son transferidos a su navegador. Un error sobre acceso denegado ha sido mostrado en su navegador Web. El WebGuard registra la detección en el fichero de informe si está activada la función de informe.

Cuarentena

En el caso de una detección, la página Web solicitada por el servidor Web y/o los datos transferidos se mueven a la cuarentena. Desde el gestor de cuarentena puede volver a restaurar el fichero afectado si éste tiene valor informativo o, si fuera necesario, puede enviarlo al Avira Malware Research Center.

omitir

La página Web solicitada por el servidor Web o los datos y archivos transmitidos son pasados por el WebGuard a su navegador.

Predeterminado

Este botón le permite seleccionar la acción que será activada de forma estándar en el cuadro de diálogo que aparece al detectar un virus. Seleccione la acción que debe estar activada de forma estándar y haga clic en el botón "Predeterminado".

Encontrará más información aquí.

Mostrar barra de progreso

Si la opción está activada, aparece una notificación en el escritorio con una barra de progreso de la descarga cuando una descarga o la descarga de contenidos de páginas Web supera un tiempo de espera de 20 segundos. Esta notificación en el escritorio sirve especialmente de control al descargar páginas Web con gran volumen de datos: al navegar con el WebGuard los contenidos de las páginas Web en el explorador de Internet no se cargan sucesivamente, ya que antes de presentarlos en el explorador de Internet se analizan acerca de la existencia de virus y malware. Esta opción está desactivada de forma estándar.

Automático

Si esta opción está activada, entonces no mostrará la ventana de acciones después de una detección de un virus o programa no deseado. El WebGuard reacciona de acuerdo a lo que configure en esta sección.

Mostrar mensajes de advertencia

Con esta opción activada, al detectar un virus o un programa no deseado aparece un mensaje de advertencia indicando las acciones que se ejecutarán.

Acción Primaria

La acción principal es la que se ejecuta cuando el WebGuard detecta un virus o programa no deseado.

Denegar acceso

El sitio Web requerido por el servidor Web y los datos solicitados no son transferidos a su navegador. Un error sobre acceso denegado ha sido mostrado en su navegador Web. El WebGuard registra la detección en el fichero de informe si está activada la función de informe.

aislar

En el caso de una detección, la página Web solicitada por el servidor Web y/o los datos transferidos se mueven a la cuarentena. Desde el gestor de cuarentena puede volver a restaurar el fichero afectado si éste tiene valor informativo o, si fuera necesario, puede enviarlo al Avira Malware Research Center.

omitir

La página Web solicitada por el servidor Web o los datos y archivos transmitidos son pasados por el WebGuard a su navegador. Con esta opción seleccionada se permite el acceso al fichero y se deja tal cual está.

Advertencia

¡El fichero afectado sigue activo en el equipo! ¡Podría causar daños graves a su sistema!

12.6.1.2. Accesos bloqueados

En **Accesos bloqueados** puede indicar los tipos de ficheros y tipos MIME (tipos de contenidos de los datos transmitidos) que debe bloquear el WebGuard. Con el filtro Web puede bloquear direcciones URL conocidas no deseadas, p. ej., URL de suplantación de identidad (phishing) y de software malintencionado (malware). El WebGuard impide la transmisión de datos de Internet a su sistema informático.

Tipos de fichero y tipos MIME (definidos por el usuario) bloqueados por el WebGuard

El WebGuard bloquea todos los tipos de ficheros y tipos MIME (tipos de contenidos de los datos transmitidos) de la lista.

Campo de entrada

En este campo se introducen los nombres de los tipos MIME y tipos de ficheros que debe bloquear el WebGuard. Para los tipos de fichero, debe indicar la extensión de fichero, p. ej. **.htm**. Para los tipos MIME, se indica el tipo de medio y, si es necesario, el subtipo. Ambas indicaciones se separan mediante una barra inclinada simple, p. ej., **video/mpeg** o **audio/x-wav**.

Nota

Los ficheros ya guardados en su sistema informático como ficheros temporales de Internet quedan bloqueados por el WebGuard, pero el explorador de Internet local puede descargarlos de su equipo. Los ficheros temporales de Internet son ficheros que guarda el explorador de Internet en el equipo para poder mostrar las páginas Web con mayor rapidez.

Nota

La lista de los tipos de fichero y tipos MIME que se deben bloquear se omite en caso de existir entradas en la lista de tipos de fichero y tipos MIME que se excluirán en WebGuard::Análisis::Excepciones.

Nota

Cuando indique los tipos de fichero y tipos MIME, no puede utilizar comodines (comodín * para tantos caracteres como desee o comodín ? para un único carácter).

Tipos MIME: ejemplos de tipos de medio:

- text = para ficheros de texto
- image = para ficheros de imagen
- video = para ficheros de vídeo
- audio = para ficheros de sonido

- `application` = para ficheros vinculados a un determinado programa

Ejemplos: tipos de fichero y tipos MIME excluidos

- `application/octet-stream` = el WebGuard bloquea ficheros del tipo MIME `application/octet-stream` (ficheros ejecutables `*.bin`, `*.exe`, `*.com`, `*dll`, `*.class`).
- `application/olescript` = el WebGuard bloquea ficheros del tipo MIME `application/olescript` (ficheros de script ActiveX `*.axs`).
- `.exe` = el WebGuard bloquea todos los ficheros con la extensión de fichero `.exe` (ficheros ejecutables).
- `.msi` = el WebGuard bloquea todos los ficheros con la extensión de fichero `.msi` (ficheros de Windows Installer).

Añadir

Este botón permite incluir en la ventana de visualización el tipo MIME o tipo de fichero introducido en el campo de introducción.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

Filtro Web

El filtro Web dispone de una base de datos interna, que se actualiza a diario, en la que se clasifican las URL por criterios de contenido.

Activar filtro Web

Si está activada esta opción se bloquean todas las direcciones URL pertenecientes a las categorías seleccionadas en la lista de filtros Web.

Lista de filtros Web

En la lista de filtros Web puede seleccionar las categorías de contenido cuyas URL debe bloquear el WebGuard.

Nota

El filtro Web se omite en caso de existir entradas en la lista de direcciones URL omitidas en WebGuard::Análisis::Excepciones.

Nota

Se consideran direcciones URL de spam o correo no solicitado las URL que se propagan con emails de correo no solicitado. La categoría de fraudes y engaños incluye páginas Web con 'trampas de suscripción y otras ofertas de servicios, cuyos costes oculta el proveedor.

12.6.1.3. Excepciones

Estas opciones permiten excluir tipos MIME (tipos de contenidos de los datos transmitidos) y tipos de ficheros para URL (direcciones de Internet) del análisis del WebGuard. El WebGuard omite los tipos MIME y las URL indicadas, es decir, estos datos no se analizan en cuanto a virus y malware al transmitirse a su equipo.

Tipos MIME omitidos por WebGuard

En este campo puede seleccionar los tipos MIME que serán ignorados por el WebGuard durante el análisis.

Tipos de fichero y tipos MIME (definidos por el usuario) omitidos por WebGuard

Todos los tipos de fichero y MIME (tipos de contenido de los datos transmitidos) de la lista serán ignorados por el WebGuard durante el análisis.

Campo de entrada

En este campo puede escribir los tipos MIME y tipos de fichero que serán ignorados por el WebGuard durante el análisis. Para los tipos de fichero, debe indicar la extensión de fichero, p. ej. **.htm**. Para los tipos MIME, se indica el tipo de medio y, si es necesario, el subtipo. Ambas indicaciones se separan mediante una barra inclinada simple, p. ej., **video/mpeg** o **audio/x-wav**.

Nota

Cuando indique los tipos de fichero y tipos MIME, no puede utilizar comodines (comodín * para tantos caracteres como desee o comodín ? para un único carácter).

Advertencia

Todos los tipos de fichero y tipos de contenido de la lista de exclusión se cargan en el explorador de Internet sin más análisis de los accesos bloqueados (lista de los tipos de fichero y tipos MIME que se bloquearán en WebGuard::Análisis::Accesos bloqueados) o del WebGuard: en todas las entradas de la lista de exclusiones se omiten las entradas de la lista de los tipos de fichero y tipos MIME que se bloquearán. No se ejecuta análisis alguno de virus y malware.

Tipos MIME: ejemplos de tipos de medio:

- text = para ficheros de texto
- image = para ficheros de imagen
- video = para ficheros de vídeo
- audio = para ficheros de sonido
- application = para ficheros vinculados a un determinado programa

Ejemplos: Tipos de fichero y tipos MIME que se omitirán

- audio/ = todos los ficheros del tipo audio se excluyen del análisis del WebGuard
- video/quicktime = todos los ficheros de vídeo del subtipo Quicktime (*.qt, *.mov) se excluyen del análisis del WebGuard
- .pdf = todos los ficheros PDF de Adobe quedan excluidos del análisis del WebGuard.

Añadir

Este botón permite incluir en la ventana de visualización el tipo MIME o tipo de fichero introducido en el campo de introducción.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

Direcciones URL omitidas por WebGuard

Todas las URL que constan en esta lista se excluyen del análisis del WebGuard.

Campo de entrada

En este campo se indican las URL (direcciones de Internet) que deben excluirse del análisis del WebGuard, p. ej., **www.nombrededominio.com**. Puede introducir partes de la URL, identificando con puntos al principio o al final el nivel de dominio: .nombrededominio.es para todas las páginas y todos los subdominios del dominio. Para escribir una página Web con cualquier dominio de nivel superior (.com o .net) debe indicarlo con un punto final: **nombrededominio.** Si escribe una secuencia de caracteres sin punto inicial o final, dicha secuencia se interpreta como dominio de nivel superior, p. ej., **net** para todos los dominios NET (www.dominio.net).

Nota

Cuando indique las direcciones URL, también puede usar el carácter comodín * para tantos caracteres como desee. Combine los comodines con puntos finales o iniciales para identificar los niveles de dominio:

.nombrededominio.*

*.nombrededominio.com

.*nombre*.com (es válido pero no se recomienda)

Las indicaciones sin puntos, como *nombre* se interpretan como parte de un dominio de nivel superior y no son útiles.

Advertencia

Todas las páginas Web de la lista de URL omitidas se cargan en el explorador de Internet sin más análisis por parte del filtro Web o del WebGuard: para todas las entradas de la lista de URL omitidas se pasan por alto las entradas del filtro Web (consulte WebGuard::Análisis::Accesos bloqueados). No se ejecuta análisis alguno de virus y malware. Por lo tanto, únicamente excluya direcciones URL de confianza del análisis del WebGuard.

Añadir

Este botón permite incluir en la ventana de visualización la URL (dirección de Internet) introducida en el campo de introducción.

Eliminar

Este botón elimina una entrada seleccionada en la lista. El botón está inactivo si no hay ninguna entrada seleccionada.

Ejemplos: URL omitidas

- www.avira.com -O BIEN- www.avira.com/*

= todas las URL con el dominio 'www.avira.com' se excluyen del análisis del WebGuard: www.avira.com/es/pages/index.php, www.avira.com/es/support/index.html, www.avira.com/es/download/index.html,.. Las URL con el dominio www.avira.es no se excluyen del análisis del WebGuard.

- avira.com -O BIEN- *.avira.com

= todas las URL con el dominio de segundo nivel y el dominio de nivel superior 'avira.com' se excluyen del análisis del WebGuard. La indicación incluye todos los subdominios existentes para '.avira.com': www.avira.com, forum.avira.com,...

- avira. -O BIEN- *.avira.*

= todas las URL con el dominio de segundo nivel 'avira' se excluyen del análisis del WebGuard. La indicación incluye todos los dominios de nivel superior o subdominios existentes para '.avira.': www.avira.com, www.avira.es, forum.avira.com,...

- .*dominio*.*

Todas las URL que contienen un dominio de segundo nivel con la cadena de caracteres 'dominio' se excluyen del análisis del WebGuard: www.dominio.com, www.nuevo-dominio.es, www.ejemplo-dominio1.es, ...

- net -O BIEN- *.net

= todas las URL con el dominio de nivel superior 'net' se excluyen del análisis del WebGuard: www.nombre1.net, www.nombre2.net,...

Advertencia

Indique con tanta precisión como sea posible las URL que desea excluir del análisis del WebGuard. Evite indicar dominios de nivel superior completos o partes de un nombre de dominio de segundo nivel, ya que existe el riesgo de que las páginas de Internet que propagan malware y programas no deseados queden excluidas del análisis del WebGuard debido a especificaciones demasiado globales. Se recomienda indicar por lo menos el dominio de segundo nivel completo y el dominio de nivel superior: nombrededominio.com

12.6.1.4. Heurística

Esta sección de configuración contiene los parámetros para la heurística del motor de análisis.

Los productos AntiVir disponen de unas heurísticas muy eficaces que permiten detectar malware desconocido de forma proactiva, es decir, antes de que se haya creado una firma de virus específica para ese software malintencionado y se haya enviado la correspondiente actualización del antivirus. La detección de virus se lleva a cabo mediante un minucioso análisis del código en cuestión para encontrar funciones típicas del malware. Si el código analizado se comporta de forma similar, se reporta como sospechoso. Sin embargo, ese código no es necesariamente malware; también pueden producirse falsas alarmas. El usuario debe decidir que hacer con el código encontrado, por ejemplo, basándose en su conocimiento o experiencia previa, puede decidir si la fuente que contiene el código es de confianza.

Heurística de macrovirus

Heurística de macrovirus

Su producto AntiVir incluye una potente herramienta de heurística para macrovirus. Con esta opción activada, se eliminan todas las macros en el caso de una reparación del documento afectado. Otra opción es que sólo se notifique la existencia de documentos sospechosos, es decir, se reciba una advertencia. Este ajuste está activado de forma estándar y es el recomendado.

Análisis heurístico y detección avanzados (AHeAD)

Activar AHeAD

Su programa AntiVir dispone de la tecnología AntiVir AHeAD, de una heurística muy eficaz que incluso detecta malware desconocido (nuevo). Si esta opción está activada, puede definir el nivel de "tolerancia" de la heurística. Este ajuste está activado de forma estándar.

Nivel de detección bajo

Si está activada la opción, detecta algo menos de malware desconocido; el riesgo de detecciones erróneas o falsas alarmas es en este caso reducido.

Nivel de detección medio

Esta configuración está activa por defecto si ha seleccionado el uso de esta heurística.

Nivel de detección alto

Si está activada la opción, se detecta bastante más malware desconocido pero hay que contar con falsas alarmas.

12.6.2 Informe

El WebGuard incluye una completa función de registro que puede ayudar al administrador en la identificación de una detección.

Protocolización

En este grupo se determina el volumen de contenido del fichero de informe.

Desactivado

Con esta opción activada, el WebGuard no crea ningún protocolo.

Desactive la protocolización sólo en casos excepcionales, p. ej. sólo cuando realice una prueba con muchos virus o programas no deseados.

Predeterminado

Con esta opción activada, el WebGuard registra información importante (detecciones, alertas y errores) en el fichero de informe, obviando información secundaria para ganar en claridad. Este ajuste está activado de forma estándar.

Ampliado

Con esta opción activada, el WebGuard registra también información secundaria.

Completo

Si la opción está activada, el WebGuard registra toda la información en el fichero de informe, incluso la correspondiente al tamaño de fichero, tipo de fichero, fecha, etc.

Limitar fichero de informe

Limitar tamaño a n MB

Si la opción está activada, el fichero de registro se puede limitar a un determinado tamaño; posibles valores: 1 a 100 MB. En la limitación del fichero de informe se concede un margen de unos 50 kilobytes para mantener reducida la carga del equipo. Si el tamaño del fichero de informe supera la magnitud indicada en 50 kilobytes, se eliminan automáticamente tantas entradas antiguas como sea necesario para alcanzar la magnitud indicada menos un 20% .

Guardar fichero de informe antes de reducir

Si está activada esta opción, se hace una copia del fichero de informe antes de reducirlo. Ubicación de copia de seguridad, ver Configuración :: General :: Directorios :: Carpeta de Informes.

Escribir configuración en fichero de informe

Al activar esta opción, la configuración del análisis directo se guarda en el fichero de informe.

Nota

Si no ha indicado ninguna limitación del fichero de informe, se borrarán de forma automática las entradas más antiguas cuando el fichero de informe haya alcanzado un tamaño de 100 MB. Se borrarán las entradas suficientes hasta que el fichero de informe alcance un tamaño de 80 MB.

12.7 Actualización

En la sección *Actualización* se configura la ejecución automática de actualizaciones y la conexión a los servidores de descarga. Se pueden configurar distintos intervalos de actualización y activar y desactivar la actualización automática.

Nota

Cuando configura su programa AntiVir en AntiVir Security Management Center, la configuración de las actualizaciones automáticas no está disponible.

Actualización automática

Activar

Si esta opción está activada, se ejecutan actualizaciones automáticas en el intervalo de tiempo indicado y para los eventos activados.

Actualización automática cada n días / horas / minutos

En este campo se puede indicar el intervalo con el que deberán ejecutarse las actualizaciones automáticas. Para modificar el intervalo de actualización, seleccionar una de las entradas de datos en el campo y cambiarla mediante los botones de flecha a la derecha del campo de introducción.

Iniciar tarea adicionalmente al conectarse a Internet (acceso telefónico a redes)

Si esta opción está activada, adicionalmente al intervalo de actualización configurado, la tarea de actualización se ejecuta en cada inicio de una conexión a Internet.

Repetir la tarea si el tiempo ya transcurrió

Con esta opción activada, se relanzan las tareas de actualización pasadas que no pudieron realizarse en su momento, por ejemplo, porque el equipo estaba apagado.

Descarga

A través de servidor Web

La actualización se ejecuta a través de un servidor Web mediante conexión HTTP. Podrá utilizar un servidor Web del productor o un servidor Web en Intranet que recibe los ficheros de actualización de un servidor Web del productor en Internet.

Nota

Encontrará configuraciones adicionales para la actualización a través de un servidor Web en: Configuración :: General :: Actualización :: Servidor Web .

A través de servidor de ficheros/carpetas compartidas

La actualización se produce a través de un servidor de ficheros en Intranet que recibe los ficheros de actualización de un servidor de descarga del productor en Internet.

Nota

Encontrará configuraciones adicionales para la actualización a través de un servidor de ficheros en: Configuración :: General :: Actualización :: Servidor de ficheros .

12.7.1 Actualización de producto

En **Actualización del producto** se configura la ejecución de actualizaciones del producto o la notificación sobre actualizaciones de producto disponibles.

Actualizaciones de producto

Descargar actualizaciones de producto e instalar automáticamente

Si está activada esta opción, se descargan las actualizaciones de producto y el componente de actualización las instala automáticamente en cuanto estén disponibles. Las actualizaciones del fichero de firmas de virus y del motor de análisis siempre se llevan a cabo y de forma independiente de esta configuración. Los requisitos para esta opción son: la configuración completa de la actualización y una conexión establecida con un servidor de descargas.

Descargar actualizaciones de producto. Si fuera necesario un reinicio, instalar la actualización después del siguiente reinicio del sistema; si no, instalarla inmediatamente.

Con esta opción activada, las actualizaciones de producto se descargan en cuanto estén disponibles. La actualización se instala automáticamente después de la descarga de los ficheros de actualización si no se precisa el reinicio del equipo. Si se trata de una actualización del producto que precisa el reinicio del equipo, la actualización del producto no se ejecuta inmediatamente después de la descarga de los ficheros de actualización, sino sólo después del siguiente reinicio del sistema ejecutado por el usuario. La ventaja es que el reinicio no se produce en un momento en el que el usuario trabaja en el equipo. Las actualizaciones del fichero de firmas de virus y del motor de análisis siempre se llevan a cabo y de forma independiente de esta configuración. Los requisitos para esta opción son: la configuración completa de la actualización y una conexión establecida con un servidor de descargas.

Notificar cuando haya nuevas actualizaciones de producto disponibles

Si está activada esta opción, sólo recibirá notificación si hay nuevas actualizaciones de producto disponibles. Las actualizaciones del fichero de firmas de virus y del motor de análisis siempre se llevan a cabo y de forma independiente de esta configuración. Los requisitos para esta opción son: la configuración completa de la actualización y una conexión establecida con un servidor de descargas. La notificación se produce mediante un mensaje en el escritorio en forma de ventana emergente y mediante un mensaje de advertencia del Updater en el Centro de control en Información general::Eventos.

Notificar nuevamente después de n día(s)

Indique en este campo después de cuántos días se debe efectuar una nueva notificación sobre actualizaciones de producto disponibles si la actualización del producto no se efectuó después de la primera notificación.

No descargar actualizaciones de producto

Si está activada la opción, no se llevan a cabo actualizaciones automáticas del producto ni notificaciones sobre la disponibilidad de dichas actualizaciones a través de Updater. Las actualizaciones del fichero de firmas de virus y del motor de análisis siempre se llevan a cabo y de forma independiente de esta configuración.

Importante

Las actualizaciones del fichero de firmas de virus y del motor de análisis se llevan a cabo con cada actualización que se ejecute, independientemente de la configuración de la actualización de producto (consulte al respecto el cap. Actualizaciones).

Nota

Si ha activado una opción para una actualización automática del producto, bajo Configuración del reinicio puede configurar otras opciones para la notificación y posibilidades de cancelación del reinicio.

12.7.2 Configuración del reinicio

Si se ejecuta una actualización de producto de su programa AntiVir, puede ser necesario reiniciar el equipo. Si ha configurado la ejecución automática de actualizaciones del producto en Actualización::Actualización del producto, puede seleccionar en **Configuración del reinicio** entre diferentes opciones para la comunicación y la cancelación del reinicio.

Nota

Cuando configure el reinicio tenga en cuenta que puede seleccionar durante la configuración en Actualización::Actualización del producto entre dos opciones para la ejecución de una actualización del producto con necesidad de reinicio del equipo:

Ejecución automática de la actualización del producto con necesidad de reinicio del equipo cuando esté disponible la actualización: La actualización y el reinicio se ejecutarán mientras esté trabajando un usuario en el equipo. Si tiene activada esta opción, pueden ser útiles las rutinas de reinicio con posibilidad de cancelación o con función de recordatorio.

Ejecución de la actualización del producto con necesidad de reinicio del equipo tras el siguiente inicio del sistema: la actualización y el reinicio se ejecutan cuando un usuario haya arrancado el equipo e iniciado la sesión. Para esta opción son recomendables las rutinas automáticas de reinicio.

Configuración del reinicio

Reiniciar el equipo después de n segundos

Con esta opción activada, se ejecuta en caso necesario **automáticamente** un reinicio una vez realizada la actualización del producto y transcurrido el intervalo de tiempo indicado. Aparece un mensaje de cuenta atrás sin la posibilidad de cancelar el reinicio del equipo.

Mensaje de recordatorio para el reinicio cada n segundos

Con esta opción activada, **no se ejecuta automáticamente** un reinicio necesario tras la actualización del producto. En el intervalo de tiempo indicado recibirá mensajes sin posibilidad de cancelación del reinicio. Los mensajes permiten confirmar el reinicio del equipo o seleccionar la opción "**Recordar en otro momento**".

Consulta si desea realizar el reinicio del equipo

Con esta opción activada, **no se ejecuta automáticamente** un reinicio necesario tras la actualización del producto. Aparecerá un único mensaje donde puede confirmar el reinicio o cancelar la rutina de reinicio.

Reiniciar el equipo sin consulta

Con esta opción activada, se ejecuta **automáticamente** un reinicio necesario tras la actualización del producto. No aparece ningún mensaje.

12.7.3 Servidor de ficheros

En caso de que haya más de un equipo en la red, su programa AntiVir puede descargar la actualización desde un servidor de ficheros en la Intranet, el cual a su vez los obtiene de un servidor de descargas del productor en Internet. Esto facilita que los programas AntiVir esté actualizado en todos los equipos con un bajo consumo de recursos.

Nota

La sección de configuración sólo está activada, si en Configuración :: Actualización:: Actualización de producto se ha seleccionado la opción **a través de servidor de ficheros / Carpetas compartidas**.

Descarga

Indique el servidor de ficheros en el que se encuentran los ficheros de actualización de su programa AntiVir, así como las carpetas necesarias '/release/update/'. Se precisa la siguiente información: file://<Dirección IP del servidor de ficheros>/release/update/. La carpeta 'release' debe ser una carpeta compartida con todos los usuarios.



El botón abre una ventana en la que puede seleccionar el directorio de descarga deseado.

Inicio de sesión en servidor**Nombre de inicio de sesión**

Introduzca un nombre de usuario para entrar en el servidor. Utilice una cuenta de usuario con derechos de acceso al directorio utilizado y compartido en el servidor.

Contraseña de inicio de sesión

Introduzca aquí la contraseña de la cuenta de usuario utilizada. Los caracteres introducidos se enmascaran con *.

Nota

Si no se introduce ningún dato en el área de inicio de sesión del servidor, no se utiliza autenticación durante el acceso al servidor de ficheros. En este caso, el usuario debe de tener suficientes derechos en el servidor de ficheros.

12.7.4 Servidor Web

La actualización puede realizarse desde un servidor Web en Interneto Intranet .

Conexión al servidor Web**Utilizar la conexión existente (red)**

Este parámetro se muestra cuando su conexión se utiliza a través de una red.

Utilizar la siguiente conexión:

Este parámetro se muestra si define su conexión de forma individual.

El Updater detecta automáticamente las conexiones disponibles. Las conexiones que no están disponibles están en gris y no pueden activarse. Puede crear una conexión de acceso telefónico a redes, por ejemplo, manualmente mediante una entrada de la agenda en Windows.

- **Usuario:** Introduzca aquí el nombre de usuario de la cuenta seleccionada.
- **Contraseña:** Indique la contraseña de esa cuenta. Por seguridad, los caracteres que teclee serán visualizados como asteriscos (*).

Nota

Si ha olvidado los datos para conectar a Internet, contacte con su proveedor de servicios de Internet.

Nota

La marcación telefónica automática del Updater por medio de herramientas de marcación telefónica (p. ej., SmartSurfer, Oleco...) todavía no está disponible en.

Finalizar la conexión de acceso telefónico a redes que se inició para la actualización

Si la opción está activada, la conexión de acceso telefónico a redes abierta para la actualización se cierra automáticamente tan pronto como la descarga finaliza correctamente.

Nota

Esta opción no está disponible en Vista. En Vista, la conexión de acceso telefónico a redes abierta para la actualización siempre finaliza en cuanto la descarga se haya ejecutado.

Descarga

Servidor predeterminado

Aquí se introducen las direcciones (URL) de los servidores Web desde los cuales se descargan las actualizaciones, así como la carpeta de actualización 'update'. Es válida la siguiente indicación de un servidor Web: http://<Dirección del servidor Web>[:Puerto]/update. Si no indica ningún puerto, se utiliza el puerto 80. De forma estándar, constan los servidores Web disponibles de Avira GmbH para actualizar. No obstante, también puede utilizar servidores Web propios, por ejemplo en Intranet. En caso de indicar más de un servidor Web, los servidores se separan mediante comas.

Predeterminado

El botón restablece las direcciones predefinidas.

Servidor priorit.

En este campo se indica la dirección (URL) del servidor Web al cual se envía la solicitud de actualización en primer lugar, así como la carpeta de actualización necesaria. Si este servidor no está disponible, la solicitud se pasa a los servidores estándar indicados. Es válida la siguiente indicación del servidor Web: http://<Dirección del servidor Web>[:Puerto]/update. Si no indica ningún puerto, se utiliza el puerto 80.

12.7.4.1. Proxy

Servidor proxy

No usar servidor proxy

Al activar esta opción, su conexión al servidor Web no se realiza a través de un servidor proxy.

Utilizar la configuración del sistema de Windows

Al activar esta opción se utiliza la configuración del sistema de Windows actual para la conexión al servidor Web a través de un servidor proxy. Se configura el sistema de Windows para utilizar un servidor proxy en el **Panel de control:: Opciones de Internet:: Conexiones :: Configuración de LAN**. En Internet Explorer también se puede acceder a Opciones de Internet en el Menú Herramientas.

Advertencia

Si utiliza un servidor proxy que requiere autenticación, indique los datos completos en la opción *Conexión a través de este servidor proxy*. La opción *Utilizar la configuración del sistema de Windows* sólo se puede utilizar para servidores proxy sin autenticación.

Conexión a través de este servidor proxy

Si su conexión al servidor Web se configura a través de un servidor proxy, introduzca aquí la información necesaria.

Dirección

Introduzca el nombre del equipo o la dirección IP del servidor proxy que desea usar para conectar al servidor Web.

Puerto

Introduzca el número de puerto del servidor proxy que desea utilizar para conectar con el servidor Web.

Nombre de inicio de sesión

Introduzca un nombre de usuario para entrar al servidor proxy.

Contraseña de inicio de sesión

Introduzca aquí la clave para el registro en el servidor proxy. Por seguridad, los caracteres que teclee serán visualizados como asteriscos (*).

Ejemplos:

Dirección:	proxy.dominio.com	Puerto:	8080
Dirección:	192.168.1.100	Puerto:	3128

12.8 General

12.8.1 Email

Ante ciertos eventos, el programa AntiVir puede enviar alertas y mensajes por email a uno o más destinatarios. Para ello se usa el protocolo simple de transferencia de correo (SMTP).

Los mensajes pueden dispararse ante diferentes eventos. Los siguientes componentes soportan el envío de emails:

- Guard: Envío de notificaciones
- Escáner: Envío de notificaciones
- Updater: Envío de notificaciones

Nota

El protocolo ESMTP no está soportado. Además la transferencia por TLS (Transport Layer Security) o SSL (Secure Sockets Layer) no es posible en la actualidad.

Mensajes de email

Servidor SMTP

Introduzca el nombre del host o su IP.

La longitud máxima del nombre del host es de 127 caracteres.

Por ejemplo:

192.168.1.100 o mail.ejemplo.com.

Dirección del remitente

Introducir aquí la dirección de email del remitente. La longitud máxima del nombre del host es de 127 caracteres.

Autenticación

Algunos servidores de correo esperan que un programa, antes de enviar un email, se autentique (registre) en el servidor. Se pueden entregar advertencias por email con autenticación a un servidor SMTP.

Usar autenticación

Al activar esta opción, se debe de introducir nombre de usuario y clave para autenticarse ante el servidor de correo.

- **Nombre de usuario:** Introduzca aquí el nombre de usuario.
- **Contraseña:** Introducir la clave aquí. La contraseña se guarda encriptada. Por seguridad, los caracteres que teclee serán visualizados como asteriscos (*).

Enviar email de prueba

Cuando se hace clic en el botón, el programa intenta enviar un email de prueba a la dirección del remitente para comprobar los datos introducidos.

12.8.2 Categorías de riesgos

Selección de categorías de riesgos

Su producto AntiVir le protege contra virus informáticos.

Además, puede ejecutar un análisis de acuerdo con las siguientes categorías de amenazas.

- Software de control de puerta trasera (BDC)
- Marcador (DIALER)
- Juegos (GAMES)
- Chistes (JOKES)
- Riesgo de seguridad-confidencialidad (Security privacy risk, SPR)
- Adware/Spyware (ADSPY)
- Utilidades de compresión no estándar (PCK)
- Ficheros con doble extensión (HEUR-DBLEXT)
- Suplantación de identidad (phishing)
- Aplicación (APPL)

Hacer clic sobre las marcas correspondientes para activar o desactivar

Activar todas

Con esta opción, se activan todos los tipos

Valores predeterminados

Este botón restablece los valores estándar predefinidos.

Nota

Si no se activa un tipo, los ficheros que se reconocen como pertenecientes al mismo, no se siguen indicando. No se anota en el fichero de informe.

12.8.3 Contraseña

Puede proteger su programa AntiVir en distintas áreas con una contraseña. Si se ha introducido una contraseña, se le solicitará cada vez que acceda al área protegida por la misma.

Contraseña

Introducir contraseña

Introduzca su contraseña aquí. Por motivos de seguridad, los caracteres que teclee serán visualizados como asteriscos (*). Puede introducir un máximo de 20 caracteres. Una vez que la clave se ha introducido, el programa no permitirá el acceso si no se introduce la contraseña correcta. Un campo vacío significa que "No hay contraseña".

Confirmar la contraseña

Introducir la contraseña mencionada arriba de nuevo para su confirmación. Por seguridad, los caracteres que teclee serán visualizados como asteriscos (*).

Nota

¡La contraseña distingue entre mayúsculas y minúsculas!

Áreas protegidas por contraseña

Su programa AntiVir puede proteger distintas áreas con una contraseña. Haciendo clic en las casillas correspondientes puede desactivarse y activarse la solicitud de contraseña para las diferentes áreas.

Área protegida con contraseña	Función
Centro de control	Si la opción está activada, se necesita la contraseña establecida para iniciar el Centro de control.
Activar/desactivar Guard	Si la opción está activada, se necesitará la contraseña establecida para activar o desactivar AntiVir Guard.
Activar/desactivar MailGuard	Si la opción está activada, se necesitará la contraseña establecida para activar o desactivar MailGuard.
Activar/desactivar FireWall	Si la opción está activada, se necesitará la contraseña establecida para activar o desactivar el FireWall.

Activar / desactivar WebGuard	Si la opción está activada, se necesitará la contraseña establecida para activar o desactivar WebGuard.
Descargar CD de rescate de Internet	Si la opción está activada, se necesitará una contraseña para iniciar la descarga del CD de rescate de Avira.
Cuarentena	Si la opción está activada, se activan todas las áreas del gestor de cuarentena que pueden protegerse con contraseña. Haciendo clic en las casillas deseadas, puede desactivarse y activarse a voluntad la solicitud de la contraseña en las diferentes áreas
Restaurar los objetos afectados	Con esta opción activada, se necesita la contraseña establecida para restaurar un objeto.
Volver a analizar objetos afectados	Con esta opción activada, se necesita la contraseña establecida para comprobar de nuevo un objeto.
Propiedades de los objetos afectados	Si la opción está activada, se necesitará la contraseña establecida para mostrar las propiedades de un objeto.
Eliminar los objetos afectados	Con esta opción activada, se necesita la contraseña establecida para eliminar un objeto.
Enviar un email a Avira	Si la opción está activada, se necesitará la contraseña establecida para enviar un objeto al Avira Malware Research Center para su análisis.
Copiar los objetos afectados	Con esta opción activada, se necesita la contraseña establecida para copiar objetos afectados.
Añadir y modificar tareas	Si la opción está activada, se necesitará la contraseña establecida para añadir y modificar tareas en el planificador.
Iniciar actualizaciones de producto	Si está activada la opción, se necesitará la contraseña establecida al iniciar la actualización del producto en el menú de actualización.
Configuración	Si la opción está activada, la configuración del programa sólo es posible tras introducir la contraseña establecida.
Cambio manual de la configuración	Con la opción activada, se precisa la contraseña establecida para el cambio manual a otro perfil de configuración.
Activar el modo experto	Si la opción está activada, se necesitará la contraseña establecida para activar el modo

	experto.
Instalación/desinstalación	Si la opción está activada, se necesitará la contraseña establecida para instalar o desinstalar el programa.

12.8.4 Seguridad

Update/Actualización

Alertar si la última actualización se produjo hace más de n días

Aquí puede introducir el máximo número de días permitidos sin actualizar. Si se sobrepasa este periodo de tiempo, se muestra un icono rojo en el Centro de control en el estado para el estado de actualización.

Mostrar nota si el fichero de firmas de virus está obsoleto

Si esta opción está activada, se mostrará un mensaje si los ficheros de firmas no están al día. Con la ayuda de la opción de alerta, puede configurar el intervalo para recibir el aviso si la última actualización no se ha producido desde hace más de cierto número de días.

Protección del producto

Nota

Las opciones de protección del producto no están disponibles si no se ha instalado el Guard durante una instalación personalizada.

Previene la finalización no deseada de procesos

Con esta opción activada, todos los procesos del programa quedan protegidos contra una finalización no deseada a causa de virus y malware, o bien contra la finalización "incontrolada" por parte de un usuario, p. ej., a través del Administrador de tareas. Esta opción está activada de forma estándar.

Protección extendida de procesos

Con esta opción activada, todos los procesos del programa quedan protegidos contra la finalización no deseada mediante métodos extendidos. La protección extendida de procesos requiere significativamente más recursos del equipo que la protección simple de procesos. La opción está activada de forma estándar. Para desactivar la opción se debe reiniciar el equipo.

Importante

¡La protección de procesos no está disponible en Windows XP 64 Bit !

Advertencia

Si está activada la protección de procesos, pueden producirse problemas de interacción con otros productos de software. En esos casos, desactive la protección de procesos.

Proteger los ficheros y las entradas del registro contra manipulaciones

Con esta opción activada, todas las entradas en el registro del programa, así como todos los ficheros del programa (ficheros binarios y de configuración) quedan protegidos contra manipulaciones. La protección contra manipulaciones consta de protección contra acceso de escritura, eliminación y parcialmente de lectura a las entradas del registro o a los ficheros de programa por parte de los usuarios o programas de terceros. Para activar la opción se debe reiniciar el equipo.

Advertencia

Tenga en cuenta que, con la opción desactivada, puede fracasar la reparación de ordenadores infectados con determinados tipos de malware.

Nota

Con esta opción activada, la modificación de la configuración y también la modificación de tareas de análisis o actualización sólo es posible por medio de la interfaz de usuario.

Importante

¡La protección de ficheros y entradas de registro no está disponible en Windows XP 64 Bit !

12.8.5 WMI

Compatibilidad con Windows Management Instrumentation (Instrumental de Administración de Windows - WMI)

Windows Management Instrumentation es una tecnología fundamental de administración de Windows que, mediante lenguajes de script y de programación, permite el acceso de lectura, escritura, local y remoto a la configuración de los equipos con Windows. Su programa AntiVir es compatible con WMI y proporciona los datos (información de estado, datos estadísticos, informes, tareas programadas, etc.), así como los eventos y métodos (detener e iniciar procesos) en una interfaz. Por medio de WMI, tiene la posibilidad de consultar datos operativos del programa y controlar el programa . Puede solicitar referencias de la interfaz WMI al fabricante. Tras firmar un acuerdo de confidencialidad, recibirá la referencia en formato PDF.

Activar compatibilidad con WMI

Si esta opción está activada, puede consultar los datos operativos del programa por medio de WMI.

Permitir activar/desactivar servicios

Si esta opción está activada, puede activar y desactivar servicios del programa por medio de WMI.

12.8.6 Directorios

Ruta temporal

En este campo puede introducir la ruta en la que deben guardarse los ficheros temporales del programa.

Usar configuración del sistema

Al activar esta opción, se usa la configuración del sistema para la gestión de los ficheros temporales.

Nota

Puede ver dónde se guardan los ficheros temporales de Windows XP - en: Inicio | Panel de Control | Sistema | Pestaña Opciones Avanzadas | Botón Variables de entorno. Aquí se muestran las variables temporales (TEMP, TMP) (TEMP, TMP) del usuario registrado, con su valor.

Usar el directorio siguiente

Al usar esta opción, se utiliza la ruta contenida en el campo.



El botón abre una ventana en la que puede seleccionar la ruta temporal.

Predeterminado

El botón restablece el directorio por defecto como directorio temporal.

Directorio para informes

Este campo contiene la ruta al directorio de informes.



Pulsando el botón se abre una ventana en la que puede seleccionar el directorio deseado.

Predeterminado

El botón restablece el directorio por defecto usado como directorio de informes.

Directorio de cuarentena

Este campo contiene la ruta del directorio de cuarentena.



Pulsando el botón se abre una ventana en la que puede seleccionar el directorio deseado.

Predeterminado

El botón restablece el directorio por defecto a usar como directorio de cuarentena.

12.8.7 Advertencias

12.8.7.1. Red

Puede enviar advertencias personalizables del escáner o del Guard a cualquier equipo de su red.

Nota

Compruebe si se ha iniciado el "servicio de alerta". Dicho servicio se encuentra (en el caso de Windows XP) en "Inicio | Configuración | Panel de control | Herramientas administrativas | Servicios".

Nota

Una alerta siempre se envía al equipo, NO a un cierto usuario.

Advertencia

Los siguientes sistemas operativos ya no admiten la funcionalidad:
Windows Server 2008 y superior
Windows Vista y superior

Enviar mensaje a

La lista en esta ventana muestra los nombres de los equipos que recibirán un mensaje al encontrarse un virus o programa no deseado.

Nota

Los equipos deben de aparecer una sola vez en esta lista.

Insertar

Con este botón, puede añadir otro equipo. Se abre una ventana en la que puede introducir los nombres de los equipos. El nombre de un equipo puede tener hasta 15 caracteres.



Este botón abre una ventana en la que puede seleccionar el equipo navegando por su red.

Eliminar

Con este botón, puede quitar de la lista la entrada seleccionada

Guard

Advertencias de red

Con esta opción activada, se envía una alerta a la red. Esta opción está deshabilitada de forma estándar.

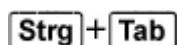
Nota

Para poder activar esta opción, en General :: Advertencias :: Red debe constar al menos un destinatario.

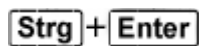
Mensaje para enviar

La ventana muestra el mensaje enviado a los equipos seleccionados cuando se detecta un virus o programa no deseado. Puede modificar este mensaje. El texto puede contener hasta 500 caracteres.

Puede usar la siguiente combinación de teclas para formatear el mensaje:



inserta una tabulación. La línea actual se desplaza varios caracteres a la derecha.



inserta un salto de línea.

El mensaje puede incluir comodines para la información que se encontró durante la búsqueda. Estos comodines serán reemplazados por el texto apropiado.

Se pueden utilizar los siguientes comodines:

- | | |
|------------|---|
| %VIRUS% | contiene el nombre del virus o del programa no deseado detectados |
| %FILE% | contiene la ruta y el nombre de fichero del fichero infectado |
| %COMPUTER% | contiene el nombre del equipo en el que se ejecuta Guard |

%NAME%	contiene el nombre del usuario que ha tenido acceso al fichero infectado
%ACTION%	contiene la acción que se ha ejecutado tras la detección del virus
%MACADDR%	contiene la dirección MAC del equipo en el que se ejecuta el Guard

Predeterminado

Este botón restaura el texto predefinido por una alerta.

Escáner

Alertas en la red

Con esta opción activada, se envía una alerta a la red. Esta opción está deshabilitada de forma estándar.

Nota

Para poder activar esta opción, en General :: Advertencias :: Red debe constar al menos un destinatario.

Mensaje para enviar

La ventana muestra el mensaje enviado a los equipos seleccionados cuando se detecta un virus o programa no deseado. Puede modificar este mensaje. El texto puede contener hasta 500 caracteres.

Puede usar la siguiente combinación de teclas para formatear el mensaje:

Strg + **Tab** inserta una tabulación. La línea actual se desplaza varios caracteres a la derecha.

Strg + **Enter** inserta un salto de línea.

El mensaje puede incluir comodines para la información que se encontró durante la búsqueda. Estos comodines serán reemplazados por el texto apropiado.

Se pueden utilizar los siguientes comodines:

%VIRUS%	contiene el nombre del virus o del programa no deseado detectados
%NAME%	contiene el nombre del usuario que inició sesión y está ejecutando el escáner

Predeterminado

Este botón restaura el texto predefinido por una alerta.

12.8.7.2. Email

Email

Ante ciertos eventos, el programa AntiVir puede enviar alertas y mensajes por email a uno o más destinatarios. Para ello se usa el protocolo simple de transferencia de correo (SMTP).

Los mensajes pueden dispararse ante diferentes eventos. Los siguientes componentes soportan el envío de emails:

- Guard: Envío de notificaciones
- Escáner: Envío de notificaciones
- Updater: Envío de notificaciones

Nota

El protocolo ESMTP no está soportado. Además la transferencia por TLS (Transport Layer Security) o SSL (Secure Sockets Layer) no es posible en la actualidad.

Mensajes de email

Servidor SMTP

Introduzca el nombre del host o su IP.

La longitud máxima del nombre del host es de 127 caracteres.

Por ejemplo:

192.168.1.100 o mail.ejemplo.com.

Dirección del remitente

Introducir aquí la dirección de email del remitente. La longitud máxima del nombre del host es de 127 caracteres.

Autenticación

Algunos servidores de correo esperan que un programa, antes de enviar un email, se autentique (registre) en el servidor. Se pueden entregar advertencias por email con autenticación a un servidor SMTP.

Usar autenticación

Al activar esta opción, se debe de introducir nombre de usuario y clave para autenticarse ante el servidor de correo.

- **Nombre de usuario:** Introduzca aquí el nombre de usuario.
- **Contraseña:** Introducir la clave aquí. La contraseña se guarda encriptada. Por seguridad, los caracteres que teclee serán visualizados como asteriscos (*).

Enviar email de prueba

Cuando se hace clic en el botón, el programa intenta enviar un email de prueba a la dirección del remitente para comprobar los datos introducidos.

Guard

Ante ciertos eventos, AntiVir Guard puede enviar alertas y mensajes a uno o varios destinatarios.

Guard

Advertencias por email

Si esta opción está activada, AntiVir Guard envía un mensaje de email con la información más importante cuando se produce un evento determinado. Esta opción está deshabilitada de forma estándar.

Notificación por email de los siguientes eventos

El análisis en tiempo real notificó una detección.

Si esta opción está activada, recibirá un email con el nombre del virus o programa no deseado y el fichero afectado siempre que el análisis en tiempo real detecte alguno de ellos.

Editar

Con el botón "Editar" se abre la ventana "Plantilla de email" en la que se puede configurar el mensaje acerca del evento "Detección durante análisis en tiempo real". Existe la posibilidad de introducir textos para el asunto y el mensaje del email. Para ello puede utilizar variables (consulte Configuración::General::Email::Alertas::Plantilla de email).

Se ha producido un error crítico en Guard.

Con esta opción activada, si se detecta un error crítico interno recibirá un email.

Nota

En este caso, contacte con Soporte e incluya los datos contenidos en el email. El fichero especificado también debería ser enviado para examinarlo.

Editar

Con el botón "Editar" se abre la ventana "Plantilla de email" en la que se puede configurar el mensaje acerca del evento "Error crítico en Guard". Existe la posibilidad de introducir textos para el asunto y el mensaje del email. Para ello puede utilizar variables (consulte Configuración::General::Alertas::Email::Plantilla de email).

Destinatario

En este campo se indican las direcciones de email de los destinatarios. Las direcciones se separan con comas. La longitud máxima de todas las direcciones (es decir, de toda la cadena de caracteres) es de 260 caracteres.

Escáner

Con ciertos eventos, el análisis on-demand puede enviar alertas y mensajes a uno más destinatarios.

Escáner

Habilita el envío de emails de alerta

Si esta opción está activada, el programa envía mensajes de email con la información más importante cuando se produce un evento determinado. Esta opción está deshabilitada de forma estándar.

Notificación por email de los siguientes eventos

Durante el análisis se notificó una detección.

Si esta opción está activada, recibirá un email con el nombre del virus o programa no deseado y el fichero afectado siempre que el análisis directo detecte alguno de ellos.

Editar

Con el botón "Editar" se abre la ventana "Plantilla de email" en la que se puede configurar el mensaje acerca del evento "Detección durante análisis". Existe la posibilidad de introducir textos para el asunto y el mensaje del email. Para ello puede utilizar variables (consulte Configuración::General::Alertas::Email::Plantilla de email).

Fin de un análisis programado.

Si la opción está activada, se envía un email tras haber ejecutado una tarea de análisis. El email contiene datos sobre cuándo se realizó el análisis y su duración, los directorios y ficheros analizados, así como sobre la detección de virus y las advertencias.

Editar

Con el botón "Editar" se abre la ventana "Plantilla de email" en la que se puede configurar el mensaje acerca del evento "Fin del análisis". Existe la posibilidad de introducir textos para el asunto y el mensaje del email. Para ello puede utilizar variables (consulte Configuración::General::Alertas::Email::Plantilla de email).

Añadir fichero de informe como datos adjuntos

Si la opción está activada, al enviar las notificaciones del escáner el fichero de informe actual del componente escáner se adjunta como datos adjuntos al email.

Dirección(es) de los destinatarios

En este campo se indican las direcciones de email de los destinatarios. Las direcciones se separan con comas. La longitud máxima de todas las direcciones (es decir, de toda la cadena de caracteres) es de 260 caracteres.

Updater

El componente Updater puede enviar mensajes por email a uno o varios destinatarios si se producen determinados eventos.

Updater

Advertencias por email

Si está activada la opción, el componente Updater envía mensajes de email con los datos más importantes cuando se produce un determinado evento. Esta opción está desactivada de forma estándar.

Notificación por email de los siguientes eventos

No se precisa actualización. El programa está actualizado.

Si la opción está desactivada, se envía un email si el Updater pudo establecer correctamente una conexión con el servidor de descargas pero éste no dispone de nuevos ficheros. Ello significa que su programa AntiVir está actualizado.

Editar

Con el botón "Editar" se abre la ventana "Plantilla de email" en la que se puede configurar el mensaje acerca del evento "No se precisa actualización". Existe la posibilidad de introducir textos para el asunto y el mensaje del email. Para ello puede utilizar variables (consulte Configuración::General::Alertas::Email::Plantilla de email).

Actualización finalizada correctamente. Se instalaron ficheros nuevos.

Si la opción está activada, se envía un email tras ejecutar cualquier actualización: puede tratarse de una actualización del producto o de una actualización del fichero de firmas de virus o del motor de análisis.

Editar

Con el botón "Editar" se abre la ventana "Plantilla de email" en la que se puede configurar el mensaje acerca del evento "Actualización correcta-Instalación de nuevos ficheros". Existe la posibilidad de introducir textos para el asunto y el mensaje del email. Para ello puede utilizar variables (consulte Configuración::General::Alertas::Email::Plantilla de email).

Actualización finalizada correctamente. Hay una nueva actualización del producto disponible.

Si la opción está activada, sólo se envía un email si se ha ejecutado una actualización del fichero de firmas de virus o del motor de análisis, sin actualización del producto, aunque hay una actualización del producto disponible.

Editar

Con el botón "Editar" se abre la ventana "Plantilla de email" en la que se puede configurar el mensaje acerca del evento "Actualización correcta-Actualización de producto disponible". Existe la posibilidad de introducir textos para el asunto y el mensaje del email. Para ello puede utilizar variables (consulte Configuración::General::Alertas::Email::Plantilla de email).

Error de actualización.

Si la opción está activada, se envía un email si se ha producido un error en la actualización.

Editar

Con el botón "Editar" se abre la ventana "Plantilla de email" en la que se puede configurar el mensaje acerca del evento "Error de actualización". Existe la posibilidad de introducir textos para el asunto y el mensaje del email. Para ello puede utilizar variables (consulte Configuración::General::Alertas::Email::Plantilla de email).

Añadir fichero de informe como datos adjuntos

Si la opción está activada, al enviar las notificaciones del Updater el fichero de informe actual del componente Updater se adjunta como datos adjuntos al email.

Destinatario

En este campo se indican las direcciones de email de los destinatarios. Las direcciones se separan con comas. La longitud máxima de todas las direcciones (es decir, de toda la cadena de caracteres) es de 260 caracteres.

Nota

En caso de los siguientes eventos siempre se envían alertas por email si hay configurados un servidor SMTP y una dirección de destinatario para las notificaciones de Updater: cualquier actualización posterior del programa requerirá actualizar el producto. No se pudo ejecutar la actualización del motor de análisis o del fichero de firmas de virus porque se requiere la actualización del producto.

El envío de estos mensajes de alerta se lleva a cabo independientemente de la configuración de las alertas de email del componente de actualización.

Plantilla de email

En la ventana *Plantilla email* se configuran las notificaciones de email de los distintos componentes sobre los eventos activados. Puede introducir un texto hasta un máximo de 128 caracteres en la línea del asunto y un texto hasta un máximo de 1024 caracteres en el campo del mensaje.

Se pueden utilizar las siguientes variables en el asunto del email y en el mensaje del email:

Variables válidas globalmente

Variable	Valor
Variables de entorno Windows	El componente de notificaciones de email es compatible con todas las variables de entorno de Windows.
%SYSTEM_IP%	Dirección IP del equipo
%FQDN%	Nombre de dominio completo (fully qualified domain name)
%TIMESTAMP%	Sello temporal del evento: formatos de hora y fecha según la configuración de idioma del sistema operativo
%COMPUTERNAME%	Nombre del equipo NetBIOS
%USERNAME%	Nombre del usuario que accede al componente
%PRODUCTVER%	Versión de producto
%PRODUCTNAME%	Nombre del producto
%MODULENAME%	Nombre del componente que envía el email
%MODULEVER%	Versión del componente que envía el email

Variables específicas de los componentes

Variable	Valor	Emails de los componentes
%ENGINEVER%	Versión del motor de análisis utilizado	Guard Escáner
%VDFVER%	Versión del fichero de firmas de virus	Guard Escáner
%SOURCE%	Nombre del fichero completamente cualificado	Guard
%VIRUSNAME%	Nombre del virus o del programa no deseado	Guard
%ACTION%	Acción que se ha ejecutado después de la detección	Guard
%MACADDR%	Dirección MAC de la primera tarjeta de red registrada	Guard
%UPDFILESLIST%	Lista de los ficheros actualizados	Updater

%UPDATETYPE%	Tipo de actualización: actualización del motor de análisis y del fichero de firmas de virus o actualización del producto con actualización del motor de análisis y fichero de firmas de virus	Updater
%UPDATEURL%	URL del servidor de descarga que se ha utilizado para la actualización	Updater
%UPDATE_ERROR%	Error de actualización en palabras	Updater
%DIRCOUNT%	Número de directorios analizados	Escáner
%FILECOUNT%	Número de ficheros analizados	Escáner
%MALWARECOUNT%	Número de virus o programas no deseados encontrados	Escáner
%REPAIREDCOUNT%	Número de ficheros afectados reparados	Escáner
%RENAMEDCOUNT%	Número de ficheros afectados a los que se cambió el nombre	Escáner
%DELETEDCOUNT%	Número de ficheros afectados eliminados	Escáner
%WIPECOUNT%	Número de ficheros afectados que fueron sobrescritos y eliminados	Escáner
%MOVEDCOUNT%	Número de ficheros afectados que se movieron a la cuarentena	Escáner
%WARNINGCOUNT%	Número de alertas	Escáner
%ENDTYPE%	Estado del final del análisis: Cancelado Finalizado correctamente	Escáner
%START_TIME%	Hora de inicio del análisis Hora de inicio de la actualización	Escáner Updater

%END_TIME%	Fin del análisis Fin de la actualización	Escáner Updater
%TIME_TAKEN%	Duración del análisis en minutos Duración de la actualización en minutos	Escáner Updater
%LOGFILEPATH%	Ruta y nombre del fichero del fichero de informe	Escáner Updater

12.8.7.3. Advertencias acústicas

Advertencia acústica

Cuando el escáner o el Guard detectan virus o malware, en el modo de acción interactivo suena un sonido de advertencia. Puede desactivar o activar el sonido de advertencia, así como seleccionar un fichero Wave distinto para el sonido de advertencia.

Nota

El modo de acción del escáner se establece en la configuración, en Escáner::Análisis::Acción en caso de detección. El modo de acción del Guard se establece en la configuración, en Guard::Análisis::Acción en caso de detección.

Sin advertencia

Si la opción está activada, en caso de que el escáner o el Guard detecten virus, no tiene lugar ninguna advertencia acústica.

Reproducir a través de altavoces del PC (sólo en modo interactivo)

Si la opción está activada, en caso de que el escáner o el Guard detecten virus, tiene lugar una advertencia acústica con el sonido de advertencia predeterminado. El sonido de advertencia se reproduce a través del altavoz interno del equipo.

Usar el siguiente fichero Wave (sólo en modo interactivo)

Si la opción está activada, en caso de que el escáner o el Guard detecten virus, tiene lugar una advertencia acústica con el fichero Wave seleccionado. El fichero Wave seleccionado se reproduce a través de un altavoz externo conectado.

Fichero Wave

En este campo, puede introducir el nombre y ruta del fichero de audio deseado. Por defecto se introduce el sonido de advertencia estándar del programa.



El botón abre una ventana en la que puede navegar hasta el fichero con la ayuda del explorador de ficheros

Prueba

Este botón se utiliza para comprobar el fichero Wave seleccionado.

12.8.7.4. Advertencias

En caso de eventos determinados, su programa AntiVir genera notificaciones en el escritorio, las denominadas Slide-Ups, para informarle sobre peligros y ejecuciones correctas o erróneas del programa, como por ejemplo la ejecución de una actualización. En *Advertencias* se puede activar o desactivar la notificación en caso de eventos determinados.

Las notificaciones de escritorio ofrecen la posibilidad de desactivar la notificación directamente en el Slide-Up. Puede deshacer la desactivación de la notificación en *Advertencias*.

Advertencias

sobre las conexiones de marcación telefónica utilizadas

Con la opción activada se le alerta con una notificación en el escritorio cuando un programa de marcación telefónica establece una conexión a través de la red de teléfono o RDSI en su equipo. Existe el peligro de que el programa de marcación sea un Dialer desconocido y no deseado que establece una conexión no gratuita. (ver Virus y más::Categorías de riesgos avanzadas: Dialers).

sobre ficheros actualizados correctamente

Con la opción activada recibe una notificación de escritorio cuando una actualización ha sido completada correctamente y se actualizaron ficheros.

sobre error de actualización

Con la opción activada recibe una notificación de escritorio en caso de una actualización errónea: no se pudo establecer una conexión con el servidor de descargas o los ficheros de actualización no se pudieron instalar.

informando de que no hace falta actualizar

Con la opción activada recibe una notificación de escritorio cuando se inició una actualización, pero la instalación de ficheros no ha sido necesaria al encontrarse su programa actualizado.

12.8.8 Eventos

Limitar tamaño de base de datos de eventos

Limita el máximo número de eventos a n entradas

Si se selecciona esta opción el máximo número de entradas listadas en la base de datos puede limitarse a cierto tamaño; valores posibles: de 100 a 10 000 entradas. Si se sobrepasa el número de entradas, las más antiguas se eliminan.

Elimina eventos con antigüedad superior a n días

Si se selecciona esta opción, los eventos listados en la base de datos se borran después de un cierto período de tiempo: Los valores permisibles están en 1 y 90 días. Esta opción se habilita de forma estándar con un valor de 30 días

No limitar el tamaño de la base de datos (eliminar eventos manualmente)

Si la opción está activada, el tamaño de la base de datos de eventos no está limitado. No obstante, en la interfaz del programa en eventos se muestran como máximo 20 000 entradas.

12.8.9 Limitar informes

Limitar el número de informes

Limitar el número a n unidades

Con esta opción activada, se puede limitar la cantidad máxima de informes; los valores permitidos son: 1 a 300. Al superar la cantidad indicada se eliminan los informes más antiguos.

Borrar todos los informes de más de n días

Si esta opción está activada, los informes se eliminan automáticamente tras un número específico de días. Los valores permisibles están en 1 y 90 días. Esta opción se habilita de forma estándar con un valor de 30 días

No limitar el número de informes (eliminar informes manualmente)

Si esta opción está activada, la cantidad de informes no está limitada.

Este manual se ha elaborado con sumo cuidado. No obstante, no se descartan errores de forma o de contenido. No se permite reproducir esta publicación o parte de ella por ningún medio sin la previa autorización por escrito de Avira Operations GmbH & Co. KG.

Versión 3er trimestre de 2011.

Los nombres de marcas y productos son marcas comerciales o registradas de sus respectivos propietarios. Las marcas protegidas no se indican como tales en este manual. Esto no significa, sin embargo, que pueden usarse libremente.



live free.™