# G DATA
# SECURITY SOFTWARE

# Índice de contenido

# 1. Introducción

En una época de interconexión global con los riesgos masivos de seguridad que esto implica, el tema de la protección antivirus ya no es un asunto de interés exclusivo de los especialistas informáticos. Por el contrario, el problema debe considerarse desde el nivel más alto de administración en el marco de una gestión de riesgos global a escala de toda la empresa. Una caída de la red informática provocada por un ataque de virus afecta al punto más vulnerable de una empresa. Las consecuencias inmediatas son inactividad de sistemas vitales para el negocio, pérdida de datos y caída de los canales de comunicación más importantes. Los virus informáticos pueden causar a una empresa daños de los que nunca se recupere.

G DATA le ofrece una protección antivirus eficaz para toda su red. El rendimiento líder de los productos de seguridad G DATA se premia desde hace años con las máximas calificaciones en numerosas pruebas y comparativas antivirus. El software G DATA Business apuesta de modo consecuente por una configuración y administración centralizadas, así como por el máximo nivel posible de automatización. Todos los clientes, ya sean estaciones de trabajo, portátiles o servidores de archivos, se gestionan de modo centralizado. Todos los procesos de los clientes se ejecutan de forma transparente en segundo plano. Las actualizaciones online automáticas permiten conseguir tiempos de reacción extremadamente breves cuando hay un ataque de virus. La gestión centralizada con el G DATA ManagementServer permite la instalación, configuración, actualización, administración remota y automatización de toda la red. Esto facilita el trabajo del administrador de sistemas, y ahorra tiempo y costes.

Le deseamos un trabajo seguro y con éxito con su software G DATA Business.

El equipo G DATA

## 1.1. Documentación

Encontrará información detallada acerca del uso del software en la ayuda del programa, que puede abrir en cualquier momento pulsando la tecla F1. Además, tiene la posibilidad de descargarse una documentación completa en formato PDF desde el área de descarga del **sitio web de G DATA**.

## 1.2. Línea de asistencia

La línea de asistencia para las licencias de red de G DATA está disponible en todo momento para todos los clientes corporativos registrados.

> Teléfono: +34 91 745 3074
> Si utiliza una tarifa plana, su llamada de soporte no tendrá costes adicionales, de acuerdo con las condiciones de tarifa.
>
> Correo electrónico: **soporte-empresas@gdata.es**
>
> Muchas consultas y asuntos ya han sido respondidos en el área de soporte de la página web de G DATA. Visítenos en:
>
> **www.gdata.es**

Antes de ponerse en contacto con atención al cliente, le rogamos que compruebe cuál es el equipamiento de su ordenador/red. Sobre todo, son importantes los siguientes datos:

- El número de versión de G DATA Administrator (figura en el menú de ayuda).

- El número de registro o el nombre del usuario para la actualización online. El número de registro figura en la orden de compra. En caso de dudas, contacte a su proveedor de servicios TI o al distribuidor responsable.
- La versión exacta de Windows (cliente y servidor).
- Componentes complementarios instalados de hardware y software (cliente y servidor).
- Mensajes de error que le hayan surgido (con el código de error, si lo tiene, y el texto exacto).

Con estos datos, la conversación con los asesores del servicio de atención al cliente se desarrollará con mayor rapidez, efectividad y éxito. Si es posible, sitúe el teléfono cerca de un ordenador en el que esté instalado el G DATA Administrator.

## 1.3. G DATA Security Labs

Si descubre un nuevo virus o un fenómeno desconocido, envíenos sin falta ese archivo mediante la función cuarentena del software G DATA. Haga clic en el área **Eventos de seguridad** con el botón derecho de ratón en el virus encontrado y seleccione allí la opción **Cuarentena: enviar a los laboratorios de G DATA Security**. Por supuesto, trataremos los datos que nos envíe con la máxima confidencialidad y discreción.

## 1.4. Soluciones G DATA Business

En la presente documentación se describe la funcionalidad de todos los módulos de G DATA Business. Si echa en falta alguna característica en la versión que ha instalado, en el **Centro de Servicio G DATA** puede recibir cómodamente información acerca de cómo actualizar o ampliar su software. Para más información acerca de nuestra gama de productos visite **www.gdata.es**.

# 2. Instalación

Inicie Windows e inserte el soporte de instalación de G DATA. Se abrirá automáticamente una ventana de instalación, que le permitirá seleccionar los componentes del software G DATA a instalar. Si en lugar de haber recibido un soporte de instalación se ha descargado el software, extraiga todos los archivos y ejecute Setup.exe. Para facilitar la instalación del software en otros clientes, puede grabar los archivos extraídos en un DVD o copiarlos a un lápiz USB. Cierre todos los demás programas antes de iniciar la instalación del software G DATA. Se pueden producir fallos de funcionamiento o una cancelación de la instalación si, p.ej., hay abiertos programas que accedan a datos que son necesarios para la instalación del software G DATA. Se pueden instalar los siguientes componentes:

- **G DATA ManagementServer**: instale en primer lugar G DATA ManagementServer en el ordenador que vaya a administrar todos los ajustes y actualizaciones relevantes de G DATA. G DATA ManagementServer es el corazón de la arquitectura G DATA y se encarga de la administración de los clientes, pide automáticamente a los servidores de actualizaciones de G DATA las actualizaciones más recientes del software y de las firmas de virus, y gestiona la protección antivirus en la red. Con la instalación del G DATA ManagementServer se instala también de forma automática el software G DATA Administrator, con el cual se gestiona el G DATA ManagementServer.
- **G DATA Administrator**: G DATA Administrator es el software con el que se gestiona el G DATA ManagementServer y que permite la administración de configuraciones y actualizaciones para todos los clientes G DATA instalados en la red. G DATA Administrator está protegido mediante contraseña, se puede instalar y ejecutar en todos los ordenadores con Windows que estén conectados en red con G DATA ManagementServer.
- **G DATA Security Client**: el software cliente proporciona la protección antivirus a los clientes y ejecuta en segundo plano, sin interfaz de usuario propia, las tareas encargadas por el G DATA ManagementServer. La instalación del software cliente se realiza, por regla general, de manera centralizada para todos los clientes a través del G DATA Administrator.
- **G DATA Boot Medium Wizard**: con ayuda del asistente de G DATA Boot Medium puede crear un CD, DVD o USB de arranque para efectuar un análisis completo de su ordenador. Este análisis se realiza antes de que arranque el sistema operativo instalado y utiliza firmas de virus actualizadas.
- **G DATA WebAdministrator**: G DATA WebAdministrator es una herramienta de administración web para el G DATA ManagementServer. Con él se puede cambiar la configuración del G DATA ManagementServer a través de una interfaz web desde el navegador.
- **G DATA MobileAdministrator**: G DATA MobileAdministrator es una herramienta de administración web para el ManagementServer optimizada para dispositivos móviles. Puede iniciarse desde un navegador web en cualquier dispositivo móvil y le ofrece las funciones de administración básicas de G DATA Administrator.
- **G DATA MailSecurity para Exchange**: G DATA MailSecurity para Exchange protege de forma centralizada todo el tráfico de correo electrónico basado en Exchange. Está disponible como un **módulo opcional**.
- **G DATA MailSecurity MailGateway**: G DATA MailSecurity MailGateway protege de forma centralizada todo el tráfico de correo SMTP y POP3 en la red. Está disponible como un **módulo opcional** y se puede instalar desde su propio soporte de instalación.

# 2.1. Primeros pasos

Le recomendamos que, en caso de sospecha fundada de infección en un ordenador, realice en primer lugar un **BootScan**.

1. Instale **G DATA ManagementServer** en su servidor. Para garantizar una protección óptima, el ordenador debe estar siempre accesible (encendido) y disponer de un acceso a Internet para la carga automática de las firmas de virus. La instalación del G DATA ManagementServer no tiene que realizarse necesariamente en un sistema operativo para servidores (consulte **Requisitos del sistema**). Durante la instalación del G DATA ManagementServer, se instala automáticamente en el servidor el **G DATA Administrator**. Con este programa, es posible administrar el G DATA ManagementServer.
2. Realice ahora el registro online. Sin un registro online no se puede llevar a cabo ninguna actualización del software ni de las firmas de virus.
3. Al iniciar por vez primera en el servidor el G DATA Administrator, se abre el **Asistente de configuración del servidor**. Con él se puede distribuir e instalar de forma remota el **software del cliente** en los clientes de la red que desee. Todos los ajustes que se efectúen con el asistente de configuración pueden modificarse posteriormente.

   Si le surge algún problema durante la **instalación remota de los clientes**, el software de cliente se puede también trasferir mediante una **sincronización de Active Directory** o instalar localmente en el cliente correspondiente con el **soporte de instalación de G DATA** o un **paquete de instalación**. Los paquetes de instalación también pueden distribuirse mediante scripts GPO/de registro. Para que el servidor esté también protegido contra los ataques de virus, se recomienda además instalar el software de cliente en el servidor.

4. Una vez efectuada la instalación y configuración del software cliente en los equipos conectados, es posible gestionar de manera centralizada la protección antivirus, así como las actualizaciones online de los programas de cliente y servidor G DATA. G DATA Administrator ofrece, entre otras, posibilidades de configuración para la protección en tiempo real mediante el **Vigilante G DATA**, así como la posibilidad de definir tareas periódicas de escaneo para analizar la red en busca de virus.

   G DATA Administrator se puede instalar en cualquier cliente de la red en caso de ser necesario resolver algún problema de configuración de forma local en un cliente. De esta forma es posible conectarse con el G DATA ManagementServer desde cualquier cliente. En caso de necesitar resolver alguna situación crítica desde fuera de la red **G DATA WebAdministrator** se puede usar con un navegador web desde cualquier PC Y con **G DATA MobileAdministrator** puede realizar la administración incluso en su navegador web móvil desde cualquier lugar.

## 2.1.1. Requisitos del sistema

Los requisitos mínimos del sistema necesarios para todas las soluciones de seguridad G DATA son:

G DATA ManagementServer

- Sistema operativo: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003
- RAM: 1 GB

G DATA Administrator/G DATA WebAdministrator/G DATA MailSecurity Administrator

- Sistema operativo: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32 bits), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003

G DATA MobileAdministrator

- Sistema operativo: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2012 R2, Windows Server 2012 o Windows Server 2008 R2

G DATA Security Client

- Sistema operativo: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista SP1, Windows XP SP3 (32 bits), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003
- RAM: 1 GB

G DATA Security Client para Linux

- Sistema operativo: Debian 6.0, 7 y 8 32- y 64-bits, OpenSUSE 11.4, 12.2, 12.3, 13.1 y 13.2, Suse Linux Enterprise Server 10 SP4, 11 SP3 y 12, Red Hat Enterprise Linux 5.11, 6.6 y 7.0, Ubuntu 10.04.4 LTS, 12.04.5 LTS, 14.04.1 LTS, 14.10 y 15.04, CentOS 5.11, 6.6 y 7.0, Fedora 19, 20, 21 y 22

G DATA Security Client para Mac

- Sistema operativo: Mac OS X 10.6 o superior

G DATA Internet Security para Android

- Sistema operativo: Android 4.0 o superior

G DATA MailSecurity MailGateway

- Sistema operativo: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32 bits), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 o Windows Server 2003
- RAM: 1 GB

G DATA MailSecurity para Exchange (plug-in para Exchange 64 bits)

- Servidor de correo: Microsoft Exchange Server 2016, Microsoft Exchange Server 2013, Microsoft Exchange Server 2010 o Microsoft Exchange Server 2007 SP1

El sistema G DATA utiliza el protocolo TCP/IP para la comunicación entre los ordenadores cliente y el servidor.

Para el uso de G DATA ManagementServer/G DATA MailSecurity MailGateway con una base de datos local SQL u otras aplicaciones complejas y exigentes en el mismo ordenador, los requisitos del sistema recomendados son:

- RAM: 4 GB
- CPU: multinúcleo

## 2.1.2. Configuración del cortafuegos

Si está usando un cortafuegos implementado en hardware o software, es posible que necesite realizar cambios en los ajustes del mismo. Configure el cortafuegos inmediatamente después de instalar el

software G DATA para asegurarse de que todas las funciones estén disponibles.

### 2.1.2.1. Puertos

Los productos G DATA utilizan diferentes puertos TCP que garantizan una comunicación segura dentro de su red. Verifique que estos puertos estén habilitados en su cortafuegos:

Servidor de administración principal/secundario

- Puerto 80 (TCP)
- Puerto 443 (TCP)
- Puerto 7161 (TCP)
- Puerto 7182 (TCP)
- Puerto 7183

Servidor de subred

- Puerto 80 (TCP)
- Puerto 443 (TCP)
- Puerto 7161 (TCP)

Clientes

- Puerto 7169 (TCP)

Servidor MailSecurity MailGateway

- Puerto 7182 (TCP)

Plugin MailSecurity para Exchange

- Puerto 7171 (TCP)
- Puerto 7185...7195 (TCP)

Los números de puerto para el software de G DATA se han seleccionado especialmente para evitar conflictos con las aplicaciones estándar existentes. No obstante, si se produjese algún conflicto de puerto, se puede por supuesto cambiar el puerto del G DATA ManagementServer. Para hacerlo, abra en primer lugar el administrador de control de servicios (**Inicio**, **Ejecutar**, *services.msc*) con derechos de administrador y detenga el servicio en segundo plano G DATA ManagementServer. Vaya a la carpeta de instalación de su producto G DATA (normalmente C:\Archivos de programa\G DATA \G DATA AntiVirus ManagementServer) y abra el archivo Config.xml en un editor de texto (como por ej. el bloc de notas). En caso necesario, cambie los números de puerto en las entradas siguientes:

- **AdminPort**: introduzca aquí el número de puerto deseado. El valor estándar es "0", (es decir, el puerto queda con el valor predeterminado de 7182).
- **ClientHttpsPort**: el valor estándar es "0" (es decir, el puerto queda con el valor predeterminado de 443). Por lo general, no conviene modificar el valor del puerto ClientHttps porque los clientes móviles Android no aceptan ningún puerto alternativo.
- **ClientHttpPort**: introduzca aquí el número de puerto deseado. El valor estándar es "0", (es decir, el puerto queda con el valor predeterminado de 80).

Si cambia los valores de los puertos ClientHttp o ClientHttps, tendrá que volver a iniciar la configuración de seguridad HTTPS para el puerto correspondiente. Tiene que abrir para ello la línea

de comandos con derechos de administrador y ejecutar *C:\Archivos de programa\G DATA\G DATA AntiVirus ManagementServer\gdmmsconfig.exe /installcert*.

Reinicie el servicio G DATA ManagementServer después de cambiar los puertos. Tenga en cuenta que si cambia el valor para AdminPort, cada vez que inicie sesión en G DATA Administrator tendrá que indicar el puerto modificado. Este dato se introduce en el formato siguiente: *nombreservidor:puerto*.

### 2.1.2.2. URLs

Para poder usar el módulo **PatchManager**, el G DATA ManagementServer tiene que poder descargar archivos de configuración y patches. Si utiliza un cortafuegos, debe permitir el tráfico entre G DATA ManagementServer y las direcciones URL siguientes:

- *gdata.cdn.heatsoftware.com*

Dependiendo del software para el que se van a desplegar patches, debe permitir el tráfico entre el ManagementServer y las direcciones URLs siguientes:

- 7-Zip: *http://downloads.sourceforge.net*
- Adobe: *ardownload.adobe.com*, *armdl.adobe.com*, *download.adobe.com*, *swupdl.adobe.com*, *www.adobe.com*
- Microsoft: *go.microsoft.com*, *download.windowsupdate.com*, *www.download.windowsupdate.com*, *download.skype.com*, *download.microsoft.com*
- Mozilla: *http://ftp.mozilla.org*
- UltraVNC: *http://support1.uvnc.com*
- VideoLAN: *http://download.videolan.org*

## 2.1.3. Soporte de arranque G DATA

Virus ocultos en el ordenador pueden impedir la instalación del software antivirus G DATA. El soporte de arranque G DATA permite combatir estas amenazas ya que se ejecuta antes de que se cargue el sistema operativo.

1. **Con el soporte de instalación**: inserte el soporte de instalación del software G DATA. En la ventana emergente haga clic en **Salir** y apague el ordenador.
   **Con el soporte de arranque creado por usted mismo**: para crear su propio G DATA boot CD, DVD o USB, tiene en primer lugar que instalar el **G DATA Boot Medium Wizard**. El asistente tiene que ejecutarse en un sistema en el que esté instalado el G DATA Security Client con firmas de virus completamente actualizadas. Una vez instalado el G DATA Boot Medium Wizard, siga las instrucciones que aparecen en pantalla para crear el soporte de arranque G DATA.
2. Reinicie el ordenador. Aparece el menú de inicio del soporte de arranque.
3. Seleccione su idioma con los botones de flecha y a continuación **G DATA AntiVirus**. Se inicia un sistema operativo Linux y aparece la interfaz gráfica del soporte de arranque de G DATA AntiVirus.

   Si tiene problemas con la visualización de la interfaz de programa, reinicie el ordenador y seleccione la opción **G DATA AntiVirus – alternativa**.
4. Cuando usted mismo crea un soporte de arranque G DATA, las firmas de virus tendrán la antigüedad de las firmas que estuvieran disponibles en el cliente G DATA Security en ese momento. Si las firmas de virus están desfasadas, el programa recomienda actualizarlas. Haga clic en **Sí** y ejecute la actualización. Asegúrese de haber introducido su número de registro o en

caso de que haya registrado su solución, sus datos de acceso.

5. Ahora verá la interfaz de programa. Haga clic en la entrada **Ordenador** para ejecutar un análisis del sistema en busca de virus y malware. Este proceso puede durar una hora o más en función del tipo de ordenador y el tamaño del disco duro.
6. Si el software G DATA encuentra cualquier tipo de virus, elimínelos con la opción propuesta en el programa. Tras la eliminación con éxito del virus se restaurará el archivo original.
7. Tras finalizar el análisis en busca de virus, haga clic en el botón Cerrar (arriba a la derecha en la interfaz de Linux) y seleccione a continuación **Salir** > **Cerrar**.
8. Retire el soporte de arranque G DATA de la unidad de disco o del puerto USB.
9. Reinicie el ordenador. Ahora arrancará de nuevo con el sistema operativo estándar. El software G DATA ya puede instalarse en un sistema libre de virus.

### 2.1.3.1. G DATA Boot Medium Wizard

Para poder crear un soporte de arranque G DATA tiene que instalar en primer lugar el G DATA Boot Medium Wizard en un sistema en el que esté instalado el G DATA Security Client con firmas de virus completamente actualizadas. Inserte el soporte de instalación G DATA y seleccione ahora el **G DATA BootMediumWizard**.

Una vez finalizada la instalación, en **Inicio** > **(Todos los) Programas** > **G DATA** > **G DATA Boot Medium Wizard**, haciendo clic en **G DATA Boot Medium Wizard**, puede generar un soporte de arranque con ayuda del asistente. No olvide realizar una actualización de las firmas de virus para que el soporte de arranque tenga las firmas más recientes. Después puede generar el soporte de arranque, grabando estos datos en un CD/DVD/USB o guardándolos como imagen ISO. La imagen ISO se puede grabar utilizando un software externo o se puede distribuir por la red a los clientes.

### 2.1.3.2. Configurar la secuencia de arranque en BIOS

Si su sistema no arranca desde el CD/DVD ROM o el dispositivo USB, puede que tenga que configurar primero esta opción. Este ajuste se realiza en el BIOS, un sistema que se inicia antes que el propio sistema operativo. Para modificar los ajustes proceda de la siguiente forma:

1. Apague el ordenador.
2. Reinicie el ordenador. Normalmente, se accede a la configuración del BIOS pulsando durante el encendido del ordenador (= al arrancar) la tecla **Supr** (a veces también las teclas **F2** o **F10**). Los pasos para modificar la secuencia de arranque pueden variar según el modelo. Encontrará más información en la documentación del fabricante.
3. También puede consultar en la documentación del fabricante de la placa base cómo se modifican los ajustes individuales de la configuración del BIOS. En definitiva la secuencia de arranque debería ser **USB**, **CD/DVD ROM**, **C:** de esta forma, el puerto USB se convierte en el 1er dispositivo de arranque, la unidad de CD/DVD ROM en el 2° y la partición del disco duro con el sistema operativo Windows, en el 3º.
4. Guarde los cambios y reinicie el ordenador. Ahora su ordenador está listo para un análisis antes del arranque del sistema.

## 2.2. Instalación del G DATA ManagementServer

Introduzca el soporte de instalación de G DATA y seleccione a continuación el componente G DATA ManagementServer. Cierre todas las aplicaciones que tenga abiertas ya que pueden provocar conflictos durante la instalación. Seleccione el idioma y haga clic en **Instalación**, para comenzar el

asistente de instalación. Lea a continuación el acuerdo de licencia para el uso de este programa. Seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**, si acepta las condiciones del acuerdo.

La selección del tipo de servidor le permite elegir entre los siguientes tipos de servidores:

- **Servidor principal**: al realizar la primera instalación, el G DATA ManagementServer siempre tiene que instalarse como servidor principal (MMS principal). El servidor principal representa la instancia centralizada de administración y configuración de la arquitectura de red. Los ordenadores que deben protegerse reciben a través del G DATA ManagementServer las actualizaciones tanto de firmas de virus como del programa. Por otro lado, todos los ajustes de cliente se realizan de manera centralizada en el G DATA ManagementServer.
- **Servidor secundario**: si se usa una instancia independiente de base de datos SQL es posible utilizar un segundo servidor (MMS secundario) que acceda a la misma base de datos que el servidor principal. En caso de que no sea posible establecer contacto con el servidor principal durante más de una hora, los clientes se conectan automáticamente al servidor secundario para cargar las actualizaciones de firmas. Tan pronto vuelva a estar disponible el servidor principal los clientes restablecen la conexión con el mismo. Ambos servidores cargan las actualizaciones de firmas de forma independiente entre sí para garantizar la protección en caso de fallo.
- **Servidor de subred**: en las redes de gran tamaño (por ejemplo, centrales de empresas con sucursales conectadas entre sí), puede ser conveniente utilizar el G DATA ManagementServer también como servidor de subred. Los servidores de subred ayudan a reducir el tráfico entre los clientes y el MMS principal. Encargándose de administrar los clientes que tengan asignados. Los servidores de subred siguen plenamente operativos, incluso cuando los servidores principal y secundario no se encuentran disponibles. Sin embargo no cargan actualizaciones de firmas de virus de forma autónoma. Introduzca el nombre del servidor principal en **Nombre del servidor principal**.

  La distribución de actualizaciones basada en la tecnología "peer to peer" supone una alternativa a la instalación de un servidor de subred. Cuando se activa esta opción se reduce en gran medida la carga de la red entre el servidor y los clientes durante la distribución de las actualizaciones. En algunas redes, esta funcionalidad puede incluso hacer innecesaria la instalación de un servidor de subred.

Después de haber seleccionado el tipo de servidor, determine que servidor de base de datos debe usar G DATA ManagementServer:

- **Instalar Microsoft SQL Server 2014 Express**: Elija la instalación SQL Server Express si está realizando una nueva instalación de G DATA ManagementServer en una red con menos de 1000 clientes. Microsoft SQL Server 2014 Express no es compatible con Windows Vista y tampoco con Windows Server 2008/2003. En esos sistemas, instale manualmente Microsoft SQL Server 2008 R2 Express antes de instalar ManagementServer o utilice una instancia de base de datos en otro equipo y utilice la opción **Utilizar una instancia de base de datos existente**. Puede encontrar más información en la guía de referencia.
- **Usar una instancia de base de datos existente**: Para redes de gran tamaño, se recomienda usar una instancia existente de Microsoft SQL Server. Si está reinstalando G DATA ManagementServer en un servidor que ya dispone de una instalación de SQL Server Express y una base de datos de G DATA ManagementServer, elija la opción de usar una instancia existente. Tras la instalación, puede configurar la conexión a SQL Server (Express).

La instalación comenzará automáticamente tras confirmar la consiguiente instalación de Microsoft SQL Server 2014 Express y/u otros prerrequisitos. Una vez finalizada la instalación, la solución de G DATA deberá activarse. Esto habilita la inmediata descarga de actualizaciones una vez finalizada la instalación.

- **Introducir un nuevo número de registro**: si instala el software G DATA por primera vez, seleccione esa opción y, a continuación, introduzca el número de registro que viene con el producto. Encontrará este número en el documento de la licencia o en la confirmación del pedido. En caso de dudas, contacte a su proveedor de servicios TI o al distribuidor responsable. Con la introducción del número de registro se activa su producto. Los datos de acceso generados (nombre de usuario y contraseña) se muestran una vez terminado el registro con éxito. **¡Asegúrese de apuntar los datos de acceso y guardarlos en un lugar seguro!** Una vez finalizado el registro con éxito, ya no será necesario introducir nuevamente la clave de licencia.

  Si al introducir el número de registro le surge algún problema, compruebe que ha introducido el número de registro de forma correcta. Dependiendo del tipo de letra utilizado, se puede interpretar mal una "I" mayúscula (de Italia) como la cifra "1", o como la letra "l" (de Lérida). Lo mismo puede ocurrir entre: "B" como "8"; "G" como "6" y "Z" como "2".

- **Introducir los datos de acceso**: si ya se ha instalado anteriormente el software G DATA, habrá recibido los datos de acceso (el nombre de usuario y la contraseña). Para instalar de nuevo el software G DATA, introduzca aquí los datos de acceso.
- **Activar más tarde**: si de momento simplemente desea tener una visión de conjunto del software o si los datos de acceso no están accesibles en ese momento, la instalación también puede realizarse sin introducir datos. Tenga en cuenta que en este caso el programa no se actualizará a través de Internet, y por tanto no le ofrecerá una protección real contra el malware. Solo con las últimas actualizaciones disponibles será posible que el software G DATA proteja de manera efectiva su ordenador. Si utiliza el software sin activación no estará suficientemente protegido. Puede introducir el número de registro o los datos de acceso posteriormente en cualquier momento. Para obtener más información lea también las **indicaciones sobre la activación posterior del software G DATA**.

  Tenga en cuenta que si el software se instala sin activarlo, solo estarán disponibles los componentes de G DATA Antivirus Business, aunque haya adquirido G DATA Client Security Business, G DATA Endpoint Protection Business u otros módulos. Los componentes adicionales se activan y están disponibles en cuanto se registra el software.

Si selecciona una instancia existente de base de datos SQL, puede llevar a cabo la configuración de la base de datos una vez que haya terminado la instalación. Para obtener más información sobre como configurar la base de datos consulte la guía de referencia técnica.

Tras la instalación del G DATA ManagementServer, el software G DATA estará en funcionamiento y listo para ser configurado. Puede que sea necesario reiniciar el servidor. El G DATA ManagementServer se arranca automáticamente cada vez que se inicie (o reinicie) el sistema.

Para administrar el G DATA ManagementServer, puede seleccionar en **Inicio** > **(Todos los) Programas** > **G DATA Administrator** la opción **G DATA Administrator** y, de ese modo, iniciar la herramienta de administración para G DATA ManagementServer.

## 2.3. Instalación de G DATA Administrator

Al realizar la instalación del **G DATA ManagementServer** se instala automáticamente en el mismo ordenador el G DATA Administrator. No es necesario instalar posteriormente el software de administrador en el servidor. Sin embargo sí es posible instalar G DATA Administrator en cualquier ordenador cliente. De este modo es posible gestionar el G DATA ManagementServer también de manera descentralizada desde cualquier ordenador de la red.

Para instalar el G DATA Administrator en un ordenador cliente, inserte el soporte de instalación G DATA y seleccione el componente **G DATA Administrator**.

Cierre entonces todas las aplicaciones que tenga abiertas ya que pueden provocar conflictos durante la instalación. El asistente de instalación le guiará a lo largo de todo el proceso. Después de la instalación se puede seleccionar la opción **G DATA Administrator** en **Inicio** > **(Todos los) Programas** > **G DATA** > **G DATA Administrator**.

## 2.4. Instalación de G DATA WebAdministrator

Introduzca el soporte de instalación G DATA y seleccione el componente **G DATA WebAdministrator**.

La instalación de G DATA WebAdministrator es sencilla e intuitiva. Después de aceptar el acuerdo de licencia, hay que seleccionar la carpeta donde se va a instalar WebAdministrator. Se recomienda instalarlo en el directorio HTTP del servidor web (por ej. \inetpub\wwwroot).

Es posible que durante la instalación sea necesario instalar algún software adicional. Los requisitos previos para la instalación de WebAdministrator son:

- **Internet Information Services (IIS) de Microsoft**: WebAdministrator es un producto basado en web y por eso el servidor en el que se instale debe también poderse utilizar como un servidor web. WebAdministrator es compatible con Microsoft Internet Information Services (IIS). Asegúrese de que se está ejecutando IIS en su servidor antes de instalar WebAdministrator. Para más información acerca de la instalación de IIS consulte la Guía de Referencia Técnica.
- **Compatibilidad con la metabase de IIS 6**: antes de la instalación de G DATA WebAdministrator es necesario habilitar los componentes de compatibilidad de la metabase de IIS en el servidor. En caso contrario la instalación del G DATA WebAdministrator no será posible. A partir de la versión Windows 7 o posteriores, esta opción la encontrará en **Inicio** > **Panel de control** > **Programas** > **Programas y características** > **Activar o desactivar las características de Windows**. Acceda a **Internet Information Services** > **Herramientas de administración web** > **Compatibilidad con la administración de IIS 6** y asegúrese de que la opción **Compatibilidad con la metabase de IIS 6** se encuentre seleccionada. Si se está utilizando un sistema operativo de servidor Microsoft, encontrará las opciones correspondientes en el **Administrador del servidor**, dentro de **Roles**. Acceda a **Servidor web (IIS)** > **Servicios role** y asegúrese de que **Compatibilidad con la metabase de IIS 6** está instalada.
- **Microsoft .NET Framework**: WebAdministrator está basado en .NET Framework de Microsoft. Si .NET Framework de Microsoft aún no está instalado en el servidor, el asistente de instalación de WebAdministrator le solicitará instalar este programa. Después de la instalación es necesario reiniciar el sistema.
- **Microsoft Silverlight**: el G DATA WebAdministrator necesita Microsoft Silverlight. Si no se ha instalado anteriormente, se le indicará la primera vez que ejecute el G DATA WebAdministrator.

Después de la instalación, aparecerá el icono de **G DATA WebAdministrator** en el escritorio de su

ordenador. El programa de instalación le proporcionará también un enlace para acceder al WebAdministrator en su navegador.

El uso de WebAdministrator sin una conexión segura a Internet supone un potencial riesgo de seguridad. Lo mejor es que use un **certificado de servidor SSL en IIS**.

## 2.5. Instalación de G DATA MobileAdministrator

Introduzca el soporte de instalación de G DATA y seleccione el componente **G DATA MobileAdministrator** mediante un clic.

La instalación de G DATA MobileAdministrator es bastante sencilla y análoga a la de **WebAdministrator**. Después de aceptar el acuerdo de licencia, seleccione la carpeta donde vaya a instalar MobileAdministrator. Se recomienda instalarlo en el directorio HTTP del servidor web (por ej. \inetpub\wwwroot).

Es posible que durante la instalación sea necesario instalar algún software adicional. Los requisitos previos para la instalación de MobileAdministrator son:

- **Internet Information Services (IIS) de Microsoft**: MobileAdministrator es un producto basado en web y por eso el servidor en el que se instale debe también poderse utilizar como un servidor web. MobileAdministrator es compatible con Microsoft Internet Information Services (IIS). Asegúrese de que se está ejecutando IIS en su servidor antes de instalar MobileAdministrator. Para más información acerca de la instalación de ISS consulte la Guía de Referencia Técnica.
- **Microsoft .NET Framework**: MobileAdministrator está basado en .NET Framework de Microsoft. Si .NET Framework de Microsoft aún no está instalado en el servidor, el asistente de instalación de MobileAdministrator le solicitará instalar este programa. Después de la instalación es necesario reiniciar el sistema.

Una vez concluida la instalación, el instalador le proporcionará un enlace para acceder a MobileAdministrator desde su smartphone a través de un navegador móvil.

El uso de MobileAdministrator sin una conexión segura a Internet supone un potencial riesgo de seguridad. Lo mejor es que use un **certificado de servidor SSL en IIS**.

## 2.6. Instalación de G DATA Security Client

G DATA Security Client protege y gestiona los clientes de la red de Windows y debe estar instalado en todos los ordenadores Windows. En función de las necesidades concretas, el despliegue del software de cliente se puede realizar mediante una **instalación remota** (a través de G DATA Administrator) o mediante una **instalación local** (con el soporte de instalación de G DATA o un paquete de instalación). Además, también es recomendable instalar G DATA Security Client en el propio servidor.

> Si instala G DATA Security Client en un servidor, asegúrese de que no se produzcan conflictos con flujos de trabajo existentes. Por ejemplo, en servidores de bases de datos y de correo electrónico debería definir excepciones de análisis y del vigilante para algunas carpetas y archivos. Encontrará más información al respecto en la Guía de referencia.

### 2.6.1. Instalación remota

La forma más fácil de instalar el software de cliente es la instalación remota mediante G DATA Administrator. El **Asistente de configuración del servidor** y el módulo **Cliente** le permite instalar

automáticamente G DATA Security Client en todos los ordenadores.

Además de las configuraciones de puertos necesarias, los requisitos previos para poder realizar una instalación remota son:

- Debe introducir una cuenta de usuario con permisos de administración. La cuenta no tiene que tener necesariamente una contraseña. En ese caso sin embargo, la máquina de destino tendrá que estar configurada para permitir inicios de sesión de red para cuentas sin contraseña. Encontrará más información en la guía de referencia. Para instalar remotamente un servidor de subred, debe establecerse una contraseña: no está permitido un campo de contraseña vacío.
- El administrador de control de servicios en el cliente, debe ser accesible remotamente usando la cuenta de usuario especificada.
- La cuenta de usuario especificada debe tener permisos de escritura para al menos un recurso compartido de red en el cliente como C$, Admin$ o un recurso compartido personalizado. El acceso puede ser habilitado abriendo **Centro de redes y recursos compartidos** y habilitando **Compartir archivos e impresoras** en **Configuración avanzada** (Windows Vista y superiores). En Windows XP habilite **Compartir archivos e impresoras** en la sección **Excepciones** del cortafuegos de Windows.
- Cuando el cliente no forma parte de un dominio, se deben configurar además otros ajustes adicionales:
  - El **Uso compartido simple de archivos** (Windows XP) o el **Asistente para compartir** (Windows Vista/Windows Server 2008 o superiores) deberá ser deshabilitado. Por defecto está habilitado en todas las instalaciones de Windows y puede ser deshabilitado abriendo cualquier carpeta en el explorador de Windows, y haciendo clic en **Organizar** > **Opciones de carpeta** > **Ver**, y desactivando la opción respectiva.
  - Cuando el cliente está utilizando Windows Vista o superior: Abra el editor de registro en el cliente y navegue hasta la siguiente clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Añada un Nuevo valor DWORD con el nombre *LocalAccountTokenFilterPolicy* poniendo como valor *1*.

En el **Asistente de configuración del servidor** que se abre automáticamente la primera vez que se inicia G DATA Administrator, obtendrá un resumen de todos los ordenadores dados de alta en su red. Además, puede agregar y activar otros ordenadores manualmente introduciendo su nombre. El módulo **Clientes** también le permite instalar G DATA Security Client, solo tiene que seleccionar con el botón derecho del ratón los ordenadores que desee de la lista y luego, en el menú contextual que aparece, seleccionar **Instalar G DATA Security Client**. En cualquier caso, una vez seleccionados los ordenadores ambos procedimiento funcionan de igual forma. En primer lugar se abre una ventana en la que debe introducir el **nombre de usuario**, la **contraseña** y el **dominio**, con derechos de acceso a los clientes. Después de seleccionar el idioma de visualización, se abre automáticamente el **Resumen de instalación**. En la mayoría de los casos será necesario reiniciar el cliente para completar la instalación. El proceso de instalación agregará un informe al módulo **Eventos de seguridad** si es necesario el reinicio.

> La **Integración de Active Directory** le permite instalar automáticamente el software de cliente también en los nuevos ordenadores que se conecten a la red. Los requisitos previos siguen siendo los mismos.

La instalación remota se puede realizar de dos modos distintos. Cuando el cliente cumple los requisitos previos, los archivos se copian directamente y se realizan los cambios necesarios en el

registro. Si el servidor solo tiene acceso al disco duro, pero no al registro o si no se cumplen otros requisitos previos, el programa de instalación se copia en el cliente y la instalación se inicia automáticamente la próxima vez que se reinicia el ordenador.

## 2.6.2. Instalación local

Si la **instalación remota** no es posible, puede instalar G DATA Security Client de manera local en los clientes. Con el soporte de instalación de G DATA puede instalar manualmente el software cliente, o bien generar un paquete de instalación que ejecute la instalación en segundo plano (esto es ideal para distribuir el software mediante scripts de inicio de sesión).

### 2.6.2.1. Soporte de instalación de G DATA

Introduzca el soporte de instalación de G DATA en ordenador cliente y seleccione a continuación el componente **G DATA Security Client**.

Durante la instalación, debe introducir el nombre de servidor o la dirección IP del servidor en el que está instalado el G DATA ManagementServer. Es necesario indicar el nombre del servidor para que el cliente pueda comunicarse con el servidor a través de la red. De manera opcional, se puede introducir un nombre de grupo. Una vez que se haya conectado con el ManagementServer, el cliente se agregará al grupo correspondiente. Para obtener más información acerca de las reglas para introducir nombres de grupo consulte la sección **Paquete de instalación**.

Para evitar un acceso no autorizado a ManagementServer, los clientes que hayan sido implementados a través de una instalación local, necesitarán ser autorizados en G DATA Administrator en: **Clientes** > **Resumen** antes de que estén totalmente funcionales.

### 2.6.2.2. Paquete de instalación

El paquete es un único archivo ejecutable (GDClientPck.exe), con el que se puede instalar G DATA Security Client. El paquete de instalación es apropiado, por ejemplo, para distribuir el cliente mediante scripts de inicio de sesión a todos los ordenadores de un dominio o para instalarlo de manera local. El paquete incluye siempre la versión actual disponible en el servidor.

Para crear un paquete de instalación, inicie G DATA Administrator. En el menú **Organización**, haga clic en la opción **Crear paquete de instalación para clientes Windows**. Se le solicitará la siguiente información:

- **ManagementServer**: El ManagementServer al cual los clientes deberán registrarse.
- **Idioma**: El idioma de instalación.
- **Grupo**: El grupo al cual el cliente será agregado tras la instalación.

  Use una barra inclinada "/" para separar nombres de grupo en una jerarquía. Caracteres especiales en los nombres de grupos deben estar marcados. Por ejemplo, hay que duplicar cada signo de comillas que aparezca en el nombre del grupo. Si un nombre de grupo contiene una barra inclinada "/", el nombre del grupo tiene que ir entre comillas.
- **Limitar validez**: El límite de la validez de un paquete de instalación. Si el paquete se instala después de este período de tiempo, se considerará no autorizado y necesitará ser autorizado manualmente en G DATA Administrator en la opción **Clientes** > **Resumen**.

Haga clic en **Aceptar** y escoja una ubicación. G DATA Administrator generará el paquete de instalación en segundo plano. A continuación, se puede copiar al equipo de destino y ejecutarse con

permisos de administrador para poder instalar G DATA Security Client. Si la instalación debe llevarse a cabo sin la interacción del usuario, ejecute el paquete de instalación con el parámetro /§_QuietInstallation="true": *GDClientPck.exe /§_QuietInstallation="true"*.

# 2.7. Instalación de G DATA Security Client para Linux

El cliente Linux puede integrarse (igual que los clientes Windows) en la infraestructura de G DATA ManagementServer, puede gestionarse de modo centralizado a través del programa G DATA Administrator y también recibir las actualizaciones automáticas de firmas de virus. La instalación básica de cliente contiene la funcionalidad de análisis de virus bajo demanda. Opcionalmente, se pueden instalar **módulos de seguridad adicionales** para servidores Linux.

Los métodos de instalación son similares a los de los clientes Windows. La **instalación remota** a través del G DATA Administrator o la **instalación local** mediante un script de instalación.

## 2.7.1. Instalación remota

La forma más sencilla de instalar G DATA Security Client para Linux es iniciar una instalación remota desde G DATA Administrator. Los requisitos previos son los siguientes:

- Los ordenadores Linux tienen que tener un servidor SSH instalado y en ejecución.
- La cuenta de usuario desde la que se instale el cliente tiene que poder iniciar sesión en el servidor SSH usando una contraseña.
- Tiene que estar disponible la resolución de nombres DNS para el ManagementServer y el cliente.

La instalación se lleva a cabo de la siguiente forma:

1. En el módulo **Clientes** seleccione un cliente Linux. Una vez seleccionado vaya al menú **Clientes** y seleccione el comando **Instalar G DATA Security Client para Linux/Mac**.
2. Seleccione el tipo de cliente (**Cliente para Linux**).
3. Opcionalmente, seleccione uno o varios Plugins (**Samba**, **Squid** o **Sendmail/Postfix**). Los requisitos previos se describen en los correspondientes capítulos.
4. Introduzca el nombre de usuario y contraseña. La cuenta debe tener permisos root.
5. Por último haga clic en **Aceptar**. A continuación se mostrará una ventana que informa del **progreso de la instalación**.

## 2.7.2. Instalación local

Si no es posible realizar una **instalación remota**, puede instalar G DATA Security Client para Linux de manera local.

1. Inicie G DATA Administrator, en el panel **Clientes** vaya al menú **Organización** y seleccione la opción **Crear script de instalación para clientes Linux/Mac**.
2. A continuación seleccione una ubicación de almacenamiento. El script se creará en segundo plano.
3. Copie el script de instalación en el cliente, después conceda los permisos necesarios para ejecutarlo (línea de comandos: *chmod +x install-client.sh*).
4. Abra una ventana de terminal y eleve el estatus de usuario tecleando *su* e introduciendo la contraseña de root. También puede ejecutar el comando del paso 5 usando *sudo*.
5. Navegue a la carpeta en la que ha copiado el archivo y ejecútelo: *./install-client.sh -t*

*<product[,product]>*.

- *ALL*: G DATA Security Client para Linux y todos los módulos adicionales
- *WS*: G DATA Security Client para Linux
- *SMB*: los módulos Samba
- *AMAVIS*: los módulos Sendmail/Postfix
- *WEB*: los módulos Squid

6. Para evitar un acceso no autorizado a ManagementServer, los clientes que implementados a través de una instalación local, necesitarán ser autorizados en G DATA Administrator en **Clientes** > **Resumen** antes de poder ser gestionados plenamente.

## 2.7.3. Módulos adicionales

G DATA Security Client para Linux contiene módulos adicionales que proporcionan seguridad a múltiples componentes de Linux. Si selecciona módulos adicionales durante la instalación remota o local, los módulos se instalan automáticamente. De todas formas es necesario llevar a cabo configuraciones adicionales en algunos módulos antes o después de la instalación.

### 2.7.3.1. Samba

Después de instalar G DATA Security Client para Linux, la seguridad de Samba puede habilitarse añadiendo la línea *vfs objects = gdvfs* al archivo de configuración Samba (generalmente /etc/samba/smb.conf). Para proteger todos los recursos compartidos, añádalo a la sección *[global]*. Si la línea está en otra sección, la protección solo se aplicará al correspondiente recurso compartido. Tras guardar el archivo de configuración, reinicie el servicio Samba.

### 2.7.3.2. Sendmail/Postfix

El módulo Sendmail/Postfix está disponible como **módulo opcional**.

El módulo Sendmail/Postfix ha sido desarrollado como un plugin para framework Amavis. Si Amavis no está disponible en el sistema, será instalado automáticamente al instalar el módulo Sendmail/Postfix. Es necesario realizar los siguientes ajustes de configuración:

1. El módulo Sendmail/Postfix requiere un servidor de correo Sendmail/Postfix operativo.
2. Asegúrese de que el servidor de correo transfiere los mensajes de correo electrónico a Amavis. Para más Información consulte la documentación de Amavis o del servidor de correo correspondiente.
3. Asegúrese de que las comprobaciones de spam y virus están habilitadas en la configuración de Amavis. Para más información consulte la documentación de Amavis.
4. Edite el archivo de configuración /etc/gdata/amavis/mms.cfg y asegúrese de que se ha introducido el nombre de (sub) dominio del servidor de correo en *localDomains* (e.g. *mail.domain.com*).

No se recomienda el uso de una instalación existente de Amavis, ya que esto requiere muchos cambios en los archivos de configuración inmediatamente después de la instalación del módulo Sendmail/Postfix.

Una vez configurado, el módulo Sendmail/Postfix comprobará automáticamente el tráfico del correo electrónico y reportará los virus a G DATA ManagementServer. Sus ajustes pueden ser configurados a través de G DATA Administrator en el módulo **Sendmail/Postfix**.

> Advertencia: si se utiliza una versión de Amavis inferior a 2.10.0 no están disponibles todas las funciones del módulo Sendmail/Postfix. Actualice a la versión 2.10.0 de Amavis o superior antes de realizar el despliegue del módulo Sendmail/Postfix para lograr una funcionalidad completa.

#### 2.7.3.3. Squid

El módulo Squid está disponible como **módulo opcional**.

Si selecciona el módulo Squid, la instalación de G DATA Security Client para Linux instala y configura automáticamente Squid. Si Squid ya está disponible en el sistema, en primer lugar se desinstalará la versión existente.

Una vez finalizada la instalación, se debe configurar el nombre de host o la dirección IP del sevidor Squid como un servidor proxy en todos los sistemas en los que Squid se encargue de filtrar el tráfico (puerto 3128). Para habilitar el análisis del tráfico HTTPS, además se debe configurar un proxy HTTPS con el nombre de host de Squid o la dirección IP y el puerto 6789. Los certificados necesarios se encuentran en la carpeta /etc/gdata/ssl del servidor Squid y deberían importarse a todos los clientes. Si está usando sus propios certificados SSL, tienen que estar guardados en el servidor en la carpeta /etc/gdata/ssl.

> Advertencia: La instalación del servidor Squid utilizará el paquete que está disponible en el repositorio respectivo de distribución. Si esta versión de Squid es inferior a 3.3.8, los escaneos de HTTPS no estarán disponibles.

Una vez habilitado, el módulo Squid comprobará automáticamente el tráfico con una lista negra y reportará los virus a G DATA ManagementServer. Sus ajustes pueden ser configurados a través del módulo **Squid** en G DATA Administrator.

## 2.8. Instalación de G DATA Security Client para Mac

G DATA Security Client para Mac ofrece una administración centralizada de la protección de malware y es gestionado por G DATA ManagementServer, permitiendo tanto la configuración a través de G DATA Administrator como también la distribución de las actualizaciones de firmas de virus.

### 2.8.1. Instalación remota

La forma más sencilla de instalar G DATA Security Client para Mac es iniciar una instalación remota desde G DATA Administrator. Los **requisitos previos** y el procedimiento de instalación son prácticamente idénticos al procedimiento que se realiza en Linux.

1. En el módulo **Clientes**, seleccione un cliente Mac, abra el menú **Clientes** y seleccione **Instalar G DATA Security Client para Linux/Mac**.
2. En **Tipo de cliente**, seleccione **Cliente para Mac**.
3. Introduzca un usuario y contraseña. La cuenta debe tener permisos root.
4. Haga clic en **Aceptar**. A continuación se mostrará una ventana que informa del **progreso de la instalación**.

### 2.8.2. Instalación local

Si no es posible realizar una instalación remota, puede instalar G DATA Security Client para Mac de manera local.

1. Inicie G DATA Administrator, en el panel **Clientes** vaya al menú **Organización** y seleccione la

opción **Crear script de instalación para clientes Linux/Mac**.

2. A continuación seleccione una ubicación de almacenamiento. El script se creará en segundo plano.
3. Copie el script de instalación en el cliente.
4. Abra una ventana de terminal y eleve el estatus de usuario tecleando *su* e introduciendo la contraseña de root. También puede ejecutar el comando del paso 5 usando *sudo*.
5. Navegue a la carpeta en la que ha copiado el archive y ejecútelo: *./install-client.sh -t WS*.
6. Para evitar un acceso no autorizado a ManagementServer, los clientes implementados a través de una instalación local necesitarán ser autorizados en G DATA Administrator en **Clientes** > **Resumen** antes de poder ser gestionados plenamente.

# 2.9. Instalación de G DATA MailSecurity

El despliegue de G DATA MailSecurity depende del servidor que esté en uso en la red. En redes que usan Microsoft Exchange Server 2007 SP1/2010/2013/2016, MailSecurity para Exchange puede instalarse como plugin. MailSecurity para Exchange se registra automáticamente con un ManagementServer y se gestiona desde el G DATA Administrator. La solución de puerta de enlace independiente MailSecurity MailGateway es compatible con cualquier tipo de servidor. Se puede configurar desde el G DATA MailSecurity Administrator, que se instala a la vez que G DATA MailSecurity.

## 2.9.1. MailSecurity para Exchange

El asistente de instalación de MailSecurity para Exchange agrega un plugin a Microsoft Exchange Server 2007 SP1/2010/2013/2016. Se debería instalar en todos los servidores Exchange que ejecutan el Mailbox Role o el Hub Transport Role.

Para instalar MailSecurity para Exchange inserte el soporte de instalación y seleccione **G DATA MailSecurity para Exchange**. El asistente de instalación le guiará durante todo el proceso. El plugin envía informes a G DATA ManagementServer, que debe haber sido instalado previamente. Una vez instalado el plugin, inicie sesión en el ManagementServer que esté usando G DATA Administrator y configure todos los parámetros de protección en el módulo **Configuración de Exchange**.

Para evitar un acceso no autorizado a ManagementServer, los clientes de Exchange implementados a través de una instalación local, necesitarán ser autorizados en G DATA Administrator en **Clientes** > **Resumen** antes de poder ser gestionados plenamente.

## 2.9.2. MailSecurity MailGateway

MailSecurity MailGateway puede instalarse en un servidor dedicado o en el propio servidor de correo. Durante la instalación de MailSecurity MailGateway pueden usarse distintas configuraciones, dependiendo del PC en red en el que se realice la instalación. En general, lo mejor es que el gateway esté situado justo detrás de su cortafuegos de red (si existe), es decir, que el flujo de datos SMTP/POP3 procedente de Internet pase a través del cortafuegos antes de llegar al MailGateway.

Para instalar MailSecurity MailGateway, inserte el soporte de instalación y presione el botón **Instalar**. En **Instalación como puerta de enlace de correo** seleccione el componente **G DATA MailSecurity**. El asistente de instalación le guiará durante todo el proceso. Si decide instalar los componentes para la evaluación estadística, aparecerá un botón **Estadística** en el área **Estado** de G DATA MailSecurity Administrator. Esta función permite visualizar información estadística relacionada con el servidor de correo y se puede configurar en **Opciones** > **Registro**.

Independientemente del despliegue elegido, es necesario realizar varios ajustes (direcciones IP, puertos) directamente después de la instalación de MailSecurity; tanto en el servidor de correo, como en el ordenador donde se ha instalado MailSecurity. Encontrará varios ejemplos de configuraciones de puertos para diferentes escenarios de despliegue en la guía de referencia.

Dependiendo de cómo esté configurada la red, MailGateway puede utilizar varios nodos para comprobar si los correos están infectados con virus o son spam:

- Si recibe los correos directamente a través de un servidor externo, en forma de correos POP3, MailGateway se puede ajustar para revisar los correos POP3 en busca de virus antes de que los abra el usuario. Puede realizar los ajustes correspondientes en el Área **Opciones** > **Entrante (POP3)**.
- Si en la red se emplea un servidor local SMTP, MailGateway puede comprobar los correos entrantes incluso antes de que estos lleguen al servidor de correo. Puede realizar los ajustes correspondientes en el Área **Opciones** > **Entrante (SMTP)**.
- Por supuesto, MailGateway también puede examinar los correos salientes para descartar la presencia de virus antes de enviarlos a los destinatarios. Puede realizar los ajustes correspondientes en el Área **Opciones** > **Saliente (SMTP)**.

## 2.10. Instalación de G DATA Internet Security para Android

Para poder aprovechar todas las posibilidades de gestión de dispositivos móviles que ofrece G DATA Mobile Device Management, puede instalar en sus dispositivos Android la versión de G DATA Internet Security especialmente diseñada para las necesidades corporativas. G DATA Administrator ofrece posibilidades de instalación para clientes Android en el área **Clientes**. Seleccione los clientes y haga clic en el botón **Enviar enlace de instalación a los clientes móviles**; se envía un correo a los dispositivos Android correspondientes con un enlace de descarga para la app Internet Security.

Abra el correo en el dispositivo móvil y pulse el enlace para descargar el archivo APK. Tenga en cuenta que tiene que estar activada la opción **Fuentes desconocidas (Permitir la instalación de aplicaciones de orígenes distintos a Play Store)** para poder instalar el archivo. Esta opción se encuentra normalmente en el menú de sistema de Android en **Ajustes** > **Seguridad** > **Administración de dispositivos**. Después de abrir el archivo APK y confirmar las autorizaciones necesarias, se instala G DATA Internet Security y se puede abrir en el menú de apps de Android.

Para finalizar la instalación es necesario que esté habilitada la administración remota. El correo contiene un enlace que inicia automáticamente G DATA Internet Security para Android y realiza los ajustes pertinentes. También se pueden introducir las informaciones manualmente. En el menú **Ajustes** > **General** seleccione la opción **Permitir administración remota** e introduzca el nombre o la dirección IP del ManagementServer en **Dirección del servidor**. En **Nombre de dispositivo** puede asignar un nombre al dispositivo de Android, con el que G DATA Administrator pueda identificarlo. En Contraseña se debe introducir la contraseña que haya establecido en G DATA Administrator (esta contraseña se indica también en el correo con el enlace de descarga que ha recibido el dispositivo Android).

El dispositivo aparece ahora junto con los demás clientes en el módulo **Clientes** de G DATA Administrator y se puede administrar desde aquí. Si el dispositivo no aparece automáticamente en esta lista, reinicie el dispositivo para forzar el registro en G DATA ManagementServer.

# 3. G DATA ManagementServer

El G DATA ManagementServer es la pieza central de la arquitectura de G DATA y se encarga de la administración de los clientes, pide automáticamente al servidor de actualizaciones de G DATA las actualizaciones más recientes del software y de las firmas de virus, y controla la protección antivirus en la red. Para la comunicación con los clientes, G DATA ManagementServer usa el protocolo TCP/IP. Para los clientes que temporalmente no tienen conexión con G DATA ManagementServer, las tareas se recopilan automáticamente y se sincronizan cuando se restablece la comunicación. G DATA ManagementServer tiene una carpeta central de cuarentena, donde los archivos sospechosos pueden guardarse cifrados de forma segura, pueden borrarse, desinfectarse o, dado el caso, reenviarse a G DATA Security Labs. G DATA ManagementServer se gestiona mediante el **G DATA Administrator**.

> Al cerrar G DATA Administrator, G DATA ManagementServer permanece activo en segundo plano y gestiona los procesos que usted ha configurado para los clientes.

# 4. G DATA Administrator

G DATA Administrator es el software para administrar el G DATA ManagementServer. Permite la gestión de los ajustes de todos los servidores y clientes de G DATA instalados en la red. G DATA Administrator está protegido mediante contraseña y puede instalarse e iniciarse desde cualquier ordenador Windows que se encuentren dentro de la red.

Tras el primer inicio, se recomienda ejecutar el **Asistente de instalación del servidor** para probar los ajustes más importantes de G DATA Administrator y G DATA Management Server y así optimizarlos para su red.

## 4.1. Iniciar G DATA Administrator

Inicie G DATA Administrator haciendo clic en la opción **G DATA Administrator** en el grupo de programas **Inicio** > **Todos los programas** > **G DATA** > **G DATA Administrator**. En la siguiente pantalla de inicio de sesión, introduzca sus datos de acceso:

- **Idioma**: Seleccione el idioma.
- **Servidor**: Introduzca el nombre del equipo en el que se instaló G DATA ManagementServer. En la parte de la derecha, un indicador de estado mostrará si ManagementServer está listo. En caso de error, si hace clic en el indicador de estado se mostrará un archivo de registro.
- **Autenticación**
  - **Autenticación de Windows**: inicio de sesión utilizando sus credenciales de administrador en Windows.
  - **Autenticación integrada**: inicio de sesión utilizando el sistema de autenticación de G DATA ManagementServer. Las cuentas de autenticación integradas pueden establecerse usando la función **Administrar usuarios**.
- **Nombre de usuario**: introduzca su usuario de administrador de Windows o su nombre de usuario de autenticación integrada.
- **Contraseña**: introduzca su contraseña de administrador de Windows o su contraseña de autenticación integrada.

Una vez introducidos los datos de acceso, haga clic en **Aceptar**.

Haga clic en la flecha situada al lado del menú signo de interrogación para abrir dos opciones adicionales. **Acerca del G DATA Administrator** muestra información de versión. **Restablecer ajustes** le permite restablecer todos los ajustes relacionados con el uso de G DATA Administrator (p. ej. tamaño de la ventana).

## 4.2. Usar G DATA Administrator

La interfaz de G DATA Administrator está organizada de la siguiente manera:

- El panel de **Resumen**, proporciona información del estado y accesos directos a elementos tales como informes, logs y actualizaciones.
- El panel **Clientes/ManagementServers** muestra todos los ManagementServers y clientes que pueden ser administrados.
- La configuración puede ser llevada a cabo utilizando los **módulos** accesibles desde áreas dedicadas en la parte de la derecha. La disponibilidad de los módulos depende de la selección actual en el panel **Clientes/ManagementServers** y del **producto** que usted disponga.

- La barra de menús ofrece acceso a los ajustes generales, y también a menús adicionales que solo se muestran cuando se seleccionan módulos concretos:
  - **Admin**: iniciar el **Asistente de configuración del servidor** y también cerrar G DATA Administrator.
  - **Organización** (consulte **Clientes/ManagementServers** > **Clientes** > **Organización**)
  - **Clientes** (consulte **Clientes** > **Resumen**)
  - **Órdenes** (consulte **Órdenes**)
  - **Cortafuegos** (consulte **Cortafuegos** > **Resumen**)
  - **Eventos de seguridad** (consulte **Registros** > **Eventos de seguridad**)
  - **Monitoreo de red**: inicia G DATA ActionCenter para usar los **módulos opcionales** de Monitoreo de red.
  - **Vista**: muestra/oculta el panel **Resumen**.
  - **?**: muestra el archivo de ayuda y la información de versión.

### 4.2.1. Resumen

El panel de resumen ofrece una vista general rápida de los informes no leídos, archivos de log e información de estado. Haciendo clic en los iconos, se accede a los respectivos módulos con ajustes de filtros preconfigurados que muestran solo los datos solicitados. La disponibilidad de los iconos depende de la **solución** que haya contratado.

- **Información**: información general e informes de error.
- **Seguridad**: informes de infección.
- **Solicitar**: solicitudes de PolicyManager, PatchManager y módulos de cortafuegos y control de apps de Android.
- **Parches**: parches de alta prioridad que todavía no han sido instalados.
- **Registros de clientes**: logs del cliente, tales como cambio en los ajustes e información del estado de tareas.
- **Registros de servidores**: información de MangementServer e informes de error.
- **Postfix**: informes del módulo Sendmail/Postfix.
- **Squid**: informes del módulo Squid.
- **Exchange**: informes de MailSecurity para Exchange.
- **Clientes no autorizados**: clientes que se han conectado al ManagementServer pero no has sido autorizados aún por el administrador.
- **Servidores no autorizados**: servidores subnet que se han conectado al ManagementServer pero no han sido autorizados aún por el administrador.
- **Clientes de Exchange no autorizados**: clientes Exchange que se han conectado al ManagementServer pero no has sido autorizados aún por el administrador.
- **Firmas**: información de versión de las firmas de virus en ManagementServer.
- **Programa**: información de versión de ManagementServer.

### 4.2.2. Clientes/ManagementServers

En el panel de gestión Clientes/ManagementServers se muestran todos los clientes y servidores gestionados por G DATA Administrator. Seleccione el panel **Clientes** para visualizar los clientes o el

panel **ManagementServers** para visualizar los distintos ManagementServers (servidor principal, secundario y servidor de subred).

Clientes y los ManagementServers se visualizan en una lista basada en nodos. Como en Windows Explorer, los nodos que contienen nodos subordinados, aparecen con un pequeño símbolo más (+). Si hace clic en ellos, la estructura se expande y habilita la vista de los nodos subyacentes. Haciendo clic en el símbolo menos (-), la lista se contrae.

En la barra de herramientas, puede ver los comandos más importantes para los clientes y para los servidores de administración, algunos de los cuales también se muestran en el menú **Organización**. La disponibilidad de estas opciones depende de los clientes/servidores que hayan sido seleccionados:

- **Actualizar**
- **Ampliar/reducir todos**: expandir o contraer todos los elementos del árbol de red.
- **Mostrar clientes desactivados**
- **Crear grupo nuevo**
- **Eliminar**
- **Activar cliente**: agregue un cliente Windows o Linux al área **Clientes** introduciendo el nombre o la dirección IP.
- **Resumen de instalación**
- **Enviar enlace de instalación a los clientes móviles**: envía un enlace de instalación a los clientes Android y iOS.

### 4.2.2.1. Clientes

El área Clientes lista los distintos tipos de clientes en cinco nodos de nivel superior:

- **Todos los servidores de administración**: Windows, Linux, Mac y clientes Android.
- **Exchange**: clientes con el plugin de MailSecurity para Exchange.
- **Sendmail/Postfix**: clientes Linux con el módulo Sendmail/Postfix.
- **Squid**: clientes Linux con el módulo Squid.
- **Administración de dispositivos móviles iOS**: todos los dispositivos iOS que se están gestionando.

Antes de que se puedan administrar clientes con G DATA Administrator, estos deben agregarse y activarse en el área Clientes. Existen varias posibilidades de agregarlos dependiendo del tipo de cliente, del tamaño y de la configuración de la red:

- Windows: use el **Asistente de configuración del servidor**, la ventana de diálogo **Búsqueda de ordenador**, la barra de herramientas **Activar cliente** o la **compatibilidad con Active Directory** para agregar clientes Windows, después implemente **G DATA Security Client**.
- Linux: use la barra de herramientas **Activar cliente** para agregar clientes Linux, después implemente **G DATA Security Client para Linux**.
- Mac: use la barra de herramientas **Activar cliente** para agregar clientes Mac, después implemente **G DATA Security Client para Mac**.
- MailSecurity para Exchange: implemente **G DATA MailSecurity para Exchange**. El cliente Exchange se agregará automáticamente.
- Android: use la barra de herramientas **Enviar enlace de instalación a los clientes móviles**

para enviar un correo electrónico al cliente. Este inicia la Implementación de **G DATA Internet Security para Android**. El cliente Android se agrega después automáticamente.

- iOS: introduzca sus datos de acceso para G DATA ActionCenter en el módulo de **ActionCenter**. Use la barra de herramientas **Enviar enlace de instalación a los clientes móviles** para enviar un correo electrónico al cliente. Después de que el usuario final haya aceptado los ajustes (Device Management configuration), el cliente iOS client se agregará automáticamente.

Los siguientes tipos de iconos se muestran en el área de clientes:


Red


ManagementServer


Grupo


Grupo (Active Directory)


Cliente


Cliente (desactivado)


Cliente portátil


Cliente móvil


Servidor Linux


Cliente Linux


Cliente MailSecurity para Exchange


Dispositivos no seleccionables. Entre ellos se encuentra, por ejemplo, la impresora de red.

Cuando se selecciona un cliente, grupo o ManagementServer, los correspondientes **módulos del cliente** serán mostrados en el área de **módulos**. Dependiendo del tipo de nodo que se seleccione, estarán disponibles unos módulos específicos. Por ejemplo, cuando se selecciona un ordenador cliente se activará la opción **Ajustes de cliente**. En cambio, en clientes móviles puede acceder a los **Ajustes móviles**.

En esta área puede importar y exportar los ajustes. Haga clic derecho en un cliente y seleccione **Exportar ajustes** para guardar la configuración de los **Ajustes de cliente** y del módulo **PolicyManager** en un archivo .dbdat. Para importar ajustes, marque un cliente o un grupo, seleccione **Importar ajustes** y defina el alcance y el archivo de configuración deseados.

### Organización

Cuando se ha seleccionado el área Clientes, se muestra **Organización** en la barra de menús, ofreciendo acceso a los ajustes relacionados con la organización del cliente.

### Actualizar

Con la función **Actualizar** puede actualizar la lista en el panel de **Clientes/ManagementServers**.

### Mostrar clientes desactivados

Los clientes que no están activados pueden hacerse visibles con esta función. Los clientes desactivados se representan mediante iconos de color gris o atenuados.

### Crear grupo nuevo

Mediante este comando se puede crear un nuevo grupo y asignarle varios clientes, de esta forma es posible aplicar ajustes a varios clientes a la vez. También se pueden definir fácilmente diferentes zonas de seguridad, ya que todos les ajustes se pueden establecer tanto para clientes individuales

como para grupos completos. Seleccione un ManagementServer o un grupo y haga clic en la opción **Crear grupo**. Después de seleccionar esta opción y poner un nombre al grupo, los clientes pueden asignarse al nuevo grupo mediante el método de arrastrar y soltar.

Para mover muchos clientes a un mismo grupo use el módulo **Clientes** > **Resumen**. Seleccione los clientes que desee mover, haga clic derecho y elija **Mover clientes**.

### Editar grupo

Esta opción abre un cuadro de diálogo en el que se pueden agregar o eliminar clientes del grupo mediante los botones **Agregar** y **Eliminar**. Solo está disponible cuando se ha seleccionado un grupo en el área **Clientes**.

### Eliminar

Use este comando para eliminar clientes individuales de la lista de clientes. La eliminación del cliente de la lista, no implica la desinstalación de G DATA Security Client.

> Para eliminar un grupo, se tienen o bien que desactivar todos los clientes que estén incluidos en él, o bien moverlos a otros grupos, según proceda. Solo se pueden eliminar los grupos que estén vacíos.

### Búsqueda de ordenador

La ventana **Búsqueda de ordenador** puede utilizarse para agregar y activar clientes en el área **Clientes**. Los clientes se pueden encontrar mediante la dirección IP y activarse directamente a través de la ventana de diálogo.

En la ventana Buscar ordenador pueden contactarse todos los ordenadores en un determinado rango de IP. El rango puede definirse mediante una **Dirección IP inicial** y una **Dirección IP final** (p.ej. 192.168.0.1 y 192.168.0.255) o mediante la dirección de subred (notación CIDR, p.ej. 192.168.0.0/24). Para asegurarse de que solo se listan los clientes disponibles, seleccione la opción **Buscar solo ordenadores accesibles (ping)**. Ahora haga clic en **Iniciar búsqueda**, para iniciar la búsqueda en la red. A continuación se listan los ordenadores a medida que se van encontrando. Si el proceso de búsqueda tarda demasiado, puede cancelar la búsqueda haciendo clic en **Cancelar búsqueda**.

A continuación se listan todos los ordenadores que responden a la comprobación de IP, incluyendo su dirección IP y nombre de equipo. Con el botón **Activar** pueden agregarse los clientes correspondientes al área **Clientes**. En el resultado de la búsqueda también pueden desactivarse los clientes activados haciendo clic en **Desactivar**.

### Asistente de reglas

Cuando los clientes se conectan a ManagementServer por primera vez, se agregan automáticamente al grupo de **Nuevos clientes** si no se ha definido ningún grupo cuando se activó el cliente o cuando se creó el paquete de instalación. El asistente de reglas puede ser usado para crear reglas que muevan nuevos clientes a los grupos predefinidos de manera regular.

Las reglas se gestionan utilizando los botones **Nuevo**, **Editar** y **Eliminar** y las flechas de dirección situadas junto a la lista de reglas. Los botones **Importar** y **Exportar** se usan para importar/exportar las reglas como archivos .json.

En **Configuración**, se definen los ajustes principales para la ejecución de reglas:

- **Horario**: las reglas son ejecutadas **Cada hora**, **Diariamente** o **Semanal**.
- **Fecha**: definir la hora exacta en el que las reglas serán ejecutadas.

- **Aplicar configuración del grupo**: cuando se mueven clientes a un grupo, reciben de forma automática los ajustes de ese nuevo grupo.
- **Mover solo clientes del grupo "Clientes nuevos"**: las reglas solo se aplican a los clientes del grupo **Clientes nuevos**. Si esta opción no está seleccionada, las reglas se aplican a todos los clientes. Esto puede causar que los clientes puedan moverse múltiples veces y por lo general debe dejarse seleccionada.
- **Ejecutar ahora**: ejecuta las reglas inmediatamente.

Utilizando una serie de ajustes, se pueden definir reglas que automáticamente muevan clientes entre grupos.

- **Tipo de regla**: seleccionar si los clientes son seleccionados por **Nombre del ordenador**, **Dirección IP**, **Dominio** o **Puerta de enlace estándar**.
- **Comodín de cliente**: introduzca la cadena de búsqueda que será usada para seleccionar clientes. Se pueden utilizar comodines. Por ejemplo, introduzca *Ventas_** para seleccionar todos los clientes con el prefijo Ventas_ (cuando se esté utilizando el ajuste de **Nombre del ordenador**) o *192.168.0.[1-100]* para seleccionar todos los clientes con direcciones IP entre 192.168.0.1 y 192.168.0.100 (en caso de que se esté utilizando el ajuste de **Dirección IP**).
- **Tipo de cliente**: seleccione que tipo de clientes se van a mover (**Todos**, **Estación de trabajo**, **Servidor**, **Dispositivo Android** u **Ordenador portátil**).
- **Grupos**: introduzca uno o más grupos o selecciónelos haciendo doble clic en un grupo en la vista de árbol. Cuando se han introducido varios grupos, los clientes seleccionados se dividirán por igual entre los grupos.

### Crear paquete de instalación para clientes Windows

Mediante esta función es posible crear un paquete de instalación para G DATA Security Client. Con este paquete de instalación se puede instalar G DATA Security Client localmente. Para obtener más información, consulte el capítulo **instalación local**.

### Crear script de instalación para clientes Linux/Mac

Mediante esta función es posible crear un script de instalación para G DATA Security Client para Linux y G DATA Security Client para Mac. Con este script de instalación se puede instalar G DATA Security Client localmente. Para obtener más Información, consulte los capítulos **Instalación local (Linux)** e **Instalación local (Mac)**.

### Resumen de instalación

Para realizar un seguimiento del progreso de la instalación, puede utilizar la ventana Resumen de instalación. Esta se abre automáticamente cuando se añade una tarea de instalación remota, pero también puede abrirse mediante el botón Resumen de instalación en la barra de herramientas del panel de **Clientes/ManagementServers**.

El Resumen de instalación muestra todas las tareas de instalación remota, finalizadas y no finalizadas. La columna **Tipo** indica el tipo de instalación (G DATA Security Client, G DATA Firewall, G DATA Internet Security para Android o servidor de subred). Una vez finalizada la instalación remota, se actualiza la columna de **Estado**. En la columna **Siguiente intento de instalación** se muestra la hora a la que se iniciará la instalación remota en los clientes que han sido agregados a través de la **sincronización con Active Directory**.

Las siguientes opciones están disponibles tras hacer clic derecho en una de las entradas:

- **Actualizar**: actualiza la lista.
- **Eliminar registro**: elimina de la lista la entrada seleccionada.
- **Mostrar informe de instalación**: muestra el informe de instalación de la entrada seleccionada.
- **Intentar de nuevo**: vuelve a intentar la instalación tras una instalación fallida.

### Enviar enlace de instalación a los clientes móviles

Puede enviar un correo electrónico de instalación a los dispositivos móviles desde la ventana Enviar enlace de instalación a los clientes móviles. Dependiendo del elemento seleccionado en el área **Clientes**, la ventana mostrará opciones para clientes **Android** o **iOS**.

Los usuarios pueden **instalar G DATA Internet Security para Android** cuando abren el correo electrónico en el cliente móvil (en el caso de clientes Android) o habilitar Device Management (en el caso de clientes iOS). Una vez finalizado el proceso correspondiente, el cliente(s) móvil aparecerá en el área **Clientes**.

> Para enviar un enlace de instalación a los clientes móviles, el G DATA ManagementServer tiene que poder enviar correos electrónicos. Asegúrese de introducir sus datos de acceso a un servidor SMTP en **Configuración general** > **Correo electrónico** > **Configuración de correo**.

### Clientes Android

Para enviar un enlace de instalación a los clientes Android, deberá introducirse la siguiente información:

- **Contraseña**: si todavía no ha introducido una contraseña de autenticación para dispositivos móviles en **Ajustes generales** > **Android** > **Autenticación para clientes Android**, puede hacerlo aquí.
- **Destinatarios**: introduzca una o varias direcciones de correo electrónico, separadas por saltos de línea o comas.
- **Asunto**: introduzca el asunto del correo electrónico de instalación.
- **Contenido**: introduzca el cuerpo de mensaje del correo electrónico de instalación. Debe contener los marcadores de posición preconfigurados para los enlaces de instalación.

Haga clic en **OK**, para enviar el enlace de instalación.

### Clientes iOS

Cuando se realiza el despliegue de Device Management en clientes iOS, hay una serie de ajustes que le permiten personalizar el aspecto de la solicitud de Device Management al usuario final:

- **Nombre**: introduzca el nombre del Device Management.
- **Descripción**: introduzca la descripción del Device Management.
- **Organización**: introduzca el nombre de su organización.
- **Acuerdo de licencia de usuario final**: introduzca un Acuerdo de licencia de usuario final.
- **Destinatarios**: introduzca una dirección de correo electrónico; si introduce varias sepárelas con saltos de líneas o comas.

Haga clic en **Aceptar** para enviar el enlace de instalación.

> Antes de enviar el enlace de instalación a un dispositivo iOS, asegúrese de que ha introducido sus datos de acceso en el módulo de **ActionCenter**.

**Active Directory**
La integración de G DATA Administrator con Active Directory permite importar todos los objetos de las unidades organizativas de los dominios locales. Para ello hay que crear un nuevo grupo en G DATA Administrator. Haga clic derecho sobre el nuevo grupo creado y seleccione la opción **Asignar entrada de Active Directory al grupo**. En la ventana de diálogo que se abre, seleccione la opción **Asignar a un grupo en Active Directory** e introduzca el servidor LDAP. El botón **Seleccionar** ofrece una selección de servidores disponibles. También es posible conectarse con otro dominio mediante el botón **Agregar**. Con la opción **Instalar automáticamente G DATA Security Client en los nuevos ordenadores agregados**, se iniciará la instalación remota de G DATA Security Client en cada ordenador que se añada al dominio de Active Directory, siempre que cumpla con los **requisitos mínimos para una instalación remota**. Introduzca el **Nombre de usuario** y **Contraseña** de una cuenta de dominio con suficientes permisos en los clientes, así como el **Idioma de instalación**.

De forma predeterminada, G DATA ManagementServer compara sus datos con Active Directory cada seis horas. Este valor puede modificarse en **Configuración general** > **Sincronización**.

### 4.2.2.2. ManagementServers

Los siguientes tipos de ManagementServers se muestran en la vista ManagementServers:

- Todos los servidores
- Servidor principal
- Servidor secundario
- Servidor de subred

Cuando se selecciona un servidor, los correspondientes **módulos de servidor** se mostrarán en el área de **módulos**.

## 4.2.3. Módulos

Dependiendo de la selección actual en el panel de **Clientes/ManagementServers**, tanto los **módulos de cliente** como los **módulos de servidor** se mostrarán en la parte derecha de la ventana. Para abrir un módulo haga clic en el módulo correspondiente.

La mayoría de los módulos disponen de una barra de herramientas. Además de las funciones específicas del módulo, se mostrarán generalmente los siguientes botones:

- **Actualizar**: actualiza el listado o vista actual.
- **Eliminar**: elimina el/los elemento(s) seleccionado(s).
- **Imprimir**: imprimir los elementos (seleccionados) del módulo actual.
- **Vista preliminar**: muestra una previsualización de la impresión.
- **Periodo**: limita los elementos mostrados a un periodo de tiempo especificado.

Para la mayoría de los módulos hay disponibles opciones generales para editar el diseño y el contenido de las listas en el área de información:

- Para ordenar un listado, haga clic en los encabezados de cada columna.
- Para añadir o eliminar columnas de la lista mostrada, haga clic con el botón derecho en cualquier encabezado de columna, haga clic en **Seleccionar columnas** y (de) seleccione las columnas que deberán ser mostradas.
- Se puede reducir el número de entradas por página. Solo hay que seleccionar el máximo

**Número por página** en el margen inferior derecho de la interfaz del programa.

- Para introducir filtros de texto, pulse el icono de filtro en los títulos de las columnas e introduzca sus criterios de filtrado.
- Arrastre uno o varios títulos de columna a la barra gris que está situada encima de los mismos, para crear un grupo basado en esas columnas. Los grupos se pueden generar y organizar jerárquicamente de distintos modos para crear vistas diferentes.

Los ajustes que se realizan en cada módulo siempre se aplican a los clientes, servidores o grupos marcados en el panel de **Clients/ManagementServers**. Si un ManagementServer o grupo ha sido seleccionado, los clientes o grupos correspondientes pueden tener establecidos valores diferentes para un ajuste determinado, en cuyo caso se marcará como tal. Cuando se guarden los ajustes, cada cliente conservará su propio valor. Solo si el valor se cambia, el cambio se aplicará a todos los clientes seleccionados. Los clientes o grupos subordinados que tengan ajustes diferentes a los ajustes del grupo serán mostrados por nombre en el panel **Clientes/grupos con configuración diferente**. Seleccione un cliente y haga clic en **Mostrar configuración** para seleccionar el mismo en el panel **Clientes/ManagementServers** y mostrar sus ajustes, o haga clic en **Restablecer a la configuración del grupo** para aplicar los ajustes del grupo a ese cliente.

Algunas opciones de administración están bloqueadas para clientes Linux o Mac. Los ajustes no disponibles para clientes Linux o Mac se resaltan en color verde.

Los ajustes solo se guardan y se transfieren a los clientes/servidores seleccionados, cuando se pulsa el botón **Aplicar**. En la mayoría de los módulos, en la parte inferior, se muestra en **Información** si las modificaciones realizadas se han aplicado con éxito. Haga clic en el botón **Descartar** para conservar la configuración actual sin aceptar los cambios.

## 4.3. Módulos del cliente

Los módulos del cliente pueden ser usados para configurar los clientes o grupos de clientes que han sido seleccionados en el área **Clientes** del panel **Clientes/ManagementServers**.

### 4.3.1. Panel de control

En el módulo panel de control encontrará información sobre el estado actual de los clientes en la red.

En **Estado de G DATA Security** puede realizar todos los ajustes básicos de seguridad para los clientes o grupos que hayan sido marcados en el panel **Clientes** e implementar cambios de inmediato en caso de ser necesario.

- Siempre y cuando la red esté configurada de manera óptima para la protección contra los virus informáticos, se verá un icono verde a la izquierda de todas las entradas que figuran aquí.
- Pero si al menos uno de los componentes presenta problemas de seguridad (por ejemplo, el vigilante está desconectado o las firmas de virus están desfasadas), aparecerá un símbolo de advertencia.
- Cuando se abre la interfaz del programa de G DATA, algunos iconos pueden mostrarse brevemente en modo de información. Esto no significa que la red esté desprotegida en ese momento. Se trata simplemente de una comprobación interna del estado de la protección antivirus. En ese momento, G DATA Administrator consulta la base de datos de G DATA ManagementServer.

Haciendo clic en la entrada correspondiente se pueden efectuar cambios en los ajustes directamente

o abrir el módulo correspondiente. Tan pronto haya optimizado los ajustes de un componente con un símbolo de advertencia, el símbolo volverá a mostrar el color verde.

El gráfico en **Conexiones del cliente** muestra un resumen de las conexiones que se han establecido con G DATA ManagementServer. Es importante que todos los clientes se conecten regularmente con G DATA ManagementServer. Debe observarse especialmente a los clientes que aparezcan en la **Lista de los 10 clientes más frecuentes - Infecciones rechazadas**. En ocasiones, la aparición de uno o más clientes en esta área es un indicador de que debe advertirse al usuario del cliente sobre un posible problema o de que se deben tomar medidas técnicas. Si las infecciones se están produciendo como consecuencia de un mal uso, sería recomendable, por ejemplo, el uso del **PolicyManager** (disponible en la solución de seguridad **G DATA Endpoint Protection Business**). **Estado de informe** muestra un resumen visual de la cantidad de infecciones, consultas y errores ocurridos en su red durante un periodo de tiempo configurable.

## 4.3.2. Clientes

En el módulo Clientes se puede verificar si los clientes funcionan correctamente y si las firmas de virus y archivos de programa están completamente actualizados.

### 4.3.2.1. Resumen

En este panel general se obtiene un resumen de todos los clientes administrados que, a su vez, pueden gestionarse también aquí. En la columna **Estado de seguridad** puede fácilmente hacer un seguimiento del estado actual de la seguridad de cada cliente.

En la barra de iconos encima de la lista tiene disponibles las siguientes opciones para la administración de los clientes:

- **Actualizar**
- **Eliminar**: elimina un cliente de la lista de clientes. Esta opción no desinstala el G DATA Security Client del cliente, y por tanto solo debería usarse para aquellos clientes que se han dado de baja o se han eliminado de la red. Si por error se elimina un cliente activo de la lista, volverá a mostrarse tan pronto se conecte con el ManagementServer (sin embargo, se pierden los ajustes específicos de grupo).
- **Imprimir**
- **Vista preliminar**
- **Instalar G DATA Security Client**
- **Desinstalar G DATA Security Client**
- **Actualizar base de datos de virus ahora**: actualiza la base de datos de virus del cliente con los archivos del G DATA ManagementServer.
- **Actualizar base de datos de virus automáticamente**: activa la actualización automática de la base de datos de virus. Los clientes comprueban periódicamente si hay firmas de virus actualizadas en G DATA ManagementServer y efectúan la actualización automáticamente.
- **Actualizar archivos de programa ahora**: actualiza los archivos de programa en el cliente con los archivos del G DATA ManagementServer. Tras la actualización del programa es posible que haya que reiniciar el cliente.
- **Actualizar archivos de programa automáticamente**: activa la actualización automática de los archivos de programa. Los clientes comprueban periódicamente si hay una nueva versión en el G DATA ManagementServer y efectúan la actualización automáticamente.

### Resumen de instalación

Si se selecciona la opción Resumen, en la barra de menús aparece una opción adicional llamada **Clientes**. El menú de **Clientes** y el menú contextual del botón derecho ofrecen las siguientes funciones:

- Instalar G DATA Security Client
- Instalar G DATA Security Client para Linux
- Desinstalar G DATA Security Client
- Resumen de instalación
- **Restablecer ajustes de grupos**: restablece los ajustes de seguridad del cliente/clientes seleccionados a la configuración de grupo
- **Mover clientes**: esta función le permite mover el/los cliente(s) seleccionado(s) a un grupo ya existente. Al seleccionar esta opción, todos los grupos existentes se muestran en una nueva ventana. Para mover el cliente a un grupo, seleccione el grupo que desee y haga clic en **Aceptar**.
- **Modificar EULA asignado**: asigna un EULA definido previamente al/los cliente(s) seleccionado(s) (solo para clientes Android).
- **Eliminar EULA asignado**: elimina un EULA definido previamente al/los cliente(s) seleccionado(s) (solo para clientes Android).
- Administración de EULA
- **Asignar servidor G DATA**: si tiene la posibilidad de asignar clientes a servidores de subred concretos con la función **Servidores** > **Resumen**, tendrá también la opción de realizar esta operación en el menú contextual.
- **Actualizar base de datos de virus ahora**
- **Actualizar base de datos de virus automáticamente**
- **Actualizar archivos de programa ahora**
- **Actualizar archivos de programa automáticamente**
- **Reinicio tras la actualización de los archivos de programa**: aquí se define la forma de reaccionar del cliente después de la actualización de los archivos de programa:
  - **Mostrar ventana informativa en el cliente**: informa al usuario que debe reiniciar su equipo en un momento determinado.
  - **Generar informe**: crea un informe en el módulo **Eventos de seguridad**.
  - **Reiniciar sin consultar**: forzar automáticamente un reinicio
- **Eliminar** (solo en el menú contextual)
- **Conceder autorización** (solo en el menú contextual): autorizar el/los cliente(s) seleccionado(s). Para evitar un acceso no autorizado a ManagementServer, los clientes que se implementen a través de una instalación local, necesitarán ser autorizados antes de que sean completamente funcionales.
- **Propiedades** (solo en el menú contextual): mostrar las propiedades del cliente seleccionado (General, información de la red, riesgos de seguridad y hardware)

**Instalar G DATA Security Client**
Seleccione la opción **Instalar G DATA Security Client** para ejecutar la **instalación remota** de G DATA Security Client en los ordenadores seleccionados.

> Para poder acceder a los clientes desactivados, deben visualizarse como activos en la lista de clientes. Al utilizar la función **Instalar G DATA Security Client** el programa se lo indicará, si es necesario, y le permitirá visualizar los clientes desactivados.

Si la instalación remota no es posible, puede también ejecutar una **instalación local** en el ordenador cliente con el soporte de instalación de G DATA o con un paquete de instalación de cliente.

**Desinstalar G DATA Security Client**
Con esta función puede desinstalar G DATA Security Client de forma remota. Antes de iniciarse la desinstalación, puede seleccionar los componentes que deben conservarse. Es posible desinstalar el software de cliente, pero mantener guardados en el servidor los informes, las tareas, los mensajes o los archivos comprimidos de copia de seguridad asignados a este cliente. Seleccione los componentes que desea eliminar y haga clic en **Aceptar** para iniciar la desinstalación. Para eliminar íntegramente el programa hay que reiniciar el cliente.

También es posible desinstalar el cliente localmente. Para ello, son necesarios permisos de administrador. En el directorio %ProgramData%\G Data\client ejecute *setup.exe* para iniciar la desinstalación. Para finalizar el proceso es necesario reiniciar el ordenador. Para desinstalar clientes Linux, use el script gdata_uninstall.sh, que normalmente se encuentra en /usr/sbin/ gdata_uninstall.sh.

**Administrar EULAs**
En la ventana Administrar EULAs puede agregar, editar y eliminar acuerdos de licencia de usuario final (EULAs) para dispositivos Android. Mediante la opción correspondiente en el menú de clientes puede asignarse a cada dispositivo Android el EULA respectivo, para asegurarse de que el cliente final ha sido informado y está de acuerdo con el despliegue de la app de G DATA Internet Security para Android.

En la ventana Administrar EULAs se listan todos los acuerdos de licencia disponibles. Para añadir otros, haga clic en **Agregar**. En la ventana **Crear EULA** puede definir el **Nombre**, **Idioma** y **Contenido** del acuerdo. Haciendo clic en **Aceptar**, se agrega el acuerdo a la lista.

Para editar un EULA existente, selecciónelo de la lista y a continuación haga clic en **Modificar**. Para eliminar un EULA, selecciónelo y haga clic en **Eliminar**.

## 4.3.2.2. Software

El inventario de software le permite supervisar el uso del software en toda la red. El programa se puede agregar a una lista blanca o negra para apoyar la gestión del software en la red.

Para gestionar el inventario tiene a su disposición los siguientes botones:

- **Actualizar**
- **Imprimir**
- **Vista preliminar**
- **Mostrar todos**: muestra todos y cada uno de los programas instalados en los clientes de la red.
- **Mostrar solo el software de la lista negra**: visualice solo el software agregado a la lista negra.
- **Mostrar solo el software que no esté en la lista blanca**: visualice el software instalado en los clientes de red que no haya sido verificado, ni clasificado por el administrador de red. De esta forma es posible agregar software fácilmente a la lista blanca o negra con un simple clic

derecho del ratón.

En el área de listas figura una lista del software instalado para todos los clientes en el área **Clientes**. Para añadir contenido a la lista negra o blanca, pulse el botón **Lista negra a nivel de toda la red** o **Lista blanca a nivel de toda la red** y, en la ventana que se abre a continuación, seleccione el botón **Agregar**. La opción **Detectar características** le permite seleccionar los programas que desee añadir a la lista negra o a la blanca, así como introducir los atributos. Para convertir un atributo en una regla, solo hay que activar la marca de verificación en la casilla correspondiente. De este modo, por ejemplo, se puede colocar el software de determinados fabricantes en la lista blanca o negra o solo versiones específicas de un programa. Si dispone de los datos necesarios, puede también introducir software directamente en la lista blanca o negra indicando sus características (sin necesidad de usar **Detectar características**).

El inventario de software está filtrado por defecto para mostrar solo las aplicaciones instaladas actualmente. Para mostrar todas las aplicaciones, incluyendo aquellas que estuvieron instaladas anteriormente, haga clic en **Restablecer los filtros**.

### 4.3.2.3. Hardware

En el inventario del hardware obtendrá información sobre el hardware empleado en los clientes.

Para gestionar el inventario tiene a su disposición los siguientes botones:

- **Actualizar**
- **Imprimir**
- **Vista preliminar**

### 4.3.2.4. Mensajes

El administrador puede enviar mensajes a clientes individuales o a grupos de clientes e informar a los usuarios de forma rápida y sencilla. Los mensajes aparecen en una pequeña ventana emergente en la parte inferior derecha del escritorio del ordenador cliente.

Para crear un nuevo mensaje, solo tiene que pulsar con el botón derecho del ratón en la vista de columnas y seleccionar **Enviar mensaje**. En el cuadro de diálogo contextual que se abre a continuación se pueden seleccionar o deseleccionar mediante una marca de verificación los clientes a los que desee enviar el mensaje. Si desea que un mensaje solo lo reciban usuarios determinados de un ordenador cliente, introduzca entonces el nombre de usuario en el apartado **Cuenta de usuario**. Escriba ahora el mensaje en el campo **Mensaje** y pulse a continuación el botón **Aceptar**.

## 4.3.3. Clientes (iOS)

Si ha seleccionado uno o varios clientes iOS en el panel **Clientes**, el modulo Clientes solo mostrará destalles relacionados con los clientes iOS seleccionados:

- **Cliente**: nombre del dispositivo.
- **Estado de seguridad**: muestra el estado de seguridad actual y muestra una advertencia si no se ha asignado un **perfil** o si el perfil aún está pendiente.
- **Perfil**: muestra el **perfil** asignado actualmente. Para cambiar un perfil de la lista, selecciónelo o seleccione - Ningún perfil – para eliminar el perfil actual.
- **Último acceso**: detalles de las conexiones más recientes entre el cliente iOS client y G DATA ActionCenter.

- **IMEI**: número de identificación del dispositivo (IMEI).
- **Capacidad**: capacidad de almacenamiento del dispositivo (GB).
- **Versión**: número de versión iOS.
- **Número de teléfono**: número de teléfono del dispositivo.
- **Correo electrónico**: dirección de correo electrónico al que se envió el enlace de instalación.
- **Nombre del producto**: nombre modelo del dispositivo.

Al hacer clic derecho en un cliente aparece el menú contextual con las siguientes opciones:

- **Eliminar administración del dispositivo**: deshabilita la gestión de dispositivos móviles en el dispositivo.
- **Eliminar**: elimina el dispositivo de la lista. Antes de eliminarlo, use **Eliminar administración del dispositivo** para deshabilitar la gestión de dispositivos móviles.
- **Volver a enviar el correo electrónico para la activación**: reenvía el enlace de instalación a los clientes con una instalación MDM inactiva o pendiente.

## 4.3.4. Ajustes de cliente

En el módulo Ajustes de cliente puede gestionar los ajustes para clientes individuales o grupos de clientes. Las opciones General, Vigilante, Correo electrónico, Web y AntiSpam le permiten configurar de forma exhaustiva la protección de los clientes en red.

## 4.3.4.1. General

En este módulo se pueden editar los ajustes básicos de los clientes seleccionados.

### G DATA Security Client

En el área G DATA Security Client se encuentran las funcionalidades básicas del cliente.

- **Comentario**: aquí puede indicar si lo desea información complementaria acerca del cliente.
- **Icono en la barra de tareas**: aquí puede elegir cuando desea que se muestre el icono de cliente en la barra de tareas: **No mostrar nunca**, **Mostrar solo en la primera sesión** (para servidores de terminal y cambio rápido de usuario de Windows) o **Mostrar siempre**. Si no se muestra el icono la funcionalidad de Security Client es muy limitada (por ejemplo, no es posible usar el **Escaneo en modo reposo** y el usuario no tiene acceso a las **Funciones de cliente**).
- **Asignado a**: por defecto, los clientes son asignados ManagementServer principal. La lista desplegable muestra el ManagementServer principal y sus servidores de subred y puede ser usada para asignar cómodamente un cliente a un servidor (de subred) específico.

### Actualizaciones

En el área Actualizaciones puede configurar las actualizaciones de las firmas de virus y de los archivos de programa.

- **Actualizar firmas de virus automáticamente**: activa la actualización automática de la base de datos de virus. Los clientes comprueban **periódicamente**, según el intervalo programado, si hay firmas de virus actualizadas en el ManagementServer. Si existen firmas de virus actualizadas, se instalan automáticamente en el cliente.
- **Actualizar los archivos de programa automáticamente**: activa la actualización automática de los archivos de programa del cliente. Los clientes comprueban **periódicamente**, según el

intervalo programado, si hay archivos de programa actualizados en el ManagementServer. Si existen archivos de programa actualizados, se instalan automáticamente en el cliente. Después de actualizar los archivos de programa puede ser necesario reiniciar el cliente. Dependiendo de los ajustes en **Reinicio tras la actualización**, el usuario del cliente tiene la posibilidad de posponer la finalización de la actualización.

- **Reinicio tras la actualización**: seleccione **Abrir ventana informativa en el cliente** para informar al usuario de que debe reiniciar el equipo tan pronto le sea posible. **Generar informe** genera un informe en el área **Eventos de seguridad**. Con la función **Reiniciar sin consultar** el ordenador cliente se reinicia automáticamente y sin consultar.
- **Configuración de actualización**: aquí se determina de dónde obtienen los clientes las actualizaciones de firmas de virus.
  - **Cargar actualización online del ManagementServer**: de manera predeterminada los clientes descargan las firmas de virus del ManagementServer. Para ello, comprueban tras cada **Intervalo de sincronización** si existen firmas nuevas.
  - **Cargar actualización online de forma autónoma**: de forma alternativa, los clientes, pueden descargar las firmas de virus de los servidores de actualizaciones de G DATA. El intervalo de sincronización se puede programar en **Configuración y planificación**.
  - **Cargar actualización online de firmas de virus obsoletas de forma autónoma si no es posible establecer conexión con el ManagementServer**: para los puestos de trabajo móviles, como por ej. portátiles, se recomienda esta opción. Si el cliente tiene conexión con el ManagementServer, descarga las actualizaciones de allí. Pero si no hay conexión con el ManagementServer, las firmas de virus se descargan automáticamente de los servidores de actualizaciones de G DATA. El intervalo de sincronización se puede programar en **Configuración y planificación**.

### Funciones de cliente

Aquí se asignan permisos o privilegios a usuarios locales para cambiar los ajustes de Security Client. Al usuario se le pueden asignar derechos amplios o muy restringidos, dependiendo de las exigencias de las directivas empresariales.

- **El usuario puede ejecutar por sí mismo análisis de virus**: en caso de sospecha inminente y justificada, el usuario puede ejecutar un análisis de virus local, y de modo autónomo con respecto al ManagementServer. Los resultados de este análisis de virus se transmitirán al ManagementServer la próxima vez que se establezca conexión. Esta función también permite a los usuarios realizar modificaciones en los ajustes de Análisis de virus (configuración local).
- **El usuario puede cargar por sí mismo actualizaciones de firmas**: si activa esta función, el usuario del ordenador cliente puede descargar las firmas de virus directamente de Internet desde el menú contextual, aunque no tenga conexión con el ManagementServer. Esto es especialmente importante en el caso de portátiles que se usan a menudo fuera de la red perimetral.
- **El usuario puede modificar las opciones de vigilante**: cuando está activada esta función, el usuario del ordenador cliente tiene la posibilidad de modificar los ajustes en el área **Vigilante**.
- **El usuario puede modificar las opciones de correo electrónico**: cuando está activada esta función, el usuario del ordenador cliente tiene la posibilidad de modificar los ajustes en las áreas **Correo electrónico** y **AntiSpam**.
- **El usuario puede modificar las opciones web**: cuando está activada esta función, el usuario del ordenador cliente tiene la posibilidad de modificar los ajustes en el área **Web**.

- **El usuario puede visualizar la cuarentena local**: si se permite visualizar la cuarentena local, el usuario puede, en caso necesario, desinfectar, borrar o recuperar datos que se encuentren en la cuarentena. Tenga en cuenta que al restaurar un archivo de la cuarentena, no se elimina ningún virus. Por este motivo, esta opción debería estar únicamente disponible para usuarios avanzados.
- **Protección por contraseña para la modificación de opciones**: para evitar la manipulación indebida de las configuraciones locales, existe la posibilidad de permitir la modificación de opciones solo si se indica una contraseña. De este modo puede evitarse, por ejemplo, que un usuario modifique los ajustes. La contraseña puede asignarse de forma individual para el cliente o grupo correspondiente; comparta la contraseña solo con los usuarios autorizados.

### Tareas de escaneo

Aquí se pueden definir excepciones para que no se para excluir determinados archivos o directorios de la comprobación durante la ejecución de las tareas de escaneo. Por ejemplo, archivos comprimidos y copias de seguridad de un disco duro o partición se pueden definir como excepciones. También se pueden definir excepciones para extensiones de archivos y excluirlos de las tareas de escaneo. Estas excepciones se pueden definir para grupos completos. Si los clientes de un grupo tienen definidos distintos directorios de excepciones, se pueden añadir directorios nuevos o borrar los existentes. Al hacerlo, se conservan los directorios definidos para un cliente concreto. El mismo procedimiento se aplica también en las excepciones del vigilante.

### Escaneo en modo reposo

Si desea que el cliente realice un análisis de virus cuando el ordenador esté en modo reposo, seleccione la opción **Escaneo en modo reposo activado**. Pulsando el botón **Editar** se puede definir el área de análisis. Por defecto, están ajustadas aquí todas las unidades de disco duro locales.

## 4.3.4.2. Vigilante

Aquí puede configurar los ajustes de protección del cliente más importantes. El vigilante no debe desactivarse, ya que este se ocupa de la protección en tiempo real frente a malware. Si el vigilante se desactiva, se carece de esta protección. Por ello, solo se recomienda desactivar el vigilante cuando haya una razón que lo justifique, por ejemplo, tareas de detección de errores o diagnóstico. Es posible definir excepciones para el vigilante. Si una aplicación debe luchar contra pérdidas de rendimiento por el uso del vigilante, se pueden definir excepciones para los respectivos archivos o procesos del programa; los archivos excluidos ya no serán analizados por el vigilante. Tenga en cuenta que agregar excepciones al vigilante puede representar un riesgo para la seguridad.

### Configuración

Los ajustes del vigilante pueden utilizarse para configurar el vigilante y definir excepciones.

- **Estado del vigilante**: aquí puede activar y/o desactivar el vigilante. Por lo general conviene dejar activado el vigilante. Supone la base para una protección antivirus permanente y completa.
- **Utilizar motores**: el software G DATA trabaja con dos motores de análisis de virus que operan independientemente entre sí. La utilización de ambos motores garantiza unos resultados óptimos en la prevención de virus. El uso de un solo motor puede aportar ventajas en el rendimiento.
- **En caso de infección**: esta opción permite definir la forma de proceder cuando se detecta un archivo infectado. Unas opciones serán más adecuadas que otras, dependiendo de para que use el ordenador cliente correspondiente:

  - **Bloquear acceso al archivo**: no se concederá acceso de lectura ni escritura a un archivo infectado.
  - **Desinfectar y mover a cuarentena**: el archivo se moverá a la cuarentena y se intentará eliminar el virus.
  - **Poner archivo en cuarentena**: en este caso el archivo infectado se pone en cuarentena. Posteriormente, el administrador del sistema puede intentar realizar una desinfección manual del archivo.
  - **Eliminar archivo infectado**: esta es una medida rigurosa que ayuda a contener de manera efectiva un virus. No obstante, en el improbable caso de que se trate de un falso positivo, esto puede provocar una pérdida de datos.
- **Archivos comprimidos infectados**: defina aquí la forma de proceder con archivos comprimidos infectados. Tenga en cuenta que un virus dentro de un archivo comprimido solo provoca daños cuando se descomprime el archivo.
- **Modo de escaneo**: defina cuando se deben escanear los archivos. El **Acceso de lectura** escanea inmediatamente cada archivo al leerlo. El **Acceso de lectura y escritura** comprueba los archivos no solo al leerlos sino también al grabarlos. Esta opción protege contra los virus que se copian por ejemplo de otro cliente posiblemente sin protección o de Internet. **Al ejecutarlos** los archivos se escanean solo al ejecutarlos.
- **Comprobar accesos a la red**: habilita el control de acceso a red.
- **Heurístico**: a través del análisis heurístico, los virus no solo se detectan basándose en la base de datos de virus actuales, sino también en función de determinadas características típicas de los tipos de virus. Este método proporciona una seguridad adicional que, sin embargo, en raros casos puede provocar una falsa alarma.
- **Analizar archivos comprimidos**: el análisis de archivos comprimidos requiere mucho tiempo y puede omitirse siempre y cuando el vigilante de virus de G DATA se encuentre activo en el sistema. Al descomprimir el archivo, el vigilante detecta el virus escondido hasta entonces e impide automáticamente su propagación. Para no penalizar en exceso el rendimiento con el análisis innecesario de grandes archivos comprimidos que apenas se utilizan, puede limitar el tamaño de los archivos a comprobar con un valor determinado expresado en kilobytes.
- **Analizar archivos comprimidos de correo**: por regla general, esta opción debería desactivarse, siempre y cuando el vigilante de virus de G DATA se encuentre activo en el sistema, ya que el análisis de archivos comprimidos de correo electrónico habitualmente requiere mucho tiempo. Además, si se detecta un correo infectado, toda la bandeja de correo se mueve a la cuarentena o se elimina (dependiendo de la configuración del escaneo de virus). En estos casos, algunos correos del archivo de correo ya no estarán disponibles. Como el vigilante bloquea la ejecución de los archivos adjuntos de correo infectados, desactivar esta opción no crea ninguna brecha de seguridad. Cuando se utiliza Outlook, los correos entrantes y salientes se comprueban adicionalmente mediante un plugin integrado.
- **Comprobar áreas del sistema al cambiar medio y al iniciar**: no se deben excluir las áreas del sistema de su ordenador (p.ej. los sectores de arranque) del análisis de virus. Puede determinar aquí si se comprueban al iniciar el sistema y/o cuando se produce un cambio de medio (DVD nuevo o similar). Como norma general, debe activar al menos una de estas dos funciones.
- **Comprobar dialer / spyware / adware / riskware**: con el software G DATA puede analizar su sistema también para detectar dialers (marcadores) y otros programas de malware (spyware, adware, riskware). Se trata, por ejemplo, de programas que establecen por su cuenta conexiones a Internet caras y que son potencialmente igual de perjudiciales que los virus en

términos de impacto económico. Spyware (programas espía) pueden, por ejemplo, almacenar sin que se dé cuenta su historial de navegación o incluso todos sus registros de teclado (también sus contraseñas) y transmitir a terceros esta información a través de Internet.

- **Notificar al usuario al detectar virus**: si se activa esta opción, cuando el vigilante detecta un virus en el cliente afectado se abre una ventana informativa avisando al usuario de que se ha detectado un virus en su sistema. Se muestran el archivo detectado, la ruta y el nombre del malware detectado.

En **Excepciones** pueden excluir determinados directorios del análisis de virus, por ejemplo, para omitir carpetas con archivos comprimidos raramente utilizados con el fin de integrarlas en una tarea de escaneo separada. Además se pueden excluir del análisis ciertos archivos y tipos de archivos. Se pueden definir las siguientes excepciones:

- **Directorio**: seleccione la carpeta (incluyendo subcarpetas) que no debe ser analizada por el vigilante.
- **Unidad**: seleccione una unidad (partición o disco duro) que desee excluir de la verificación del vigilante.
- **Archivo**: aquí puede introducir el nombre del archivo que desee excluir del análisis del vigilante. Puede utilizar comodines.

  El funcionamiento de los comodines es el siguiente: el signo de interrogación (?) representa caracteres sueltos. El signo de asterisco (*) representa una secuencia completa de caracteres. Para proteger, por ejemplo, todos los archivos con la extensión exe, introduzca **.exe*. Para proteger, por ejemplo, archivos de distintos formatos de hojas de cálculo (por ejemplo, xls o xlsx), introduzca simplemente **.xls?*. Para proteger, por ejemplo, archivos de formatos distintos que tengan un nombre que comience igual, deberá introducir *text*.**. Esto afectaría a los archivos text1.txt, text2.txt, text3.txt etc.
- **Proceso**: si un determinado proceso no debe ser supervisado por el vigilante, introduzca aquí la ruta del directorio y el nombre del proceso en cuestión (por ejemplo *C:\Windows\system32\cmd.exe*).

Puede repetir este procedimiento siempre que lo considere necesario y puede borrar o modificar las excepciones disponibles en la ventana Excepciones.

### Supervisión de comportamiento

La supervisión de comportamiento proporciona mayor protección contra archivos y procesos maliciosos. A diferencia del vigilante, no funciona basándose en las firmas, sino que analiza el comportamiento real de un proceso. Para llevar a cabo una evaluación, la supervisión de comportamiento aplica diferentes criterios, tales como el acceso de escritura al registro y la posible creación de entradas de inicio automático. Si existen suficientes criterios que llevan a la conclusión de que un programa está exhibiendo una conducta sospechosa, se efectúa la acción predeterminada en la opción **En caso de amenaza**. Están disponibles las opciones siguientes: **Solo registrar**, **Detener programa** y **Detener programa y poner en cuarentena**.

Todas las acciones llevadas a cabo por la supervisión de comportamiento se incluyen en un informe que se agrega al área de **Eventos de seguridad**. Si algún programa es identificado erróneamente como una amenaza, puede usar el informe correspondiente para incluir el programa en la lista blanca. Puede editar o eliminar las entradas de la lista blanca haciendo clic en **Editar la lista blanca para toda la red**.

### ExploitProtection

Este tipo de ataques buscan específicamente vulnerabilidades en programas de terceros instalados en el cliente. ExploitProtection comprueba constantemente si existen irregularidades en el comportamiento del software instalado. Si un comportamiento inusual es detectado en algún proceso de software, se lleva a cabo la acción que haya sido definida en **En caso de exploit**: **Solo registrar** o **Bloquear la ejecución**. En caso de que **Notificar al usuario en caso de exploit** esté habilitado, el usuario recibirá también una notificación.

Todas las acciones llevadas a cabo por ExploitProtection se incluyen en un informe que se agrega al área de **Eventos de seguridad**. Si algún programa es identificado erróneamente como una amenaza, puede usar el informe correspondiente para incluir el programa en la lista blanca. Puede editar o eliminar las entradas de la lista blanca haciendo clic en **Editar la lista blanca para toda la red**.

### USB Keyboard Guard

USB Keyboard Guard protege a los clientes frente a los llamados "ataques BadUSB". Dispositivos USB reprogramados con funcionalidades adicionales maliciosas, como cámaras, lápices USB o impresoras, que pueden hacerse pasar por teclados cuando se conectan a un ordenador. Con el fin de evitar que estos dispositivos ejecuten de forma automática comandos no autorizados, USB Keyboard Guard solicitará al usuario una confirmación cuando detecta un dispositivo USB que se identifica como teclado. Si el usuario de hecho ha conectado un teclado, puede autorizarlo sin más. Si por el contrario, el dispositivo se identifica como teclado, pero el usuario ha conectado otro tipo de dispositivo, no debería autorizarlo, ya que puede suponer un riesgo.

Independientemente de la decisión que tome el usuario, se agregará un informe al área de **Eventos de seguridad**. Si el usuario ha autorizado un dispositivo, el administrador puede no obstante bloquearlo haciendo clic derecho en el informe y revocando la autorización.

## 4.3.4.3. Correo electrónico

En cada G DATA Security Client se puede instalar una protección antivirus para los correos electrónicos. Se vigilan los puertos estándar para los protocolos POP3, IMAP y SMTP. Para Microsoft Outlook se utiliza además un plugin especial. Este plugin comprueba automáticamente la presencia de virus en todos los correos entrantes e impide que se envíen correos infectados.

### Correos entrantes

El área Correos entrantes define las opciones para el análisis de los correos entrantes.

- **En caso de infección**: defina la forma de proceder cuando se detecta un archivo infectado. Unas opciones serán más adecuadas que otras dependiendo de para que use el ordenador cliente correspondiente.
- **Comprobar virus en correos recibidos**: cuando se activa esta opción, se verifican todos los correos electrónicos que recibe el cliente en busca de virus.
- **Comprobar correos no leídos al iniciar el programa (solo en Microsoft Outlook)**: esta opción se utiliza para escanear los correos electrónicos en busca de virus que recibe el cliente mientras está desconectado. En cuanto se abre Outlook, el programa comprueba todos los correos no leídos que haya en la bandeja de entrada y sus subcarpetas.
- **Adjuntar informe a los correos infectados recibidos**: en caso de que un correo enviado al cliente esté infectado por un virus, recibirá en el cuerpo de ese correo, debajo del propio texto del correo, el mensaje *¡NOTA! Este correo electrónico contiene el siguiente virus*, seguido del nombre

del virus. Además, antes del asunto encontrará el aviso *[VIRUS]*. Si tiene activada la opción **Eliminar adjunto/texto**, se le comunicará además que la parte infectada del correo electrónico ha sido eliminada.

### Correos salientes

El área Correos salientes define las opciones para el análisis de los correos salientes.

- **Comprobar correos antes del envío**: para evitar que se envíen correos infectados con virus, el software de G DATA le ofrece la posibilidad de verificar que los correos salientes están exentos de virus antes de enviarlos. Si se da la eventualidad de que un correo electrónico esté infectado con un virus, aparece el mensaje *El correo [asunto] contiene el virus siguiente: [nombre del virus]*. El correo correspondiente no será enviado.
- **Adjuntar informe a correo saliente**: en el cuerpo del correo saliente se muestra un informe debajo del texto del correo. El informe consta de la frase *Verificada la ausencia de virus por G DATA AntiVirus*, siempre que tenga activada la opción **Comprobar correos antes del envío**. Además se pueden indicar aquí la información de versión y últimas noticias sobre virus (**Información sobre la versión**).

### Opciones de escaneo

El área Opciones de escaneo configura los parámetros de análisis para los correos entrantes y salientes.

- **Utilizar motores**: el software G DATA trabaja con dos motores de análisis de virus que operan de forma independiente. La utilización de ambos motores garantiza unos resultados óptimos en la prevención de virus. Por el contrario, el uso de un único motor puede aportar ventajas en el rendimiento.
- **OutbreakShield**: OutbreakShield detecta y neutraliza las amenazas de los programas maliciosos en los correos masivos antes incluso de que estén disponibles las actualizaciones de las firmas de virus correspondientes. OutbreakShield se informa a través de Internet acerca de ciertas concentraciones de correos sospechosos y cierra prácticamente en tiempo real la brecha que existe entre el comienzo de un envío masivo de correos y su bloqueo mediante las firmas de virus adaptadas especialmente para ese virus. En **Modificar** puede determinar si OutbreakShield debe utilizar firmas adicionales para aumentar la eficacia en la detección. Además, puede introducir los datos de acceso para la conexión a Internet o un servidor proxy para que OutbreakShield pueda realizar descargas automáticas de firmas de Internet.

### Mensajes de aviso

El área Mensajes de aviso configura los mensajes de aviso para los destinatarios de correos infectados.

- **Notificar al usuario al detectar virus**: los destinatarios de un mensaje infectado serán informados automáticamente mediante un mensaje emergente de aviso de virus.

### Protección Outlook

Protección Outlook permite analizar los correos en Outlook con ayuda del plugin integrado.

- **Proteger Microsoft Outlook mediante un plugin integrado**: al activar esta función se inserta una nueva función en el programa Outlook del cliente, en el menú **Herramientas** con el nombre **Comprobar carpeta**. Independientemente de la configuración del G DATA Administrator, el usuario puede examinar la carpeta de correo que haya seleccionado para ver si contiene virus. Para efectuar un análisis en busca de virus en los archivos adjuntos utilice la

opción **Comprobar si hay virus en mensaje** del menú **Herramientas**. Una vez finalizado el proceso, aparecerá una pantalla de información con un resumen del resultado del análisis de virus. Aquí puede consultar si se completó el análisis de virus, recibir información acerca del número de correos y archivos adjuntos escaneados, los eventuales errores de lectura, los virus que se hayan encontrado y cómo se han procesado.

### Vigilancia de puerto

En general, se supervisan los puertos estándar para POP3 (110), IMAP (143) y SMTP (25). Si la configuración de puertos de su sistema es diferente, puede adaptarla según corresponda.

## 4.3.4.4. Web

En este área se pueden definir en profundidad los ajustes de escaneo para el tráfico de Internet y la banca online. Si selecciona no comprobar los contenidos de Internet, el **Vigilante de virus** intervendrá de todas formas cuando se intente acceder a los archivos infectados que se hayan descargado. Por lo tanto, aún sin la verificación de los contenidos de Internet el sistema en el ordenador cliente correspondiente está también protegido, siempre y cuando el vigilante de virus esté activado.

### Contenidos de Internet (HTTP)

El área Contenidos de Internet (HTTP) se ocupa de la configuración de escaneo para el tráfico de datos HTTP.

- **Procesar contenidos de Internet (HTTP)**: los contenidos web HTTP se analizan en busca de virus al navegar en Internet. No se ejecutan en absoluto los contenidos web infectados y tampoco se visualizan las páginas correspondientes. Si en la red se utiliza un proxy para acceder a Internet, entonces se tiene que introducir el puerto del servidor que utiliza el proxy. De lo contrario, no es posible comprobar el tráfico de Internet. El **Control del contenido web** (disponible en G DATA Endpoint Protection Business) utiliza también esta configuración.
- **Impedir tiempo de espera en el navegador**: el software G DATA procesa los contenidos web antes de que se visualicen en su navegador de Internet. Para esto se necesita cierto tiempo, dependiendo del tráfico de datos. Por este motivo puede suceder que el navegador de Internet muestre un mensaje de error por no haber recibido inmediatamente los datos solicitados, que están siendo comprobados en ese momento por el antivirus. Poniendo una marca en la opción Impedir tiempo de espera en el navegador se evita este mensaje de error. Tan pronto como se hayan comprobado todos los datos del navegador en busca de virus, se transferirán al navegador web.
- **Límite de tamaño para descargas**: aquí puede deshabilitar la comprobación HTTP para los contenidos web demasiado grandes. Los contenidos serán comprobados después por el vigilante en cuanto se active cualquier rutina maliciosa. La ventaja de esta limitación de tamaño reside en que no se producen retrasos al descargar archivos grandes debido al control de virus.
- **Excepciones de protección web en toda la red**: esta función le permite excluir determinados sitios web de la comprobación por parte de la protección web.

### BankGuard

Los troyanos bancarios se están convirtiendo en una amenaza cada vez más peligrosa. La tecnología BankGuard asegura las transacciones bancarias desde el principio y las protege inmediatamente allí donde se produce el ataque. G DATA BankGuard comprueba en tiempo real las bibliotecas de red usadas, asegurando así que ningún troyano bancario esté manipulando el navegador de Internet.

Esta protección inmediata y proactiva funciona en más del 99% de las transacciones bancarias y le protege incluso de los troyanos todavía desconocidos. BankGuard debe activarse para todos los clientes que usen Internet Explorer, Firefox y/o Chrome.

### 4.3.4.5. AntiSpam

El módulo AntiSpam está disponible en las **soluciones** Client Security Business, Endpoint Protection Business y Managed Endpoint Security.

Si marca la casilla **Utilizar filtro antispam**, se examinará la correspondencia electrónica del cliente en busca de posibles correos basura. Puede configurar que aparezca un mensaje de advertencia en el asunto del correo cuando se detecte que un correo es spam o caiga bajo sospecha de spam.

> Si el **plugin de Microsoft Outlook** está habilitado los correos basura se moverán automáticamente a la carpeta de correo no deseado. Para otros clientes de correo electrónico se puede definir una regla en el programa de correo del cliente especificando, por ejemplo, que los correos que tengan el aviso [Spam] en el asunto, se transfieran automáticamente a una carpeta especial para los correos de spam y basura. Para realizar ajustes antispam si usa Microsoft Exchange vaya a **Ajustes Exchange** > **AntiSpam**.

## 4.3.5. Configuración de Exchange

G DATA MailSecurity para Exchange está disponible como **módulo opcional**.

En el módulo Configuración de Exchange puede realizar los ajustes para el plugin de Exchange de G DATA MailSecurity. El módulo está disponible tan pronto se instala el plugin en Exchange Server 2007 SP1, 2010 o 2013.

### 4.3.5.1. General

El área General le permite configurar las actualizaciones, la protección antivirus y los ajustes de escaneo para el plugin Exchange para MailSecurity.

**Actualizar firmas de virus automáticamente**
Al igual que el resto de los clientes, los clientes Exchange se pueden actualizar automáticamente.

- **Actualizar firmas de virus automáticamente**: activa la actualización automática de las firmas de virus. Los clientes Exchange comprueban **periódicamente**, según el intervalo programado, si hay firmas de virus actualizadas en el G DATA ManagementServer. Si hay firmas de virus actualizadas disponibles, se instalan automáticamente en el cliente.
- **Actualizar archivos de programa automáticamente**: activa la actualización automática de los archivos de programa. Los clientes comprueban **periódicamente**, según el intervalo programado, si hay archivos de programa actualizados en el G DATA ManagementServer. Si hay archivos de programa actualizados disponibles, se instalan automáticamente en el cliente.

**Protección antivirus**
Para habilitar la protección antivirus active la casilla de verificación **Escaneo al acceder**. El escaneo en tiempo real comprueba todos los correos electrónicos, los archivos adjuntos y otros objetos en busca de malware cuando se reciben o se envían. En **Opciones de escaneo** puede determinar cómo proceder si se detecta cualquier contenido malicioso.

**Opciones de escaneo**
Los ajustes de escaneo son similares a los ajustes disponibles para el **Vigilante** y las **Órdenes de escaneo**.

- **Ambos motores**: defina si ambos motores deben estar activos o solo uno de ellos. Se recomienda el uso de ambos motores.
- **En caso de infección**: el plugin de Exchange puede reaccionar de diferentes formas frente a archivos infectados. Se recomienda la opción **Desinfectar (si no es posible: poner en cuarentena)**.
- **Tipos de archivo**: se puede limitar la verificación a archivos de programa y documentos, de esta forma se puede acelerar el proceso. Sin embargo, se recomienda comprobar todos los archivos.
- **Usar heurística**: el análisis heurístico hace posible detectar malware basándose en características típicas del malware, esto complementa la detección tradicional basada en firmas.
- **Analizar archivos comprimidos**: es posible analizar los archivos comprimidos en busca de malware sin necesidad de descomprimirlos. Si se encuentra malware, dependiendo de los ajustes, se desinfecta el archivo comprimido o se elimina por completo, incluyendo también los archivos no infectados. O, dependiendo de los ajustes que haya realizado, el correo electrónico se envía a la cuarentena junto con el archivo comprimido.

## 4.3.5.2. AntiSpam

El área AntiSpam del plugin de Exchange se encarga de filtrar los mensajes de spam antes de que lleguen al destinatario. Solo está disponible en servidores Exchange que ejecutan la función "Hub Transport Role".

Los mensajes de spam se clasifican en tres categorías distintas: **Sospecha de spam**, **Probabilidad de spam alta** y **Probabilidad de spam muy alta**. Puede personalizar la reacción del plugin de Exchange para cada una de estas categorías:

- **Reacción**
  - **Entregar correo**: se entrega el mensaje de correo electrónico al destinatario.
  - **Poner correo en cuarentena**: el mensaje de correo electrónico se envía a la cuarentena.
  - **Rechazar correo**: se rechaza el mensaje de correo electrónico.
  - **Mover correo a la carpeta de spam**: se mueve el correo electrónico a la carpeta de spam.
- **Prefijo en el asunto**: se agrega un prefijo en el asunto del mensaje de correo electrónico, como por ejemplo *[SPAM?]*.
- **Mensaje en el cuerpo**: agrega un texto al cuerpo del mensaje de correo electrónico.
- **Crear informes**: agrega un informe al módulo **Eventos de seguridad**.

Además de estas tres categorías de spam, puede definir una lista blanca y una lista negra. Mensajes de correo electrónico procedentes de direcciones o dominios registrados en la lista blanca no se comprueban nunca en busca de spam. Por el contrario, a direcciones o dominios registrados en la lista negra se aplican siempre los ajustes seleccionados para **Probabilidad de spam muy alta**. Tanto la lista blanca como la lista negra pueden ser exportadas e importadas como archivos .json.

## 4.3.6. Ajustes Android

El módulo Ajustes Android le permite acceder fácilmente a las capacidades de gestión de G DATA Administrator para dispositivos móviles Android.

## 4.3.6.1. General

Aquí se pueden realizar los ajustes para las actualizaciones automáticas, protección web, análisis de virus y sincronización, así como dos opciones generales para la administración de dispositivos:

- **Comentario**: aquí puede indicar, si lo desea, información complementaria sobre el cliente.
- **Nombre del dispositivo**: nombre del modelo del dispositivo.

### Actualizaciones

En el área Actualizaciones encontrará los ajustes relacionados con las actualizaciones.

- **Automático**: aquí puede establecer si el cliente móvil Android debe buscar automáticamente firmas de virus y actualizaciones de software. Si las actualizaciones no se van a descargar de forma automática, el usuario puede iniciar una actualización manualmente. Si opta por la actualización automática, puede determinar la frecuencia y, además, si la actualización se va a realizar en la red de telefonía móvil o únicamente a través de WiFi.

### Protección web

La Protección web bloquea sitios web de phishing impidiendo que se abran en el navegador Android y en Chrome. Debido a que se requiere un cierto tráfico de datos para verificar la lista de sitios web de phishing, se puede configurar la protección web para realizar esta verificación solamente a través de WiFi. Por lo tanto, la sección de Protección web incluye la posibilidad de limitar la protección web a las redes inalámbricas.

- **Activado**: active la protección web para proteger los dispositivos móviles Android al acceder a Internet. Se puede habilitar como una protección general para todo el tráfico web o solo cuando el acceso se produzca vía redes inalámbricas.

### Comprobación de virus

El área Comprobación de virus le permite definir los parámetros para los análisis de virus bajo demanda (on demand) y en tiempo real (on access).

- **Al instalar una app**: activa la comprobación automática de todas las aplicaciones que se instalan.
- **Periódico**: aquí se puede definir un análisis periódico. Active para ello la casilla Periódico y establezca luego la **Frecuencia**.
- **Modo de ahorro de batería**: aplaza el análisis periódico cuando el smartphone funciona en modo de ahorro de batería.
- **Solo en el proceso de carga**: aquí se puede definir que el escaneo periódico solo se efectúe cuando el dispositivo móvil se encuentre en estado de carga.
- **Tipo**: aquí se puede establecer si se va realizar una comprobación del **Sistema (análisis completo)** o solo las **Aplicaciones instaladas**.

### Sincronización

La opción de sincronización establece la frecuencia con la que un cliente móvil Android sincroniza sus datos con el ManagementServer. Puede establecer la frecuencia y decidir si la sincronización se puede

realizar solo a través de WiFi o también a través de la red de datos móviles.

## 4.3.6.2. Directrices

Tiene la posibilidad de definir directrices para diferentes tipos de dispositivos móviles, esto le permite bloquear ciertas funciones en los dispositivos y así proteger su red corporativa.

### Configuración general

En Configuración general seleccione el **Tipo de teléfono** al que pertenece el dispositivo o los dispositivos seleccionados. De esta forma selecciona el perfil de ajustes que usará G DATA Internet Security para Android:

- **Corporativo**: G DATA Internet Security para Android usará los ajustes del perfil corporativo. Este perfil se sincroniza con regularidad con el G DATA ManagementServer. No se permite al usuario el acceso a ningún tipo de ajustes. Se recomienda este ajuste para los dispositivos corporativos.
- **Privado**: G DATA Internet Security para Android usará los ajustes del perfil privado. Este perfil no se sincroniza con el G DATA ManagementServer. Se permite al usuario el acceso a todos los ajustes de G DATA Internet Security para Android.
- **Mixto**: se permite al usuario cambiar libremente entre los perfiles corporativo y privado.

  Advertencia: Al habilitar el modo **Privado** o **Mixto**, el usuario tendrá acceso a funcionalidades que no pueden ser gestionadas centralmente. Se recomienda el uso del modo **Corporativo** para todos los dispositivos Android gestionados.

Se pueden gestionar las siguientes funciones, independientemente del tipo de dispositivo móvil:

- **Permitir acceso a la cámara**: permite el acceso a la cámara del dispositivo (Android 4.0 o posterior).
- **Cifrado necesario**: aquí tiene que estar activado el cifrado completo del dispositivo (Android 3.0 y superior).
- **Permitir dispositivos con root**: permita o prohíba aquí los dispositivos con root. Cuando la función está desactivada, los dispositivos con root se bloquean con la contraseña que se ha definido en **Protección antirrobo**. Si está habilitada, los dispositivos con root no podrán acceder a redes inalámbricas definidas en **Permitir acceso a WLAN si se cumplen los requisitos**.

### Permitir acceso a WLAN si se cumplen los requisitos

Para dispositivos con root, puede bloquearse el acceso a una determinada red inalámbrica. Esto hace posible permitir el acceso a la red corporativa inalámbrica solo a aquellos dispositivos que cumplan las políticas de la empresa.

Introduzca el **SSID** de la red corporativa para la que se quiere activar el acceso. Seleccione el **Cifrado** e introduzca la **Contraseña** (si la red está codificada).

## 4.3.6.3. Pérdida/robo

El área Pérdida/robo ofrece amplias funciones para asegurar la protección de los dispositivos y sus datos en caso de robo. Para proteger dispositivos móviles perdidos o robados, la app Internet Security ofrece diferentes medidas que se pueden activar a distancia mediante un SMS. Los dispositivos robados o perdidos se pueden bloquear, borrar, localizar a distancia o silenciar, enviando al dispositivo perdido un SMS con los comandos respectivos desde un número de teléfono de confianza. Mediante la función de mensajería en la nube de Google también puede ejecutar estas

funciones antirrobo manualmente en cualquier momento.

Antes de especificar las medidas antirrobo, deben realizarse algunos ajustes generales. Es necesaria una **Contraseña de mantenimiento a distancia** (un código PIN numérico). Es necesario incluir esta contraseña cuando se envían comandos SMS, de esta forma se impide que usuarios no autorizados envíen comandos de bloqueo o similares al dispositivo. El comando para resetear a distancia la contraseña de mantenimiento solo puede enviarse desde el **Número de teléfono de confianza**. Algunos de los **Comandos SMS** desencadenan un informe u otro tipo de notificaciones. Estas notificaciones se envían al dispositivo que emitió el comando. Opcionalmente, también se pueden enviar a una **Dirección de correo** (p. ej. la información sobre la ubicación).

### Comandos SMS permitidos

Aquí se pueden establecer las acciones antirrobo que pueden llevarse a cabo en el dispositivo mediante el envío de un comando SMS. Este comando tiene que incluir la contraseña de mantenimiento. Seleccione la marca de verificación correspondiente, dependiendo de las funciones que desee activar:

- **Localizar el dispositivo**: el dispositivo enviará un informe de localización por SMS. Si se ha introducido una dirección de correo electrónico en **Protección antirrobo**, la posición del dispositivo robado o perdido también se enviará a esa dirección de correo. Para activar este comando, envíe un SMS con el mensaje: *Contraseña* **locate**.
- **Eliminar los datos personales**: aquí puede restablecer el dispositivo robado o perdido al estado de fábrica. Se borran todos los datos personales. Para activar este comando, envíe un SMS con el mensaje: *Contraseña* **wipe**.
- **Reproducir un tono de advertencia**: el dispositivo reproducirá una señal acústica hasta que se inicie Internet Security. Esto facilita localizar el dispositivo móvil perdido. Para activar este comando, envíe un SMS con el mensaje: *Contraseña* **ring**.
- **Silenciar el dispositivo**: si no desea que el dispositivo robado o perdido atraiga la atención mediante tonos acústicos de llamada o de otro tipo, puede silenciarlo con esta función. La funcionalidad del tono de advertencia para volver a encontrar el dispositivo permanecerá activa y no se verá perjudicada. Para activar este comando, envíe un SMS con el mensaje: Contraseña **mute**.
- **Bloquear la pantalla**: puede bloquear la pantalla del dispositivo robado o perdido y de esta forma impedir que el dispositivo se pueda seguir utilizando. Para activar este comando, envíe un SMS con el mensaje: *Contraseña* **lock**. Si no se ha establecido ninguna contraseña, se usará la contraseña de mantenimiento a distancia establecida.
- **Establecer la contraseña para el bloqueo de pantalla**: asigne una contraseña para desbloquear el dispositivo después de haber enviado el comando de bloqueo. Para activar este comando, envíe un SMS con el mensaje: *Contraseña* **set device password:** *Contraseña del dispositivo*.

Para cambiar la contraseña de mantenimiento a distancia, envíe un SMS al dispositivo móvil desde el número de teléfono que había introducido en **Número de teléfono de confianza**. El comando para esta función es: **remote password reset:** *Contraseña*.

### Detección de robo

Internet Security para Android recuerda qué tarjeta SIM se encontraba en el dispositivo móvil durante la instalación. Si se cambia esta tarjeta en algún momento, p. ej. porque el dispositivo ha sido robado y revendido, pueden efectuarse de forma automática determinadas acciones:

- **Bloquear la pantalla**: tiene la misma funcionalidad que las opciones de **Comandos SMS permitidos**.
- **Localizar el dispositivo**: tiene la misma funcionalidad que las opciones de **Comandos SMS permitidos**.

**Función de emergencia**
Mediante la mensajería en la nube de Google, pueden ejecutarse medidas de emergencia en el dispositivo móvil robado/perdido. Estas funcionan incluso cuando el dispositivo móvil se utiliza sin tarjeta SIM. En primer lugar hay que configurar la mensajería en la nube de Google. Introduzca en **Configuración general** > **Android** la **Identificación del remitente** y la **Clave API**. Seleccione cualquiera de las siguientes acciones y haga clic en **Ejecutar función**, para enviar el comando correspondiente al dispositivo móvil:

- **Localizar el dispositivo**: con la misma funcionalidad que las opciones de **Comandos SMS permitidos**.
- **Silenciar el dispositivo**: con la misma funcionalidad que las opciones de **Comandos SMS permitidos**.
- **Reproducir un tono de advertencia**: con la misma funcionalidad que las opciones de **Comandos SMS permitidos**.
- **Establecer el bloqueo de pantalla con el siguiente PIN**: con la misma funcionalidad que las opciones de **Comandos SMS permitidos**.
- **Activar el bloqueo de pantalla con PIN**: con la misma funcionalidad que las opciones de **Comandos SMS permitidos**.
- **Restablecer la configuración de fábrica**: con la misma funcionalidad que las opciones de **Comandos SMS permitidos**.

### 4.3.6.4. Apps

El panel de Apps permite configurar al acceso a las apps de dispositivos gestionados. Para bloquear o permitir apps, tiene que decidir primero si va a utilizar el filtro para apps en el modo de **Lista negra** o de **Lista blanca**. En el modo de lista negra solo se bloquea o restringe el acceso a aquellas apps que están en la lista negra, o se protege el acceso a las mismas mediante contraseña. Todas las demás apps pueden utilizarse. En el modo de lista blanca solo se permiten aquellas apps que están en la lista blanca o se protege el acceso a las mismas mediante contraseña. El acceso a todas las demás apps estará bloqueado. La **Contraseña** (un código PIN) se utiliza para poder acceder a las apps bloqueadas. Además, puede indicar una dirección de **Correo electrónico de recuperación**, a la que enviar la contraseña en caso de olvido.

En **Apps disponibles** se listan todas las apps que se instalaron en el dispositivo móvil correspondiente. Para cada app se muestra el **Nombre**, la **Versión** y el **Tamaño**. Mediante los botones de flecha puede mover las apps de la lista blanca a la negra y viceversa. Aquí también puede asignarse la **Protección por contraseña** para las apps listadas correspondientes.

### 4.3.6.5. Directorio telefónico

El panel Directorio telefónico permite una administración avanzada de los contactos. En la app Internet Security los contactos se pueden agregar a una lista de contactos, y tanto los contactos como sus comunicaciones pueden ocultarse en el dispositivo móvil de forma que estos no se muestren en la lista de contactos y directorio telefónico normales. En combinación con estas

funciones, el directorio telefónico de la app Internet Security puede sustituir completamente al directorio telefónico oficial de Android, creando un entorno de contactos gestionado para escenarios, en los que las posibilidades de comunicación de un dispositivo móvil deben limitarse a un subconjunto de contactos previamente aprobado.

La lista principal muestra todos los contactos que se han agregado al directorio telefónico de Internet Security. Para cada contacto se especifica **Nombre**, **Apellido**, **Número(s) de teléfon**o y **Dirección**. Con el menú desplegable **Visibilidad** puede establecerse si el contacto correspondiente se muestra (**Visible**) o no se muestra (**Oculto**) en el directorio telefónico normal de Android. Además, pueden ocultarse todas las llamadas y mensajes SMS de los contactos en cuestión en **Comunicación oculta**.

Para agregar un contacto al directorio telefónico, haga clic en **Agregar entrada**. En la ventana de la **Base de datos de contactos** se muestran todos los contactos que se hayan definido. Seleccione uno o varios contactos y haga clic en **Seleccionar** para agregar los contactos al directorio telefónico. Para eliminar un contacto del directorio telefónico, haga clic en **Deseleccionar entrada**.

Para agregar un contacto a la base de datos de contactos, haga clic en el botón **Crear contacto** de la barra de iconos o en **Importar contactos** para importar contactos de la Unidad Organizativa (OU) de Active Directory. Al crear un contacto, debería indicarse al menos el **Nombre** o el **Apellido**. Además puede agregar una o varias direcciones postales, así como direcciones de correo electrónico, números de teléfono, números de fax y organizaciones. Para eliminar un contacto de la base de datos de contactos, selecciónelo y haga clic en el icono de borrado en la barra de iconos o seleccione la opción **Eliminar** en el menú contextual.

## 4.3.6.6. Llamadas / SMS

El filtro de llamadas permite filtrar las llamadas y los mensajes SMS entrantes, así como las llamadas salientes. Con la misma base de datos que se utiliza en el panel **Directorio telefónico**, puede agregar muy fácilmente contactos a una lista negra o blanca, así como definir filtros generales.

### SMS/llamadas entrantes

En SMS/llamadas entrantes puede definirse cómo debe gestionar Internet Security las comunicaciones entrantes. Desactive **Permitir llamadas de números anónimos a pesar del filtro** para bloquear todas las llamadas anónimas. Si activa el filtro adicional **Permitir todos los números del directorio telefónico**, se permite la comunicación a través del filtro solo con los contactos del directorio telefónico de Android o de Internet Security, así como los contactos de la lista blanca.

Con la función **Modo de filtro** puede definir determinadas medidas para las llamadas y los mensajes SMS entrantes. Seleccione **Lista negra** para permitir la comunicación con todos los contactos excepto los que estén en la lista negra, o seleccione **Lista blanca** para permitir el contacto solo con los contactos que están en la lista blanca. Al hacer clic en **Agregar entrada**, puede agregar a la lista correspondiente cualquier contacto de la base de datos de contactos, y con **Deseleccionar entrada** puede eliminarlo de la lista.

### Llamadas salientes

En Llamadas salientes puede definirse cómo debe gestionar Internet Security las llamadas salientes. Si activa el filtro adicional **Permitir todos los números del directorio telefónico**, se permite contactar solo con los contactos del directorio telefónico de Android o de Internet Security, así como los contactos de la lista blanca.

Con la función **Modo de filtro** puede definir determinadas medidas para las llamadas y los mensajes SMS entrantes. Seleccione **Lista negra** para permitir la comunicación con todos los contactos

excepto los que estén en la lista negra, o seleccione **Lista blanca** para permitir el contacto solo con los contactos que están en la lista blanca. Al hacer clic en **Agregar entrada**, puede agregar a la lista correspondiente cualquier contacto de la base de datos de contactos, y con **Deseleccionar entrada** puede eliminarlo de la lista.

Si un usuario intenta llamar a un número bloqueado, se le informa del bloqueo y se le ofrece la posibilidad de solicitar el desbloqueo del número. Este proceso agrega un informe en el módulo **Eventos de seguridad**, mediante el cual el administrador puede crear directamente una entrada en la lista negra o en la lista blanca.

## 4.3.7. Ajustes de iOS

El módulo Ajustes de iOS le permite acceder fácilmente a las capacidades de gestión de G DATA Administrator para administrar dispositivos iOS.

### 4.3.7.1. General

Aquí puede introducir observaciones y asignar un perfil al cliente o los clientes seleccionados:

- **Descripción**: introduzca observaciones, por ejemplo informaciones acerca del dispositivo o de su configuración. Las observaciones solo se muestran en el G DATA Administrator.
- **Perfil activo**: muestra el **perfil** asignado. Para modificar el perfil, seleccione un perfil de la lista, o seleccione **- Ningún perfil -** para eliminar el perfil actual.

Además de las observaciones y la configuración del perfil, en el área General también se muestran los ajustes realizados cuando se desplegó Device Management en el dispositivo. Incluidos el nombre, la descripción, la organización y el Acuerdo de licencia para el usuario final.

### 4.3.7.2. Perfiles

El uso de perfiles le permite implementar directivas de seguridad en dispositivos iOS concretos o en grupos de dispositivos iOS. Use el botón **Añadir perfil** de la barra de iconos para definir un perfil nuevo. Introduzca el **Nombre** y una **Descripción** (opcional). Cada perfil puede contener hasta cinco directivas, cada una de ellas centrada en una rama específica de la configuración. En **Añadir directiva**, seleccione una de las siguientes directivas y haga clic en el botón "más" para agregarla al perfil:

- **Limitaciones de la funcionalidad**: desactiva funciones específicas de los dispositivos iOS (como por ej. el uso de la cámara, Siri o iCloud).
- **Limitaciones de apps**: desactiva aplicaciones concretas o ajustes de las aplicaciones (como por ej. YouTube, iTunes Store o Safari).
- **Limitaciones de contenidos multimedia**: desactiva tipos de contenidos específicos de los medios de comunicación, basándose en varios sistemas de clasificación.
- **Configuración de código de acceso**: obliga a respetar el cumplimiento de las normas estándares en el código de acceso iOS (como por ej. la longitud mínima, la complejidad mínima y un número máximo de intentos fallidos).
- **WiFi**: permite que el dispositivo iOS se conecte a una red inalámbrica específica.

Seleccione una directiva para editar los ajustes. Para guardar el perfil y sus directivas, haga clic en **Aplicar**. Si edita un perfil que ya ha sido asignado a un dispositivo, este se sincronizará con el dispositivo y agregará un informe al módulo **Registros (iOS)** tan pronto como el dispositivo lo

aplique.

Es posible importar y exportar perfiles simplemente haciendo clic en el botón respectivo. Los ajustes de los perfiles se guardan en un archivo JSON.

### 4.3.7.3. Antirrobo

El módulo antirrobo permite activar en el dispositivo iOS seleccionado una de las tres acciones siguientes:

- **Bloquear dispositivo**: se activa la pantalla de bloqueo del dispositivo (incluyendo contraseña de código de acceso, si se ha establecido alguno).
- **Restablecer la configuración de fábrica**: se borra el dispositivo. Tenga en cuenta que se eliminan todos los datos y también se desactiva Device Management.
- **Eliminar bloqueo de contraseña**: se elimina la contraseña de código de acceso.

Haga clic en **Ejecutar función** para ejecutar la acción seleccionada. Se creará un informe de estado en **Registros (iOS)**.

## 4.3.8. Sendmail/Postfix

El módulo Sendmail/Postfix está disponible como **módulo opcional**.

Sendmail/Postfix proporciona acceso para los ajustes del plugin del servidor mail Sendmail/Postfix de los clientes Linux.

### 4.3.8.1. Configuración

En Configuración puede configurar la protección antivirus:

- **Reacción**: definir las acciones a realizar cuando se detectan correos electrónicos infectados (**Eliminar adjuntos infectados** o **Poner mensaje en cuarentena**).
- **Prefijo en la línea del asunto**: añadir una cadena de texto en el campo asunto del correo. (P. ej. *[VIRUS]*).
- **Mensaje en el texto**: añadir una notificación al cuerpo del mensaje (p.ej. *Este correo electrónico contiene virus*).

### 4.3.8.2. AntiSpam

A través de los ajustes AntiSpam, el plugin Sendmail/Postfix filtrará y comprobará automáticamente si hay spam en los correos electrónicos entrantes.

Los mensajes de spam están incluidos en tres categorías diferentes: **Sospecha de spam**, **Probabilidad de spam alta** y **Probabilidad de spam muy alta**. Para cada una de esas categorías, se puede personalizar la acción que el plugin deberá llevar a cabo.

- **Reacción**
  - **Entregar correo**: El mensaje de correo será enviado al destinatario.
  - **Eliminar mensaje**: Se eliminará el mensaje de correo.
- **Prefijo en la línea del asunto**: Añadir una cadena de texto en el campo asunto del correo. (P. ej. *[SPAM]*).
- **Mensaje en el texto**: Añadir un texto al cuerpo del mensaje.

- **Crear informes**: Añadir un informe al módulo de **Eventos de seguridad**.

Adicionalmente a estas tres categorías de spam, se puede definir tanto una lista blanca como una negra. Los correos electrónicos de direcciones o dominios de la lista blanca, no se comprueban en busca de spam; direcciones y dominios en la lista negra se tratan siempre de acuerdo a la configuración de **Probabilidad de spam muy alta**. Tanto la lista blanca como la lista negra pueden ser exportadas e importadas como archivos .json.

### 4.3.9. Squid

El módulo Squid está disponible como **módulo opcional**.

El módulo Squid puede utilizarse para configurar los ajustes del plugin del proxy Squid de los clientes Linux. En **Protección antivirus**, se pueden configurar los siguientes ajustes:

- **Activado**: habilita la protección antivirus para Squid.
- **Utilizar antiphishing**: habilita las búsquedas en la nube para mejorar la protección.
- **Crear informes**: agrega un informe al módulo de **Eventos de seguridad** cuando se encuentre un virus.

En **Lista negra**, haga clic en **Agregar** para añadir a la lista negra un **Dominio**, **Dirección IP** (Client) o un **Tipo de MIME**. Las entradas en la lista negra se bloquean siempre.

### 4.3.10. Órdenes

En esta área se definen las órdenes (tareas) para los clientes o grupos. Hay dos clases distintas de órdenes, las órdenes únicas y las órdenes periódicas. Las tareas únicas se realizan una vez en el momento establecido. Para las periódicas se programa un horario. No hay límite numérico a la hora de definir diferentes órdenes. Pero, como norma general y para no perjudicar el rendimiento del sistema, conviene que las órdenes no coincidan en el tiempo.

En el área Órdenes están disponibles las siguientes informaciones para cada tarea:

- **Nombre**: el nombre con el que haya designado la tarea. La longitud del nombre introducido no está limitada.
- **Tipo**: el tipo de orden, como una orden de escaneo o una orden de reconocimiento de software.
- **Cliente**: aquí figura el nombre de los clientes correspondientes. Solo se pueden definir tareas para los clientes activados.
- **Grupo**: los distintos clientes se puede reunir en grupos. En este caso no aparecen los ordenadores individuales sino el nombre del grupo.
- **Estado**: aquí se muestra el estado o el resultado de una tarea. El programa informa, por ejemplo, si se está ejecutando una tarea o si ya ha concluido y también si se ha encontrado algún virus.
- **Última ejecución**: esta columna indica cuándo se ha efectuado por última vez la tarea correspondiente.
- **Intervalo de tiempo**: aquí figura con qué frecuencia se repite una tarea, de acuerdo con la programación definida.
- **Volumen**: que medios están incluidos en la tarea (por ejemplo, los discos duros locales).

Para editar las tareas, seleccione el comando **Propiedades** en el menú contextual (clic derecho).

En la barra de iconos sobre la lista de tareas están disponibles las siguientes opciones:

- **Actualizar**
- **Eliminar**
- **Orden de escaneo único**: con esta función se pueden definir órdenes de escaneo para ordenadores individuales o grupos de ordenadores. En el área correspondiente del cuadro de diálogo de configuración se pueden determinar el volumen de análisis y otros ajustes de escaneo.
- **Orden de escaneo periódico**: con esta función se pueden programar órdenes de escaneo.
- **Orden de copia de seguridad**: aquí se define el tiempo y el volumen de la copia de seguridad de los datos para clientes o grupos (**módulo** de Backup opcional).
- **Orden de restauración**: con esta función se pueden restaurar copias de seguridad de forma centralizada en los clientes o los grupos (**módulo** de Backup opcional).
- **Orden de reconocimiento de software**: lista el software y los patches instalados en los clientes (**módulo** PatchManager opcional).
- **Orden de distribución de software**: programar la distribución del software y de los patches (**módulo** PatchManager opcional).
- **Ejecutar inmediatamente**: seleccione esta función para ejecutar de nuevo tareas de escaneo único ya realizadas o canceladas. Si se trata de tareas de escaneo periódicas, esta función hace que se ejecuten inmediatamente, independientemente de la planificación horaria.
- **Registros**: acceda a los registros de las tareas correspondientes.
- **Mostrar órdenes de grupo en detalle**: en las tareas de grupo muestra todas las entradas correspondientes. Esta opción solo está disponible si hay seleccionado un grupo en la lista de ordenadores.

Cuando se selecciona el módulo tareas, aparece un menú adicional llamado **Tareas** en la barra de menú. En este menú están disponible las siguientes opciones:

- **Mostrar órdenes de grupo en detalle**
- **Ejecutar inmediatamente**: seleccione esta función para ejecutar de nuevo las tareas seleccionadas, independientemente de las especificaciones horarias definidas.
- **Cancelar**: cancele una tarea en curso.
- **Eliminar**: borre las tareas seleccionadas.
- **Restaurar copia de seguridad**: restaure copias de seguridad de los clientes o grupos (**módulo** de Backup opcional).
- **Nuevo**: cree una tarea.

### 4.3.10.1. Órdenes de escaneo

En la ventana **Nueva orden de escaneo** los administradores pueden definir órdenes de escaneo únicas u órdenes de escaneo periódicas. Para configurar una tarea por completo hay que tener en cuenta los aspectos **Planificación de la tarea**, **Escáner** y **Volumen de análisis**. Cada una de ellas se puede configurar de forma precisa en su propia área.

Las opciones que hay disponibles dependen del tipo de cliente para el que se esté planificando la tarea. Por ejemplo, si se está planificando una tarea para un servidor Exchange (si se ha instalado MailSecurity), las opciones relacionadas con amenazas específicas de los clientes no estarán

disponibles.

### Planificación de la tarea

Aquí puede establecer el **Nombre** que desea ponerle a la orden de escaneo. Es aconsejable utilizar nombres explicativos, como *Análisis de archivos comprimidos* o *Análisis mensual*, para describir la tarea de manera única y poder así encontrarla fácilmente en la tabla resumen. Mediante la opción **Transmitir el progreso de escaneo al servidor regularmente** (cada 2 minutos), puede visualizar en G DATA Administrator el progreso de una tarea de análisis en curso, recibiendo una indicación porcentual.

Además, se pueden asignar permisos a los usuarios para detener o cancelar la tarea a través del menú contextual de la bandeja del sistema. La función **Apagar el ordenador tras la comprobación de virus cuando no haya ningún usuario registrado** es otra opción diseñada para reducir la carga administrativa. Si un equipo no está encendido a la hora programada para llevar a cabo una tarea periódica de escaneo, mediante la opción **Ejecutar automáticamente la orden en el próximo inicio del sistema si el ordenador está apagado en el momento programado de comienzo**, el escaneo se puede iniciar más tarde, cuando vuelva a encenderse el ordenador.

Para las tareas de escaneo únicas se puede definir una hora de inicio. Para las órdenes periódicas se puede establecer el momento y la frecuencia en la que se va a realizar el análisis en busca de virus. Si selecciona **Al arrancar el sistema** se suprimirán las especificaciones de la planificación horaria y el software G DATA ejecutará el análisis siempre cuando se reinicie el ordenador. Con la opción **Diariamente** se puede definir, por ejemplo, en **Días de la semana** en que días concretos de la semana se debe llevar a cabo un análisis de virus (laborables, solo cada dos días, los fines de semana, etc.).

> Si se crea una tarea de escaneo única, solamente estará disponible la opción **Utilizar hora de inicio**. Si no se especifica ninguna hora de inicio, el escaneo se iniciará inmediatamente después de su creación.

Si la orden de escaneo incluye uno o más recursos compartidos de red en los que la cuenta del equipo del cliente no tiene permisos (p. ej. *Client001$*), introduzca un nombre de usuario y una contraseña pertenecientes a una cuenta con los permisos apropiados en **Contexto de usuario (opcional)**.

### Escáner

En el menú Escáner se puede definir la configuración con la que debe ejecutarse la orden de análisis. Están disponibles las siguientes opciones:

- **Utilizar motores**: el software G DATA trabaja con dos motores de análisis de virus que operan independientemente entre sí (ver **Ajustes de cliente** > **Vigilante**).
- **En caso de infección**: esta opción permite definir la forma de proceder cuando se detecta un archivo infectado (ver **Ajustes de cliente** > **Vigilante**).
- **Archivos comprimidos infectados**: determine como deben tratarse los archivos comprimidos infectados (ver **Ajustes de cliente** > **Vigilante**).
- **Tipos de archivo**: aquí puede determinar los tipos de archivo que G DATA debe comprobar en busca de posibles virus. Tenga en cuenta que el análisis completo de todos los archivos de un ordenador puede tardar un tiempo considerable.
- **Prioridad de escáner**: mediante los niveles de prioridad **Alto**, **Medio** y **Bajo** puede determinar si el análisis en busca de virus se debe realizar con prioridad alta (en este caso el análisis es más rápido, aunque posiblemente afecte al rendimiento de otras aplicaciones) o con prioridad baja

(el análisis necesitará más tiempo, pero no afectará a otras aplicaciones). En función del momento en que se lleve a cabo el análisis de virus será conveniente elegir uno u otro ajuste.

- **Configuración**: defina aquí los análisis de virus adicionales que deba ejecutar el software G DATA. Los ajustes por defecto son los más recomendables; pero dependiendo del tipo de aplicación, el ahorro de tiempo que supone pasar por alto estos análisis puede compensar una mínima pérdida de seguridad. La mayor parte de los ajustes son idénticos a los que se pueden realizar en el área **Ajustes de cliente** > **Vigilante**. Además de estos, también hay ajustes específicos para las tareas de escaneo:
  - **Comprobar RootKits**: un rootkit intenta esquivar los métodos convencionales de detección de virus. Con esta opción puede buscar específicamente rootkits sin tener que realizar análisis completo del disco duro y de los datos guardados.
  - **Utilizar todos los procesadores**: en sistemas multinúcleo use puede distribuir la carga del análisis de virus entre todos los procesadores, con lo cual el análisis se ejecuta bastante más rápido. La desventaja de esta opción es que hay menos capacidad de procesamiento disponible para otras aplicaciones. Use esta opción solo cuando la tarea de escaneo se realice en momentos en que el sistema normalmente no está siendo utilizado (por ejemplo, por la noche).

### Volumen de análisis

Mediante el área Volumen de análisis se puede restringir la tarea de escaneo a determinados directorios (a la hora de planificar una tarea de escaneo para un cliente) o buzones (a la hora de planificar una tarea de escaneo para un servidor Exchange). La ventana de selección de directorio le permitirá seleccionar carpetas de ordenadores locales y en red.

## 4.3.10.2. Órdenes de copia de seguridad

Backup está disponible como **módulo opcional**.

Aquí los administradores pueden planificar tareas de copia de seguridad de los datos de los clientes, y proteger así de forma centralizada los archivos importantes.

### Planificación de la tarea

Aquí puede establecer el **Nombre** que desee ponerle a la tarea de copia de seguridad. Es aconsejable utilizar nombres explicativos, como por ej. copia de seguridad mensual o copia de seguridad parcial de comerciales, para caracterizar la tarea inequívocamente y facilitar de esta forma su identificación en la tabla resumen. Se puede definir el tiempo y la frecuencia en que se va a realizar la copia de seguridad, y también si se trata de una **Copia de seguridad parcial** (diferencial) o una **Copia de seguridad completa**. En la copia de seguridad parcial solo se guardan los datos que hayan cambiado desde la última copia de seguridad completa. Aunque así ahorra tiempo al crear la copia de seguridad, la restauración resulta más laboriosa porque hay que reconstruir los datos a partir de varios archivos diferentes de copia de seguridad.

Para evitar los problemas derivados de la sobrecarga de un portátil no conectado a la red eléctrica se puede elegir el ajuste **No ejecutar en funcionamiento con la batería**. Las copias de seguridad de los dispositivos móviles entonces solo se realizan cuando están conectados a la red eléctrica. Con la opción **Diariamente** se puede definir, en **Días de la semana**, que días concretos se debe llevar a cabo la copia de seguridad (laborables, solo cada dos días, los fines de semana, etc.).

En **Configuración general** > **Copia de seguridad** se puede establecer en qué directorio se guardarán las copias de seguridad además de configurar informes relacionados con la cantidad de

espacio libre disponible.

**Selección de archivos/directorios**
En el área Selección de archivos/directorios puede determinar qué carpetas se tienen que respaldar exactamente en los diferentes clientes o grupos. En el área **Alcance de la copia de seguridad** se pueden agregar carpetas de cualquier cliente. Si se activa la marca de verificación correspondiente en **Excluir archivos**, se pueden excluir de la copia de seguridad archivos y carpetas determinados (como por ej. **Archivos temporales** o **Archivos de sistema**). Además, se pueden definir excepciones individuales indicando en la lista de excepciones la extensión de determinados tipos de archivo.

Si desea guardar la copia de seguridad creada en un directorio determinado antes de transmitirla al ManagementServer, puede indicar esta ubicación específica en **Memoria caché**. Si la opción **Utilizar ruta estándar del cliente** está activada y se ha indicado una ruta absoluta, la copia de seguridad se almacenará en el directorio que se haya indicado. Si esta opción no está activada, G DATA Security Client establecerá el buffer de la copia de seguridad en la partición en la que haya más espacio libre disponible. Se crea entonces el directorio G DATA\Backup en el directorio raíz de esta partición.

## 4.3.10.3. Órdenes de restauración

Backup está disponible como **módulo opcional**.

Las tareas de restauración se pueden planificar de varias formas. Haga clic en el menú **Órdenes** sobre **Nuevo** > **Orden de restauración** o en la barra de iconos sobre el botón **Orden de restauración**. Se abre la ventana **Restaurar copia de seguridad** y entonces se puede seleccionar una copia de seguridad para la restauración. Alternativamente puede buscarse la copia de seguridad en la lista de órdenes. Haga clic con el botón derecho del ratón sobre la orden y seleccione **Restaurar copia de seguridad**.

La ventana Restaurar copia de seguridad muestra información básica sobre la orden de copia de seguridad seleccionada. Dependiendo del número de veces que se haya ejecutado la orden, contendrá una o varias copias de seguridad. Para cada copia de seguridad se muestra en la lista la **Fecha de la copia de seguridad**, el **Cliente**, el **Tipo de copia de seguridad**, el **Número de archivos** y el **Tamaño (en MB)**. En la lista **Restaurar en cliente** puede seleccionar el cliente en el que deben restablecerse los archivos (este no tiene por qué ser el mismo cliente que en el que se creó la copia de seguridad). Haga clic en **Aceptar**, para abrir la ventana de configuración de la restauración.

Los ajustes para la restauración pueden configurarse en dos pestañas. **Selección de archivos** le permite buscar dentro de la copia de seguridad. Haga clic en **Restaurar solo archivos seleccionados del archivo comprimido**, para activar una estructura de directorios en la que seleccionar los archivos que desee restaurar. Haga clic en **Restaurar todos los archivos del archivo comprimido** para desactivar la estructura de directorios y restaurar todos los archivos. En la pestaña **Opciones** puede configurar los ajustes para la tarea. Puede introducir en **Nombre de tarea** un título descriptivo. Si quiere restaurar los archivos en su directorio original, active **Restaurar archivos a los directorios originales**. Si quiere restaurarlos en otro distinto, seleccione otro **Directorio de destino**. Finalmente puede decidir cómo proceder cuando existan conflictos de versión con archivos existentes en **Sobrescribir archivos existentes**. Después de aceptar los ajustes se agrega la orden de restauración al módulo de órdenes y se ejecuta inmediatamente.

## 4.3.10.4. Órdenes de reconocimiento de software

PatchManager está disponible como **módulo opcional**.

Con esta función se puede determinar si los patches disponibles son aplicables para determinados clientes o grupos. Las órdenes de reconocimiento de software pueden programarse aquí. Están disponibles las siguientes opciones:

- **Ejecución**: decida cuándo debe ejecutarse la tarea de reconocimiento de software.
  - **Temporalizado**: ejecuta la tarea de acuerdo a un **Horario**, que puede definirse usando uno de los parámetros **de inmediato**, **una vez**, **cada hora**, **diariamente**, **semanal**, **mensual** o **Al establecer conexión a Internet**.
  - **Tan pronto esté disponible**: ejecuta la tarea cada vez que hay un nuevo patch disponible.

Para seleccionar los patches que deben ser verificados en cuanto a usabilidad, use una de las siguientes opciones en **Volumen**:

- **Patch específico**: elija uno o varios patches de la lista.
- **Mediante características**: introduzca las características del software que desee reconocer. Para agregar determinadas características (el **Fabricante**, el **Nombre del producto**, la **Urgencia** o el **Idioma**) como criterio de selección, active la marca de verificación en la característica correspondiente e introduzca una palabra clave. Se puede, por ej., verificar solo software de ciertos fabricantes o solo versiones concretas. Para filtrar se permite el uso de comodines como *?* y ***. Active la opción **Solo patches** si la tarea no debe verificar paquetes completos de software o de actualizaciones de programa.

Seleccione **Instalar patches aplicables automáticamente**, de forma que cada vez que se verifique la aplicabilidad de un patch, este se instale automáticamente.

Si se planifica la orden de reconocimiento de software desde el módulo **Resumen de estado** del PatchManager, la tarea se aplica al patch y a los clientes seleccionados allí. Si se planifica desde el módulo **Configuración de patches**, es necesario seleccionar el cliente o los clientes, para los que se debe verificar la aplicabilidad. Si se planifica desde el módulo **Órdenes**, es necesario seleccionar el patch o los patches para los que se debe verificar la aplicabilidad – la tarea se ejecutará en los clientes o grupos que estén seleccionados en ese momento.

## 4.3.10.5. Órdenes de distribución de software

PatchManager está disponible como **módulo opcional**.

Aquí puede definir cuándo se van a instalar en los clientes o grupos los patches seleccionados aplicables. Las órdenes de distribución de software se pueden gestionar y programar aquí. Están disponibles las siguientes opciones:

- **De inmediato**: la tarea de distribución se ejecuta inmediatamente.
- **Inmediatamente después del encendido**: la tarea de distribución se ejecuta inmediatamente después del siguiente reinicio.
- **Después del login**: la tarea de distribución se realiza la próxima vez que un usuario inicie sesión en el cliente.
- **Instalar en el tiempo especificado**: la tarea de distribución se ejecuta a una hora específica, según el horario programado (las otras opciones programadas no entran en vigor hasta que no

se haya llegado a este punto en el tiempo).

- **Instalar con retraso**: se programa una demora en la ejecución de la tarea. Las ventajas son que el proceso de arranque y la distribución de patches no afectan al mismo tiempo el rendimiento del cliente.

Si se planifica la orden de distribución de software desde el módulo **Resumen de estado** del PatchManager, la tarea se aplica al patch y a los clientes seleccionados allí. Si se planifica desde el módulo **Configuración de patches**, es necesario seleccionar el cliente o los clientes, en los que se debe instalar el patch. Si se planifica desde el módulo **Órdenes**, es necesario seleccionar el patch o los patches que tienen que ser instalados – los patches se instalarán en los clientes o grupos que estén seleccionados en ese momento.

### 4.3.10.6. Ordenes de restauración

PatchManager está disponible como **módulo opcional**.

Estas órdenes se usan para desinstalar patches que ya han sido distribuidos En la lista de **Órdenes**, haga clic derecho en la tarea de distribución correspondiente y seleccione **Restaurar**. De forma alternativa, seleccione en el módulo **Resumen de estado** del PatchManager el cliente y el patch específico y, por último, la opción **Restaurar** del menú contextual.

En la ventana de **Órdenes de restauración** puede introducir un **Nombre de tarea** para identificar fácilmente la tarea de restauración. Una vez introducido el nombre, haga clic en **Aceptar** para agregar la tarea a la lista de **Órdenes**. Se ejecutará inmediatamente.

## 4.3.11. PolicyManager

El módulo PolicyManager está disponible en las **soluciones** Endpoint Protection Business y Managed Endpoint Security.

El PolicyManager incluye un control de las aplicaciones, los dispositivos y los contenidos web, así como una supervisión del tiempo de utilización de Internet. Estas funciones permiten una implementación integral de las directivas de la empresa para el uso de los ordenadores propios de la empresa. A través del PolicyManager, un administrador del sistema, puede establecer si se pueden utilizar (y en qué medida) dispositivos de almacenamiento masivo externo o medios ópticos. También puede definir qué sitios web se pueden visitar y en qué periodo determinado, y qué programas se pueden utilizar en los ordenadores de la empresa.

### 4.3.11.1. Control de aplicación

Con el Control de aplicación se puede restringir el uso de determinados programas. Para alcanzar este objetivo, en la opción **Estado** defina si las limitaciones se deben aplicar a todos los usuarios (incluidos los administradores) o solo a los usuarios que no tengan permisos de administrador en el ordenador cliente.

En el apartado **Modo** se determina si la lista de control de aplicación va a ser una lista blanca o una lista negra:

- **Lista blanca**: solo las aplicaciones incluidas en esta lista se pueden usar en el ordenador cliente.
- **Lista negra**: las aplicaciones indicadas aquí no se pueden utilizar en el ordenador cliente.

Para crear una nueva regla pulse el botón **Nuevo**. Se puede elegir entre los siguientes tipos de reglas:

- **Fabricante**: se utiliza la información del fabricante que figura en los archivos de programa para permitir o bloquear el uso de estas aplicaciones. Puede o bien introducir aquí directamente el nombre del fabricante o bien emplear el botón ... para buscar un archivo en concreto desde el que pueda leerse e importarse la información del fabricante.
- **Archivo**: aquí puede bloquear o permitir determinados archivos de programa para el cliente correspondiente. Se puede introducir el nombre del archivo para bloquear / permitir en general el acceso a los archivos de ese nombre o bien se puede hacer clic en el botón **Averiguar características** de un archivo para definir selectivamente por sus características un archivo determinado. En caso necesario, puede utilizar como comodín para cualquier contenido un asterisco (*) al principio y/o al final de las características **Nombre de archivo**, **Nombre del producto** y **Copyright**.
- **Directorio**: con esta función puede permitir o bloquear directorios completos (opcionalmente, incluyendo los subdirectorios).

### 4.3.11.2. Control de dispositivos

Con ayuda del control de dispositivos se puede limitar el acceso a dispositivos de almacenamiento externos. De este modo, se puede impedir el uso de lápices USB, memorias USB, unidades de CD/DVD e incluso limitar el uso de cámaras web.

En la opción **Estado** defina si las limitaciones son aplicables a todos los usuarios (incluidos los administradores) de ese ordenador cliente o solo a los usuarios que no tengan permisos de administrador. La opción **Dispositivos**, le permite restringir el uso de los mismos según el tipo de **Dispositivo** teniendo en cuenta los siguientes ajustes:

- **Permiso**
  - **Leer / escribir**: hay acceso total al dispositivo.
  - **Leer**: solo hay acceso de lectura, pero no está permitido guardar datos.
  - **Prohibir acceso**: no está permitido el acceso al dispositivo, ni de lectura ni de escritura. El usuario no puede utilizar el dispositivo.
- **Autorización temporal**: Si el uso de un dispositivo ha sido permitido temporalmente desde un directiva de Policy Manager en el módulo **Eventos de seguridad**, se mostrará aquí el periodo de tiempo. Haga clic en el icono X para cancelar el permiso temporal.

En los ajustes de **Lista blanca** se puede volver a permitir, con ciertas limitaciones, el uso del dispositivo que se hubiese restringido de algún modo (Leer/ Prohibir el acceso) a un cliente concreto. Al pulsar el botón **Nuevo** se abre una ventana de diálogo en la que se visualizan los dispositivos con restricciones de uso. Si ahora pulsa **...** puede hacer una excepción para determinados dispositivos.

- **Utilizar ID de medio**: defina que solo se puedan utilizar determinados CDs o DVDs con una unidad de CD/DVD, por ejemplo, presentaciones especiales de la empresa grabadas en CD.
- **Utilizar ID de hardware**: defina que solo se puedan utilizar determinados lápices USB. Con listas blancas para dispositivos de almacenamiento individuales basadas en una ID de hardware, el administrador de red tiene la posibilidad de controlar qué empleados tienen autorización para transmitir datos.

Para determinar el ID del medio o del hardware, seleccione un cliente desde la lista **Seleccionar origen**. El ID correspondiente se leerá automáticamente. Seleccionando **(Búsqueda local..)** puede averiguar el ID del medio o del hardware conectado al PC en el cual G DATA Administrator está

instalado.

### 4.3.11.3. Control del contenido web

El control del contenido web tiene por objetivo permitir al usuario el acceso a Internet en el ámbito de su trabajo, pero a la vez impedirle la navegación en páginas web no deseadas o en determinadas áreas temáticas. Puede permitir áreas selectivamente activando una marca de verificación para el cliente correspondiente o prohibirlas quitando la marca de verificación. Las categorías cubren una gran cantidad de áreas temáticas y G DATA las actualiza regularmente. De este modo, se evita que el administrador de red tenga que ocuparse de mantener las listas blancas y negras.

En la opción **Estado** especifique si las limitaciones son aplicables a todos los usuarios de ese cliente (incluyendo los administradores) o solo a los usuarios que no tengan derechos de administrador.

En **Excepciones para toda la red**, es posible asegurar que ciertos sitios de internet sean bloqueados o permitidos en la empresa a nivel global, a través de toda la red, independientemente de los ajustes que se hayan establecido en las **Categorías permitidas**. Para realizar esta acción, haga clic en **Agregar**, seleccione **Permitir** o **Bloquear**, introduzca la **Dirección** y haga clic en **Aceptar** para agregar la excepción. Haga clic en **Editar**, para modificar una excepción existente o **Eliminar** la(s) excepción(es).

### 4.3.11.4. Tiempo de utilización de Internet

En el área de Tiempo de utilización de Internet se puede limitar el uso general de Internet a determinados periodos de tiempo. También es posible configurar un contingente de tiempo de uso de Internet. En la opción **Estado** especifique si las limitaciones son aplicables a todos los usuarios de ese cliente (incluyendo los administradores) o solo a los usuarios que no tengan derechos de administrador. En el lado derecho puede usar los controles deslizantes disponibles para establecer la cuota de que dispone cada ordenador cliente para el uso de Internet. Se puede establecer un contingente de tiempo diario, semanal o mensual; por ejemplo, la entrada *04 20:05* representa un tiempo de utilización de Internet de 4 días, 20 horas y 5 minutos.

> Cuando aparecen conflictos en los ajustes para el uso de Internet cuenta siempre el dato de menor valor. Por lo tanto, si establece un límite temporal de cuatro días al mes, pero admite cinco días en una semana, el software reduce el uso de Internet del usuario automáticamente a cuatro días.

Cuando el correspondiente usuario intenta acceder a Internet más allá del periodo autorizado, aparece una ventana emergente en el navegador que le informa de que ha excedido su cuota de tiempo. En el área de Horarios de bloqueo, además de limitar el tiempo de uso de Internet, puede bloquear determinados intervalos. Los periodos bloqueados se muestran en rojo, los periodos permitidos, en verde. Para permitir o bloquear un periodo de tiempo, simplemente márquelo con el ratón. Aparece entonces un menú contextual junto al puntero del ratón. Este menú ofrece dos posibilidades, **Autorizar tiempo** o **Bloquear tiempo**. Cuando el correspondiente usuario intenta acceder a Internet durante los periodos bloqueados, aparecerá una ventana emergente en el navegador que le informa que en ese momento no tiene acceso a Internet.

## 4.3.12. Cortafuegos

El módulo del Cortafuegos está disponible en las **soluciones** Client Security Business, Endpoint Protection Business, y Managed Endpoint Security.

## 4.3.12.1. Resumen

Aquí pueden configurarse ajustes generales del cortafuegos para los clientes seleccionados.

### Configuración

En esta sección encontrará ajustes generales relacionados con el cortafuegos.

- **Activar G DATA Firewall**: activa/desactiva el cortafuegos.

  Nota: a partir de la versión 14, es necesario actualizar los clientes que no tengan instalado el módulo cortafuegos a la nueva versión antes de poder activar el cortafuegos.
- **Notificar aplicaciones bloqueadas**: cuando el ordenador cliente está conectado con G DATA ManagementServer, en el área de **Eventos de seguridad** se avisa al administrador del sistema acerca de las aplicaciones que ha bloqueado el cortafuegos del cliente correspondiente.
- **Conjunto de reglas**: seleccione el conjunto de reglas que se deben aplicar al cliente:
  - **Modo piloto automático**: G DATA configura automáticamente las reglas y el cortafuegos las aplica en Segundo plano sin interacción con el usuario. En el modo de piloto automático, el cortafuegos optimiza su conjunto de reglas de forma autónoma con el paso del tiempo.
  - Todos los conjuntos de reglas que han sido creados en el área **Conjuntos de reglas**.

### Uso dentro de la red interna

Aquí se definen los ajustes que se aplican cuando el cliente se utiliza en misma red que el ManagementServer:

- **El usuario puede activar y desactivar el cortafuegos**: el administrador de la red, puede permitir al usuario del ordenador cliente desactivar el cortafuegos temporalmente. Esta opción solo está disponible mientras el cliente esté dentro de la red de la empresa y, debería estar al alcance solo de usuarios avanzados.

### Uso fuera de la red interna

Aquí se definen los ajustes que se aplican cuando el cliente se utiliza en una red distinta de la del ManagementServer:

- **Utilizar configuración fuera de la red para clientes móviles**: para proteger de forma óptima los portátiles cuando no se encuentran en la misma red que el G DATA ManagementServer, es posible reemplazar automáticamente el conjunto de reglas del cortafuegos por un conjunto de reglas optimizado para fuera de la red. En cuanto el ordenador portátil se conecta de nuevo con la red del G DATA ManagementServer, el conjunto de reglas estándar se restaura automáticamente.

  Nota: solo es posible usar la configuración fuera de la red si el cortafuegos no se ejecuta en modo piloto automático en la red interna. Si un cliente utiliza el piloto automático en la red interna, usará este mismo ajuste cuando se encuentre fuera de la red.
- **Conjunto de reglas**: seleccione el conjunto de reglas que se deben aplicar al cliente:
  - **Modo piloto automático**: ver **Cortafuegos** > **Resumen** > **Configuración**.
  - Todos los conjuntos de reglas que han sido creados en el área **Conjuntos de reglas**.
- **El usuario puede editar la configuración remota**: permite a los usuarios avanzados configurar fuera de la red su cortafuegos según criterios individuales. En cuando el ordenador portátil se conecte de nuevo con G DATA ManagementServer, las modificaciones realizadas serán sustituidas por las reglas que el administrador de la red haya especificado para ese

cliente.

### 4.3.12.2. Conjuntos de reglas

En el área Conjuntos de reglas puede crear conjuntos de reglas para diferentes áreas de red. El número de reglas para el cortafuegos que puede incluir un conjunto de reglas no está limitado.

Si selecciona un conjunto de reglas encontrará el listado de las reglas que contiene en **Conjunto de reglas**. Para crear o editar conjuntos de reglas existentes use los botones **Nuevo**, **Borrar**, **Importar** y **Exportar**. En **Ajustes** se pueden configurar las siguientes opciones:

- **Nombre**: el nombre que designa el conjunto de reglas seleccionado.
- **Comentario**: una descripción del conjunto de reglas seleccionado.
- **Modo invisible activado**: cuando está habilitado bloquea solicitudes que tratan de verificar la accesibilidad de los puertos en el ordenador. Esto dificulta que los atacantes puedan obtener información sobre el sistema.

Las reglas que forman parte del conjunto de reglas seleccionado se muestran en la parte inferior. Vaya a **Reglas** si desea **crear una nueva regla/editar una regla existente**, borrar una regla o iniciar el **Asistente** para reglas. Las reglas del cortafuegos se ejecutan por orden, según el rango que ocupen en el conjunto de reglas. Puede modificar el orden de cada regla en **Rango** usando los botones **Inicio**, **Hacia arriba**, **Hacia abajo** y **Fin**.

#### Agregar conjunto de reglas

Introduzca un **Nombre** y de forma alternativa, una **Comentario**. Seleccione **Modo invisible activo** para bloquear solicitudes que tratan de verificar la accesibilidad de los puertos en el ordenador. En **Seleccione aquí las reglas que desea utilizar del conjunto de reglas predeterminado**, puede seleccionar una o varias de las reglas predefinidas para agregarlas al nuevo conjunto de reglas. Tras hacer clic en **Aceptar**, el conjunto de reglas aparecerá en el resumen de **Conjunto de reglas**.

#### Crear regla/editar regla

Para agregar reglas nuevas o modificar reglas existentes, utilice los botones **Nuevo** y **Editar** en el área **Reglas**.

- **Nombre**: en las reglas preconfiguradas y generadas automáticamente, se muestra el nombre del programa para el que se aplica la regla correspondiente.
- **Regla activa**: puede activar o desactivar una regla quitando la marca de verificación, sin tener que borrarla en ese momento.
- **Comentario**: aquí se indica cómo se creó la regla. Las reglas predeterminadas para el conjunto de reglas llevan el texto *Reglas predefinidas*, las reglas que se generan a partir del diálogo de la alarma de cortafuegos llevan el texto *Generada mediante consulta* y a las reglas que genera el administrador o el usuario a través del diálogo avanzado se les puede añadir un comentario propio.
- **Dirección de conexión**: defina si en este caso se trata de una regla para conexiones entrantes, salientes o de ambos tipos.
- **Acceso**: determine si para el programa correspondiente dentro de este conjunto de reglas se permite o se rechaza el acceso.
- **Protocolo**: seleccione a qué protocolos de conexión desea permitir o rechazar el acceso. Para ello, tiene la posibilidad de bloquear o habilitar protocolos en general o de vincular el uso del protocolo al empleo de una o varias aplicaciones determinadas (**Asignar aplicaciones**). Del

mismo modo, puede definir exactamente los puertos que desea o no desea utilizar con el botón **Asignar puertos**.

- **Intervalo temporal**: configure el acceso a los recursos de red también en función del tiempo y de esta forma asegurar que un acceso se realice solo en estas horas, por ejemplo horario normal de trabajo, y no fuera de ellas.
- **Rango de direcciones IP**: es aconsejable regular el uso de la red mediante una limitación del rango de direcciones IP, especialmente para las redes con direcciones IP fijas. Un rango de direcciones IP claramente definido reduce considerablemente el peligro de un ataque.

### Asistente para reglas

El asistente para reglas le ayuda a definir con facilidad, reglas adicionales para el conjunto de reglas seleccionado o modificar reglas ya existentes.

El asistente para reglas le permite realizar las siguientes acciones:

- **Permitir o denegar el acceso de una aplicación determinada**: con esta función puede seleccionar una aplicación concreta y autorizarle o denegarle el acceso a la red dentro del marco del conjunto de reglas elegido. Para ello, seleccione en el asistente el programa deseado (ruta del programa) e introduzca en la **Dirección de conexión** si el programa debe bloquearse para conexiones entrantes, salientes o conexiones de los dos tipos. De esta forma, por ejemplo, puede impedir que el software de su reproductor de MP3 transmita datos sobre sus gustos musicales (conexión saliente) o que se encargue de que no se realicen actualizaciones automáticas del programa (conexión entrante).
- **Abrir o bloquear un puerto determinado**: en el asistente tiene la posibilidad de cerrar completamente determinados puertos o abrirlos únicamente para una aplicación determinada (por ejemplo, su software CRM).
- **Agregar una o varias reglas por defecto**: puede agregar reglas desde el conjunto de reglas estándar al conjunto de reglas seleccionado.
- **Copiar una regla existente**: puede crear una copia de una regla existente para editarla posteriormente.

## 4.3.13. PatchManager

PatchManager está disponible como **módulo opcional**.

PatchManager permite controlar con una sola interfaz la implementación de patches para todos los clientes administrados. PatchManager se puede usar para gestionar las actualizaciones tanto de los programas de Microsoft, como para los de otros fabricantes. Se puede probar y verificar cada patch, así como colocarlo en una lista negra, distribuirlo o retirarlo mediante una restauración (rollback). Esto es aplicable tanto para clientes individuales como para grupos.

## 4.3.13.1. Resumen de estado

El área Resumen de estado le ofrece un resumen detallado de los patches y su estado de implementación dentro de la red. Se enumeran para cada cliente y por orden alfabético todos los patches disponibles. Esta exhaustiva lista le permite comprobar fácilmente si todos los clientes están actualizados con todos los patches relevantes. También le permite planificar directamente la implementación de los patches. Un conjunto de gráficos muestra claramente informaciones acerca de los patches que aún no están instalados y permite evaluar rápidamente si hay patches importantes que necesitan ser instalados.

De forma predeterminada este resumen está agrupado por **Estado**, **Prioridad**, **Fabricante** y **Producto**, para poder determinar de forma más rápida si los patches importantes ya se han instalado o no. En la lista están excluidos tanto instaladores para programa completos, así como cualquier entrada bloqueada. Haga clic en **Restablecer los filtros** para restablecer los filtros. Las categorías se pueden ampliar para visualizar todos los patches que contienen las subcategorías.

Se pueden planificar diferentes clases de tareas para cada patch y cada cliente. Haga clic derecho sobre uno o varios patches y seleccione una de las siguientes opciones:

- **Comprobar si los patches son aplicables**: para planificar una tarea que comprueba si los patches seleccionados funcionan en los clientes seleccionados. En la ventana **Reconocimiento de software** se puede planificar la tarea.
- **Instalar patches**: en la ventana de **Distribución de software** se puede planificar la distribución de uno o varios patches en los clientes seleccionados.
- **Restaurar** para planificar una **restauración** de patches ya en uso en los clientes seleccionados.
- **Bloquear patches**: para bloquear uno o varios patches de forma que no se distribuyan a los clientes. Cuando se bloquean patches, estos tampoco se tienen en cuenta cuando se llevan a cabo tareas de evaluación y distribución (automatizadas).
- **Desbloquear patches**: para desbloquear uno o varios patches.
- **Propiedades**: para obtener más información sobre el patch correspondiente.

La columna de **Estado** muestra el estado de cada patch y las tareas de despliegue de patches planificadas o en curso.

### 4.3.13.2. Configuración

Aquí hay disponibles varias opciones para configurar la distribución de patches.

- **Activar PatchManagement**: activar o desactivar PatchManager.
- **Modo**: decidir si PatchManager debe ejecutar tareas de evaluación o distribución automatizadas.
  - **Manual**: PatchManager no ejecuta tareas de evaluación o distribución automatizadas.
  - **Comprobar uso de patches con alta prioridad automáticamente**: cada vez que se libera un patch de alta prioridad, PatchManager ejecuta automáticamente una tarea de evaluación en los clientes. Esto ahorra esfuerzos al no tener que planificar las tareas por separado.
  - **Instalar patches con alta prioridad automáticamente**: cada vez que se libera un patch de alta prioridad, PatchManager ejecuta automáticamente una tarea de instalación en todos los clientes (en los que el patch sea aplicable). El despliegue de patches puede ocasionalmente causar problemas de compatibilidad. Se recomienda evaluar los patches en un entorno no productivo antes de realizar el despliegue en el entorno productivo.
- **El usuario puede visualizar y solicitar patches**: el usuario tiene permiso para visualizar los patches disponibles y solicitar el despliegue.
- **El usuario puede rechazar la instalación de patches**: el usuario tiene permiso para denegar al menos temporalmente la instalación de un patch. Puede establecer cuántas veces puede rechazar el usuario una instalación hasta que la instalación se ejecute de forma obligatoria, y determinar cuántas veces debe intentar el sistema la instalación de un patch.

### 4.3.13.3. Configuración de patches

En el área Configuración de patches se pueden administrar de forma centralizada todos los patches conocidos y aplicables a todo el sistema. Un conjunto de gráficos muestra informaciones sobre los patches, los productos y los proveedores.

De modo predeterminado, los patches están agrupados por **Fabricante**, **Producto** y **Prioridad**; esto le permite encontrar rápidamente los patches para el producto correspondiente. En la lista están excluidos tanto instaladores para programas completos, así como cualquier entrada bloqueada. Haga clic en **Restablecer los filtros** para restablecer los filtros. Las categorías se pueden ampliar para visualizar todos los patches que contienen las subcategorías.

Haciendo clic con el botón derecho del ratón en uno o más patches se puede seleccionar las siguientes opciones:

- **Comprobar si los patches son aplicables**: para determinar si los patches seleccionados resultan aptos para usarlos en los clientes administrados. En ventana **Reconocimiento de software** puede planificar la tarea.
- **Instalar patches**: en la ventana de **Distribución de software** se puede planificar una tarea de distribución de uno o varios patches en los clientes seleccionados.
- **Bloquear patches**: para bloquear uno o varios patches de forma que no se distribuyan a los clientes. Cuando se bloquean patches, estos tampoco se tienen en cuenta cuando se llevan a cabo tareas de evaluación y distribución (automatizadas).
- **Desbloquear patches**: para desbloquear uno o varios patches.
- **Propiedades**: para obtener más información sobre el patch correspondiente.

La columna **Prioridad** muestra la prioridad de cada patch. Aquí también se pueden modificar las prioridades estándar definidas basándose en las especificaciones de la base de datos interna de PatchManager (**Baja**, **Normal**, **Alta**).

## 4.3.14. Registros

El módulo Registros muestra todos los **Eventos de seguridad** relacionados con el cliente, como por ejemplo alarmas de virus, solicitudes del PolicyManager, y **Registros de infraestructura** como por ejemplo cambios en los ajustes e informaciones de estado de tareas de escaneo.

### 4.3.14.1. Eventos de seguridad

Todos los virus detectados, solicitudes e informes del PolicyManager y todos los mensajes del cortafuegos se muestran en este área. Además, se muestran mensajes del sistema referentes a instalaciones, reinicios, etc. En la primera columna de la lista, la columna **Estado**, se muestra el tipo de evento (por ejemplo, **Virus encontrado** o **Archivo puesto en cuarentena**).

Si ha configurado las tareas de análisis de virus de forma que los virus encontrados solo se registren, puede seleccionar con ayuda del menú contextual (clic derecho), el menú **Eventos de seguridad** o la barra de herramientas, una o varias entradas de la lista y modificar esta reacción. Además de solo registrar, es posible eliminar y poner los archivos en cuarentena.

En el menú **Eventos de seguridad** y en menú contextual (clic derecho) están disponibles las siguientes funciones:

- **Vista**: defina si desea ver todos los informes o solo un tipo determinado de informes.

  - **Ocultar informes dependientes**: si hay informes idénticos disponibles (basados en los campos **Cliente**, **Remitente**, **Archivo / correo / contenido**) con esta función puede ocultar los mensajes o informes repetidos. Solo se muestra entonces la entrada más reciente.
  - **Ocultar informes leídos**: oculte los informes que ya haya leído.
- **Eliminar virus del archivo** (solo para informes de virus): intenta eliminar el virus del archivo original.
- **Poner archivo en cuarentena** (solo para informes de virus): mueva los archivos seleccionados a la carpeta de cuarentena. Los archivos se guardan codificados en la carpeta de Cuarentena del G DATA ManagementServer. Los archivos originales se borran. Al codificarlos se asegura que el virus no pueda causar ningún daño. Tenga en cuenta que para cada archivo en cuarentena existe un informe. Cuando borra un informe, se borra también el archivo correspondiente en la carpeta de cuarentena. Puede enviar un archivo de la carpeta de cuarentena al **Servicio de emergencia antivirus** para su análisis. Simplemente abra el menú contextual del informe de cuarentena haciendo clic derecho. Después de seleccionar la razón del envío, pulse el botón **Aceptar** en el cuadro de diálogo de informe.
- **Eliminar archivo** (solo para informes de virus): borra el archivo original en el cliente.
- **Definir como excepción del vigilante** (solo para informes del vigilante, solo en el menú contextual): crea una entrada en la lista blanca del vigilante en base al informe (ver **Ajustes de cliente** > **Vigilante** > **Configuración**).
- **Definir como excepción del ExploitProtection** (solo para informes de ExploitProtection; solo en el menú contextual): crea una entrada en la lista blanca de ExploitProtection basada en el informe (ver **Ajustes de cliente** > **Vigilante** > **Configuración**).
- **Anular el desbloqueo del teclado**: revoca la autorización otorgada a un teclado que fue detectado por USB Keyboard Guard y autorizado por el usuario final.
- **Cuarentena: limpiar y recuperar** (solo para informes de cuarentena): se intenta eliminar el virus del archivo. Si se consigue, el archivo limpio se coloca de nuevo en su lugar de origen en el cliente correspondiente. Si el virus no se puede eliminar, el archivo no se mueve a su ubicación original.
- **Cuarentena: restaurar** (solo para informes de cuarentena): mueve el archivo desde la carpeta de cuarentena a su lugar de origen en el cliente. Tenga en cuenta que el archivo se restablece a su estado original y sigue estando infectado.
- **Cuarentena: enviar a los laboratorios de G DATA Security** (solo para informes de cuarentena): si descubre un nuevo virus o un fenómeno desconocido, envíenos en cualquier caso ese archivo mediante la función cuarentena del software G DATA. Por supuesto, trataremos los datos que nos envíe con la máxima confidencialidad y discreción.
- **Cuarentena: eliminar archivo e informe** (solo para informes de cuarentena): borra los informes seleccionados y elimina los archivos correspondientes que estén en cuarentena.
- **Incluir URL en la lista blanca** (solo para informes relacionados con **Control de contenido web**): agrega la URL a la lista blanca para toda la red.
- **Incluir URL en la lista negra** (solo para informes relacionados con **Control de contenido web**): agrega la URL a la lista negra para toda la red.
- **Eliminar informe**: elimina los informes seleccionados. Si los informes a los que pertenece un archivo de cuarentena deben ser eliminados, deberá confirmarlo una vez más. En este caso, se eliminarán también los archivos en cuarentena.
- **Reducir informes**: si hay informes idénticos disponibles (basados en los campos **Cliente**,

**Remitente**, **Archivo / correo / contenido**) con esta función puede borrar los mensajes o informes repetidos.

La opción Reducir informes solo se aplica a los informes que se visualizan en ese momento. Si hay un filtro activo, todos los informes que estén ocultos no se tendrán en cuenta al realizar la limpieza. Si hay disponibles más de una página de informes, la limpieza solo se efectuará en la página activa.

- **Exportar informes** (solo en el menú contextual): exporta el informe, los informes seleccionados o la lista completa en un archivo XML.
- **Marcar como leído** (solo en el menú contextual): marca el informe seleccionado como leído.
- **Marcar como no leído** (solo en el menú contextual): marca el informe seleccionado como no leído.
- **Detalles/acciones** (solo en el menú contextual): algunos informes le permiten planificar directamente una tarea. Por ejemplo, si un cliente ha solicitado una restauración de patches, puede hacer clic derecho en el informe correspondiente y seleccionar Detalles/Acciones. En la ventana **Restauración** del módulo **Distribución de software** puede planificar directamente una tarea de restauración, sin tener que abrir el módulo **PatchManager** para seleccionar el patch y el cliente correspondiente.

La barra de iconos del módulo de Eventos de seguridad ofrece las siguientes opciones y configuración de filtros:

- **Actualizar**
- **Eliminar**
- **Imprimir**
- **Vista preliminar**
- **Eliminar virus**
- **Poner en cuarentena**
- **Eliminar archivo**
- **Recuperar archivo de la cuarentena**
- **Limpiar archivo y recuperarlo de la cuarentena**
- **Ocultar informes dependientes**
- **Ocultar informes leídos**
- **Periodo**

### 4.3.14.2. Registros de infraestructura

En esta área se visualizan informaciones del estado de los clientes, como por ejemplo actualizaciones del estado de las tareas de escaneo, actualizaciones de las firmas de virus y cambios en los ajustes.

El menú contextual o menú de clic derecho ofrece las siguientes funciones:

- **Actualizar**
- **Eliminar**
- **Marcar como leído**: marca los informes seleccionados como leídos.
- **Mark como no leído**: marca los informes seleccionados como no leídos.
- **Exportar**: exporta el informe, los informes seleccionados o la lista completa en un archivo XML.

La barra de iconos del módulo Registros de infraestructura ofrece las siguientes opciones y configuración de filtros:

- **Actualizar**
- **Eliminar**
- **Imprimir**
- **Vista preliminar**
- **Ocultar informes leídos**: oculta informes que ya han sido leídos.
- **Periodo**

### 4.3.15. Registros (iOS)

Si selecciona uno o varios clientes iOS en el área de **Clientes**, el módulo Registros solo le muestra detalles relacionados con los clientes iOS seleccionados. Los informes incluyen informaciones de estado relativas al despliegue de perfiles y acciones antirrobo.

- **Estado**: informe de estado.
- **Cliente**: nombre del dispositivo.
- **Fecha/Hora**: informe de marca temporal, con la fecha y hora.

Haga clic derecho en un informe y seleccione **Borrar** para eliminar el informe de la lista.

### 4.3.16. Estadística

En esta área de tareas puede visualizarse la información estadística sobre la propagación de virus y las infecciones en los clientes y en los correos electrónicos de Exchange Server, así como el estado de seguridad de la red administrada. Hay diferentes vistas disponibles; la información puede representarse en forma de texto o también en un gráfico (diagrama de barras o de sectores). La vista correspondiente puede seleccionarse en **Vista**. Hay información disponible sobre los **Clientes** (no disponible se ha seleccionado un servidor Exchange), sobre el **Virus detectados por**, sobre la **Lista de virus más frecuentes** y sobre la **Lista de infecciones bloqueadas**.

## 4.4. Módulos de servidor

Los módulos de servidor se pueden usar para configurar el servidor seleccionado en el área **Servidores** del panel **Clientes/ManagementServers**.

### 4.4.1. Servidores

Los módulos de servidor ofrecen varias funciones para gestionar los servidores, como por ejemplo informaciones de estado y versión, gestión de servidores de subred, gestión de usuarios y registros.

#### 4.4.1.1. Resumen

El panel Resumen se puede usar para comprobar informaciones de estado del servidor y para gestionar e instalar servidores de subred. Muestra las siguientes propiedades del servidor:

- **Nombre**: el nombre del servidor.
- **Tipo**: el tipo de servidor (Servidor principal, Servidor de subred, Servidor secundario).
- **Servidor**: el nombre del ManagementServer que ejerce el control (solo para servidores de subred y servidores secundarios).

- **Número de clientes**: número de clientes asignados en la actualidad al servidor seleccionado.
- **Último acceso**: marca temporal (fecha y hora) de la última sincronización con el ManagementServer principal (solo para servidores de subred).
- **Estado de datos**: el último intento de actualizar las firmas de virus.
- **Versión**: número de versión y fecha.
- **Estado**: información de estado del servidor, como por ejemplo actualizaciones.
- **Actualización de programa**: si una actualización está disponible para un servidor de subred, se mostrará aquí el estado de la misma.

En la barra de herramientas y el menú contextual (clic derecho) encontrará disponibles las siguientes opciones:

- **Actualizar**
- **Asistente de configuración del servidor**
- **Eliminar**: elimina un servidor de subred de la lista. El Software no será eliminado del servidor de subred.
- **Sincronizar** (solo en el menú contextual): con el botón puede ejecutar de forma manual la sincronización del servidor de subred.
- **Asignar clientes**: puede asignar clientes o grupos de clientes a servidores de subred concretos que canalizarán la comunicación de estos clientes con el servidor principal, optimizando de este modo el uso de la red. La asignación de clientes o grupos a los servidores de subred es independiente de la agrupación de clientes en el panel **Clientes/ManagementServers**. Esto implica que los clientes que están asignados a diferentes servidores de subred pueden, de todas formas, agruparse.
- **Agregar servidor de subred**: haga clic en el botón para agregar un servidor de subred nuevo. Introduzca el **Nombre del ordenador** del servidor de subred nuevo, así como una Cuenta de usuario con permisos de administrador en este servidor de subred. Confirme los datos introducidos con **Aceptar** para iniciar la instalación remota. La ventana **Resumen de instalación** le permite observar el estado de la instalación. Los requisitos previos para la instalación remota de un servidor de subred son los mismos que para la **instalación remota de G DATA Security Client**. Los servidores de subred usan Microsoft SQL Server 2014 Express, el cual no soporta Windows Vista o Windows Server 2008/2003. En estos sistemas, los servidores de subred pueden instalarse a través de la opción servidor de subred en la instalación local de G DATA Management Server.
- **Desinstalar servidor**: inicia una desinstalación remota del servidor de subred elegido. **Resumen de instalación** le permite observar el estado en el que se encuentra la desinstalación. La desinstalación remota solo puede ejecutarse en servidores de subred autorizados.
- **Otorgar Autorización**: para evitar un acceso no autorizado al servidor de datos, debe autorizar los servidores de subred locales. Solo después de la autorización se sincronizarán los datos del ManagementServer con los servidores de subnet.

  Los servidores de subred agregados mediante una instalación remota desde **Agregar servidor de subred**, reciben automáticamente la autorización. Por el contrario los servidores de subred agregados de manera local y los que han sido actualizados a la versión 13 deben ser autorizados manualmente.
- **Permitir actualización de programa** (solo en el menú contextual): los servidores de subred con ManagementServer versión 12, requieren una instalación manual de la base de datos del

servidor antes de poder actualizar a la versión 14. En tales sistemas, instale primeramente Microsoft SQL Server 2014 Express (Windows Server 2008 R2/Windows 7 y posteriores) o Microsoft SQL Server 2008 R2 Express (Windows Server 2003/2008/Windows Vista), después use esta opción para permitir la actualización del programa. Después de la actualización, use GdmmsConfig.exe en el servidor de subred para configurar la conexión con la base de datos. Para más información consulte la guía de referencia.

- **Propiedades** (solo en el menú contextual): se visualizan las propiedades del servidor seleccionado, incluyendo la versión del ManagementServer, las firmas de virus y los archivos de programa del cliente.

**Asistente de configuración del servidor**
Con el Asistente de configuración del servidor se pueden configurar algunos de los ajustes principales del G DATA ManagementServer. El asistente se ejecuta automáticamente al iniciar por primera vez G DATA Administrator; pero también se puede ejecutar posteriormente en **Servidores** > **Resumen** desde el menú **Admin**.

En primer lugar hay que activar todos los clientes que se van a gestionar con el software G DATA. Para activarlos, marque los clientes que desea habilitar y haga clic en el botón **Activar**. Es posible que algunos ordenadores no estén incluidos en la lista (por ejemplo, si el ordenador en cuestión llevaba tiempo sin conectarse o si no ha habilitado compartir archivos e impresoras). Para activar estos clientes, introduzca el nombre del ordenador en el campo de entrada **Ordenador**. Tras hacer clic en **Activar** se incluirá el ordenador en la lista de clientes. Una vez activados todos los ordenadores que se desean proteger, haga clic en **Siguiente** para continuar. Si ha activado clientes, la casilla **Instalar el software de cliente automáticamente en los ordenadores activados** estará marcada por defecto. Si prefiere distribuir el software en los clientes más tarde, desactive esta opción desmarcando la casilla.

Los siguientes pasos del asistente le ayudan a configurar algunos de los ajustes más comunes:

- **Actualización online**: configure las actualizaciones de las firmas de virus y los archivos de programa. Para más Información consulte el modulo **Actualizaciones**.
- **Notificación por correo electrónico**: configure los ajustes del servidor de correo, grupos de destinatarios y notificaciones de alerta. Encontrará más información en **Configuración general** > **Correo electrónico**.
- **Ajustes para dispositivos móviles**: configure la gestión de los dispositivos móviles para. Encontrará más Información en **Configuración general** > **Android**.
- **Ajustes para el acceso a G DATA ActionCenter**: se requieren credenciales para ActionCenter para habilitar la gestión de dispositivos iOS y la supervisión de red. Encontrará más Información en el módulo ActionCenter.

Pulsando **Finalizar** se cierra el asistente. Si selecciona la opción **Instalar el software de cliente automáticamente en los ordenadores activados**, el asistente de configuración del servidor realiza una **Instalación remota** de G DATA Security Client en todos los dispositivos de red seleccionados.

## 4.4.1.2. Administración de usuarios

Como administrador del sistema, puede otorgar acceso a otros usuarios a la interfaz del G DATA Administrator. Para ello, haga clic en el botón **Nuevo** y, a continuación, escriba el **Nombre de usuario**, los **Permisos** de este usuario (**Leer**, **Leer / escribir**, **Leer / escribir / restaurar copias de seguridad**), defina el **Tipo de cuenta** (**Inicio de sesión integrado**, **Usuario de Windows**, **Grupo de**

**usuarios de Windows**) y asigne una **Contraseña** para este usuario.

### 4.4.1.3. Registros de infraestructura

En el área Registros de infraestructura se visualizan informaciones de estado del servidor, como por ejemplo actualizaciones de las firmas de virus y de archivos de programa. La opciones disponibles en la barra de herramientas y el menú contextual son idénticas a las que hay disponibles en el módulo clientes **Registros** > **Registros de infraestructura**.

## 4.4.2. Configuración general

El módulo Configuración general se puede usar para configurar ajustes generales del servidor, como por ejemplo la sincronización entre los servidores de subred y los clientes, directorios de copia de seguridad, ajustes del servidor de correo y ajustes de gestión de dispositivos móviles.

### 4.4.2.1. Limpieza

Los ajustes de Limpieza le permiten configurar que algunos elementos se eliminen de forma automática después de un periodo concreto de tiempo:

- **Eliminar automáticamente registros de infraestructura**: elimina los registros de con una antigüedad mayor de la establecida.
- **Eliminar registros de escaneo automáticamente**: elimina los registros de escaneo con una antigüedad mayor de la establecida.
- **Eliminar automáticamente eventos de seguridad**: elimina los informes cuando transcurra cierta cantidad de meses.
- **Eliminar historial de informes automáticamente**: elimina el historial de informes al cabo de unos meses definidos.
- **Eliminar clientes automáticamente tras inactividad**: elimina los clientes que no se han conectado desde hace una determinada cantidad de días.
- **Eliminar archivos de patches automáticamente**: elimina automáticamente los archivos de patches después de un tiempo especificado.

### 4.4.2.2. Sincronización

En el área de Sincronización puede definir el intervalo de sincronización entre clientes, servidores de subred y ManagementServer principal:

- **Intervalo de sincronización con el servidor principal para comprobar si existen nuevas actualizaciones**: introduzca aquí el intervalo de tiempo en el que los clientes se conectan al servidor para comprobar si existen nuevas actualizaciones y configuraciones. El valor estándar establecido es de cinco minutos. Si se activa la marca de verificación en **Notificar a los clientes en caso de modificación de las opciones del servidor**, los clientes reciben inmediatamente una notificación cuando hay cambios en los ajustes, independientemente del intervalo desincronización.
- **Servidor de subred**: en esta área puede definir el intervalo para la sincronización entre MMS y el servidor de subred(s). Si marca la opción **Transmitir inmediatamente informes nuevos al servidor principal**, los informes nuevos se transmitirán inmediatamente al servidor principal, independientemente de los ajustes definidos aquí.
- **Active Directory**: aquí se define el intervalo en que G DATA ManagementServer sincroniza el

contenido de Active Directory. Si configura una sincronización diaria, puede definir la hora exacta a la que se debe realizar la sincronización. La sincronización de Active Directory solo se realiza cuando se haya **asignado** como mínimo un grupo a una unidad organizativa de Active Directory.

### 4.4.2.3. Límite de carga

Si se marca la casilla **Activar límite de carga**, es posible establecer cuántos clientes pueden realizar al mismo tiempo las acciones que se indican. De esta manera, se puede distribuir la carga para que, por ejemplo, no se produzca un aumento de latencia en la red al efectuar actualizaciones o informes simultáneamente.

### 4.4.2.4. Copia de seguridad

Backup está disponible como **módulo opcional**.

Para garantizar que las órdenes de copia de seguridad se ejecuten con éxito, deberá haber espacio suficiente disponible, tanto en el servidor (memoria de backup) como en el cliente (caché de backup). Puede definir valores mínimos para mensajes de advertencia y mensajes de error tanto para el servidor como para los clientes. Si el espacio libre en el servidor o el cliente es menor que el umbral de advertencia ajustado, se genera un informe de advertencia en el módulo **Eventos de seguridad** y se limpia automáticamente el caché del cliente, conservando solo el último archivo y eliminando todos los demás (si se han subido al ManagementServer). Si el espacio libre en el servidor o el cliente es menor que el umbral de error ajustado, se genera un informe de error en el módulo **Eventos de seguridad**. El almacenamiento de copia de seguridad y el caché del cliente se limpian automáticamente. Si sigue sin haber suficiente espacio libre en el disco o en el servidor, no se ejecutarán las copias de seguridad.

En **Directorios de copia de seguridad del lado del servidor** se puede introducir la ruta en la que se guardarán todas las copias de seguridad acumuladas. Si no se introduce ningún directorio, todas las copias de seguridad se guardan en C:\ProgramData\G DATA\AntiVirus ManagementServer\Backup o bien en C:\Documents and Settings\Todos los usuarios\Application Data\G DATA\AntiVirus ManagementServer\Backup.

Como todas las copias de seguridad creadas con el software G DATA están cifradas, las contraseñas de las copias de seguridad también se pueden exportar y guardar para un uso posterior. Con el botón **Importar archivos comprimidos de copia de seguridad** se permite el acceso a las copias de seguridad guardadas en otras carpetas.

### 4.4.2.5. Correo electrónico

El G DATA ManagementServer puede enviar automáticamente mensajes de alarma por correo electrónico cuando se producen determinados eventos. Los ajustes requeridos se efectúan en esta área. La notificación por correo electrónico se activa colocando la marca de verificación en los eventos susceptibles de notificación. Mediante la opción **Limitación** se puede evitar la recepción excesiva de correos en caso de una infección masiva de virus. Haga clic en **Activar prueba de alarma**, para enviar una alarma de prueba al grupo de destinatarios.

Para realizar modificaciones en la **Configuración de correo** pulse el botón de configuración avanzada ( ).

**Configuración de correo**
Introduzca aquí el **Servidor SMTP** y el **Puerto** (normalmente 25) que G DATA ManagementServer deba usar para enviar correos. También se necesita una dirección de remitente (válida) para que se puedan enviar los correos. En caso de que su servidor SMTP requiera autenticación, haga clic en **Autenticación SMTP** para realizar los ajustes necesarios. Puede configurar el procedimiento para **SMTP AUTH** (iniciar sesión directamente en el servidor SMTP) o para **SMTP después de POP3**, si el servidor SMTP lo requiere.

En **Grupos de correo** se pueden administrar listas de diferentes destinatarios, por ej. el equipo de administración, los técnicos, etc.

### 4.4.2.6. Android

El área para Android dispone de algunos ajustes generales para la autenticación de clientes móviles y la mensajería de la nube de Google.

Introduzca en **Autenticación para clientes móviles** una **Contraseña**, con la que el dispositivo Android tiene que autenticarse en el ManagementServer. Para poder realizar acciones de emergencia, tiene que introducir la **ID del emisor** y la **Clave API** de su cuenta del servicio de mensajería en la nube de Google (GCM). Pueden configurarse cuentas gratuitas para esta notificación en **code.google.com/apis/console**. Encontrará más información al respecto en la Guía de referencia.

## 4.4.3. Actualizaciones

Todos los clientes tienen una copia propia local de la base de datos de virus, de esta forma se garantiza también la protección cuando no disponen de conexión con el G DATA ManagementServer o con Internet. La actualización de las firmas de virus en el cliente se realiza en dos pasos que, por supuesto, pueden automatizarse. En el primer paso se descargan los archivos más actuales del servidor de actualizaciones G DATA y se copian a una carpeta del G DATA ManagementServer. En el segundo paso se distribuyen los nuevos archivos a los clientes (consulte el área de tareas **Ajustes de cliente** > **General**).

### 4.4.3.1. Actualizaciones de firmas

En el área de actualizaciones de firmas puede configurar el proceso de descarga de actualizaciones de las firmas de virus desde el servidor de actualizaciones al G DATA ManagementServer.

En **Estado** están disponibles las siguientes informaciones y ajustes:

- **Versión de motor A**: la versión actual de las firmas de virus para el motor A en el G DATA ManagementServer.
- **Versión de motor B**: la versión actual de las firmas de virus para el motor B en el G DATA ManagementServer.
- **Última ejecución**: marca temporal (fecha y hora) de la última ejecución del proceso de actualización de las firmas de virus.
- **Estado**: el estado en que se encuentra el proceso de actualización de las firmas de virus.
- **Actualizar estado**: actualiza la visualización del campo **Estado**.
- **Iniciar actualización ahora**: inicia una actualización inmediata de la base de datos de las firmas de virus en el G DATA ManagementServer.

En **Actualizaciones automáticas** se pueden programar las actualizaciones de las firmas de virus. Solo necesita marcar la opción **Ejecutar actualización periódicamente** especificando el momento o la frecuencia con que deben realizarse las mismas. Para que la actualización se realice automáticamente, G DATA ManagementServer debe estar conectado a Internet, además es necesario haber introducido el nombre de usuario y la contraseña que recibió cuando registró la licencia en **Actualizaciones** > **Datos de acceso y configuración**. Si el servidor se conecta a Internet a través de un servidor proxy introduzca sus credenciales de proxy.

La distribución de las actualizaciones se puede realizar de forma centralizada (desde el ManagementServer o el servidor de subred a los clientes) o bien, activando la marca de verificación correspondiente, también de modo descentralizado, peer to peer (permitiendo que clientes ya actualizados distribuyan las actualizaciones a otros clientes). Asegúrese en este caso de adaptar la **configuración del puerto**.

### 4.4.3.2. Actualizaciones de programa

En el área de actualizaciones de archivos de programa puede configurar el proceso de descarga de actualizaciones de archivos de programa desde el servidor de actualizaciones al G DATA ManagementServer.

En **Archivos de programa (cliente)** están disponibles las siguientes informaciones y ajustes:

- **Versión actual**: la versión actual de los archivos de programa del G DATA ManagementServer.
- **Última ejecución**: marca temporal (fecha y hora) de la última ejecución del proceso de actualización de los archivos de programa.
- **Estado**: el estado en que se encuentra el proceso de actualización de los archivos de programa.
- **Actualizar estado**: actualiza la visualización del campo **Estado**.
- **Iniciar actualización ahora**: inicia una actualización inmediata de los archivos de programas del cliente en el G DATA ManagementServer.

En **Actualizaciones automáticas** se pueden programar las actualizaciones de los archivos de programa. Los ajustes son idénticos a los ajustes disponibles en **Actualizaciones de firmas**.

> El G DATA ManagementServer solo se puede actualizar desde el menú de inicio. Para actualizar los archivos de programa del G DATA ManagementServer, debe seleccionar en el grupo de programas G DATA ManagementServer del menú Inicio la opción **Actualización online**.

### 4.4.3.3. Distribución escalonada

En el área **Distribución escalonada** se puede establecer si las actualizaciones de los archivos de programa se transfieren a todos clientes a la vez o progresivamente. La distribución escalonada reduce la carga del sistema que conlleva inevitablemente una actualización de programa de estas características.

Si opta por una distribución escalonada, puede definir manualmente que clientes deben ser los primeros en recibir la actualización o dejar que la selección para el primer grupo se realice de forma automática. También puede elegir el número total de grupos y la demora en el despliegue entre los diferentes grupos.

### 4.4.3.4. Datos de acceso y configuración

Cuando realiza el registro online recibe los datos de acceso para la actualización de la base de datos de virus y los archivos de programa. Introdúzcalos en **Usuario** y **Contraseña**. Seleccione en **Región el servidor** de actualizaciones más cercano, para garantizar una velocidad óptima al descargar las actualizaciones. Por lo general, conviene mantener activa siempre la **Comprobación de versión** (que viene activada por defecto ya que garantiza una velocidad de actualización óptima. Si surgen problemas con los archivos locales de la base de datos de virus, desactive la comprobación de versión. De este modo, durante la siguiente actualización online, se comprueba la integridad de todos los archivos de la base de datos de virus y los archivos defectuosos se descargan de nuevo.

Con el botón **Configuraciones proxy** se abre una ventana en la que se pueden introducir las credenciales del servidor proxy. Introdúzcalas solo en el caso de que solo sea posible ejecutar la actualización online a través de un servidor proxy.

> El software G DATA puede utilizar los datos de conexión de Internet Explorer (a partir de la versión 4). Configure en primer lugar Internet Explorer y compruebe si puede acceder a la página de prueba de nuestro servidor de actualización: http://ieupdate.gdata.de/test.htm. Desconecte, a continuación, la opción **Utilizar servidor proxy**. Introduzca en **Cuenta de usuario** la cuenta que ha configurado para Internet Explorer (es decir, la cuenta con la que haya iniciado la sesión en su ordenador).

### 4.4.3.5. Restaurar firmas

En caso de falsas alarmas o de problemas similares que pueden surgir en raras ocasiones, puede ser recomendable bloquear la actualización de las firmas de virus en curso y utilizar en su lugar una de las actualizaciones de firmas anteriores. Introduzca en **Restauraciones** cuántas actualizaciones de firmas de virus desea tener de reserva para Restauraciones. Como valor estándar se aplican aquí las últimas cinco actualizaciones de firmas del motor correspondiente.

En caso de que surjan problemas con la actualización en curso del motor A o B, el administrador de red puede bloquear por un periodo de tiempo esa actualización y distribuir a los clientes y servidores de subred una actualización de firmas anterior.

> No es posible realizar restauraciones en los clientes que no están conectados con el G DATA ManagementServer (por ejemplo, los ordenadores portátiles en viajes de negocios). No se puede deshacer un bloqueo de nuevas actualizaciones transmitido por el servidor al cliente sin establecer conexión con el G DATA ManagementServer.

Seleccione en la lista desplegable el **Motor** afectado, en **Actualizaciones bloqueadas** se enumeran las actualizaciones más recientes de este motor. Seleccione la actualización o las actualizaciones que deben bloquearse, y haga clic en Aceptar. De esta forma se bloquea la distribución de estas actualizaciones y los clientes que las hayan recibido antes se restablecen a la última actualización no bloqueada. Esto ocurre en cuanto se conectan al ManagementServer. De forma opcional, puede bloquear automáticamente nuevas actualizaciones hasta una determinada fecha, que se puede seleccionar. Solo a partir de entonces se ejecutarán actualizaciones en los clientes. Utilice para ello la función **Bloquear nuevas actualizaciones hasta**.

## 4.4.4. ReportManager

El ReportManager le proporciona una visión general del estado de los clientes, la seguridad del sistema y el despliegue de patches. Con el ReportManager se pueden generar informes programados

y distribuirlos a grupos predefinidos.

En la barra de herramientas están disponibles las siguientes opciones:

- **Actualizar**
- **Eliminar**
- **Añadir nuevo plan de informes**: en la ventana de diálogo correspondiente se puede definir un nuevo informe y programar una tarea de informes.

Para realizar una copia de seguridad de las definiciones de informes, haga clic en **Exportar**. Por el contrario para restaurar las definiciones haga clic en **Importar**. Haga clic derecho del ratón en una o más definiciones de informes y luego en **Eliminar** para eliminarlas; o en **Ejecutar de inmediato**, para ejecutarlas de nuevo directamente. Para editar un informe, haga clic en **Propiedades**.

### 4.4.4.1. Definición del informe

La ventana Definición del informe le permite especificar qué módulos de informe, con sus correspondientes informaciones y estadísticas, va a contener el informe. Una vez seleccionados los módulos, se puede programar una tarea para generar periódicamente el informe correspondiente.

Esta ventana cuenta con opciones de programación semejantes a las que hay disponibles para la mayoría de tareas programadas. Una vez definido el **Nombre** del informe y el **Idioma** en que se va a redactar, establezca el intervalo de tiempo para el informe (una vez, diariamente, semanalmente, mensualmente, etc.). En los **Grupos de destinatarios** se puede establecer la lista de destinatarios que van a recibir ese informe. Puede usar los grupos creados en **Configuración general** > **Correo electrónico** > **Configuración de correo** o también definir directamente nuevos grupos de destinatarios. Además, en el campo de entrada **Destinatarios adicionales** puede añadir más direcciones de correo para el informe correspondiente (los destinatarios van separados por comas).

Se pueden agregar módulos a un informe concreto haciendo clic en el botón **Nuevo** en **Módulos seleccionados**. La disponibilidad de los módulos depende de la solución de seguridad de G DATA que use. Los módulos para la planificación del informe se dividen en tres categorías, **Cliente en general**, **Protección del cliente** y **PatchManager**. Seleccione el módulo correspondiente y configure los ajustes en el área inferior de la ventana. Para cada módulo se puede elegir también un formato especial de salida. Se puede elegir entre **Tabla**, **Diagrama de líneas**, **Diagrama de barras (3D)** o **Diagrama de sectores (3D)**. Tenga en cuenta que no todos los módulos son compatibles con el formato de salida. En algunos módulos se puede además definir un **Límite** para la cantidad de los datos representados o seleccionar en consonancia un marco cronológico para la representación. Haga clic en **Aceptar** para agregar los módulos seleccionados al informe correspondiente. Para **Editar** o **Eliminar** módulos use los botones correspondientes. Cuando acabe de seleccionar y configurar los módulos, en **Vista preliminar** puede realizar un informe de prueba con los ajustes realizados. Por último haga clic en **Aceptar** para guardar el informe.

Cuando se ha ejecutado la tarea, el informe creado aparece en el resumen del **ReportManager** y se envía a los destinatarios seleccionados. Para ver todas las instancias de un informe, solo tiene que hacer doble clic en el informe respectivo y abrir los informes asociados.

El ordenador en el que se ejecuta G DATA Administrator debe disponer de Internet Explorer 8 o superior, para poder mostrar la vista preliminar de los informes y la vista de instancias del informe.

### 4.4.5. Administración de licencias

El resumen de licencias le dará una visión general de cuántas licencias de G DATA tiene instaladas en su red. Si necesita licencias adicionales puede ponerse en contacto con el Centro de actualizaciones de G DATA en cualquier momento, pulsando el botón **Ampliar licencias**.

El botón **Exportar** le permite obtener un archivo de texto con un resumen de todas las licencias en uso.

### 4.4.6. G DATA ActionCenter

Para gestionar los dispositivos iOS el G DATA Administrator se conecta al G DATA ActionCenter. **Cree una cuenta** e introduzca aquí su **Nombre de usuario** y **Contraseña**.

Para poder usar G DATA ActionCenter es necesario disponer de una licencia de G DATA válida. Asegúrese de que ha introducido su **Nombre de usuario** y su **Contraseña** para las actualizaciones online en **Actualizaciones** > **Datos de acceso y configuración**.

> La comunicación con G DATA ActionCenter depende de las características de seguridad que están disponibles en Windows Vista y versiones posteriores. iOS Mobile Device Management y Monitoreo de red no están disponibles en el G DATA ManagementServer y el G DATA Administrator en máquinas que ejecutan Windows XP o Windows Server 2003.

# 5. G DATA WebAdministrator

G DATA WebAdministrator es un software de gestión basado en la web para G DATA ManagementServer. Se puede utilizar para editar y actualizar ajustes para el G DATA ManagementServer en un navegador a través de una interfaz web.

## 5.1. Iniciar G DATA WebAdministrator

Una vez completada la instalación, para iniciar el G DATA WebAdministrator, no tiene más que hacer doble clic en el icono correspondiente del escritorio. Alternativamente, puede también abrir el navegador de Internet e ir a la URL que se le comunicó al terminar el proceso de instalación La URL consta de una dirección IP o el nombre del ordenador en el que se ejecuta IIS y donde está instalado WebAdministrator, y del sufijo de la carpeta (p.ej. *http://10.0.2.150/GDAdmin/*). Si todavía no ha instalado el plug-in para el navegador Silverlight de Microsoft, ahora se le solicitará descargarlo.

Entonces se abrirá automáticamente una página de inicio de sesión para el acceso al G DATA WebAdministrator. Introduzca aquí, igual que en **G DATA Administrator**, el **Idioma**, el **Servidor**, la **Autenticación**, el **Usuario** y la **Contraseña** y pulse el botón **OK**. Por defecto, normalmente se introduce el nombre del servidor, pero pude modificarlo si es necesario. Elija la **Autenticación Windows** para iniciar sesión con sus credenciales de Windows; o la **Autenticación Integrada** para usar las credenciales que definió en su momento.

## 5.2. Empleo de G DATA WebAdministrator

La interfaz del programa G DATA WebAdministrator es muy parecida a la de G DATA Administrator. Después de abrir sesión verá el panel de control que le ofrece un panorama general de su red, los clientes y el estado de G DATA ManagementServer.

Las funciones de WebAdministrator son idénticas a las de G DATA Administrator. Se explican detalladamente en el capítulo **G DATA Administrator**.

# 6. G DATA MobileAdministrator

G DATA MobileAdministrator es una interfaz intuitiva y móvil para la gestión del programa G DATA ManagementServer. Se puede emplear para editar y actualizar rápidamente ajustes a través de una interfaz optimizada para dispositivos móviles. Las funciones principales y de mayor uso de G DATA Administrator se han agrupado para permitir su utilización en los entornos de una amplia gama de smartphones diferentes.

## 6.1. Iniciar G DATA MobileAdministrator

Una vez instalado, G DATA MobileAdministrator se puede abrir desde cualquier navegador. Para ello solo tiene que iniciar su navegador y abrir la URL que se le comunicó al final del proceso de instalación. La URL consta de una dirección IP o el nombre del ordenador en el que se ejecuta IIS y donde está instalado MobileAdministrator, y del sufijo de la carpeta (p. ej. *http://10.0.2.150/GDMobileAdmin/*).

La página de inicio de sesión de MobileAdministrator tiene una estructura idéntica a la página de inicio de sesión de **G DATA Administrator** y **G DATA WebAdministrator**. Introduzca aquí el **Servidor**, el **Usuario**, la **Contraseña** y el **Idioma**. Seleccione la **Autenticación de Windows** si desea iniciar sesión con sus credenciales de Windows (dominio); o **Autenticación integrada** para iniciar sesión con las credenciales que se definieron en su momento. Si desea que sus datos de acceso (excepto la contraseña) estén disponibles de nuevo la próxima vez que abra la página de inicio de sesión, seleccione **Recordar los datos de usuario**. Pulse en **Inicio de sesión** para finalizar el proceso.

## 6.2. Usar G DATA MobileAdministrator

Al abrir sesión en G DATA MobileAdministrator se visualiza el menú principal. Están disponibles cuatro funciones: **Panel de control**, **Informes**, **Clientes** y **ReportManager**. Para cerrar el programa, pulse el botón **Cerrar sesión** situado arriba a la derecha.

### 6.2.1. Panel de control

En el panel de control de G DATA MobileAdministrator se muestran las principales estadísticas sobre su red. De modo análogo a la vista del panel de control en G DATA Administrator, aquí se obtiene una vista general del G DATA ManagementServer y sus clientes. Además, se pueden visualizar estadísticas sobre las conexiones de clientes y las infecciones bloqueadas.

Seleccione **Estado de G DATA Security** para obtener un resumen más detallado sobre el estado de los servidores y los clientes. MobileAdministrator le muestra cuantos clientes tienen instalado G DATA Security Client y le ofrece información sobre el estado de actualización de las firmas de virus y otros componentes del programa, como por ej. el vigilante, el análisis de correo, OutbreakShield y el cortafuegos. Se pueden realizar directamente restauraciones de ambos motores abriendo la subsección de las firmas de virus. El estado del propio ManagementServer se puede observar con más detalle si se selecciona **Estado del servidor**.

Encontrará más estadísticas en **Conexiones del cliente** y **Lista de los 10 clientes más frecuentes - Infecciones rechazadas**. Pulse **Estado de informe** para visualizar informaciones acerca de infecciones, solicitudes e informes de errores.

### 6.2.2. Informes

Aquí encontrará informes sobre virus, eventos de Cortafuegos y mensajes del PolicyManager. Se trata de una representación optimizada para dispositivos móviles que contiene la misma información que figura en el G DATA Administrator en el área de **Eventos de seguridad**.

Seleccione en **Periodo** si desea visualizar los informes del día anterior, de los últimos siete días o del último mes. MobileAdministrator le mostrará las categorías para las que hay informes disponibles. Pulse una de las categorías para obtener un listado de los eventos registrados. Los informes se pueden filtrar por nombre. Puede abrir cualquier informe para ver más detalles y tomar medidas, si es necesario.

### 6.2.3. Clientes

MobileAdministrator ofrece un resumen de todos los clientes que administra G DATA ManagementServer. Hay información detallada de cada cliente y los principales ajustes de seguridad se pueden modificar directamente con el MobileAdministrator.

En la vista general se puede visualizar una lista de todos los ordenadores que administra G DATA ManagementServer. Esta lista se puede filtrar también por nombre. Seleccionando un cliente determinado se pueden visualizar varias estadísticas acerca de las versiones y actualizaciones de ese cliente. Además, se pueden modificar directamente ajustes importantes de seguridad. Se puede por ejemplo activar y desactivar el **Vigilante**, determinar si se van a procesar o no **Contenidos de Internet (HTTP)**, así como activar y desactivar el **Escaneo en modo reposo** o el **Cortafuegos**. También se pueden gestionar y editar ajustes tales como **Control de aplicación**, **Control de dispositivos**, **Control del contenido web** y **Tiempo de utilización de Internet**.

### 6.2.4. ReportManager

ReportManager es una versión optimizada para dispositivos móviles del área de **ReportManager** en G DATA Administrator. Le permite configurar informes, programarlos y obtener una vista previa.

Para agregar una nueva orden de informe, pulse la opción **Añadir planificación**. Los informes ya existentes están listados en la ventana principal y pueden ser editados con solo pulsarlos; es posible modificar todos los aspectos de la tarea. Introduzca un **Nombre**, defina el **Idioma** y seleccione los destinatarios en **Grupos de destinatarios** o introduzca **Destinatarios adicionales**. Puede programar la tarea y seleccionar un **Intervalo** o definir una fecha y hora concretas. En **Módulos seleccionados**, puede elegir los módulos de informe que desee incluir en este informe. Los módulos son los mismos que hay disponibles en G DATA Administrator. Edite, agregue o elimine módulos y pulse **Guardar** volver a la ventana principal. Si es necesario puede visualizar el informe en **Vista preliminar** antes de guardarlo. Las tareas duplicadas o innecesarias se pueden eliminar.

# 7. G DATA Security Client

G DATA Security Client proporciona la protección antivirus a los clientes Windows y ejecuta en segundo plano, sin interfaz de usuario propia, las tareas encargadas por el G DATA ManagementServer. Los clientes tienen sus propias firmas de virus y su propio programador para que se puedan efectuar las tareas también en modo fuera de línea (por ejemplo, en los ordenadores portátiles que no tienen conexión permanente con el G DATA ManagementServer).

Después de **instalar** el software de cliente, el usuario del cliente tiene a su disposición un icono en la bandeja del sistema con el que puede acceder a funciones de protección de virus, independientemente de los tiempos programados por el administrador. La funciones que el usuario tiene disponibles, las tiene que definir en calidad de administrador en el área **Ajustes de cliente** de G DATA Administrator.

Haciendo clic con el botón derecho del ratón sobre este icono de G DATA Security Client el usuario puede abrir un menú contextual que le ofrece acceso a todas funciones disponibles.

## 7.1. Análisis de virus

Con esta opción, el usuario puede examinar selectivamente su ordenador con G DATA Security Client, incluso fuera de los periodos de verificación establecidos por G DATA Administrator, para descartar la presencia de virus.

El usuario también puede analizar dispositivos extraíbles, CDs o DVDs, la memoria, el área de inicio automático y archivos o directorios individuales. De este modo, los usuarios de portátiles que en raras ocasiones conectan su ordenador a la red de la empresa pueden prevenir eficazmente los ataques de virus. Mediante la ventana **Opciones** los usuarios del cliente pueden determinar las medidas que se deben tomar en caso de detectar un virus (como por ej. mover el archivo al área de cuarentena local).

> El usuario también puede comprobar con facilidad archivos o directorios en el Explorador de Windows marcándolos y activando la función **Comprobar virus (G DATA Antivirus)** en el menú contextual.

Mientras se está realizando un análisis en busca de virus, independientemente de si se ha iniciado a nivel local o si es parte de una tarea de escaneo, en el menú contextual están disponibles las siguientes entradas:

- **Prioridad del análisis de virus**: el usuario puede aquí establecer la prioridad del análisis de virus. Con la opción **Alta**, el análisis de virus se efectúa con rapidez, pero como contrapartida puede ralentizar notablemente el trabajo de otros programas en ese ordenador. Con el ajuste **Baja** el análisis de virus tarda más en comparación, pero en cambio se puede seguir trabajando durante el proceso en el ordenador cliente sin grandes limitaciones. Esta opción solo está disponible cuando se ha iniciado un análisis de virus local.
- **Detener el análisis de virus**: esta opción le permite al usuario detener un análisis de virus local. Las órdenes de escaneo determinadas por el G DATA ManagementServer pueden detenerse solo si el administrador ha activado la opción **El usuario puede detener o cancelar la orden**.
- **Cancelar el análisis de virus**: esta opción le permite al usuario cancelar un análisis de virus local. Las órdenes de escaneo determinadas por el G DATA ManagementServer pueden cancelarse solo si el administrador ha activado al crearlas la opción **El usuario puede detener o cancelar la orden**.

- **Mostrar ventana de escaneo**: el usuario puede visualizar el progreso y los resultados del análisis de virus. Esta opción solo está disponible cuando se ha iniciado un análisis local.

La opción Análisis de virus puede activarse y desactivarse en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

## 7.2. Desactivar el vigilante

Con este comando el usuario puede desactivar el vigilante de G DATA durante cierto periodo de tiempo (desde 5 minutos hasta el próximo reinicio del PC). Desactivar el vigilante de forma temporal puede ser útil durante procesos de copia de archivos que requieren mucho tiempo, ya que así se acelera el proceso de copiado. No obstante, hay que tener en cuenta que la protección antivirus en tiempo real se encuentra desactivada durante este periodo.

La opción Desactivar el vigilante puede activarse y desactivarse en el G DATA Administrator, en **Ajustes de cliente** > **General** > **Funciones de cliente**.

## 7.3. Opciones

El usuario del ordenador cliente tiene en Opciones la posibilidad de modificar los ajustes de seguridad para los siguientes componentes: **Vigilante**, **Correo electrónico**, **Análisis de virus** (local), **Web/IM** y **AntiSpam**. De este modo, es posible desactivar todos los mecanismos de protección del software G DATA en el cliente. Por tanto, esta opción solo debe ser accesible para los usuarios conocedores de la materia. Las distintas posibilidades de ajuste se explican detalladamente en el área **Ajustes de cliente**.

Las diferentes configuraciones puede activarse y desactivarse en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

## 7.4. Cuarentena

Cada cliente tiene un directorio de cuarentena local al que se pueden mover los archivos infectados (dependiendo de la configuración del vigilante/orden de escaneo). Un archivo puesto en cuarentena no puede, aunque contenga un virus, ejecutar ninguna rutina maliciosa. Al ponerlos en la cuarentena, los archivos infectados se comprimen y cifran automáticamente. Los archivos destinados a la cuarentena que sean mayores de 1 MB se almacenan siempre automáticamente en la cuarentena local del cliente para no sobrecargar de manera innecesaria la red en caso de un ataque masivo de virus. Todos los archivos menores de 1 MB se transfieren a la carpeta de cuarentena de G DATA ManagementServer. Esta configuración no se puede modificar. La cuarentena de cliente se encuentra en el directorio %ProgramData%\G DATA\AntiVirusKit Client\Quarantine. La cuarentena de G DATA ManagementServer se encuentra en el directorio %ProgramData%\G DATA\AntiVirus ManagementServer\Quarantine.

Si se detecta un archivo infectado de menos de un 1 MB en un cliente sin conexión con G DATA ManagementServer, el archivo se guarda en la cuarentena local y solo se transfiere a la cuarentena de G DATA ManagementServer la próxima vez que el cliente se conecte con él. En la carpeta de cuarentena se pueden desinfectar los archivos infectados. Si esto no funciona, los archivos se pueden eliminar desde allí y, si es necesario, moverlos desde la cuarentena a su ubicación original.

> Nota: con la opción **Restaurar** no se elimina el virus. Solo debe elegir esta opción cuando un programa no pueda funcionar sin el archivo afectado y no le sea posible recuperarlo de otra forma.

La opción Cuarentena puede activarse y desactivarse en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

## 7.5. Actualizaciones/patches

PatchManager está disponible como **módulo opcional**.

La ventana Actualizaciones/patches muestra un resumen de las actualizaciones y patches para el ordenador cliente.

En el área **Instalado** verá todos los patches y actualizaciones que hayan sido instalados en el sistema. Con un doble clic en la entrada correspondiente se obtiene información más detallada. Si un patch o una actualización parecen estar causando problemas, el usuario puede seleccionar la entrada correspondiente y hacer clic en **Desinstalar**. Se envía automáticamente una solicitud de desinstalación al administrador. El **Estado** del patch o actualización cambia y el administrador recibe un **informe** con una solicitud de restauración. Independientemente de las tareas de reconocimiento de software programados, el usuario puede también buscar patches actuales para su sistema con el botón **Buscar actualizaciones**.

En el área **Disponible** se muestran todos los patches, actualizaciones y paquetes de software aplicables en el cliente. Con un doble clic en la entrada correspondiente se obtiene información más detallada. El usuario puede solicitar la instalación haciendo clic en **Instalar**. El **Estado** del patch o actualización cambia y el Administrador recibe un **informe** con una solicitud de distribución de software.

La opción Actualizaciones/patches puede activarse y desactivarse en el G DATA Administrator en **PatchManager** > **Configuración**.

## 7.6. Actualización online

A través del programa G DATA Security Client también se pueden efectuar actualizaciones online de las firmas de virus desde el ordenador cliente, si no tiene conexión al G DATA ManagementServer (ver **Ajustes de cliente** > **General** > **Actualizaciones**).

La opción Actualización online puede activarse y desactivarse en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

## 7.7. Desactivar Cortafuegos

El módulo del Cortafuegos está disponible en las **soluciones** Client Security Business, Endpoint Protection Business, y Managed Endpoint Security.

Mediante Desactivar cortafuegos los usuarios pueden desactivar el cortafuegos, incluso si el cliente se encuentra aún conectado a la red corporativa. Cuando el cortafuegos está desactivado, puede volver a activarse mediante la opción **Activar cortafuegos**.

La opción Desactivar cortafuegos puede activarse y desactivarse en el G DATA Administrator, en **Cortafuegos** > **Resumen** (**El usuario puede activar y desactivar el cortafuegos**).

## 7.8. Cortafuegos

El módulo del Cortafuegos está disponible en las **soluciones** Client Security Business, Endpoint Protection Business, y Managed Endpoint Security.

La opción cortafuegos carga la interfaz del cortafuegos. Cuando el cliente está en la red de G DATA ManagementServer el servidor administra el cortafuegos de manera centralizada. Cuando el cliente se conecta a otra red, por ejemplo un portátil que se conecta a la red privada de casa, la interfaz del cortafuegos puede usarse para realizar los ajustes de fuera de sitio.

La opción Cortafuegos puede activarse y desactivarse en el G DATA Administrator, en **Cortafuegos** > **Resumen** (**El usuario puede modificar la configuración fuera de la red**).

### 7.8.1. Estado

En el módulo Estado se muestran informaciones acerca del estado actual del cortafuegos en el cliente. Haciendo doble clic en cualquiera de las entradas, se pueden realizar acciones directamente o ir a la zona respectiva del programa.

- **Seguridad**: esta acción le permite al usuario activar o desactivar el cortafuegos. Esta opción solo está disponible si se ha activado en el G DATA Administrator (**Cortafuegos** > **Resumen** > **El usuario puede activar y desactivar el cortafuegos**).
- **Modo**: el cortafuegos puede funcionar de forma automática (modo piloto automático) o de forma manual (conjuntos de reglas). Cambiar esta opción directamente en el cliente solo es posible si el cliente se encuentra fuera de la red del ManagementServer y la opción se ha activado en el G DATA Administrator (**Cortafuegos** > **Resumen** > **El usuario puede cambiar la configuración fuera de la red**).
- **Redes**: aquí se muestran las **Redes**, a las que el equipo está conectado y también los conjuntos de reglas que están en uso.
- **Ataques rechazados**: aquí se realiza un listado de los ataques que registra y previene el cortafuegos.
- **Radar de aplicaciones**: muestra que programas están siendo bloqueados en este momento por el cortafuegos. Si desea autorizar a alguna de estas aplicaciones el uso de la red, basta con seleccionarla y hacer clic en el botón **Permitir**.

### 7.8.2. Redes

En el módulo redes encontrará un listado de todas las redes a las que está conectado el ordenador, así como el conjunto de reglas asignado a cada una de ellas para protegerla. Seleccione una red y haga clic en **Editar** para ver o modificar los ajustes para esa red. Solo es posible modificar los ajustes de una red si permitido específicamente (**Cortafuegos** > **Resumen** > **El usuario puede activar y desactivar el cortafuegos**) o si el dispositivo está siendo usado fuera de la red interna (**Cortafuegos** > **Resumen** > **El usuario puede modificar la configuración fuera de la red**).

- **Información de red**: muestra informaciones acerca de la red, incluyendo la dirección IP, la máscara de subred, la puerta de enlace, y los servidores DNS y WINS.
- **Cortafuegos activo en esta red**: aquí puede activar o desactivar la protección del cortafuegos.
- **Uso compartido de la conexión a Internet**: permite el uso compartido de la conexión a Internet.
- **Permitir configuración automática (DHCP)**: permite la configuración DHCP.
- **Conjunto de reglas**: puede elegir cual **Conjunto de reglas** predefinido se debe aplicar a esta conexión. Haga clic en **Editar** conjunto de reglas para abrir el **Asistente para reglas**.

## 7.8.3. Conjuntos de reglas

En el módulo Conjunto de reglas puede crear y editar conjuntos de reglas (grupo de reglas para el cortafuegos que se pueden aplicar a las redes).

- **Nueva regla**: aquí puede crear un nuevo conjunto de reglas. Introduzca un **Nombre** y decida que reglas del conjunto de reglas predeterminadas para redes inseguras, seguras o que deben ser bloqueadas deben formar parte de este nuevo conjunto de reglas.
- **Eliminar**: elimine el conjunto de reglas seleccionado. No es posible borrar los conjuntos de reglas estándar.
- **Editar**: edite el conjunto de reglas seleccionado usando el **Asistente para reglas**.

El módulo conjunto de reglas contiene conjuntos de reglas predeterminadas para los siguientes tipos de redes:

- **Conexión directa con Internet**: abarca reglas relacionadas con el acceso directo a Internet.
- **Redes inseguras**: generalmente abarca redes abiertas con acceso a Internet.
- **Redes seguras**: las redes empresariales y las redes domésticas son generalmente redes seguras.
- **Redes que deben ser bloqueadas**: este conjunto de reglas se puede utilizar cuando se debe bloquear el acceso a una red determinada.

### 7.8.3.1. Asistente para reglas

El Asistente para reglas le permite definir nuevas reglas para el conjunto de reglas seleccionado, o modificar las reglas ya existentes. El Asistente para reglas es especialmente recomendable para los usuarios que no están familiarizados con la tecnología de cortafuegos. Para un control más exhaustivo de las reglas individuales use el **Editor avanzado de conjuntos de reglas (modo experto)**.

En el Asistente para reglas hay disponibles varias reglas. Todas ellas se pueden usar para permitir o bloquear rápidamente un tipo de tráfico concreto. Para la mayoría de las reglas se puede definir la **Dirección**, de esta forma es posible bloquear para un programa concreto, las conexiones entrantes, salientes o en ambas direcciones.

- **Autorizar o bloquear aplicaciones**: seleccione en el disco duro una aplicación concreta para concederle o denegarle de forma explícita el acceso a la red controlada por el conjunto de reglas.
- **Autorizar o bloquear servicios de red**: bloquear uno o más puertos es una forma rápida de cerrar vulnerabilidades, que pueden ser explotadas por los hackers. El asistente le ofrece la posibilidad de bloquear puertos por completo o solo para determinadas aplicaciones.
- **Uso compartido de archivos e impresoras**: permitir o bloquear el uso compartido de archivos e impresoras.
- **Autorizar o bloquear servicios de domino**: permitir o bloquear servicios de dominio de red.
- **Uso compartido de la conexión a Internet**: permitir o bloquear uso compartido de la conexión a Internet (ICS).
- **Autorizar o bloquear los servicios de VPN**: permitir o bloquear redes virtuales privadas (VPN).
- **Editor avanzado de conjuntos de reglas (modo experto)**: iniciar el **Editor avanzado de**

**conjuntos de reglas**.

### 7.8.3.2. Editor avanzado de conjuntos de reglas

El Editor avanzado de conjuntos de reglas permite la creación de reglas altamente específicas. Se puede usar para crear todas las reglas que también están disponibles en el asistente de reglas, pero también es compatible con ajustes personalizados.

La ventana del Editor avanzado de conjuntos de reglas es semejante al panel **Conjunto de reglas** del módulo **Cortafuegos** de G DATA Administrator. Se puede usar para crear, editar, borrar y clasificar reglas dentro del conjunto de reglas. Además de las opciones disponibles en el G DATA Administrator, el Editor avanzado de conjunto de reglas le ofrece las siguientes opciones:

- **Acción a realizar si no se cumple ninguna regla**: aquí puede especificar qué acción tomar cuando no hay una regla asignada: **Denegar**, **Permitir** o **Consultar al usuario**.
- **Modo Adaptativo**: el modo adaptativo es compatible con aplicaciones que usan la tecnología feedback channel (por ejemplo FTP y numerosos juegos en línea). Estas aplicaciones se conectan a un equipo remoto y negocian un canal de retroalimentación con él, que el equipo remoto entonces usa para revertir la conexión a la aplicación. Si se activa el modo adaptativo, el cortafuegos detecta este canal de retroalimentación y lo permite sin necesidad de consultas por separado.
- **Restablecer**: puede borrar todas la modificaciones en los conjuntos de reglas y todas las normas auto aprendidas.

Puede editar reglas individuales simplemente haciendo doble clic en una regla o en el botón **Editar**. El editor de reglas individuales corresponde a la ventana **Editar regla** en el G DATA Administrator.

## 7.8.4. Registros

El módulo Registros muestra una descripción detallada de todas las conexiones entrantes y salientes. Aquí encontrará las informaciones relacionadas con cada conexión, como por ejemplo la dirección, el puerto local, el host remoto, el puerto remoto y el motivo que llevó a decidir permitir o bloquear la conexión.

Haga clic en **Eliminar** para borrar la entrada de registro seleccionada o **Eliminar todo** para borrar todas las entradas de registro. El botón **Detalles** muestra información detallada sobre el registro seleccionado.

Haga clic derecho en cualquier entrada de registro para acceder al menú contextual. Además de la vista **Detalles**, este incluye otras opciones como la posibilidad de crear una nueva regla basada en una entrada de registro, editar una regla que ha llevado a permitir o bloquear una conexión, y filtrar las entradas de registro del módulo Registros.

## 7.8.5. Ajustes

La ventana ajustes solo está disponible si se han habilitado los permisos correspondientes en G DATA Administrator (**Cortafuegos** > **Resumen** > **El usuario puede activar y desactivar el cortafuegos** y **El usuario puede modificar la configuración fuera de la red**).

- **Seguridad**: el usuario puede activar o desactivar el cortafuegos.
- **Modo**: el cortafuegos puede funcionar de forma automática (modo piloto automático) o de forma manual (modo conjunto de reglas).

# 8. G DATA Security Client para Linux

El servicio G DATA Security Client para Linux se ejecuta en segundo plano y proporciona recursos de análisis virus. Para servidores Linux, hay disponibles módulos adicionales para Samba, Sendmail y Postfix y Squid (consulte **Instalar G DATA Security Client para Linux**).

G DATA Security Client para Linux consta de una **interfaz gráfica de usuario** y una **aplicación de línea de comandos**.

## 8.1. Interfaz gráfica de usuario

Encontrará un acceso directo a la interfaz gráfica de G DATA Security Client para Linux en el menú de aplicaciones o un sitio parecido, dependiendo de la distribución de Linux. De forma alternativa, inicie la interfaz ejecutando */opt/gdata/bin/gdavclient-qt*.

Después de iniciar la interfaz, haga clic en el icono de G DATA Security Client para Linux para abrir su interfaz. Puede configurar que opciones van a estar disponibles en el módulo **Ajustes de cliente** del G DATA Administrator.

Haga clic en el icono de la bandeja para abrir el menú contextual. Este menú le ofrece acceso a los siguientes ajustes:

- **Comprobar**
- **Cuarentena**
- **Actualizar**
- **Ayuda**
- **Iniciar G DATA Security Client**: inicia el G DATA Security Client para Linux y visualiza el módulo **Estado**.
- **Acerca de G DATA Security Client**

Todos los módulos están protegidos contra cambios no deseados de los ajustes. Haga clic en el botón de bloqueo, que se encuentra en la esquina inferior izquierda, para permitir que se realicen cambios en los ajustes. Si se requieren permisos root, se solicitará al usuario que introduzca un nombre de usuario y una contraseña.

### 8.1.1. Estado

El módulo Estado ofrece una visión rápida de conjunto del estado de protección actual del cliente. Los iconos de estado se pueden utilizar para evaluar si existe un riesgo inmediato para el cliente o si el cliente está completamente seguro.

- **Último comprobación**: la fecha y hora del último **Análisis de virus**. Use el botón **Comprobar el equipo ahora** para iniciar un análisis completo en busca de virus.
- **Última actualización**: la fecha y hora de la última **Actualización**. Use el botón **Actualizar ahora** para iniciar una actualización inmediata de las firmas de virus.

### 8.1.2. Comprobar

El análisis en busca de virus se puede usar para escanear en busca de malware el ordenador en su totalidad o un archivo o directorio específico. Cuando se detecta un virus, en el cliente se realizará la acción que se haya definido en **Ajustes**. Se enviará una notificación al ManagementServer y se

agregará un informe al módulo **Eventos de seguridad** en el G DATA Administrator.

Seleccione una de las siguientes opciones y haga clic en **Iniciar comprobación**:

- **Análisis completo del sistema**: escanea todos los archivos y directorios; el ordenador por completo.
- **Comprobar áreas de sistema**: escanea el sector de arranque.
- **Comprobar directorios/archivos**: escanea directorios o archivos concretos. El ámbito se puede definir en **Ámbito**.

Se pueden configurar los siguientes ajustes:

- **Reacción a archivos infectados**: defina la forma de reaccionar cuando en el análisis se detecta un archivo infectado:
  - **Solo registrar** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
  - **Desinfectar** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
  - **Eliminar** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
  - **Mover a cuarentena** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
  - **Preguntar al usuario**: el usuario final recibe un mensaje de notificación y tiene que decidir qué acción se llevar a cabo.
- **Si la desinfección falla**: si se ha seleccionado la opción **Desinfectar** pero no es posible desinfectar el archivo, se llevará a cabo una acción alternativa.
- **Reacción a archivos comprimidos**: aquí se define qué acción se debe llevar a cabo cuando en el análisis se detecta un archivo comprimido infectado.
- **Tipos de archivos** (consulte **Órdenes** > **Órdenes de escaneo** > **Escáner**)

En **Avanzado**, se pueden configurar los siguientes ajustes avanzados:

- **Heurísticas** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
- **Comprobar áreas de sistema** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
- **Comprobar archivos comprimidos** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
- **Ignorar archivos comprimidos mayores de** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
- **Limitación de tamaño**: se define un tamaño máximo. No se analizarán los archivos que sean más grandes.

Use la lista de archivos y directorios en **Excepciones** para excluir elementos concretos del análisis de virus.

El módulo Comprobar se puede habilitar o deshabilitar en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

### 8.1.3. Actualizar

El módulo Actualizar se asegura de que G DATA Security Client para Linux disponga de las firmas de virus más actuales y disfrute de una protección óptima.

La fecha y la hora de la última actualización de las firmas de virus se pueden visualizar en **Última**

**actualización**. La información de versión de firmas para ambos motores las encontrará en **Motor A** y **Motor B**. Haga clic en **Actualizar las firmas de virus** para iniciar una actualización de las firmas de virus de forma inmediata.

Los ajustes relacionados con la actualización de las firmas de virus se pueden configurar en **Ajustes**:

- **Fuente de actualización**: configure si el cliente debe cargar las firmas de virus del ManagementServer o directamente del servidor de actualizaciones G DATA (consulte **Ajustes de cliente** > **General** > **Actualizaciones**).
- **Programar**: defina cuando y con qué frecuencia deben descargarse las actualizaciones de las firmas de virus (**Manual**, **Cada hora** o **Diario**).
- **Servidor Proxy**: introduzca el servidor proxy que debe usarse para establecer la conexión con el servidor de actualizaciones G DATA.
- **Datos de acceso**: introduzca los datos de acceso que deben usarse para la autenticación en el servidor de actualizaciones G DATA.

**Programar**, **Servidor Proxy** y **Datos de acceso** solo se usan si **Fuente de actualización** se ha configurado para no **Descarga de actualizaciones de firmas de virus de ManagementServer**. Para obtener más información consulte **Ajustes de cliente** > **General** > **Actualizaciones**.

El modulo Actualizar se puede habitar o deshabilitar en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente** (**El usuario puede cargar por sí mismo actualizaciones de firmas**).

### 8.1.4. Cuarentena

En el módulo Cuarentena se pueden visualizar los elementos que el **Análisis de virus** ha movido a la cuarentena.

Para cada elemento se pueden visualizar las siguientes características:

- **Nombre de archivo**: el nombre y el directorio del elemento infectado.
- **Nombre de virus**: el nombre del virus detectado.
- **Tamaño de archivo**: el tamaño del elemento.

Seleccione uno o varios elementos y haga clic en uno de los siguientes botones:

- **Desinfectar y restaurar**: elimina el virus y restaura el elemento a su ubicación de origen.
- **Restaurar**: restaura el elemento a su ubicación de origen. ¡Advertencia: si el elemento no es desinfectado en primer lugar, puede infectar el sistema!
- **Eliminar**: Elimina el elemento de la cuarentena.

El módulo Cuarentena se puede habilitar o deshabilitar en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

### 8.1.5. Acerca de G DATA Security Client

La ventana **Acerca de** muestra la información del estado de G DATA Security Client para Linux y solo podrá abrirse a través del icono de la bandeja. Se mostrará la siguiente información:

- **Versión**: la versión instalada en el cliente actualmente.

- **ManagementServer**: el estado actual de la conexión con ManagementServer.
- **Estado del software de seguridad**: el estado actual de los servicios que se ejecutan en segundo plano en el cliente.

# 8.2. Aplicación de línea de comandos

Como alternativa a la interfaz gráfica de usuario también está disponible la interfaz de línea de comandos para configurar y ejecutar G DATA Security Client para Linux. **Gdavclient-cli** es la forma más común de iniciar un análisis de virus y una actualización de las firmas de virus desde la línea de comandos. De forma alternativa, **gdavclientc** puede configurar y ejecutar escaneos, mostrar la información de versión, actualizar las firmas de virus y gestionar el servicio daemon de escaneo. Ambas aplicaciones se tienen que ejecutar con privilegios root para garantizar pleno acceso al sistema de archivos.

## 8.2.1. gdavclient-cli

Por defecto, gdavclient-cli se encuentra en la carpeta /usr/bin. La sintaxis de gdavclient-cli es de la forma: *gdavclient-cli [<options>] <files/paths>*. Algunas de sus opciones son:

- **--status**: muestra el estado de gdavclientd y gdavserver daemons.
- **--version**: muestra la información de versión.
- **--mmsconnection**: muestra información relacionada con la conexión con el G DATA ManagementServer.
- **--lastscan**: muestra el último registro de escaneo.
- **--lastupdate**: muestra información acerca de la última actualización de las firmas de virus.
- **--update**: actualiza las firmas de virus.
- **--sysinfo**: crea un archivo denominado *gdatahwinfo-<Fecha>.tar.gz*, el cual contiene archivos de depuración tales como archivos de registro y de configuración.

Si se especifica un directorio o un archivo o archivos concretos, gdavclient-cli inicia un análisis en busca de virus.

## 8.2.2. gdavclientc

Por defecto, gdavclientc se encuentra en la carpeta /usr/bin. Es independiente del G DATA ManagementServer y extrae sus valores de configuración de /etc/gdata/gdav.ini. La sintaxis de gdavclientc es de la forma: *gdavclientc [<options>] <command>*. Los comandos que se pueden utilizar son:

- **scan:<path>**: inicia un escaneo del archivo o archivos en el directorio correspondiente. *<path>* puede ser una ruta de acceso absoluta o relativa a un archivo o a una carpeta (que se escanearán de forma recurrente). Se permite el uso de comodines (*, ?).
- **scanboot**: realiza un escaneo del registro de arranque. Se escanearán todos los medios no ópticos listados en /proc/partitions.
- **abort**: finaliza el escaneo actual.
- **start**: inicia gdavserver.
- **stop**: detiene gdavserver.
- **restart**: detiene y reinicia gdavserver.

- **updateVDB<:engine>**: inicia una actualización de las firmas de virus para el motor *EngineA* o el motor *EngineB*. Una vez completada la actualización debería reiniciarse el servicio scan server con el comando *restart*.
- **dump**: muestra la configuración actual.
- **set:<key>=<value>**: configura una opción específica en la configuración de gdavserver, y sobrescribe la opción existente (que fue extraída de /etc/gdata/gdav.ini). Estas opciones se establecen solo de manera temporal y se perderán cuando se detenga gdavserver.
- **get:<key>**: muestra el valor actual de una opción específica de la configuración de gdavserver.
- **reload**: vuelve a extraer, cargar todos los valores de /etc/gdata/gdav.ini.
- **engines**: lista los nombres de todos los motores de escaneo en uso.
- **baseinfo**: muestra la información de versión.
- **coreinfo**: muestra la información de versión del motor de virus.
- **pid**: muestra la PID de gdavserver.

Si se utiliza **scan:** command para iniciar una comprobación de análisis de virus, se podrán usar las siguientes opciones:

- **-s**: además de los resultados normales del análisis, se mostrará un resumen de los resultados.
- -**x**: además de los resultados normales del análisis, se mostrará un resumen de los resultados (en formato XML).

# 9. G DATA Security Client para Mac

G DATA Security Client para Mac proporciona protección a los clientes Mac OS X. Ejecuta análisis de virus programados y análisis locales bajo demanda y proporciona protección en tiempo real a través de los módulos del Vigilante.

Una vez finalizada la **instalación** del software cliente, el usuario tendrá a su disposición un icono. Es necesario aprobar que ajustes van a estar disponibles. Estos se definen en módulo **Ajustes de cliente** del G DATA Administrator.

Haga clic en el icono de la bandeja para abrir el menú contextual, en el que están disponibles los siguientes ajustes:

- **Activar/Desactivar el vigilante**
- **Comprobar**
- **Cuarentena**
- **Actualizar**
- **Ayuda**
- **Iniciar G DATA Security Client**: inicia G DATA Security Client para Mac y muestra el módulo **Estado**.
- **Acerca de G DATA Security Client**

Todos los módulos están protegidos contra cambios no deseados de los ajustes. Haga clic en el botón de bloqueo, que se encuentra en la esquina inferior izquierda, para permitir que se realicen cambios en los ajustes. Si se requieren permisos root, se solicitará al usuario que introduzca un nombre de usuario y una contraseña.

## 9.1. Estado

El módulo estado ofrece una visión rápida de conjunto del estado de protección actual del cliente. Los iconos de estado se pueden utilizar para evaluar si existe un riesgo inmediato para el cliente o si el cliente está completamente seguro.

- **Vigilante**: el estado actual del **Vigilante**. Se puede desactivar (temporalmente) usando el menú desplegable.
- **Último comprobación**: la fecha y hora del último **Análisis de virus**. Use el botón **Analizar ahora** para iniciar un análisis completo en busca de virus.
- **Última actualización**: la fecha y hora de la última **Actualización**. Use el botón **Actualizar ahora** para iniciar una actualización inmediata de las firmas de virus.

## 9.2. Vigilante

El vigilante realiza análisis en busca de virus en segundo plano de todos los archivos a los que se accede y actúa de inmediato cuando detecta un virus.

Se pueden configurar los siguientes ajustes:

- **Estado**
  - **Habilitado**: activa el vigilante (recomendado).
  - **Deshabilitado**: desactiva el vigilante de forma permanente. Desactivar el vigilante supone

un riesgo de seguridad.
    - **Deshabilitado hasta el próximo reinicio**: Desactiva el vigilante. Tras reiniciar el sistema, el vigilante se activa de forma automáticamente.
    - **Deshabilitado durante ... minutos**: desactiva el vigilante durante un periodo de tiempo (en minutos) determinado. Una vez finalizado este periodo de tiempo el vigilante se activa automáticamente.
- **Reacción a archivos infectados**: defina qué acción se debe llevar a cabo cuando el vigilante detecta un archivo infectado. Están disponibles las siguientes opciones:
    - **Solo registrar** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
    - **Desinfectar** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
    - **Eliminar** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
    - **Mover a cuarentena** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
    - **Preguntar al usuario**: el usuario final recibe un mensaje de notificación y tiene que decidir qué acción se llevar a cabo.
- **Si la desinfección falla**: si se ha seleccionado la opción **Desinfectar** pero no es posible desinfectar el archivo, se llevará a cabo una acción alternativa.
- **Reacción a archivos comprimidos**: aquí se define que acción se debe tomar cuando el Vigilante detecta un archivo comprimido infectado.
- **Tipos de archivos** (consulte **Órdenes** > **Órdenes de escaneo** > **Escáner**)

En **Avanzado**, se pueden configurar los siguientes ajustes avanzados:

- **Heurísticas** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
- **Comprobar áreas de sistema** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
- **Comprobar archivos comprimidos** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
- **Ignorar archivos comprimidos mayores de** (consulte **Ajustes de cliente** > **Vigilante** > **Configuración**)
- **Limitación de tamaño**: se define un tamaño máximo. No se analizarán los archivos que sean más grandes.

Use la lista de archivos y directorios en **Excepciones** para excluir elementos concretos del análisis de virus.

El módulo Vigilante se puede habilitar o deshabilitar en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

## 9.3. Comprobar

El análisis en busca de virus se puede usar para escanear en busca de malware el ordenador en su totalidad o un archivo o directorio específico. Cuando se detecta un virus, en el cliente se realizará la acción que se haya definido en **Ajustes**. Se enviará una notificación al ManagementServer y se agregará un informe al módulo **Eventos de seguridad** en el G DATA Administrator.

Seleccione una de las siguientes opciones y haga clic en **Iniciar análisis de virus**:

- **Análisis completo del sistema**: escanea todos los archivos y directorios; el ordenador por completo.

- **Comprobar áreas de sistema**: escanea el sector de arranque.
- **Comprobar directorios/archivos**: escanea directorios o archivos concretos. El ámbito se puede definir en **Ámbito**.

En **Ajustes**, se pueden configurar los ajustes y excepciones (consulte **Vigilante**).

El módulo Comprobar se puede habilitar o deshabilitar en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

## 9.4. Actualizar

El módulo Actualizar se asegura de que G DATA Security Client para Mac disponga de las firmas de virus más actuales y disfrute de una protección óptima.

La fecha y la hora de la última actualización de las firmas de virus se pueden visualizar en **Última actualización**. La información de versión de firmas para ambos motores las encontrará en **Motor A** y **Motor B**. Haga clic en **Actualizar las firmas de virus** para iniciar una actualización de las firmas de virus de forma inmediata.

Los ajustes relacionados con la actualización de las firmas de virus se pueden configurar en **Ajustes**:

- **Fuente de actualización**: configure si el cliente debe cargar las firmas de virus del ManagementServer o directamente del servidor de actualizaciones G DATA (consulte **Ajustes de cliente** > **General** > **Actualizaciones**).
- **Programar**: defina cuando y con qué frecuencia deben descargarse las actualizaciones de las firmas de virus (**Manualmente**, **Cada hora** o **Diariamente**).
- **Servidor Proxy**: introduzca el servidor proxy que debe usarse para establecer la conexión con el servidor de actualizaciones G DATA.
- **Datos de acceso**: introduzca los datos de acceso que deben usarse para la autenticación en el servidor de actualizaciones G DATA.

**Programar**, **Servidor Proxy** y **Datos de acceso** solo se usan si **Fuente de actualización** se ha configurado para no **Descarga de actualizaciones de firmas de virus de ManagementServer**. Para obtener más información consulte **Ajustes de cliente** > **General** > **Actualizaciones**.

El módulo Actualizar se puede habilitar o deshabilitar en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente** (**El usuario puede cargar por sí mismo actualizaciones de firmas**).

## 9.5. Cuarentena

En el módulo Cuarentena se pueden visualizar los elementos que el **Análisis de virus** ha movido a la cuarentena.

Para cada elemento se pueden visualizar las siguientes características:

- **Nombre de archivo**: el nombre y el directorio del elemento infectado.
- **Nombre de virus**: el nombre del virus detectado.
- **Tamaño de archivo**: el tamaño del elemento.

Seleccione uno o varios elementos y haga clic en uno de los siguientes botones:

- **Desinfectar y restaurar**: elimina el virus y restaura el elemento a su ubicación de origen.
- **Restaurar**: restaura el elemento a su ubicación de origen. ¡Advertencia: si el elemento no es desinfectado en primer lugar, puede infectar el sistema!
- **Eliminar**: Elimina el elemento de la cuarentena.

El módulo Cuarentena se puede habilitar o deshabilitar en el G DATA Administrator en **Ajustes de cliente** > **General** > **Funciones de cliente**.

## 9.6. Acerca de G DATA Security Client

La ventana Acerca de muestra información de estado de G DATA Security Client para Mac:

- **Versión**: la versión instalada en el cliente actualmente.
- **ManagementServer**: el nombre del ManagementServer al que se conecta el cliente.
- **Estado del software de seguridad**: el estado actual de los servicios que se ejecutan en segundo plano en el cliente.

# 10. G DATA ActionCenter

G DATA ActionCenter le ofrece acceso en la nube a los servicios de G DATA. Las funciones están organizadas en módulos. Una vez que haya **creado una cuenta**, inicie sesión en **https://ac.gdata.de** para acceder a la interfaz web. Puede seleccionar un módulo en la ventana principal o en el menú situado en la esquina superior derecha:

- **Dispositivos móviles**: gestión de dispositivos móviles para las soluciones retail de G DATA.
- **Monitoreo de red**: permite monitorear la infraestructura de la red con el fin de prevenir caídas de red y hacer posibles tiempos de respuesta más rápidos.

En los ajustes se mostrarán los siguientes accesos directos:

- **Permisos**: Gestione permisos de otras cuentas de ActionCenter, como por ejemplo permisos de solo lectura para **Monitoreo de red**.
- **Grupos de correo electrónico**: configure grupos de destinatarios para habilitar informes y notificaciones, como por ejemplo la funcionalidad de mensajes de alerta de **Monitoreo de red**.

ActionCenter también hace posible la gestión de dispositivos móviles iOS, estableciendo la comunicación entre los dispositivos iOS y G DATA ManagementServer. La configuración de la gestión de los dispositivos móviles iOS se lleva a cabo a través del nodo **iOS Mobile Device Management** en la ventana **Clientes/ManagementServers** de G DATA Administrator.

## 10.1. Crear y vincular una cuenta

Para abrir la página de registro haga clic en **Registrarse** en la página de inicio de sesión del ActionCenter. En primer lugar introduzca y confirme una **Dirección de correo electrónico**, a continuación introduzca una **Contraseña** y acepte los términos y condiciones. Por último haga clic en **Registrarse**. Tan pronto hayamos recibido sus datos, le enviaremos un enlace de confirmación de e-mail a la dirección de correo electrónico que nos haya facilitado durante el registro.

Tan pronto haga clic en el enlace de confirmación, el nombre de usuario y la contraseña estarán configurados en G DATA Administrator en el módulo **ActionCenter**, y se habrá establecido el vínculo entre G DATA ManagementServer y G DATA ActionCenter.

## 10.2. Módulos

Esta funcionalidad de G DATA ActionCenter ha sido dividida en varios módulos. Para las soluciones empresariales, ActionCenter ofrece el módulo de monitoreo de red.

### 10.2.1. Monitoreo de red

El monitoreo de red está disponible como **módulo opcional**.

Este módulo permite a los administradores mantener vigilado el estado de su infraestructura de red. Es posible definir **métricas**, y obtener así de los clientes una amplia selección de Información estadística, que puede ser visualizada en el panel de mando.

#### 10.2.1.1. Dashboard

El panel de mando muestra estadísticas actualizadas para todas las **métricas**, así como una visión general de todos los **servidores** y **dispositivos** que pueden ser gestionados. Si agrega una métrica a favoritos, aparece un widget de resumen en el panel de mando mostrando el nombre del dispositivo

asociado, el último valor y un diagrama de tendencia.

En la parte central del panel de mando se muestran informaciones de estado. En **Aceptar**, encuentra un listado de todas las métricas que no han reportado una violación de umbral. Cuando una métrica reporta un valor por encima o por debajo del umbral definido previamente, su estado cambia a **Advertencia**. A partir de tres violaciones de umbral el estado cambia a **Crítica**. En los diferentes estados, las métricas están agrupadas por categorías. Esto permite una visión detallada de la categoría afectada en estos momentos.

La sección **Registros** muestra las entradas de registro para todas las métricas definidas. Se agregan entradas de registro cuando una métrica reporta por primera vez un valor, cuando reporta un error y cuando su estado cambia (por ejemplo de **Aceptar** a **Crítica**). Al hacer clic en una entrada de registro se abre la página correspondiente con el conjunto de **Métrica**.

Cuando se están administrando múltiples servidores, la lista desplegable en la parte superior del panel de mando, podrá ser usada para crear y seleccionar vistas en el panel de mando. Haga clic en crear panel de mando, introduzca un nombre para el mismo y asigne uno o varios ManagementServers.

## 10.2.1.2. Información general de métricas

Para definir una métrica se asigna una **plantilla de métrica** a uno o varios dispositivos. Según los parámetros definidos en la plantilla, se crearán periódicamente informes estadísticos específicos desde el dispositivo(s). Haga clic en **Crear métricas** para **crear una métrica**.

Encontrará un resumen de todas las métricas definidas en la página Información general de métricas. Al hacer clic en una métrica se abre la página asociada a esa **Métrica** concreta. La lista de métricas se puede filtrar por estado o categoría. Están disponibles las siguientes informaciones para cada entrada de la lista:

- **ManagementServer**: el ManagementServer que gestiona el dispositivo al que se ha asignado la plantilla de métricas.
- **Dispositivo**: el dispositivo al que se ha asignado la plantilla de métricas.
- **Estado**: el estado actual de en qué se encuentra cada métrica (**Aceptar**, **Advertencia**, **Crítica** o **Desconocido**).
- **Métrica**: el nombre asignado a la plantilla que se ha usado para crear la métrica.
- **Categoría**: la categoría dela plantilla que se ha usado para crear la métrica.
- **Objetivo**: el dispositivo de destino de la plantilla que se ha usado para crear la métrica.

### Agregar métrica

Crear una métrica implica asignar una o varias **plantillas de métricas** a uno o varios dispositivos. El proceso disponible en la página Agregar métrica se compone de cuatro pasos:

1. **Seleccionar platilla de métricas**: seleccione una o varias plantillas. Las plantillas están organizadas en categorías.
2. **Seleccionar dispositivos**: seleccione uno o varios dispositivos. Los dispositivos están organizados en carpetas, agrupados por ManagementServer. En el nivel superior de la estructura de carpetas, es posible seleccionar los propios ManagementServers (siempre que se haya seleccionado en el primer paso una plantilla de métricas de la categoría **ManagementServer**).

3. **Verifique los dispositivos seleccionados**: asegúrese de que todos los dispositivos a los que hay que aplicar la plantilla o plantillas elegidas han sido seleccionados.
4. **Resumen**: haciendo clic en **Crear métrica** puede crear la métrica o métricas correspondientes y volver a **Información general de métricas**.

### Métrica

En la página Métrica puede obtener informaciones detalladas de una métrica seleccionada. En la parte superior de la página se muestran el **Nombre**, el **Dispositivo** y el **ManagementServer**, y también su estado actual. Utilizando la opción **Favoritos**, puede anclar métricas en el **Dashboard**.

Puede personalizar la vista de diagrama para obtener una visión general inmediata de las tendencias. Los ajustes por defecto muestran los valores correspondientes a las 6 últimas horas. Puede cambiar este rango en el menú desplegable.

En **Resumen** puede consultar informaciones relacionadas con los siguientes parámetros:

- **Intervalo de medición**: el intervalo con el que la métrica envía nuevos valores al ActionCenter.
- **Último valor**: el valor más reciente incluyendo la fecha y la hora (marca temporal).
- **Mínimo**: el valor más bajo jamás registrado.
- **Máximo**: el valor más alto jamás registrado.
- **Umbral** (solo se muestra si se ha establecido un umbral): el valor de umbral actual.
- **Por encima del umbral** (solo se muestra si se ha establecido un umbral): el porcentaje de los valores registrados que superan el valor de umbral establecido.
- **Por debajo del umbral** (solo se muestra si se ha establecido un umbral): el porcentaje de valores registrados que caen por debajo del valor de umbral establecido.

En **Registro de métrica** se muestran todas las entradas de registro para la métrica. Se agregan entradas de registro cuando una métrica reporta un valor por primera vez, cuando reporta un error y cuando su estado cambia (por ejemplo de **Aceptar** a **Crítica**).

### Gestionar plantillas de métricas

Una platilla métrica contiene los parámetros para un escenario específico de monitoreo de red. Las plantillas pueden asignarse a uno o varios dispositivos, creando **métricas**.

En la página de Gestión de plantillas de métricas están listadas todas las plantillas. Para cada entrada de la lista están disponibles las siguientes informaciones:

- **Nombre**: el nombre de la plantilla.
- **Comentario**: información específica para distinguir unas plantillas de otras.
- **Categoría**: categoría a la que pertenece la plantilla (**Dispositivos**, **Procesos local**, **Red**, **ManagementServer**, **Impresora** o **Dispositivos SNMP**).
- **Métrica**: define el tipo de información que se está monitoreando, dependiendo de la **Categoría** que se haya seleccionado.
- **Utilizados por**: el número de dispositivos a los que se ha asignado una **métrica** usando esta plantilla.

Al hacer clic en una platilla se abre la página **Editar platilla**. Haga clic en **Crear plantilla** para crear una nueva plantilla de métrica.

### Crear plantilla

Para crear una plantilla métrica es necesario introducir una serie de parámetros obligatorios y opcionales:

- **Categoría**: seleccione aquí la categoría a la que pertenece la plantilla (**Dispositivos**, **Procesos local**, **Red**, **ManagementServer**, **Impresora** o **Dispositivos SNMP**).
- **Métrica**: seleccione aquí el tipo de Información que se debe monitorear, dependiendo de la **Categoría** que se haya seleccionado.
- **Nombre**: el nombre de la plantilla.
- **Comentario**: información específica para distinguir unas plantillas de otras.

En función de la **Categoría** y de la **Métrica** están disponibles algunos de los siguientes ajustes:

- **Objetivo**: el destino en el que se va a recopilar la Información seleccionada. Este valor no se puede cambiar y está ajustado por defecto en *localhost*. Esto implica que la Información se recogerá en el dispositivo al que se ha asignado la plantilla métrica.
- **Nombre de host**: el nombre de host del dispositivo en el que se va a monitorear la información seleccionada. Este no tiene necesariamente que ser el dispositivo al que se asignará la plantilla métrica. Es posible agregar varios nombres de host; cuando se asigna la plantilla métrica a un dispositivo se crearán múltiples métricas.
- **Dirección URL**: la URL para la que se va a monitorear la información seleccionada. Es posible agregar varias URLs; cuando se asigna la plantilla métrica a un dispositivo se crearán múltiples métricas.
- **Instancia de SQL Server**: la instancia de SQL Server para la que se va a monitorear la información seleccionada. Haga clic en la lupa para visualizar la lista de instancias de SQL Server disponibles por ManagementServer.

Los ajustes opcionales dependen también de la **Categoría** y la **Métrica** seleccionada e incluye uno o varios de los siguientes valores:

- **Valor de umbral**: establece un valor de umbral.
- **Condición del valor de medición**: dicta cómo se interpreta el valor de umbral. El estado de la métrica cambiará de **Aceptar** a **Advertencia** y a **Crítica** cuando el valor medido esté por debajo o por encima del umbral.
- **Índice de CPU**: introducir la CPU para la que se va a monitorear la información seleccionada o introducir *_Total*para monitorear todas las CPUs.
- **Letra de unidad**: introducir la unidad para la que se va a monitorear la información seleccionada o introducir *_Total*para monitorear todas las unidades.
- **Nombre del proceso**: introducir el nombre de proceso para el cual se va a monitorear la información seleccionada o introduzca *_Total*para monitorear todos los procesos.
- **Nombre del adaptador de red**: introducir el adaptador de red para el que se va a monitorear la información seleccionada o introducir *si se desean monitorear todos los adaptadores de red.
- **Base de datos de SQL Server**: introducir la base de datos para la cual se va a monitorear la información seleccionada o introducir *_Total*si se desean monitorear todas las bases de datos.
- **Tiempo de espera de la solicitud**: introduzca el tiempo de espera de petición para solicitudes de ping.
- **Código de estado HTTP previsto**: si la solicitud de HTTP devuelve un código de estado distinto

del que hay definido aquí, entonces se considera como una violación de umbral y se cambia el estado de la métrica.

- **Nombre de la comunidad SNMP**: introduzca la cadena de comunidad SNMP que requiere el dispositivo de destino. El fabricante del dispositivo establece esta cadena de comunidad y normalmente se encuentra en la documentación del dispositivo.

En **Ajustes de alertas** se pueden configurar mensajes de alerta por correo electrónico:

- **Condición de alerta**: se envía un mensaje de alerta solo cuando el estado de la métrica cambia a **Crítico** o cuando cambia a **Advertencia o crítico**.
- **Notificar solo a los grupos de correo electrónico seleccionados**: el mensaje de alerta se enviará a los grupos de correo electrónico seleccionados, que pueden definirse mediante la página de **Grupos de correo electrónico**.

**Editar plantilla**
En la página Editar plantilla se pueden editar plantillas de métricas existentes. Todos los ajustes se corresponden con los que se establecieron cuando se creó la plantilla. Los ajustes de solo lectura no pueden ser modificados:

- **Categoría**
- **Métrica**
- **Utilizados por**
- **Objetivo**
- **Nombre de host**
- **URL**

Todos los demás ajustes se pueden editar libremente. Haga clic en **Guardar plantilla** para guardar los cambios. Los cambios realizados en una plantilla existente se aplicarán a todas las métricas que estén basadas en la plantilla seleccionada.

## 10.2.1.3. Información general de servidores

Aquí se muestran todos los ManagementServers vinculados con la cuenta del ActionCenter. Por servidor aparece una lista con los **dispositivos** asociados, las **métricas** y las impresoras. La Información se puede filtrar hacienda clic en cualquiera de las categorías en **Filtros**.

Al hacer clic en un servidor se abre la página de **Información del servidor**, que permite el acceso a las siguientes informaciones y ajustes:

- **Nombre de host**: el nombre de host del servidor.
- **Versión**: el número de versión del ManagementServer.
- **Último acceso**: marca temporal (fecha y hora) de la última sincronización entre el servidor y el ActionCenter.
- **Métricas**: número de métricas asociadas con el servidor seleccionado.
- **Dispositivos**: número de dispositivos asociados con el servidor seleccionado.
- **Impresoras**: número de impresoras asociadas con el servidor seleccionado.
- **Comentario**: información relacionada con el servidor y que ayuda a distinguir unos servidores de otros.

- **Acceso API**: habilitado por defecto. Si se deshabilita el acceso API, no se elimina el servidor del ActionCenter, pero se impide que envíe informes.
- **Etiquetas**: agrega una o varias etiquetas, que pueden ser usadas para filtrar la información.

Haciendo clic en **Establecer permisos**, se puede acceder en modo lectura a este servidor desde otra cuenta de ActionCenter. Para enviar una invitación, basta con introducir la dirección de correo electrónico en el campo **E-mail** y hacer clic en **Enviar invitación**. Tras iniciar sesión en Action Center y aceptando la invitación enviada en el link, el destinatario tendrá acceso de solo lectura a todas las funcionalidades del monitoreo de red de este servidor. Desde la página **Permisos**, se pueden ver o rechazar los permisos.

> Si la dirección de correo electrónico no está todavía asociada con una cuenta de ActionCenter, se le pedirá al destinatario crear una cuenta. Acto seguido, podrá aceptar la invitación.

Haga clic en **Eliminar el servidor** para eliminar el servidor del ActionCenter. Se eliminarán también todos los **dispositivos** asociados, las **métricas** y los registros.

#### 10.2.1.4. Información general de dispositivos

Aquí encontrará una lista, que incluye todos los dispositivos gestionados por los ManagementServers vinculados con la cuenta del ActionCenter. Es posible filtrar la lista haciendo clic en **Filtro** y seleccionando el ManagementServer correspondiente en la estructura de carpetas.

Cada dispositivo aparece con su nombre y además, con todas las métricas asociadas. Al hacer clic en una métrica se abre la página de la **Métrica** correspondiente.

## 10.3. Ajustes

El área de ajustes contiene las configuraciones que pueden ser usadas por otros módulos de ActionCenter.

### 10.3.1. Permisos

La página de permisos puede ser usada por el administrador de permisos que se han concedido en **Monitoreo de red** > **Información general de servidores**. Las cuentas de ActionCenter que cuenten con permisos, se muestran listadas bajo el respectivo ManagementServer. Para eliminar un permiso de la cuenta seleccionada, es necesario hacer clic en **Eliminar**.

### 10.3.2. Grupos de correo electrónico

En Grupos de correo electrónico se agrupan una o varias direcciones de correo electrónico, y se utilizan para el envío de informes y notificaciones, como por ej. alertas de umbral del módulo de **Monitoreo de red**. En la página de Grupos de correo electrónico se muestran todos los grupos de correo electrónico y las direcciones de e-mail asociadas.

Haga clic en **Agregar grupo de correo electrónico** para crear un nuevo grupo de e-mail. Introduzca un **Nombre**, seleccione el **Idioma del correo electrónico** deseado y, por ultimo haga clic en **Agregar**. Para agregar una nueva dirección de correo electrónico a un grupo, seleccione el grupo correspondiente e introduzca la **Dirección de correo electrónica** en **Modificar grupo "Grupo"**, y haga clic en **Agregar dirección de correo electrónico a "Grupo"**. Repita este paso para agregar múltiples direcciones de correo electrónico a un mismo grupo.

# 11. G DATA MailSecurity MailGateway

G DATA MailSecurity está disponible como **módulo opcional**.

G DATA MailSecurity MailGateway proporciona protección integral para la comunicación corporativa por correo electrónico. Todos los correos electrónicos entrantes y salientes se analizan mediante una puerta de enlace independiente del servidor. Junto con el programa en sentido estricto, que se ejecuta en segundo plano, se instala automáticamente el **G DATA MailSecurity Administrator** que le permite acceder sin restricciones a todas las funciones y opciones de MailGateway. Este Administrator lo encontrará en **Inicio** > **(Todos los) programas** > **G DATA MailSecurity** > **G DATA MailSecurity**. Aunque cierre el administrator, MailGateway permanece activo en segundo plano.

El mantenimiento de MailGateway se puede realizar desde cualquier otro ordenador, siempre y cuando cumpla los requisitos de sistema de la herramienta G DATA MailSecurity Administrator. Para instalar el Administrador MailSecurity en otro ordenador de red sin instalar también el propio software MailGateway, lo único que necesita hacer es simplemente iniciar otra vez el setup y seleccionar el botón **G DATA MailSecurity Administrator**.

# 12. G DATA MailSecurity Administrator

G DATA MailSecurity está disponible como **módulo opcional**.

El G DATA MailSecurity Administrator es el software de gestión para el G DATA MailSecurity MailGateway que, controlado a nivel central por el administrador de sistemas, asegura toda la correspondencia electrónica basada en los protocolos SMTP y POP3 en toda la red. El Administrator está protegido mediante contraseña y puede iniciarse en cualquier ordenador con Windows. Todas las modificaciones posibles de parámetros en el escáner de virus y en las actualizaciones de firmas de virus se pueden realizar a distancia.

## 12.1. Iniciar el G DATA MailSecurity Administrator

La herramienta de Administrator para administrar el Gateway de correo se abre haciendo clic en la entrada **G DATA MailSecurity** en el grupo de programas **Inicio** > **(Todos los) programas** > **G DATA MailSecurity** del menú de inicio. Al iniciar el Administrador se le pedirá el servidor y la contraseña. Introduzca en el campo **Servidor** el nombre del ordenador o la dirección IP del ordenador en que se haya instalado el gateway de correo.

Al iniciar sesión por primera vez aún no dispone de Contraseña. Sin introducir una contraseña, haga clic en el botón **Aceptar**. Se abre entonces una ventana de introducción de contraseña en la que se puede definir en el campo **Nueva contraseña** una nueva contraseña para el G DATA MailSecurity Administrator. Confirme la contraseña introducida introduciéndola de nuevo el campo **Confirmar nueva contraseña** y luego haga clic en **Aceptar**. La contraseña se puede definir de nuevo en cualquier momento en el área **Opciones** en el área **Avanzado** pulsando el botón **Modificar contraseña**.

## 12.2. Configurar el G DATA MailSecurity Administrator

La barra de menú del G DATA MailSecurity Administrator ofrece las siguientes opciones:

- **Opciones**: aquí puede modificar todos los ajustes básicos para el funcionamiento de G DATA MailSecurity y adaptarlos a sus necesidades individuales.
- **Actualización**: en el área de actualización online se pueden definir parámetros básicos para la descarga automática desde Internet de las firmas de virus actuales. La planificación horaria de estas descargas se puede amoldar a las propias necesidades y además se pueden actualizar los archivos de programa de G DATA MailSecurity.
- **Filtro antispam**: le ofrece un acceso directo a la configuración del **Filtro antispam** en el módulo **Filtros**.
- **Ayuda**: aquí se accede a la ayuda en línea del producto.
- **Información**: aquí obtendrá información de versión del programa.

### 12.2.1. Opciones

En el área de opciones se pueden efectuar numerosos ajustes para adaptar G DATA MAILSECURITY de forma óptima al entorno y las condiciones de su red. Con este fin hay una serie de áreas de configuración ordenadas por temas en las distintas fichas que se pueden poner en primer plano haciendo clic en el área correspondiente.

## 12.2.1.1. Entrante (SMTP)

En esta área tiene la posibilidad de llevar a cabo todos los ajustes necesarios para el control de virus de los correos SMTP entrantes en su servidor de correo.

### Recepción

Aquí puede determinar si se van a procesar los correos entrantes. En general está predefinido el puerto 25. Si debido a alguna circunstancia especial este puerto estándar no se puede utilizar, puede definir con el botón **Configurar** otros ajustes de puerto y de protocolo para los correos entrantes.

### Transmisión

Para la transmisión de los correos entrantes a su servidor de correo desactive la opción **Utilizar DNS para enviar los correos** e introduzca el servidor deseado en **Transmitir correos a este servidor SMTP**. Introduzca también el **Puerto** que vaya a utilizar para transmitir los correos al servidor SMTP. Si se van a utilizar varias tarjetas de red, en **IP de origen** se puede seleccionar y definir cuál de estas tarjetas quiere utilizar.

### Protección antes de la retransmisión (Relaying)

Para impedir abusos sobre el servidor de correo, con la opción **Aceptar correos entrantes solo para los siguientes dominios o direcciones** se pueden -y se deben- establecer los dominios a los que se pueden enviar correos SMTP. Con esta medida cierra el paso a que su servidor se utilice para la transmisión de correos basura a otros dominios.

> **Nota**: Si no introduce aquí ningún dominio no se aceptará tampoco ningún correo. Si desea que se acepten todos los correos de todos los dominios, tiene que introducir aquí *.*(asterisco punto asterisco).

La protección de relay se puede implementar también alternativamente mediante una lista de direcciones válidas de correo electrónico. No se aceptarán los correos electrónicos para destinatarios que no estén en la lista. Para automatizar la actualización de estas direcciones de correo, se pueden leer de modo periódico y automático de **Active Directory**. Para la conexión con Active Directory se requiere .NET Framework 1.1 o superior.

## 12.2.1.2. Saliente (SMTP)

En esta área tiene la posibilidad de llevar a cabo todos los ajustes necesarios para el control de virus de los correos SMTP salientes en su servidor de correo.

### Recepción

Mediante la casilla de verificación **Procesar correo saliente** se define si los correos SMTP salientes se van a comprobar o no en busca de virus. En **Direcciones IP/subredes de los ordenadores que envían correos salientes** puede establecer las direcciones IP de las que llegan los correos para revisar. Si hay varias direcciones IP aplicables, sepárelas entre sí mediante comas. Es necesario indicar este dato para que el gateway de correo pueda distinguir entre correos entrantes y salientes. En general, el puerto 25 esa predefinido para la recepción de los correos salientes. Si debido a alguna circunstancia especial este puerto estándar no se puede utilizar, puede definir con el botón **Configurar** otros ajustes de puerto y de protocolo para los correos salientes.

### Transmisión

Active la entrada **Utilizar DNS para enviar los correos** para que los correos se envíen directamente al servidor de correo correspondiente del dominio de destino. Si desea enviar los correos por vía indirecta mediante un relay (como por ej. un proveedor), desactive entonces la opción **Utilizar DNS**

**para enviar los correos** e introduzca el relay en **Transmitir correos a este servidor SMTP**. Si hay disponibles varias tarjetas de red, en **IP de origen** se puede seleccionar y definir cuál de estas tarjetas quiere utilizar.

## 12.2.1.3. Entrante (POP3)

En esta área tiene la posibilidad de ajustar los parámetros necesarios para el control de virus de los correos POP3 entrantes en su servidor de correo.

### Consultar

Con la opción **Procesar consultas POP3** se activa la posibilidad de traerse los correos POP3 vía G DATA MAILSECURITY del servidor POP3 correspondiente, comprobar si tienen virus y retransmitirlos luego a los destinatarios mediante el servidor de correo. Para ello tiene que indicar, en su caso, el **Puerto** que emplee su programa de correo para las consultas POP3 (por lo general el puerto 110). En función del tráfico de correo electrónico, puede producirse un retraso de varios segundos cuando el usuario recupera sus mensajes POP3. Seleccione **Evitar superación del tiempo de espera en el programa de correo** para evitar que el destinatario pueda encontrarse con un error de tiempo de espera (timeout) cuando los datos no están disponibles de inmediato.

Los programas de correo basados en POP3 se pueden configurar manualmente. Para ello hay que utilizar en el programa de correo como servidor POP3 entrante 127.0.0.1 o el servidor de su gateway de correo y anotar el nombre del servidor de correo externo delante del nombre de usuario, separado por dos puntos. Es decir, por ej. en vez de *Servidor POP3:mail.xxx.es/nombre de usuario:josé cualquiera* escriba *Servidor POP3:127.0.0.1/nombre de usuario:mail.xxx.es:jose cualquiera*. Para poder efectuar la configuración manual necesaria, consulte en el manual de instrucciones de su programa de correo qué pasos hay que seguir para la configuración manual.

### Recogida

Especifique en la opción **Recoger correos de este servidor POP3** el servidor POP3 desde el que vaya a recoger los correos (por ej. *pop3.proveedorserviciocorreo.es*).

### Filtro

Cuando un correo POP3 es rechazado como consecuencia de una verificación de contenido o porque está infectado con un virus, se puede informar automáticamente al remitente del correo sobre esta circunstancia. El mensaje substitutorio predeterminado para los correos rechazados es el siguiente: *El administrador de sistemas ha rechazado el correo.* Pero puede configurar un texto propio para estas funciones de notificación. También se pueden utilizar comodines que transfieran ciertos datos relacionados con el correo rechazado al texto de notificación. Para el texto libre correspondiente al **Asunto** y al **Texto del correo** se pueden utilizar los siguientes comodines (definidos por el signo de porcentaje seguido de una letra minúscula):

- %v > Virus
- %s > Remitente
- %r > Destinatario
- %c > CC
- %d > Fecha
- %u > Asunto
- %h > Encabezamiento
- %i > IP de remitente

## 12.2.1.4. Comprobación de virus

En la comprobación de virus se pueden configurar las opciones de comprobación de virus para los correos entrantes y salientes.

### Entrante

Como norma general, la función **Comprobar si hay virus en correos entrantes** se debe tener activada, y también se debe tener en cuenta qué opción se quiere utilizar **En caso de infección**.

- **Solo registrar**
- **Desinfectar (si no es posible: solo registrar)**
- **Desinfectar (si no es posible: cambiar de nombre)**
- **Desinfectar (si no es posible: borrar)**
- **Cambiar de nombre adjuntos infectados**
- **Borrar adjuntos infectados**
- **Eliminar mensaje**

Las opciones que solo prevén registrar los virus entrantes solo se deben utilizar si el sistema ya está protegido de modo permanente contra los ataques de virus (p. ej., con la protección antivirus de G DATA Antivirus Business).

En el caso de que se encuentren virus se puede elegir entre numerosas opciones de notificación. Se puede añadir un aviso de virus en el asunto y en el texto del correo infectado para informar al destinatario del correo sobre esta circunstancia. También se puede enviar un mensaje sobre la detección de virus a determinadas personas, como por ej. al administrador de sistemas o al empleado responsable, para informarles de que se ha enviado un virus a una dirección de correo electrónico en su red. Si hay varias direcciones de destinatarios hay que separarlas mediante punto y coma.

El texto de las funciones de notificación se puede configurar de modo personalizado. Aquí se utilizan los mismos comodines que en **Entrante (POP3)** > **Filtro**.

### Saliente

Como norma general, se deben tener siempre activadas las funciones **Comprobar si hay virus en correos salientes** y **No enviar un correo infectado**. Con esta configuración, ningún virus podrá salir de su red y causar algún daño a los destinatarios. En el caso de que se encuentren virus se puede elegir entre numerosas opciones de notificación. Se puede **Informar al remitente del correo infectado** y, en **Enviar mensaje de virus a las personas siguientes**, comunicar p. ej. a administradores del sistema o a los empleados responsables de que iba a enviarse un virus desde su red. Si hay varias direcciones de destinatarios hay que separarlas mediante punto y coma.

El texto de las funciones de notificación se puede configurar de modo personalizado. Para hacerlo hay que pulsar el botón **...** situado a la derecha. Se pueden usar comodines para agregar información al **Asunto** y al **Texto del correo**. Aquí se utilizan los mismos comodines que en **Entrante (POP3)** > **Filtro**.

Adicionalmente, en **Opciones** > **Comprobación de virus** y en el punto **Añadir informe a los correos salientes (no infectados)**, se permite añadir en los correos comprobados por G DATA MailSecurity un informe al final del texto del e-mail en el que se indica expresamente que ese correo ha sido comprobado por G DATA MailSecurity. Este informe, por supuesto, se puede modificar conforme a las propias necesidades o suprimirse enteramente.

### G DATA ManagementServer

Si se está utilizando MailGateway como parte de una solución corporativa de G DATA, marcando la casilla **Notificar los virus detectados al G DATA ManagementServer**, se informa a G DATA ManagementServer de los virus detectados por el gateway de correo, proporcionándole de este modo una visión completa de la carga y peligro de virus a los que está sometida su red.

## 12.2.1.5. Parámetros de escaneo

En esta área se puede optimizar la capacidad de detección de virus de G DATA MailSecurity y adaptarla a los propios requerimientos. Como norma general se puede decir que al reducir la capacidad de detección de virus aumenta el rendimiento del sistema en su totalidad, mientras que una elevación de la capacidad de detección tendrá posiblemente como consecuencia pérdidas de rendimiento. En estos casos hay que sopesar los pros y los contras.

Aquí tiene a su disposición las siguientes funciones:

- **Utilizar motores**: G DATA MailSecurity trabaja con dos motores antivirus, dos unidades de análisis de virus básicamente independientes entre sí. En el apartado Utilizar motores se configura la forma de colaboración mutua de los dos motores. La utilización de ambos motores garantiza unos resultados óptimos en la detección de virus. Por el contrario, la utilización de un único motor puede aportar ventajas en el rendimiento, es decir, el proceso de análisis puede acelerarse usando un único motor.
- **Tipos de archivo**: con la opción Tipos de archivo puede determinar los tipos de archivo que deberá comprobar G DATA MailSecurity ante posibles virus. Le recomendamos aquí la detección automática de tipo, con la que automáticamente solo se comprueban archivos que, en teoría, son susceptibles de tener un virus. Si desea definir Ud. mismo los tipos de archivo que deben someterse a la comprobación de virus, utilice la función **Definido por el usuario**. Haciendo clic en el botón **...** se abre un cuadro de diálogo en el que se pueden indicar los tipos de archivo deseados en el campo de entrada superior y transferirlos luego con el botón de **Agregar**. Aquí también puede utilizar comodines.

  El signo de interrogación (?) representa caracteres sueltos. El signo de asterisco (*) representa una secuencia completa de caracteres. Para comprobar, p.ej., todos los archivos con la extensión .exe, introduzca **.exe*. Para comprobar, p.ej., archivos de distintos formatos de hojas de cálculo (p.ej., xlr, xls), introduzca simplemente **.xl?*. Para proteger, p.ej., archivos de formatos distintos que tengan un nombre que comience igual, deberá introducir, p.ej., *text*.**.
- **Heurística**: en el análisis heurístico se detectan los virus, no solo utilizando los bancos de datos de virus actuales, sino también en función de determinadas características de los tipos de virus. Este método es otro rasgo extra de seguridad que, sin embargo, en casos muy esporádicos puede producir una falsa alarma.
- **Comprobar archivos comprimidos**: se debe tener activado siempre la comprobación de los archivos comprimidos.
- **OutbreakShield**: con el OutbreakShield pueden identificarse y combatirse los pequeños daños provocados por envíos masivos de e-mails, antes de que estén disponibles las firmas de virus actualizadas. OutbreakShield se informa a través de Internet acerca de ciertas concentraciones de correos sospechosos y cierra prácticamente en tiempo real la brecha que existe entre el comienzo de un envío masivo de correos y su combate mediante las firmas especialmente adaptadas del virus. Si desea aplicar OutbreakShield, introduzca en el botón **Ajustes** si utiliza un servidor proxy y, en su caso, los **Datos de acceso para la conexión a Internet** para permitir en cualquier momento a OutbreakShield acceder a Internet. En OutbreakShield se puede definir el

texto del correo que recibirá un destinatario de correo cuando se rechace un correo masivo dirigido a él.

Como el OutbreakShield, debido a su arquitectura independiente, no puede desinfectar los adjuntos de correo infectados, ni renombrarlos ni ponerlos en cuarentena, el texto substitutorio informa al usuario de que no se le ha entregado un correo sospechoso o infectado. Si se selecciona el punto **Eliminar mensaje** en la opción **En caso de infección** en **Comprobación de virus**, OutbreakShield no enviará notificaciones para los emails que hayan sido rechazados. En este caso se borran directamente todos los correos infectados, incluyendo los que solo hayan sido detectados por OutbreakShield.

- **Protección antiphishing**: active la protección antiphishing para bloquear correos que intentan obtener contraseñas, información de tarjetas de crédito y otros datos personales haciéndose pasar por mensajes de instituciones fiables.

## 12.2.1.6. Cola de espera

En este área puede establecer la frecuencia y el intervalo del nuevo envío de los correos que MailGateway no haya podido redireccionar al servidor de correo correspondiente.

Por lo general, los correos llegan a la cola de espera después de la comprobación de virus por parte de G DATA MailSecurity. Puede haber varias razones para que los correos se encuentren en cola de espera. Así por ej., puede haber un fallo en el servidor al que desee redireccionar el correo después de la comprobación de virus.

### Correos que no se pueden entregar

En el apartado **Intervalo de repetición** se indican los intervalos en que G DATA MailSecurity debe proceder a un nuevo intento de envío. Por ejemplo, la indicación *1, 1, 1, 4,* significa que G DATA MailSecurity intenta enviar el correo una vez cada hora en las tres primeras horas y luego en intervalos regulares de 4 horas. En el **Tiempo de espera de error** se define cuándo se cancela definitivamente el envío y se borra el correo.

Se puede **Informar cada hora a los remitentes de correos en cola de espera**. Si no desea informar con regularidad a los remitentes sobre los correos que no se pueden entregar, introduzca aquí simplemente un *0*. Aunque esté desactivada la opción de informar a los remitentes sobre los correos no transmitidos, se informará de todas formas al remitente cuando su correo definitivamente no se pueda entregar y se borre del servidor.

Con el botón **Restablecer valores estándar** se pueden restablecer los ajustes estándar en el área de la cola de espera.

### Limitación de tamaño

El tamaño de la cola de espera se puede limitar de modo opcional, lo que supone una medida de protección contra los ataques de denegación de servicio. Cuando se excede la limitación de tamaño ya no se aceptan más correos electrónicos en la cola de espera.

## 12.2.1.7. Avanzado

En la zona Avanzado se pueden modificar los ajustes generales de G DATA MailSecurity.

### Banner SMTP

De modo predeterminado, el campo **Dominio** contiene el nombre del ordenador. Al enviar correos salientes mediante DNS debería introducirse aquí el nombre de dominio completo (FQDN) incluyendo el nombre del ordenador seguido de un punto y el nombre del domino, para permitir búsquedas

inversas. Active **Mostrar solo dominio**, para suprimir la indicación de la versión del servidor en la comunicación con otros servidores.

**Limitación**
Para limitar el número de conexiones SMTP que G DATA MailSecurity procesa simultáneamente hay que activar la marca de verificación delante de **Limitar el número de conexiones de cliente SMTP**. G DATA MailSecurity autorizará entonces solo el número máximo de conexiones que haya definido. Con esta opción se puede adaptar el filtrado de correos a la capacidad del hardware que se utilice para el gateway o pasarela de correo.

**Mensajes del sistema**
La **Dirección de remitente para mensajes de sistema** es la dirección de correo electrónico que se emplea, por ejemplo, para informar al remitente y al destinatario de correos infectados de que sus correos se encuentran en la cola de espera. Los avisos de sistema de G DATA MailSecurity no tienen relación con los mensajes generales sobre los virus encontrados. Los avisos de sistema suelen ser informaciones con un carácter más bien general que no están directamente vinculadas a un correo posiblemente infectado. Así, G DATA MailSecurity enviará p. ej. un aviso de sistema cuando el control antivirus no esté ya garantizado por alguna razón.

**Ajustes**
Con los botones **Importar** y **Exportar** se pueden guardar los ajustes de las opciones de programa en un archivo XML y volver a importarlos de nuevo cuando sea necesario.

**Modificar contraseña**
Aquí se puede modificar la contraseña que se haya establecido al iniciar por primera vez G DATA MailSecurity. Para esta operación solo hay que introducir la contraseña vigente actualmente en **Contraseña antigua** y luego la nueva contraseña en **Nueva contraseña** y **Confirmar nueva contraseña**. Haciendo clic en el botón de **Aceptar** se efectúa la modificación de la contraseña.

## 12.2.1.8. Registro

En el área de registro se puede analizar desde el punto de vista estadístico el tráfico de correo en su servidor (que haya sido guardado en la base de datos). Los resultados de esta función de estadística se pueden obtener desde el área de estadística de la interfaz del programa, haciendo clic en el botón **Estadística** situado en el área de programa **Estado**. Alternativamente, también se pueden guardar los datos analizados en un archivo log externo (maillog.txt). Con las funciones **Solo correos basura** y **Limitar el número de e-mails** se puede limitar, en caso necesario, el tamaño de este archivo log.

## 12.2.2. Actualización

En el área de actualizaciones se pueden efectuar numerosos ajustes para adaptar G DATA MailSecurity idóneamente al entorno y las condiciones de su red. Aquí se pueden actualizar las firmas de virus y los archivos de programa de G DATA MailSecurity de modo manual o automático.

## 12.2.2.1. Configuración

Si se está utilizando MailSecurity como parte de una solución corporativa de G DATA, puede evitar descargas redundantes habilitando **Utilizar firmas de virus del G DATA Security Client**, y obtener estas directamente del G DATA Security Client instalado. Con la función **Ejecutar por sí mismo la actualización online de las firmas de virus** G DATA MailSecurity efectúa esta operación de modo autónomo. Con el botón **Ajustes y programación** se accede a un área en que se pueden introducir todos los parámetros y ajustes necesarios para las actualizaciones online manuales y automáticas.

### Datos de acceso

En el apartado Datos de acceso tiene que introducir el **Nombre del usuario** y la **Contraseña** que haya recibido al registrar G DATA MailSecurity. Con estos datos se realizará la autenticación en el servidor de actualizaciones de G DATA para que la actualización de las firmas se realice de forma completamente automática.

Haga clic en el botón **Registrarse en el servidor**, si todavía no se ha registrado en el servidor G DATA. Simplemente tiene que introducir el número de registro (lo encontrará en el dorso del manual del usuario) y sus datos de cliente, y luego hacer clic en **Registro**. Los datos de acceso (el nombre de usuario y la contraseña) se muestran inmediatamente. Anote estos datos y guárdelos en un lugar seguro. Para registrarse en el servidor (igual que para las actualizaciones online de las firmas de virus) se necesita una conexión a Internet.

### Planificación horaria de la actualización online (base de datos de virus)

Mediante el módulo Planificación horaria de la actualización online se puede determinar cuándo y con qué frecuencia debe producirse la actualización automática. En el campo **Ejecutar** se introduce un valor de referencia que luego se especifica con la opción **Fecha**.

Con la opción **Diariamente** se puede definir, por ejemplo, en **Días de la semana** que su ordenador solo lleve a cabo una actualización en días laborables o, solo cada dos días, o bien durante los fines de semana en que no se use para trabajar. Para modificar las fechas y las horas en la opción **Fecha**, simplemente marque el elemento que quiera modificar (p. ej., día, hora, mes, año) con el ratón y utilice luego las flechas del teclado o los pequeños símbolos de flecha a la derecha del campo de entrada para moverse cronológicamente por el correspondiente elemento.

### Configuración de Internet

En caso de que utilice un ordenador protegido por un cortafuegos o tenga alguna configuración especial con respecto al acceso a Internet, será necesario que configure su **Servidor proxy**. Solo deberá cambiar esta configuración cuando la actualización online falle. En caso de ser necesario, diríjase a su proveedor de internet para determinar la dirección proxy que debe utilizar.

Los datos de acceso para la conexión a Internet (nombre de usuario y contraseña) son de gran importancia, si la actualización de internet está basada en un calendario programado. Sin estos datos no se puede realizar ninguna conexión automática con Internet. Tenga también en cuenta que en los ajustes generales de Internet (p.ej. para su programa de correo o su navegador de Internet) debe estar habilitado el inicio de sesión automático. G DATA MailSecurity puede iniciar el proceso de actualización online sin un registro automático, pero luego deberá esperar a que el usuario confirme la conexión a Internet con **Aceptar**. Con la selección en **Región del servidor de actualizaciones** se puede elegir un servidor de actualizaciones de su región, para, eventualmente, optimizar la transmisión de datos.

### Cuenta de usuario

En la opción **Cuenta de usuario** se introduce una cuenta de usuario del ordenador MailGateway que tenga acceso a Internet.

> **Nota**: Tenga cuidado de no confundir los datos que introduzca en **Datos de acceso** y **Cuenta de usuario**.

## 12.2.2.2. Firmas de virus

Con los botones **Actualizar base de datos de virus** y **Actualizar estado** puede también iniciar actualizaciones de firmas de virus independientemente de las especificaciones que tenga definidas en

la planificación horaria.

### 12.2.2.3. Archivos de programa

Con el botón **Actualización de programa** puede actualizar también los archivos de programa de G DATA MailSecurity en cuanto se produzcan modificaciones y mejoras.

## 12.3. Áreas de programa

El programa G DATA MailSecurity se maneja de un modo básicamente intuitivo y está estructurado de forma muy clara. Usando las diferentes áreas, que puede seleccionar en G DATA MailSecurity Administrator mediante los iconos situados a la izquierda, puede cambiar al área de programa correspondiente y llevar a cabo acciones, definir parámetros o verificar procesos.

### 12.3.1. Estado

En el área de estado del Administrator obtendrá información básica sobre el estado actual de su sistema y del Gateway de correo. Estos datos figuran a la derecha de la entrada correspondiente en forma de texto, número o fecha.

- Mientras que G DATA MailSecurity tenga una configuración ideal que le proteja de los virus informáticos, se verá el símbolo de un semáforo en verde a la izquierda de las entradas citadas.
- Pero si uno de los componentes no tuviera el ajuste ideal (p.ej., las firmas de virus no están actualizadas o la comprobación de virus, desactivada), un símbolo de atención le indica esta circunstancia.

Haciendo doble clic en la correspondiente entrada (o seleccionando la entrada y haciendo clic en el botón **Editar**) se pueden realizar directamente operaciones o cambiar al área de programa correspondiente. En cuanto haya optimizado los ajustes de un componente con el símbolo de atención, el símbolo en el área de estado cambiará de nuevo al semáforo en verde. Están disponibles las siguientes entradas:

- **Procesamiento de los correos entrantes**: el procesamiento de los correos entrantes se encarga de que el Gateway de correo compruebe los correos antes de redireccionarlos a los destinatarios. Efectuando un clic doble en esta entrada se accede a la ventana de configuración correspondiente (barra del menú: **Opciones** > **Entrante (SMTP)** y **Opciones** > **Entrante (POP3)**) y una vez allí se puede adaptar el tratamiento de los correos entrantes a los propios requerimientos.
- **Comprobación de virus en correo entrante**: la comprobación de los correos entrantes impide a los correos infectados entrar en su red. Efectuando un clic doble en esta entrada se accede a la ventana de configuración correspondiente (barra del menú: **Opciones** > **Comprobación de virus**) y una vez allí se puede adaptar la comprobación de los correos entrantes a los propios requerimientos.
- **Procesamiento de los correos salientes**: el procesamiento de los correos salientes se encarga de que el Gateway de correo compruebe los correos antes de redireccionarlos a los destinatarios. Efectuando un clic doble en esta entrada se accede a la ventana de configuración correspondiente (barra del menú: **Opciones** > **Saliente (SMTP)**) y una vez allí se puede adaptar el tratamiento de los correos salientes a los propios requerimientos.
- **Comprobación de virus en correo saliente**: la comprobación de los correos salientes impide que se envíen archivos infectados desde su red. Efectuando un clic doble en esta entrada se accede a la ventana de configuración correspondiente (barra del menú: **Opciones** >

**Comprobación de virus**) y una vez allí se puede adaptar la comprobación de los correos salientes a los propios requerimientos.

- **OutbreakShield**: con el OutbreakShield pueden identificarse y combatirse los daños provocados por envíos masivos de e-mails, antes de que estén disponibles las firmas de virus actualizadas. OutbreakShield obtiene información a través de Internet, acerca de ciertas concentraciones de correos sospechosos y cierra prácticamente en tiempo real, la brecha que existe entre el comienzo de un envío masivo de correos y su combate mediante las firmas de virus, especialmente adaptadas.
- **Actualizaciones automáticas**: las firmas de virus se pueden actualizar por sí solas. Conviene tener activada en general la opción para las actualizaciones automáticas. Efectuando un clic doble en esta entrada se accede a la ventana de configuración correspondiente (barra del menú: **Actualización**), donde se puede adaptar la frecuencia de actualización a los requerimientos individuales.
- **Fecha de las firmas de virus**: cuanto más actualizadas estén las firmas de virus, más segura será la protección. Las firmas de virus se deben actualizar con la máxima frecuencia y, en la medida de lo posible, hay que automatizar este proceso. Efectuando un clic doble en esta entrada se accede a la ventana de configuración correspondiente (barra del menú: **Actualización**), donde se puede efectuar también directamente una actualización online (independientemente de los horarios programados).
- **Filtro antispam**: el **Filtro antispam** le ofrece amplias posibilidades de configuración para cerrar el paso de forma eficaz a los correos electrónicos con contenidos o procedencia indeseados (por ejemplo de expedidores de correos en masa).
- **Spam-OutbreakShield**: con el Spam-OutbreakShield se pueden combatir con rapidez y seguridad los correos masivos. Antes de recoger los correos, Spam-OutbreakShield, explora Internet para detectar concentraciones extraordinarias de correos sospechosos impidiendo que estos lleguen al buzón del destinatario.

Si durante la instalación ha activado la opción **Estadística** de correo, podrá acceder a un análisis estadístico del tráfico de correo o del volumen de spam pulsando el botón Estadística. La estadística se puede configurar en el menú de **Opciones** del Administrator, en el área **Registro**.

## 12.3.2. Filtro

En el área de filtro, se pueden aplicar filtros con gran sencillez, para bloquear tanto el correo entrante y saliente, como eliminar automáticamente del correo los contenidos potencialmente peligrosos. Los filtros correspondientes se visualizan en la lista del área de filtros y pueden activarse o desactivarse con las casillas de verificación situadas a la izquierda de cada registro.

- **Importar**: también puede guardar en un archivo XML filtros individuales con sus ajustes especiales para utilizarlos de nuevo en ese o en otro ordenador.
- **Exportar**: también puede guardar en un archivo XML filtros individuales con sus ajustes especiales para utilizarlos de nuevo en ese o en otro ordenador. Para exportar varios filtros, selecciónelos con el ratón y mantenga presionada la tecla Ctrl.
- **Nuevo**: con el botón Nuevo se pueden crear nuevas reglas de filtrado. Cuando se crea un nuevo filtro, se abre una ventana de selección en la que puede determinar el tipo de filtro básico. Los demás detalles acerca del filtro, pueden ser creados a través de un asistente, el cual le guiará en ese tipo de filtrado. De este modo se crean con la mayor comodidad filtros contra cualquier amenaza imaginable.

- **Editar**: con el botón Editar se pueden editar los filtros existentes.
- **Eliminar**: para borrar definitivamente un filtro, márquelo haciendo clic en él con el ratón y pulse luego el botón Eliminar.
- **Estadística**: para consular la información estadística de cada filtro.
- **Protocolo**: para el **Filtro antispam** hay un registro con una lista en la que figuran los correos considerados spam. En el registro se ven también los criterios que han llevado a clasificar el correo como spam (valores de índice de spam). En caso de que un correo se haya clasificado erróneamente como spam, aquí se puede informar online al servidor de OutbreakShield de que se ha producido una detección errónea (falso positivo). OutbreakShield comprueba de nuevo el correo y - si realmente se había etiquetado de modo erróneo como spam - lo clasifica de allí en adelante como no sospechoso. En esta transacción solo se transmite el checksum, y no el contenido del correo.

  Por supuesto, su red sigue estando protegida frente a los virus independientemente de las reglas de filtrado específicas, ya que G DATA MailSecurity siempre está examinando en segundo plano los correos que entran y salen. Las reglas de filtrado tienen más bien la finalidad de mantener sus cuentas de correo a salvo de correos indeseados, spam y scripts poco fiables, minimizando así potenciales focos de infección antes del examen de virus propiamente dicho que realiza G DATA MailSecurity.

Para todos los tipos de filtrado, se puede indicar un nombre para el filtro correspondiente en el campo **Nombre**; en **Observación** se pueden especificar observaciones y notas internas sobre el filtro en cuestión. En la opción **Dirección** se puede definir de modo general si una regla de filtrado solo se aplica a los **Correos entrantes**, solo a los **Correos salientes** o a **Ambas direcciones**.

En la sección **Reacción** puede determinar la forma de proceder con los correos que cumplan los criterios de filtrado, es decir, los clasificados como spam. El texto para las funciones **Notificar al remitente de correo** y **Enviar mensaje a las personas siguientes** se puede redactar de modo personalizado. Solo tiene que hacer clic en el botón a la derecha de la reacción correspondiente. Se pueden utilizar caracteres comodín para introducir información en los campos **Asunto** y **Texto del correo**. Aquí se utilizan los mismos comodines que en **Entrante (POP3)** > **Filtro**.

### 12.3.2.1. Filtrar confirmación de lectura

Este filtro borra las consultas de confirmación de lectura para los correos entrantes y/o salientes.

### 12.3.2.2. Desactivar secuencias de comandos HTML

Este filtro desactiva los scripts en la parte HTML de un correo. Los scripts, que en una página web tienen cierta lógica, si van acompañando un correo HTML, son más bien molestos. En algunos casos, las secuencias de comandos HTML se usan activamente para infectar el ordenador, ya que tienen la posibilidad no solo de difundirse al abrir un fichero adjunto, sino que pueden activarse incluso en la vista previa de un mensaje de correo.

### 12.3.2.3. Desactivar referencias externas

Muchos boletines e información de productos en formato HTML contienen enlaces que se muestran y se ejecutan cuando se abre el correo. Puede tratarse, por ej., de gráficos que no se envían junto con el correo, sino que se cargan con posterioridad automáticamente mediante un hipervínculo. Pero estos gráficos no son siempre inofensivos, también pueden contener rutinas dañinas, por eso, lo más conveniente es desactivar estas referencias. Al texto en sí del correo no le afecta esta desactivación.

## 12.3.2.4. Filtro de lista gris

Los filtros de lista gris son un método efectivo de reducir el volumen de spam. Tan pronto como un correo electrónico entra en el sistema, el filtro de la lista gris devuelve una solicitud al servidor de envío para reenviar el mensaje. Como la mayoría de los emisores de spam no suelen utilizar una administración de cola y reenvían sus correos muy raramente al mismo servidor SMTP, el mensaje no será reenviado.

- **Tiempos de espera (minutos)**: con este ajuste se puede definir cuánto tiempo se bloquea la transmisión de los correos sospechosos. Una vez transcurrido este intervalo, el correo se transmite en el siguiente intento de entrega. Cuando el destinatario reacciona a ese remitente, se le saca de la lista del filtro de lista gris y se introduce en una lista blanca. A partir de entonces, ya no se bloquea ni se demora la entrega de los correos de este emisor.
- **Tiempos de validez (días)**: para que la lista blanca de los remitentes deseados permanezca actualizada, la dirección del remitente solo permanece un cierto tiempo en la lista blanca antes de volver al estado de lista gris. El contador para el remitente correspondiente se restablece de nuevo cada vez que envía correo. Si, por ejemplo, programa un valor de más de 30 días, puede dejar permanentemente en la lista blanca un boletín mensual que desea recibir.

> El filtro de lista gris solo se puede seleccionar cuando está activado también el **Filtro antispam** de G DATA MailSecurity, y existe una base de datos SQL instalada en el servidor.

## 12.3.2.5. Filtrar datos adjuntos

A la hora de filtrar archivos hay muchas posibilidades de filtrar los adjuntos de correo electrónico. La mayoría de virus de correo electrónico se propagan a través de estos adjuntos, que, por lo general, incluyen archivos ejecutables más o menos ocultos. Puede tratarse del clásico archivo EXE, que incluye un programa dañino, pero también de scripts VB, que en algunas circunstancias pueden esconder archivos de imágenes, de video o música aparentemente seguros. Por lo general, todo usuario debería tener mucho cuidado al ejecutar los archivos adjuntos y en caso de duda, es mejor enviar una consulta al remitente de un correo, antes de que se ejecute un programa que él no ha solicitado.

En **Extensiones de archivo** se puede definir una lista de las distintas extensiones de los archivos sobre las que aplicar el filtro correspondiente. Aquí puede incluir, por ejemplo, todos los archivos ejecutables en un filtro (p.ej. archivos EXE y COM), pero filtrar también otros formatos (p. ej. MPEG, AVI, MP3, JPEG, JPG, GIF etc.), cuando debido a su tamaño, representen una carga para el servidor de correo. Por supuesto, puede filtrar también cualquier otro tipo de archivos comprimidos (como p. ej. ZIP, RAR o CAB). Separe todas las extensiones de fichero de un grupo de filtros mediante punto y coma, p. ej. *.exe; *.dll. En la opción Modo, introduzca las extensiones de los archivos que desee autorizar (**Permitir solo los adjuntos indicados**) o prohibir (**Filtrar adjuntos indicados**).

La función **Filtrar adjuntos en los correos incrustados** se ocupa de que también se filtren los tipos de datos seleccionados en **Extensiones de archivo** en los correos que sean, a su vez, un anexo dentro de otro e-mail. Esta opción debe activarse como norma general. Mediante la función **Solo cambiar el nombre de los datos adjuntos** no se borran automáticamente los anexos que se deben filtrar sino que simplemente se les cambia el nombre. Esto es especialmente útil, por ejemplo, con archivos ejecutables (como p.ej. EXE y COM), pero también con archivos de Microsoft Office, que podrían incluir scripts y macros ejecutables. Al renombrar un archivo adjunto éste no podrá abrirse simplemente con un clic de ratón, sino que primero debe ser guardado por el destinatario y llegado el caso renombrado de nuevo, antes de poder volver a utilizarse. Si la marca de verificación de Solo cambiar el nombre de

los datos adjuntos no está activa, se borrarán directamente los archivos adjuntos.

En **Sufijo** introduzca los caracteres con los que desee ampliar la extensión de archivo. De este modo se evita que se ejecute un archivo con un simple clic (p. ej. *.exe_danger). Con la opción **Insertar mensaje en el texto del mensaje de correo electrónico** puede informar al destinatario del correo filtrado de que un archivo adjunto se ha borrado o renombrado debido a una regla de filtro.

### 12.3.2.6. Filtro de contenido

El filtro de contenido le permite bloquear cómodamente los correos que incluyan determinados temas o textos. Solo tiene que introducir en **Expresión regular** las palabras clave y las expresiones a las que deba reaccionar G DATA MailSecurity. Luego introduzca en **Área de búsqueda** en qué áreas de un correo se deben buscar estas expresiones. Con el botón **Nuevo** a la derecha del campo de entrada para la Expresión regular se puede introducir con comodidad el texto generado por una acción del filtro. Aquí puede combinar texto a su elección con los operadores lógicos Y y O.

> Si, por ejemplo, introduce *alcohol Y drogas,* en un correo que contuviese por ejemplo los términos *alcohol* y *drogas* el filtro se activaría, pero no con un correo que solo incluyese la palabra *alcohol* o solo la palabra *drogas*. El operador lógico Y parte de la premisa de que todos los elementos unidos con Y están disponibles, el operador lógico O solo presupone que un elemento, por lo menos, está disponible.

También se puede omitir la ayuda de entrada de Expresión regular y combinar entre sí cualquier término de búsqueda. Para ello solo hay que introducir los conceptos de búsqueda y enlazarlos mediante operadores lógicos. "O" corresponde a la línea de separación "|" (Mayúsculas + 1). "Y" corresponde al signo "&" (Mayúsculas + 6).

### 12.3.2.7. Filtro de remitentes

El filtro de remitentes le permite bloquear de una forma sencilla e-mails provenientes de determinados remitentes. Simplemente tiene que introducir en **Direcciones/dominios** las direcciones de correo electrónico o los nombres de los dominios frente a los que G DATA MailSecurity tenga que reaccionar. En caso de que haya varias entradas, puede separarlas mediante punto y coma. También se pueden filtrar y descartar automáticamente los correos sin remitente definido.

### 12.3.2.8. Filtro de destinatarios

Con el filtro de destinatarios se pueden bloquear con comodidad los e-mails para destinatarios determinados. Simplemente tiene que introducir en **Direcciones/dominios** las direcciones de correo electrónico o los nombres de los dominios frente a los que G DATA MailSecurity tenga que reaccionar. En caso de que haya varias entradas, puede separarlas mediante punto y coma. También se pueden filtrar y descartar automáticamente los correos con campo de destinatario vacío (es decir, los correos que solo contengan destinatarios en los campos CCO y/o CC).

### 12.3.2.9. Filtrar spam

El filtro antispam le ofrece amplias posibilidades de configuración para bloquear de forma eficaz los correos electrónicos con contenidos o procedencia indeseados (p. ej., de remitentes de correos en masa). El programa verifica numerosas características de los correos electrónicos que son típicas del spam. Teniendo en cuenta las características encontradas en el mensaje se calcula un valor que refleja la probabilidad de que sea spam. Para esta acción hay disponibles varias pestañas en las que figuran ordenadas por temas todas las posibilidades de configuración relevantes.

### Filtro

Introduzca en **Nombre** y **Observación** qué nombre desea dar al filtro y qué informaciones adicionales pueden ser necesarias para ello. En **Reacción** puede determinar qué procedimiento debe seguir el filtro antispam con los emails que posiblemente incluyen spam. Aquí se pueden distinguir tres niveles, que dependen del grado de probabilidad que G DATA MailSecurity atribuya a que el correo en cuestión sea spam.

En **Sospecha de spam** se determina como tratar los emails en los que G DATA MailSecurity encuentra algunos elementos de spam. En estos casos no tiene por qué tratarse siempre de Spam, sino que en algunos casos puede también tratarse de boletines de noticias o envíos publicitarios que el destinatario sí desea recibir. En estos casos se recomienda avisar al destinatario de la sospecha de spam. En **Probabilidad de spam alta** se agrupan los emails que incluyen muchas características de spam y solo en casos muy raros son deseados por el destinatario. En **Probabilidad de spam muy alta** se encuentran los emails que cumplen todos los criterios del correo spam. En este caso prácticamente nunca se trata de mensajes deseados y rechazar este tipo de correos está recomendado la mayoría de las veces. Estas tres reacciones de distinto grado se pueden configurar individualmente.

Así, en **Rechazar correo** tiene la posibilidad de que el correo ni siquiera llegue a su servidor de correo. El destinatario no recibe este correo en absoluto. Con la opción **Insertar aviso de spam en asunto y texto** se puede poner en conocimiento de un destinatario que es spam un correo así identificado. Con la opción **Informar al remitente del correo** se puede enviar un correo automático de respuesta al remitente del correo identificado como spam. En esta respuesta automática se le informa de que su correo ha sido considerado spam. Pero debido a que precisamente en el negocio del spam muchas direcciones de correo solo se utilizan una vez, hay que sopesar la conveniencia de utilizar esta función. Con la función **Transmitir a las personas siguientes** se pueden redireccionar automáticamente los correos sospechosos de spam, por ej. al administrador de sistemas.

### Lista blanca

Mediante la lista blanca puede excluir de forma explícita de la sospecha de spam, determinadas direcciones de remitentes o dominios. Simplemente introduzca en el campo **Direcciones/dominios** la dirección de correo (p. ej. *newsletter@gdata.es*) o bien el dominio (p. ej. *gdata.es*), que desea excluir de la sospecha de spam y G DATA MailSecurity considerará que los e-mails de este remitente o dominio del remitente no son spam. Con el botón **Importar** puede también incluir listas ya confeccionadas de direcciones de correo o de dominios en la lista blanca. Las direcciones y dominios deben aparecer en la lista en renglones separados. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Con el botón **Exportar** también puede exportar la lista blanca como archivo de texto.

### Lista negra

Mediante una lista negra se puede presuponer explícitamente que determinadas direcciones de remitentes o dominios posiblemente son spam. Simplemente introduzca en el campo **Direcciones/ dominios** la dirección de correo (p.ej. *newsletter@megaspam.de.vu*) o el dominio (p.ej. *megaspam.de.vu*) que desee poner bajo sospecha de spam y G DATA MailSecurity tratará, como norma general, los e-mails de este remitente o dominio como Correos con probabilidad de spam muy alta. Con el botón **Importar** puede también incluir listas ya confeccionadas de direcciones de correo o de dominios en la lista negra. Las direcciones y dominios deben aparecer en la lista en renglones separados. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Con el botón **Exportar** también puede exportar la lista negra como archivo de texto.

### Listas negras en tiempo real

En Internet se encuentran listas negras que contienen direcciones IP de servidores de los que se tiene constancia de que a través de ellos se envía spam. G DATA MailSecurity averigua mediante consultas por DNS a las RBL (Realtime Blacklists, listas negras en tiempo real) si el servidor remitente está incluido en esta lista negra. En caso afirmativo, aumenta la probabilidad de spam. Como norma general debería utilizar aquí el ajuste estándar, aunque en la **Lista negra 1**, **2** y **3** pueden indicarse direcciones propias de listas negras de Internet.

### Palabras clave (asunto)

Mediante la lista de palabras clave también puede poner los correos bajo sospecha de spam en función de las palabras utilizadas en la línea del asunto. Si aparece como mínimo uno de los términos en la línea de asunto, aumenta la probabilidad de spam. Esta lista se puede modificar según las propias necesidades con los botones **Agregar**, **Modificar** y **Eliminar**. Mediante el botón **Importar** puede también añadir a su lista otras listas ya confeccionadas de palabras clave. Cada entrada debe aparecer en la lista en un renglón propio. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Mediante el botón **Exportar** también puede exportar la lista de palabras clave como archivo de texto. Marcando la opción **Buscar solo palabras completas** puede determinar que G DATA MailSecurity busque en el texto del asunto solo palabras completas de tal forma que un término como *sex*se considerará sospechoso de spam, mientras que p.ej. la expresión *sexto* pasará el filtro sin problemas.

### Palabras clave (texto del correo)

Mediante la lista de palabras clave también puede poner correos bajo sospecha de spam en función de las palabras utilizadas en el texto del correo. Si aparece como mínimo uno de los términos en el texto del correo electrónico, aumenta la probabilidad de spam. Esta lista se puede modificar según las propias necesidades con los botones **Agregar**, **Modificar** y **Eliminar**. Mediante el botón **Importar** puede también añadir a su lista otras listas de palabras clave ya confeccionadas. Cada entrada debe aparecer en la lista en un renglón propio. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Mediante el botón **Exportar** también puede exportar la lista de palabras clave como archivo de texto. Marcando la opción Buscar solo palabras completas puede determinar que G DATA MailSecurity busque en el texto del asunto solo palabras completas de tal forma que un término como *sex*se considerará sospechoso de spam, mientras que p.ej. la expresión *sexto* pasará el filtro sin problemas.

### Filtro de contenido

El filtro de contenido consiste en un filtro inteligente basado en el método Bayes, que calcula la probabilidad de spam basándose en las palabras utilizadas en el texto del correo. Para ello, este filtro no se basa únicamente en listas fijas de palabras, sino que aprende con cada correo que se recibe. Mediante el botón **Consultar contenido de tabla** pueden consultarse las listas de palabras que utiliza el filtro de contenido para la clasificación de un correo como spam. Mediante el botón **Restablecer tablas** se borran todos los contenidos aprendidos de las tablas y el filtro de contenido autoadaptable comienza desde el principio el proceso de aprendizaje.

### Ajustes profesionales

En esta área puede modificar a un nivel muy detallado la detección de spam de G DATA MailSecurity, para adaptarla a las condiciones de su servidor de correo. Sin embargo, se recomienda en estos casos utilizar por norma general los ajustes estándar. Realice modificaciones en los ajustes profesionales únicamente si conoce la materia y sabe perfectamente lo que está haciendo.

Seleccione **Valores índice de spam** para editar los diferentes valores que se utilizan para clasificar

correos sospechosos de contener spam, alta probabilidad de spam o probabilidad de spam muy alta. Recomendamos los valores estándar.

### 12.3.2.10. Filtro IP

El filtro IP veda la recepción de correos procedentes de ciertos servidores determinados. Los filtros se pueden usar en el modo tanto de lista blanca como de lista negra. Introduzca en el Campo **Nombre** el nombre de la regla, y en **Observación** introduzca la información sobre por qué quiere bloquear o permitir las distintas direcciones IP. A continuación introduzca cada una de las direcciones IP en **Direcciones IP**. Haga clic en **Agregar** y la lista de direcciones IP registradas se transferirá a la lista de las direcciones IP bloqueadas. En el Modo se puede definir si el filtro IP en el modo de lista blanca solo permitirá rangos de direcciones IP definidos o si, en el modo de lista negra, solo se bloquean rangos de direcciones IP determinados. La lista de las direcciones IP se puede también exportar como archivo txt y, a la inversa, importar una lista txt con direcciones IP.

### 12.3.2.11. Filtro de idiomas

Con el filtro de idiomas puede definir automáticamente como spam correos en determinados idiomas. Si, p. ej., no suele tener contacto por correo electrónico con ninguna persona de habla inglesa, puede filtrar muchísimos correos basura definiendo el inglés como idioma de spam. Seleccione aquí los idiomas en los que no suele recibir correos para aumentar considerablemente la efectividad de G DATA MailSecurity para los correos escritos en estos idiomas.

## 12.3.3. Colas de espera

En el área de colas de espera se pueden ver de una ojeada los correos entrantes y salientes que llegan al Gateway de correo y que son examinados con respecto al contenido y a la presencia de virus. Por lo general, los correos son retransmitidos inmediatamente ya que apenas son mínimamente retardados por MailGateway y enseguida se borran de nuevo de la lista de colas de espera. En cuanto un correo no es apto para la entrega al destinatario o se producen retrasos en la entrega al destinatario (porque el servidor correspondiente, por ejemplo, no está disponible en ese momento), en la lista de cola de espera se señaliza esta circunstancia. G DATA MailSecurity intentará enviar nuevamente el correo en los intervalos que se hayan establecido (en **Opciones** > **Cola de espera**).

Con este sistema se puede realizar siempre un seguimiento de si la entrega de correo no ha tenido lugar o se ha producido con retraso. Con el botón **Entrante/saliente** se cambia de la vista de lista para correos entrantes a la vista de lista para correos salientes. Con el botón **Repetir ahora**, un correo marcado que no haya podido ser entregado se puede entregar de nuevo - independientemente de los tiempos que haya definido para una nueva entrega en **Opciones** > **Cola de espera**. Con el botón **Eliminar** se eliminan definitivamente de la cola los correos no aptos para la entrega.

## 12.3.4. Actividad

En el área de actividad se puede ver en cualquier momento un resumen de las acciones realizadas por G DATA MailSecurity. Estas acciones figuran con **Hora**, **ID** y **Acción** en la lista de actividades. Con la barra de desplazamiento de la derecha se puede navegar hacia arriba y hacia abajo en el registro. Al pulsar el botón **Restablecer** se borra el registro generado hasta el momento y G DATA MailSecurity empieza de nuevo a registrar las actividades. Con la función **Desactivar desplazamiento de pantalla** se sigue actualizando la lista pero las últimas actividades no se muestran directamente en primer lugar. Así puede navegar en ella de modo selectivo.

Mediante la etiqueta ID, puede descubrir las acciones registradas y asignada a un mismo

correo. Así, las operaciones con el mismo ID siempre se corresponden (por ej. 12345 Cargando correo, 12345 procesando correo, y 12345 enviando correo).

### 12.3.5. Virus detectados

En el área de virus encontrados encontrará información detallada sobre el momento en que G DATA MailSecurity ha encontrado un correo infectado, las medidas que se han tomado, de qué tipo de virus se trata y quiénes son realmente el remitente y el destinatario del correo en cuestión. Con la opción **Eliminar** se borra el mensaje de virus seleccionado de la lista de virus encontrados.

# 13. FAQ

## 13.1. Instalación

### 13.1.1. Después de la instalación del cliente, algunas aplicaciones son bastante más lentas que antes

El vigilante supervisa en segundo plano todos los accesos a los archivos y verifica si hay virus en los archivos de acceso. Esta actividad conlleva normalmente una demora prácticamente imperceptible. Pero si la aplicación tiene muchos archivos o abre con mucha frecuencia algunos archivos, se pueden producir demoras considerables. Para eludir esto, desactive primero temporalmente el vigilante para asegurarse de que este componente es el causante de las pérdidas de velocidad. Si el ordenador afectado accede a los archivos de un servidor, también deberá desactivarse temporalmente el vigilante en el servidor. Si el vigilante es el origen del problema, normalmente puede resolverse definiendo una excepción (es decir, archivos exentos de análisis). Primero hay que averiguar cuáles son los archivos a los que se accede frecuentemente. Estos datos pueden determinarse con un programa como, por ejemplo, MonActivity. En caso necesario, diríjase a nuestro **ServiceCenter**.

> Por supuesto, el rendimiento también se puede aumentar empleando un solo motor para el análisis en busca de virus en vez de los dos. Esta modalidad se presta sobre todo en sistemas antiguos y se puede ajustar en **el área del vigilante**.

### 13.1.2. He instalado el software G DATA sin registro. ¿Cómo puedo registrar el software?

Para registrar el software tras la instalación, abra la **Actualización online** en **Inicio** > **(Todos los) programas** > **G DATA** > **G DATA ManagementServer**. Allí encontrará la disponible la opción **Registro online**. Al hacer clic sobre este botón, se abre el formulario de registro. Introduzca el número de registro que acompaña al producto. Encontrará este número en la confirmación del pedido. En caso de dudas, contacte a su proveedor de servicios TI o al distribuidor responsable.

Con la introducción del número de registro se activa su producto. Los datos de acceso creados se muestran una vez terminado correctamente el registro. **¡Es imprescindible apuntar estos datos de acceso!** Una vez finalizado el registro, ya no será posible introducir nuevamente la clave de licencia. Si al introducir el número de registro le surge algún problema, compruebe que ha apuntado el número de registro correcto. Dependiendo del tipo de letra utilizado, se puede interpretar mal una "I" mayúscula (de Italia) como la cifra "1", o como la letra "l" (de Lima). Lo mismo puede ocurrir entre: "B" como "8"; "G" como "6" y "Z" como "2".

> Si ha adquirido G DATA Client Security Business, G DATA Endpoint Protection Business o el módulo adicional G DATA PatchManager y en la instalación no los ha activado, los módulos Cortafuegos, PatchManager y PolicyManager se habilitarán después de la correcta activación. Hasta ese momento solo estarán disponibles las funciones de G DATA Antivirus Business.

### 13.1.3. MailSecurity para Exchange

#### 13.1.3.1. MailSecurity y Exchange Server 2007

Si actualiza MailSecurity para Exchange en Microsoft Exchange Server 2007, Es necesario que esté presente en el sistema .NET Framework 3.5 o superior. Si Microsoft .NET Framework 3.5 o superior no está disponible, GDVSService fallará al iniciar tras la actualización efectuada. Con la instalación de Microsoft .NET Framework 3.5 o superior antes de actualizar MailSecurity para Exchange asegurará una completa funcionalidad.

#### 13.1.3.2. Actualizar a la versión 12

Debido a cambios en el procedimiento de instalación, las instalaciones de MailSecurity para Exchange que fueron implementadas inicialmente en la versión 12 no podrán actualizarse a la versión 14, incluso si se han actualizado previamente a la versión 13.0 o 13.1. En este caso, la versión previa de MailSecurity para Exchange deberá ser desinstalada antes de instalar la versión 14. Adicionalmente, debe asegurarse que MailSecurity para Exchange se instala en todos los servidores de Exchange que estén ejecutando los roles de transporte Hub o de Mailbox.

#### 13.1.3.3. MailSecurity, Servidor Exchange 2000 y AVM Ken!

Si usa AVM Ken! y desea instalar G DATA MailSecurity en el mismo ordenador que el servidor Ken!, diríjase por favor a nuestro **equipo de soporte** para obtener información detallada.

Si usa el Servidor Exchange 2000 y desea instalar G DATA MailSecurity en el mismo ordenador que el Servidor Exchange, o si quiere modificar los puertos para los correos entrantes y salientes al Servidor Exchange, diríjase por favor a nuestro **equipo de soporte** para obtener información detallada.

#### 13.1.3.4. Instalación en una red con varios controladores de dominio

Si se instala MailSecurity para Exchange en una red con varios controladores de dominio de Directorio Activo, el asistente de instalación requerirá que la herramienta Repadmin.exe esté presente en el sistema. Repadmin.exe es disponible como parte del rol de servicios de dominio del directorio activo, el rol de servicios de directorio ligero de directorio activo, y las herramientas de servicio de directorio activo de dominio (Herramientas de administración remota del servidor). Antes de iniciar el asistente de instalación de MailSecurity para Exchange, cerciórese de que alguno o varios de estos componentes estén presentes.

## 13.2. Mensajes de error

### 13.2.1. Cliente: "Los archivos de programa han sido modificados o están dañados"

Para garantizar una protección óptima frente a los virus, los archivos de programa se revisan con regularidad para verificar su integridad. Si se detecta algún error, se añade el informe **Los archivos de programa han sido modificados o están dañados**. Borre el informe y cargue la actualización más reciente de los archivos de programa G DATA Security Client de nuestro servidor de actualizaciones. A continuación, actualice los archivos de programa en los clientes afectados. Póngase en contacto con **nuestro equipo de soporte**, si aparece de nuevo el informe de error.

### 13.2.2. Cliente: "La base de datos de virus está dañada."

Para garantizar una protección óptima frente a los virus, la base de datos de virus se revisa con regularidad para verificar su integridad. Si se detecta algún fallo, se añade el informe **La base de datos de virus está dañada**. Borre el informe y cargue la actualización más reciente de la base de datos de virus de nuestro servidor de actualizaciones. A continuación, actualice la base de datos de virus en los clientes afectados. Póngase en contacto con **nuestro equipo de soporte**, si aparece de nuevo el informe de error.

### 13.2.3. "Para instalar G Data MailSecurity se necesita, como mínimo, Microsoft Exchange Server 2007 SP1."

Si le aparece el mensaje de error "Para instalar G DATA MailSecurity se necesita, como mínimo, Microsoft Exchange Server 2007 SP1", significa que no se cumplen los requisitos mínimos para

instalar el plugin para Exchange de G DATA MailSecurity. Para instalar G DATA MailSecurity se necesita como mínimo Microsoft Exchange Server 2007 SP1. Tiene que instalarse antes que G DATA MailSecurity. Para más información consulte **Instalación** y **Requisitos del sistema**.

# 13.3. Clientes Linux

## 13.3.1. Instalación

La instalación de G DATA Security Client para Linux y G DATA Security Client para Mac utiliza un repositorio localizado en el ManagementServer. Si se implementa un cliente de Linux o un cliente de Mac, los archivos binarios requeridos serán copiados desde el repositorio de ManagmentServer al cliente. Si estos archivos no están disponibles en este repositorio, se descargarán desde los servidores de actualización de G DATA, y se añadirán al repositorio de ManagementServer y posteriormente implementados en el cliente.

## 13.3.2. Procesos en segundo plano

Para comprobar si los procesos de G DATA Security Client para Linux están en ejecución, introduzca lo siguiente en una ventana del terminal:

linux:~# *ps ax|grep av*

Deberán mostrarse las siguientes salidas:

/usr/local/sbin/gdavserver
/usr/local/sbin/gdavclientd

Los procesos pueden ser iniciados introduciendo con los siguientes comandos:

linux:~# */etc/init.d/gdavserver start*
linux:~# */etc/init.d/gdavclient start*

y detenerlos con:

linux:~# */etc/init.d/gdavserver stop*
linux:~# */etc/init.d/gdavclient stop*

Para ello es indispensable tener permisos "root".

## 13.3.3. Archivos de registro (Logs)

Las instalaciones remotas de G DATA Security Client para Linux están registradas en /var/log/gdata_install.log. Los registros de información y errores del proceso gdavclientd están en /var/log/gdata/avclient.log. Los registros de información y errores del proceso gdavserver en /var/log/gdata/gdavserver.log, el cual es de utilidad para la resolver problemas de conexión con G DATA ManagementServer.

> Si desea ver varios mensajes, puede ajustar previamente en los archivos de configuración /etc/gdata/gdav.ini y etc/gdata/avclient.cfg la entrada *LogLevel*con el valor 7. (Si no existe es deberá crearlo manualmente). Atención: un alto nivel de registro produce muchos mensajes, con lo que aumentan rápidamente los archivos de registro (log). ¡Establezca siempre el nivel de registro en un nivel bajo!

### 13.3.4. Prueba de conexión con el servidor

Utilice la línea de comando gdavclientc para comprobar el funcionamiento del servidor de exploración gdavserver. Mediante los comandos *baseinfo* y *coreinfo* se puede obtener información de versión. Para ejecutar una prueba de exploración de virus, ejecute el comando: *scan<path>*. Para más información, consulte la sección gdavclientc.

### 13.3.5. Conexión con G DATA ManagementServer

La conexión con G DATA ManagementServer está configurada en /etc/gdata/avclient.cfg. Compruebe si la dirección IP de G DATA ManagementServer está introducida correctamente. De lo contrario, borre la información incorrecta e introduzca directamente la dirección IP correcta de G DATA ManagementServer o vuelva a activar el cliente para Linux desde G DATA Administrator.

## 13.4. Otros

### 13.4.1. ¿Cómo puedo comprobar si los clientes tienen una conexión con el G DATA MANAGEMENTSERVER?

La columna **Último acceso** en el área resumen de **Clientes** contiene la fecha en la que el cliente se conectó por última vez con G DATA ManagementServer. Con el ajuste estándar, los clientes contactan con el G DATA ManagementServer cada cinco minutos (si no se están ejecutando órdenes de escaneo en ese momento). Una conexión fallida puede deberse a las siguientes causas:

- El cliente está desactivado o no está conectado a la red.
- No se puede establecer ninguna conexión TCP/IP entre el cliente y el G DATA ManagementServer. Compruebe los ajustes de la red y las autorizaciones de puerto.
- El cliente no puede determinar la dirección IP del servidor, (p. ej. la resolución de nombres DNS no funciona). La conexión se puede comprobar con el comando telnet desde la línea de comandos. En el servidor el puerto TCP 7161 tiene que estar disponible, en el cliente los puertos TCP 7167 o TCP 7169 deben estar disponibles. Compruebe la conexión con el comando *telnet <NOMBRE DEL SERVIDOR> <NÚMERO DE PUERTO>*

  Tenga en cuenta que en Windows Vista, Windows 7 y Server 2008 (R2), el comando telnet no está disponible por defecto. Por ello, active la función de Windows correspondiente o bien agréguela como función nueva. Si la conexión del cliente con el servidor está intacta, en el indicador de comandos aparece una colección de símbolos crípticos. Si la conexión del servidor con el cliente está intacta, aparece una ventana de entrada vacía.

### 13.4.2. Mi buzón ha sido puesto en cuarentena

Esto ocurre si en el buzón hay un correo infectado. Para recuperar el archivo, cierre el programa de correo en el cliente afectado y, si ha creado un archivo nuevo, bórrelo. A continuación, abra el informe correspondiente con el G DATA Administrator y haga clic en **Cuarentena: Restaurar**. Póngase en contacto con nuestro equipo de soporte si no funciona la restauración del archivo.

### 13.4.3. Conectar con ManagementServer mediante IP

En la instalación se pregunta por el nombre del servidor. Pero el nombre del servidor puede sustituirse por la dirección IP, en caso de que la conexión al ManagementServer sea solamente mediante una dirección IP en vez de serlo mediante el nombre de servidor. También se puede sustituir con posterioridad el nombre del servidor por la dirección IP una vez que G DATA ManagementServer esté instalado. Para ello, edite el archivo Config.xml (Situado en la instalación del directorio de G DATA

ManagementServer) y cambie el valor de MainMMS por el de la dirección IP.

Para poder establecer la conexión del servidor a los clientes también mediante la dirección IP, los clientes tienen que haber sido activados en G DATA Administrator con su dirección IP. Esto se puede hacer manualmente o con la **sincronización de Active Directory**. Cuando los clientes se instalen directamente desde un medio de instalación, el programa de instalación preguntará tanto el nombre del servidor como el del ordenador. Introduzca la dirección IP correspondiente.

## 13.4.4. Ubicaciones de almacenamiento y rutas

Firmas de virus de G DATA Security Client

- Windows XP / Server 2003 / Server 2003 R2: C:\Archivos de programa\Common files\G DATA \AVKScanP\BD o G DATA
- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\Archivos de programa (x86)\Common Files\G DATA\AVKScanP\BD o G DATA

Firmas de virus de G DATA ManagementServer

- Windows Server 2003 / Server 2003 R2: C:\Documents and settings\Todos los usuarios \Application Data\G DATA\AntiVirus ManagementServer\Updates
- Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Server 2008 / Server 2008 R2 / Server 2012 / Server 2012 R2: C:\ProgramData\G DATA\AntiVirus ManagementServer \Updates

G DATA Security Client - Cuarentena

- Windows XP / Server 2003 / Server 2003 R2: C:\Archivos de programa\Todos los usuarios \Application Data\G DATA\AntiVirusKit Client \Quarantine
- Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Server 2008 / Server 2008 R2 / Server 2012 / Server 2012 R2: C:\ProgramData\G DATA\AntiVirusKit Client \Quarantine

G DATA ManagementServer - Cuarentena

- Windows Server 2003 / Server 2003 R2: C:\Archivos de programa\Todos los usuarios\Application Data\G DATA\AntiVirus ManagementServer\Quarantine
- Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Server 2008 / Server 2008 R2 / Server 2012 / Server 2012 R2: C:\ProgramData\G DATA\AntiVirus ManagementServer \Quarantine

Bases de datos G DATA ManagementServer

Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Server 2003 / Server 2003 R2 / Server 2008 / Server 2008 R2 / Server 2012 / Server 2012 R2:

- C:\Archivos de programa (x86)\Microsoft SQL Server\MSSQL12.GDATA2014\MSSQL\Data \GDATA_AntiVirus_ManagementServer_*.mdf
- C:\Archivos de programa (x86)\Microsoft SQL Server\MSSQL12.GDATA2014\MSSQL\Data \GDATA_AntiVirus_ManagementServer_log_*.ldf

## 13.4.5. ¿Cómo se activa un certificado de servidor SSL en IIS 7 o 7.5?

Para facilitar una comunicación segura entre los clientes y WebAdministrator / MobileAdministrator, se recomienda activar un certificado de servidor SSL en Internet Information Services (IIS).

Para activar un certificado de servidor SSL en IIS 7 y 7.5 (Windows Vista/Windows Server 2008 y superior), abra el **Administrador de Internet Information Services (IIS)**. Si usa Windows Server 2008, podrá encontrar el administrador IIS en **Inicio** > **Todos los programas** > **Herramientas administrativas**. Otra alternativa es hacer clic en **Inicio** > **Ejecutar** e introducir el comando *inetmgr*. Este comando se puede utilizar también en los ordenadores con Windows 7.

Seleccione su servidor en **Conexiones**. Seleccione luego la categoría **IIS** y haga doble clic en **Certificados de servidor**. Pulse ahora **Crear certificado autofirmado**. Después de introducir un nombre para el certificado, este se genera y se muestra en el resumen de certificados de servidor. Tenga en cuenta que la fecha estándar de expiración para el certificado es exactamente de un año.

Para emplear el certificado para la comunicación, seleccione la página correspondiente en el área de **Conexiones**. En el área **Acciones** en el lado derecho se pueden seleccionar ahora **Enlaces**. Haga clic en **Agregar** para establecer un nuevo enlace. En **Tipo** seleccione https en el menú desplegable y en **Certificado SSL**, el certificado que definió antes. Haga clic en **Aceptar** para cerrar el enlace.

El acceso a WebAdministrator y a MobileAdministrator mediante una conexión segura se puede realizar ahora sustituyendo el prefijo *http://*en el navegador por *https://*, por ej. *https://nombre del servidor/gdadmin*. Como ha creado usted mismo su certificado, puede ser que el navegador muestre un aviso antes de permitirle abrir WebAdministrator o MobileAdministrator. No obstante, la comunicación con el servidor está totalmente encriptada.

## 13.4.6. ¿Cómo se activa un certificado de servidor SSL en IIS 5 o 6?

Para facilitar una comunicación segura entre los clientes y WebAdministrator / MobileAdministrator, se recomienda activar un certificado de servidor SSL en Internet Information Services (IIS).

Para activar un certificado de servidor SSL en IIS 5 (Windows XP) o IIS 6 (Windows Server 2003), emplee la herramienta de Microsoft SelfSSL que se puede encontrar en las herramientas del kit de recursos IIS 6.0 (se puede descargar gratuitamente en la **página web de Microsoft**). Si ejecuta aquí el tipo de setup personalizado, podrá elegir las herramientas que desea instalar. Elija **SelfSSL 1.0**. Después de la instalación, abra la línea de comandos de SelfSSL en **Inicio** > **Programas** > **Recursos IIS** > **SelfSSL**.

Con una sola entrada podrá generar ahora un certificado autofirmado para su página Web. Escriba *selfssl /N:CN=localhost /K:2048 /V:365 /S:1 /T* y pulse luego **Intro**. Confirme la generación del certificado pulsando la tecla S. Ahora se genera un certificado para la página IIS estándar en su servidor local y el localhost se agrega a la lista de los certificados de confianza. La longitud de la clave es de 2048 caracteres y tiene una validez de 365 días exactamente. Si su página no es la página IIS estándar en su servidor local, puede determinar la página correspondiente en su servidor en **Inicio** > **Programas** > **Administración** > **Administrador de Internet Information Services (IIS)** y modificar el parámetro */S:1*como corresponda.

El acceso a WebAdministrator y a MobileAdministrator mediante una conexión segura se puede realizar ahora sustituyendo el prefijo *http://*en el navegador por *https://*, por ej. https://nombre del servidor/gdadmin. Como ha creado usted mismo su certificado, puede ser que el navegador muestre un aviso antes de permitirle abrir WebAdministrator o MobileAdministrator. No obstante, la comunicación con el servidor está totalmente encriptada.

# 14. Licencias



**SharpSerializer**



**Json.NET**



**DotNetZip**

exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

**PhoneNumbers.dll / PushSharp**

PhoneNumbers.dll and PushSharp are distributed under the Apache License 2.0 (www.apache.org/licenses).

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by

applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

# Índice