

# Bitdefender®

## GravityZone



GUÍA DE INSTALACIÓN

## Bitdefender GravityZone Guía de Instalación

fecha de publicación 2019.08.22

Copyright© 2019 Bitdefender

### Advertencia legal

**Todos los derechos reservados.** Ninguna parte de este libro puede ser reproducida o transmitida de forma alguna, ni por ningún medio, electrónico o mecánico, incluyendo fotocopia, grabación o mediante un sistema de almacenamiento y recuperación, sin la autorización previa por escrito de un representante de Bitdefender. La inclusión de breves citas de reseñas se puede hacer sólo con la mención de la fuente citada. El contenido no puede ser modificado en forma alguna.

**Advertencia y Renuncia de Responsabilidad.** Este producto y su documentación están protegidos por los derechos de autor. La información en este documento se proporciona "tal cual", sin garantía. Aunque se han tomado todas las precauciones durante la preparación de este documento, los autores no tendrán responsabilidad alguna ante ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en el mismo.

Este documento contiene enlaces a sitios web de terceros que no están bajo el control de Bitdefender, por lo que Bitdefender no se hace responsable por el contenido de ningún sitio enlazado. Si usted accede a sitios web de terceros listados en este documento, lo hará bajo su responsabilidad. Bitdefender proporciona estos vínculos solamente para su conveniencia, y la inclusión del enlace no implica la aprobación por parte de Bitdefender o aceptar responsabilidad alguna sobre el contenido del sitio de terceros.

**Marcas Registradas.** En este documento pueden aparecer nombres de marcas registradas. Todas las marcas registradas y no registradas, en este documento, son propiedad exclusiva de sus respectivos propietarios, y respectivamente reconocidas.

# Tabla de contenidos

Prólogo .....	v
1. Convenciones utilizadas en esta guía .....	v
1. Acerca de GravityZone .....	1
2. Capas de protección de GravityZone .....	2
2.1. Antimalware .....	2
2.2. Control avanzado de amenazas .....	3
2.3. Antiexploit avanzado .....	4
2.4. Cortafuego .....	4
2.5. Control de Contenido .....	4
2.6. Administración de parches .....	4
2.7. Control de dispositivos .....	5
2.8. Cifrado completo del disco duro .....	5
2.9. Análisis de riesgos en endpoints (ERA) .....	5
2.10. Disponibilidad de capas de protección de GravityZone .....	6
3. Architecture GravityZone .....	7
3.1. Consola web (GravityZone Control Center) .....	7
3.2. Agentes de seguridad .....	7
3.2.1. Bitdefender Endpoint Security Tools .....	7
3.2.2. Bitdefender Endpoint Security Tools for Windows Legacy .....	9
3.2.3. Endpoint Security for Mac .....	10
4. Requisitos .....	11
4.1. Control Center .....	11
4.2. Protección de endpoint .....	11
4.2.1. Hardware .....	12
4.2.2. Sistemas operativos soportados .....	15
4.2.3. Sistemas de archivo compatibles .....	20
4.2.4. Navegadores soportados .....	21
4.2.5. Uso de tráfico .....	21
4.3. Cifrado completo del disco duro .....	23
4.4. Puertos de comunicación de GravityZone .....	25
5. Instalación de la protección .....	26
5.1. Administración de Licencias .....	26
5.1.1. Encontrar un reseller .....	26
5.1.2. Activación de su licencia .....	27
5.1.3. Comprobar los detalles de licencia actuales .....	28
5.2. Instalación de los agentes de seguridad .....	28
5.2.1. Preparándose para la Instalación .....	29
5.2.2. Instalación local .....	31
5.2.3. Instalación remota .....	39
5.2.4. Preparación de sistemas Linux para el análisis on-access .....	45
5.2.5. Cómo funciona la detección de red .....	47
5.3. Instalación del Cifrado de disco completo .....	50

5.4. Administrador de Credenciales .....	51
5.4.1. Añadir credenciales al Gestor de credenciales .....	51
5.4.2. Eliminación de credenciales del Gestor de credenciales .....	53
6. Integraciones .....	54
6.1. Integración con Amazon EC2 .....	54
7. Desinstalación de la protección en endpoints .....	55
8. Obtener Ayuda .....	58
8.1. Centro de soporte de Bitdefender .....	58
8.2. Solicitar ayuda .....	60
8.3. Usar la herramienta de soporte .....	60
8.3.1. Uso de la herramienta de soporte en sistemas operativos Windows .....	60
8.3.2. Uso de la herramienta de soporte en sistemas operativos Linux .....	62
8.3.3. Uso de la herramienta de soporte en sistemas operativos Mac .....	64
8.4. Información de contacto .....	65
8.4.1. Direcciones .....	65
8.4.2. Distribuidor Local .....	65
8.4.3. Oficinas de Bitdefender .....	66
A. Apéndices .....	69
A.1. Tipos de archivo compatibles .....	69

## Prólogo

Esta guía va dirigida a los administradores de TI encargados de implementar la protección de GravityZone en las instalaciones de su organización. Los administradores de TI en busca de información sobre GravityZone pueden encontrar en esta guía los requisitos de GravityZone y los módulos de protección disponibles.

Este documento se dedica a explicar cómo implementar los agentes de seguridad de Bitdefender en todo tipo de endpoints de su empresa, así como la forma de configurar la solución GravityZone.

## 1. Convenciones utilizadas en esta guía

### Convenciones Tipográficas

Esta guía recurre a varios estilos de texto para mejorar su lectura. La siguiente tabla le informa sobre dichos estilos y su significado.

Apariencia	Descripción
ejemplo	Los nombres de comandos en línea y sintaxis, rutas y nombres de archivos, configuración, salidas de archivos y texto de entrada se muestran en caracteres de espacio fijo.
<a href="http://www.bitdefender.com">http://www.bitdefender.com</a>	Los enlaces URL le dirigen a alguna localización externa, en servidores http o ftp.
<a href="mailto:gravityzone-docs@bitdefender.com">gravityzone-docs@bitdefender.com</a>	Las direcciones de e-mail se incluyen en el texto como información de contacto.
"Prólogo" (p. v)	Este es un enlace interno, hacia alguna localización dentro del documento.
opción	Todas las opciones del producto se muestran utilizando caracteres en <b>negrita</b> .
palabra clave	Las opciones de interfaz, palabras clave o accesos directos se destacan mediante caracteres en <b>negrita</b> .

## Admoniciones

Las advertencias son notas dentro del texto, marcadas gráficamente, que le facilitan información adicional relacionada con el párrafo que está leyendo.



### **Nota**

La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.



### **Importante**

Esta requiere su atención y no es recomendable saltársela. Normalmente proporciona información importante aunque no extremadamente crítica.



### **Aviso**

Se trata de información crítica que debería tratar con extrema cautela. Nada malo ocurrirá si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente peligroso.

## 1. ACERCA DE GRAVITYZONE

GravityZone es una solución de seguridad empresarial diseñada desde cero para la virtualización y la nube, con el fin de ofrecer servicios de seguridad a endpoints físicos y máquinas virtuales en la nube privada y pública.

GravityZone es un producto con una consola de administración unificada disponible en la nube, alojada por Bitdefender, o como appliance virtual que se aloja en las instalaciones de la organización, y proporciona un único punto para la implementación, aplicación y administración de las políticas de seguridad para cualquier número de endpoints de cualquier tipo y en cualquier ubicación.

GravityZone aporta múltiples capas de seguridad para endpoints: antimalware con monitorización del comportamiento, protección contra amenazas de día cero, inclusión de aplicaciones en la lista negra y entorno de pruebas, cortafuego, control de dispositivos y control de contenidos.

## 2. CAPAS DE PROTECCIÓN DE GRAVITYZONE

GravityZone proporciona las siguientes capas de protección:

- Antimalware
- Control avanzado de amenazas
- Antiexploit avanzado
- Cortafuego
- Control de Contenido
- Administración de parches
- Control de dispositivos
- Cifrado completo del disco duro
- Análisis de riesgos en endpoints (ERA)

### 2.1. Antimalware

La capa de protección antimalware se basa en el análisis de firmas y en el análisis heurístico (B-HAVE, ATC) contra virus, gusanos, troyanos, spyware, adware, keyloggers, rootkits y otros tipos de software malicioso.

La tecnología de análisis antimalware de Bitdefender se basa en las siguientes tecnologías:

- Primero, se utiliza un método de análisis tradicional donde el contenido analizado se compara con la base de datos de firmas. La base de datos de firmas contiene patrones de bytes específicos para conocer los peligros y se actualiza regularmente por Bitdefender. Este método de análisis es efectivo contra amenazas confirmadas que han sido descubiertas y documentadas. Sin embargo, no importa lo rápidamente que se actualice la base de datos de firmas, siempre hay una ventana de tiempo vulnerable entre que la amenaza es descubierta y una solución es lanzada.
- Contra las amenazas de nueva generación indocumentadas, una segunda capa de protección facilitada por **B-HAVE**, un motor heurístico de Bitdefender. Los algoritmos heurísticos detectan el malware en función de las características de su comportamiento. B-HAVE ejecuta los archivos sospechosos en un entorno virtual para analizar su impacto en el sistema y asegurarse de que no supongan una amenaza. Si se detecta una amenaza, el programa está prevenido de ejecutarlo.



## Motores de análisis

Bitdefender GravityZone puede configurar automáticamente los motores de análisis al crear los paquetes de agentes de seguridad según la configuración del endpoint.

El administrador también puede personalizar los motores de análisis, pudiendo elegir entre varias tecnologías de análisis:

1. **Análisis local**, cuando el análisis se realiza localmente en el endpoint. El modo de análisis local es adecuado para máquinas potentes, con los contenidos de seguridad almacenados localmente.
2. **Análisis híbrido con motores ligeros (nube pública)**, con una huella media, que utiliza el análisis en la nube y, parcialmente, los contenidos de seguridad locales. Este modo de análisis conlleva el beneficio de un menor consumo de recursos, aunque implica el análisis fuera de las instalaciones.
3. **Análisis centralizado en la nube pública o privada**, con una huella reducida que requiere un Security Server para el análisis. En este caso, el conjunto de contenidos de seguridad no se almacena localmente y el análisis se descarga en el Security Server.



### Nota

Existe un reducido conjunto de motores almacenados localmente, necesarios para descomprimir los archivos comprimidos.

4. **Análisis centralizado (análisis en nube pública o privada con Security Server) con reserva\* en análisis local (motores completos)**
5. **Análisis centralizado (análisis en nube pública o privada con Security Server) con reserva\* en análisis híbrido (nube pública con motores ligeros)**

## 2.2. Control avanzado de amenazas

Para las amenazas que logran eludir incluso el motor heurístico, existe otra capa de seguridad denominada Advanced Threat Control (ATC).

Advanced Threat Control monitoriza continuamente los procesos en ejecución y detecta las conductas sospechosas, como por ejemplo los intentos de ocultar el tipo de proceso, ejecutar código en el espacio de otro proceso (secuestro de memoria del proceso para escalado de privilegios), replicar, descartar archivos, ocultarse a las aplicaciones de listado de procesos, etc. Cada comportamiento

sospechoso aumenta la calificación del proceso. Cuando se alcanza un límite, salta la alarma.

## 2.3. Antiexploit avanzado

El Antiexploit avanzado, basado en el aprendizaje automático, es una nueva tecnología proactiva que detiene los ataques de día cero canalizados a través de exploits evasivos. El Antiexploit avanzado ataja los últimos exploits en tiempo real y mitiga las vulnerabilidades de corrupción de memoria que pueden eludir otras soluciones de seguridad. Protege las aplicaciones más habituales, como por ejemplo navegadores, Microsoft Office o Adobe Reader, así como otras que pueda imaginar. Vigila los procesos del sistema y protege contra las violaciones de la seguridad y el secuestro de procesos existentes.

## 2.4. Cortafuego

El Cortafuego controla el acceso de las aplicaciones a la red y a Internet. Se permite automáticamente el acceso a una amplia base de datos de aplicaciones legítimas y conocidas. Más aun, el cortafuegos puede proteger el sistema contra escaneo de puertos, restringir ICS y avisar cuando se conecten a la red Wi-Fi nuevos nodos.

## 2.5. Control de Contenido

El módulo de Control de contenidos ayuda a hacer cumplir las políticas de la empresa para el tráfico permitido, el acceso Web, la protección de datos y el control de aplicaciones. Los administradores pueden definir las opciones de análisis de tráfico y las exclusiones, programar el acceso Web bloqueando o permitiendo ciertas categorías Web o URLs, configurar las reglas de protección de datos y definir permisos para el uso de aplicaciones concretas.

## 2.6. Administración de parches

La Administración de parches, que está completamente integrada en GravityZone, mantiene actualizados los sistemas operativos y las aplicaciones de software al tiempo que proporciona visibilidad completa del estado de los parches en los endpoints administrados de Windows.

El módulo de Administración de parches de GravityZone incluye varias características, como análisis de parches bajo demanda o programados, aplicación manual o automática de parches o informes de los parches que faltan.

Puede obtener más información sobre los proveedores y productos compatibles con la Administración de parches de GravityZone en este [artículo de la base de conocimientos](#).



### Nota

La Administración de parches es un complemento disponible con una clave de licencia independiente para todos los paquetes de GravityZone existentes.

## 2.7. Control de dispositivos

El módulo de control de dispositivos permite evitar la fuga de datos confidenciales y las infecciones de malware a través de dispositivos externos conectados a los endpoints. Para ello, aplica políticas con reglas de bloqueo y excepciones a una amplia gama de tipos de dispositivos (como por ejemplo unidades flash USB, dispositivos Bluetooth, reproductores de CD/DVD, dispositivos de almacenamiento, etc.).

## 2.8. Cifrado completo del disco duro

Esta capa de protección le permite proporcionar un cifrado de disco completo en los endpoints, mediante la administración de BitLocker en Windows y FileVault y diskutil en macOS. Puede cifrar y descifrar los volúmenes, ya sean de arranque o no, con unos pocos clics, mientras que GravityZone gestiona todo el proceso con una mínima intervención de los usuarios. Además, GravityZone almacena las claves de recuperación necesarias para desbloquear los volúmenes cuando los usuarios olvidan sus contraseñas.

## 2.9. Análisis de riesgos en endpoints (ERA)

La Análisis de riesgos en endpoints (ERA, por sus siglas en inglés) identifica, evalúa y repara las debilidades de los endpoints de Windows a través de análisis de riesgos para la seguridad (bajo demanda o según programación mediante política) teniendo en cuenta un gran número de indicadores de riesgo. Una vez que haya analizado su red buscando ciertos indicadores de riesgo, obtendrá una visión de conjunto del estado de su red en cuanto al riesgo mediante el panel de control de **Administración de riesgos**, disponible en el menú principal. Podrá resolver ciertos riesgos de seguridad automáticamente desde GravityZone Control Center y ver las recomendaciones para mitigar la exposición de los endpoints.

## 2.10. Disponibilidad de capas de protección de GravityZone

La disponibilidad de las capas de protección de GravityZone difiere según el sistema operativo del endpoint. Para obtener más información, consulte el artículo de la base de conocimientos [Disponibilidad de capas de protección de GravityZone](#).

## 3. ARCHITECTURE GRAVITYZONE

La solución de GravityZone incluye los siguientes componentes:

- [Consola Web Control Center](#)
- [Agentes de seguridad](#)

### 3.1. Consola web (GravityZone Control Center)

Las soluciones de seguridad de Bitdefender se gestionan en GravityZone desde un único punto de administración, la consola Web Control Center, que facilita el acceso y la administración de la estrategia general de seguridad, las amenazas a la seguridad global, y el control sobre todos los módulos de seguridad que protegen a los equipos de escritorio virtuales o físicos y a los servidores. Equipado con la Arquitectura Gravity, Control Center es capaz de abordar las necesidades de incluso las organizaciones más grandes.

Control Center, una interfaz basada en Web, se integra con los sistemas de monitorización y administración existentes para aplicar fácilmente el sistema de protección a las estaciones de trabajo y servidores no administrados.

### 3.2. Agentes de seguridad

Para proteger su red con Bitdefender, debe instalar los agentes de seguridad de GravityZone apropiados en los endpoints de la red.

- [Bitdefender Endpoint Security Tools](#)
- [Bitdefender Endpoint Security Tools for Windows Legacy](#)
- [Endpoint Security for Mac](#)

#### 3.2.1. Bitdefender Endpoint Security Tools

GravityZone garantiza la protección de máquinas físicas y virtuales en Windows y Linux con Bitdefender Endpoint Security Tools, un agente de seguridad inteligente sensible al entorno que se adapta al tipo de endpoint. Bitdefender Endpoint Security Tools se puede implementar en cualquier máquina, ya sea virtual o física, y proporciona un sistema de análisis flexible que constituye una solución ideal para entornos mixtos (físicos, virtuales y en la nube).

Bitdefender Endpoint Security Tools utiliza una sola plantilla de política para las máquinas físicas y virtuales y una fuente de kit de instalación para cualquier entorno (físico o virtual) que ejecute las versiones actuales de Windows. Se instala un kit

independiente en las versiones antiguas de Windows. Para más información, consulte [BEST for Windows Legacy](#).

## Capas de protección

Con Bitdefender Endpoint Security Tools hay disponibles las siguientes capas de protección:

- [Antimalware](#)
- [Control avanzado de amenazas](#)
- [Cortafuego](#)
- [Control de Contenido](#)
- [Administración de parches](#)
- [Control de dispositivos](#)
- [Cifrado completo del disco duro](#)
- [Análisis de riesgos en endpoints \(ERA\)](#)

## Roles de endpoint

- [Usuario con Permisos](#)
- [Relay](#)
- [Servidor de almacenamiento en caché de parches](#)

### Usuario con Permisos

Los administradores del Control Center pueden conceder privilegios de Usuario avanzado a los usuarios de endpoints mediante los ajustes de políticas. El módulo de Usuario avanzado otorga privilegios de administración a nivel de usuario, lo que permite al usuario del endpoint acceder a los ajustes de seguridad y modificarlos a través de una consola local. Control Center recibe una notificación cuando un endpoint está en modo de Usuario avanzado y el administrador de Control Center siempre puede sobrescribir los ajustes de seguridad locales.



### Importante

Este módulo solo está disponible para sistemas operativos soportados de servidor y equipos de escritorio Windows. Para más información, diríjase a [“Sistemas operativos soportados”](#) (p. 15).

### Relay

Los agentes de endpoint con rol de Bitdefender Endpoint Security Tools Relay actúan como servidores de comunicaciones, de actualizaciones y proxy para otros

endpoints de la red. Los agentes de endpoint con rol de relay son especialmente necesarios en organizaciones con redes aisladas, donde todo el tráfico se canaliza a través de un único punto de acceso.

En las empresas con redes distribuidas, los agentes de relay ayudan a reducir el uso de ancho de banda, al evitar que los endpoints protegidos se conecten directamente a GravityZone.

Una vez que se instala un agente Bitdefender Endpoint Security Tools Relay en la red, se pueden configurar otros endpoints mediante política para comunicarse con Control Center a través del agente de relay.

Los agentes Bitdefender Endpoint Security Tools Relay sirven para lo siguiente:

- Detección de todos los endpoints desprotegidos de la red.  
Esta funcionalidad es esencial para la implementación del agente de seguridad en un entorno de GravityZone en la nube.
- Implementación del agente de endpoint dentro de la red local.
- Actualización de los endpoints protegidos de la red.
- Garantía de la comunicación entre Control Center y los endpoints conectados.
- Funcionamiento como servidor proxy para endpoints protegidos.
- Optimización del tráfico de red durante las actualizaciones, implementaciones, análisis y otras tareas que consumen recursos.

### Servidor de almacenamiento en caché de parches

Los endpoints con rol de relay también pueden actuar como servidor de almacenamiento en caché de parches. Con este rol habilitado, los relays sirven para almacenar parches de software descargados de los sitios web del proveedor y distribuirlos a los endpoints objetivo de su red. Cuando un endpoint conectado tiene software al que le falten parches, los obtiene del servidor y no del sitio web del proveedor, lo que optimiza el tráfico generado y la carga del ancho de banda de la red.



#### Importante

Este rol adicional está disponible registrando un complemento de Administración de parches.

### 3.2.2. Bitdefender Endpoint Security Tools for Windows Legacy

A medida que avanzan las tecnologías de seguridad, algunas características de Bitdefender Endpoint Security Tools ya no son compatibles con las versiones

anteriores de Windows. Bitdefender Endpoint Security Tools for Windows Legacy es un kit independiente diseñado para proteger estas versiones de Windows sin comprometer la seguridad de las actuales.

Bitdefender Endpoint Security Tools for Windows Legacy no se puede implementar a distancia desde la consola de GravityZone. Los administradores deben instalar el paquete BEST for Windows Legacy manualmente o utilizando una herramienta de terceros, como Microsoft SCCM.

## Capas de protección

Con Bitdefender Endpoint Security Tools for Windows Legacy hay disponibles las siguientes capas de protección:

- Antimalware
- Control avanzado de amenazas



### Importante

Advanced Threat Control no está disponible para Windows Server 2003.

## Roles de endpoint

- Protección de Exchange

Los roles de usuario avanzado y de relay no están disponibles con BEST for Windows Legacy.

## 3.2.3. Endpoint Security for Mac

Endpoint Security for Mac es un agente de seguridad diseñado para proteger estaciones de trabajo y portátiles Macintosh basados en Intel. La tecnología de análisis disponible es la de **Análisis local**, con contenidos de seguridad almacenados localmente.

## Capas de protección

Con Endpoint Security for Mac hay disponibles las siguientes capas de protección:

- Antimalware
- Control de Contenido
- Control de dispositivos
- Cifrado completo del disco duro



## 4. REQUISITOS

Todas las soluciones GravityZone se instalan y administran a través del Control Center.

### 4.1. Control Center

Para acceder a la consola web Control Center, es necesario lo siguiente:

- Internet Explorer 9 o superior, Mozilla Firefox 14 o superior, Google Chrome 15 o superior, Safari 5 o superior, Microsoft Edge 20 o superior, Opera 16 o superior
- Resolución de pantalla recomendada: 1280 x 800 o superior



#### **Aviso**

Control Center no funcionará o se mostrará correctamente en Internet Explorer 9+ con la Vista de compatibilidad habilitada, que equivaldría a utilizar una versión de navegador no soportada.

### 4.2. Protección de endpoint

Para proteger su red con Bitdefender, debe instalar los agentes de seguridad de GravityZone en los endpoints de la red. A tal fin, necesita un usuario de Control Center con privilegios de administración sobre los servicios que precise instalar y sobre los endpoints de la red bajo su administración.

Los requisitos para el agente de seguridad son diferentes en función de si tiene roles de servidor adicionales, como por ejemplo Relay, Protección de Exchange o Servidor de almacenamiento en caché de parches. Para obtener más información sobre los roles de los agentes, consulte [“Agentes de seguridad” \(p. 7\)](#).

## 4.2.1. Hardware

### Agente de seguridad sin roles

#### Uso CPU

Sistemas objetivo	Tipo CPU	Sistemas operativos compatibles (SO)
Estaciones de trabajo	Procesador compatible Intel® Pentium a 1 GHz o más	Microsoft Windows XP SP3 32 bits y Windows XP SP2 64 bits
	Procesador compatible Intel® Pentium a 2 GHz o más	SO de escritorio Microsoft Windows, excepto Windows XP
	Intel® Core 2 Duo, 2 GHz o más	macOS
Dispositivos inteligentes	Procesador compatible Intel® Pentium a 800 MHz o más	SO integrados Microsoft Windows
Servidores	Mínimo: Procesador compatible Intel® Pentium a 2,4 GHz	SO Microsoft Windows Server y SO Linux
	Recomendado: CPU multinúcleo Intel® Xeon, 1,86 GHz o más	

12

### Memoria RAM libre

#### En la instalación (MB)

SO	MOTOR ÚNICO					
	Análisis local		Análisis híbrido		Análisis central.	
	Solo AV	Opc. complet.	Solo AV	Opc. complet.	Solo AV	Opc. complet.
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	n/a	n/a	n/a	n/a

#### Para el uso diario (MB)\*

SO	Antivirus (motor único)			Módulo de protección			
	Local	Híbrido	Centralizado	Análisis comportamiento	Cortafuego	Control contenidos	Usa...
Windows	75	55	30	+13	+17	+41	+2
Linux	200	180	90	-	-	-	-
macOS	300	-	-	-	-	-	-

\* Las cantidades cubren el uso diario de clientes de endpoint, sin tener en cuenta las tareas adicionales, como análisis bajo demanda o actualizaciones de productos.

## Espacio Libre en Disco

### En la instalación (MB)

SO	MOTOR ÚNICO						MOTOR DUAL			
	Análisis local		Análisis híbrido		Análisis central.		Análisis local + central.		Análisis híbrido + central.	
	Solo AV	Opc. complet.	Solo AV	Opc. complet.	Solo AV	Opc. complet.	Solo AV	Opc. complet.	Solo AV	Opc. complet.
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1300	1450	800	950	300	450	1300	1450	800	950
macOS	1024	1024	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

### Para el uso diario (MB)\*

SO	Antivirus (motor único)			Módulo de protección			
	Local	Híbrido	Centralizado	Análisis comportamiento	Cortafuego	Control contenidos	Usa...
Windows	410	190	140	+12	+5	+60	+8
Linux	500	200	110	-	-	-	-
macOS	1024	-	-	-	-	-	-

\* Las cantidades cubren el uso diario de clientes de endpoint, sin tener en cuenta las tareas adicionales, como análisis bajo demanda o actualizaciones de productos.

## Agente de seguridad con rol de Relay

El rol de Relay necesita recursos de hardware adicionales a la configuración básica del agente de seguridad. Estos requisitos se deben al Servidor de actualizaciones y a los paquetes de instalación alojados por el endpoint:

Número de endpoints conectados	CPU para el Servidor de actualizaciones	RAM	Espacio libre en disco para el Servidor de actualizaciones
1-300	Mínimo: Procesador Intel® Core™ i3 o equivalente, 2 vCPU por núcleo	1.0 GB	10 GB
300-1000	Mínimo: Procesador Intel® Core™ i5 o equivalente, 4 vCPU por núcleo	1.0 GB	10 GB



### Aviso

Los agentes de relay requieren discos SSD debido a la gran cantidad de operaciones de lectura y escritura.



### Importante

- Si desea guardar los paquetes de instalación y las actualizaciones en otra partición distinta a donde está instalado el agente, asegúrese de que ambas particiones tengan suficiente espacio libre en el disco (10 GB) pues, de lo contrario, el agente abortará la instalación. Esto solo es necesario en la instalación.
- En los endpoints de Windows, deben habilitarse los vínculos simbólicos local a local.

## Agente de seguridad con rol de Servidor de almacenamiento en caché de parches

El agente con el rol de Servidor de almacenamiento en caché de parches debe cumplir los siguientes requisitos acumulativos:

- Todos los requisitos de hardware del agente de seguridad simple (sin roles)

- Todos los requisitos de hardware del rol de Relay
- Además, 100 GB de espacio libre en el disco para almacenar los parches descargados

**Importante**

Si desea guardar los parches en otra partición distinta a donde está instalado el agente, asegúrese de que ambas particiones tengan suficiente espacio libre en el disco (100 GB) pues, de lo contrario, el agente abortará la instalación. Esto solo es necesario en la instalación.

## 4.2.2. Sistemas operativos soportados

### Equipo de escritorio de Windows

#### Soporte total

- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

#### Soporte limitado

En estos sistemas operativos, el agente de seguridad solo tiene antimalware y Advanced Threat Control. Usuario avanzado y relay no son compatibles.

- Windows Vista con Service Pack 1
- Windows XP con Service Pack 2 (64 bits)
- Windows XP con Service Pack 3 (32bit)

**Aviso**

Bitdefender no es compatible con las compilaciones del programa Windows Insider.

## Windows incorporado y de tablet

### Soporte total

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

### Soporte limitado

En estos sistemas operativos, el agente de seguridad solo admite antimalware y Advanced Threat Control. Usuario avanzado y relay no son compatibles.

- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded con Service Pack 2<sup>(1)</sup>
- Windows XP Tablet PC Edition<sup>(1)</sup>

**Aviso**

(1) Deben instalarse estos componentes concretos del sistema operativo integrado:

- Protocolo de red TCP/IP con Cliente para redes Microsoft
- Archivos binarios de soporte de base
- Administrador de filtros
- Soporte de caché de DNS
- Instalador de Windows
- Proveedor de Instalador de Windows WMI
- Servicio de estación de trabajo
- WinHTTP
- DLL de recursos de Windows XP Service Pack 2
- Inicio de sesión de Windows (estándar)
- Shell del explorador
- Formato NTFS

## Servidor Windows

### Soporte total

- Windows Server 2019
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

### Soporte limitado

En estos sistemas operativos, el agente de seguridad solo admite antimalware y Advanced Threat Control. Usuario avanzado y relay no son compatibles. Windows Server 2008 y Windows Small Business Server (SBS) 2008 también son compatibles con la Protección de Exchange.

- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows Small Business Server (SBS) 2008
- Windows Small Business Server (SBS) 2003
- Windows Home Server



#### Importante

Bitdefender Endpoint Security Tools es compatible con la tecnología Windows Server Failover Cluster (WSFC).

## Linux



#### Importante

Los endpoints de Linux utilizan puestos de licencia del grupo de licencias para sistemas operativos de servidor.

- Ubuntu 14.04 LTS o superior
- Red Hat Enterprise Linux / CentOS 6.0 o superior

- SUSE Linux Enterprise Server 11 SP4 o superior
- OpenSUSE Leap 42.x
- Fedora 25 o superior<sup>(1)</sup>
- Debian 8.0 o superior
- Oracle Linux 6.3 o superior
- Amazon Linux AMI 2016.09 o superior



### Aviso

(1) En Fedora 28, Bitdefender Endpoint Security Tools requiere la instalación manual del paquete `libnsl` mediante la ejecución del siguiente comando:

```
sudo dnf install libnsl -y
```

## Requisitos previos de Active Directory

Al integrar endpoints de Linux con un dominio de Active Directory a través del daemon de servicios de seguridad del sistema (SSSD), asegúrese de que la herramienta **ldbsearch** esté instalada.

## Compatibilidad para análisis on-access

El análisis on-access está disponible para todos los sistemas operativos guest soportados. En sistemas Linux, se proporciona soporte de análisis on-access en las siguientes situaciones:

Versiones del kernel	Distribuciones Linux	Requisitos on-access
2.6.38 o superior*	Red Hat Enterprise Linux / CentOS 6.0 o superior Ubuntu 14.04 o superior SUSE Linux Enterprise Server 11 SP4 o superior OpenSUSE Leap 42.x Fedora 25 o superior Debian 9.0 o superior Oracle Linux 6.3 o superior	<b>Fanotify</b> (opción del kernel) debe estar habilitado.





Versiones del kernel	Distribuciones Linux	Requisitos on-access
	Amazon Linux AMI 2016.09 o superior	
2.6.38 o superior	Debian 8	<p><b>Fanotify</b> debe estar habilitado y establecido en modo de aplicación obligatoria y, luego, hay que recompilar el paquete del kernel.</p> <p>Para más información, consulte <a href="#">este artículo de la base de conocimientos</a>.</p>
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender proporciona soporte mediante <b>DazukoFS</b> con módulos del kernel precompilados.
Todos los demás kernels	Todos los demás sistemas compatibles	El módulo <b>DazukoFS</b> debe compilarse manualmente. Para obtener más información, consulte <a href="#">"Compilación manual del módulo DazukoFS"</a> (p. 45).

\* Con ciertas limitaciones descritas más adelante.

## Limitaciones de análisis on-access


Versiones del kernel	Distribuciones Linux	Detalles
2.6.38 o superior	Todos los sistemas compatibles	<p>El análisis on-access solo monitoriza los recursos compartidos montados bajo las siguientes condiciones:</p> <ul style="list-style-type: none"> <li>● <b>Fanotify</b> está activado tanto en sistemas remotos como locales.</li> <li>● El recurso compartido se basa en los sistemas de archivos CIFS y NFS.</li> </ul>

Versiones del kernel	Distribuciones Linux	Detalles
		 <b>Nota</b> El análisis on-access no analiza los recursos compartidos montados utilizando SSH o FTP.
Todos los kernels	Todos los sistemas compatibles	No se admite el análisis on-access en sistemas con <b>DazukoFS</b> para recursos compartidos montados en rutas ya protegidas por el módulo on-access.

-  **Nota**  
 Fanotify y DazukoFS permiten que aplicaciones de terceros controlen el acceso a archivos en sistemas Linux. Para obtener más información, consulte:
- Páginas de manual de Fanotify:  
<http://www.xypron.de/projects/fanotify-manpages/man7/fanotify.7.html>.
  - Sitio Web del proyecto Dazuko: <http://dazuko.dnsalias.org/wiki/index.php/About>.

## macOS

- macOS Mojave (10.14.x)
- macOS High Sierra (10.13.x)
- macOS Sierra (10.12.x)
- OS X El Capitan (10.11.x)
- OS X Yosemite (10.10.5)
- OS X Mavericks (10.9.5)

-  **Nota**  
 Ha dejado de prestarse soporte a OS X Mountain Lion (10.8.5), pero las instalaciones existentes seguirán recibiendo actualizaciones de contenidos de seguridad.

### 4.2.3. Sistemas de archivo compatibles

Bitdefender se instala y protege los siguientes sistemas de archivos:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

**Nota**

El análisis on-access no es compatible con NFS ni CIFS/SMB.

## 4.2.4. Navegadores soportados

Se ha comprobado el funcionamiento de la seguridad del navegador del endpoint con los siguientes navegadores:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

## 4.2.5. Uso de tráfico

- **Tráfico de actualizaciones de producto entre el cliente de endpoint y el servidor de actualizaciones**

Las actualizaciones periódicas del producto Bitdefender Endpoint Security Tools generan el siguiente tráfico de descarga en cada cliente de endpoint:

- En sistemas operativos Windows: ~20 MB
  - En sistemas operativos Linux: ~26 MB
  - En macOS: ~25 MB
- **Tráfico de actualizaciones de contenidos de seguridad descargados entre el cliente de endpoint y el Servidor de actualizaciones (MB/día)**

Tipo de Servidor de actualizaciones	Tipo de motor de análisis		
	Local	Híbrido	Central.
Relay	65	58	55
Servidor de actualizaciones público de Bitdefender	3	3.5	3

## ● Tráfico de análisis centralizado entre el cliente de endpoint y Security Server

Objetos analizados	Tipo tráfico		Bajada (MB)	Subida (MB)
Archivos*	Primer análisis		27	841
	Análisis en caché		13	382
Sitios Web**	Primer análisis	tráfico web	621	N/A
		Security Server	54	1050
	Análisis en caché	tráfico web	654	N/A
		Security Server	0.2	0.5

\* Los datos proporcionados se han medido con 3,49 GB de archivos (6658 archivos), de los cuales 1,16 GB eran archivos portables ejecutables (PE).

\*\* Los datos proporcionados se han medido para los 500 sitios Web mejor clasificados.

## ● Tráfico de análisis híbrido entre el cliente de endpoint y Cloud Services de Bitdefender

Objetos analizados	Tipo tráfico		Bajada (MB)	Subida (MB)
Archivos*	Primer análisis		1.7	0.6
	Análisis en caché		0.6	0.3
tráfico web**	tráfico web		650	N/A
	Cloud Services de Bitdefender		2.6	2.7

\* Los datos proporcionados se han medido con 3,49 GB de archivos (6658 archivos), de los cuales 1,16 GB eran archivos portables ejecutables (PE).

\*\* Los datos proporcionados se han medido para los 500 sitios Web mejor clasificados.



### Nota

La latencia de red entre el cliente de endpoint y el servidor en la nube de Bitdefender debe ser inferior a 1 segundo.

## ● Tráfico entre los clientes Bitdefender Endpoint Security Tools Relay y el Servidor de actualizaciones para descargar contenidos de seguridad

Los clientes con rol de Bitdefender Endpoint Security Tools Relay descargan ~16 MB / día\* del servidor de actualizaciones.

\* Disponible con clientes Bitdefender Endpoint Security Tools a partir de la versión 6.2.3.569.

- **Tráfico entre clientes de endpoint y la consola web Control Center**

Se genera un promedio de tráfico de 618 KB/día entre los clientes de endpoint y la consola Web Control Center.

### 4.3. Cifrado completo del disco duro

El Cifrado de disco completo de GravityZone le permite utilizar BitLocker en los endpoints de Windows y FileVault y la utilidad de línea de comandos diskutil en los endpoints de Mac a través de Control Center.

Para garantizar la protección de datos, este módulo proporciona el cifrado de disco completo en discos fijos, tanto en volúmenes que son de arranque como en los que no, y almacena las claves de recuperación en caso de que los usuarios olviden sus contraseñas.

El módulo de cifrado utiliza los recursos de hardware existentes en su entorno de GravityZone.

En cuanto al software, los requisitos son casi los mismos que para BitLocker, FileVault y la utilidad de línea de comandos diskutil, y la mayoría de las limitaciones dependen de estas herramientas.

#### Para Windows

El cifrado de GravityZone es compatible con BitLocker, a partir de la versión 1.2, en equipos con y sin chip de módulo de plataforma segura (TPM).

GravityZone admite BitLocker en endpoints con los siguientes sistemas operativos:

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 8 Enterprise

- Windows 8 Pro
- Windows 7 Ultimate (con TPM)
- Windows 7 Enterprise (con TPM)
- Windows Server 2019\*
- Windows Server 2016\*
- Windows Server 2012 R2\*
- Windows Server 2012\*
- Windows Server 2008 R2\* (con TPM)

\* Estos sistemas operativos no incluyen BitLocker, por lo que debe instalarse por separado. Para obtener más información acerca de la implementación de BitLocker en Windows Server, consulte estos artículos de la base de conocimientos de Microsoft:

- <https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server>
- [https://technet.microsoft.com/en-us/library/cc732725\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx)



### Importante

GravityZone no admite el cifrado en Windows 7 y Windows 2008 R2 sin TPM.

Para obtener información detallada sobre los requisitos de BitLocker, consulte este artículo de la base de conocimientos de Microsoft: [https://technet.microsoft.com/en-us/library/cc766200\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx)

## Para Mac

GravityZone es compatible con FileVault y diskutil en endpoints de macOS con los siguientes sistemas operativos:

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)
- OS X Yosemite (10.10)
- OS X Mavericks (10.9)

**Nota**

Puede instalar el agente de Bitdefender en Mac OS X Mountain Lion (10.8), pero el módulo Cifrado no estará disponible.

## 4.4. Puertos de comunicación de GravityZone

GravityZone es una solución distribuida, lo que significa que sus componentes se comunican entre sí mediante la red local o Internet. Cada componente utiliza una serie de puertos para comunicarse con los demás. Debe asegurarse de que estos puertos estén abiertos para GravityZone.

Para obtener información detallada sobre los puertos de GravityZone, consulte [este artículo de la base de conocimientos](#).

## 5. INSTALACIÓN DE LA PROTECCIÓN

Para proteger su red con Bitdefender, debe instalar los agentes de seguridad de GravityZone en los endpoints. A tal fin, necesita un usuario de GravityZone Control Center con privilegios de administración sobre los endpoints bajo su administración.

### 5.1. Administración de Licencias

GravityZone se licencia con una sola clave para todos los servicios de seguridad, excepto para el Cifrado de disco completo, que tiene una clave independiente para la licencia anual.

Puede probar gratuitamente GravityZone durante un periodo de 30 días. Durante el periodo de evaluación todas las funciones están totalmente operativas y puede usar el servicio en cualquier número de equipos. Si desea continuar utilizando los servicios, deberá optar por un plan de suscripción de pago y realizar la compra antes de que finalice el periodo de prueba.

Para comprar una licencia, contacte con un reseller de Bitdefender o contáctenos a través del e-mail [enterprisesales@bitdefender.com](mailto:enterprisesales@bitdefender.com).

Su suscripción es administrada por Bitdefender o por el partner de Bitdefender que le vende el servicio. Algunos partners de Bitdefender son proveedores de servicios de seguridad. Dependiendo de sus acuerdos de suscripción, el uso diario de GravityZone puede ser administrado tanto internamente por su empresa como externamente por el proveedor de servicios de seguridad.

#### 5.1.1. Encontrar un reseller

Nuestros resellers le proporcionarán toda la información que necesite y le ayudarán a elegir la mejor opción de licencia para usted.

Para encontrar un reseller de Bitdefender en su país:

1. Acceda a la página del [Buscador de partners](#) en el sitio Web de Bitdefender.
2. Seleccione el país en el que reside para ver la información de contacto de los partners de Bitdefender disponibles.
3. Si no encuentra un reseller Bitdefender en su país, no dude en contactar con nosotros por correo en [comercial@bitdefender.es](mailto:comercial@bitdefender.es).



## 5.1.2. Activación de su licencia

Cuando adquiere un plan de suscripción pagado por primera vez, se le expide una clave de licencia. La suscripción a GravityZone se habilita activando esta clave de licencia.



### Aviso

Activar una licencia NO agrega sus características a la licencia activa actual. En su lugar, la nueva licencia invalida la antigua. Por ejemplo, activar una licencia de 10 endpoints sobre otra de 100 endpoints NO dará como resultado una suscripción de 110 endpoints. Por el contrario, reducirá el número de endpoints cubiertos de 100 a 10.

Se le envía la licencia a través de e-mail cuando la compra. Dependiendo de su acuerdo de servicio, una vez que su clave de licencia es expedida, su proveedor de servicio puede activarla por usted. O bien, puede activar su licencia manualmente siguiendo estos pasos:

1. Conéctese a Control Center usando su cuenta.
2. Haga clic en su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi empresa**.
3. Compruebe la información acerca de la licencia actual en la sección **Licencia**.
4. En la sección **Licencia**, seleccione el tipo de **Licencia**.
5. En el campo de **Clave de licencia**, introduzca su clave de licencia.
6. Haga clic en el botón **Comprobar** y espere a que Control Center recupere la información acerca de la clave de licencia introducida.
7. En el campo **Clave de complemento**, introduzca la clave para un complemento específico, como el Cifrado.
8. Haga clic en **Añadir**. Los detalles del complemento aparecen en una tabla: tipo, clave y opción para eliminarla.
9. Haga clic en **Guardar**.
10. Para poder utilizar el complemento, debe cerrar sesión en Control Center y luego volver a iniciar sesión. Esto hará que las características del complemento sean visibles en GravityZone.

### 5.1.3. Comprobar los detalles de licencia actuales

Para ver los detalles de su licencia:

1. Inicie sesión en Control Center con su dirección de e-mail y contraseña recibidos por correo electrónico.
2. Haga clic en su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi empresa**.
3. Compruebe la información acerca de la licencia actual en la sección **Licencia**. También puede hacer clic en el botón **Comprobar** y esperar a que Control Center recupere la información más reciente acerca de la clave de licencia actual.

## 5.2. Instalación de los agentes de seguridad

Para proteger sus endpoints físicos y virtuales, debe instalar un agente de seguridad en cada uno de ellos. Además de gestionar la protección del endpoint local, el agente de seguridad también se comunica con Control Center para recibir las órdenes del administrador y para comunicar los resultados de sus acciones.

Para más información sobre los agentes de seguridad disponibles, consulte [“Agentes de seguridad” \(p. 7\)](#).

En máquinas Windows y Linux, el agente de seguridad puede tener dos roles y es posible instalarlo de la siguiente manera:

1. Como un simple agente de seguridad para sus endpoints.
2. Como [relay](#), actuando como agente de seguridad y también servidor de comunicaciones, de actualizaciones y proxy para otros endpoints de la red.



#### Aviso

- El primer endpoint en el que instale la protección ha de tener rol de relay, o no podrá implementar remotamente el agente de seguridad en otros endpoints de la misma red.
- El endpoint de relay debe estar encendido y conectado para que los agentes conectados se comuniquen con Control Center.

Puede instalar los agentes de seguridad en endpoints físicos y virtuales [ejecutando los paquetes de instalación localmente](#) o [ejecutando las tareas de instalación remotamente](#) desde Control Center.

Es muy importante leer y seguir cuidadosamente las instrucciones para prepararse para la instalación.

En el modo normal, los agentes de seguridad tienen una interfaz de usuario mínima. Sólo permite a los usuarios comprobar el estado de protección y ejecutar tareas de seguridad básicas (actualizaciones y análisis), sin permitir el acceso a la configuración.

Si el administrador de red lo habilita mediante el paquete de instalación y la política de seguridad, el agente de seguridad también se puede ejecutar en [modo de Usuario avanzado](#) en endpoints de Windows, lo que permite que el usuario del endpoint vea y modifique los ajustes de política. No obstante, el administrador de Control Center siempre puede controlar qué ajustes de política se aplican, imponiendo su criterio al modo de Usuario avanzado.

El idioma mostrado por la interfaz de usuario en los endpoints de Windows protegidos se define por defecto en el momento de la instalación en función del idioma de su cuenta de GravityZone.

En Mac, el idioma mostrado por la interfaz de usuario se define en el momento de la instalación en función del idioma del sistema operativo del endpoint. En Linux, el agente de seguridad no tiene una interfaz de usuario localizada.

Para instalar la interfaz de usuario en otro idioma en determinados endpoints de Windows, puede crear un paquete de instalación y establecer el idioma preferido en sus opciones de configuración. Esta opción no está disponible para endpoints Mac y Linux. Para obtener más información sobre la creación de paquetes de instalación, consulte [“Crear paquetes de instalación”](#) (p. 32).

## 5.2.1. Preparándose para la Instalación

Antes de la instalación, siga estos pasos preparatorios para asegurarse de que todo vaya bien:

1. Asegúrese de que los endpoints objetivo cumplen los [requisitos mínimos del sistema](#). Para algunos endpoints, puede que necesite instalar el service pack del sistema operativo más reciente disponible o liberar espacio en disco. Configure una lista de endpoints que no cumplan los requisitos necesarios para que pueda excluirlos de la administración.
2. Desinstale (no vale simplemente inhabilitar) cualquier antimalware existente o software de seguridad de Internet de los endpoints objetivo. Ejecutar el agente de seguridad simultáneamente con otro software de seguridad en un endpoint puede afectar a su funcionamiento y causar serios problemas en el sistema.

Muchos de los programas de seguridad incompatibles se detectan automáticamente y se eliminan durante la instalación.

Para más información y para consultar la lista de software de seguridad detectado por Bitdefender Endpoint Security Tools para los sistemas operativos Windows actuales, consulte [este artículo de la base de conocimientos](#).

Para consultar la lista de software de seguridad detectado por Bitdefender Endpoint Security Tools para los sistemas operativos Windows antiguos, consulte [este artículo de la base de conocimientos](#).



### Importante

Si desea implementar el agente de seguridad en un equipo con Bitdefender Antivirus for Mac 5.x, primero debe quitar manualmente este último. Para obtener una guía de los pasos a dar, consulte [este artículo de la base de conocimientos](#).

3. La instalación requiere disponer de privilegios de administrador y acceso a Internet. Si los endpoints objetivo están en un dominio de Active Directory, debe usar las credenciales de administrador de dominio para la instalación remota. De no ser así, asegúrese de que tiene a mano las credenciales necesarias para todos los endpoints.
4. Los endpoints deben tener conexión con Control Center.
5. Se recomienda utilizar una dirección IP fija para el servidor de relay. Si no establece una dirección IP fija, utilice el nombre de host de la máquina.
6. Para implementar el agente a través de un relay de Linux, deben cumplirse las siguientes condiciones adicionales:
  - El endpoint de relay debe tener instalado el paquete Samba (`smbclient`) versión 4.1.0 o superior y el comando/binario `net` para poder implementar agentes de Windows.



### Nota

El comando/binario `net` viene generalmente con los paquetes `samba-client` o `samba-common`. En algunas distribuciones de Linux (como CentOS 7.4), el comando `net` solo se instala cuando se instala la suite completa de Samba (Common + Client + Server). Asegúrese de que su endpoint de relay disponga del comando `net`.

- Los endpoints de Windows objetivo deben tener habilitados el Recurso compartido de red y el Recurso compartido administrativo.
- Los endpoints objetivo de Linux y Mac deben tener SSH habilitado.

7. A partir de macOS High Sierra (10.13), después de instalar Endpoint Security for Mac de forma manual o remota, se solicita a los usuarios que aprueben las extensiones del kernel de Bitdefender en sus equipos. Mientras los usuarios no aprueben las extensiones del kernel de Bitdefender, no funcionarán algunas características de Endpoint Security for Mac. Para eliminar la intervención del usuario, puede aprobar previamente las extensiones del kernel de Bitdefender incluyéndolas en una lista blanca mediante una herramienta de administración de dispositivos móviles.

## 5.2.2. Instalación local

Una forma de instalar el agente de seguridad en un endpoint es ejecutar un paquete de instalación localmente.

Puede crear y administrar paquetes de instalación en la página **Red > Paquetes**.

Bitdefender GravityZone						
Bienvenido: Admin						
Panel de Control	<a href="#">+ Añadir</a> <a href="#">↓ Descargar</a> <a href="#">📧 Enviar enlaces de descarga</a> <a href="#">🗑 Eliminar</a> <a href="#">🔄 Actualizar</a>					
Red						
<b>Paquetes</b>	<input type="checkbox"/>	Nombre	Tipo	Idioma	Descripción	Estado
Tareas	<input type="checkbox"/>	EPS-R	BEST	English	relay	Listo para descargar
Políticas	<input type="checkbox"/>	Endpoint Package	BEST	English	en	Listo para descargar
Informes						

La página Paquetes



### Aviso

- La primera máquina en la que instale la protección ha de tener rol de relay, o no podrá implementar el agente de seguridad en otros endpoints de la red.
- La máquina de relay debe estar encendida y conectada para que los clientes se comuniquen con Control Center.

Una vez instalado el primer cliente, este se utilizará para detectar otros endpoints de la misma red, basándose en el mecanismo de Detección de redes. Para información detallada sobre la detección de redes, consulte [“Cómo funciona la detección de red”](#) (p. 47).

Para instalar el agente de seguridad localmente en un endpoint, siga estos pasos:

1. [Cree un paquete de instalación](#) según sus necesidades.

**Nota**

Este paso no es obligatorio si ya se ha creado un paquete de instalación para la red correspondiente a su cuenta.

2. [Descargue el paquete de instalación](#) en el endpoint objetivo.

Como alternativa, puede [enviar por correo electrónico los enlaces de descarga del paquete de instalación](#) a varios usuarios de su red.

3. [Ejecute el paquete de instalación](#) en el endpoint objetivo.

## Crear paquetes de instalación

Para crear un paquete de instalación:

1. Conéctese e inicie sesión en Control Center.
2. Vaya a la página **Red > Paquetes**.
3. Haga clic en el botón **+ Añadir** en la parte superior de la tabla. Aparecerá una nueva ventana de configuración.

### Nuevo paquete de punto final

**General**

Nombre: \*

best

Descripción:

Idioma:

Español

Empresa:

COMP

Módulos:

☒ Antimalware

☒ Control avanzado de amenazas

☒ Cortafuegos

☒ Control Contenido

☒ Control de dispositivos

☐ Usuario con Permisos

Funciones:

☐ Relay ⓘ

Modo de análisis ⓘ

Crear paquetes - Opciones

4. Escriba un nombre adecuado y una descripción para el paquete de instalación que quiere crear.
5. En el campo **Idioma**, seleccione el idioma deseado para la interfaz del cliente.

**Nota**

Esta opción solo está disponible para algunos sistemas operativos Windows.

6. Seleccione los módulos de protección que desea instalar.

**Nota**

Solo se instalarán los módulos soportados por cada sistema operativo. Para más información, diríjase a [“Agentes de seguridad” \(p. 7\)](#).

7. Seleccione el rol del endpoint objetivo:

- **Relay**, para crear el paquete para un endpoint con rol de relay. Para más información, diríjase a [“Relay” \(p. 8\)](#)

**Aviso**

Los sistemas operativos antiguos no admiten el rol de relay. Para más información, diríjase a [“Sistemas operativos soportados” \(p. 15\)](#).

- **Servidor de caché de Administración de parches**, para convertir al relay en un servidor interno de distribución de parches de software. Este rol se muestra cuando se selecciona el rol de relay. Para más información, diríjase a [“Servidor de almacenamiento en caché de parches” \(p. 9\)](#)
8. **Modo de análisis.** Elija la tecnología de análisis que mejor se adapte a su entorno de red y a los recursos de sus endpoints. Puede definir el modo de análisis eligiendo uno de los siguientes tipos:
    - **Automática.** En este caso, el agente de seguridad detectará automáticamente la configuración del endpoint y adaptará la tecnología de análisis en consecuencia:
      - Análisis local (con motores completos) para equipos físicos con hardware de alto rendimiento.

**Nota**

Se consideran equipos de bajo rendimiento aquellos que tienen una frecuencia de CPU inferior a 1,5 GHz o menos de 1 GB de memoria RAM.

- **Personal.** En este caso, puede configurar el modo de análisis escogiendo entre diversas tecnologías de análisis para máquinas físicas y virtuales:
  - Análisis híbrido (con motores ligeros)
  - Análisis local (con motores completos)

El modo de análisis por defecto para las instancias de EC2 es Análisis local (todos los contenidos de seguridad se almacenan en el agente de seguridad instalado y el análisis se ejecuta localmente en la máquina). Si desea analizar sus instancias de EC2 con un Security Server, deberá configurar en consecuencia el paquete de instalación del agente de seguridad y la política aplicada.

El modo de análisis por defecto para las máquinas virtuales de Microsoft Azure es Análisis local (todos los contenidos de seguridad se almacenan en el agente de seguridad instalado y el análisis se ejecuta localmente en la máquina). Si desea analizar sus máquinas virtuales de Microsoft Azure con un Security Server, deberá configurar en consecuencia el paquete de instalación del agente de seguridad y la política aplicada.

Para obtener más información con respecto a las tecnologías de análisis disponibles, consulte [“Motores de análisis”](#) (p. 3)



### Aviso

Endpoint Security (agente antiguo) solo es compatible con el análisis local.

9. Seleccione **Analizar antes de la instalación** si quiere asegurarse de que las máquinas están limpias antes de instalar el cliente en ellas. Se ejecutará un análisis rápido en la nube de las máquinas objetivo correspondientes antes de empezar la instalación.
10. En los endpoints Windows, Bitdefender Endpoint Security Tools se instala en el directorio de instalación por defecto. Seleccione **Usar ruta de instalación personalizada** si desea instalar Bitdefender Endpoint Security Tools en una ubicación diferente. En este caso, escriba la ruta deseada en el campo correspondiente. Utilice las reglas de Windows al escribir la ruta (por ejemplo, D:\carpeta). Si la carpeta especificada no existe, se creará durante la instalación.
11. Si lo desea, puede establecer una contraseña para evitar que los usuarios desinstalen la protección. Seleccione **Contraseña de desinstalación** e introduzca la contraseña deseada en los campos correspondientes.



12. Si los endpoints objetivo se encuentran en el inventario de red de **Grupos personalizados**, puede elegir trasladarlos a una carpeta especificada inmediatamente después de haber finalizado la implementación de agentes de seguridad.

Seleccione **Usar carpeta personalizada** y elija una carpeta en la tabla correspondiente.

13. En la sección **Implementador**, seleccione la entidad a la que se conectarán los endpoints objetivo para instalar y actualizar el cliente:

- **Bitdefender Cloud**, si desea actualizar los clientes directamente desde Internet.

En este caso, también puede definir los ajustes del proxy, si es que los endpoints objetivo se conectan a Internet a través de un proxy. Seleccione **Utilizar un proxy para la comunicación** e introduzca los ajustes necesarios del proxy en los campos que figuran a continuación.

- **Endpoint Security Relay**, si desea conectar los endpoints a un cliente de relay instalado en su red. Todas las máquinas con rol de relay detectadas en su red figurarán en la tabla que se muestra a continuación. Seleccione la máquina de relay que desee. Los endpoints conectados se comunicarán con Control Center solo mediante el relay especificado.



### Importante

El puerto 7074 debe estar abierto para que funcione la implementación mediante Bitdefender Endpoint Security Tools Relay.

14. Haga clic en **Guardar**.

El nuevo paquete creado se añadirá a la lista de paquetes.




### Nota

Los ajustes configurados en un paquete de instalación se aplicarán a los endpoints inmediatamente después de la instalación. En cuanto se aplique una política al cliente, se harán cumplir los ajustes configurados en la política en sustitución de determinados ajustes del paquete de instalación (como por ejemplo, servidores de comunicaciones o ajustes de proxy).

## Descargar los paquetes de instalación

Para descargar los paquetes de instalación de los agentes de seguridad:

1. Inicie sesión en Control Center desde el endpoint en el que desee instalar la protección.
2. Vaya a la página **Red > Paquetes**.
3. Seleccione el paquete de instalación que desee descargar.
4. Haga clic en el botón  **Descargar** en la zona superior de la tabla y seleccione el tipo de instalador que quiera utilizar. Hay disponibles dos tipos de archivos de instalación:

- **Downloader.** El downloader primero descarga el kit de instalación completo desde los servidores de la nube de Bitdefender y luego inicia la instalación. Es pequeño en tamaño y puede ejecutarse tanto en sistemas de 32-bit como de 64-bit (lo que lo hace más fácil de distribuir). Por otro lado, requiere una conexión a Internet activa.
- **Kit completo.** Los kits de instalación completos tienen mayor tamaño y han de ejecutarse en el tipo concreto de sistema operativo.

El kit completo se utiliza para instalar la protección en los endpoints sin conexión a Internet o con conexiones lentas. Descargue este archivo en un endpoint conectado a Internet y distribúyalo a otros endpoints usando un medio de almacenamiento externo o compartiéndolo en la red.



### Nota

Versiones de kit completo disponibles:

- **SO Windows:** sistemas de 32 bits y 64 bits
  - **SO Windows heredado:** sistemas de 32 bits y 64 bits
  - **SO Linux:** sistemas de 32 bits y 64 bits
  - **macOS:** solo sistemas de 64 bits
- Asegúrese de usar la versión correcta para el sistema donde instala.

5. Guarde el archivo en el endpoint.




### Aviso

- No hay que cambiar el nombre del ejecutable de descarga, pues de lo contrario no podrá descargar los archivos de instalación del servidor de Bitdefender.

6. Además, si ha elegido el Descargador, puede crear un paquete MSI para los endpoints de Windows. Para más información, consulte [este artículo](#) de la base de conocimiento.

## Enviar enlaces de descarga de paquetes de instalación por correo electrónico

Es posible que tenga que informar rápidamente a otros usuarios de que hay un paquete de instalación listo para descargar. En tal caso, siga los pasos descritos a continuación:

1. Vaya a la página **Red > Paquetes**.
2. Seleccione el paquete de instalación que desee.
3. Haga clic en el botón  **Enviar enlaces de descarga** en la zona superior de la tabla. Aparecerá una nueva ventana de configuración.
4. Introduzca la dirección de correo electrónico de cada usuario que desea que reciba el enlace de descarga del paquete de instalación. Pulse **Intro** tras cada dirección.  
Asegúrese de la validez de todas las direcciones de correo electrónico que introduzca.
5. Si desea ver los enlaces de descarga antes de enviarlos por correo electrónico, haga clic en el botón **Enlaces de instalación**.
6. Haga clic en **Enviar**. Se envía un correo electrónico que contiene el enlace de instalación a cada dirección de correo electrónico especificada.

## Ejecutar los paquetes de instalación

Para que funcione la instalación, el paquete de instalación debe ejecutarse utilizando privilegios de administrador.

El paquete se instala de manera diferente en cada sistema operativo como se describe a continuación:

- En los sistemas operativos Windows y macOS:
  1. En el endpoint objetivo, descargue el archivo de instalación de Control Center o cópielo desde un recurso compartido de red.
  2. Si ha descargado el kit completo, extraiga los archivos del archivo comprimido.

3. Ejecute el archivo ejecutable.
4. Siga las instrucciones que aparecen en la pantalla.

**Nota**

En macOS, después de instalar Endpoint Security for Mac, se solicita a los usuarios que aprueben las extensiones del kernel de Bitdefender en sus equipos. Mientras los usuarios no aprueben las extensiones del kernel de Bitdefender, no funcionarán algunas características del agente de seguridad. Para más información, consulte [este artículo de la base de conocimientos](#).

- En sistemas operativos Linux:
  1. Conéctese e inicie sesión en Control Center.
  2. Descargue o copie el archivo de instalación en el endpoint objetivo.
  3. Si ha descargado el kit completo, extraiga los archivos del archivo comprimido.
  4. Dótese de privilegios de root ejecutando el comando `sudo su`.
  5. Cambie los permisos del archivo de instalación para poder ejecutarlo:

```
# chmod +x installer
```

6. Ejecutar los archivos de instalación:

```
# ./installer
```

7. Para comprobar que el agente se ha instalado en el endpoint, ejecute este comando:

```
$ service bd status
```

Una vez instalado el agente de seguridad, el endpoint se mostrará como administrado en Control Center (página **Red**) en unos minutos.



### Importante

Si utiliza la administración de VMware Horizon View Persona, se recomienda configurar la política de grupo de Active Directory para excluir los siguientes procesos de Bitdefender (sin la ruta completa):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationsservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Estas exclusiones deben aplicarse siempre que el agente de seguridad se ejecute en el endpoint. Para más información, consulte esta [página de la documentación de VMware Horizon](#).

## 5.2.3. Instalación remota

Gracias a las tareas de instalación, Control Center le permite instalar remotamente el agente de seguridad en endpoints detectados en la red.

Una vez que haya instalado localmente el primer cliente con rol de relay, pueden tardarse unos minutos en que el resto de endpoints de la red aparezcan en Control Center. Desde este punto, puede instalar remotamente el agente de seguridad en endpoints bajo su administración mediante tareas de instalación desde Control Center.

Bitdefender Endpoint Security Tools incluye un mecanismo automático de detección de redes que le permite detectar otros endpoints de su red. Los endpoints detectados se muestran como **no administrados** en la página **Red**.

Para activar la detección de redes, primero debe tener instalado Bitdefender Endpoint Security Tools en al menos un endpoint de la red. Este endpoint se utilizará para analizar la red e instalar Bitdefender Endpoint Security Tools en los endpoints desprotegidos.

Para información detallada sobre la detección de redes, consulte [“Cómo funciona la detección de red”](#) (p. 47).

## Requisitos de la instalación remota

Para que funcione la instalación remota:

- Debe haber instalado Bitdefender Endpoint Security Tools Relay en su red.
- Para Windows:
  - Debe estar habilitado el recurso compartido administrativo `admin$`. Configure todas las estaciones de trabajo objetivo para que no utilicen el uso compartido de archivos avanzado.
  - Configure el Control de cuentas de usuario (UAC) según el sistema operativo que se ejecute en los endpoints objetivo. Si los endpoints están en un dominio de Active Directory, puede utilizar una política de grupo para configurar el Control de cuentas de usuario. Para más información, consulte [este artículo de la base de conocimientos](#).
  - Inhabilite Windows Firewall o configúrelo para permitir el tráfico a través del protocolo Compartir archivos e impresoras.

**Nota**

La implementación remota solo funciona en los sistemas operativos modernos, a partir de Windows 7/Windows Server 2008 R2, para los cuales Bitdefender brinda soporte total. Para más información, diríjase a [“Sistemas operativos soportados”](#) (p. 15).

- En Linux, debe habilitarse SSH.
- En macOS deben estar habilitados el inicio de sesión remoto y el uso compartido de archivos.

## Ejecución de tareas de instalación remota

Para ejecutar una tarea de instalación remota:

1. Conéctese e inicie sesión en Control Center.
2. Diríjase a la página **Red**.
3. Seleccione el grupo deseado desde el panel lateral izquierdo. Las entidades contenidas en el grupo seleccionado se muestran en la tabla del panel lateral derecho.

**Nota**

Opcionalmente, puede aplicar filtros para mostrar únicamente los endpoints no administrados. Haga clic en el menú **Filtros** y seleccione las siguientes opciones:

**No administrados** de la pestaña **Seguridad** y **Todos los elementos recursivamente** de la pestaña **Profundidad**.

4. Seleccione las entidades (endpoints o grupos de endpoints) en las que desee instalar la protección.
5. Haga clic en el botón ⓘ **Tareas** de la zona superior de la tabla y seleccione **Instalar**.

El asistente de **Instalar cliente** se está mostrando.

Instalar cliente

Opciones

☒ Ahora  
☐ Programado

☐ Reiniciar auto. (si es necesario)

Administrador de Credenciales

Usuario	Contraseña	Descripción	Acción
<input type="checkbox"/> admin	*****		ⓧ

Primera página — Página 1 de 1 — Última página 20

1 elementos

Instalación de Bitdefender Endpoint Security Tools desde el menú Tareas

6. En la sección **Opciones**, configure el momento de la instalación:
  - **Ahora**, para poner en marcha la implementación de inmediato.
  - **Programado**, para configurar el intervalo de recurrencia de la implementación. En este caso, seleccione el intervalo de tiempo que desee (cada hora, a diario o semanalmente) y configúrelo según sus necesidades.



### Nota

Por ejemplo, cuando hay que realizar determinadas operaciones en el equipo objetivo antes de instalar el cliente (como la desinstalación de otros programas y el reinicio del sistema operativo), puede programar la tarea de implementación para que se ejecute cada 2 horas. La tarea se lanzará en los equipos objetivo cada 2 horas hasta que culmine correctamente.

7. Si quiere que los endpoints objetivo se reinicien automáticamente para completar la instalación, seleccione **Reiniciar automáticamente (si es necesario)**.
8. En la sección **Administrador de credenciales**, especifique las credenciales administrativas necesarias para la autenticación remota en los endpoints objetivo. Puede añadir las credenciales escribiendo el usuario y contraseña para cada sistema operativo objetivo.



### Importante

Para estaciones Windows 8.1, debe proporcionar las credenciales de la cuenta de administrador integrada o de una cuenta de administrador de dominio. Para obtener más información, consulte [este artículo de la base de conocimientos](#).

Para añadir las credenciales del sistema operativo requeridas:

- a. Introduzca el nombre de usuario y contraseña de una cuenta de administrador en los campos correspondientes del encabezado de la tabla.

Si los equipos están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

Utilice las normas de Windows cuando introduzca el nombre de una cuenta de usuario:

- Para las máquinas de Active Directory, utilice estas sintaxis: `usuario@dominio.com` y `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas de ambas maneras (`nombredeusuario@dominio.com` y `dominio\nombredeusuario`).
- Para las máquinas del grupo de trabajo es suficiente con introducir solo el nombre de usuario, sin el nombre del grupo de trabajo.

Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta.

- b. Haga clic en el botón **Añadir**. La cuenta se añade a la lista de credenciales.



### Nota

Las credenciales especificadas se guardan automáticamente en su [Gestor de credenciales](#) para que no tenga que volver a introducirlas la próxima vez. Para acceder al Gestor de credenciales, señale su nombre de usuario en la esquina superior derecha de la consola.





### Importante

Si las credenciales proporcionadas no son válidas, la implementación del cliente fallará en los endpoints correspondientes. Asegúrese de actualizar las credenciales del SO introducidas en el Gestor de credenciales cuando éstas cambien en los endpoints objetivo.

9. Marque las casillas de verificación correspondientes a las cuentas que desee usar.



### Nota

Se mostrará un mensaje de advertencia si todavía no ha seleccionado credenciales. Este paso es obligatorio para instalar de forma remota el agente de seguridad en los endpoints.

10. En la sección **Implementador**, configure el relay al que se conectarán los endpoints objetivo para instalar y actualizar el cliente:

- Todas las máquinas con rol de relay detectadas en su red figurarán en la tabla disponible en la sección **Implementador**. Cada nuevo cliente debe estar conectado por lo menos a un cliente de relay de la misma red, que actuará como servidor de actualizaciones y de comunicaciones. Seleccione el relay que quiere vincular a los endpoints objetivo. Los endpoints conectados se comunicarán con Control Center solo mediante el relay especificado.



### Importante

El puerto 7074 debe estar abierto para que funcione la implementación mediante el agente de relay.

Implementador

Implementador:

Endpoint Security Relay

Nombre	IP	Nombre/IP del servidor per...	Etiqueta
CO_SUPA	192.168.0.183		N/A
FC-WIN7-X64-01	192.168.3.80		N/A

Primera Página
Página 0 de 0
Última página 20
0 elementos

- Si los endpoints objetivo se comunican con el agente de relay mediante un proxy, también tiene que definir los ajustes del proxy. En este caso, seleccione **Utilizar un proxy para la comunicación** e introduzca los ajustes necesarios del proxy en los campos que figuran a continuación.
11. Tiene que seleccionar un paquete de instalación para la implementación actual. Haga clic en la lista **Usar paquete** y seleccione el paquete de instalación que desee. Aquí puede encontrar todos los paquetes de instalación creados con anterioridad para su cuenta y también el paquete de instalación por defecto disponible con Control Center.
12. Si es necesario, puede modificar algunos de los ajustes del paquete de instalación seleccionado haciendo clic en el botón **Personalizar** junto al campo **Usar paquete**.
- Abajo aparecerán los ajustes del paquete de instalación y puede hacer los cambios que precise. Para más información sobre la modificación de paquetes de instalación, consulte [“Crear paquetes de instalación” \(p. 32\)](#).
- Si desea guardar las modificaciones como un paquete nuevo, seleccione la opción **Guardar como paquete**, situada en la parte inferior de la lista de ajustes de paquetes, e introduzca un nombre para el nuevo paquete de instalación.
13. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.
- Puede ver y administrar las tareas en la página **Red > Tareas**.



### Importante

Si utiliza la administración de VMware Horizon View Persona, se recomienda configurar la política de grupo de Active Directory para excluir los siguientes procesos de Bitdefender (sin la ruta completa):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationsservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Estas exclusiones deben aplicarse siempre que el agente de seguridad se ejecute en el endpoint. Para más información, consulte esta [página de la documentación de VMware Horizon](#).

## 5.2.4. Preparación de sistemas Linux para el análisis on-access

Bitdefender Endpoint Security Tools for Linux incluye posibilidades de análisis on-access que funcionan con determinadas distribuciones Linux y versiones del kernel. Para más información, consulte los [requisitos del sistema](#).

A continuación aprenderá a compilar manualmente el módulo DazukoFS.

### Compilación manual del módulo DazukoFS

Siga los siguientes pasos para compilar DazukoFS para la versión del kernel del sistema y luego cargar el módulo:

1. Descargue las cabeceras del kernel apropiadas.

- En sistemas **Ubuntu**, ejecute este comando:

```
$ sudo apt-get install linux-headers-`uname -r`
```

- En sistemas **RHEL/CentOS**, ejecute este comando:

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. En sistemas **Ubuntu**, necesita build-essential:

```
$ sudo apt-get install build-essential
```

3. Copie y extraiga el código fuente de DazukoFS en el directorio que prefiera:

```
# mkdir temp
# cd temp
# cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
# tar -xzf dazukofs-source.tar.gz
# cd dazukofs-3.1.4
```

4. Compile el módulo:

```
# make
```

## 5. Instale y cargue el módulo:

```
# make dazukofs_install
```

### Requisitos para la utilización del análisis on-access con DazukoFS

Para que el análisis on-access funcione con DazukoFS, se deben cumplir una serie de condiciones. Compruebe si alguna de las afirmaciones que figuran a continuación corresponde a su sistema Linux y siga las instrucciones para evitar problemas.

- La política SELinux debe estar desactivada o configurada como **Tolerante**. Para consultar y ajustar la opción de política SELinux, edite el archivo `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools es compatible exclusivamente con la versión DazukoFS incluida en el paquete de instalación. Si DazukoFS ya está instalado en el sistema, desinstálelo antes de instalar Bitdefender Endpoint Security Tools.
- DazukoFS es compatible con ciertas versiones del kernel. Si el paquete DazukoFS incluido con Bitdefender Endpoint Security Tools no es compatible con la versión del kernel del sistema, el módulo dará error al cargarse. En dicho caso, puede actualizar el kernel a la versión soportada o recompilar el módulo DazukoFS para su versión del kernel. Puede encontrar el paquete DazukoFS en el directorio de instalación de Bitdefender Endpoint Security Tools:

```
/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz
```

- Al compartir archivos a través de servidores dedicados como NFS, UNFSv3 o Samba, tiene que iniciar los servicios en el siguiente orden:
  1. Activar el análisis on-access mediante política desde Control Center.  
Para más información, consulte la Guía del administrador de GravityZone.
  2. Inicie el servicio de uso compartido de red.

Para NFS:

```
# service nfs start
```

Para UNFSv3:

```
# service unfs3 start
```

Para Samba:

```
# service smb start
```



### Importante

Para el servicio NFS, DazukoFS solo es compatible con el Servidor de usuarios NFS.

## 5.2.5. Cómo funciona la detección de red

Además de la integración con Active Directory, GravityZone también incluye un mecanismo automático de detección de redes pensado para detectar los equipos del grupo de trabajo.

GravityZone se basa en el servicio **Microsoft Computer Browser** y en la herramienta **NBTscan** para realizar la detección de redes.

El servicio Computer Browser es una tecnología de red utilizada por los equipos basados en Windows para mantener listas actualizadas de dominios, grupos de trabajo y los equipos en ellos, y para suministrar estas listas a equipos cliente que lo soliciten. Los equipos detectados en la red por el servicio Computer Browser pueden visualizarse ejecutando el comando de **net view** en una ventana de símbolo del sistema.

```
Z:\>net view
Server Name      Remark
-----
\\SCIREFDL
\\SCIREFJM
\\SCIREFLL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

El comando Net view

La herramienta NBTscan analiza las redes de equipos con NetBIOS. Consulta a todos los endpoints de la red y recupera información como la dirección IP, el nombre NetBIOS del equipo y la dirección MAC.

Para activar la detección automática de red, primero debe tener instalado Bitdefender Endpoint Security Tools Relay en al menos un equipo de la red. Este equipo se utilizará para analizar la red.



### Importante

Control Center no utiliza la información de red del Active Directory o de la función de mapa de red disponible en Windows Vista y posterior. El mapa de red se basa en una tecnología de detección de red diferente: el protocolo Link Layer Topology Discovery (LLTD).

Control Center no está directamente implicado en la operativa del servicio Computer Browser. Bitdefender Endpoint Security Tools solo consulta al servicio Computer Browser respecto a la lista de estaciones de trabajo y servidores visible actualmente en la red (conocida como lista de examen) y luego la envía a Control Center. Control Center procesa la lista de examen, añadiendo nuevos equipos detectados a su lista de **Equipos no administrados**. Los equipos anteriormente detectados no se borran después de una nueva consulta de detección de red, así que deberá excluir y borrar manualmente los equipos que ya no estén en la red.

La consulta inicial de la lista de examen la lleva a acabo el primer Bitdefender Endpoint Security Tools instalado en la red.

- Si el relay está instalado en un equipo de un grupo de trabajo, solo se verán en Control Center los equipos de ese grupo de trabajo.
- Si el relay está instalado en un equipo de un dominio, solo se verán en Control Center los equipos de ese dominio. Los equipos de otros dominios pueden detectarse si hay una relación de confianza con el dominio donde está instalado el relay.

Las consultas posteriores sobre detección de red se realizan regularmente cada hora. Para cada nueva consulta, Control Center divide el espacio de equipos administrados en áreas de visibilidad y luego designa un relay en cada área donde realizar la tarea. Un área de visibilidad es un grupo de equipos que se detectan entre ellos. Normalmente, un área de visibilidad se define por un grupo de trabajo o dominio, pero esto depende de la topología de la red y su configuración. En algunos casos, un área de visibilidad puede consistir en múltiples dominios y grupos de trabajo.

Si un relay seleccionado falla al realizar la consulta, Control Center espera a la siguiente consulta programada, sin escoger otro relay para intentarlo de nuevo.

Para una visibilidad de toda la red, el relay debe estar instalado en al menos un equipo de cada grupo de trabajo o dominio de su red. Lo ideal sería que Bitdefender Endpoint Security Tools estuviera instalado en al menos un equipo en cada subred.

## Más sobre el servicio Microsoft Computer Browser

Datos sobre el servicio Computer Browser:

- Funciona independientemente de Active Directory.
- Funciona exclusivamente en redes IPv4 y opera independientemente dentro de los límites de un grupo LAN (grupo de trabajo o dominio). Se compila y mantiene una lista de examen para cada grupo LAN.
- Normalmente utiliza transmisiones del servidor sin conexión para comunicarse entre nodos.
- Utiliza NetBIOS en TCP/IP (NetBT).
- Requiere resolución de nombre de NetBIOS. Se recomienda tener una infraestructura de Servicio de Windows de nombre de Internet (WINS) funcionando en la red.
- No está habilitado por omisión en Windows Server 2008 y 2008 R2.

Para información detallada sobre el servicio Computer Browser, compruebe la [Referencia técnica del servicio de navegador del equipo](#) en Microsoft Technet.

## Requisitos de descubrimiento de red

Para detectar satisfactoriamente todos los equipos (servidores y estaciones de trabajo) que se administrarán desde Control Center, se necesita lo siguiente:

- Los equipos deben estar unidos a un grupo de trabajo o dominio y conectados a través de una red local IPv4. El servicio Computer Browser no funciona en redes IPv6.
- Varios equipos en cada grupo LAN (grupo de trabajo o dominio) deben ejecutar el servicio Computer Browser. Los controladores de dominio primario también deben ejecutar el servicio.
- Las NetBIOS en TCP/IP (NetBT) deben estar habilitadas en los equipos. El cortafuegos local debe permitir el tráfico NetBT.
- Si utiliza un relay de Linux para detectar otros endpoints de Linux o Mac, debe instalar Samba en los endpoints objetivo, o incorporarlos a Active Directory y

utilizar DHCP. De esta forma, NetBIOS se configurará automáticamente para ellos.

- La compartición de archivos debe estar habilitada en los equipos. El cortafuegos local debe permitir la compartición de archivos.
- Hay que establecer una infraestructura de Windows Internet Naming Service (WINS) que funcione correctamente.
- Para Windows Vista y posterior, la detección de red ha de estar activada (**Panel de control > Centro de redes y recursos compartidos > Cambiar ajustes de compartición avanzados**).

Para poder activar esta característica, han de iniciarse los siguientes servicios:

- Cliente DNS
  - Publicación de recurso de detección de función
  - Descubrimiento de SSDP
  - Host de dispositivo UPnP
- En entornos con múltiples dominios, se recomienda establecer relaciones de confianza entre dominios de manera que los equipos puedan acceder a las listas de examen de otros dominios.

Los equipos desde los cuales Bitdefender Endpoint Security Tools accede al servicio Computer Browser deben poder resolver nombres NetBIOS.



#### Nota

El mecanismo de detección de redes funciona en todos los sistemas operativos soportados, incluyendo las versiones de Windows Embedded, siempre que se cumplan los requisitos.

## 5.3. Instalación del Cifrado de disco completo

El Cifrado de disco completo requiere su activación según la clave de licencia.

Para obtener información detallada sobre las claves de licencia, consulte [“Administración de Licencias” \(p. 26\)](#).

Los agentes de seguridad de Bitdefender admiten el Cifrado de disco completo desde la versión 6.2.22.916 en Windows y 4.0.0173876 en Mac. Para asegurarse de que los agentes son totalmente compatibles con este módulo, tiene dos opciones:

- Instale los agentes de seguridad con el módulo de Cifrado incluido.



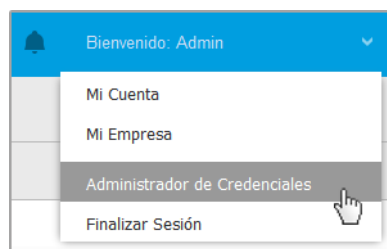
- Utilice la tarea **Reconfigurar**.

Para obtener información detallada sobre el uso del Cifrado de disco completo en su red, consulte el capítulo **Políticas de seguridad > Cifrado** de la Guía del administrador de GravityZone.

## 5.4. Administrador de Credenciales

El Gestor de credenciales le ayuda a definir las credenciales necesarias para la autenticación remota en los distintos sistemas operativos de su red.

Para abrir el Gestor de credenciales, haga clic en su nombre de usuario en la esquina superior derecha de la página y seleccione **Gestor de credenciales**.

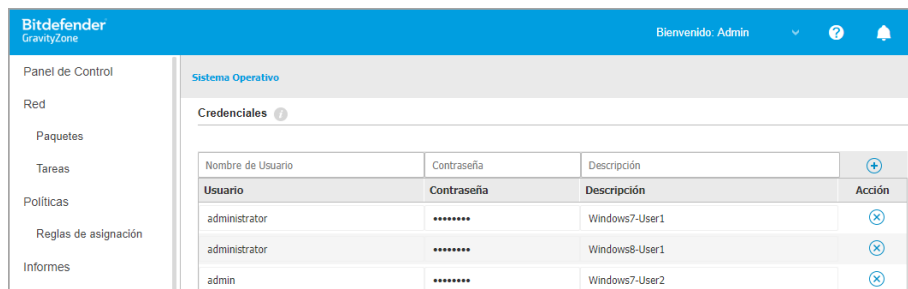


El menú Gestor de credenciales

### 5.4.1. Añadir credenciales al Gestor de credenciales

Con el Gestor de credenciales puede gestionar las credenciales de administrador necesarias para la autenticación remota cuando se envían tareas de instalación a equipos y máquinas virtuales de su red.

Para añadir un conjunto de credenciales:



## Administrador de Credenciales

1. Escriba el nombre de usuario y contraseña de una cuenta de administrador para cada uno de los sistemas operativos objetivo en los campos correspondientes de la zona superior del encabezado de la tabla. Opcionalmente puede añadir una descripción que le ayudará a identificar más fácilmente cada cuenta. Si los equipos están en un dominio, es suficiente con introducir las credenciales del administrador del dominio.

Utilice las normas de Windows cuando introduzca el nombre de una cuenta de usuario:

- Para las máquinas de Active Directory, utilice estas sintaxis: `usuario@dominio.com` y `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas de ambas maneras (`nombredeusuario@dominio.com` y `dominio\nombredeusuario`).
- Para las máquinas del grupo de trabajo es suficiente con introducir solo el nombre de usuario, sin el nombre del grupo de trabajo.

2. Haga clic en el botón **+ Añadir** del lateral derecho de la tabla. El nuevo conjunto de credenciales se añade a la tabla.




### Nota

Si no ha especificado las credenciales de autenticación, necesitará introducirlas cuando ejecute tareas de instalación. Las credenciales especificadas se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

## 5.4.2. Eliminación de credenciales del Gestor de credenciales

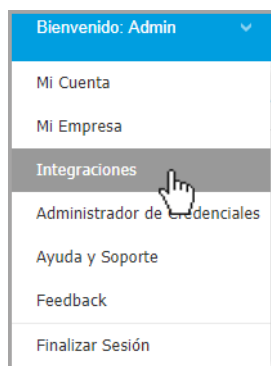
Para eliminar credenciales obsoletas del Gestor de credenciales:

1. Vaya a la fila de la tabla que contiene las credenciales que desea eliminar.
2. Haga clic en el botón  **Eliminar** a la derecha de la fila de la tabla correspondiente. La cuenta seleccionada se eliminará.

## 6. INTEGRACIONES

GravityZone ofrece la posibilidad de integrar Control Center con soluciones de terceros.

Puede configurar la integración de sus soluciones de terceros en la página **Integraciones**, a la cual puede acceder señalando su nombre de usuario en la esquina superior derecha de la consola y eligiendo **Integraciones**.



Desde esta página, puede añadir, editar o eliminar las integraciones según sus necesidades.

### 6.1. Integración con Amazon EC2

Si su empresa tiene una licencia de servicio Bitdefender Security for AWS o utiliza una suscripción de prueba a Bitdefender Security for AWS, puede configurar la integración con este servicio desde GravityZone Control Center e implementar, administrar y monitorizar la seguridad de Bitdefender de forma centralizada en su inventario de instancias. Bitdefender aloja los servidores de análisis de su propiedad en la nube de AWS para garantizar una huella óptima en las instancias protegidas y para eliminar la sobrecarga de análisis que se produce con el software de seguridad tradicional.

Para obtener información completa sobre la arquitectura Bitdefender Security for AWS, los requisitos previos, el modo de suscripción y la creación y administración de la integración con Amazon EC2, consulte la [Guía de integración de Amazon EC2](#).

## 7. DESINSTALACIÓN DE LA PROTECCIÓN EN ENDPOINTS

Tiene dos opciones para desinstalar los agentes de seguridad:

- **Remotamente** en Control Center
- **Manualmente** en la máquina objetivo



### Aviso

Los agentes de seguridad son esenciales para mantener a los endpoints a salvo de cualquier tipo de amenaza, por lo que desinstalarlos puede poner en peligro toda la red.

### Desinstalación remota

Para desinstalar la protección de Bitdefender de cualquier endpoint administrado de forma remota:

1. Acceda a la página **Red**.
2. Seleccione el contenedor que desee del panel de la izquierda. Todos los equipos del contenedor seleccionado se muestran en la tabla del panel de la derecha.
3. Seleccione los endpoints de los que desea desinstalar el agente de seguridad de Bitdefender.
4. Haga clic en **Tareas**, en la zona superior de la tabla, y elija **Desinstalar cliente**. Se muestra una ventana de configuración.
5. En la ventana de la tarea **Desinstalar agente** puede elegir si desea conservar los archivos en cuarentena en el endpoint o borrarlos.
6. Haga clic en **Guardar** para crear la tarea. Aparecerá un mensaje de confirmación.

Puede ver y administrar la tarea en **Red > Tareas**.

Si desea volver a instalar los agentes de seguridad, consulte [“Instalación de los agentes de seguridad” \(p. 28\)](#).

### Desinstalación local

Para desinstalar manualmente el agente de seguridad de Bitdefender de una máquina con Windows:

1. Dependiendo de su sistema operativo:

- En Windows 7, acceda a **Inicio > Panel de control > Desinstalar un programa** en la categoría **Programas**.
  - En Windows 8, acceda a **Configuración > Panel de control > Desinstalar un programa** en la categoría **Programas**.
  - En Windows 8.1, haga clic con el botón derecho en el botón **Inicio** y, a continuación, seleccione **Panel de control > Programas y características**.
  - En Windows 10, acceda a **Inicio > Configuración > Sistema > Aplicaciones y características**.
2. En la lista de programas, seleccione el agente de Bitdefender que desee.
  3. Haga clic en **Desinstalar**.
  4. Introduzca la contraseña de Bitdefender, en caso de que se hubiese habilitado en la política de seguridad. Durante la desinstalación, puede ver el progreso de la tarea.

Para desinstalar manualmente el agente de seguridad de Bitdefender de una máquina con Linux:

1. Abra el terminal.
2. Obtenga acceso root mediante los comandos `su` o `sudo su`.
3. Desplácese mediante el comando `cd` hasta la siguiente ruta:  
`/opt/BitDefender/bin`
4. Ejecute el script:

```
# ./remove-sve-client
```

5. Introduzca la contraseña de Bitdefender para continuar, en caso de que se hubiese habilitado en la política de seguridad.

Para desinstalar manualmente el agente de Bitdefender de un Mac:

1. Acceda a **Finder > Aplicaciones**.
2. Abra la carpeta Bitdefender.
3. Haga doble clic en **Desinstalación de Bitdefender para Mac**.
4. En la ventana de confirmación, haga clic en **Comprobar** y **Desinstalar** para continuar.

Si desea volver a instalar los agentes de seguridad, consulte [“Instalación de los agentes de seguridad” \(p. 28\)](#).

## 8. OBTENER AYUDA

Bitdefender se esfuerza en proporcionar a sus clientes un incomparable soporte rápido y eficiente. Si experimenta algún problema o si tiene cualquier duda sobre su producto Bitdefender, diríjase a nuestro [Centro de soporte online](#). Dispone de muchos recursos que puede utilizar para encontrar rápidamente una solución o respuesta a su problema. O, si lo prefiere, puede contactar con el equipo de Atención al Cliente de Bitdefender. Nuestro soporte responderá a todas sus preguntas en un corto periodo y le proporcionarán la asistencia que necesite.



### Nota

Puede encontrar información sobre los servicios y políticas de soporte que ofrecemos en nuestro Centro de Soporte técnico.

### 8.1. Centro de soporte de Bitdefender

El [Centro de soporte de Bitdefender](#) es el lugar al que acudir para obtener toda la asistencia técnica que necesite para su producto de Bitdefender.

Podrá encontrar rápidamente una solución o una respuesta a su consulta:

- Artículos de la base de conocimiento
- Foro de soporte de Bitdefender
- Documentación del Producto

Puede además usar su motor de búsqueda favorito para encontrar más información sobre seguridad informática, los productos Bitdefender y la empresa.

### Artículos de la base de conocimiento

La Base de conocimientos de Bitdefender es un repositorio de información online sobre los productos Bitdefender. Almacena, en un formato de fácil acceso, los informes sobre los resultados del soporte técnico en curso y las actividades de solución de errores por los equipos de soporte y desarrollo de Bitdefender, junto con artículos más generales sobre prevención de virus, la administración de las soluciones Bitdefender con explicaciones detalladas, y muchos otros artículos.

La Base de conocimiento de Bitdefender es de acceso público y puede consultarse gratuitamente. La amplia información que contiene es otro medio de proporcionar a los clientes de Bitdefender el soporte técnico y el conocimiento que necesitan. Las solicitudes de información general o informes de errores de los clientes de



Bitdefender se incluyen en la Base de conocimientos de Bitdefender en forma de soluciones a los bugs, instrucciones de depuración de errores o artículos informativos como apoyo a los archivos de ayuda de los productos.

La base de conocimientos de Bitdefender para productos corporativos está permanentemente disponible en <http://www.bitdefender.com/support/business.html>.

## Foro de soporte de Bitdefender

El Foro de Soporte de Bitdefender proporciona a los usuarios de Bitdefender una forma fácil de obtener ayuda y ayudar a otros. Puede publicar cualquier problema o consulta relacionada con su producto Bitdefender.

El soporte técnico de Bitdefender monitoriza el foro en busca de nuevas publicaciones con el fin de ayudarle. Podrá obtener una respuesta o una solución de un usuario de Bitdefender con más experiencia.

Antes de postear su problema o pregunta, por favor, busque en el foro un tema similar o relacionado.

El Foro de Soporte de Bitdefender está disponible en <http://forum.bitdefender.com>, en 5 idiomas diferentes: Inglés, Alemán, Francia, España y Rumano. Haga clic en el enlace **Protección empresarial** para acceder a la sección dedicada a los productos corporativos.

## Documentación del Producto

La documentación del producto es la fuente más completa de información sobre su producto.

La forma más sencilla de acceder a la documentación es desde la página **Ayuda y soporte** de Control Center. Haga clic en su nombre de usuario en la esquina superior derecha de la consola, seleccione **Ayuda y soporte** y, a continuación, elija el enlace de la guía en la que está interesado. La guía se abrirá en una nueva pestaña de su navegador.

También puede consultar y descargar la documentación en el **Centro de soporte**, en la sección **Documentación** disponible en las páginas de soporte de todos los productos.

## 8.2. Solicitar ayuda

Puede solicitar ayuda a través de nuestro Centro de soporte técnico online: Rellene el [formulario de contacto](#) y envíelo.

## 8.3. Usar la herramienta de soporte

La herramienta de soporte GravityZone está diseñada para ayudar a los usuarios y a los técnicos de soporte a obtener fácilmente la información que necesitan para la resolución de problemas. Ejecute la herramienta de soporte en los equipos afectados, y envíe el archivo resultante con la información de la resolución del problema al representante de soporte de Bitdefender.

### 8.3.1. Uso de la herramienta de soporte en sistemas operativos Windows

#### Ejecución de la aplicación de la herramienta de soporte

Para generar el registro en el equipo afectado, siga uno de estos métodos:

- [Línea de comandos](#)
- [Asistente con GUI](#)

Si BEST no se ha instalado en el equipo, use el archivo ejecutable de la herramienta de soporte de BEST.

#### Método de línea de comandos

1. Abra el símbolo del sistema con privilegios administrativos.
2. Diríjase a la carpeta de instalación del producto. La ruta por defecto es:  
`C:\Archivos de programa\Bitdefender\Endpoint Security`
3. Recopile y guarde los registros ejecutando este comando:

```
Product.Support.Tool.exe collect
```

Los registros se guardan por defecto en `C:\Windows\Temp`.

Como alternativa, si desea guardar el registro de la herramienta de soporte en una ubicación personalizada, use la ruta opcional:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

### Ejemplo:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Mientras se ejecuta el comando, podrá ver una barra de progreso en la pantalla. Tras finalizar el proceso, se muestra el nombre del archivo comprimido que contiene los registros y su ubicación.

### Método de asistente con GUI

1. Descargue la herramienta de soporte de BEST desde los enlaces correspondientes que se indican a continuación:
  - Para el sistema operativo Windows de 32 bits, haga clic [aquí](#).
  - Para el sistema operativo Windows de 64 bits, haga clic [aquí](#).
2. Siga las instrucciones de la pantalla para ejecutar la herramienta de soporte. Puede encontrar el archivo de salida en el Escritorio como un archivo comprimido con el siguiente nombre:  
BDST\_[nombredeequipo]\_[fechaactual].

### Enviar el archivo de registro

Para enviar el registro de la herramienta de soporte, según el método utilizado, siga los pasos que se exponen a continuación:

Si ha utilizado la línea de comandos:

1. Acceda a C:\Windows\Temp y busque el archivo comprimido denominado ST\_[nombredeequipo]\_[fechaactual].
2. Dentro del archivo comprimido, abra el archivo `problem.txt`.
3. Indique los datos necesarios en el archivo.
4. Adjunte el archivo comprimido a su ticket de soporte para proceder a la resolución del problema.

Si ha utilizado el asistente con GUI:

1. Acceda al Escritorio y busque el archivo comprimido denominado BDST\_[nombredeequipo]\_[fechaactual].
2. Adjunte el archivo comprimido a su ticket de soporte para proceder a la resolución del problema.

### 8.3.2. Uso de la herramienta de soporte en sistemas operativos Linux

En el caso de los sistemas operativos Linux, la herramienta de soporte va integrada con el agente de seguridad de Bitdefender.

Para recopilar información del sistema Linux mediante la herramienta de soporte, ejecute el siguiente comando:

```
# /opt/BitDefender/bin/bdconfigure
```

con las siguientes opciones disponibles:

- `--help` para obtener una lista con todos los comandos de la herramienta de soporte
- `enablelogs` para activar los registros del módulo de comunicaciones y del producto (todos los servicios se reiniciarán automáticamente)
- `enablelogs` para desactivar los registros del módulo de comunicación y del producto (todos los servicios se reiniciarán automáticamente)
- `deliverall` para crear:
  - Un archivo comprimido que contiene los registros de instalación, depositado en la carpeta `/var/log/BitDefender` con el siguiente formato: `bitdefender_nombreMáquina_hora.tar.gz`.

Una vez creado el archivo comprimido:

1. Se le preguntará si desea desactivar los registros. De ser necesario, los servicios se reiniciarán automáticamente.
  2. Se le preguntará si desea eliminar los registros.
- `deliverall -default` proporciona la misma información que en la opción anterior, pero se adoptarán las acciones por defecto para los registros, sin preguntar al usuario (los registros se desactivan y se eliminan).

También puede ejecutar el comando `/bdconfigure` directamente desde el paquete BEST (completo o downloader) sin tener el producto instalado.

Para informar de un problema de GravityZone que afecte a los sistemas Linux, siga los siguientes pasos, usando las opciones descritas anteriormente:

1. Active los registros del módulo de comunicaciones y del producto.
2. Trate de reproducir el problema.
3. Desactive los registros.
4. Cree el archivo comprimido con los registros.
5. Abra un ticket de soporte de correo electrónico mediante el formulario disponible en la página **Ayuda y soporte** de Control Center, con una descripción del problema y adjuntando el archivo comprimido de los registros.

La herramienta de soporte para Linux ofrece la siguiente información:

- Las carpetas `etc`, `var/log`, `/var/crash` (si existe) y `var/epag` de `/opt/BitDefender`, que contienen los ajustes y registros de Bitdefender
- El archivo `/var/log/BitDefender/bdinstall.log`, que contiene la información sobre la instalación
- El archivo `Network.txt`, que contiene los ajustes de red y la información de conectividad de la máquina
- El archivo `product.txt`, que incluye el contenido de todos los archivos `update.txt` de `/opt/BitDefender/var/lib/scan` y una lista recursiva completa de todos los archivos de `/opt/BitDefender`.
- El archivo `system.txt`, que contiene información general del sistema (versiones del kernel y de la distribución, RAM disponible y espacio libre en el disco duro)
- El archivo `users.txt`, que contiene información sobre el usuario
- Otra información referente al producto en relación con el sistema, como por ejemplo las conexiones externas de los procesos y el uso de la CPU
- Registros del sistema.

### 8.3.3. Uso de la herramienta de soporte en sistemas operativos Mac

Para enviar una solicitud al equipo de soporte técnico de Bitdefender, ha de proporcionar lo siguiente:

- Una descripción detallada del problema que se ha encontrado.
- Una captura de pantalla (si procede) del mensaje de error exacto que aparece.
- El registro de la herramienta de soporte.

Para obtener información del sistema Mac mediante la herramienta de soporte:

1. Descargue el [archivo ZIP](#) que contiene la herramienta de soporte.
2. Extraiga el archivo **BDProfiler.tool** del archivo comprimido.
3. Abra una ventana de Terminal.
4. Acceda a la ubicación del archivo **BDProfiler.tool**.

Por ejemplo:

```
cd /Users/Bitdefender/Desktop;
```

5. Dote al archivo de permisos de ejecución:

```
chmod +x BDProfiler.tool;
```

6. Ejecute la herramienta.

Por ejemplo:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Pulse **Y** e introduzca la contraseña cuando se le pida que proporcione la contraseña del administrador.

Espere un par de minutos a que la herramienta acabe de generar el registro. Hallará el archivo comprimido resultante (**Bitdefenderprofile\_output.zip**) en su escritorio.

## 8.4. Información de contacto

La eficiente comunicación es la clave para un negocio con éxito. Durante los últimos 15 años, Bitdefender se ha forjado una reputación incuestionable de lucha constante para mejorar la comunicación y así aumentar las expectativas de nuestros clientes y partners. Por favor no dude en contactar con nosotros.

### 8.4.1. Direcciones

Departamento de ventas: [enterprisesales@bitdefender.com](mailto:enterprisesales@bitdefender.com)  
Centro de soporte: <http://www.bitdefender.com/support/business.html>  
Documentación: [gravityzone-docs@bitdefender.com](http://gravityzone-docs@bitdefender.com)  
Distribuidores locales: <http://www.bitdefender.es/partners>  
Programa de Partners: [partners@bitdefender.com](mailto:partners@bitdefender.com)  
Relaciones con la Prensa: [prensa@bitdefender.es](mailto:prensa@bitdefender.es)  
Envío de virus: [virus\\_submission@bitdefender.com](mailto:virus_submission@bitdefender.com)  
Envío de Spam: [spam\\_submission@bitdefender.com](mailto:spam_submission@bitdefender.com)  
Notificar abuso: [abuse@bitdefender.com](mailto:abuse@bitdefender.com)  
Sitio Web: <http://www.bitdefender.com>

### 8.4.2. Distribuidor Local

Los distribuidores locales de Bitdefender están preparados para responder a cualquier pregunta relacionada con su área, tanto a nivel comercial como en otras áreas.

Para encontrar un distribuidor de Bitdefender en su país:

1. Visite <http://www.bitdefender.es/partners>.
2. Ir a **Localizador de Partner**.
3. La información de contacto de los distribuidores locales de Bitdefender debería mostrarse automáticamente. Si esto no sucede, seleccione el país en el que reside para ver la información.
4. Si no encuentra un distribuidor Bitdefender en su país, no dude en contactar con nosotros por correo en [enterprisesales@bitdefender.com](mailto:enterprisesales@bitdefender.com).

### 8.4.3. Oficinas de Bitdefender

Las oficinas de Bitdefender están listas para responder a cualquier pregunta relativa a sus áreas de acción, tanto a nivel comercial como en otros asuntos. Sus direcciones y contactos están listados a continuación.

#### Estados Unidos

**Bitdefender, LLC**

PO Box 667588

Pompano Beach, FL 33066

United States

Teléfono (comercial&soporte técnico): 1-954-776-6262

Comercial: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Web: <http://www.bitdefender.com>

Centro de soporte: <http://www.bitdefender.com/support/business.html>

#### Francia

**Bitdefender**

49, Rue de la Vanne

92120 Montrouge

Fax: +33 (0)1 47 35 07 09

Teléfono: +33 (0)1 47 35 72 73

Correo: [b2b@bitdefender.fr](mailto:b2b@bitdefender.fr)

Página web: <http://www.bitdefender.fr>

Centro de soporte: <http://www.bitdefender.fr/support/business.html>

#### España

**Bitdefender España, S.L.U.**

Avda. Diagonal, 357, 1º 1ª

08037 Barcelona

España

Fax: (+34) 93 217 91 28

Tel (oficina&comercial): (+34) 93 218 96 15

Teléfono (soporte técnico): (+34) 93 502 69 10

Comercial: [comercial@bitdefender.es](mailto:comercial@bitdefender.es)

Página web: <http://www.bitdefender.es>

Centro de soporte: <http://www.bitdefender.es/support/business.html>



## Alemania

### Bitdefender GmbH

Technologiezentrum Schwerte

Lohbachstrasse 12

D-58239 Schwerte

Deutschland

Tel (oficina&comercial): +49 (0) 2304 94 51 60

Teléfono (soporte técnico): +49 (0) 231 98 92 80 16

Comercial: [firmenkunden@Bitdefender.de](mailto:firmenkunden@Bitdefender.de)

Página web: <http://www.bitdefender.de>

Centro de soporte: <http://www.bitdefender.de/support/business.html>

## Reino Unido e Irlanda

Genesis Centre Innovation Way

Stoke-on-Trent, Staffordshire

ST6 4BF

UK

Teléfono (comercial&soporte técnico): (+44) 203 695 3415

Correo: [info@bitdefender.co.uk](mailto:info@bitdefender.co.uk)

Comercial: [sales@bitdefender.co.uk](mailto:sales@bitdefender.co.uk)

Página web: <http://www.bitdefender.co.uk>

Centro de soporte: <http://www.bitdefender.co.uk/support/business.html>

## Rumania

### BITDEFENDER SRL

rsOrhideea Towe

15A Orhideelor Street

060071 Bucharest, Sector 6

Fax: +40 21 2641799

Teléfono (comercial&soporte técnico): +40 21 2063470

Comercial: [sales@bitdefender.ro](mailto:sales@bitdefender.ro)

Página web: <http://www.bitdefender.ro>

Centro de soporte: <http://www.bitdefender.ro/support/business.html>

## Emiratos Árabes Unidos

### Bitdefender FZ-LLC

Dubai Internet City, Building 17

Office # 160

Dubai, UAE

Teléfono (comercial&soporte técnico): 00971-4-4588935 / 00971-4-4589186

Fax: 00971-4-44565047

Comercial: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Web: <http://www.bitdefender.com>

Centro de soporte: <http://www.bitdefender.com/support/business.html>

## A. Apéndices

### A.1. Tipos de archivo compatibles

Los motores de análisis antimalware incluidos en las soluciones de seguridad de Bitdefender pueden analizar todos los tipos de archivo que puedan contener amenazas. La lista siguiente incluye los tipos de archivo que se analizan más comúnmente.

{\*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;



xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;  
xsn; xtp; xz; z; zip; zl?; zoo