



Bitdefender® ENTERPRISE

**SMALL OFFICE
SECURITY**
Guía de inicio rápido >>

Small Office Security

Guía de inicio rápido

fecha de publicación 2015.01.06

Copyright© 2015 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 en críticas sólo puede ser posible 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.

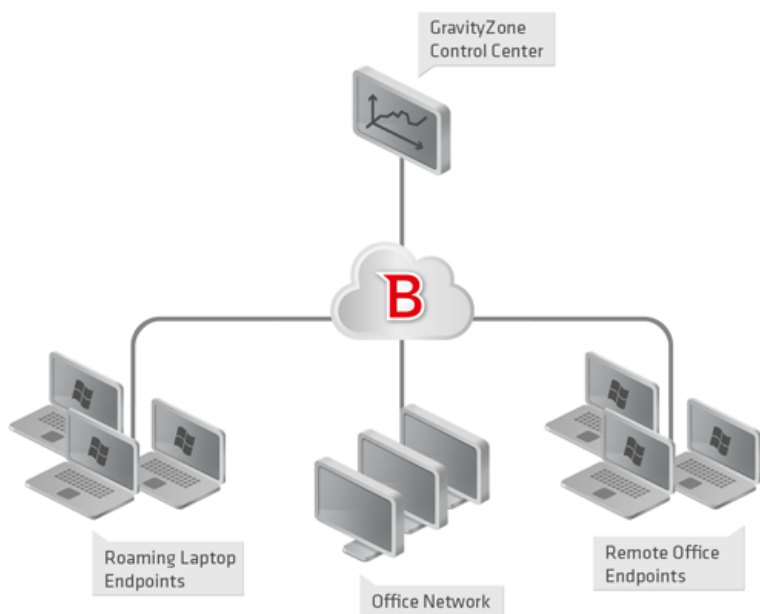


Tabla de contenidos

1. Acerca de Small Office Security	1
2. Iniciando	3
2.1. Conectar a Control Center	3
2.2. Control Center en resumen	4
2.2.1. Descripción general de Control Center	4
2.2.2. Datos de tablas	5
2.2.3. Barras de herramientas de acción	6
2.2.4. Menú Contextual	7
2.3. Gestionar su cuenta	7
2.4. Administración de su empresa	8
2.5. Cambiar la Contraseña de Inicio de Sesión	10
3. Administración de Licencias	12
3.1. Activar una licencia	12
3.2. Comprobar los detalles de licencia actuales	13
4. Instalación y configuración	15
4.1. Preparándose para la Instalación	15
4.2. Instalación del servicio en los equipos	16
4.2.1. Instalación local	17
4.2.2. Instalación remota	20
4.3. Organización de los equipos (opcional)	25
4.4. Creación y asignación de una política de seguridad	26
5. Estado de Monitorización de Seguridad	30
6. Analizar equipos administrados	32
7. Obtener Ayuda	34
A. Requisitos	35
A.1. Requisitos de Security for Endpoints	35
A.1.1. Sistemas operativos soportados	35
A.1.2. Requisitos de Hardware	36
A.1.3. Navegadores soportados	36
A.1.4. Puertos de comunicación de Small Office Security	37
A.2. Cómo funciona la detección de red	37
A.2.1. Más sobre el servicio Microsoft Computer Browser	38
A.2.2. Requisitos de descubrimiento de red	39

1. Acerca de Small Office Security

Small Office Security es un servicio de protección contra malware basado en la nube desarrollado por Bitdefender para equipos que ejecutan sistemas operativos de Microsoft Windows y Macintosh. Utiliza un modelo centralizado de implementación múltiple de software como servicio adecuado para clientes corporativos, al tiempo que se apoya en tecnología de protección comprobadas en el campo del malware desarrolladas por Bitdefender para el mercado de consumo.



Architecture Small Office Security

El servicio de seguridad es hospedado en la nube pública de Bitdefender. Los suscriptores tienen acceso a una interfaz de administración basada en la web llamada **Control Center**. Desde esta interfaz, los administradores pueden remotamente instalar y administrar la protección contra malware en todos sus equipos basados en Windows y Macintosh como: servidores y estaciones de trabajo dentro de la red interna, puntos finales portátiles itinerantes o puntos finales de oficina remotos.

Una aplicación local llamada **Endpoint Security** se instala en cada equipo protegido. Los usuarios locales tienen visibilidad limitada y acceso de solo lectura a los ajustes de seguridad,

que se administran de manera central por el administrador desde la Control Center; mientras que el análisis, actualización y los cambios de configuración se realizan normalmente en segundo plano.

2. Iniciando

Security for Endpoints puede configurarse y administrarse utilizando Control Center, una interfaz basada en web alojada en Bitdefender.

Tras el registro para la versión de evaluación o la adquisición del servicio, recibirá un e-mail del Servicio de registro de Bitdefender. Este correo contiene su información de inicio de sesión.

2.1. Conectar a Control Center

El acceso a Control Center se realiza a través de las cuentas de usuario. Recibirá su información de inicio de sesión por correo una vez que se haya creado su cuenta.

Requisitos:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Resolución de pantalla recomendada: 1024x768 o superior

Para conectarse a Control Center:

1. Abra su navegador Web.
2. Acceda a la siguiente dirección: <https://gravityzone.bitdefender.com>
3. Escriba la dirección de correo y contraseña de su cuenta.
4. Haga clic en **Inicio de sesión**.

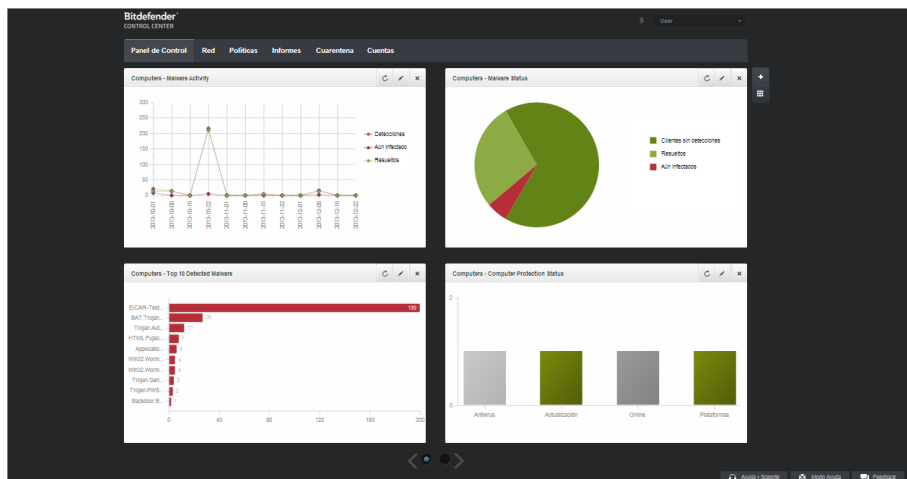


Nota

Si ha olvidado su contraseña, utilice el enlace de recuperación de contraseña para recibir una nueva. Debe proporcionar la dirección de correo de su cuenta.

2.2. Control Center en resumen

Control Center está organizada para permitir el acceso fácil a todas las funciones. Utilice la barra de menú en el área superior para navegar por la consola. Las características disponibles dependen del tipo de usuario que accede a la consola.



el Panel de control

2.2.1. Descripción general de Control Center

Los usuarios con rol de administrador de empresa tienen todos los privilegios para la configuración de Control Center y los ajustes de seguridad de red, mientras que los usuarios con rol de administrador tienen acceso a las características de seguridad de red, incluyendo la administración de usuarios.

En función de su rol, los administradores de Small Office Security pueden acceder a las siguientes secciones desde la barra de menús:

Panel de Control

Visualice tablas de fácil lectura que proporcionan información clave sobre seguridad referente a su red.

Red

Instalar protección, aplicar políticas para gestionar las opciones de seguridad, ejecutar tareas de forma remota y crear informes rápidos.

Políticas

Crear y administrar las políticas de seguridad.

Informes

Conseguir informes de seguridad relativos a los equipos cliente administrados.

Cuarentena

Administrar de forma remota los archivos en cuarentena.


Cuentas

Administrar el acceso a Control Center para otros empleados de la empresa.



Nota

Este menú solo está disponible para usuarios con privilegios de Administración de usuarios.

Por otra parte, en la esquina superior derecha de la consola, el icono  **Notificaciones** proporciona acceso fácil a los mensajes de notificación y también a la página **Notificaciones**.

Al apuntar sobre su nombre en la esquina superior derecha de la consola, aparecen las siguientes opciones disponibles.

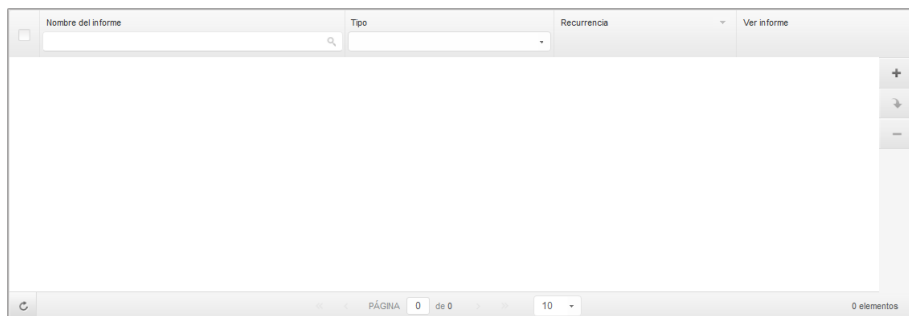
- **Mi cuenta.** Haga clic en esta opción para gestionar sus detalles de la cuenta y las preferencias.
- **Mi Empresa.** Haga clic en esta opción para gestionar la información de su cuenta de empresa y sus preferencias.
- **Administrador de Credenciales.** Haga clic en esta opción para añadir y administrar las credenciales de autenticación necesarias para tareas de instalación remotas.
- **Finalizar Sesión.** Haga clic en esta opción para cerrar la sesión de su cuenta.

En la esquina inferior derecha de la consola están a su disposición los siguientes enlaces:

- **Ayuda y soporte.** Haga clic en este botón para obtener ayuda e información de soporte.
- **Modo Ayuda.** Haga clic en este botón para habilitar una función de ayuda que proporciona tooltips cuando sitúa el ratón sobre los elementos de Control Center. Hallará información útil referente a las características de Control Center.
- **Feedback.** Haga clic en este botón para mostrar un formulario que le permitirá escribir y enviar sus comentarios acerca de su experiencia con Small Office Security.

2.2.2. Datos de tablas

Las tablas se usan frecuentemente en la consola para organizar los datos en un formato más fácil de usar.



La página de Informes - Tabla de informes

Navegar por las páginas

Las tablas con más de 10 entradas se distribuyen en varias páginas. Por omisión, solamente se muestran 10 entradas por página. Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla. Puede cambiar el número de entradas mostradas en una página seleccionando una opción diferente desde el menú junto a los botones de navegación.

Buscar entradas específicas


Para encontrar fácilmente entradas específicas, utilice los cuadros de búsqueda disponibles bajo los encabezados de las columnas.

Introduzca el término a buscar en el campo correspondiente. Los elementos coincidentes se muestran en la tabla según escribe. Para restablecer el contenido de la tabla, vacíe los campos de búsqueda.

Ordenar datos

Para ordenar datos según una columna específica, haga clic en el encabezado de la columna. Haga clic en el encabezado de la columna para invertir el orden de clasificación.

Actualizar los datos de la tabla

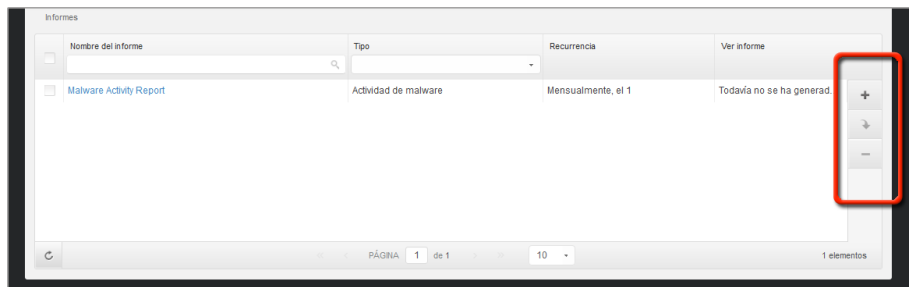
Para asegurarse de que la consola muestra la última información, haga clic en el botón  **Actualizar** en la esquina inferior izquierda de la tabla.

2.2.3. Barras de herramientas de acción

Dentro de Control Center, las barras de herramientas de acción le permiten realizar operaciones específicas que pertenecen a la sección en la que se encuentra. Cada barra de herramientas consiste en un conjunto de iconos que normalmente se colocan en el lateral

derecho de la tabla. Por ejemplo, la barra de herramientas de acción en la sección **Informes** le permite realizar las siguientes operaciones:

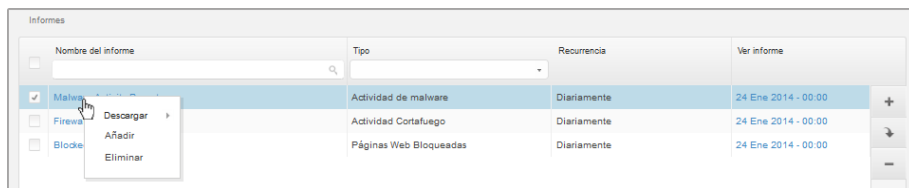
- Crear un nuevo informe.
- Descargar informes generados por un informe programado.
- Eliminar un informe programado.



La página de Informes - Barras de herramientas de acción

2.2.4. Menú Contextual

Desde el menú de contexto también se puede acceder a los comandos de la barra de herramientas. Haga clic con el botón derecho en la sección del Centro de control que esté utilizando y seleccione el comando que precise de la lista disponible.

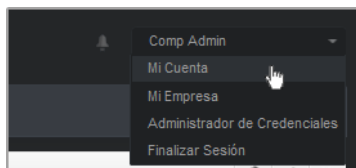


La página de Informes - Menú contextual

2.3. Gestionar su cuenta

Para consultar o cambiar sus detalles de cuenta y configuración:

1. Apunte a su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi cuenta**.



El menú de Cuenta de usuario

2. Modifique o actualice sus detalles de cuenta en **Detalles de cuenta**.
 - **Nombre y apellidos.** Introduzca su nombre completo.
 - **Correo.** Esta es su dirección de correo de contacto e inicio de sesión. Los informes y notificaciones de seguridad importantes se envían a esta dirección. Las notificaciones de correo se envían automáticamente siempre que se detectan situaciones de riesgo importantes en la red.
 - **Contraseña.** Un enlace **Cambiar contraseña** le permite cambiar su contraseña de inicio de sesión.
3. Configure las opciones de cuenta según sus preferencias en **Configuración**.
 - **Zona horaria.** Elija en el menú la zona horaria de la cuenta. La consola mostrará la información de la hora de acuerdo con la zona horaria seleccionada.
 - **Idioma.** Elija en el menú el idioma de visualización de la consola.
 - **Tiempo de espera de sesión.** Seleccione el intervalo de tiempo de inactividad antes de que expire su sesión de usuario.
4. Haga clic en **Guardar** para aplicar los cambios.



Nota

No puede eliminar su propia cuenta.

2.4. Administración de su empresa

Como usuario con rol de Administrador de empresa, puede comprobar o modificar los datos de su empresa y la configuración de la licencia:

1. Señale su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi empresa**.

Detalles de la empresa

Nombre Empresa:

Direcciones:

ID:

Teléfono:

Logotipo: El logotipo debe ser de 200x30 px, y estar en formato png o jpg

Permitir a otras empresas administrar la seguridad de esta empresa

Licencia

Número de Serie:

Fecha de caducidad: 30 Jun 2019
Usado: 19
Disponible para instalar: 313
Total: 333

Bitdefender Partner

Nombre Empresa:

ID:

Direcciones:

Teléfono:

Vincular esta empresa a MyBitdefender (opcional)

Mi página de empresa

2. En **Detalles de la empresa**, introduzca la información de su empresa, como por ejemplo el nombre de la empresa, la dirección y el teléfono.
3. Puede cambiar el logotipo que aparece en Control Center y también en los informes de su empresa y en las notificaciones de correo electrónico como se indica a continuación:
 - Haga clic en **Cambiar** para buscar el logotipo en su equipo. El formato de archivo de imagen debe ser .png o .jpg y el tamaño de la imagen ha de ser 200x30 píxeles.
 - Haga clic en **Predeterminada** para borrar la imagen y restaurar la proporcionada por Bitdefender.
4. Por defecto, su empresa puede ser administrada por las cuentas de partner de otras empresas que puedan tener a la suya en su Bitdefender Control Center. Puede bloquear el acceso de esas empresas a su red deshabilitando la opción **Permitir a otras empresas administrar la seguridad de esta empresa**. Una vez hecho esto, su red ya no será visible en la Control Center de otras empresas y ya no podrán administrar su suscripción.
5. Puede consultar y modificar los detalles de su licencia en la sección **Licencia**.
 - Para añadir una nueva clave de licencia:
 - a. En el **menú Tipo**, seleccione un tipo de suscripción de **licencia**.

- b. Introduzca la licencia en el campo **Clave de licencia**.
 - c. Haga clic en el botón **Comprobar** y espere a que Control Center recupere la información acerca de la clave de licencia introducida.
- Para verificar los detalles de su clave de licencia, consulte la información que se muestra debajo de la clave de licencia:
 - **Fecha de caducidad**: la fecha hasta la cual se puede utilizar la clave de licencia.
 - **Utilizado**: el número de puestos utilizados de la cantidad total de puestos de la clave de licencia. Un puesto de licencia se utiliza cuando se ha instalado el cliente de Bitdefender en un punto final de la red bajo su administración.
 - **Disponible para instalar**: el número de puestos libres de la cantidad total de puestos de un grupo de licencias mensuales (excluyendo los puestos utilizados).
 - **Total**: el número total de puestos de licencia disponibles para su suscripción.
6. En **Partner de Bitdefender** puede encontrar información acerca de su empresa proveedora de servicios.

Para cambiar su proveedor de servicios administrados:

 - a. Haga clic en el botón **Cambiar**.
 - b. Introduzca el ID de empresa del partner en el campo **ID del partner**.



Nota

Todas las empresas puede encontrar su ID en la página **Mi empresa**. Una vez que haya llegado a un acuerdo con una empresa partner, su representante debe proporcionarle su ID del Control Center.

- c. Haga clic en **Guardar**.

Una vez hecho esto, su empresa se traslada automáticamente de la Control Center del partner anterior a la del nuevo.
7. Opcionalmente, puede vincular su empresa a su cuenta de MyBitdefender mediante los campos proporcionados.
8. Haga clic en **Guardar** para aplicar los cambios.

2.5. Cambiar la Contraseña de Inicio de Sesión

Tras haberse creado su cuenta recibirá un correo electrónico con las credenciales de inicio de sesión.

- Cambie la contraseña de inicio de sesión por defecto la primera vez que visite Control Center.
- Cambie periódicamente su contraseña de inicio de sesión.

Para cambiar la contraseña de inicio de sesión:

1. Apunte a su nombre de usuario en la esquina superior derecha de la consola y seleccione **Mi cuenta**.
2. En **Detalles de cuenta**, haga clic en **Cambiar contraseña**.
3. Escriba su contraseña actual y la nueva contraseña en los campos correspondientes.
4. Haga clic en **Guardar** para aplicar los cambios.

3. Administración de Licencias

El servicio de seguridad proporcionado por Small Office Security requiere una clave de licencia válida.

Puede probar gratuitamente Small Office Security 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 el servicio, deberá optar por un plan de suscripción de pago y realizar la compra antes de que finalice el periodo de prueba.

Existen dos maneras de suscribirse al servicio:

- Suscribirse a través de un reseller de Bitdefender. Nuestros distribuidores le asistirán con toda la información que necesite y le ayudarán a elegir el mejor plan de suscripción para usted. Algunos distribuidores ofrecen servicios de valor añadido, como soporte premium, y otros pueden proporcionarle un servicio totalmente gestionado.

Para encontrar un reseller 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 partners 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 reseller Bitdefender en su país, no dude en contactar con nosotros por correo en comercial@bitdefender.es.
- Suscribirse desde el [sitio Web de Bitdefender](#).

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 Small Office Security puede ser administrado tanto internamente por su empresa como externamente por el proveedor de servicios de seguridad.

3.1. Activar una licencia

Cuando adquiere un plan de suscripción pagado por primera vez, se le expide una clave de licencia. La suscripción a Small Office Security 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 puntos finales encima de otra de 100 puntos finales NO dará como resultado una suscripción de 110 puntos finales. Al contrario, reducirá el número de puntos finales 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 de cliente.
2. Sitúe el cursor en su cuenta de usuario en la esquina superior derecha de la consola y seleccione **Mi empresa**.



Nota

Este privilegio es privativo de las cuentas de administrador de empresa.

3. Compruebe la información acerca de la licencia actual en la sección **Licencia**.
4. En el **menú Tipo**, seleccione un tipo de suscripción de **licencia**.
5. Introduzca la licencia en el campo **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. Haga clic en **Guardar**.

3.2. Comprobar los detalles de licencia actuales

Para comprobar el estado de su suscripción:

1. Inicie sesión en Control Center con su dirección de e-mail y contraseña recibidos por correo electrónico.
2. Sitúe el cursor en su cuenta de usuario en la esquina superior derecha de la consola y seleccione **Mi empresa**.



Nota

Este privilegio es privativo de las cuentas de administrador de empresa.

3. Compruebe la información acerca de la licencia actual en la sección **Licencia**:
 - **Fecha de caducidad**: la fecha hasta la cual se puede utilizar la clave de licencia.
 - **Utilizado**: el número de puestos utilizados de la cantidad total de puestos de la clave de licencia. Un puesto de licencia se utiliza cuando se ha instalado el cliente de Bitdefender en un punto final de la red bajo su administración.

- **Disponible para instalar:** el número de puestos libres de la cantidad total de puestos de un grupo de licencias mensuales (excluyendo los puestos utilizados).
 - **Total:** el número total de puestos de licencia disponibles para su suscripción.
4. Haga clic en **Guardar**.

4. Instalación y configuración

La instalación y configuración es bastante sencilla. Estos son los pasos principales:

1. [Paso 1 - Preparación para la instalación.](#)
2. [Paso 2 - Instalación del servicio en los equipos.](#)
3. [Paso 3 - Organización de los equipos en grupos \(opcional\).](#)
4. [Paso 4 - Creación y configuración de una política de seguridad.](#)

Para los dos primeros pasos se requiere información de inicio de sesión en el equipo. Los otros dos pasos se ejecutan desde Control Center.

4.1. Preparándose para la Instalación

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

1. Asegúrese de que los equipos cumplen los [requisitos de sistema mínimos](#). Para algunos equipos es posible que tenga que instalar el último service pack disponible o liberar espacio en disco. Configure una lista de equipos que no cumplan los requisitos necesarios para que pueda excluirlos de la administración.
2. Desinstale (no sólo desactive) cualquier antimalware, cortafuego o software de seguridad de su equipo. Ejecutar Endpoint Security simultáneamente con otro software de seguridad en un equipo puede afectar a su funcionamiento y causar serios problemas en el sistema.

Muchos de los programas de seguridad con los que Endpoint Security no es compatible, se detectan y eliminan automáticamente durante la instalación. Para más información y para ver la lista de software de seguridad detectado, consulte [este artículo de la base de conocimientos](#).



Importante

No es necesario preocuparse de las funciones de seguridad de Windows (Windows Defender, Windows Firewall), ya que se desactivan automáticamente antes de que se inicie la instalación.

3. La instalación requiere disponer de privilegios de administrador y acceso a Internet. Asegúrese de que tiene a mano las credenciales necesarias para todos los equipos.
4. Los equipos deben tener conexión con Control Center.

4.2. Instalación del servicio en los equipos

Security for Endpoints está indicado para estaciones de trabajo, portátiles y servidores que ejecuten Microsoft® Windows. Para proteger equipos con Security for Endpoints debe instalar Endpoint Security (el software cliente) en cada uno de ellos. Endpoint Security administra la protección en el equipo local. También se comunica con Control Center para recibir los comandos del administrador y enviar los resultados de sus acciones.

Puede instalar Endpoint Security con uno de los siguientes roles (disponibles en el asistente de instalación):

1. **Punto final**, cuando el equipo correspondiente es un punto final normal de la red.
2. **Endpoint Security Relay**, cuando otros puntos finales de la red utilizan el equipo en cuestión para comunicarse con Control Center. El rol Endpoint Security Relay instala Endpoint Security junto con un servidor de actualizaciones, que puede utilizarse para actualizar los demás clientes de la red. Los puntos finales de la misma red se pueden configurar mediante políticas para comunicarse con Control Center a través de uno o varios equipos con rol Endpoint Security Relay. Así, cuando un Endpoint Security Relay no está disponible, se pasa al siguiente para garantizar la comunicación del equipo con Control Center.



Aviso

- El primer equipo en que instale la protección ha de tener rol de Endpoint Security Relay, o no podrá implementar Endpoint Security en otros equipos de la red.
- El equipo con rol de Endpoint Security Relay debe estar encendido y conectado para que los clientes se comuniquen con Control Center.

Hay dos métodos de instalación:

- **Instalación local.** Descargue los paquetes de instalación de Control Center en cada equipo y luego ejecute la instalación de Endpoint Security localmente. Otra opción es descargar el paquete, guardarlo en un recurso compartido de red y enviar a los usuarios de la empresa invitaciones por correo electrónico con el enlace al paquete, pidiéndoles descargar e instalar la protección en sus equipos. La instalación local está guiada por un asistente.
- **Instalación remota.** Una vez que haya instalado localmente el primer cliente con rol de Endpoint Security Relay, pueden tardarse unos minutos en que el resto de equipos de la red aparezcan en Control Center. La protección de Security for Endpoints puede entonces instalarse remotamente desde la consola en otros equipos de la red. La instalación remota se ejecuta en segundo plano, sin que el usuario lo perciba.

Endpoint Security posee 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.

Por defecto, el idioma mostrado por la interfaz de usuario en los equipos protegidos se define en el momento de la instalación basándose en el idioma de su cuenta. Para instalar la interfaz de usuario en otro idioma en determinados equipos, puede crear un paquete de instalación y establecer el idioma preferido en las opciones de configuración del paquete. Para obtener más información sobre la creación de paquetes de instalación, consulte [“Crear paquetes de instalación de Endpoint Security”](#) (p. 17).

4.2.1. Instalación local

La instalación local requiere descargar desde Control Center y ejecutar el paquete de instalación en cada equipo objetivo. Puede crear distintos paquetes de instalación en función de los requisitos concretos de cada equipo (por ejemplo, la ruta de instalación o el idioma de la interfaz de usuario).

Crear paquetes de instalación de Endpoint Security

Para crear un paquete de instalación de Endpoint Security:

1. Conéctese e inicie sesión en Control Center usando su cuenta.
2. Vaya a la página **Red > Paquetes**.

Nombre	Idioma	Descripción	Estado
<input type="checkbox"/> Rly	English		Listo para descargar
<input type="checkbox"/> EPSr	English	company1	Listo para descargar

La página Paquetes

3. Haga clic en el botón **+ Añadir** del lateral derecho de la tabla. Aparecerá una nueva ventana de configuración.

Seguridad de puntos finales

Opciones

Avanzado

Detalles

Nombre: * EPS-ES

Descripción: Endpoint Security ES

General

Rol: Endpoint Security Relay

Empresa: Seleccionar empresa

Módulos a instalar:

Antimalware ⓘ

Cortafuegos ⓘ

Control de Contenido

Configuración

Idioma: Español

Analizar antes de la instalación

Usar ruta de instalación personalizada

Contraseña de desinstalación

Contraseña: Haga clic aquí para cambiarla

Confirmar contraseña: Por favor, vuelva a introducir

Endpoint Security de Bitdefender desinstalará automáticamente otros software de seguridad.

Siguinte > Cancelar

Crear paquetes Endpoint Security - Opciones

4. Escriba un nombre adecuado y una descripción para el paquete de instalación que quiere crear.
5. Seleccione el rol del equipo objetivo:
 - **Punto final.** Seleccione esta opción para crear el paquete para un punto final normal.
 - **Endpoint Security Relay.** Seleccione esta opción para crear el paquete para un punto final con rol Endpoint Security Relay. Endpoint Security Relay es un rol especial que instala un servidor de actualizaciones en el equipo objetivo junto con Endpoint Security. Éste puede utilizarse para actualizar los demás clientes de la red, reduciendo el uso de ancho de banda entre las máquinas clientes y Control Center.
6. Seleccione la empresa donde se utilizará el paquete de instalación.
7. Seleccione los módulos de protección que desea instalar.
8. En el campo **Idioma**, seleccione el idioma deseado para la interfaz del cliente.

9. Seleccione **Analizar antes de la instalación** si quiere estar seguro de que los equipos están limpios antes de instalar Endpoint Security en ellos. Se ejecutará un análisis rápido en la nube en los equipos correspondientes antes de empezar la instalación.
10. Endpoint Security se instala en los equipos seleccionados en el directorio de instalación predeterminado. Seleccione **Usar ruta de instalación personalizada** si desea instalar Endpoint Security 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. Haga clic en **Siguiente**.
13. Dependiendo del rol del paquete de instalación (punto final o Endpoint Security Relay), escoja la entidad a la que se conectarán periódicamente los equipos objetivo para actualizar el cliente:
 - **Bitdefender Cloud**, si desea actualizar los clientes directamente desde Internet.
 - **Endpoint Security Relay**, si desea conectar los puntos finales a un Endpoint Security Relay instalado en su red. Todos los equipos con rol de Endpoint Security Relay detectados en su red figurarán en la tabla que se muestra a continuación. Seleccione el Endpoint Security Relay que desee. Los puntos finales conectados se comunicarán con Control Center solo mediante el Endpoint Security Relay especificado.




Importante

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

14. Haga clic en **Guardar**.

El nuevo paquete de instalación aparecerá en la lista de paquetes de la empresa objetivo.

Descarga e instalación de Endpoint Security

1. Conéctese a <https://gravityzone.bitdefender.com/> utilizando su cuenta desde el equipo en el cual desee instalar la protección.
2. Vaya a la página **Red > Paquetes**.
3. Seleccione la empresa adecuada de la lista disponible bajo la cabecera de columna **Empresa**. Solo se mostrarán los paquetes disponibles para la empresa seleccionada.
4. Seleccione el paquete de instalación de Endpoint Security que desee descargar.
5. Haga clic en el botón  **Descargar** a la derecha 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.** El kit completo se utiliza para instalar la protección en los equipos sin conexión a Internet o con conexiones lentas. Descargue este archivo en un equipo conectado a Internet y distribúyalo a otros equipos usando un medio de almacenamiento externo o compartiéndolo en la red. Tenga en cuenta que hay dos versiones disponibles para Windows: una para sistemas de 32 bits y la otra para sistemas de 64 bits. Asegúrese de usar la versión correcta para el equipo donde instala.
6. Guarde el archivo en el equipo.
 7. Ejecutar el paquete de instalación.



Nota

Para que funcione la instalación, el paquete de instalación debe ejecutarse utilizando privilegios de administrador o desde una cuenta de administrador.

8. Siga las instrucciones que aparecen en la pantalla.

Una vez instalado Endpoint Security, el equipo se mostrará como administrado en Control Center (página **Red**) en unos minutos.

4.2.2. Instalación remota

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

Para facilitar la implementación, Security for Endpoints incluye un mecanismo automático de detección de redes que le permite detectar equipos en su red. Los equipos detectados se muestran como **equipos no administrados** en la página de **Red**.

Para habilitar la detección de redes y la instalación remota, debe tener Endpoint Security ya instalado en al menos un equipo en la red. Este equipo se utilizará para analizar la red e instalar Endpoint Security en los equipos no protegidos. Pueden tardarse unos minutos en que el resto de equipos de la red aparezcan en Control Center.

Requisitos de la instalación remota

Para que funcione el descubrimiento de red, deben cumplirse una serie de requisitos. Para saber más, consulte [“Cómo funciona la detección de red” \(p. 37\)](#).

Para que funcione la instalación remota:

- Cada equipo objetivo debe tener habilitados la compartición de recursos administrativos admin\$. Configure cada estación de trabajo objetivo para el uso compartido de archivos avanzado.
- Desactive temporalmente el control de cuentas de usuario para todos los equipos que ejecutan sistemas operativos Windows que incluyan esta característica de seguridad (Windows Vista, Windows 7, Windows Server 2008, etc.). Si los equipos están en un dominio, puede utilizar una política de grupo para desactivar el Control de Cuentas de Usuario de forma remota.
- Desactive o apague la protección del cortafuego en los equipos. Si los equipos están en un dominio, puede utilizar una política de grupo para desactivar el Firewall de Windows de forma remota.

Ejecución de tareas de instalación remota de Endpoint Security


Para ejecutar una tarea de instalación remota:

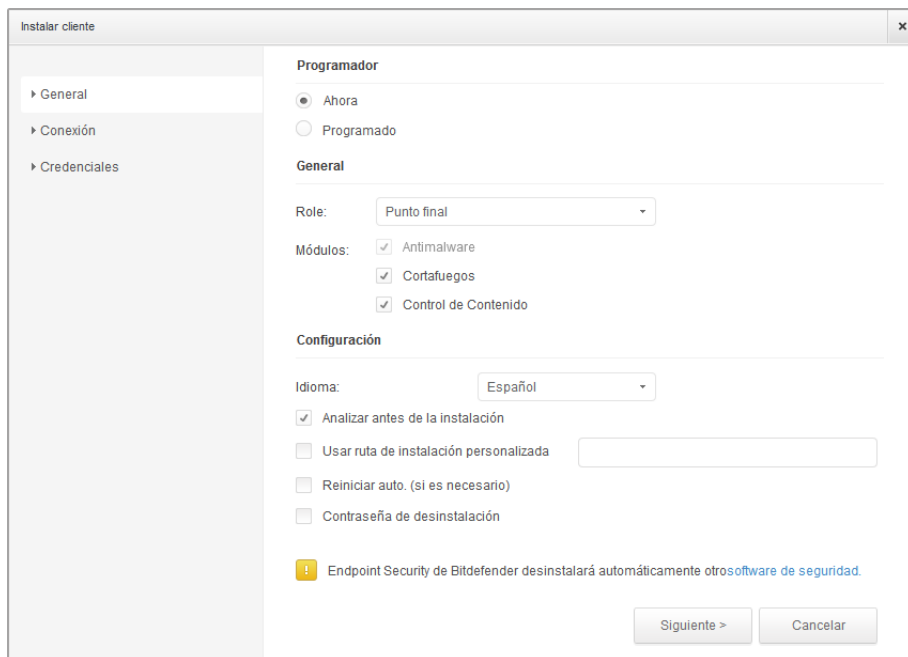
1. Conéctese e inicie sesión en Control Center.
2. Diríjase a la página **Red**.
3. Seleccione el grupo de red deseado en el panel de la izquierda. Las entidades contenidas en el grupo seleccionado se muestran en la tabla del panel lateral derecho.



Nota

Opcionalmente, puede aplicar filtros para mostrar únicamente los equipos no administrados. Haga clic en el botón **Filtros** y seleccione las siguientes opciones: **No administrados** de la categoría **Seguridad** y **Todos los elementos recursivamente** de la categoría **Profundidad**.

4. Seleccione las entidades (equipos o grupos de equipos) en las que desee instalar la protección.
5. Haga clic en el botón  **Tareas** del lateral derecho de la tabla y seleccione **Instalar cliente**. El asistente de **Instalar cliente** se está mostrando.



Instalación de Endpoint Security desde el menú Tareas

6. Configure las opciones de instalación:

- Programe 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.

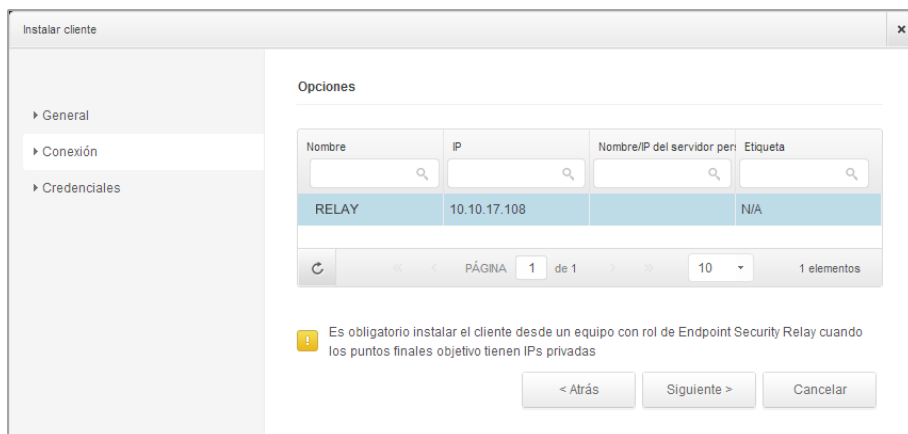


Nota

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.

- Seleccione los módulos de protección que desea instalar. Tenga en cuenta que sólo la protección antimalware está disponible para los sistemas operativos de servidor.
- En el campo **Idioma**, seleccione el idioma deseado para la interfaz del cliente.

- Seleccione **Analizar antes de la instalación** si quiere estar seguro de que los equipos están limpios antes de instalar Endpoint Security en ellos. Se ejecutará un análisis rápido en la nube en los equipos correspondientes antes de empezar la instalación.
- Endpoint Security se instala en los equipos seleccionados en el directorio de instalación predeterminado. Seleccione **Usar ruta de instalación personalizada** si desea instalar Endpoint Security 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.
- Durante la instalación silenciosa, se analiza el equipo en busca de malware. A veces es necesario un reinicio del sistema para completar la eliminación del malware. Seleccione **Reiniciar automáticamente (si es necesario)** para asegurarse de que el malware detectado es eliminado por completo antes de la instalación. De lo contrario la instalación puede fallar.
- 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.
- Haga clic en **Siguiente**.
- La pestaña **Conexión** muestra la lista de puntos finales con rol de Endpoint Security Relay instalados en la red. Cada nuevo cliente debe estar conectado por lo menos a un Endpoint Security Relay de la misma red, que actuará como Servidor de actualizaciones y de comunicaciones. Seleccione el Endpoint Security Relay que quiere vincular a los nuevos clientes.



7. Haga clic en **Siguiente**.

8. En la sección **Administrador de credenciales**, especifique las credenciales administrativas necesarias para la autenticación remota en los puntos finales seleccionados. Puede añadir las credenciales requeridas escribiendo el usuario y contraseña de 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](#).



Nota

Se mostrará un mensaje de advertencia si todavía no ha seleccionado credenciales. Este paso es obligatorio para instalar de forma remota Endpoint Security en los equipos.

<input checked="" type="checkbox"/>	Usuario	Contraseña	Descripción	Acción
<input type="checkbox"/>	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input data-bbox="938 719 960 743" type="button" value="+"/>
<input checked="" type="checkbox"/>	user@domain.com	*****		
<input checked="" type="checkbox"/>	domainuser	*****		

El usuario deberá estar en la forma DOMINIO\NOMBRE DE USUARIO, donde DOMINIO es el nombre NetBios del dominio.

Para añadir las credenciales del sistema operativo requeridas:

- Escriba el nombre de usuario y contraseña de una cuenta de administrador para cada uno de los sistemas operativos objetivo en los campos correspondientes. 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 convenciones de Windows cuando introduzca el nombre de una cuenta de usuario de dominio, por ejemplo, `usuario@dominio.com` o `dominio\usuario`. Para asegurarse de que las credenciales introducidas funcionarán, añádalas en ambas formas (`usuario@dominio.com` y `dominio\usuario`).



Nota

Las credenciales especificadas se guardan automáticamente en su Gestor de credenciales para que no tenga que volver a introducirlas la próxima vez.

- b. Haga clic en el botón * **Añadir**. La cuenta se añade a la lista de credenciales.
 - c. Marque las casillas de verificación correspondientes a la cuenta que desea usar.
9. Haga clic en **Guardar**. Aparecerá un mensaje de confirmación.

Puede ver y administrar las tareas en la página **Red > Tareas**.

4.3. Organización de los equipos (opcional)

Las redes de la empresa se muestran en el panel izquierdo de la página **Red**. Existe un grupo raíz predeterminado para cada una de sus empresas. Todos sus equipos protegidos o detectados se sitúan automáticamente en este grupo.

Si administra un número grande de equipos (diez o más), probablemente necesite organizarlos en grupos. Organizar los equipos en grupos le ayuda a administrarlos más eficientemente. La ventaja principal es que puede usar las políticas de grupo para cumplir distintos requisitos de seguridad.

Puede organizar los equipos creando grupos bajo el grupo por defecto de la empresa y moviendo los equipos al grupo adecuado.

Antes de empezar a crear grupos, piense en las razones por las que los necesita y elabore un esquema de agrupación. Por ejemplo, puede agrupar los equipos basándose en uno o en una combinación de los siguientes criterios:

- Estructura de la organización (Ventas, Marketing, Control de calidad, Dirección, etc.).
- Necesidades de seguridad (equipos de escritorio, portátiles, servidores, etc.).
- Ubicación (sede central, oficinas locales, trabajadores remotos, oficinas domésticas, etc.).



Nota

- Los grupos creados pueden contener tanto equipos como otros grupos.
- Cuando selecciona un grupo en el panel del lado izquierdo, puede ver todos los equipos excepto los ubicados en subgrupos. Para ver todos los equipos incluidos en un grupo y en todos sus subgrupos, haga clic en el menú filtros localizado encima de la tabla y seleccione **Tipo > Equipos** y **Profundidad > Todos los elementos recursivamente**.

Para organizar la red del cliente en grupos:

1. Diríjase a la página **Red**.
2. En el panel de la izquierda, en **Empresas**, seleccione la empresa cliente que desee administrar.



Nota

Para empresas partner bajo su cuenta con privilegios de administración de redes, seleccione el grupo **Redes**.

3. Haga clic en el botón **+ Añadir grupo** en la parte superior del panel izquierdo.
4. Escriba un nombre descriptivo para el grupo y haga clic en **Aceptar**. El nuevo grupo se muestra bajo la empresa correspondiente.
5. Siga los pasos previos para crear grupos adicionales.
6. Mover equipos desde el grupo raíz al grupo adecuado:
 - a. Marque las casillas de verificación correspondientes a los equipos que quiere mover.
 - b. Arrastre y suelte su selección sobre el grupo deseado en el panel izquierdo.

4.4. Creación y asignación de una política de seguridad

Una vez instalada, la protección de Security for Endpoints puede configurarse y administrarse desde Control Center utilizando las políticas de seguridad. Una política especifica la configuración de seguridad a aplicar en los equipos objetivo.

Inmediatamente después de la instalación, se asigna a los equipos la política predeterminada, que está definida con las opciones de protección recomendadas. Para comprobar las opciones de protección predeterminadas, diríjase a la página **Políticas** y haga clic en el nombre de la política predeterminada. Puede cambiar los ajustes de protección como precise, y también configurar características de protección adicionales, creando y asignando políticas personalizadas.



Nota

No puede editar o borrar la política predeterminada. Sólo puede utilizarla como una plantilla para crear nuevas políticas.

Puede crear tantas políticas como precise en función de los requisitos de seguridad. Por ejemplo, puede configurar diferentes políticas para estaciones de trabajo, portátiles y servidores de oficina. Un enfoque distinto es crear políticas independientes para cada una de las redes de cliente.

Esto es lo que necesita saber sobre políticas:

- Las políticas se crean en la página **Políticas** y se asignan a puntos finales en la página **Red**.
- Los puntos finales solo pueden tener una política activa en cada momento.
- Las políticas se transfieren a los equipos objetivos inmediatamente una vez creadas o modificadas. La configuración debería aplicarse a los puntos finales en menos de un

minuto (siempre que estén conectados). Si un equipo está desconectado, la configuración se aplicará tan pronto como vuelva a conectarse.

- La política se aplica únicamente a los módulos de protección instalados. Tenga en cuenta que sólo la protección antimalware está disponible para los sistemas operativos de servidor.
- No puede editar políticas creadas por otros usuarios (a menos que los propietarios de la política lo permitan en los ajustes de la política), pero puede sobrescribirlas asignando a los elementos objetivos una política diferente.
- Los equipos de una cuenta de empresa se pueden administrar mediante políticas. Esto puede hacerlo tanto el administrador de la empresa como el partner que creó la cuenta. Las políticas creadas desde la cuenta de partner no se pueden modificar desde la cuenta de empresa.

Para crear una nueva política:

1. Diríjase a la página **Políticas**.
2. Haga clic en el botón **+ Añadir** del lateral derecho de la tabla. Este comando crea una nueva política empezando desde la plantilla de política predeterminada.
3. Escriba un nombre descriptivo para la política. Al elegir un nombre, considere el propósito y objetivo de la política.
4. A continuación, configure las opciones de la política. La configuración de seguridad predeterminada es recomendable para todas las situaciones.
5. Haga clic en **Guardar**. La nueva política se muestra en la tabla **Políticas**.

Una vez definidas las políticas necesarias en la sección **Políticas**, puede asignarlas a los elementos de red en la sección **Red**.

A todos los objetos de red se les asigna inicialmente la política predeterminada.



Nota

Solo puede asignar políticas que haya creado usted mismo. Para asignar una política creada por otro usuario, primero debe duplicarla en la página de **Políticas**.

Para asignar una política:

1. Diríjase a la página **Red**.
2. Marque la casilla de verificación del elemento de red deseado. Puede seleccionar uno o varios objetos solo del mismo nivel.
3. Haga clic en el botón **Asignar política** a la derecha de la tabla.



Nota

También puede hacer clic con el botón derecho en un grupo del árbol de red y elegir **Asignar política** en el menú contextual.

Se muestra la ventana **Asignación de política** :

Ajustes de asignación de políticas

4. Configure los ajustes de asignación de políticas para los objetos seleccionados:

- Consulte las asignaciones de políticas actuales para los objetos seleccionados en la tabla bajo la sección **Objetivos**.
- **Asignar la siguiente plantilla de política.** Seleccione esta opción para asignar a los objetos objetivo una política del menú mostrado a la derecha. Solo están disponibles en el menú las políticas creadas desde su cuenta de usuario.
- **Hereditado desde arriba.** Seleccione la opción **Heredar desde arriba** para asignar la política del grupo padre a los objetos de red seleccionados.
- **Forzar herencia de políticas para objetos.** De forma predeterminada cada objeto de red hereda la política del grupo padre. Si cambia la política del grupo, se verán afectados todos los hijos del mismo, excepto los miembros del grupo a los que haya asignado específicamente otra política.

Seleccione la opción **Forzar herencia de políticas para objetos** para aplicar la política escogida a un grupo, incluyendo a los hijos del mismo que tuvieran asignada una política diferente. En este caso, la tabla situada a continuación mostrará los hijos del grupo seleccionado que no heredan la política del grupo.

5. Haga clic en **Finalizar** para guardar y aplicar los cambios.

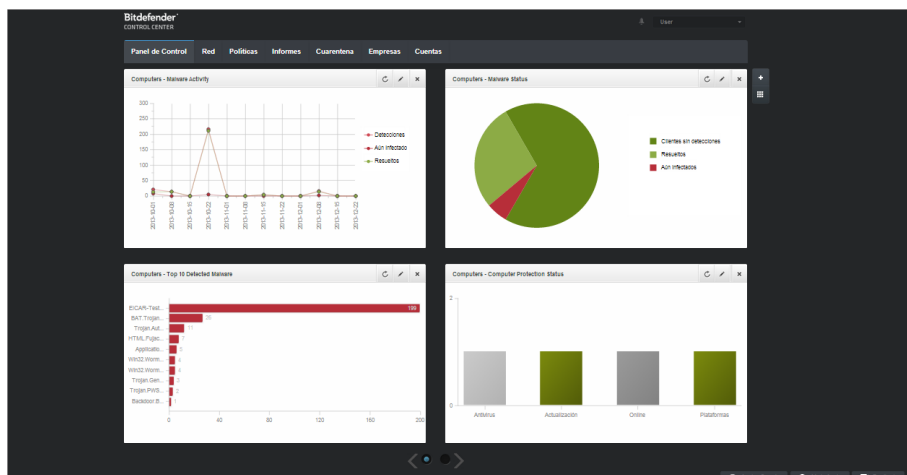
Las políticas se aplican a los elementos de red objetivos inmediatamente tras la edición de las asignaciones de la política o tras modificar sus ajustes. La configuración debería aplicarse a los elementos de red en menos de un minuto (siempre que estén conectados). Si un equipo

o elemento de red no está conectado, la configuración se aplicará tan pronto como vuelva a conectarse.

Para comprobar si se ha asignado la política correctamente, acceda a la página de **Red** y haga clic en el nombre del objeto que le interese para mostrar la ventana de **Detalles**. Consulte la sección de **Política** para ver el estado de la política actual. Si está en estado pendiente, la política no se ha aplicado todavía al objeto objetivo.

5. Estado de Monitorización de Seguridad

La principal herramienta de monitorización de Security for Endpoints es el panel de control de Control Center, una pantalla de visualización personalizable que le proporciona una visión general de su red.






el Panel de control

Compruebe regularmente la página **Panel de control** para ver información en tiempo real sobre el estado de seguridad de la red.

Los portlets del panel muestran diversa información de seguridad utilizando tablas de fácil lectura, permitiendo por ello una identificación rápida de cualquier problema que pudiera requerir su atención.

Esto es lo que necesita saber sobre la administración de su panel de control:

- Control Center viene con varios portlets de panel de control predefinidos. También puede añadir más portlets mediante el botón **+ Añadir portlet** de la derecha del panel de control.
- Cada portlet del panel incluye un informe detallado en segundo plano, accesible haciendo clic sobre el gráfico.


- La información mostrada por los portlets se refiere solo a los objetos de red de su cuenta. Puede personalizar la información mostrada en un portlet (tipo, intervalo de los informes, objetivos) haciendo clic en el icono  **Editar portlet** de su barra de título.
Por ejemplo, puede configurar portlets para mostrar información de una determinada empresa de su red.
- Puede eliminar fácilmente cualquier portlet haciendo clic en el icono  **Eliminar** en su barra de título. Una vez eliminado el portlet, ya no puede recuperarlo. Sin embargo, puede crear otro portlet exactamente con la misma configuración.
- Haga clic en los elementos de la leyenda, cuando existan, para ocultar o mostrar la variable correspondiente en la gráfica.
- Puede reorganizar los portlets del panel de control para que se adapten mejor a sus necesidades, haciendo clic en el botón  **Reorganizar portlets** de la derecha del panel de control. Luego, puede arrastrar y soltar los portlets en la posición deseada.
- Los portlets se muestran en grupos de cuatro. Utilice el control deslizante situado en la parte inferior de la página para navegar por los grupos de portlets.

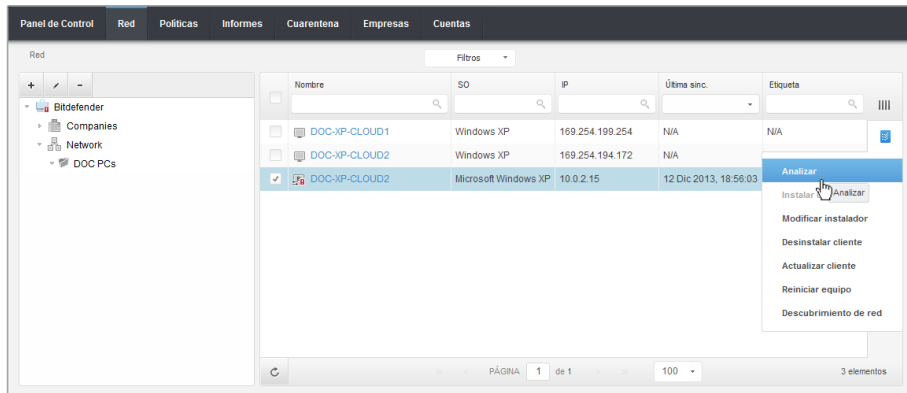
6. Analizar equipos administrados

Hay tres formas de analizar los equipos protegidos por Endpoint Security:

- El usuario registrado en el equipo puede iniciar un análisis desde la interfaz de usuario de Endpoint Security.
- Puede crear tareas de análisis programadas usando la política.
- Ejecute una tarea de análisis inmediata desde la consola.

Para ejecutar de forma remota una tarea de análisis en uno o varios equipos:

1. Diríjase a la página **Red**.
2. Seleccione el grupo de red deseado en el panel de la izquierda. Todos los equipos del grupo seleccionado se muestran en la tabla del panel lateral derecho.
3. Seleccione las entidades que desee que se analicen. Puede seleccionar determinados equipos administrados o todo un grupo.
4. Haga clic en el botón  **Tareas** del lateral derecho de la tabla y seleccione **Analizar**. Aparecerá una nueva ventana de configuración.



Tarea de análisis de equipos

5. En la pestaña **General**, seleccione el tipo de análisis del menú **Tipo**:

- **Quick Scan** busca el malware que se esté ejecutando en el sistema, sin llevar a cabo ninguna acción. Si se encuentra malware durante un análisis Quick Scan, debe ejecutar una tarea de análisis completo del sistema para eliminar el malware detectado.
- **Análisis completo** analiza el equipo por completo en busca de todo tipo de malware que pueda amenazar su seguridad, como virus, spyware, adware, rootkits y otros.

- **Análisis personalizado** le permite elegir las ubicaciones a analizar y configurar las opciones de análisis.
6. Haga clic en **Guardar** para crear la tarea de análisis. Aparecerá un mensaje de confirmación.

**Nota**

Una vez creada, la tarea de análisis se iniciará inmediatamente en los equipos conectados.

Si un equipo está desconectado, se analizará tan pronto como vuelva a conectarse.

7. Puede ver y administrar las tareas en la página **Red > Tareas**.

7. Obtener Ayuda

Para encontrar recursos de ayuda adicionales u obtener asistencia de Bitdefender:

- Haga clic en el enlace **Ayuda y soporte** en la esquina inferior derecha de Control Center.
- Acceda a nuestro [Centro de Soporte online](#).

Para abrir un ticket de soporte por correo electrónico, utilice [este formulario web](#).

A. Requisitos

A.1. Requisitos de Security for Endpoints

A.1.1. Sistemas operativos soportados

Security for Endpoints actualmente protege los siguientes sistemas operativos:

Sistemas operativos de estaciones de trabajo:

- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista con Service Pack 1
- Windows XP con Service Pack 2 64 bits
- Windows XP con Service Pack 3
- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)
- Mac OS X Mavericks (10.9.x)

Tablets y sistemas operativos integrados:

- 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
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded con Service Pack 2*
- Windows XP Tablet PC Edition*

*Deben instalarse módulos específicos del sistema operativo para que funcione Security for Endpoints.

Sistemas operativos de servidor:

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

- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 con Service Pack 1
- Windows Home Server

A.1.2. Requisitos de Hardware

- Procesador Intel® Pentium compatible:

Sistemas operativos de estaciones de trabajo

- 1 GHz o más para Microsoft Windows XP SP3, Windows XP SP2 64 bit y Windows 7 Enterprise (32 y 64 bit)
- 2 GHz o más para Microsoft Windows Vista SP1 o superior (32 y 64 bit), Microsoft Windows 7 (32 y 64 bit), Microsoft Windows 7 SP1 (32 y 64 bit), Windows 8
- 800 MHz o más para Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded con Service Pack 2, Microsoft Windows XP Tablet PC Edition

Sistemas operativos de servidor

- Mínimo: CPU de un solo núcleo a 2,4 GHz
- Recomendado: CPU Intel Xeon multinúcleo a 1,86 GHz o más

- **Memoria RAM libre:**

- Para Windows 512 MB mínimos, 1 GB recomendados
- Para Mac: 1 GB mínimo

- **Espacio en disco duro:**

- 1.5 GB de espacio libre en disco



Nota

Se requieren al menos 6 GB de espacio libre en disco para entidades con rol de Endpoint Security Relay, dado que almacenarán todos los paquetes de instalación y actualizaciones.

A.1.3. Navegadores soportados

La seguridad del navegador del punto final se ha comprobado que funciona con los siguientes navegadores:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

A.1.4. Puertos de comunicación de Small Office Security

La siguiente tabla proporciona información de los puertos utilizados por los componentes de Small Office Security:

Puerto	Usabilidad
80 (HTTP) / 443 (HTTPS)	Puerto utilizado para acceder a la consola Web de Control Center.
80	Puerto del Servidor de Actualización.
8443 (HTTPS)	Puerto utilizado por el software cliente/agente para conectarse al Servidor de comunicación.
7074 (HTTP)	Comunicación con Endpoint Security Relay (si está disponible)

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

A.2. Cómo funciona la detección de red

Security for Endpoints incluye un mecanismo automático de detección de red pensado para detectar los equipos del grupo de trabajo.

Security for Endpoints se basa en el **servicio Microsoft Computer Browser** para realizar una detección de red. 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

Para activar el descubrimiento (detección) de la red, primero debe tener instalado Endpoint Security 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 forma parte activa de la operación del servicio de Computer Browser. Endpoint Security sólo 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 Endpoint Security instalado en la red.

- Si Endpoint Security está instalado en un equipo de un grupo de trabajo, sólo los equipos de ese grupo de trabajo serán visibles en Control Center.
- Si Endpoint Security está instalado en un equipo de dominio, sólo los equipos de ese dominio serán visibles en Control Center. Los equipos de otros dominios pueden detectarse si hay una relación de confianza con el dominio donde Endpoint Security está instalado.

Las consultas posteriores sobre detección de red se realizan regularmente cada hora. Para cada nueva pregunta, Control Center divide el espacio administrado de los equipos en áreas de visibilidad y entonces designa un Endpoint Security 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 Endpoint Security seleccionado falla al realizar la consulta, Control Center espera a la siguiente consulta programada, sin escoger otro Endpoint Security para intentarlo de nuevo.

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

A.2.1. 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.

A.2.2. Requisitos de descubrimiento de red

Para poder 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.
- 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 Endpoint Security 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.