



Bitdefender® ENTERPRISE

**SECURITY FOR
VIRTUALIZED
ENVIRONMENTS**
Guía del administrador
(Multiplataforma) >>

Security for Virtualized Environments de Bitdefender

Guía del administrador (Multiplataforma)

fecha de publicación 2013.02.04

Copyright© 2013 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 citas breves en artículos sólo es posible con la mención de la fuente citada. El contenido no puede modificarse de forma alguna.

Advertencia y Renuncia de Responsabilidad. El presente producto y su documentación están protegidos por copyright. La información en este documento se provee "tal como está", sin garantía. Aunque se ha tomado toda precaución en la preparación de este documento, los autores no tendrán ninguna responsabilidad con ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en este trabajo.

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 del contenido de cualquier sitio enlazado. Si usted accede a los sitios web de terceros listados en este documento, lo hará bajo su propia responsabilidad. Bitdefender proporciona estos enlaces sólo por conveniencia, y la inclusión del enlace no implica que Bitdefender apruebe o acepte ninguna responsabilidad por el contenido del sitio del tercero.

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 Security for Virtualized Environments	1
2. Pasos de la Instalación	4
2.1. Compatibilidad y requisitos	4
2.2. Preparándose para la Instalación	7
2.3. Pasos de la Instalación	8
2.4. Configuración de los appliances SVE	9
2.4.1. Configuración de Security Console	9
2.4.2. Configuración de Security Virtual Appliance	10
2.4.3. Cambio de contraseña de administrador	11
2.5. Configuración de su cuenta de empresa	11
2.6. Instalación del Silent Agent en MVs	14
2.6.1. Preparándose para la Instalación	15
2.6.2. Instalación local	15
2.6.3. Instalación remota	16
2.6.4. Cómo funciona la detección de red	17
2.6.5. Activar el soporte para el análisis on-access en VMs Linux	20
2.6.6. Creación de una plantilla de MV con el Silent Agent	22
2.7. Instalación recomendada con múltiples SVAs	23
3. Iniciando	24
3.1. Conectar a Security Console	24
3.2. Descripción general de Security Console	25
3.3. Directrices de configuración y administración	26
3.4. Cambiar la contraseña de inicio de sesión predeterminada	27
3.5. Gestionar su cuenta	27
3.6. Trabajar con datos de la tabla	29
4. Licencias y registro	30
4.1. Encontrar un reseller	30
4.2. Comprobar los detalles de licencia actuales	30
4.3. Registro de su producto	31
5. Panel de monitorización	32
5.1. Portlets de panel	32
5.2. Administrar Portlets	34
6. Administración de equipos (Máquinas Virtuales)	35
6.1. Acerca de equipos administrados, no administrados y excluidos	36
6.2. Sobre equipos offline	36
6.3. Enumerando máquinas Security Virtual Appliance	37
6.4. Utilización de grupos	37
6.5. Buscar y ordenar equipos	39
6.6. Comprobación del sistema y detalles de protección	40

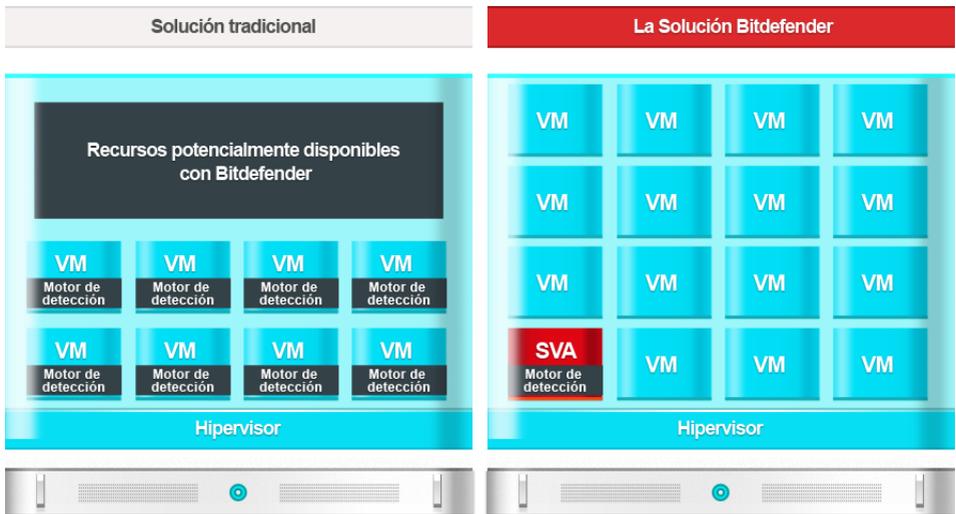
6.7. Comprobar y modificar la configuración de seguridad	40
6.8. Crear informes rápidos	41
6.9. Excluyendo Equipos de la Administración	41
6.10. Eliminar equipos de la consola	42
7. Políticas de Seguridad	44
7.1. Creando Nuevas Políticas	45
7.2. Configurar opciones de política	45
7.2.1. Resumen	46
7.2.2. General	46
7.2.3. Antimalware	50
7.3. Monitorizar la Ejecución de Política	60
7.4. Comprobar y Cambiar la Asignación de Políticas	61
7.5. Renombrando Políticas	61
7.6. Eliminando Políticas	62
8. Ejecutar y administrar tareas	63
8.1. Instalación de protección en MVs no administradas	63
8.2. Análisis en MVs administradas	64
8.3. Desinstalar la protección de las MVs	64
8.4. Ver y administrar tareas	65
8.4.1. Comprobar estado de ejecución y resultados	65
8.4.2. Eliminar Tareas	65
9. Usar informes	66
9.1. Tipos de informes disponibles	66
9.2. Creando Informes	68
9.3. Ver y administrar informes generados	69
9.3.1. Visualizando los Informes	70
9.3.2. Buscar detalles del informe	70
9.3.3. Guardar Informes	71
9.3.4. Imprimiendo los Informes	71
9.3.5. Enviar informes por correo	71
9.3.6. Eliminación automática de informes	71
9.3.7. Eliminar Informes	72
9.4. Administrar informes programados	72
9.4.1. Ver último informe generado	72
9.4.2. Renombrar informes programados	72
9.4.3. Editar informes programados	73
9.4.4. Eliminar informes programados	73
10. Cuarentena	75
10.1. Navegación y búsqueda	75
10.2. Restaurar archivos de la cuarentena	76
10.3. Eliminación automática de archivos de la cuarentena	76
10.4. Eliminar archivos de la cuarentena	77
11. Cuentas de usuario	78
11.1. Crear cuentas de usuario	78
11.2. Editar cuentas	79
11.3. Eliminar cuentas	79

11.4. Restablecer las contraseñas de inicio de sesión	80
12. Registro de actividad del usuario	81
13. Obtener Ayuda	82
13.1. Centro de soporte de Bitdefender	82
13.2. Solicitar ayuda	83
13.3. Información de contacto	83
13.3.1. Direcciones Web	84
13.3.2. Distribuidor Local	84
13.3.3. Oficinas de Bitdefender	84
A. Apéndices	87
A.1. Lista de tipos de archivos de aplicación	87
A.2. Usar variables de sistema	87
Glosario	89

1. Acerca de Security for Virtualized Environments

Las organizaciones hoy en día confían en las tecnologías de virtualización para incrementar el retorno de su inversión en infraestructuras de centros de datos. La consolidación de las cargas de trabajo de servidor y usuario final en infraestructuras compartidas ha conducido a la reducción de costes por deduplicación de recursos de hardware. La virtualización también proporciona ventajas operativas significativas mediante aprovisionamiento casi al instante a medida que las organizaciones crean y se apoyan en nubes públicas y privadas.

Para darse cuenta de todo el potencial de los centros de datos virtualizados, las organizaciones deben también ponerse como objetivo la consolidación de elementos de las propias cargas de trabajo, siendo la seguridad un elemento que debe estar presente en todas las cargas de trabajo. Para obtener tasas de consolidación y beneficios operacionales cada vez mayores, las organizaciones no deben sacrificar la seguridad mientras sus valiosas firmas cada vez están más amenazadas por atacantes aún más dedicados, sofisticados y especializados.



Bitdefender enfoque

Security for Virtualized Environments (SVE) es la primera solución de seguridad global para centros de datos virtualizados. SVE no sólo protege servidores y sistemas de usuario final

Windows, sino también sistemas Linux y Solaris. Integrado con VMware vShield y VMware vCenter, su arquitectura única también le permite defender sistemas que se ejecuten sobre cualquier tecnología de virtualización de sistemas. A medida que las organizaciones aumentan sus tasas de consolidación, la seguridad de Bitdefender que ha sido diseñada para, desde el primer día, proporcionar una seguridad fiable, proactiva y avanzada en entornos virtualizados se convierte en la piedra angular para construir y mejorar las estrategias de virtualización del centro de datos.

Cuando se instala en entornos VMware, SVE se beneficia de vShield Endpoint. No obstante, SVE no depende de la tecnología de virtualización; protege cualquier entorno basado en cualquier tecnología de virtualización.

Componentes

Security Virtual Appliance

Security for Virtualized Environments deduplica y centraliza buena parte de la funcionalidad en un único appliance virtual dedicado en cada host físico. Este appliance virtual de análisis de Linux reforzado se ocupa de las necesidades de análisis y mantenimiento (actualizaciones, mejoras, RAM, IOPS, etc.) de los clientes antimalware.

Security Console

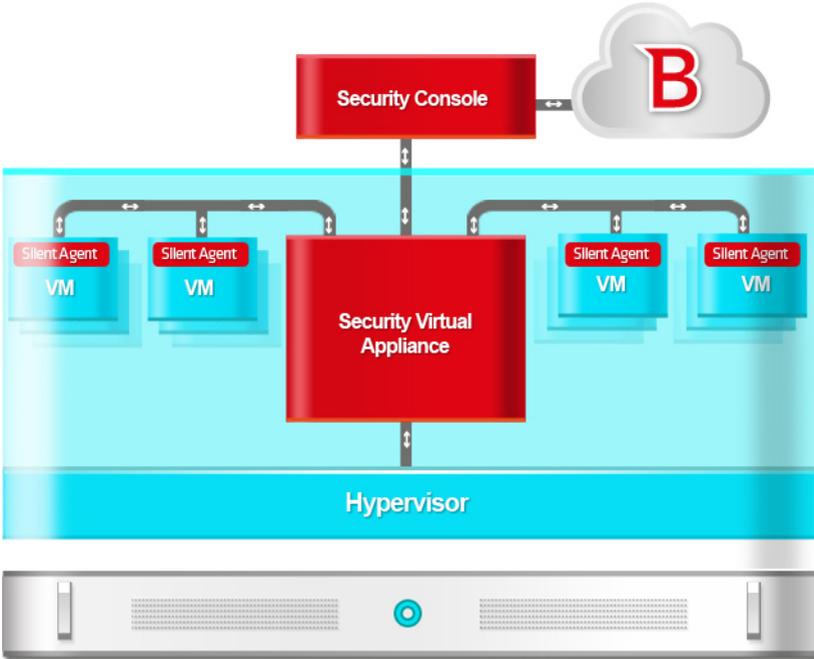
Security Console es una interfaz Web central utilizada para la implementación, configuración, monitorización, y generación de informes sobre el estado de seguridad de los centros de datos y los sistemas de usuario final. Basándose en la Bitdefender Gravity Architecture, una única Consola de seguridad y almacén de datos son fácilmente escalables horizontalmente desde las implementaciones más pequeñas hasta las más grandes.

Security Console se distribuye como un appliance virtual. El appliance Security Console también incluye el **Servidor de Actualizaciones**, componente que gestiona todas las tareas de actualización de productos y de firmas. El Servidor de Actualización es el único componente que necesita acceso a Internet para poder comunicarse con Bitdefender Cloud.

Silent Agent

Silent Agent es el componente en el lado del guest que facilita los análisis de memoria, al acceder o bajo demanda. Es una aplicación ligera, que a su vez tiene la función secundaria de mantener al corriente al usuario sobre el estado de seguridad local.

Silent Agent debe estar instalado en cada máquina virtual para que esté protegida (a diferencia de los entornos VMware donde Security for Virtualized Environments está integrado con vShield Endpoint). El kit de Silent Agent está disponible vía Security Console.



Componentes y operativa

2. Pasos de la Instalación

2.1. Compatibilidad y requisitos

Security for Virtualized Environments se entrega dentro de un Security Virtual Appliance corriendo en una distribución Linux Server reforzada (kernel 2.6) y gestionado por Security Console. Security Console se distribuye como un appliance virtual.

Plataformas de virtualización soportadas

Security for Virtualized Environments soporta las siguientes plataformas de virtualización:

- VMware vSphere 5.1, 5.0, 4.1 con VMware vCenter Server 5.1, 5.0, 4.1
- VMware View 5.1, 5.0
- Citrix XenServer 6.0, 5.6 o 5.5 (incluyendo Xen Hypervisor)
- Citrix XenDesktop 5.5 o 5.0 (incluyendo Xen Hypervisor)
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2012 o 2008 R2
- Windows Server 2012 o 2008 R2 (incluyendo Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (incluyendo KVM Hypervisor)
- [Kernel-based Virtual Machine \(KVM\)](#)
- Oracle VM 3.0



Importante

En los entornos VMware, puede utilizar Security for Virtualized Environments con VMware vShield Endpoint. Para más información, incluyendo requisitos adicionales, revise la documentación correspondiente a Security for Virtualized Environments.

Requisitos de Security Console

El appliance de Security Console es una máquina virtual preconfigurada. Este appliance debe instalarse en un host en su entorno virtualizado.

Debe dotar a cada host de Security Console de los siguientes recursos:

- Espacio en disco: 15 GB.
- La asignación de recursos de memoria y CPU para el appliance de Security Console depende del número de máquinas virtuales protegidas. La siguiente tabla indica los recursos recomendados que deben asignarse:

Número de MVs protegidas	RAM	CPUs
<100	2 GB	2 CPUs
100 - 1000	4 GB	2 CPUs
>1000	8 GB	4 CPUs

Para un mejor rendimiento, puede asignar más recursos si están disponibles.

Se puede acceder a Security Console mediante los siguientes navegadores web:

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

Resolución de pantalla recomendada: 1024x768 o superior

Requisitos de Security Virtual Appliance

El Security Virtual Appliance es una máquina virtual preconfigurada ejecutada en una distribución de servidor Linux reforzado (kernel 2.6). El número de instalaciones de Security Virtual Appliance necesarias depende principalmente del número y tipo de máquinas virtuales a proteger y de los recursos disponibles en los hosts. No necesita instalar Security Virtual Appliance en cada host.

Debe dotar a cada Security Virtual Appliance de los siguientes recursos:

- Espacio en disco: 8 GB.
- La asignación de recursos de memoria y CPU para el Security Virtual Appliance depende del número y tipo de MVs ejecutadas en el host. La siguiente tabla indica los recursos recomendados que deben asignarse:

Número de MVs protegidas	RAM	CPUs
1-50 MVs	2 GB	2 CPUs
51-100 MVs	2 GB	4 CPUs
101-200 MVs	4 GB	6 CPUs

Para un mejor rendimiento, puede asignar más recursos si están disponibles.

Sistemas operativos de guest soportados

Security for Virtualized Environments actualmente protege los siguientes sistemas operativos:

- Windows Server 2012

- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003 / Windows Server 2003 R2
- Windows 8
- Windows 7
- Windows Vista
- Windows XP con Service Pack 3 (32-bit) / Service Pack 2 (64-bit)
- Red Hat Enterprise Linux / CentOS 6.2, 6.1, 5.7, 5.6
- Ubuntu 11.04, 10.04
- SUSE Linux Enterprise Server 11
- OpenSUSE 12, 11
- Fedora 16, 15



Nota

La protección para los guests de Solaris no está disponible aún para la presente versión.

En análisis on-access está disponible para todas las versiones de Windows soportadas. También está disponible un módulo beta de análisis on-access para distribuciones Linux específicas y versiones del kernel, como se muestra en la siguiente tabla:

Distribuciones Linux	Versión Kernel
Ubuntu 10.04	2.6.32-44
RHEL/CentOS 5.7, 5.6	2.6.18-308
RHEL/CentOS 6.2, 6.1	2.6.32-279

Requisitos de Silent Agent e impacto en el sistema

Silent Agent puede instalarse en máquinas virtuales que se ejecuten en cualquiera de los sistemas operativos soportados. No existen requisitos hardware o software específicos que deban cumplirse. Como puede ver en la siguiente tabla, Silent Agent utiliza una cantidad mínima de recursos del sistema.

Plataforma	RAM	Espacio en disco
Windows	20/25* MB	60 MB
Linux	50 MB	70 MB

*20 MB cuando está activa la opción Modo silencioso y 25 MB cuando está desactivada. Cuando se habilita el Modo Silencioso, la interfaz gráfica de usuario (GUI) del Silent Agent no se carga automáticamente al inicio del sistema, liberando los recursos correspondientes.

2.2. Preparándose para la Instalación

Para la instalación necesita los siguientes componentes:

- Una plantilla de máquina virtual que contiene Security Virtual Appliance
- Una plantilla de máquina virtual que contiene Security Console

El kit de instalación de Silent Agent se incluye en el appliance de Security Console. Después de implementar y configurar los appliances de manera satisfactoria, podrá descargar el kit de instalación o instalar remotamente Silent Agent en sus máquinas virtuales desde la interfaz web de Security Console.

Para obtener los appliances Security for Virtualized Environments, debe enviar una petición para evaluar Security for Virtualized Environments a través de la página web de Bitdefender o, si ya es cliente, contactando con su representante de Bitdefender. Los enlaces de descarga se le enviarán por email tras revisarse su solicitud.

Security Console se instalará en un solo host en el entorno virtualizado. El número de instalaciones de Security Virtual Appliance necesarias depende principalmente del número y tipo de máquinas virtuales a proteger y de los recursos disponibles en los hosts. Los ajustes de asignación de recursos por omisión de Security Virtual Appliance se recomiendan hasta 100 clientes. Para más clientes, asigne más recursos o instale instancias Security Virtual Appliance adicionales.

Debe considerar lo siguiente:

- Cada uno de los appliances instalados deben usar también una dirección IP reservada asignada por DHCP o una dirección IP fija. Los appliances se configuran por omisión para obtener direcciones IP usando DHCP.
- El appliance de Security Console debe tener acceso a Internet debido a que descarga y distribuye actualizaciones de todos los componentes del producto. También debe ser accesible desde todas las máquinas en el entorno virtualizado.
- Las instancias Security Virtual Appliance deben tener conexión de red con el appliance Security Console y con todos los equipos que usan sus servicios de análisis.
- Configure el cortafuegos local en las máquinas virtuales para permitir la conectividad con los otros componentes de Security for Virtualized Environments en los siguientes puertos:
 - 7081 - el puerto de comunicación entre el Silent Agent y el Security Virtual Appliance.
 - 7083 - el puerto de comunicaciones Secure Sockets Layer (SSL) entre Silent Agent y Security Virtual Appliance.
 - 8082 - el puerto de comunicación entre el Silent Agent y la Security Console.
 - 7074 - el puerto del Servidor de actualización en el appliance de Security Console.
- Para una protección constante, los appliances instalados deben estar siempre activos.

2.3. Pasos de la Instalación

Debe seguir estos pasos para instalar todos los componentes de Security for Virtualized Environments:

1. Implemente la Security Console en un host desde su entorno virtualizado.
Iníciela. Configure esta MV de manera que tenga acceso a Internet para obtener actualizaciones de producto y que también pueda accederse por Bitdefender Silent Agents y Security Virtual Appliances.
2. Implemente el Security Virtual Appliance en los hosts que sea necesario. El número de instalaciones de Security Virtual Appliance necesarias depende principalmente del número y tipo de máquinas virtuales a proteger y de los recursos disponibles en los hosts. Los ajustes de asignación de recursos por omisión de Security Virtual Appliance se recomiendan hasta 100 clientes. Para más clientes, asigne más recursos o instale instancias Security Virtual Appliance adicionales.
Inicie todos los appliances instalados. Estas MVs necesitan conectividad de red con los agentes silenciosos Bitdefender asociados y con Security Console.
3. Los appliances se configuran por omisión para obtener direcciones IP usando DHCP. Configure el servidor DHCP para reservar direcciones IP para todos los appliances instalados. De no ser así, debe configurar cada uno de ellos para usar una IP estática. Lea el siguiente paso para la configuración de IP estática.
4. Configure appliances instalados desde su consola CLI. Para más información, diríjase a [“Configuración de los appliances SVE” \(p. 9\)](#).
5. Conéctese a la Security Console mediante HTTPS y configure su cuenta de empresa. Para más información, diríjase a [“Configuración de su cuenta de empresa” \(p. 11\)](#).
6. Instale el Silent Agent en las instancias que desee proteger. Para instrucciones de instalación, consulte [“Instalación del Silent Agent en MVs” \(p. 14\)](#).
7. Cree y asigne políticas a máquinas virtuales para configurar las opciones de protección y para dirigir las a la instancia Security Virtual Appliance preferida. Para más información, diríjase a [“Políticas de Seguridad” \(p. 44\)](#).



Nota

En un entorno virtualizado con múltiples instalaciones de Security Virtual Appliance, el agente utilizará inicialmente la Security Virtual Appliance por omisión configurada en la [cuenta de empresa de la Security Console](#). Tan pronto como se aplique la política en la máquina virtual, el agente usará el Security Virtual Appliance configurado mediante los ajustes de política. Utilice la política para dirigir al agente a la instancia Security Virtual Appliance preferida. Para más información, diríjase a [“Instalación recomendada con múltiples SVAs” \(p. 23\)](#).

Se recomienda agrupar primero máquinas virtuales (por instancias Security Virtual Appliance, host físico u otros criterios) y después asignar políticas de grupo. Para más información, diríjase a [“Utilización de grupos”](#) (p. 37).

2.4. Configuración de los appliances SVE

Security Console y Security Virtual Appliance tienen interfaces de línea de comandos que permiten configurar ajustes básicos, incluyendo los ajustes de red.

Las credenciales de inicio de sesión por omisión son las mismas para ambos appliances:

- Nombre de usuario: `administrador`
- Contraseña: `admin`

2.4.1. Configuración de Security Console

El script de configuración de la Security Console le permite configurar el appliance con ajustes de red estática. Si ha creado una reserva de IP para el appliance en el servidor DHCP, no necesita ejecutar el script de configuración.

Para configurar la Security Console con ajustes de red estática:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client). Como alternativa, puede conectarse al appliance vía SSH.
2. Inicie sesión utilizando las credenciales por omisión.
3. Obtenga privilegios de root ejecutando el comando `sudo su` y luego introduciendo la contraseña de `admin`.
4. Ejecute el comando `sc-setup`.
5. Introduzca los ajustes de red: Dirección IP, máscara de red, puerta de enlace, servidores de DNS.
6. Teclee `Y` y pulse Intro para guardar los cambios.



Nota

Si está conectado al appliance por medio de un cliente SSH, al cambiar los ajustes de red se cerrará inmediatamente su sesión.

7. Asegúrese de que el appliance tiene configurada la dirección IP designada. Puede comprobar la configuración IP ejecutando el siguiente comando:

```
$ ifconfig eth0
```

2.4.2. Configuración de Security Virtual Appliance

El script de configuración del Security Virtual Appliance le permite configurar el appliance con las direcciones de la Security Console y el servidor de actualizaciones, así como los ajustes de red estática. Antes de instalar el Security Virtual Appliance, asegúrese de que el appliance Security Console está configurado con la dirección IP designada.

Para configurar el Security Virtual Appliance:

1. Acceda a la consola del appliance desde su herramienta de administración de la virtualización (por ejemplo, vSphere Client). Como alternativa, puede conectarse al appliance vía SSH.
2. Inicie sesión utilizando las credenciales por omisión.
3. Obtenga privilegios de root ejecutando el comando `sudo su` y luego introduciendo la contraseña de `admin`.



Importante

Para ejecutar con éxito el script de configuración del Security Virtual Appliance, éste debe contar con conexión de red con el appliance Security Console. Si no dispone de servidor DHCP en la red local, deberá configurar manualmente los ajustes de la red del Security Virtual Appliance antes de ejecutar el script de configuración. Puede asignar una dirección IP temporal y una dirección para la puerta de enlace en el appliance ejecutando los siguientes comandos:

```
$ sudo ifconfig eth0 <IP address> netmask <subnet mask>
```

```
$ sudo route add default gw <gateway IP address>
```

Utilice luego el script de configuración para configurar todos los ajustes de red necesarios.

4. Ejecute el comando `sc-setup`.
5. Introduzca la dirección IP o nombre del host de la máquina Security Console.
6. Introduzca la dirección IP o nombre del host del servidor local de actualización. Ya que la actualización local se ejecuta en la máquina Security Console, debe introducir la dirección IP o nombre del host de la máquina.
7. Opcionalmente, puede configurar el appliance con ajustes de red estática. Si ha creado una reserva de IP para el appliance en el servidor DHCP, sáltese esta configuración pulsando Intro.
 - a. Teclee `Y` y pulse Intro para continuar.
 - b. Introduzca los ajustes de red: Dirección IP, máscara de red, puerta de enlace, servidores de DNS.

- c. Teclee **Y** y pulse Intro para guardar los cambios.



Nota

Si está conectado al appliance por medio de un cliente SSH, al cambiar los ajustes de red se cerrará inmediatamente su sesión.

8. Asegúrese de que el appliance tiene configurada la dirección IP designada. Puede comprobar la configuración IP ejecutando el siguiente comando:

```
$ ifconfig eth0
```

2.4.3. Cambio de contraseña de administrador

Para evitar el acceso no autorizado al CLI de los appliances de Bitdefender, se recomienda cambiar la contraseña por omisión de la cuenta de administrador. El proceso de cambio de contraseña es el mismo para ambos appliances.

Para cambiar la contraseña:

1. Acceda a la consola del appliance en el vSphere Client. Como alternativa, puede conectarse al appliance vía SSH.
2. Inicie sesión utilizando las credenciales por omisión.
3. Ejecute el comando `passwd`.
4. Introduzca la contraseña actual (por omisión `admin`).
5. Introduzca la nueva contraseña. Asegúrese de elegir una contraseña fuerte que pueda recordar fácilmente. Para una contraseña fuerte, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (tales como #, \$ o @).
6. Introduzca de nuevo la nueva contraseña.

2.5. Configuración de su cuenta de empresa

Una vez que ha implementado los appliances de Security for Virtualized Environments, debe conectarse a la Security Console mediante HTTPs y configurar su cuenta de empresa.

Para configurar su cuenta de empresa:

1. Abra su navegador Web.



Nota

Requisitos:

- Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari u Opera
- Resolución de pantalla recomendada: 1024x768 o superior

2. Introduzca la dirección IP de la MV de la Security Console (usando https). Se mostrará una página de inicio de sesión.
3. Inicie sesión con las credenciales por omisión:
 - Nombre de usuario: `default@company.com`
 - Contraseña: `default`
4. Lea y confirme que está de acuerdo con los términos del servicio. Si no acepta estos términos, no podrá utilizar el servicio.
5. Facilite toda la información necesaria para configurar su cuenta de empresa.
 - a. Bajo **Detalles de cuenta**, configure los detalles de su cuenta de empresa.
 - **Nombre y apellidos.**
 - **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.** Establezca una contraseña de inicio de sesión. La contraseña ha de tener entre 8 y 128 caracteres y debe contener al menos un carácter en mayúsculas, uno en minúsculas y un número o carácter especial.
 - **Nombre de la empresa.**
 - b. Debajo de **Ajustes predeterminados de Silent Agent**, configure los ajustes por omisión que deberán incluirse en el kit de Silent Agent y en la política por omisión.
 - **Dirección de Security Console.** Introduzca la dirección IP de la MV de la Security Console. Silent Agent utiliza estas direcciones para comunicarse con la Security Console.
 - **Dirección Security Virtual Appliance** . Escriba la dirección IP de la instancia Security Virtual Appliance a la que se conecta ese Silent Agent de forma predeterminada. Si ha implementado múltiples instancias de Security Virtual Appliance, utilizará políticas para direccionar los agentes a la instancia de Security Virtual Appliance adecuada. Para más información, diríjase a [“Instalación recomendada con múltiples SVAs” \(p. 23\)](#).
 - **Usar SSL.** Seleccione esta opción si desea asegurar la comunicación entre Silent Agent y el Security Virtual Appliance usando Secure Sockets Layer (SSL). Tenga en cuenta que activar el cifrado SSL para el tráfico Silent Agent - Security Virtual Appliance afectará ligeramente al rendimiento.



Nota

La comunicación entre Silent Agent y Security Console siempre se cifra usando SSL, con independencia de cómo configure esta opción.

El puerto de comunicación Silent Agent - Security Virtual Appliance depende del uso del cifrado SSL:

- El puerto utilizado para la comunicación asegurada con SSL es el 7083.
- El puerto usado para la comunicación no segura es el 7081.

c. Bajo **Configuración proxy**, seleccione **Usar proxy** si la máquina Security Console se conecta a Internet a través de un servidor proxy. Debe configurar las siguientes opciones:

- Dirección del servidor proxy.
- Número de puerto usado por el servidor proxy.
- Nombre de usuario reconocido por el proxy.
- Contraseña válida para el nombre de usuario especificado anteriormente.



Nota

Security Console no soporta servidores proxy que usen la autenticación de Active Directory. Se describe una alternativa para el método de autenticación NTLM en este [artículo de la base de datos de conocimientos](#).

d. Bajo **Configuración SMTP**, puede configurar Security Console para enviar informes por e-mail y notificaciones usando un servidor de correo externo en lugar del servidor de correo postfix incorporado. Si no especifica ninguna configuración, Security Console usa el servidor de correo incluido.

- **IP/ Nombre del host.** Introduzca la dirección IP o el nombre del host del servidor de correo que va a enviar los e-mails.
- **Puerto.** Introduzca el puerto utilizado para conectarse con el servidor de correo.
- **Nombre de Usuario.** Si el servidor SMTP requiere autenticación, introduzca una dirección de e-mail / nombre de usuario reconocible.
- **Contraseña.** Si el servidor SMTP requiere autenticación, introduzca la contraseña del usuario especificado anteriormente.
- **Desde el nombre.** Introduzca el nombre que quiere que aparezca en campo De del e-mail (el nombre del remitente).
- **Desde el e-mail.** Introduzca la dirección de e-mail que quiere que aparezca en el campo De del e-mail (dirección de e-mail del remitente).



Nota

Security Console no soporta conexión cifrada (SSL, TLS) al servidor de correo.

e. En **Licencia** puede ver los detalles de la licencia actual. Para más información, diríjase a [“Licencias y registro”](#) (p. 30).

- f. Configure las opciones de cuenta según sus preferencias en **Configuración**.
- **Zona horaria.** Elija desde 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 desde el menú el idioma de visualización de la consola.
 - **Logotipo.** Puede cambiar el logotipo predeterminado con forma de nube de Security Console con el logotipo de su empresa. Esto le permitirá personalizar el diseño de los informes PDF. Para cambiar el logo, haga clic en **Personalizar** y cargue el archivo de imagen del logotipo desde su equipo. Se aplican las siguientes restricciones:
 - Dimensiones del logotipo: 81x41 pixels.
 - Formatos de archivo soportados: PNG y JPG.
- g. Haga clic en **Enviar** para guardar los cambios.

2.6. Instalación del Silent Agent en MVs

Para proteger las máquinas virtuales con Security for Virtualized Environments, debe instalar Silent Agent (el software de cliente) en cada una de ellas. Silent Agent administra la protección en la MV local. Envía solicitudes de análisis al Security Virtual Appliance, que realiza el análisis en sí. También se comunica con la Security Console para recibir las órdenes del administrador y enviar los resultados de sus acciones.

Antes instalar el Silent Agent:

- Asegúrese de que todos los pasos anteriores en el proceso de instalación de Security for Virtualized Environments se han completado. Para más información, diríjase a [“Pasos de la Instalación”](#) (p. 8).
- Prepare la instalación como se indica en [“Preparándose para la Instalación”](#) (p. 15).

Hay dos métodos de instalación:

- **Instalación local.** Utilice el enlace de instalación de Security Console para descargar e instalar Silent Agent de manera local en máquinas virtuales individuales. Para más información, diríjase a [“Instalación local”](#) (p. 15).



Importante

La instalación local es actualmente el único método de instalación disponible para las MVs de Linux.

- **Instalación remota.** Una vez instalado en una máquina virtual, Silent Agent detecta automáticamente las máquinas virtuales Windows visibles en la red local. La protección de Security for Virtualized Environments puede instalarse en máquinas virtuales de forma remota desde la consola. La instalación remota se ejecuta en segundo plano, sin que el usuario lo perciba. Para más información, diríjase a [“Instalación remota”](#) (p. 16) y [“Cómo funciona la detección de red”](#) (p. 17).

2.6.1. Preparándose para la Instalación

Prepare la instalación en las máquinas virtuales como se expone a continuación:

1. Asegúrese de que las máquinas virtuales ejecutan un **sistema operativo del guest soportado**. Para algunas MVs, puede que necesite instalar la última versión del service pack del sistema operativo disponible.
2. Desinstale (no solo deshabilite) cualquier software antimalware existente en las máquinas virtuales. Ejecutar otro software de seguridad simultáneamente con Security for Virtualized Environments puede afectar al funcionamiento y provocar graves problemas en el sistema.
3. La instalación requiere privilegios de administrador. Para la instalación remota, asegúrese de tener las credenciales de administrador para todas las máquinas virtuales.
4. Los appliances virtuales de Security Console deben estar iniciados y accesibles desde las máquinas virtuales. Los archivos de instalación se descargan de la máquina virtual de la Security Console.

2.6.2. Instalación local

La instalación local puede realizarla usted mismo conectándose a cada máquina virtual, o puede solicitar ayuda a los usuarios de las máquinas virtuales. Requiere ejecutar un pequeño archivo de instalación que puede descargar desde Security Console. El archivo de instalación viene en dos versiones (Windows y Linux).



Importante

La instalación local es actualmente el único método de instalación disponible para las instancias de Linux.

Para obtener o distribuir los enlaces de descarga para la instalación local:

1. Conéctese a Security Console usando su **cuenta de empresa**.
2. Vaya a la página **Equipos > Área de instalación**.
3. Haga clic en el botón **Enlace** y elija **Ver**. La ventana que aparece le proporciona los enlaces de descarga del instalador Web para Windows y el script de instalación de Linux. Utilice el enlace para descargar un archivo de instalación pequeño, que puede ejecutar en el equipo local para instalar la protección. También puede copiar el archivo a un recurso compartido de red accesible desde las máquinas virtuales.
4. Otra opción es enviar a los usuarios dentro de la red de la organización invitaciones de correo con el enlace de la instalación, pidiéndoles que descarguen e instalen la protección en sus equipos. Para enviar el enlace, haga clic en el botón **Enlace** y elija **Enviar por email**. Las invitaciones por e-mail están pensadas para ser enviadas sólo a usuarios de Windows, ya que contienen sólo el enlace al instalador Web para Windows.

Para instalar de manualmente el Silent Agent en una máquina virtual de Windows:

1. Descargue el instalador Web del Silent Agent de Windows desde la Security Console.
2. Localice el archivo de instalación descargado y haga doble clic en él. El instalador Web descarga el paquete de instalación completo desde el appliance de Security Console y comienza su instalación.
3. Espere a que la instalación se complete. Se descargan e instalan las últimas versiones de los archivos de programa y se inician los servicios de Bitdefender. Este paso puede tardar un par de minutos.

La ventana de instalación se cierra automáticamente una vez que se haya completado la instalación.

Para instalar manualmente el Silent Agent en una máquina virtual de Linux:

1. Descargue el script de instalación de Linux del Silent Agent desde la Security Console. Si tiene el enlace de descarga, ejecute el siguiente comando en un terminal:

```
$ wget --no-check-certificate <download link>
```

El archivo descargado se llama `descargador`.

2. Conceda permiso de ejecución al usuario actual en el archivo `descargador`.

```
$ chmod u+x downloader
```

3. Ejecutar `descargador` como root. El script descarga el paquete de instalación completo de la instancia de Security Console y posteriormente comienza la instalación.

```
$ sudo ./downloader
```

La instalación finalizará normalmente en menos de un minuto.

2.6.3. Instalación remota

Para hacer la implementación más fácil, Security for Virtualized Environments incluye un mecanismo de descubrimiento de red automático basado en el cual Silent Agent puede instalarse en máquinas virtuales Windows remotamente desde Security Console. Los equipos detectados se muestran como **equipos no administrados** en la página de **Equipos**. Para información detallada sobre la detección de redes, consulte [“Cómo funciona la detección de red”](#) (p. 17).

Para activar la detección de redes y la instalación automática, debe tener primero Silent Agent instalado en al menos una máquina virtual en la red. Esta máquina se utilizará para analizar la red e instalar Silent Agent en las máquinas desprotegidas.



Nota

Una vez instalado el primer Silent Agent, puede llevar unos pocos minutos que aparezcan visibles en la Security Console el resto de equipos de la red.



Nota

Cada máquina objetivo debe tener habilitada la compartición de administrador admin\$ para que funcione la instalación.

Para instalar manualmente la protección en máquinas virtuales:

1. Conéctese a Security Console usando su **cuenta de empresa**.
2. **Instalar protección manualmente** en una máquina virtual en la red. Espere unos minutos después de la instalación mientras Silent Agent detecta equipos en su red local.
3. Vaya a la página **Equipos > Ver equipos**. Aquí es donde puede ver las máquinas virtuales protegidas y los equipos detectados en la red local donde se ha instalado Silent Agent. También podrían detectarse los equipos físicos si estuvieran conectados a la red virtual.
4. Haga clic en el menú **Mostrar** localizado encima de la tabla (a la izquierda) y elija **Equipos no administrados**. De esta manera, solo se muestran equipos detectados que no están protegidos actualmente por Security for Virtualized Environments.
5. Si ha organizado los equipos en grupos, seleccione el grupo deseado desde el panel izquierdo. Para ver todos sus equipos, haga clic con el botón derecho en el grupo raíz y elija **Ver todos los equipos**.
6. Marque las casillas de verificación correspondientes a las máquinas virtuales en las que quiere instalar la protección.
7. Haga clic en **Tareas** y elija **Instalar** desde el menú. Se mostrará la ventana Opciones de instalación.
8. Proporcione las credenciales de administrador necesarias para la autenticación remota en las máquinas virtuales seleccionadas.
Introduzca el nombre de usuario y contraseña de una cuenta de administrador para cada uno de los equipos seleccionados. 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, dominio\usuario o usuario@dominio.com).
9. Haga clic en **Instalar Silent Agent**. Aparecerá una ventana de configuración.
10. Puede ver y administrar la tarea en la página **Equipos > Ver tareas**.

2.6.4. Cómo funciona la detección de red

Security for Virtualized Environments 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.



Importante

Security for Virtualized Environments 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).

Security for Virtualized Environments no está directamente implicado en la operativa del servicio Computer Browser. Silent Agent 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 Security Console. Security Console 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 Silent Agent instalado en la red.

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

Las consultas posteriores sobre detección de red se realizan regularmente cada hora. Para cada nueva consulta, Security Console divide el espacio de equipos administrados en áreas de visibilidad y luego designa un Silent Agent en cada área donde realizar la tarea. Un área de visibilidad es un grupo de equipos que se detectan entre sí. 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 Silent Agent seleccionado falla al realizar la consulta, Security Console espera a la siguiente consulta programada, sin escoger otro Silent Agent para intentarlo de nuevo.

Para una visibilidad de toda la red, Silent Agent deberá estar instalado en al menos un equipo en cada grupo de trabajo o dominio en su red. Lo ideal sería que Silent Agent 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 Windows Internet Naming Service (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 poder detectar satisfactoriamente todos los equipos (servidores y estaciones de trabajo) que se administrarán desde Security Console, 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 estar ejecutando el servicio Computer Browser. Los controladores primarios de dominios 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 Silent Agent accede al servicio Computer Browser deben poder resolver nombres NetBIOS.



Nota

El mecanismo de descubrimiento de red opera para todos los sistemas operativos Windows soportados, siempre que se cumplan los requisitos.

2.6.5. Activar el soporte para el análisis on-access en VMs Linux

La versión Linux de Silent Agent incluye un módulo beta de análisis on-access que funciona con [versiones del kernel y de distribuciones Linux específicas](#). El soporte de análisis on-access puede activarse manualmente en cada máquina virtual.

El análisis on-access requiere el módulo del kernel cargable DazukoFS. DazukoFS es un sistema de archivos apilable que permite a las aplicaciones de terceros controlar el acceso de archivo en sistemas Linux. Para más información, diríjase a <http://www.dazuko.org>.

El paquete de instalación de Silent Agent incluye e instala automáticamente DazukoFS. Una vez instalado, DazukoFS debe montarse encima de todos los directorios que quiera analizar en tiempo real.



Importante

Silent Agent 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 Silent Agent.

Para activar el soporte de análisis on-access en una máquina virtual Linux con Silent Agent instalado:

1. [Cargue el modulo kernel DazukoFS](#).
2. [Monte los directorios a monitorizar usando DazukoFS](#).

Una vez activo el soporte, el análisis on-access puede administrarse remotamente desde Security Console usando políticas.



Importante

Para que funcione DazukoFS y el análisis on-access, la política SELinux debe estar desactivada o configurada como **permitir**. Para consultar y ajustar la opción de política SELinux, edite el archivo `/etc/selinux/config`.

Cargar el módulo DazukoFS

Durante la instalación de Silent Agent, DazukoFS está definido para cargarse automáticamente en el momento del arranque. Para cargar el módulo inmediatamente tras la instalación, debe reiniciar la máquina virtual o ejecutar el comando siguiente:

```
# modprobe /lib/modules/`uname -r`/kernel/fs/dazukofs/dazukofs.ko
```



Nota

Si el paquete DazukoFS incluido con Silent Agent no es compatible con la versión del kernel de 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 Silent Agent:

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

Para obtener más información sobre la compilación y carga de DazukoFS para una versión del kernel no soportada, consulte este [artículo de la base de datos de conocimiento](#).

Para comprobar si está cargado DazukoFS, ejecute el siguiente comando:

```
# lsmod | grep dazukofs
```

Si el módulo está cargado, el comando muestra una línea que empieza con `dazukofs`.



Nota

Para descargar el módulo kernel DazukoFS, primero debe desmontar los directorios monitorizados y luego asegurarse de detener los servicios de Bitdefender.

Para detener los servicios de Bitdefender, ejecute este comando:

```
# /opt/BitDefender/bin/bd stop
```

Tras descargar el módulo, reinicie los servicios de Bitdefender usando este comando:

```
# /opt/BitDefender/bin/bd start
```

Administrar los directorios monitorizados

Montar todos los directorios que desee analizar usando DazukoFS. DazukoFS monitoriza todo el árbol de directorios bajo un directorio montado.



Importante

Si monta un directorio desde un árbol de directorios monitorizado por DazukoFS usando otro sistema de archivos, el análisis on-access ya no funcionará para ese árbol de directorios.

Por consiguiente, asegúrese de montar DazukoFS sobre un árbol de directorios solamente tras montar los otros sistemas de archivos necesarios.

Para montar un directorio usando DazukoFS, ejecute el siguiente comando:

```
# mount -t dazukofs <directory_path> <directory_path>
```

Por ejemplo, para activar el análisis on-access para el directorio de inicio, el comando es:

```
# mount -t dazukofs /home /home
```



Nota

No puede montar DazukoFS sobre el sistema de archivo raíz (/).

Para comprobar la lista de directorios montados con DazukoFS, ejecute el siguiente comando:

```
# mount | grep dazukofs
```

El comando muestra cada directorio montado en una línea independiente.

Para dejar de monitorizar un directorio específico, ejecute el siguiente comando:

```
# umount <directory_path>
```

2.6.6. Creación de una plantilla de MV con el Silent Agent

A partir de la versión 1.2.4 de Security for Virtualized Environments, Silent Agent detecta automáticamente cuándo se ejecuta en una máquina creada desde una plantilla y crea una instancia ID única. En consecuencia, no se precisa ninguna configuración especial para incluir Silent Agent en una plantilla de máquina virtual.

Para crear una plantilla de máquina virtual con el Silent Agent:

1. Cree la máquina virtual que se utilizará para crear la plantilla.
2. Prepare el sistema (por ejemplo, instale el software necesario).
3. Instale el Silent Agent en la máquina virtual descargando y ejecutando el archivo de instalación desde la Security Console. Para más información, diríjase a [“Instalación local”](#) (p. 15).
4. Compruebe que la máquina virtual se muestra en la Security Console como administrada. Vaya a la página **Equipos > Ver equipos**.
5. Apague la máquina y guárdela como una plantilla.

2.7. Instalación recomendada con múltiples SVAs

El número de instalaciones necesarias de Security Virtual Appliance depende de lo siguiente:

- Número de máquinas virtuales y tipo de virtualización (VDI o virtualización del servidor)
- Recursos disponibles en los hosts
- Topología de red y conectividad entre los hosts y entre las máquinas virtuales
- Requisitos para evitar fallos

Es importante indicar que Silent Agent está configurado de forma predeterminada para usar el Security Virtual Appliance especificado en la [Cuenta de empresa de Security Console](#). En entornos con múltiples instalaciones de Security Virtual Appliance, puede redirigir instancias específicas de Silent Agent a diferentes Security Virtual Appliance utilizando políticas. Cuando crea una política, puede especificar lo siguiente:

- Máquinas virtuales o grupos a los que aplicar la política (objetivo de la política).
- Instancias Security Virtual Appliance a las que se pueden conectar los agentes incluidos en el objetivo de la política. Los ajustes pueden configurarse en el apartado de políticas **General > Avanzado**. Puede cambiar la dirección de Security Virtual Appliance existente o añadir las direcciones de otras instancias Security Virtual Appliance. Silent Agent selecciona una de las instancias de Security Virtual Appliance especificadas, basándose en la prioridad asignada, disponibilidad y carga actual (normal, con sobrecarga, bajo de carga).

El enfoque recomendado es para configurar políticas con las direcciones de todas las instancias disponibles de Security Virtual Appliance y basarse en el mecanismo de balanceo de carga para distribuir los agentes automáticamente. Ajuste el Security Virtual Appliance preferido para las instancias Silent Agent seleccionadas con prioridad 1.

Para aprender cómo utilizar políticas, diríjase a [“Políticas de Seguridad”](#) (p. 44).

3. Iniciando

Security for Virtualized Environments puede configurarse y administrarse usando la Security Console, una interfaz web central.

Al usar Security Console, puede hacer lo siguiente:

- Administre su licencia.
- Instale protección en máquinas virtuales.
- Visualizar toda la red (máquinas virtuales administradas, equipos no protegidos detectados en la red).
- Obtenga información detallada sobre una máquina virtual administrada.
- Ejecute de forma remota tareas en máquinas virtuales (instalar, desinstalar, analizar).
- Asigne políticas a las máquinas virtuales administradas para configurar y gestionar la protección.
- Monitorizar la protección.
- Obtener informes de fácil lectura centralizados sobre las máquinas virtuales administradas.
- Comprobar y administrar remotamente archivos en cuarentena.
- Crear y administrar cuentas de usuario para otros empleados de la empresa.
- Comprobar el registro de actividad del usuario.

3.1. Conectar a Security Console

El acceso a Security Console se realiza a través de las cuentas de usuario.

Para conectarse a Security Console:

1. Requisitos:
 - El appliance virtual de Security Console debe estar encendido, conectado a Internet y accesible desde cualquier equipo.
 - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari u Opera
 - Resolución de pantalla recomendada: 1024x768 o superior
2. Abra su navegador Web.
3. Vaya a la dirección IP del host de la consola (usando https).
4. Escriba la dirección de correo y contraseña de su cuenta.
5. 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.

La primera vez que inicie sesión en la consola, se le solicitará que lea y confirme que está de acuerdo con los términos del servicio. Si no acepta estos términos, no podrá utilizar el servicio.

3.2. Descripción general de Security Console

Security Console 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.

Panel de Control

Visualice tablas de fácil lectura que proporcionan información clave sobre seguridad referente a su red. Para más información, diríjase a [“Panel de monitorización”](#) (p. 32).

Equipos

Instalar la protección, administrar los equipos y ejecutar tareas de forma remota. Para más información, diríjase a [“Administración de equipos \(Máquinas Virtuales\)”](#) (p. 35).

Políticas

Crear, aplicar y administrar las políticas de seguridad. Para más información, diríjase a [“Políticas de Seguridad”](#) (p. 44).

Informes

Obtenga informes de seguridad relativos a los equipos administrados. Para más información, diríjase a [“Usar informes”](#) (p. 66).

Cuarentena

Administrar de forma remota los archivos en cuarentena. Para más información, diríjase a [“Cuarentena”](#) (p. 75).

Cuentas

Administre sus detalles de cuenta y preferencias. Crear y administrar cuentas de usuario para otros empleados de la empresa. Para más información, diríjase a [“Cuentas de usuario”](#) (p. 78).

Log

Compruebe el registro de actividad del usuario. Para más información, diríjase a [“Registro de actividad del usuario”](#) (p. 81).

En la esquina superior derecha de la consola puede encontrar los siguientes enlaces:

- **Nombre de usuario.** Haga clic en su nombre de usuario para administrar la información de su cuenta y sus preferencias.
- **Ayuda y Soporte.** Haga clic en este enlace para encontrar información de soporte y ayuda.

- **Finalizar Sesión.** Haga clic en este enlace para cerrar la sesión de su cuenta.

3.3. Directrices de configuración y administración

Aquí tiene algunas directrices para ayudarle a empezar:

1. Diríjase a la página **Cuentas > Mi cuenta** para administrar los detalles de su cuenta. Se recomienda que cambie la contraseña de inicio de sesión predeterminada. Puede personalizar el diseño del informe PDF cargando el logo de su empresa.
2. Diríjase a la página **Equipos > Área de instalación** e instale Silent Agent (el software cliente) en las máquinas virtuales. Para instrucciones de instalación, consulte [“Instalación del Silent Agent en MVs”](#) (p. 14).
3. Si administra un número grande de equipos (diez o más), organícelos en grupos para administrarlos más eficientemente:
 - a. Vaya a la página **Equipos > Ver equipos**.
 - b. Cree grupos en el panel izquierdo haciendo clic con el botón derecho sobre el grupo raíz (o un grupo que haya creado) y seleccione **Crear grupo**.
 - c. Haga clic en el grupo raíz; luego, seleccione los equipos y arrastre y suelte su selección en el grupo deseado.
4. La configuración de protección en los equipos se establece automáticamente según la política de seguridad predeterminada. Para comprobar las opciones de protección predeterminadas, diríjase a la página **Políticas > Ver políticas** y haga clic en el nombre de la política predeterminada.

No puede editar la política predeterminada. Para cambiar la configuración de protección predeterminada:

- a. Diríjase a la página **Políticas > Nueva política** y cree una nueva política.
 - b. Configure las opciones de la política según sea necesario.
5. Más tarde, para administrar y monitorizar la protección, haga lo siguiente:
 - Compruebe regularmente la página **Panel de control** para ver en tiempo real la información sobre la protección de Security for Virtualized Environments.
 - Vaya a la página **Informes > Nuevo informe** para crear los informes que necesite. Se recomienda crear informes programados para los tipos de informe que necesite normalmente. Para ver un informe generado, vaya a la página **Informes > Ver informes** y haga clic en el nombre del informe.
 - Utilice las tareas en la página **Equipos > Ver equipos** para analizar las MVs protegidas, instalar protección de manera remota en MVs no administradas o eliminar completamente la protección.

3.4. Cambiar la contraseña de inicio de sesión predeterminada

Se recomienda que cambie la contraseña de inicio de sesión predeterminada. También es aconsejable cambiar su contraseña de inicio de sesión periódicamente.

Para cambiar la contraseña de inicio de sesión:

1. Vaya a la página **Cuentas > Mi cuenta**.
2. Escriba una nueva contraseña en los campos correspondientes (en **Detalles de cuenta**).
3. Haga clic en **Enviar** para guardar los cambios.

3.5. Gestionar su cuenta

Para comprobar y cambiar sus detalles de cuenta y configuración:

1. Vaya a la página **Cuentas > Mi cuenta**.
2. Modifique o actualice sus detalles de cuenta en **Detalles de cuenta**.
 - **Nombre y apellidos.**
 - **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.** Para cambiar su contraseña de inicio de sesión, escriba una nueva en los campos correspondientes.
 - **Nombre de la empresa.**
3. **¡Sólo cuenta de empresa!** Debajo de **Ajustes predeterminados de Silent Agent**, configure los ajustes por omisión que deberán incluirse en el kit de Silent Agent y en la política por omisión.
 - **Dirección de Security Console.** Introduzca la dirección IP de la MV de la Security Console. Silent Agent utiliza estas direcciones para comunicarse con la Security Console.
 - **Dirección Security Virtual Appliance .** Escriba la dirección IP de la instancia Security Virtual Appliance a la que se conecta ese Silent Agent de forma predeterminada. Si ha implementado múltiples instancias de Security Virtual Appliance, utilizará políticas para direccionar los agentes a la instancia de Security Virtual Appliance adecuada. Para más información, diríjase a [“Instalación recomendada con múltiples SVAs”](#) (p. 23).
 - **Usar SSL.** Seleccione esta opción si desea asegurar la comunicación entre Silent Agent y el Security Virtual Appliance usando Secure Sockets Layer (SSL). Tenga en

cuenta que activar el cifrado SSL para el tráfico Silent Agent - Security Virtual Appliance afectará ligeramente al rendimiento.



Nota

La comunicación entre Silent Agent y Security Console siempre se cifra usando SSL, con independencia de cómo configure esta opción.

El puerto de comunicación Silent Agent - Security Virtual Appliance depende del uso del cifrado SSL:

- El puerto utilizado para la comunicación asegurada con SSL es el 7083.
- El puerto usado para la comunicación no segura es el 7081.

4. **¡Sólo cuenta de empresa!** Bajo **Configuración proxy**, seleccione **Usar proxy** si la máquina Security Console se conecta a Internet a través de un servidor proxy. Debe configurar las siguientes opciones:

- Dirección del servidor proxy.
- Número de puerto usado por el servidor proxy.
- Nombre de usuario reconocido por el proxy.
- Contraseña válida para el nombre de usuario especificado anteriormente.



Nota

Security Console no soporta servidores proxy que usen la autenticación de Active Directory. Se describe una alternativa para el método de autenticación NTLM en este [artículo de la base de datos de conocimientos](#).

5. **¡Sólo cuenta de empresa!** Bajo **Configuración SMTP**, puede configurar Security Console para enviar informes por e-mail y notificaciones usando un servidor de correo externo en lugar del servidor de correo postfix incorporado. Si no especifica ninguna configuración, Security Console usa el servidor de correo incluido.

- **IP/ Nombre del host.** Introduzca la dirección IP o el nombre del host del servidor de correo que va a enviar los e-mails.
- **Puerto.** Introduzca el puerto utilizado para conectarse con el servidor de correo.
- **Nombre de Usuario.** Si el servidor SMTP requiere autenticación, introduzca una dirección de e-mail / nombre de usuario reconocible.
- **Contraseña.** Si el servidor SMTP requiere autenticación, introduzca la contraseña del usuario especificado anteriormente.
- **Desde el nombre.** Introduzca el nombre que quiere que aparezca en campo De del e-mail (el nombre del remitente).
- **Desde el e-mail.** Introduzca la dirección de e-mail que quiere que aparezca en el campo De del e-mail (dirección de e-mail del remitente).



Nota

Security Console no soporta conexión cifrada (SSL, TLS) al servidor de correo.

6. **¡Sólo cuenta de empresa!** En **Licencia** puede ver los detalles de la licencia actual. Para más información, diríjase a **“Licencias y registro”** (p. 30).
7. Configure las opciones de cuenta según sus preferencias en **Configuración**.
 - **Zona horaria.** Elija desde 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 desde el menú el idioma de visualización de la consola.
 - **Logotipo.** Puede cambiar el logotipo predeterminado con forma de nube de Security Console con el logotipo de su empresa. Esto le permitirá personalizar el diseño de los informes PDF. Para cambiar el logo, haga clic en **Personalizar** y cargue el archivo de imagen del logotipo desde su equipo. Se aplican las siguientes restricciones:
 - Dimensiones del logotipo: 81x41 pixels.
 - Formatos de archivo soportados: PNG y JPG.
8. Haga clic en **Enviar** para guardar los cambios.

3.6. Trabajar con datos de la tabla

Las tablas se usan frecuentemente en la consola para organizar los datos en un formato más fácil de usar. Puede que esta información le sea útil:

- Las tablas pueden distribuirse en varias páginas (por omisión se muestran únicamente diez entradas por página). Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla. Para cambiar el número de entradas mostradas en una página, seleccione una opción desde el menú junto a los botones de navegación.
- Para encontrar fácilmente lo que está buscando, utilice los cuadros de búsqueda o las opciones de filtrado bajo los encabezados de columna.
- También puede hacer clic en los encabezados de la columna para ordenar la información por una columna específica. Haga clic en el encabezado de la columna nuevamente para cambiar el sentido de ordenación.

Para asegurarse de que se está mostrando la última información, haga clic en el botón  **Refrescar** en la esquina inferior izquierda de la tabla.

4. Licencias y registro

Security for Virtualized Environments incluye un período de prueba gratuito de 30 días, durante el cual puede probar el producto y decidir si es la solución adecuada para su organización. Para continuar utilizando el producto tras expirar el periodo de prueba, debe adquirir una clave de licencia y usarla para registrar el producto.



Importante

Si no registra el producto, dejarán de funcionar los análisis antimalware, las actualizaciones de firmas de malware y las mejoras del producto.

La versión multiplataforma de Security for Virtualized Environments se licencia por cada máquina virtual. Para comprar una licencia, contacte con un reseller de Bitdefender o contáctenos a través del e-mail enterprisesales@bitdefender.com. Por favor, escriba su correo en inglés para que podamos ayudarle rápidamente.

4.1. 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. 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 ocurre, seleccione su país de residencia 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. Por favor, escriba su correo en inglés para que podamos ayudarle rápidamente.

4.2. Comprobar los detalles de licencia actuales

Para ver los detalles de su licencia:

1. Conéctese a Security Console usando su **cuenta de empresa**.
2. Vaya a la página **Cuentas > Mi cuenta**.
3. En **Licencia** puede ver los detalles de licencia actuales.

4.3. Registro de su producto

Para registrar su producto o cambiar su clave de licencia actual:

1. Conéctese a Security Console usando su **cuenta de empresa**.
2. Vaya a la página **Cuentas > Mi cuenta**.
3. Bajo **Licencia**, haga clic en el enlace disponible. Se mostrará la página **Información de licencia**. Si el producto ya ha sido registrado con una clave de licencia, puede ver la información sobre la misma.
4. Introduzca la clave de licencia en el campo correspondiente.
5. Haga clic en **Cambiar clave**.

5. Panel de monitorización

Cada vez que se conecta a Security Console, se muestra la página **Panel** automáticamente. El panel de control es una página de estado que consiste en siete portlets que le proporcionan una rápida visión general sobre la seguridad de todas las máquinas virtuales protegidas.

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. Cada portlet del panel incluye un informe detallado en segundo plano, accesible haciendo clic sobre el gráfico.

Algunos portlets ofrecen información de estado, mientras otros informan sobre los sucesos de la seguridad en el último periodo. Puede comprobar y configurar el periodo de informe de un portlet haciendo clic en el botón  de su barra de título.

5.1. Portlets de panel

El panel de control consiste en los siguientes portlets:

Estado de la Red

Le proporciona información detallada sobre el estado general de seguridad de la red. Los equipos se agrupan basándose en estos criterios:

- Los equipos no administrados no tienen instalada la protección Security for Virtualized Environments y su estado de seguridad no puede evaluarse. Los agentes de Security for Virtualized Environments instalados en máquinas virtuales protegidas detectan automáticamente los equipos no administrados. Pueden representar no solo máquinas virtuales, sino también equipos físicos (si están conectados a la red virtual).
- Los equipos offline normalmente tienen la protección Security for Virtualized Environments instalada, pero no hay actividad reciente de Silent Agent. El estado de seguridad de los equipos offline no puede evaluarse con precisión porque la información sobre su estado no es reciente. Para más información, diríjase a [“Sobre equipos offline”](#) (p. 36).
- Los equipos protegidos tienen instalada la protección Security for Virtualized Environments y no se han detectado amenazas de seguridad.
- Los equipos vulnerables tienen instalada la protección de Security for Virtualized Environments, pero determinadas condiciones impiden la adecuada protección del sistema. Los detalles del informe le muestran qué aspectos de la seguridad necesitan abordarse.

Estado del equipo

Le proporciona diversas informaciones de estado relativas a los equipos en los que se ha instalado la protección Security for Virtualized Environments.

- Estado de actualización de protección
- Estado de protección antimalware
- Estado de la licencia
- Estado de actividad de la red (online/offline)

Puede aplicar filtros según aspectos de la seguridad y estado para encontrar la información que está buscando.

Equipos más infectados

Muestra los equipos más infectados en la red en un periodo de tiempo específico.

Malware más detectado

Le muestra las principales amenazas malware detectadas en la red en un periodo de tiempo específico.

Actividad de malware

Le ofrece detalles generales y por equipo sobre las amenazas de malware detectadas en la red en un periodo de tiempo específico. Puede ver:

- Número de detecciones (archivos que se han encontrado infectados con malware)
- Número de infecciones resueltas (archivos que han sido desinfectados o aislados con éxito en la carpeta de cuarentena)
- Número de infecciones bloqueadas (archivos que no pudieron desinfectarse pero se ha rechazado el acceso ellos; por ejemplo, un archivo infectado almacenado en algún formato comprimido propietario)

Estado malware de los equipos

Le ayuda a encontrar cuántos y cuáles de los equipos protegidos han sido afectados por malware en un periodo de tiempo específico y cómo se han tratado las amenazas. Los equipos se agrupan basándose en estos criterios:

- Equipos sin detecciones (no se ha detectado ninguna amenaza malware en el periodo de tiempo especificado)
- Equipos con malware solucionado (todos los archivos detectados han sido desinfectados correctamente o aislados en la carpeta de cuarentena local)
- Equipos con malware bloqueado (se ha rechazado el acceso a algunos de los archivos detectados)

Notificaciones

Este portlet, que aparece minimizado por omisión, le informa sobre los riesgos de seguridad existentes en el entorno virtualizado. Las notificaciones también se le envían por email.

5.2. Administrar Portlets

El panel de control es fácil de configurar basándose en las preferencias individuales.

Puede minimizar los portlets para centrarse en la información en la que está interesado. Cuando minimiza un portlet, se elimina del panel de control y su barra de título aparece en la parte inferior de la página. Los portlets restantes se dimensionan automáticamente para ajustarse a la pantalla. Todos los portlets minimizados pueden restaurarse en cualquier momento.

Para gestionar un portlet, utilice los botones de su barra de título:

-  La opción de refresco cargará datos para cada portlet.
-  Haga clic en este botón para configurar las opciones del portlet. Algunos portlets incluyen datos de un periodo de tiempo específico.
-  Minimice el portlet en la parte inferior de la página.
-  Restaure un portlet minimizado.

6. Administración de equipos (Máquinas Virtuales)

Para ver información de los equipos (máquinas virtuales) en su entorno virtualizado y administrar su seguridad, diríjase a la página **Equipos > Ver equipos**. Además de las máquinas virtuales protegidas por Security for Virtualized Environments, también puede ver otras MVs detectadas en la red virtual. También podrían detectarse los equipos físicos si estuvieran conectados a la red virtual.

Desde la página **Ver equipos**, puede hacer lo siguiente:

- [Organice las máquinas virtuales en grupos](#) para administrar su seguridad de forma más eficiente. Esto se recomienda si administra un gran número de MVs (diez o más).
- [Comprobar el sistema y los detalles de protección](#).
- [Ver y modificar la configuración de las políticas de seguridad](#).
- Ejecute tareas de análisis en máquinas virtuales de forma remota para instalar o desinstalar la protección Security for Virtualized Environments. Para más información, consulte [“Ejecutar y administrar tareas” \(p. 63\)](#).
- [Cree informes rápidos](#) para obtener diversa información de seguridad sobre máquinas virtuales específicas.

La página contiene dos paneles:

- El panel izquierdo le ayuda a [organizar sus máquinas virtuales en grupos](#).
- El panel de la derecha contiene una tabla que muestra las máquinas virtuales e información útil sobre ellas:
 - Nombre y dirección IP de la MV.
 - Sistema operativo instalado en la MV.
 - Actualice el estado de la protección de Security for Virtualized Environments.
 - Cuando la MV se ha detectado por última vez.



Nota

Es importante supervisar el campo **Visto por última vez** dado que largos periodos de inactividad podrían indicar que el equipo está desconectado.

El icono situado al lado del nombre de cada equipo le informa rápidamente sobre ese equipo:

- Máquina virtual en la que está instalada la protección Security for Virtualized Environments.

- ❑ Equipo físico o virtual en el que la protección de Security for Virtualized Environments no ha sido instalada aún, detectado en la red virtual por MVs protegidas.
- ☑ Equipo que ha excluido de la administración.

6.1. Acerca de equipos administrados, no administrados y excluidos

Los equipos se organizan en tres categorías principales:

- **Equipos administrados** - MVs en las que se ha instalado la protección Security for Virtualized Environments.
- **Equipos no administrados** - los equipos detectados en los que la protección Security for Virtualized Environments todavía no se ha instalado.



Nota

Una vez instalado en una MV, Silent Agent detecta automáticamente los equipos visibles en la red local. Los equipos no administrados estarán disponibles en la página **Ver equipos** en cuanto sean detectados. También podrían detectarse los equipos físicos si estuvieran conectados a la red virtual.

- **Equipos excluidos** - equipos que ha excluido de la administración.

Utilice el menú **Mostrar** ubicado encima de la tabla (a la izquierda) para elegir las categorías de equipo a mostrar.

6.2. Sobre equipos offline

Los equipos offline normalmente tienen la protección Security for Virtualized Environments instalada, pero no hay actividad reciente de Silent Agent. Se considera que los equipos están offline si Silent Agent está inactivo durante más de 1 minuto.

Posibles razones por las cuales los equipos aparecen offline:

- El equipo está apagado, en suspensión o hibernando.



Nota

Los equipos normalmente aparecen online incluso cuando están bloqueados o el usuario está desconectado.

- Silent Agent se ha desinstalado manualmente del equipo. En estos casos, debe eliminar manualmente el equipo de la página **Equipos > Ver equipos**.
- Silent Agent no puede comunicarse con la Security Console. El puerto de comunicación es el 8082. La comunicación puede ser bloqueada por el cortafuegos local o por el cortafuegos de una red o router.

- Puede que Silent Agent no esté funcionando adecuadamente.

Para averiguar cuánto tiempo han estado inactivos los equipos:

1. Vaya a la página **Equipos > Ver equipos**.
2. Compruebe el campo **Visto por última vez**. Para encontrar fácilmente la información que necesita, escoja **Offline** del menú correspondiente y después ordene los equipos por periodo de inactividad haciendo clic en la cabecera de la columna.

Puede ignorar periodos de inactividad más cortos (minutos, horas) pues probablemente sean resultado de una situación temporal. Por ejemplo, el equipo está actualmente apagado.

Los periodos de inactividad más largos (días, semanas) normalmente indican un problema con el equipo.

6.3. Enumerando máquinas Security Virtual Appliance

Para ver las máquinas Security Virtual Appliance implementadas en su entorno:

1. Vaya a la página **Equipos > Ver equipos**.
2. Haga clic en el menú **Mostrar** ubicado encima de la tabla (a la izquierda) y elija **Security Virtual Appliances**.

Solamente puede ver información de las máquinas Security Virtual Appliance existentes. No hay tareas rápidas o informes disponibles para Security Virtual Appliance.

Si la columna **Actualizar** muestra el estado **pendiente**, hay una actualización disponible para la máquina Security Virtual Appliance correspondiente. Security Virtual Appliance solamente puede actualizarse manualmente desde la consola de la máquina virtual. Para obtener más información, busque en las notas de la versión de la actualización disponible en el [Centro de soporte de Bitdefender](#).

6.4. Utilización de grupos

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

Los grupos se muestran en el panel izquierdo de la página **Ver equipos**. Inicialmente, sólo está el grupo raíz con el nombre de su empresa. Todas las MVs en las que ha instalado la protección Security for Virtualized Environments, además de las detectadas en la red, se sitúan automáticamente en este grupo. Puede organizar sus MVs creando grupos bajo el grupo raíz y luego mover las MVs al grupo adecuado.



Importante

Por favor, tenga en cuenta lo siguiente:

- Un grupo puede contener tanto máquinas virtuales como otros grupos.
- Cuando selecciona un grupo en el panel de la izquierda, puede ver todas las MVs excepto las ubicadas en sus subgrupos. Para ver todas las MVs incluidas en el grupo y en sus subgrupos, haga clic con el botón derecho en el grupo y elija **Ver todos los equipos**.

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 MVs basándose en uno de los siguientes criterios o en una combinación de ellos:

- Host o red virtual de la que forman parte.
- Estructura de la organización (Ventas, Marketing, Control de calidad, Desarrollo de software, Dirección, etc.).
- Necesidades de seguridad (desktops, portátiles, servidores, etc.).
- Ubicación (sede central, oficinas locales, trabajadores remotos, oficinas domésticas, etc.).

Creando Grupos

Para dividir su entorno virtualizado en grupos:

1. Haga clic con el botón derecho en el grupo raíz en el panel izquierdo y seleccione **Crear grupo**. Un nuevo grupo (llamado **Nuevo Grupo**) aparecerá debajo del grupo padre en el árbol de menú.
2. Renombre el grupo creado recientemente.
3. Siga los pasos previos para crear grupos adicionales.
4. [Mover MVs](#) desde el grupo raíz al grupo adecuado.

Para crear subgrupos:

1. Haga clic con el botón derecho en el grupo dentro del cual desea crear el subgrupo, y seleccione la opción **Crear grupo**. Un nuevo grupo (llamado **Nuevo Grupo**) aparecerá debajo del grupo padre en el árbol de menú.
2. Renombre el grupo creado recientemente.

Renombrando Grupos

Para renombrar un grupo, haga clic con el botón derecho sobre él, seleccione **Renombrar grupo** e introduzca un nuevo nombre.

Moviendo Grupos

Los grupos pueden moverse a cualquier sitio dentro de la jerarquía del grupo. Para mover un grupo, arrastre y suéltelo desde la ubicación actual a la nueva.

Mover MVs a otro grupo

Para mover las MVs desde el grupo actual a otro grupo:

1. Marque las casillas de verificación correspondientes a las MVs que quiere mover.
2. Arrastre y suelte su selección sobre el grupo deseado en el panel izquierdo.

Eliminando Grupos

Sólo puede eliminar grupos vacíos (que no contengan equipos).

Para eliminar un grupo:

1. Mueva todos los equipos del grupo a otros grupos. Si el grupo incluye subgrupos, puede elegir mover todos los subgrupos en lugar de equipos individuales.
2. Haga clic con botón derecho en el grupo y seleccione **Eliminar grupo**. Tendrá que confirmar esta acción haciendo clic en **Sí**.

6.5. Buscar y ordenar equipos

Dependiendo del número de MVs, la tabla de equipos puede ampliarse a varias páginas (sólo se muestran de forma predeterminada 10 entradas por página). Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla. Para cambiar el número de entradas mostradas en una página, seleccione una opción desde el menú junto a los botones de navegación.

Si hay muchas entradas, puede utilizar los cuadros de búsqueda o los menús bajo los encabezados de columna para filtrar la información mostrada. Por ejemplo, puede buscar un equipo específico o elegir ver solamente los equipos offline.

También puede hacer clic en los encabezados de la columna para ordenar la información por una columna específica. Por ejemplo, si desea ordenar los equipos por el nombre, haga clic en el encabezado **Nombre del equipo**. Si hace clic en el encabezado otra vez, los equipos se mostrarán en orden inverso.

Al usar grupos, seleccione un grupo en el panel izquierdo para ver los equipos que contiene. Tenga en cuenta que de forma predeterminada no se muestran los equipos ubicados en subgrupos. Para ver todos los equipos incluidos en el grupo y sus subgrupos, haga clic con el botón derecho en el grupo y elija **Ver todos los equipos**.

6.6. Comprobación del sistema y detalles de protección

Desde la página **Ver equipos**, puede encontrar diversa información sobre cualquier equipo:

- Los detalles generales del equipo, tales como su nombre, dirección IP o sistema operativo.
- Configuración de políticas de seguridad.
- Licencia y estado de actualización de la protección de Security for Virtualized Environments.
- Estado de protección antimalware (habilitado o deshabilitado).
- Información relativa al malware detectado en el equipo.
- Último registro de análisis.

Para obtener detalles del sistema y la protección:

1. Vaya a la página **Equipos > Ver equipos**.
2. Si ha organizado las máquinas virtuales en grupos, seleccione el grupo deseado en el panel izquierdo. Para ver todas sus MVs, haga clic con el botón derecho en el grupo raíz y elija **Ver todos los equipos**.
3. Haga clic en el nombre de la MV en la que esté interesado. Se muestra la página de detalles del equipo. Haga clic en los enlaces disponibles para obtener más información.

6.7. Comprobar y modificar la configuración de seguridad

Opciones de seguridad en las máquinas virtuales que se administran usando políticas. Para más información, diríjase a [“Políticas de Seguridad” \(p. 44\)](#).

Para ver la configuración de seguridad aplicada en una máquina virtual concreta:

1. Vaya a la página **Equipos > Ver equipos**.
2. Si ha organizado las máquinas virtuales en grupos, seleccione el grupo deseado en el panel izquierdo. Para ver todas sus MVs, haga clic con el botón derecho en el grupo raíz y elija **Ver todos los equipos**.
3. Haga clic en el nombre de la MV en la que esté interesado.
4. Compruebe el campo **Política activa**. Haga clic en el nombre de la política para ver su configuración.
5. Si la política predeterminada está activa, no puede cambiar la configuración de seguridad. Debe crear una nueva política y asignarla a la MV.

Si ya ha asignado una nueva política a la MV, puede cambiar las opciones de seguridad según sea necesario. Por favor, tenga en cuenta que cualquier cambio que haga se aplicará también a todas las demás MVs en las que está activa la política.

6.8. Crear informes rápidos

Para crear informes rápidos desde la página **Ver equipos**:

1. Haga clic en el menú **Mostrar** localizado encima de la tabla (a la izquierda) y elija **Equipos administrados**.
2. Si ha organizado las máquinas virtuales en grupos, seleccione el grupo deseado en el panel izquierdo. Para ver todas sus MVs, haga clic con el botón derecho en el grupo raíz y elija **Ver todos los equipos**.
3. Marque las casillas de verificación correspondientes a las MVs que se incluirán en el informe.
4. Haga clic en **Informes** y elija el **tipo de informe** desde el menú. Los informes de actividad solamente incluirán datos de la última semana.

6.9. Excluyendo Equipos de la Administración

Silent Agent detecta automáticamente todos los equipos visibles en la red local. Los equipos detectados se muestran en Security Console como no administrados, de forma que pueda instalar remotamente la protección en ellos. También podrían detectarse los equipos físicos si estuvieran conectados a la red virtual.

Si no tiene en mente administrar algunos de los equipos detectados, puede moverlos a la lista **Equipos excluidos**. De esta forma no se preocupará de ellos.

Para excluir de la administración a los equipos detectados:

1. Vaya a la página **Equipos > Ver equipos**.
2. Haga clic en el menú **Mostrar** localizado encima de la tabla (a la izquierda) y elija **Equipos no administrados**.
3. Marque las casillas de verificación correspondientes a las máquinas virtuales que desea excluir.
4. Haga clic en el botón **Tareas** en la esquina superior derecha de la página y seleccione **Excluir**.

Si la protección se instala manualmente en una máquina virtual excluida, se trasladará automáticamente a la lista **Equipos administrados**.

Para ver los equipos excluidos:

1. Vaya a la página **Equipos > Ver equipos**.

2. Desde el menú encima de la tabla, elija **Equipos excluidos**.
3. Si quiere restaurar un equipo excluido, debe eliminarlo de la consola. Haga clic en el botón **Tareas** en la esquina superior derecha de la página y elija **Eliminar**.

6.10. Eliminar equipos de la consola

Hay varias situaciones en las que puede que desee eliminar equipos desde la consola:

- Para limpiar de entradas duplicadas o equipos inactivos la lista de equipos administrados. Por ejemplo, al reinstalar el sistema operativo en una máquina virtual sin eliminar previamente el Silent Agent, debe borrar manualmente la entrada correspondiente de la lista.
- Para limpiar de entradas duplicadas o equipos inactivos la lista de equipos no administrados.
- Para restaurar un equipo excluido.

Si el equipo eliminado está todavía conectado a la red, al final será detectado y mostrado en la consola como no administrado.

Para eliminar máquinas virtuales administradas:

1. Vaya a la página **Equipos > Ver equipos**.
2. Haga clic en el menú **Mostrar** localizado encima de la tabla (a la izquierda) y elija **Equipos administrados**.
3. Si ha organizado las máquinas virtuales en grupos, seleccione el grupo deseado en el panel izquierdo. Para ver todas sus MVs, haga clic con el botón derecho en el grupo raíz y elija **Ver todos los equipos**.
4. Marque las casillas de verificación correspondientes a las MVs que quiere eliminar.



Nota

- Compruebe el campo **Detectada por última vez** para identificar MVs inactivas durante un largo periodo de tiempo.
 - Busque u ordene los equipos por nombre para identificar entradas duplicadas o MVs que hayan sido desconectadas permanentemente de la red.
5. Haga clic en el botón **Tareas** en la esquina superior derecha de la página y elija **Desinstalar Silent Agent**. Se desinstalará la protección en las MVs seleccionadas y se eliminarán de la consola.

Para eliminar los equipos excluidos:

1. Vaya a la página **Equipos > Ver equipos**.
2. Desde el menú encima de la tabla, elija **Equipos excluidos**.

3. Marque las casillas de verificación correspondientes a los equipos que desea eliminar.
4. Haga clic en el botón **Tareas** en la esquina superior derecha de la página y elija **Eliminar**.

Para eliminar equipos no administrados:

1. Primero debe [excluir de la administración](#) los equipos no administrados que desee eliminar.
2. Elimine los equipos excluidos como se ha descrito anteriormente.

7. Políticas de Seguridad

Una vez instalada, la protección de Security for Virtualized Environments puede configurarse y administrarse desde Security Console utilizando las políticas de seguridad. Una política específica la configuración de seguridad a aplicar en las máquinas virtuales objetivo.

Inmediatamente después de la instalación, se asigna a las máquinas virtuales la política predeterminada, que está preconfigurada con las opciones de protección recomendadas. La política predeterminada está indicada para usarse como plantilla para crear nuevas políticas.

Dado que la política predefinida no puede editarse, debe crear al menos una nueva política para cambiar las opciones de protección en las máquinas virtuales. Si administra un número grande de máquinas virtuales (diez o más), puede que desee crear varias políticas para aplicar diferentes configuraciones basadas en los requisitos de seguridad.

Esto es lo que necesita saber sobre políticas:

- Hay una única plantilla de política predeterminada que permite configurar todas las opciones de protección. Algunos ajustes de política no están disponibles para Linux y así se indica en esta documentación.
- Las políticas se transfieren inmediatamente a las máquinas virtuales objetivo una vez creadas o modificadas. La configuración debería aplicarse a las máquinas virtuales en menos de un minuto (siempre que estén conectadas). Si una máquina virtual no está conectada, la configuración se aplicará tan pronto como vuelva a conectarse.
- Pueden asignarse políticas tanto a máquinas virtuales individuales como a grupos de máquinas virtuales. El objetivo de la política no puede ser una combinación de máquinas virtuales y grupos.
- Pueden asignarse varias políticas en un momento dado a una máquina virtual. Sin embargo, siempre habrá una única política activa: aquella que se haya creado o modificado en último lugar.
- Las opciones de análisis on-access solamente tienen efecto en máquinas Windows y en las máquinas Linux específicas en las cuales está [activo el soporte de análisis on-access](#).

Para ver y administrar la configuración de seguridad y las políticas, diríjase a la página **Políticas > Ver políticas**. Las políticas existentes se muestran en la tabla. Para cada política, puede ver:

- Nombre de política.
- Objetivo de política (máquinas virtuales o grupos a los que se aplica la política).
- Cuántas de las máquinas virtuales objetivo cumplen con la política.

- El usuario que creó la política.
- Hora en la que se modificó por última vez la política.

7.1. Creando Nuevas Políticas

Para crear una nueva política:

1. Diríjase a la página **Políticas > Nueva política**.
2. Escriba un nombre descriptivo para la política. Al elegir un nombre, considere el propósito y objetivo de la política.
3. Seleccione una plantilla de política desde el menú. La nueva política se iniciará con la configuración de la política de plantilla.
4. Configure el objetivo de la política (las máquinas virtuales a las que se aplicará la política). Puede seleccionar una de de las siguientes opciones:
 - **Grupos.** Seleccione esta opción para aplicar la política a los grupos de máquinas virtuales administradas. Haga clic en el enlace correspondiente y elija los grupos deseados.



Nota

La política se aplicará automáticamente a cualquier máquina virtual que se añada posteriormente al grupo seleccionado.

- **Equipos.** Seleccione esta opción para aplicar la política a máquinas virtuales individuales. Haga clic en el enlace correspondiente y elija las máquinas virtuales deseadas.
5. Haga clic en **Enviar** para crear la política e ir a la página de políticas.
 6. A continuación, configure las opciones de la política. Para información detallada, diríjase a [“Configurar opciones de política”](#) (p. 45).
 7. Haga clic en **Guardar** para guardar los cambios y aplicar los ajustes de protección a las máquinas virtuales objetivo. La nueva política se mostrará en la página **Ver políticas**.

7.2. Configurar opciones de política

Las opciones de la política pueden configurarse en el momento de crear la política. Puede modificarlas más adelante según sea necesario.



Importante

No puede editar la política predeterminada. No se guardarán los cambios. Para cambiar la configuración de protección, cree una nueva política.

Para cambiar la configuración de una política:

1. Diríjase a la página **Políticas > Ver políticas**.
 2. Haga clic en el nombre de la política. Esto abrirá la página de políticas.
 3. Configure las opciones de la política según sea necesario. Los ajustes se organizan en las siguientes categorías:
 - [Resumen](#)
 - [General](#)
 - [Antimalware](#)
- Puede seleccionar la categoría de configuración usando el menú del lateral izquierdo de la página.



Importante

Algunos ajustes de política no están disponibles para Linux:

- **General.** Los ajustes del servidor de análisis en la pestaña [Avanzado](#) y los ajustes del proxy en la pestaña [Actualización](#) se aplican tanto a Windows como a Linux. Todas las demás opciones de configuración de esta categoría sólo están disponibles para la versión Windows de Silent Agent.
 - **Antimalware.** Las opciones de análisis on-access solamente tienen efecto en máquinas Windows y en las máquinas Linux específicas en las cuales está [activo el soporte de análisis on-access](#).
4. Haga clic en **Guardar** para guardar los cambios y aplicarlos a las máquinas virtuales objetivo. Para abandonar la página de política sin guardar los cambios, haga clic en **Cancelar**.

7.2.1. Resumen

La página resumen contiene los detalles de la política general:

- **Nombre de política.** Puede renombrar la política introduciendo un nuevo nombre en este campo.
- **Objetivo especificado.** Si quiere cambiar el objetivo de la política, haga clic en el enlace y seleccione un nuevo objetivo.
- **Conforme.** Este campo indica cuántas de las máquinas virtuales objetivo cumplen la política.

7.2.2. General

Los ajustes generales le ayudan a administrar las opciones de visualización de la interfaz de usuario, preferencias de actualización, protección por contraseña y otros ajustes de Silent Agent.

Los ajustes se organizan bajo las siguientes pestañas:

- [Visualizar](#)
- [Avanzado](#)
- [Actualización](#)



Importante

Los ajustes del servidor de análisis en la pestaña [Avanzado](#) y los ajustes del proxy en la pestaña [Actualización](#) se aplican tanto a Windows como a Linux. Todas las demás opciones de configuración de esta categoría sólo están disponibles para la versión Windows de Silent Agent.

Pestaña Mostrar

En esta sección puede configurar las opciones de visualización de la interfaz de usuario. Silent Agent tiene una mínima interfaz de usuario, que permite al usuario en la máquina virtual revisar el estado de protección y eventos.

- **Modo Oculto.** Cuando se habilita el Modo Silencioso, la interfaz gráfica de usuario (GUI) del Silent Agent no se carga automáticamente al inicio del sistema, liberando los recursos correspondientes. Así mismo, no se muestra el icono del Silent Agent  en el área de notificación de Windows (también conocida como bandeja del sistema). El icono del área de notificación permite a los usuarios abrir la ventana principal del programa y acceder a la información del producto. Incluso aunque el icono del área de notificación no esté disponible, los usuarios pueden en cualquier caso acceder a la ventana principal del programa desde el menú Inicio de Windows.
- **Información del soporte técnico.** Rellene los campos para personalizar la información de soporte y contacto disponible en Silent Agent. Los usuarios pueden acceder a esta información desde la ventana Silent Agent haciendo clic en el icono  en la esquina inferior derecha (o de forma alternativa en el icono  Silent Agent del área de notificación del sistema y haciendo clic en **Acerca de**).

Pestaña avanzada

En esta sección puede configurar los ajustes generales y la contraseña de desinstalación.

- **Eliminar eventos con una antigüedad superior a {30} días.** Silent Agent mantiene un registro detallado de los eventos relacionados con la actividad en el equipo. Por omisión, los eventos se eliminan del registro pasados 30 días. Si desea cambiar este intervalo, seleccione una opción diferente desde el menú.
- **Enviar informes de bloqueos a Bitdefender.** Seleccione esta opción de forma que los informes se envíen a los laboratorios de Bitdefender para su análisis si Silent Agent se bloquea. Los informes ayudarán a nuestros ingenieros a descubrir qué causó el problema y evitar que éste vuelva a ocurrir. No se enviará información personal.

- **Configuración de contraseña.** Para evitar que usuarios con derechos administrativos desinstalen la protección, debe configurar una contraseña.

Para establecer la contraseña, o cambiar la contraseña actual, seleccione **Activar contraseña** e introduzca la contraseña deseada. Para eliminar la protección por contraseña, seleccione **Desactivar contraseña**.

- **Servidores de análisis.** Silent Agent está configurado de forma predeterminada para usar el Security Virtual Appliance especificado en la [Cuenta de empresa de Security Console](#). En entornos con diversas instalaciones de Security Virtual Appliance, debe especificar las instancias Security Virtual Appliance a las que se puede conectar Silent Agent. Puede cambiar la dirección de Security Virtual Appliance existente o añadir las direcciones de otras instancias Security Virtual Appliance.

Silent Agent selecciona una de las instancias de Security Virtual Appliance especificadas, basándose en la prioridad asignada, disponibilidad y carga actual (normal, con sobrecarga, bajo de carga).

- Si el Security Virtual Appliance con prioridad 1 no está disponible inicialmente, o deja de estarlo más tarde, Silent Agent intenta conectar con el Security Virtual Appliance con prioridad 2 y así sucesivamente, hasta que encuentre un Security Virtual Appliance que esté disponible.
- Si la instancia de Security Virtual Appliance seleccionada informa repetidamente de sobrecarga, Silent Agent reinicia el proceso de selección, e intenta conectarse a una instancia de Security Virtual Appliance que tenga una carga normal. Si esta instancia no estuviera disponible, Silent Agent se conecta a la instancia de Security Virtual Appliance con menos carga o menos sobrecargada (si la hubiera).
- Si la instancia de Security Virtual Appliance seleccionada informa repetidamente de sobrecarga, Silent Agent busca y se conecta a una instancia de Security Virtual Appliance que tenga una carga normal (si la hubiera).



Nota

El mecanismo de balanceo de carga ayuda a mejorar el rendimiento, a recuperar rápidamente en caso de fallos de Security Virtual Appliance y ahorra recursos en los hosts en los que Security Virtual Appliance está por debajo de carga.

Para añadir un Security Virtual Appliance:

1. Escriba la dirección IP o nombre del Security Virtual Appliance en el campo de edición.
2. Si quiere asegurar la comunicación entre el Silent Agent y el Security Virtual Appliance utilizando Secure Sockets Layer (SSL), seleccione **Usar SSL**. Tenga en cuenta que activar el cifrado SSL para el tráfico Silent Agent - Security Virtual Appliance afectará ligeramente al rendimiento.

El puerto de comunicación Silent Agent - Security Virtual Appliance depende del uso del cifrado SSL:

- El puerto utilizado para la comunicación asegurada con SSL es el 7083.
 - El puerto usado para la comunicación no segura es el 7081.
3. Haga clic en el botón **+** **Añadir**.
 4. Utilice los iconos Subir/Bajar en la columna **Acción** para establecer la prioridad del Security Virtual Appliance. Si el primer servidor de análisis no está disponible, los agentes lo intentarán con el segundo y así sucesivamente.



Importante

Ajuste el Security Virtual Appliance preferido para las instancias Silent Agent seleccionadas con prioridad 1.

Para eliminar un Security Virtual Appliance de la lista, haga clic en el botón **X** **Eliminar** correspondiente.

Pestaña Actualizar

En esta sección puede configurar las opciones de actualización de Silent Agent. Las actualizaciones son muy importantes ya que permiten luchar contra las últimas amenazas.

- **Intervalo de actualización (horas).** Silent Agent comprueba automáticamente si existen descargas e instala actualizaciones de producto cada hora (configuración predeterminada). Las actualizaciones automáticas se ejecutan de forma silenciosa en segundo plano.

Para cambiar el intervalo de actualización automática, seleccione una opción diferente desde el menú. Tenga en cuenta que la actualización automática no se puede desactivar.



Nota

Aunque el análisis en sí se realiza en el Security Virtual Appliance, que se actualiza automáticamente con regularidad, Silent Agent tiene un conjunto reducido de firmas que se utilizan para las operaciones de preanálisis (como la extracción de archivos desde archivos comprimidos). Los archivos de firmas locales del agente se actualizan automáticamente junto a los del Security Virtual Appliance, con independencia de cómo haya configurado esta opción. Todas las actualizaciones se envían a través del appliance Security Console evitando así el incremento en el tráfico de Internet.

- **Posponer reinicio.** Algunas actualizaciones necesitan reiniciar el sistema para instalarse y funcionar adecuadamente. Al seleccionar esta opción, el programa seguirá trabajando con los archivos antiguos hasta que se reinicie el equipo, sin informar al usuario. Por el contrario, una notificación de la interfaz de usuario solicitará a éste el reinicio del sistema siempre que lo requiera una actualización.

Si elige posponer el reinicio, puede establecer la hora adecuada a la que las máquinas virtuales se reiniciarán automáticamente si (aún) es necesario. Esta opción puede ser muy útil para los servidores virtualizados. Si es necesario, seleccione **Reiniciar tras**

instalar las actualizaciones y especifique cuándo es conveniente reiniciar (diaria o semanalmente en un día determinado, a una hora determinada del día).

- **Activar proxy.** Seleccione esta opción si las máquinas virtuales se conectan a Internet a través de un servidor proxy. Hay dos opciones para establecer la configuración del proxy:
 - **Importar conf. proxy navegador predet.** Silent Agent puede importar la configuración proxy desde los navegadores más populares, incluyendo las últimas versiones de Internet Explorer, Mozilla Firefox y Opera.
 - **Usar configuración del proxy personalizada.** Si conoce los ajustes del proxy, seleccione esta opción y luego especifíquelos:
 - **Servidor** - escriba la IP del servidor proxy.
 - **Puerto** - introduzca el puerto utilizado para conectar con el servidor proxy.
 - **Nombre de usuario** - escriba un nombre de usuario que el proxy reconozca.
 - **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.

7.2.3. Antimalware

Security for Virtualized Environments protege máquinas virtuales contra todo tipo de amenazas de malware (virus, troyanos, spyware, rootkits, adware y otros). La protección antimalware tiene dos componentes:

- **Análisis On-access:** evita que nuevas amenazas de malware se introduzcan en el sistema.
- **Análisis bajo demanda:** permite detectar y eliminar malware que ya reside en su sistema.

Basado en los ajustes configurados en la política, el agente instalado en la máquina virtual decide qué archivos necesitan analizarse y envía una solicitud de análisis al Security Virtual Appliance. El análisis actual se lleva a cabo en el Security Virtual Appliance utilizando tanto el método de detección heurística como basado en firmas. El resultado del análisis se devuelve al agente, que realiza la acción adecuada en función de los ajustes de política y las instrucciones recibidas desde el Security Virtual Appliance.

Por omisión, cuando se detecte un virus u otro malware, Silent Agent intentará eliminar automáticamente el código malware del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección. Las instrucciones de desinfección se obtienen de Security Virtual Appliance. Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse. Los archivos en cuarentena se almacenan localmente en las máquinas virtuales, pero pueden verse y administrarse de forma remota desde la página [Cuarentena](#).

Los usuarios avanzados pueden configurar exclusiones de análisis si no desean que se analicen ciertos archivos o tipos de archivo.

Los ajustes se organizan bajo las siguientes pestañas:

- [Tiempo real](#)

- [Bajo dem](#)
- [Exclusiones](#)
- [Cuarentena](#)



Importante

Las opciones de análisis on-access solamente tienen efecto en máquinas Windows y en las máquinas Linux específicas en las cuales está [activo el soporte de análisis on-access](#).

Pestaña On-access

El análisis on-access evita que nuevas amenazas de malware entren en su sistema analizando los archivos conforme se va accediendo a ellos (se abren, se mueven, se copian o se ejecutan).

Para configurar el análisis on-access:

1. Utilice el conmutador para activar o desactivar el análisis on-access. Si desactiva el análisis on-access, las máquinas virtuales serán vulnerables al malware.
2. Elija el nivel de protección que mejor se adapte a sus necesidades. Para una rápida configuración, arrastre el deslizador a lo largo de la escala hasta un nivel de protección predefinido. Use la descripción del lateral derecho de la escala como guía para su elección.
3. Los usuarios avanzados pueden configurar las opciones de análisis seleccionando la casilla **Personalizado** y haciendo clic en el botón correspondiente.

Opciones de personalización. Los ajustes de análisis están organizados en dos pestañas de la forma siguiente:

- **Tipos de archivo.** Puede configurar Silent Agent para analizar todos los archivos a los que se ha accedido (con independencia de su extensión), sólo archivos de programa o extensiones de archivo específicas que considere peligrosas. Analizando todos los archivos proporciona una mejor protección, mientras analizando solo aplicaciones puede ser utilizado para mejorar el rendimiento del sistema.



Nota

Los archivos de aplicaciones son mucho más vulnerables a los ataques de malware que otro tipo de archivos. Para más información, diríjase a [“Lista de tipos de archivos de aplicación”](#) (p. 87).

Si desea que únicamente se analicen extensiones específicas, seleccione **Extensiones definidas por el usuario** desde el menú correspondiente e introduzca las extensiones (separadas por punto y coma ";") en el campo correspondiente.

- **Archivos.** Seleccione **Analizar dentro de los archivos** si desea activar el análisis on-access de los archivos comprimidos. Analizar dentro de archivos es un proceso lento, requiere muchos recursos, por esta razón no lo recomendamos para la protección en tiempo real. Los archivos comprimidos que contienen archivos infectados no

representan una amenaza inmediata para la seguridad del sistema. El malware puede afectar al sistema sólo si el archivo infectado se extrae del archivo comprimido y se ejecuta sin tener activada la protección de análisis on-access.

Si decide utilizar esta opción, puede configurar las siguientes opciones y optimización:

- **Limitar tamaño de archivo a {10} MB.** Puede establecer un límite máximo de tamaño aceptado para los archivos analizados en tiempo real. Seleccione la casilla correspondiente e introduzca el tamaño máximo del archivo (en MB).
- **Máxima profundidad de archivo (niveles).** Marque la casilla de verificación correspondiente y elija la profundidad de archivo máxima desde el menú. Para el mejor rendimiento elija el valor más bajo; para la máxima protección seleccione el más alto.



Nota

Los archivos comprimidos y archivos ZIP por debajo de 256 KB se analizan automáticamente incluso aunque esté desactivada la opción **Analizar en el interior de los archivos**.

- **Varios.** Seleccione la casilla de verificación correspondiente para activar las opciones de análisis deseadas.
 - **Analizar sólo nuevos&modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.
 - **Análisis aplazado.** Seleccione esta opción para dar prioridad al análisis de archivos accedidos por funciones de lectura sobre aquellos accedidos por funciones de escritura. El fin de esto es optimizar el proceso de análisis.
 - **Analizar en busca de keyloggers.** Los Keyloggers registran lo que escribe en el teclado y envían informes por Internet a alguien con malas intenciones (hacker). El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.
- **Acciones del Análisis.** Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:
 - **Archivos infectados.** Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender. Silent Agent puede eliminar normalmente el código malware de un archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.
Si se detecta un archivo infectado, Silent Agent intentará desinfectarlo automáticamente. Si falla la desinfección, el archivo se mueve a la cuarentena con el fin de contener la infección.



Importante

Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Dado que B-HAVE es una tecnología de análisis heurístico, Silent Agent no puede asegurar que el archivo esté realmente infectado con malware. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

Cuando se detecte un archivo sospechoso, los usuarios no podrán acceder a ese archivo para evitar una posible infección.

Aunque no se recomienda, puede cambiar las acciones predeterminadas. Dispone de las siguientes opciones:

Desinfectar

Elimina el código de malware de los archivos infectados. Se recomienda siempre mantener esta como la primera acción a aplicar en los archivos infectados.

Mover a Cuarentena

Mueva los archivos detectados desde su ubicación actual a la carpeta de cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de cuarentena desde la página [Cuarentena](#) de la consola.

Eliminar

Elimina los archivos detectados del disco, sin mostrar advertencia alguna. Se aconseja que evite utilizar esta acción.

Acceso denegado

Bloquear el acceso a los archivos detectados.

Pestaña Bajo demanda

En esta sección puede configurar las tareas de análisis antimalware que se ejecutarán periódicamente en las máquinas virtuales objetivo, según el calendario que especifique. Los análisis se realizan en segundo plano en silencio, sin que el usuario sepa de ellos.

Aunque no es obligatorio, se recomienda programar un análisis completo del sistema que se ejecute semanalmente en todos los equipos. Analizar los equipos frecuentemente es una medida de seguridad proactiva que puede ayudar a detectar y bloquear malware que pudiera superar las funciones de protección en tiempo real.

Administración de tareas de análisis

La tabla de Tareas de análisis le informa de las tareas de análisis existentes, ofreciéndole importante información de cada una de ellas:

- Nombre de tarea y tipo.
- Hora en la que se ejecutó la tarea por primera vez.
- Programa basado en que la tarea se ejecute regularmente (recurrencia).
- Acciones que puede llevar a cabo en la tarea de análisis.

Puede configurar fácilmente la tarea de análisis por omisión para que se ejecute cuando lo necesite. **Análisis completo del sistema** comprueba todo el sistema buscando todo tipo de malware que amenace su seguridad, como son virus, spyware, adware, rootkits y otros. Las opciones de análisis de la tarea de análisis predeterminada están preconfiguradas y no se pueden cambiar.

Además de la tarea de análisis predeterminada (que no puede eliminar o duplicar), puede crear todas las tareas de análisis personalizadas que desee. Una tarea de análisis personalizada le permite elegir las ubicaciones específicas a analizar y configurar las opciones de análisis.

Para crear y configurar una tarea nueva, haga clic en **Añadir tarea** y elija el tipo de tarea que desea crear. Para modificar la configuración de una tarea existente, haga clic en el nombre de esa tarea. Consulte el siguiente tema para saber cómo configurar las opciones de tareas.

Para eliminar una tarea de la lista, haga clic en el botón correspondiente **X Eliminar**.

Configurando una Tarea de Análisis

Las opciones de tarea de análisis se organizan bajo tres pestañas: General - configurar el nombre de la tarea, programar la ejecución y objetivo de análisis; Opciones - elegir un perfil de análisis para la configuración rápida de las opciones de análisis; Avanzada - configurar las opciones de análisis en detalle. Las pestañas Opciones y Avanzado están disponibles solo para tareas de análisis personalizadas. Sólo se puede acceder a la pestaña Avanzado tras marcar la casilla de verificación **Personalizado** en la pestaña Opciones.

Se describen a continuación las opciones desde la primera pestaña a la última:

- **Detalles de tarea.** Elija un nombre descriptivo para la tarea para poder identificar fácilmente de qué se trata. Al elegir un nombre, tenga en cuenta el objetivo de la tarea de análisis y posiblemente la configuración de análisis.
- **Programador.** Utilice las opciones de programación para configurar el programa de análisis. Puede configurar el análisis para que se ejecute cada pocas horas, días o semanas, empezando a una hora y fecha específica.

Tenga en cuenta que las máquinas virtuales deben estar encendidas a la hora programada. Un análisis programado no se ejecutará en su momento adecuado si la máquina virtual está apagada, hibernando o en modo suspensión, o si ningún usuario ha iniciado sesión. En tales situaciones, el análisis se aplazará hasta la próxima vez.

- **Objetivo.** Añada a la lista todas las ubicaciones que desee analizar en las máquinas virtuales objetivo.

Para añadir un nuevo archivo o carpeta a analizar:

1. Elija desde el menú, bien una ubicación predefinida o bien la opción **Rutas específicas**.
2. Especifique la ruta del objeto a analizar en el campo de edición.
 - Si ha escogido una ubicación predefinida, complete la ruta según sea necesario. Por ejemplo, para analizar la carpeta `Archivos de programa completa`, es suficiente con seleccionar la ubicación predefinida correspondiente desde el menú. Para analizar una carpeta específica desde `Archivos de programa`, debe completar la ruta añadiendo una barra invertida (`\`) y el nombre de la carpeta.



Nota

Para más información, diríjase a [“Usar variables de sistema”](#) (p. 87).

- Si ha elegido **Rutas específicas**, escriba la ruta completa del objeto a analizar. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todas las MVs objetivo.

3. Haga clic en el botón **+** **Añadir**.

Para editar una ubicación existente, haga clic en ella. Para eliminar una ubicación de la lista, haga clic en el botón **X** **Eliminar** correspondiente.

- **Opciones de Análisis.** Para una configuración rápida de las opciones de análisis, elija uno de los perfiles de análisis predefinidos. Mueva el control deslizante por la escala hasta el perfil de protección que mejor se ajuste a sus necesidades. Use la descripción del lateral derecho de la escala como guía para su elección.

Las opciones de análisis de la pestaña **Avanzado**, basadas en el perfil seleccionado, se configuran automáticamente. Sin embargo, si lo desea, puede configurarlas en detalle. Para hacerlo, marque la casilla de verificación **Personalizado** y luego diríjase a la pestaña **Avanzado**.

- **Operaciones de análisis.**

- **Ejecutar la tarea con baja prioridad.** Disminuye la prioridad del proceso de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.

- **Apagar el equipo cuando finalice la tarea.** Esta opción puede ser útil cuando usted ejecuta análisis durante horas no laborables.
- **Tipos de archivo.** Use estas opciones para especificar qué tipos de archivos desea que sean analizados. Puede configurar Silent Agent para analizar todos los archivos (con independencia de su extensión), sólo archivos de programa o extensiones de archivo específicas que considere peligrosas. Analizando todos los archivos se proporciona una mejor protección, mientras que analizar solo aplicaciones puede ser utilizado solamente para realizar un análisis más rápido.



Nota

Los archivos de aplicaciones son mucho más vulnerables a los ataques de malware que otro tipo de archivos. Para más información, diríjase a [“Lista de tipos de archivos de aplicación” \(p. 87\)](#).

Si desea que únicamente se analicen extensiones específicas, seleccione **Extensiones definidas por el usuario** desde el menú correspondiente e introduzca las extensiones (separadas por punto y coma ";") en el campo correspondiente.

- **Archivos.** Los archivos comprimidos que contienen archivos infectados no representan una amenaza inmediata para la seguridad del sistema. El malware puede afectar al sistema sólo si el archivo infectado es extraído del archivo comprimido y ejecutado sin tener la protección en tiempo real activada. Sin embargo, recomendamos utilizar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso si esta no es una amenaza inmediata.



Nota

El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema.

- **Analizar el interior de los archivos.** Seleccione esta opción si desea comprobar los archivos comprimidos en busca de malware. Si decide utilizar esta opción, puede configurar las siguientes opciones y optimización:
 - **Limitar tamaño de archivo a {10} MB.** Puede establecer un límite de tamaño aceptado máximo para los archivos a analizar. Seleccione la casilla correspondiente e introduzca el tamaño máximo del archivo (en MB).
 - **Máxima profundidad de archivo (niveles).** Marque la casilla de verificación correspondiente y elija la profundidad de archivo máxima desde el menú. Para el mejor rendimiento elija el valor más bajo; para la máxima protección seleccione el más alto.



Nota

Los archivos comprimidos y archivos ZIP por debajo de 256 KB se analizan automáticamente incluso aunque esté desactivada la opción **Analizar en el interior de los archivos**.

- **Analizar archivos de correo.** Seleccione esta opción si quiere comprobar los archivos de correo en busca de malware.
- **Varios.** Seleccione la casilla de verificación correspondiente para activar las opciones de análisis deseadas.
 - **Analizar memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.
 - **Analizar cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en las máquinas virtuales.
 - **Analizar en busca de Rootkits.** Seleccione esta opción para analizar en busca de [rootkits](#) y objetos ocultos que utilicen este tipo de software.
 - **Analizar sólo nuevos&modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.
 - **Ignorar keyloggers comerciales.** Seleccione esta opción si se ha instalado software comercial keylogger en las MVs objetivo. Los keyloggers comerciales son programas legítimos de monitorización de equipos cuya función básica es grabar todo lo que se escribe en el teclado.
- **Acciones del Análisis.** Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:
 - **Archivos infectados.** Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender.Silent Agent puede eliminar normalmente el código malware de un archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

Si se detecta un archivo infectado, Silent Agent intentará desinfectarlo automáticamente.Si falla la desinfección, el archivo se mueve a la cuarentena con el fin de contener la infección.



Importante

Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico.Dado que B-HAVE es una tecnología de análisis heurístico, Silent Agent no puede asegurar que el archivo esté realmente infectado con malware.Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

Las tareas de análisis se configuran de forma predeterminada para ignorar los archivos sospechosos.Quizá desee cambiar la acción predeterminada para mover archivos sospechosos a la cuarentena.Los archivos en cuarentena se envían periódicamente

para su análisis a los laboratorios de Bitdefender. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

- **Rootkits.** Los rootkits representan un software especializado utilizado para ocultar archivos del sistema operativo. Aunque no son dañinos por su naturaleza, los rootkits se usan normalmente para ocultar malware o para encubrir la presencia de un intruso en el sistema.

Los rootkits detectados y archivos ocultos se ignoran de forma predeterminada.

Aunque no se recomienda, puede cambiar las acciones predeterminadas. Puede indicar la segunda acción a realizar en caso que la primera falle, y diferentes acciones para cada categoría. Seleccione, en los menús correspondientes, la primera y segunda acción a realizar para cada tipo de archivo detectado. Dispone de las siguientes opciones:

Desinfectar

Elimina el código de malware de los archivos infectados. Se recomienda siempre mantener esta como la primera acción a aplicar en los archivos infectados.

Mover a Cuarentena

Mueva los archivos detectados desde su ubicación actual a la carpeta de cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Puede administrar los archivos de cuarentena desde la página [Cuarentena](#) de la consola.

Eliminar

Elimina los archivos detectados del disco, sin mostrar advertencia alguna. Se aconseja que evite utilizar esta acción.

Ninguna acción

No se aplicará ninguna acción a los archivos detectados. Estos archivos solamente aparecerán en el registro de análisis.

Pestaña exclusiones

En esta sección puede configurar las reglas de exclusión del análisis. Las exclusiones se pueden aplicar al análisis on-access, bajo demanda o a ambos. Existen cuatro tipos de exclusiones basadas en el objeto de la exclusión:

- **Exclusiones de archivo:** el archivo especificado solamente se excluye del análisis.
- **Exclusiones de carpeta:** todos los archivos dentro de una carpeta específica y todas sus subcarpetas se excluyen del análisis.
- **Exclusiones de extensiones:** todo los archivos que tengan la extensión especificada se excluirán del análisis.
- **Exclusiones de procesos:** cualquier objeto al que acceda el proceso excluido será también excluido del análisis.



Importante

Las exclusiones de análisis son para utilizarlas en circunstancias especiales o seguir las recomendaciones de Microsoft o de Bitdefender. Para una lista actualizada de exclusiones recomendadas por Microsoft, consulte este [artículo](#). Si dispone de un archivo de prueba de EICAR que use para probar la protección antimalware periódicamente, debería excluirlo del análisis on-access.

Utilice el conmutador para activar o desactivar las exclusiones.

Para configurar una regla de exclusión:

1. Seleccione el tipo de exclusión desde el menú.
2. Dependiendo del tipo de exclusión, especifique el objeto a excluir de la forma siguiente:
 - **Exclusiones de extensiones.** Introduzca la extensión de archivo que desea excluir. Antes de excluir las extensiones, infórmese para ver cuáles son objetivos normales del malware y cuáles no.
 - **Exclusiones de archivos, carpeta y proceso.** Debe especificar la ruta al objeto excluido en las máquinas virtuales objetivo.
 - a. Elija desde el menú, bien una ubicación predefinida o bien la opción **Rutas específicas**.
 - b. Si ha escogido una ubicación predefinida, complete la ruta según sea necesario. Por ejemplo, para excluir la carpeta `Archivos de programa` completa, es suficiente con seleccionar la ubicación predefinida correspondiente desde el menú. Para excluir una carpeta específica de `Archivos de programa`, debe completar la ruta añadiendo una barra invertida (`\`) y el nombre de la carpeta. Para procesar exclusiones debe añadir también el nombre del archivo ejecutable de la aplicación.



Nota

Para más información, diríjase a [“Usar variables de sistema”](#) (p. 87).

- c. Si ha elegido **Rutas específicas**, escriba la ruta completa del objeto a excluir. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todas las MVs objetivo.
3. Seleccione los tipos de análisis a los que se aplicará la regla. Algunas exclusiones pueden ser relevantes sólo para el análisis on-access y algunas sólo para el análisis bajo demanda, mientras que otras pueden ser recomendables para ambos.
 4. Haga clic en el botón **+** **Añadir**. La nueva regla se añadirá a la lista.

Para eliminar una regla de la lista, haga clic en el botón correspondiente **X** **Eliminar**.

Pestaña Cuarentena

En este apartado puede modificar la configuración de la cuarentena. Puede configurar Silent Agent para que realice automáticamente las siguientes acciones:

- **Eliminar archivos con antigüedad superior a {30} días.** Por defecto, los archivos con antigüedad superior a 30 días se eliminan automáticamente. Si desea cambiar este intervalo, seleccione una opción diferente desde el menú.
- **Enviar los archivos en cuarentena a Bitdefender para su posterior análisis.** Mantenga esta opción seleccionada para enviar automáticamente los archivos en cuarentena a los Laboratorios de Bitdefender. Los investigadores de malware de Bitdefender analizarán los archivos de muestra. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

Por omisión, los archivos de cuarentena se envían automáticamente al laboratorio de Bitdefender cada hora. Si desea cambiar este intervalo, seleccione una opción diferente desde el menú.

- **Volver a analizar la cuarentena tras actualizar las firmas malware.** Mantenga seleccionada esta opción para analizar automáticamente los archivos en cuarentena después de cada actualización de firmas malware. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

7.3. Monitorizar la Ejecución de Política

Para comprobar si una política se ha aplicado en las máquinas virtuales objetivo:

1. Diríjase a la página **Políticas > Ver políticas**.
2. Compruebe el estado en la columna **Conforme**. Puede ver cuántas de las máquinas virtuales objetivo son compatibles.
3. Haga clic en el enlace para abrir una ventana con más información. Todas las máquinas virtuales a las que se ha asignado la política se muestran en una tabla. Puede comprobar el estado de cumplimiento para cada máquina objetivo.



Nota

Si hay muchas entradas, puede utilizar los cuadros de búsqueda o los menús bajo los encabezados de columna para filtrar la información mostrada. También puede hacer clic en los encabezados de la columna para ordenar la información por una columna específica. Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla.

7.4. Comprobar y Cambiar la Asignación de Políticas

Pueden asignarse políticas tanto a máquinas virtuales individuales como a grupos de máquinas virtuales.

Para comprobar y cambiar las asignaciones de la política:

1. Diríjase a la página **Políticas > Ver políticas**.
2. Haga clic en el nombre de la política. Esto abrirá la página de políticas.
3. Las máquinas virtuales o grupos asignados se enumeran en el campo **Objetivos específicos**. Haga clic en el enlace para ver más detalles y cambiar las asignaciones actuales. Por favor, tenga en cuenta que no puede cambiar el tipo de objetivo (máquinas virtuales o grupos).
4. Para cambiar las asignaciones actuales, siga estos pasos:
 - a. Dependiendo del tipo de objetivo, proceda como sigue:
 - Si la política se ha asignado en principio a grupos, seleccione los nuevos grupos en los que desea que se aplique la política.
 - Si la política se ha asignado originalmente a máquinas virtuales, debe seleccionar las nuevas máquinas virtuales a las que desea aplicar la política. Antes de nada, desmarque la casilla de verificación **Mostrar sólo los equipos seleccionados** en la esquina superior izquierda de la ventana. Seguidamente, marque las casillas de verificación correspondientes a las máquinas virtuales deseadas.



Nota

Si hay muchas entradas, puede utilizar los cuadros de búsqueda o los menús bajo los encabezados de columna para filtrar la información mostrada. También puede hacer clic en los encabezados de la columna para ordenar la información por una columna específica. Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla.

- b. Haga clic en **Cambiar** para guardar el nuevo objetivo.
- c. Haga clic en **Guardar** para aplicar los cambios de la política.

7.5. Renombrando Políticas

Las políticas deberían tener nombres descriptivos de forma que usted u otro administrador pueda identificarlas rápidamente.

Para renombrar una política:

1. Diríjase a la página **Políticas > Ver políticas**.
2. Haga clic en el nombre de la política. Esto abrirá la página de políticas.

3. Escriba un nombre nuevo para la política.
4. Haga clic en **Guardar** para aplicar los cambios de la política.

7.6. Eliminando Políticas

Si ya no necesita una política, elimínela. Al eliminar una política, a las máquinas virtuales a las que afectaba se les asignará la política del grupo padre. Si no se aplica otra política, finalmente se aplicará la política predeterminada.

Para eliminar una política:

1. Diríjase a la página **Políticas > Ver políticas**.
2. Seleccione la casilla correspondiente.
3. Haga clic en el botón **Eliminar** en la esquina superior derecha de la página. Tendrá que confirmar esta acción haciendo clic en **Sí**.

8. Ejecutar y administrar tareas

Puede ejecutar de forma remota diversas tareas administrativas en las MVs desde la página **Ver equipos**. Esto es lo que puede hacer:

- Instalar la protección en MVs detectadas.
- Analice las MVs administradas en busca de malware.
- Eliminar la protección de las MVs.



Nota

La instalación remota y las tareas de eliminación sólo están disponibles para MVs de Windows.

Las tareas pueden monitorizarse y administrarse desde la página **Equipos > Ver tareas**.

8.1. Instalación de protección en MVs no administradas

Una vez que ha instalado el agente Security for Virtualized Environments en una máquina virtual, éste detectará automáticamente equipos en la red local. La protección de Security for Virtualized Environments puede instalarse en esos equipos de forma remota desde la consola. La instalación remota se ejecuta en segundo plano, sin que el usuario lo perciba.



Aviso

Antes de realizar la instalación, asegúrese de desinstalar el software antimalware ya existente en las MVs. Instalar Security for Virtualized Environments sobre software de seguridad ya existente puede afectar al funcionamiento y ocasionar graves problemas en el sistema.

Para instalar remotamente la protección de Security for Virtualized Environments en una o varias MVs detectadas:

1. Vaya a la página **Equipos > Ver equipos**.
2. Haga clic en el menú **Mostrar** localizado encima de la tabla (a la izquierda) y elija **Equipos no administrados**.
3. Si ha organizado las MVs en grupos, seleccione el grupo deseado en el panel izquierdo. Para ver todas sus MVs, haga clic con el botón derecho en el grupo raíz y elija **Ver todos los equipos**.
4. Marque las casillas de verificación correspondientes a las MVs en las que quiere instalar la protección.

5. Haga clic en **Tareas** y elija **Instalar** desde el menú. Se mostrará la ventana Opciones de instalación.
6. Proporcione las credenciales de administrador necesarias para la autenticación remota en las máquinas virtuales seleccionadas.

Introduzca el nombre de usuario y contraseña de una cuenta de administrador para cada uno de los equipos seleccionados. 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, `dominio\usuario` o `usuario@dominio.com`).

7. Haga clic en **Instalar Silent Agent**. Aparecerá una ventana de configuración.
8. Puede ver y administrar la tarea en la página **Equipos > Ver tareas**.

8.2. Análisis en MVs administradas

Hay dos maneras de analizar las MVs protegidas por Security for Virtualized Environments:

- 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 una o varias MVs:

1. Vaya a la página **Equipos > Ver equipos**.
2. Haga clic en el menú **Mostrar** localizado encima de la tabla (a la izquierda) y elija **Equipos administrados**.
3. Si ha organizado las MVs en grupos, seleccione el grupo deseado en el panel izquierdo. Para ver todas sus MVs, haga clic con el botón derecho en el grupo raíz y elija **Ver todos los equipos**.
4. Marque las casillas de verificación correspondientes a las MVs que quiere analizar.
5. Haga clic en **Tareas** y elija **Analizar** desde el menú.
6. Haga clic en **Solicitar análisis**. Aparecerá una ventana de configuración.
7. Puede ver y administrar la tarea en la página **Equipos > Ver tareas**.

8.3. Desinstalar la protección de las MVs

Para desinstalar remotamente la protección de Security for Virtualized Environments en una o varias MVs:

1. Vaya a la página **Equipos > Ver equipos**.
2. Haga clic en el menú **Mostrar** localizado encima de la tabla (a la izquierda) y elija **Equipos administrados**.

3. Si ha organizado las MVs en grupos, seleccione el grupo deseado en el panel izquierdo. Para ver todas sus MVs, haga clic con el botón derecho en el grupo raíz y elija **Ver todos los equipos**.
4. Marque las casillas de verificación correspondientes a las MVs en las que desea desinstalar la protección.
5. Haga clic en **Tareas** y elija **Desinstalar protección** desde el menú.
6. Haga clic en **Desinstalar**. Aparecerá una ventana de configuración.
7. Puede ver y administrar la tarea en la página **Equipos > Ver tareas**.

8.4. Ver y administrar tareas

Las tareas que ha creado pueden verse y administrarse en la página **Equipos > Ver tareas**. Puede ver las tareas existentes y los detalles sobre ellas:

- Nombre de la tarea.
- Progreso de ejecución en las MVs objetivo.
- Cuando se crearon las tareas.

8.4.1. Comprobar estado de ejecución y resultados

Las tareas empezarán a ejecutarse inmediatamente en las MVs on-line, pero necesitarán de un tiempo para completarse (más o menos, dependiendo de la tarea).

Para comprobar si una tarea se ha ejecutado en las MVs objetivo:

1. Diríjase a la página **Equipos > Ver tareas**.
2. Encuentre la tarea en la lista y verifique el campo **Progreso**. Puede ver en cuántas de las MVs objetivo se ha ejecutado la tarea.
3. Para acceder al informe de la tarea, que proporciona información sobre la ejecución de la tarea, haga clic en el nombre de la tarea.

El informe de tareas consiste en una página de Resumen y una página de Detalles.

8.4.2. Eliminar Tareas

Una vez que se ha ejecutado la tarea y ya no necesita el informe de tarea, es mejor eliminarlo.

Para eliminar una o más tareas:

1. Diríjase a la página **Equipos > Ver tareas**.
2. Marque las casillas de verificación correspondientes a las tareas que desea eliminar.
3. Haga clic en el botón **Eliminar** ubicado encima de la tabla. Aparecerá una ventana de configuración.

9. Usar informes

Security Console le permite crear y visualizar informes centralizados sobre el estado de seguridad de las máquinas virtuales. Los informes pueden usarse para múltiples propósitos, tales como:

- Monitorizar y asegurar el cumplimiento de las políticas de seguridad de la empresa.
- Comprobando y evaluando el estado de seguridad de la red virtual.
- Identificar los problemas de seguridad, amenazas y vulnerabilidades.
- Monitorizar los incidentes de seguridad y la actividad malware.
- Proporcionando una administración superior con datos de fácil interpretación sobre la seguridad de la MV.

Hay disponibles varios tipos de informes diferentes para que pueda conseguir fácilmente la información que necesita. La información se presenta a través de gráficos circulares de fácil comprensión, tablas y diagramas, permitiéndole comprobar rápidamente el estado de seguridad de la red virtual e identificar las incidencias de seguridad.

Los informes pueden consolidar información de toda la red virtual o únicamente de grupos MV específicos. De este modo, en un sólo informe puede encontrar la siguiente información:

- Información estadística referida a todas o grupos de máquinas virtuales protegidas.
- Información detallada para cada máquina virtual protegida.
- La lista de MVs que cumplen un criterio específico (por ejemplo, aquellas que tienen desactivada la protección antimalware).

Todos los informes generados están disponibles en Security Console durante un periodo predeterminado de 90 días, pero puede guardarlos en su equipo o enviarlos por correo. Los formatos disponibles incluyen Portable Document Format (PDF) y Comma-Separated Values (CSV).

9.1. Tipos de informes disponibles

Esta es la lista de tipos de informes disponibles:

Actualización

Muestra el estado de actualización de la protección de Security for Virtualized Environments instalada en los equipos seleccionados. Usando los filtros disponibles, puede descubrir fácilmente qué clientes se han actualizado o no, en un periodo de tiempo específico.

Estado del equipo

Le proporciona diversas informaciones de estado relativas a los equipos seleccionados en los que se ha instalado la protección Security for Virtualized Environments.

- Estado de actualización de protección
- Estado de la licencia
- Estado de actividad de la red (online/offline)
- Estado de protección antimalware

Puede aplicar filtros según aspectos de la seguridad y estado para encontrar la información que está buscando.

Actividad de malware

Le ofrece detalles generales y por equipo sobre las amenazas de malware detectadas en un periodo de tiempo específico en los equipos seleccionados. Puede ver:

- Número de detecciones (archivos que se han encontrado infectados con malware)
- Número de infecciones resueltas (archivos que han sido desinfectados o aislados con éxito en la carpeta de cuarentena)
- Número de infecciones bloqueadas (archivos que no pudieron desinfectarse pero se ha rechazado el acceso ellos; por ejemplo, un archivo infectado almacenado en algún formato comprimido propietario)

Estado del módulo de protección

Le informa del estado de la protección antimalware en los equipos seleccionados. El estado de protección puede habilitarse o deshabilitarse. Los detalles del informe también proporcionan información sobre el estado de actualización.

Puede aplicar filtros según estado para encontrar la información que está buscando.

Equipos más infectados

Muestra los equipos más infectados durante un periodo de tiempo específico entre los equipos seleccionados.

Malware más detectado

Le muestra las amenazas malware más detectadas en un periodo de tiempo específico en los equipos seleccionados.

Estado de la Red

Le proporciona información detallada sobre el estado general de seguridad de la red. Los equipos se agrupan basándose en estos criterios:

- Los equipos no administrados no tienen instalada la protección Security for Virtualized Environments y su estado de seguridad no puede evaluarse. Los agentes de Security for Virtualized Environments instalados en máquinas virtuales protegidas detectan automáticamente los equipos no administrados. Pueden representar no solo máquinas virtuales, sino también equipos físicos (si están conectados a la red virtual).
- Los equipos offline normalmente tienen la protección Security for Virtualized Environments instalada, pero no hay actividad reciente de Silent Agent. El estado

de seguridad de los equipos offline no puede evaluarse con precisión porque la información sobre su estado no es reciente. Para más información, diríjase a [“Sobre equipos offline”](#) (p. 36).

- Los equipos protegidos tienen instalada la protección Security for Virtualized Environments y no se han detectado amenazas de seguridad.
- Los equipos vulnerables tienen instalada la protección de Security for Virtualized Environments, pero determinadas condiciones impiden la adecuada protección del sistema. Los detalles del informe le muestran qué aspectos de la seguridad necesitan abordarse.

Estado malware de los equipos

Le ayuda a encontrar cuántos y cuáles de los equipos seleccionados han sido afectados por malware en un periodo de tiempo específico y cómo se han tratado las amenazas. Los equipos se agrupan basándose en estos criterios:

- Equipos sin detecciones (no se ha detectado ninguna amenaza malware en el periodo de tiempo especificado)
- Equipos con malware solucionado (todos los archivos detectados han sido desinfectados correctamente o aislados en la carpeta de cuarentena local)
- Equipos con malware bloqueado (se ha rechazado el acceso a algunos de los archivos detectados)

Ejecutivo

Le permite exportar las gráficas desde los portlets del panel de control a un archivo PDF.

9.2. Creando Informes

Para crear un informe:

1. Vaya a la página **Informes > Nuevo informe**.



Nota

Si se encuentra en la página **Ver informes** o **Informes programados**, simplemente haga clic en el botón **Nuevo** ubicado encima de la tabla.

2. Seleccione el tipo de informe deseado desde el menú. Para más información, diríjase a [“Tipos de informes disponibles”](#) (p. 66).
3. Escriba un nombre descriptivo para el informe. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe.
4. Configure el objetivo del informe. Seleccione una de las opciones disponibles y haga clic en el enlace correspondiente para elegir el grupo o máquinas virtuales individuales que se incluirán en el informe.

5. Configure la recurrencia del informe (programación). Puede elegir crear el informe inmediatamente, diariamente, semanalmente (en un día específico de la semana) o mensualmente (en un día específico del mes).
6. Configure las opciones del informe.
 - a. Para la mayor parte de los tipos de informe, cuando crea un informe inmediato, debe especificar el periodo de generación de informes. El informe incluirá únicamente información sobre periodo de tiempo seleccionado.
 - b. Varios tipos de informes ofrecen opciones de filtrado para ayudarle a encontrar fácilmente la información en la que está interesado. Utilice las opciones de filtrado para obtener únicamente la información deseada. Por ejemplo, para un informe de **Estado de actualización** puede elegir ver sólo la lista de MVs protegidas que se han actualizado (o, por el contrario, las que no se han actualizado) en el período de tiempo seleccionado.



Nota

Cuando visualiza el informe en la consola, toda la información está disponible, independientemente de las opciones seleccionadas. Si de todas formas descarga o envía por correo el informe, se incluirá en el archivo PDF únicamente el resumen del informe y la información seleccionada. Los detalles completos del informe sólo estarán disponibles en formato CSV.

- c. Para recibir el informe por correo, seleccione la opción correspondiente.
7. Haga clic en **Generar** para crear el informe.
 - Si ha elegido crear un informe inmediato, se mostrará en la página [Ver informes](#). El tiempo requerido para crear los informes puede variar dependiendo del número de MVs administradas. Por favor, espere a que finalice la creación del informe. Una vez que se ha creado el informe, puede verlo haciendo clic sobre su nombre.
 - Si ha elegido crear un informe programado, se mostrará en la página [Informes programados](#).

9.3. Ver y administrar informes generados

Para ver y administrar los informes generados, vaya a la página **Informes > Ver informes**. Esta página se muestra automáticamente tras crear un informe inmediato.



Nota

Los informes programados pueden administrarse desde la página [Informes > Informes programados](#).

Puede ver los informes generados e información útil acerca de ellos:

- Nombre del informe y tipo.
- Cuando se generó el informe.

Para ordenar los informes por una columna específica, haga clic simplemente en el encabezado de esa columna. Haga clic nuevamente sobre el encabezado para cambiar el sentido de ordenación.

Cada informe se marca con uno de los siguientes iconos para indicarle si el informe está programado o no:

-  Indica un informe para una única vez.
-  Indica un informe programado.

Para asegurarse de que se está mostrando la última información, haga clic en el botón  **Refrescar** en la esquina inferior izquierda de la tabla.

9.3.1. Visualizando los Informes

Para ver un informe:

1. Vaya a la página **Informes > Ver informes**.
2. Haga clic en el nombre del informe que quiere ver. Para encontrar fácilmente el informe que está buscando, puede ordenar los informes por nombre, tipo u hora de creación.

Todos los informes consisten en una página Resumen y una página de Detalles.

- La página Resumen le ofrece datos estadísticos (gráficos circulares y diagramas) para todas las MVs o grupos objetivo. En la parte inferior de la página puede ver información general sobre el informe, como el período del informe (si es aplicable), objetivo del informe, etc.
- La página de Detalles le proporciona información detallada de cada MV administrada. En algunos informes, es posible que necesite hacer clic en el área del gráfico de tarta de la página Resumen para ver los detalles.

Use las pestañas de la esquina superior izquierda del informe para ver la página deseada.

9.3.2. Buscar detalles del informe

Los detalles del informe se muestran en una tabla que consiste en varias columnas que ofrecen variada información. La tabla puede distribuirse en varias páginas (por omisión se muestran únicamente 10 entradas por página). Para navegar por las páginas de detalle, use los botones en la parte inferior de la tabla.

Para encontrar fácilmente lo que está buscando, utilice los cuadros de búsqueda o las opciones de filtrado bajo los encabezados de columna.

Para ordenar los detalles del informe por una columna específica, haga clic simplemente en el encabezado de esa columna. Haga clic nuevamente sobre el encabezado para cambiar el sentido de ordenación.

9.3.3. Guardar Informes

Los informes generados están disponibles, de forma predeterminada, en Security Console durante 90 días. Pasado este periodo, se eliminan automáticamente.

Si necesita que los informes estén disponibles durante periodos de tiempo más largos, puede guardarlos en su equipo. El resumen del informe y la información del informe seleccionada estarán disponibles en formato PDF, mientras que los detalles del informe completo estarán disponibles en formato CSV.

Para guardar el informe que está visualizando en su equipo:

1. Haga clic en el botón **Exportar** en la esquina superior derecha de la página de informe. Aparecerá una ventana de descarga.
2. Descargue el archivo `.zip` en su equipo. Dependiendo de la configuración de su navegador, el archivo puede ser descargado automáticamente a una ubicación de descarga predeterminada.

9.3.4. Imprimiendo los Informes

Para imprimir un informe, primero debe guardarlo en su equipo.

9.3.5. Enviar informes por correo

Para enviar por correo el informe que está viendo:

1. Haga clic en el botón **Email** en la esquina superior derecha de la página de informe. Aparecerá una ventana.
2. Si lo desea puede cambiar el nombre del informe.
3. Introduzca las direcciones de correo de las personas a las que desea enviar el informe, separándolas por punto y coma (;).
4. Haga clic en **Enviar email**.

9.3.6. Eliminación automática de informes

Los informes generados están disponibles, de forma predeterminada, en Security Console durante 90 días. Pasado este periodo, se eliminan automáticamente.

Para modificar el periodo de eliminación automático para los informes generados:

1. Vaya a la página **Informes > Ver informes**.
2. Haga clic en el enlace en la parte inferior de la tabla.
3. Seleccione el nuevo período desde el menú.
4. Haga clic en **Aceptar**.

9.3.7. Eliminar Informes

Para eliminar un informe:

1. Vaya a la página **Informes > Ver informes**.
2. Seleccione el informe.
3. Haga clic en el botón **Eliminar** ubicado encima de la tabla.

9.4. Administrar informes programados

Cuando se crea un informe, puede elegir configurar una planificación basada en que el informe se generará automáticamente (a intervalos de tiempo regulares). Tales informes se denominan informes programados.

Los informes generados estarán disponibles en la página **Informes > Ver informes** durante un periodo predeterminado de 90 días. También se le enviarán por correo si ha seleccionado esta opción.

Para administrar informes programados, vaya a la página **Informes > Informes programados**. Puede ver todos los informes programados y la información útil acerca de ellos:

- Nombre del informe y tipo.
- Programación basada en la cual el informe se genera automáticamente.
- Cuando se generó el informe por última vez.

9.4.1. Ver último informe generado

Desde la página **Informes > Informes programados**, puede ver fácilmente el informe generado más recientemente haciendo clic en el enlace de la columna **Último informe generado**.

9.4.2. Renombrar informes programados

Los informes generados por un informe programado basan en él su nombre. Renombrar un informe programado no afecta a los informes generados anteriormente.

Para renombrar un informe programado:

1. Vaya a la página **Informes > Informes programados**.
2. Haga clic en el nombre del informe.
3. Cambie el nombre del informe en el campo correspondiente. Elija un nombre descriptivo para el informe para poder identificar fácilmente de qué se trata. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe.

4. Haga clic en **Enviar** para guardar los cambios.

9.4.3. Editar informes programados

Para cambiar la configuración de un informe programado:

1. Vaya a la página **Informes > Informes programados**.
2. Haga clic en el nombre del informe.
3. Cambiar los ajustes del informe según sea necesario. Puede cambiar lo siguiente:
 - **Nombre del informe.** Elija un nombre descriptivo para el informe para poder identificar fácilmente de qué se trata. Al elegir un nombre, tenga en cuenta el tipo de informe y objetivo, y posiblemente las opciones del informe. Los informes generados por un informe programado basan en él su nombre.
 - **Objetivo del informe.** La opción seleccionada indica el tipo de objetivo del informe actual (bien sean grupos o máquinas virtuales individuales). Haga clic en el enlace correspondiente para ver el objetivo del informe actual. Para cambiarlo, haga clic en cualquiera de los dos enlaces y seleccione los grupos o MVs que desee incluir en el informe.
 - **Recurrencia de informe (calendario).** Puede configurar el informe para que se genere de forma automática diariamente, semanalmente (en un día específico de la semana) o mensualmente (en un día específico del mes). Dependiendo del programa seleccionado, el informe incluirá sólo datos del último día, semana o mes, respectivamente.
 - **Opciones de informe.** Puede elegir recibir el informe por email. La mayoría de informes poseen opciones de filtrado para ayudarle a encontrar fácilmente la información en la que está interesado. Cuando visualiza el informe en la consola, toda la información está disponible, independientemente de las opciones seleccionadas. Si de todas formas descarga o envía por correo el informe, se incluirá en el archivo PDF únicamente el resumen del informe y la información seleccionada. Los detalles completos del informe sólo estarán disponibles en formato CSV.
4. Haga clic en **Enviar** para guardar los cambios.

9.4.4. Eliminar informes programados

Cuando ya no se necesita un informe programado, lo mejor es eliminarlo. Al eliminar un informe programado no se borrarán los informes que ha generado automáticamente hasta ese momento.

Para eliminar un informe programado:

1. Vaya a la página **Informes > Informes programados**.
2. Seleccione el informe.

3. Haga clic en el botón **Eliminar** ubicado encima de la tabla.

10. Cuarentena

Security for Virtualized Environments puede aislar los archivos infectados con malware y los archivos sospechosos en un área segura denominada cuarentena. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Los archivos en cuarentena se almacenan localmente en las máquinas virtuales. Para hacerle la vida más fácil, el contenido de la cuarentena es administrado automáticamente.

Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de malware de Bitdefender. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

Además, los archivos en cuarentena se analizan tras cada actualización de firmas malware. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

Security Console proporciona información detallada de todos los elementos en cuarentena, para que así pueda monitorizar fácilmente amenazas sin resolver y brotes de malware. Para comprobar y gestionar los archivos en cuarentena, diríjase a la página **Cuarentena**.

La información sobre los archivos en cuarentena se muestra en una tabla. Se le proporciona la siguiente información:

- Nombre dado a la amenaza malware por los investigadores de seguridad de Bitdefender.
- Ruta al archivo sospechoso o infectado en la máquina virtual en la que fue detectado.
- Máquina virtual en la que se detectó la amenaza.
- Hora en la que el archivo fue puesto en cuarentena.
- Acción pendiente solicitada por el administrador para llevarse a cabo sobre el archivo de la cuarentena.

Para asegurarse de que se está mostrando la última información, haga clic en el botón  **Refrescar** en la esquina inferior izquierda de la tabla. Esto puede ser necesario cuando dedique más tiempo a la página.

10.1. Navegación y búsqueda

Dependiendo del número de MVs administradas y de la naturaleza de las infecciones, el número de archivos en cuarentena puede ser a veces muy grande. La tabla puede distribuirse en varias páginas (por omisión se muestran únicamente 10 entradas por página).

Para moverse por las páginas, use los botones de navegación en la parte inferior de la tabla. Para cambiar el número de entradas mostradas en una página, seleccione una opción desde el menú junto a los botones de navegación.

Si hay muchas entradas, puede utilizar los cuadros de búsqueda bajo los encabezados de columna para filtrar la información mostrada. Por ejemplo, puede buscar una amenaza específica detectada en la red o una máquina virtual específica. También puede hacer clic en los encabezados de la columna para ordenar la información por una columna específica.

10.2. Restaurar archivos de la cuarentena

En ocasiones particulares, puede que necesite restaurar archivos en cuarentena, bien sea a sus ubicaciones originales o a una ubicación alternativa. Una situación de ese tipo es cuando quiere recuperar archivos importantes almacenados en un fichero comprimido infectado que ha sido movido a la cuarentena.

Para restaurar uno o más archivos de la cuarentena:

1. Vaya a la página **Cuarentena**.
2. Compruebe la lista de archivos en la cuarentena y marque las casillas de verificación correspondientes de aquellos que desee restaurar.
3. Haga clic en el botón **Restaurar** en la esquina superior derecha de la página.
4. Elija la ubicación a donde quiere que se restauren los archivos seleccionados (bien sea la ubicación original o una personalizada de la máquina virtual objetivo).

Si elige restaurar en una ubicación personalizada, debe introducir la ruta en el campo correspondiente. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todas las MVs objetivo. Para más información, diríjase a [“Usar variables de sistema”](#) (p. 87).

5. Haga clic en **Restaurar** para solicitar la acción de restauración del archivo. Puede observar la acción pendiente en la columna **Acción**.
6. La acción solicitada se envía a las MVs objetivo inmediatamente o tan pronto como vuelvan a estar online. Una vez restaurado un archivo, la entrada correspondiente desaparece de la tabla de cuarentena.

10.3. Eliminación automática de archivos de la cuarentena

Por defecto, los archivos con antigüedad superior a 30 días se eliminan automáticamente. Esta configuración puede modificarse editando la política asignada a las máquinas virtuales.

Para modificar el intervalo de eliminación automático para los archivos en cuarentena:

1. Diríjase a la página **Políticas > Ver políticas**.

- Encuentre la política asignada a las MVs en las que quiere cambiar la configuración y haga clic en su nombre.
- Vaya a la sección **Antimalware > Cuarentena**.
- Seleccione el periodo de eliminación automática deseado desde el menú.
- Haga clic en **Guardar** para guardar los cambios.

10.4. Eliminar archivos de la cuarentena

Si quiere eliminar archivos de la cuarentena manualmente, debería primero asegurar que los archivos que ha elegido para borrar no son necesarios. Use estos consejos cuando elimine archivos de la cuarentena:

- Un archivo puede ser en sí mismo el propio malware. Si su investigación le lleva a una situación de este tipo, puede buscar esa amenaza específica en la cuarentena y eliminarla.
- Puede eliminar con seguridad:
 - Elementos del archivo no importantes.
 - Archivos de instalación infectados.

Para eliminar uno o más archivos de la cuarentena:

- Vaya a la página **Cuarentena**.
- Compruebe la lista de archivos en la cuarentena y marque las casillas de verificación correspondientes de aquellos que desee eliminar.
- Haga clic en el botón **Eliminar** en la esquina superior derecha de la página. Puede observar la acción pendiente en la columna **Acción**.
- La acción solicitada se envía a las MVs objetivo inmediatamente o tan pronto como vuelvan a estar online. Una vez que se ha eliminado un archivo, la entrada correspondiente desaparecerá de la tabla Cuarentena.

11. Cuentas de usuario

Security for Virtualized Environments puede configurarse y administrarse desde **cuenta de empresa** en Security Console creada después de la instalación. Esta es la cuenta de administrador de su empresa.

Para permitir a otros empleados de la empresa acceder a Security Console, puede crear cuentas adicionales de usuario desde su cuenta de empresa. Las cuentas de usuario pueden utilizarse para limitar el acceso a las características de Security Console o a grupos específicos de las máquinas virtuales.

Puede crear dos tipos de cuentas:

Administrador

Las cuentas de administrador ofrecen acceso completo a todas las áreas de la consola, permitiendo a los usuarios el control total sobre Security for Virtualized Environments. Puede permitir el acceso a todo el entorno virtualizado o solo a un grupo MV.

Informador

Las cuentas de informador ofrecen acceso limitado a las funciones de la consola. Los usuarios solo pueden ver el panel de control, informes y las secciones de registros de actividad, sin poder ver o cambiar la MV o su configuración de seguridad. Puede permitir el acceso a todo el entorno virtualizado o solo a un grupo MV.

Para crear y administrar las cuentas de usuario, dirijase a la página **Cuentas > Usuarios**.

Las cuentas existentes se muestran en la tabla. Para cada cuenta, puede ver:

- Nombre del propietario de la cuenta.
- Dirección de correo de la cuenta (usada para iniciar sesión en Security Console y también como dirección de contacto). 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.
- Grupo MV del que se encarga el usuario.
- Función de usuario (administrador / informador).

11.1. Crear cuentas de usuario

Cree cuentas de usuario para delegar la responsabilidad de generación de informes o tareas administrativas en otras personas.

Para crear una cuenta de usuario:

1. Vaya a la página **Cuentas > Usuarios**.
2. Haga clic en el botón **Nuevo** en la esquina superior derecha de la página.
3. Rellene los detalles de la cuenta en **Detalles de cuenta**.
 - **Nombre y apellidos**. Escriba el nombre completo del propietario de la cuenta.
 - **Correo**. Escriba la dirección de correo del usuario (que utilizará el usuario para iniciar sesión en Security Console). La información de inicio de sesión se enviará a esta dirección inmediatamente después de crear la cuenta.
 - **Función del usuario**. Seleccione la función del usuario:
 - **Administrador** - tiene derechos administrativos sobre las máquinas virtuales asignadas.
 - **Informador** - posee acceso limitado a la consola, y sólo puede monitorizar y crear informes sobre la seguridad de las máquinas virtuales asignadas.
 - **Grupo**. Elija el grupo MV del que se hará cargo el usuario. El resto de la red virtual será invisible para el usuario. Por omisión, el usuario puede ver toda la red virtual.
4. Puede configurar las opciones de cuenta en **Configuración**.
 - **Zona horaria**. Elija desde 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 desde el menú el idioma de visualización de la consola.
5. Haga clic en **Enviar**. La nueva cuenta se mostrará en la lista de cuentas de usuario.

11.2. Editar cuentas

Edite las cuentas para mantener al día los detalles de la cuenta o cambiar la configuración de la misma.

Para editar una cuenta de usuario:

1. Vaya a la página **Cuentas > Usuarios**.
2. Haga clic en el nombre de usuario.
3. Cambie la configuración y detalles de la cuenta según sea necesario.
4. Haga clic en **Enviar** para guardar los cambios.

11.3. Eliminar cuentas

Elimine las cuentas cuando ya no sean necesarias. Por ejemplo, si el propietario de la cuenta ya no está en la empresa.

Para eliminar una cuenta:

1. Vaya a la página **Cuentas > Usuarios**.
2. Seleccione la cuenta desde la lista.
3. Haga clic en el botón **Eliminar** en la esquina superior derecha de la página.

11.4. Restablecer las contraseñas de inicio de sesión

Los propietarios de cuentas que olviden su contraseña pueden restablecerla usando el enlace de recuperación de contraseña en la página de inicio de sesión. También puede restablecer una contraseña de inicio de sesión olvidada editando la cuenta correspondiente desde la consola.

Para restablecer la contraseña de inicio de sesión para un usuario:

1. Vaya a la página **Cuentas > Usuarios**.
2. Haga clic en el nombre de usuario.
3. Escriba una nueva contraseña en los campos correspondientes (en **Detalles de cuenta**).
4. Haga clic en **Enviar** para guardar los cambios. Asegúrese de informar al propietario de la cuenta sobre la nueva contraseña.

12. Registro de actividad del usuario

Security Console registra todas las operaciones y acciones ejecutadas por los usuarios. Los eventos registrados incluyen lo siguiente:

- Iniciar y cerrar sesión
- Crear, editar, renombrar, eliminar cuentas de usuario
- Crear, editar, renombrar, eliminar políticas
- Crear, editar, renombrar, eliminar informes
- Eliminar, restaurar archivos de cuarentena
- Eliminar o mover equipos entre grupos
- Crear, mover, renombrar, eliminar grupos

Para examinar los registros de actividad del usuario, vaya a la página **Log**.

Los eventos registrados se muestran en una tabla. Las columnas de la tabla le proporcionan información sobre los eventos listados:

- Nombre del usuario que realizó la acción.
- Tipo de cuenta de usuario.
- Acción que produjo el evento.
- Tipo de objeto de la consola afectado por la acción.
- Objeto específico afectado por la acción.
- Dirección IP desde la que se conecta el usuario.
- Hora en la que sucedió el evento.

Para encontrar fácilmente lo que está buscando, utilice los cuadros de búsqueda o las opciones de filtrado bajo los encabezados de columna. Para ordenar los eventos por una columna específica, haga clic simplemente en el encabezado de esa columna. Haga clic nuevamente sobre el encabezado para cambiar el sentido de ordenación.

Para ver información detallada sobre un evento, selecciónelo y compruebe la sección bajo la tabla.

Para asegurarse de que se está mostrando la última información, haga clic en el botón  **Refrescar** en la esquina inferior izquierda de la tabla.

13. 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. Nuestros representantes de soporte responderán a sus preguntas con diligencia 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.

13.1. Centro de soporte de Bitdefender

El Centro de soporte de Bitdefender, disponible en <http://enterprise.bitdefender.com/support>, es el lugar al que acudir para encontrar toda la asistencia técnica que necesite para su producto 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 conocimiento 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://enterprise.bitdefender.com/support>.

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 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.

Puede consultar y descargar la última versión de la documentación para los productos corporativos de Bitdefender en [Centro de soporte](#) > Documentación.

13.2. Solicitar ayuda

Puede contactar con nosotros para solicitar ayuda a través de nuestro Centro de Soporte en línea:

1. Visite <http://enterprise.bitdefender.com/support/contact-us.html>.
2. Utilice el formulario de contacto para abrir un ticket de soporte por correo electrónico o acceda a otras opciones de contacto disponibles.

13.3. Información de contacto

La comunicación eficiente es la clave para un negocio de éxito. Durante los últimos 10 años, Bitdefender ha establecido una reputación incuestionable de lucha constante para mejorar

la comunicación y así aumentar las expectativas de nuestros clientes y partners. Si usted tuviera cualquier pregunta, no dude en contactar con nosotros.

13.3.1. Direcciones Web

Departamento de ventas: enterprisesales@bitdefender.com
Centro de soporte: <http://enterprise.bitdefender.com/support>
Documentación: documentation@bitdefender.com
Distribuidores locales: <http://www.bitdefender.es/partners>
Programa de Partners: partners@bitdefender.com
Relaciones con la Prensa: prensa@bitdefender.es
Oportunidades de Trabajo: jobs@bitdefender.com
Envío de virus: virus_submission@bitdefender.com
Envío de Spam: spam_submission@bitdefender.com
Notificar abuso: abuse@bitdefender.com
Sitio Web: <http://enterprise.bitdefender.com>

13.3.2. 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 ocurre, seleccione su país de residencia 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. Por favor, escriba su correo en inglés para que podamos ayudarle rápidamente.

13.3.3. 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 otros medios de contacto se listan a continuación.

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

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

Centro de soporte: <http://www.bitdefender.es/businesshelp>

Rumania

BITDEFENDER SRL

West Gate Park, Building H2, 24 Preciziei Street

Bucharest, Sector 6

Fax: +40 21 2641799

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

Comercial: sales@bitdefender.ro

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

Centro de soporte: <http://www.bitdefender.ro/businesshelp>

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

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

Centro de soporte: <http://www.bitdefender.com/businesshelp>

Alemania

Bitdefender GmbH

Airport Office Center

Robert-Bosch-Straße 2

59439 Holzwickede

Deutschland

Tel (oficina&comercial): +49 (0)2301 91 84 222

Teléfono (soporte técnico): +49 (0)2301 91 84 444

Comercial: vertrieb@bitdefender.de

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

Centro de soporte: <http://www.bitdefender.de/businesshelp>

Reino Unido e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK

Teléfono (comercial&soporte técnico): +44 (0) 8451-305096

Correo: info@bitdefender.co.uk

Comercial: sales@bitdefender.co.uk

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

Centro de soporte: <http://www.bitdefender.co.uk/businesshelp>

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

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

Centro de soporte: <http://www.bitdefender.com/businesshelp>

A. Apéndices

A.1. Lista de tipos de archivos de aplicación

Los motores de análisis antimalware incluidos en las soluciones Bitdefender pueden configurarse para limitar el análisis únicamente a los archivos de aplicaciones (o programas). Los archivos de aplicaciones son mucho más vulnerables a los ataques de malware que otro tipo de archivos.

Esta categoría incluye los archivos con las siguientes extensiones:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpv; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.2. Usar variables de sistema

Algunas de las opciones disponibles en la consola requieren especificar la ruta en las máquinas virtuales objetivo. Se aconseja utilizar variables de sistema (donde sea adecuado) para asegurar que la ruta es válida en todas las MVs objetivo.

Aquí está la lista de variables de sistema predefinidas:

`%ALLUSERSPROFILE%`

La carpeta del perfil Todos los usuarios. Ruta típica:

`C:\Documents and Settings\All users`

`%APPDATA%`

La carpeta Application Data del usuario que ha iniciado sesión. Ruta típica:

- **Windows XP:**
C:\Documents and Settings\{username}\Application Data
- **Windows Vista/7:**
C:\Usuarios\{username}\AppData\Roaming

%HOMEPATH%

Las carpetas de usuario. Ruta típica:

- **Windows XP:**
\Documents and Settings\{username}
- **Windows Vista/7:**
\Usuarios\{username}

%LOCALAPPDATA%

Los archivos temporales de las aplicaciones. Ruta típica:

C:\Usuarios\{username}\AppData\Local

%PROGRAMFILES%

La carpeta Archivos de programa. Una ruta típica es C:\Archivos de programa.

%PROGRAMFILES(X86)%

La carpeta Archivos de programa para aplicaciones de 32 bits (en sistemas de 64 bits). Ruta típica:

C:\Archivos de programa (x86)

%COMMONPROGRAMFILES%

La carpeta Common Files. Ruta típica:

C:\Archivos de Programa\Archivos Comunes

%COMMONPROGRAMFILES(X86)%

La carpeta Common files para aplicaciones de 32 bits (en sistemas de 64 bits). Ruta típica:

C:\Archivos de Programa (x86)\Archivos Comunes

%WINDIR%

El directorio Windows o SYSROOT. Una ruta típica sería C:\Windows.

Glosario

ActiveX

El ActiveX es un modelo para escribir programas de manera que otros programas y sistemas operativos puedan usarlos. La tecnología ActiveX se utiliza junto con Microsoft Internet Explorer para hacer páginas web interactivas que se vean y comporten como programas, y no como páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, pulsar botones, interactuar de otras formas con una página web. Los controles ActiveX normalmente se escriben en Visual Basic.

ActiveX es notable por la ausencia absoluta de mandos de seguridad; los expertos de la seguridad computacional desapruaban el empleo de ActiveX en Internet.

Actualización

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

Bitdefender tiene su propio módulo para realizar las actualizaciones, permitiéndole a usted buscar manualmente las actualizaciones o bien hacer una actualización automática del producto.

Adware

El Adware habitualmente se combina con aplicaciones que son gratuitas a cambio que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan después que el usuario acepte los términos de licencia que declaran el propósito de la aplicación, no se comete ningún delito. Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar preocupación acerca de su privacidad a aquellos usuarios que no son plenamente conscientes de los términos de la licencia.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Applet de Java

Es un programa de Java diseñado para funcionar solamente en una página web. Para usarlo tendría que especificar el nombre del applet y la dimensión (de ancho y de largo --- en pixels) que éste usará. Al acceder a una página web, el navegador descarga el

applet desde un servidor y lo abre en el ordenador del usuario (del cliente). Los applets difieren de las aplicaciones al ser gobernados por un protocolo de seguridad muy estricto.

Por ejemplo, aunque los applets se puedan ejecutar directamente en el ordenador del cliente, no pueden leer o escribir información en aquel ordenador. Además, los applets tienen restricciones en cuanto a leer y escribir información desde la misma área a la que pertenecen.

Appliance virtual

Una imagen de máquina virtual que contiene tanto un sistema operativo preconfigurado como una aplicación para facilitar la instalación y configuración de la aplicación en un entorno virtualizado.

Archivo Comprimido

Disco, cinta o directorio que contiene ficheros almacenados.

Fichero que contiene uno o varios ficheros en formato comprimido.

Archivo de informe

Es un archivo que lista las acciones realizadas. Bitdefender genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos infectados y sospechosos que se han detectado.

Área de notificación del Sistema

Elemento introducido con el sistema Windows 95, la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

Backdoor

Se trata de un agujero de seguridad dejado intencionalmente por los diseñadores o los administradores. El objetivo de estos agujeros no es siempre dañino; algunos sistemas operativos funcionan con unas cuentas privilegiadas, creadas para los técnicos de servicio u operadores de mantenimiento.

Cliente de mail

Un cliente de e-mail es una aplicación que permite enviar y recibir mensajes.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención

de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

Correo

Correo electrónico. Un servicio que envía mensajes a otros ordenadores mediante las redes locales o globales.

Descargar

Para copiar informaciones (por lo general un fichero entero) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un fichero desde un servicio online al ordenador personal. También se refiere al proceso de copiar ficheros desde un servidor de la red a un ordenador conectado a la red.

Elementos de Inicio

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo: una pantalla, un fichero audio, un calendario de tareas u otras aplicaciones pueden ser elementos de startup. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Eventos

Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

Explorador

Forma abreviada de Navegador de Web, aplicación de software empleada para ubicar y cargar las páginas web. Los dos navegadores más populares son Netscape Navigator y Microsoft Internet Explorer, sendos navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos incluyen información multimedia: sonido e imágenes, aunque requieran plugins para ciertos formatos.

Extensión de un archivo

La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Hay varios sistemas operativos que utilizan extensiones de archivos (Por Ej. Unix, VMS, MS-DOS). Por lo general las extensiones tienen de uno a tres caracteres. Por ejemplo, ".c" para archivos de código fuente en lenguaje C, ".ps" para PostScript, ".txt" para documentos de texto.

Falso positivo

Ocurre cuando un analizador identifica un fichero como infectado cuando éste no lo es.

Firma de virus

Es la secuencia binaria de un virus, utilizada por los antivirus para detectar y eliminar los virus.

Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede agregar a otros programas.

Heurístico

Es un método para identificar nuevos virus, que se basa en ciertas reglas y no en firmas específicas de los virus. La ventaja del análisis heurístico reside en la dificultad de engañarlo con una nueva versión de un virus ya existente. Sin embargo, ocasionalmente puede notificar sobre la existencia de unos códigos sospechosos en los programas normales, generando el "falso positivo".

Hypervisor

Un programa que permite ejecutar múltiples sistemas operativos en un solo equipo.

IP

Internet Protocol - Protocolo enrutable dentro del protocolo TCP/IP y que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblado de los paquetes IP.

Línea de comando

En una interfaz con línea de comando, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

Malware

Malware es el término genérico que define al software diseñado para causar daños - una contracción de 'malicious software'. Todavía no se usa de forma universal, pero su popularidad como términos general para definir virus, troyanos, gusanos y código móvil malicioso está creciendo.

Máquina virtual

Un entorno de software aislado que emula un equipo físico en el cual puede ejecutarse un sistema operativo y aplicaciones.

Memoria

Área de almacenamiento interno en un ordenador. El término memoria se refiere al almacenamiento de información en forma de virutas y la palabra almacenamiento se emplea para la memoria guardada en cintas o disquetes. Cada ordenador tiene una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

No Heurístico

Este método de análisis se basa en firmas de virus específicas. La ventaja del análisis no heurístico es que no se le puede engañar por algo que parecería ser un virus. Por consiguiente, no genera alarmas falsas.

Phishing

Es el acto de enviar un e-mail a un usuario simulando pertenecer a una empresa existente, e intentar estafarlo solicitándole información privada con la que después se efectuará el robo. El e-mail conduce al usuario a visitar una página Web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Programas Empaquetados

Son ficheros en formato comprimido. Muchos sistemas operativos y varias aplicaciones contienen comandos que le permiten a usted empaquetar un fichero para que ocupe menos espacio en la memoria. Por ejemplo: tiene un fichero de texto conteniendo diez caracteres espacio consecutivos. Normalmente, para esto necesitaría diez bytes de almacenamiento.

Sin embargo, un programa que puede empaquetar ficheros podría reemplazar los caracteres mencionados por una serie a la que le sigue el número de espacios. En este caso, los diez espacios requieren dos bytes. Ésta es solamente una técnica para empaquetar programas o ficheros, hay muchas otras también.

Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el punto final de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX

y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricos, si éstos incorporan el software apropiado.

Los rootkits no son maliciosos por naturaleza. Por ejemplo, los sistemas operativos y algunas aplicaciones esconden sus archivos críticos mediante rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar archivos o logs, y evitar su detección.

Ruta

Las direcciones exactas de un fichero en un ordenador, generalmente descritas mediante un sistema jerárquico: se empieza por el límite inferior, mostrando un listado que contiene la unidad de disco, el directorio, los subdirectorios, el fichero mismo, la extensión del fichero si tiene alguna. Esta suma de informaciones es una ruta completamente válida.

La ruta entre dos puntos, como por ejemplo el canal de comunicación entre dos ordenadores.

Script

Es otro término para macro o fichero batch y se constituye de una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Sector de arranque

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

Sistema operativo del guest

Un sistema operativo aislado que funciona dentro de otro sistema operativo (el host) dentro de un sistema virtualizado.

Sistema operativo del host

Un sistema operativo dentro del cual otros sistemas operativos (los guests) se ejecutan por virtualización.

Spam

Correo basura o los posts basura en grupos de noticias, también denominado correo no solicitado.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información acerca de las direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al Troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del Spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los caballos troyanos no se multiplican; sin embargo pueden ser igual de peligrosos. Unos de los tipos más insidiosos de Troyano es un programa que pretende desinfectar su ordenador y que en realidad introduce virus.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

Unidad de disco

Es un dispositivo que lee la información y / o la escribe en un disco.

Una unidad de disco duro lee y escribe en los discos duros.

Una unidad de disquetera abre disquetes.

Las unidades de disco pueden ser internas (guardadas en el ordenador) o externas (guardadas en una caja separada conectada al ordenador).

Virus

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

Virus de boot

Es un virus que infecta el sector de arranque de un disco duro o disquete. Al intentar arrancar el sistema desde un disco infectado con un virus de boot, el virus quedará cargado en la memoria. A partir de ese momento, cada vez que intente arrancar el sistema, tendrá el virus activo en la memoria.

Virus de macro

Es un tipo de virus informático, que se encuentra codificado como un macro incluido en un documento. Muchas aplicaciones, como las de Microsoft Word o Excel, soportan fuertes lenguajes de macro.

Estas aplicaciones permiten introducir una macro en un documento y también que la macro se ejecute cada vez que se abra el documento.

Virus Polimórfico

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.