bitdefender
BUSINESS SOLUTIONS

# SECURITY FOR MAIL SERVERS

Guía de usuario

# Bitdefender Security for Mail Servers
*Guía de usuario*

Publication date 2012.12.03


Bitdefender

# Table of Contents

# Acuerdo de Licencia de Software

SI NO ACEPTA LOS TÉRMINOS DE LA LICENCIA, NO INSTALE EL PRODUCTO. AL SELECCIONAR "ACEPTO", "OK", "CONTINUAR", "SI" O AL INSTALAR O USAR EL SOFTWARE DE ALGÚN MODO, ESTÁ INDICANDO QUE HA ENTENDIDO POR COMPLETO Y HA ACEPTADO LOS TÉRMINOS DE ESTE ACUERDO.

Estos términos cubren las Soluciones y Servicios BitDefender dedicados a las empresas incluidas en su licencia, tales como la información relacionada y cualquier actualización o mejora de las aplicaciones entregadas bajo los términos de la licencia comprada, o cualquier acuerdo de servicio relacionado según lo definido en la documentación y cualquier copia de estos artículos.

Este Contrato de Licencia representa un acuerdo legal entre Usted (como persona física o jurídica) y BITDEFENDER para la utilización del software de Bitdefender identificado anteriormente, que incluye el software y servicios informáticos y puede incluir también soporte físico adjunto, materiales impresos, así como la documentación electrónica u “online” (designada aquí como “Bitdefender”), todo lo cual está protegido por la legislación y tratados internacionales referentes al copyright. La instalación, copia u otra forma de utilización del producto BitDefender, significa que acepta los términos de este contrato. Si no está de acuerdo con los términos de este acuerdo, no instale o use BitDefender.

Licencia BitDefender. BitDefender está protegido por las leyes de derechos de autor (el copyright), las leyes de la propiedad intelectual y otros tratados internacionales que sean de aplicación. El producto de software BitDefender es un producto con licencia. La licencia va junto con el producto y no se vende por separado.

CONCESIÓN DE LICENCIA. Por la presente, BITDEFENDER le concede a usted y sólo la siguiente licencia no exclusiva, limitada, instransferible y con pago de derechos para el uso de BitDefender.

SOFTWARE DE APLICACIÓN. Usted puede instalar y usar BitDefender, en tantos de ordenadores como sea necesario considerando la limitación impuesta por el número total de usuarios autorizados. Usted puede hacer una copia adicional a modo de copia de seguridad.

LICENCIA DE USUARIO CORPORATIVO. Esta licencia se aplica al software BitDefender que puede instalarse en un sólo equipo que proporcione servicios a la red. Puede instalar este producto en todos los ordenadores en los que sea necesaria su instalación, mientras no se supere la limitación en cuanto al número de usuarios para los cuales se ofrecen servicios de red. Esta limitación se refiere número total de usuarios que tiene que ser inferior o igual al número de usuarios de la licencia.

LICENCIA DE USUARIO DOMÉSTICO. Esta licencia se aplica al software BitDefender que puede instalarse en un sólo equipo y que no proporcione servicios a la red. Cada usuario primario puede instalar este software sobre un sólo ordenador y puede hacer una copia adicional para la reserva sobre un dispositivo diferente. El número de usuarios primarios permitidos es el número de los usuarios de la licencia.

PERIODO DE LICENCIA. La licencia concedida a continuación comenzará en la fecha de adquisición de BitDefender y expirará al final del período para el cual compró la licencia.

CADUCIDAD. El producto dejará de realizar sus funciones inmediatamente después de la expiración de la licencia.

ACTUALIZACIONES. Si Bitdefender tiene disponible una actualización de producto (upgrade), debe ser un usuario registrado para usar el producto identificado por BITDEFENDER para poder beneficiarse de dicha actualización. BitDefender incluye como "upgrade" la versión actual que reemplaza o / y substituye el producto básico con licencia. El comprador puede utilizar el producto actualizado en las condiciones estipuladas en los términos del presente contracto. Si hay alguna actualización de algún componente del paquete de software para el cual tiene licencia para un sólo producto, BitDefender puede ser transferido y usado sólo como parte del paquete de producto y no puede ser separada para usarse en más ordenadores de los autorizados por medio de la licencia. Los términos y condiciones de esta licencia reemplazan y sustituyen cualquier acuerdo previo que pueda haber existid entre usted y BITDEFENDER respecto al producto original o el producto actualizado resultante.

COPYRIGHT. Todos los derechos, títulos y todos los beneficios como derechos de copia de Bitdefender (incluyendo pero no limitándose a cualquier imagen, fotografía, logo, animación, vídeo, audio, música, texto y "applets" incorporados en Bitdefender), los materiales impresos adjuntos y cualquier copia de BITDEFENDER son propiedad de BITDEFENDER. BitDefender está protegido por la legislación y tratados internacionales referentes al copyright. Así pues, Usted debe tratar a BitDefender como a cualquier otro producto con copyright. No debe copiar el material que acompaña al producto BitDefender. El comprador tiene la obligación de incluir todos los documentos originales de Copyright para todas las copias creadas independientemente del medio de grabación o en el BitDefender adquirido. Está prohibido entregar licencias y también alquilar, vender, o realizar "leasing" para el producto BitDefender. Tampoco debe rediseñar, recompilar, desensamblar, crear trabajos derivativos, modificar, traducir o realizar cualquier intento para descubrir el código fuente de BitDefender.

LÍMITES DE LA GARANTÍA. BITDEFENDER garantiza el funcionamiento del programa Bitdefender, de acuerdo con lo especificado en el manual y ayuda electrónica incluidas

en el producto durante treinta días a partir de la fecha de recepción. La rotura de esta garantía supone que BITDEFENDER, en su opinión, puede reemplazar el servicio defectuoso hasta el recibimiento del servicio dañado, o devolver el dinero que pagó por BitDefender. BITDEFENDER no garantiza que BitDefender será ininterrumpido, libre de errores o que los errores serán corregidos. BITDEFENDER no garantiza que BitDefender cubrirá sus requisitos

CON EXCEPCIÓN DE LO EXPLÍCITAMENTE DISPUESTO EN ESTE ACUERDO, BITDEFENDER NIEGA CUALQUIER OTRA GARANTÍA, EXPLICITA O IMPLÍCITA, EN LO QUE CONCIERNE A LOS PRODUCTOS BITDEFENDER, MEJORAS, MANTENIMIENTO O SOPORTE RELACIONADO, ASÍ COMO CUALQUIER OTRO MATERIAL (TANGIBLE O INTANGIBLE) O SERVICIOS SUMINISTRADOS POR ÉL. BITDEFENDER, POR LA PRESENTE, NIEGA EXPRESAMENTE CUALQUIER GARANTÍA Y CONDICIÓN IMPLÍCITA, INCLUYENDO, SIN RESTRICCIÓN, LAS GARANTÍAS IMPLÍCITAS DE VALOR COMERCIAL, IDONEIDAD PARA UN OBJETIVO PARTICULAR, TÍTULO, NO INTERFERENCIA, EXACTITUD DE DATOS, EXACTITUD DE CONTENIDO INFORMATIVO, INTEGRACIÓN DEL SISTEMA, Y LA NO INFRACCIÓN DE DERECHOS DE UN TERCERO POR FILTRADO, DESHABILITACIÓN, O ELIMINACIÓN DEL SOFTWARE DE DICHO TERCERO, SPYWARE, ADWARE, COOKIES, CORREO ELECTRÓNICO, DOCUMENTOS, PUBLICIDAD O SIMILARES, TANTO SI SURGE POR ESTATUTO, LEY, CURSO DEL TRATO, COSTUMBRE Y PRÁCTICA O USO COMERCIAL.

TÉRMINOS LEGALES. El usuario que analiza, prueba o evalúa BitDefender será responsable de los perjuicios que pudieran producirse por el uso incorrecto de BitDefender. En ningún caso, BITDEFENDER se hará responsable por ningún tipo de daño incluyendo, sin limitaciones, los daños directos o indirectos que deriven de la utilización del producto BitDefender aunque BITDEFENDER haya sido advertido de la existencia o la posibilidad de aparición de tales daños.

ALGUNOS ESTADOS NO PERMITEN LA LIMITACIÓN O LA EXCLUSIÓN DE RESPONSABILIDAD DE DAÑOS SECUNDARIOS O CONSIGUIENTES, ENTONCES LA LIMITACIÓN CITADA ANTERIORMENTE PUEDE NO APLICARSE A USTED.

EN NINGÚN CASO LA RESPONSABILIDAD DE BITDEFENDER EXCEDERÁ EL PRECIO DE COMPRA PAGADO POR USTED POR LA COMPRA DE BITDEFENDER. Las condiciones estipuladas en esta sección se aplicarán tanto si acepta, utiliza, evalúa o prueba BitDefender.

AVISO IMPORTANTE A LOS USUARIOS. ESTE SOFTWARE PUEDE CONTENER ERRORES, Y NO ESTÁ INDICADO SU UTILIZACIÓN EN NINGÚN MEDIO QUE REQUIERA UN GRADO ALTO DE RIESGO Y QUE NECESITE ALTA ESTABILIDAD. ESTE PRODUCTO DE SOFTWARE NO ESTÁ DESTINADO A SECTORES DE LAS

AREAS DE AVIACIÓN, CENTRALES NUCLEARES, SISTEMAS DE TELECOMUNICACIONES, ARMAS, O SISTEMAS RELACIONADOS CON LA SEGURIDAD DIRECTA O INDIRECTA DE LA VIDA. TAMPOCO ESTÁ INDICADO PARA APLICACIÓNES O INSTALACIONES DONDE UN ERROR DE FUNCIONAMIENTO PODRÍA PROVOCAR LA MUERTE, DAÑOS FÍSICOS O DAÑOS CONTRA LA PROPIEDAD.

GENERAL. Este Contrato está gobernado por las leyes de Rumania y por la legislación y tratados internacionales relativos al copyright. La jurisdicción y venia exclusiva para adjudicar cualquier disputa que derive de esos Términos de Contrato pertenece a los juzgados de Rumania.

Los precios, gastos y tarifas del uso de BitDefender están sujetos a cambios sin previo aviso.

En caso de invalidez de cualquier cláusula de este Acuerdo, la invalidez no afectará la validez de las partes restantes de este Acuerdo.

BitDefender y los logos BitDefender son las marcas registradas por BITDEFENDER. Todas otras marcas registradas usadas en el producto o en materiales asociados son la propiedad de sus respectivos dueños.

La licencia quedará rescindida inmediatamente sin previo aviso si usted viola cualquiera de sus términos y condiciones. Usted no tendrá derecho a un reembolso por parte de BITDEFENDER o de ninguno de los distribuidores o revendedores de BitDefender como consecuencia de la rescisión. Los términos y condiciones acerca de la confidencialidad y restricciones sobre el uso permanecerán en vigor hasta después de cualquier rescisión.

BITDEFENDER podrá revisar estos Términos en cualquier momento y los términos revisados se aplicarán automáticamente a las versiones correspondientes del Software distribuido con dichos términos revisados. Si cualquier parte de estos Términos fuera encontrado nulo o impracticable, la validez del resto de los Términos no se verá afectada, ya que seguirán siendo válidos y practicables.

En caso de controversia o inconsistencia entre las traducciones a otros idiomas de estos Términos, prevalecerá la versión en inglés emitida por BITDEFENDER.

Contactar con BITDEFENDER, en la C/ Balmes 191, 08006 Barcelona, España, por teléfono a +34 902 190 765 o Fax: + 34 93 217 91 28, dirección de correo: office@bitdefender.com

# Prólogo

Esta *guía del usuario* está dirigido a todos los administradores de sistemas que han elegido Bitdefender Security for Mail Servers como solución de seguridad para correo electrónico de su email de archivo. La información presentada en este documento es apta no sólo para expertos en informática, sino para todas aquellas personas capaces de trabajar con Linux o UNIX.

Este manual le describirá el producto Bitdefender Security for Mail Servers, le guiará a través del proceso de instalación y le enseñará a configurarlo. Descubrirá cómo utilizar Bitdefender Security for Mail Servers, cómo actualizarlo, probarlo y personalizarlo. En resumen, aprenderá a integrar este con varios software y a sacarle el máximo provecho a Bitdefender.

Le deseamos una provechosa y agradable lectura.

## 1. Convenciones utilizadas en este libro

### 1.1. Convenciones tipográficas

En este manual se utilizan distintos estilos de texto con el fin de mejorar su lectura. Su aspecto y significado se indica en la tabla que aparece continuación.

| *Apariencia* | *Descripción* |
|---|---|
| `variable` | Las variable y algunos datos numéricos son imprimidos con caracteres `monospaced`. |
| http://www.bitdefender.es | Los enlaces URL le dirigen a alguna ubicación externa, en servidores http o ftp. |
| soporte@bitdefender.es | Los Correos son incluidos en el texto como información de contacto. |
| Chapter 4 "*Instalación de paquetes*" (p. 15) | Este es un enlace interno, hacia alguna localización dentro del documento. |
| `nombre de archivo` | Los archivos y carpetas se muestran usando una fuente `monoespaciada`. |
| `ENV_VAR` | Las variables de entorno son `MAYÚSCULAS MONOESPACIADAS`. |

| *Apariencia* | *Descripción* |
|---|---|
| *enfatizado* | *Texto enfatizado* especialmente marcado para llamar su atención. |
| “texto citado” | Proporcionado como referencia. |
| **comando** | La línea de comando son impresas con caracteres en **negrita**. |
| `# comando-parameter` | Los ejemplos de comando son impreso en caracteres en negrita monoespaciado en un entorno especialmente marcado. El mensaje puede ser uno de los siguientes.<br>**#** La raíz del sistema. Debe ser superusuario con el fin de ejecutar este comando.<br>**$** El usuario normal. No necesita privilegios especiales para ejecutar el comando. |
| `screen output` | La pantalla y el código listado se muestran en caracteres monoespaciados en un entorno especialmente marcado. |
| **bdlogd(8)** | Se refiera a una página del manual. |

## 1.2. Admoniciones

Las advertencias son notas en texto, marcado gráficamente, ofreciendo información adicional relacionada al parágrafo actual.

***Note***
La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, tales como características específicas o un enlace a hacia temas relacionados.

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

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

# 2. Estructura del Manual

El manual consiste en cuatro partes, contiene los siguientes temas: Descripción y características, Instalación, Uso y Obtener Ayuda. Un glosario y las páginas de manual de UNIX se proporcionan para aclarar diferentes aspectos de Bitdefender, lo que podría ocasionar problemas técnicos.

**Descripción .** Una breve introducción a Bitdefender. En él se explica que es Bitdefender, y la División de Seguridad de Datos. Se le presenta Bitdefender Security for Mail Servers, sus características, los componentes de productos y los fundamentos de la integración y el mecanismo de escaneo.

**Pasos de la Instalación .** Instrucciones paso a paso para la instalación de Bitdefender en un sistema. Comenzando por los requisitos previos para lograr una instalación correcta, se le guiará a través de todo el proceso de instalación. Por último, el procedimiento de desinstalación se describe en el caso de que necesite desinstalar Bitdefender.

**Iniciando .** Descripción de la administración básica y del mantenimiento de Bitdefender.

**Modo Avanzado .** Se le presentan las herramientas de configuración de Bitdefender, como obtener información en tiempo de ejecución, como probar la eficiencia del antivirus, como realizar actualizaciones y como registrar el producto.

**Administración Remota .** Aprenderá cómo sacar el mejor partido de Bitdefender remotamente, utilizando varias herramientas de administración remota.

**Obtener Ayuda .** Dónde mirar y dónde pedir ayuda si algo no funciona bien. Se le presentó la Base de Conocimiento y ofreció Bitdefender y Bitdefender Información socios contacto para llamar, si es necesario.

**Apéndices .** Los Apéndices presentan una información exhaustiva sobre la configuración, plantillas de correo y un debate en profundidad sobre las partes más engorrosas.

**Glosario .** El Glosario trata de explicar algunos términos técnico y poco comunes que encontrará en las páginas de este documento.

# 3. Petición de Comentarios

Le invitamos a ayudarnos a mejorar el manual. Hemos comprobado y verificado toda la información para mejorar nuestra capacidad, pero es posible que las características hayan cambiado (o incluso hayamos cometido errores). Por favor, escríbanos para contarnos cualquier tipo de defecto que encuentre en este manual o cómo cree que se podría mejorar, y así ayudarnos a ofrecerle la mejor documentación posible.

Haganoslo saber enviando un e-mail a documentation@bitdefender.com.

# Descripción

# 1. Características y Beneficios

**Amplia protección anti-malware para Servidores de Correo basados en UNIX.** Diseñado para servidores de correo basados en UNIX, Bitdefender Security for Mail Servers proporciona conjuntamente tecnologías antivirus, antispyware, antispam, antiphishing y filtrado de contenido, para proteger el tráfico de correo de las compañías y de los proveedores de servicios. Gracias a su compatibilidad con las principales plataformas de correo, la solución le ofrece una protección fiable frente a nuevo malware emergente e intentos de robo de datos confidenciales y valiosos.

## 1.1. Características

- Implementación rápida y sencilla
- Fácil integración con sus actuales servicios de correo
- Compatible con las principales plataformas de correo
- Protección heurística proactiva contra amenazas 'zero-day'
- Múltiples capas de filtros antispam
- Filtro de contenido y archivos adjuntos
- Protección antispyware y antiphishing
- Interfaz intuitiva
- Disponible en versiones de 32-bit y 64-bit

## 1.2. Beneficios Principales

- Protección del e-mail frente al Malware
  - Combate el malware proveniente del e-mail, filtrando y bloqueando mensajes que contienen código peligroso activo
  - Proporciona protección anti-phishing al detectar proactivamente los mensajes falsificados que intentan engañar al destinatario para que revele sus datos confidenciales
  - Ofrece la posibilidad de manejar riskware de manera separada (aplicaciones que presentan una potencial amenaza, pero que algunos grupos de usuarios pueden necesitar)
- Compatibilidad
  - Incluye agentes dedicados para una integración automática con la mayoría de los agentes de transferencia de correo más populares, como Sendmail (milter), Postfix, Courier, gmail y CommuniGate Pro

- Cumple totalmente con FHS (FIlesystem Hierarchy Standard), operando de una manera completamente no intrusiva
- Compatible con la mayoria de plataformas basadas en Unix con paquetes rpm, deb and generic .tar.run

- Incremento de la Productividad Empresarial
  - Reduce el tráfico de correo y ahorra recursos de red gracias a sus amplias capacidades de protección antimalware
  - A través de su optimizado proceso de análisis, aumenta la velocidad de entrega de los mensajes y reduce la carga de trabajo del servidor
  - Mejora la productividad de los Administradores de TI y previene la perdido de información confidencial filtro todos los mediante a través del servidor de correo basado en:
    - contenido (asunto, cuerpo, destinatario, remitente) y adjunto
    - el criterio definido para los grupos de usuario existente
  - Incluye un sistema de protección antispam multi-capa sumamente eficiente, que:
    - reduce el tráfico de correo clasificando con precisión los mensajes como spam, phishing o legitimos.
    - bloquea correo no solicitado basándose en varios filtros, entre los cuales:
      - el Filtro Bayesiano, el cual puede entrenar para que aprenda de los correos spam específicos recibidos por su servidor.
      - El filtro en tiempo real de la lista negra (RBL), el cual identifica el spam basado en la reputación de los servidores de correo como remitentes de spam
    - Permite personalizar la sensibilidad del filtro antispam, estableciendo umbrales restrictivos o permisivos en cada uno de los grupos de usuario
  - Incluye soporte WBL (Lista Blanca y Negra), lo que le permite crear una lista con las direcciones de confianza o direcciones a bloquear, cuyos mensajes siempre se aceptarán o rechazarán respectivamente
- Mayor Facilidad de Uso
  - Le permite filtrar el tráfico de correo más flexiblemente, apalancamiento antivirus, antispam, políticas de filtro de contenido y adjuntos para diferentes grupos o usuarios
  - Genere estadísticas detalladas e informes relacionados con la actividad de la solución
  - Envia notificaciones personalizables por correo sobre esta actividad
  - Le permite configurar remotamente la protección de correo mediante estas herramientas de administración

- Una interfaz de linea de comando dedicado le permite realizar tareas de configuración y administración después de instalar
- Puede aislar los correos peligrosos o restringidos en una zona de cuarentena para ser tratados más tarde
- En el área de cuarentena se pueden realizar búsquedas basadas en expresiones regulares, remitente, destinatatio, fecha y causa.
- Permite realizar acciones de administración vía SNMP por medio de este Plug-in SNMP Daemon
- Puede enviar alertas de virus y administración a tres host diferentes, a través del plug-in de registros SNMP

# 2. arquitectura de Bitdefender

Bitdefender es una estructura modular muy complejo. Se compone de varios componentes centrales y módulos adicionales, cada uno de ellos es asignado a tareas específicas. Los módulos se cargan durante el inicio de Bitdefender y habilitado o no, de acuerdo a las preferencias del usuario. En un sistema UNIX, estos componentes se ejecutan como daemons, en uno o múltiples hilos y se comunican con los demás.

## 2.1. Módulos principales

Listados por sus nombres de archivo, los módulos principales son representados en la siguiente tabla.

| *Módulo* | *Descripción* |
|---|---|
| **bdmond** | El monitor central de Bitdefender es el supervisor de varios módulos de Bitdefender. Cuando uno de ellos falla, el Monitor Principal aísla el objeto causante del error en un directorio de cuarentena especial, notifica al administrador y reinicia el módulo involucrado. Así, incluso si un proceso muere, no afecta a toda la actividad de filtrado, garantizando una continua protección del servidor. |
| **bdscand** | Este es el Daemon de análisis de Bitdefender. Su propósito es integrar los motores de análisis, recibir peticiones de análisis de varios daemons, como el daemon de correo o el de archivo. Analiza los objetos, toma las acciones necesarias y envía de vuelta el objeto y los resultados del análisis. |
| **bdmaild** | El archivo Daemon de Bitdefender tiene el rol de recibir solicitudes de análisis de los agentes de la integración de MTA. Llama al Daemon de análisis para realizar el análisis, esperando el resultado del análisis de este. Entonces aplica sus acciones y devuelve los resultados al agente de integración MTA. |
| **bdregd** | El Registro de Bitdefender está compuesta por el programa de **bdregd** y un conjunto de archivos XML, donde se almacena el la configuración de Bitdefender. El daemon recibe peticiones de lectura de y escribir al archivo de configuración, peticiones iniciadas por otros procesos. El Registro puede recibir solicitudes de otros hosts también, usando una conexión segura TCP en el puerto `8138`. Toda comunicación remota se realiza utilizando SSL (Secure Socket Layer). Esto |

| Módulo | Descripción |
|---|---|
| | solamente es útil cuando usted utiliza alguna Consola de Administración Remota, eventualmente ejecutándose en algunos Sistemas Operativos no UNIX. Si no, por razones de seguridad, se recomienda mantener estas características desactivadas (están desactivadas por defecto).<br><br>  <br>***Editando manualmente el Registro***<br>Aún cuando los archivos XML son legibles (y escribibles), nunca debe intentar editarlos manualmente. Debido a su alta complejidad, los archivos XML sólo debe ser modificado por medio de las herramientas de configuración que se proporcionan, tales como les comandos o las consolas **bdsafe** de administración remota. |
| **bdlogd** | El Logger de Bitdefender es un componente complejo, el manejo de todas las actividades de tala y la notificación de Bitdefender. Hay varios tipos de log, todos ellos realizados por plugins.<br><br>● *registro de archivos:* se envían los datos a un archivo de registro normal, respetando un formato típico.<br>● *notificación de correo:* se envían alertas por e-mail al administrador del servidor o al remitente y receptores de un e-mail, en eventos especiales (como un e-mail infectado).<br>● *Informe de Virus y Spam en Tiempo Real:* se envían estadísticas anónimas a los Laboratorios Bitdefender, para mantener un mapa de actividad del malware y para detectar brotes.<br>● *SNMP:* pueden enviarse notificaciones a través del protocolo SNMP al host designado. |
| **bdlived** | The Bitdefender Live! Update is the module responsible with updating the scanning engines and some other Bitdefender components. The module runs continuously and periodically checks the update server. It can also be triggered manually or by the Update Pushing mechanism.<br><br>  <br>***More about Live! Update***<br>Bitdefender Live! Update and the update process are described in Chapter 14 "*Actualizaciones*" (p. 73). |

| *Módulo* | *Descripción* |
|---|---|
| **bdsnmpd** | **bdsnmpd** acepta mensajes SNMP GET y SET relacionados con las claves de registro de BitDefender. Así, un usuario autorizado es capaz de leer y modificar algunas de las configuraciones de BitDefender de manera remota. |

## 2.2. Los agentes de integración

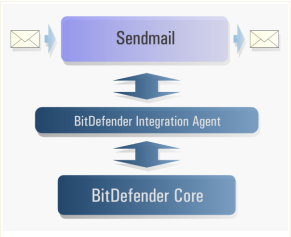
El cuerpo del mensaje y sus adjuntos serán verificados en orden de detectar archivos infectados y puertas traseras, troyanos y archivos gusano para prevenir su expansión en la red.

Solo los mensajes limpios serán enviados a los clientes de correo o a los destinatarios del correo fuera de la compañía. Basado en la opción del administrador, los mensajes infectados son desinfectados, borrados o aislados en una ubicación concreta en el servidor, la zona de cuarentena.

### 2.2.1. Sendmail

El agente Sendmail es la solución de filtrado para los servidores de correo Sendmail con interface Milter. Milter permite que programas de terceros accedan a los mensajes a traves de varias llamadas.

The incoming email will normally arrive to Sendmail, from local or remote machines. Through the milter interface, Sendmail allows the Bitdefender agent to inspect the email. The agent calls the Bitdefender core to scan it and, after scanning, the results are passed through the milter interface back to Sendmail, which will deliver the message as usual, if there is something to deliver.

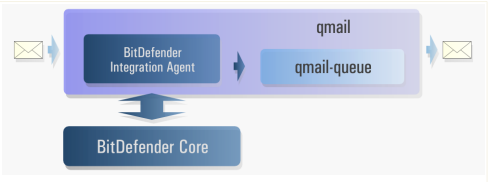



**Integración Sendmail**

### 2.2.2. qmail

Inside the qmail MTA, **qmail-queue** is the central component. All the emails coming from local or remote senders pass through this component. Therefore email traffic can be captured by capturing the traffic of **qmail-queue**.

Remote or local incoming emails are first passed to the Bitdefender qmail integration agent. This will send them to the Bitdefender core for scanning and then to the original **qmail-queue**, which will deliver them as usual. From the qmail point-of-view, the filtering process is transparent.

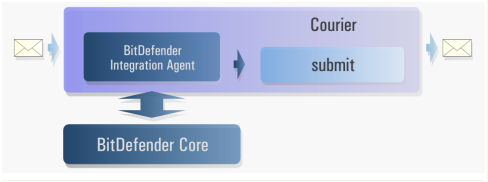



**Integración qmail**

## 2.2.3. Courier

The central module of the Courier system is **submit**, an uniform mechanism which ads messages to the mail queue. Capturing its traffic is capturing the server's traffic.

Remote or local incoming emails are first passed to the Bitdefender Courier integration agent, named **bdcourier**. This will pass them on to the Bitdefender core for scanning and then to the original **submit**, which will enqueue them as usual. From the Courier point-of-view, the filtering process is transparent.

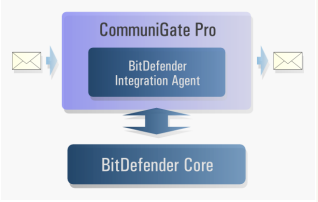



**Integración Courier**

## 2.2.4. CommuniGate Pro

El agente de integración de Bitdefender debe incorporarse con CommuniGate Pro, utilizando su propio mecanismo de filtrado, para recibir el tráfico de correo.

Remote or local incoming emails are passed to the Bitdefender CommuniGate Pro agent, registered as intrinsic filter. This will call the Bitdefender core to scan the emails and then pass them back to the MTA, which will process them as usual.

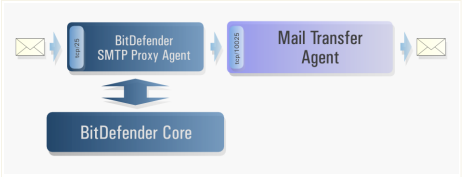



**Integración CommuniGate Pro**

## 2.2.5. Proxy SMTP

La integración SMTP varia con cada MTA. Como no podemos cubrir todas las posibles variantes,

ofrecemos una pequeña descripción de la integración para que usted decida como aplicarla en su servidor SMTP.



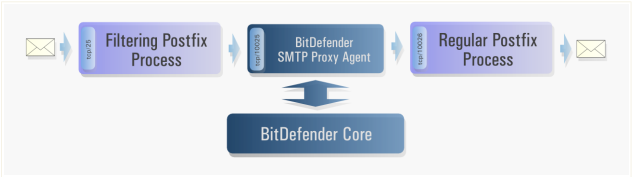

**Integración SMTP Proxy**

The incoming email will arrive on port `25` of the machine. On this port it is not the original Mail Transport Agent that is listening, but a special Bitdefender component, the SMTP Proxy module. On receiving the message, the Bitdefender Agent will pass it to the Bitdefender core for scanning. The core does the usual scanning and passes the results back to the agent. If found clean or if there is something to pass to the MTA, Bitdefender SMTP Proxy agent contacts the MTA on the new port this is configured to listen on, by default `10025`, and sends the email, as if coming from the original source. The whole filtering process is transparent to the Mail Transport Agent.

***Bitdefender y MTA en diferentes máquinas***
Bitdefender SMTP Proxy can be installed on one machine passing the scanned emails to the MTA, running on another machine. In this case, the MTA can listen on the default SMTP port, `25`, as usual.

## 2.2.6. Postfix

The Postfix integration agent is virtual: there is no specific Bitdefender component to perform the MTA integration. Instead, for Postfix you can use the general `SMTP Proxy` agent, adequately configured.




**Integración Postfix**

Briefly, the integration is made using the external, medium-weight, real-time Content Inspection method, as described in the original Postfix documentation. There are two Postfix processes running. The first one, listening on the standard SMTP port, receives all the incoming traffic and does the usual email filtering. The second one, listening on a higher port, by default `10026`, receives the email from the filter and sends it to the standard processing. In the middle, there is the Bitdefender Postfix

agent listening on another higher port, `10025` by default. It receives all the traffic passed from the first process, passes it to the Bitdefender core for scanning and finally sends the traffic to the second Postfix process.

# Pasos de la Instalación

# 3. Requisitos

Bitdefender Security for Mail Servers se puede instalar en basadas en paquetes distribuciones de Linux (rpm o deb) y versiones TBZ basadas en FreeBSD. Se soporta otras distribuciones utilizando el paquete de sistema ipkg, con la misma funcionalidad. Los paquetes incluyen todos los scripts necesarios para pre-instalación, post-instalación, pre-desinstalación y post-desinstalación. El tipo de paquete adecuado debe ser instalado de acuerdo con la distribución.

## 3.1. Requisitos del Sistema

Antes de instalar Bitdefender Security for Mail Servers, debe comprobar que su sistema cumple con los siguientes requisitos:

### 3.1.1. Requisitos de hardware

**Procesador**

x86 compatible, mínimo 800MHz, pero no espere un gran rendimiento en este caso. Un procesador de generación i686, a 1.4Ghz, sería una mejor opción.

**Memoria**

Mínimo aceptable 128MB (recomendado al menos 256MB para un mejor rendimiento).

**Espacio libre en disco**

El espacio mínimo libre en disco para instalar y ejecutar Bitdefender Security for Mail Servers es 60 MB. Pero el directorio de registro y la cuarentena necesita más espacio - 200MB de espacio libre.

**Conexión de Internet**

Bitdefender Security for Mail Servers se ejecutará sin conexión a Internet, el procedimiento de actualización requiere un enlace HTTP activo, aunque sea a través del servidor proxy. Por lo tanto la conexión a Internet es un REQUISITO para poner actualizar la protección.

### 3.1.2. Requisitos de software

**Requisitos Linux**

El kernel de Linux debe ser como mínimo 2.6.18.

Bitdefender requiere `glibc` versión 2.3.1, o posterior y, `libstdc++` de `gcc 4` o posterior.

Las distribuciones Linux soportadas son las siguientes:

- RedHat enterprise Linux 3 o posterior
- SuSE Linux Enterprise Server 9 o posterior
- Suse Linux 8.2 o posterior
- RedHat Linux 9
- Fedora Core 1 o posterior
- Debian GNU/Linux 3.1 o posterior
- Slackware 9.x o posterior
- Mandrake/Mandriva 9.1 o posterior
- Gentoo 1.4 o posterior

**Requisitos para FreeBSD:**

Las versiones soportadas de FreeBSD son 5.4-RELEASE o posterior.

Las versiones antiguas de FreeBSD ya no son soportadas.

### 3.1.3. Versiones mínimas requeridas de servidores de correo

**Sendmail**

versión 8.12.1, con interfaz Milter

**Postfix**

cualquier versión 2.x

**qmail**

mínimo versión 1.03

**Courier**

mínimo versión 0.42.x

**CommuniGate Pro**

mínimo versión 4.1.1

**SMTP**

cualquier servidor SMTP capaz de escuchar en otro puerto que el `25`

## 3.2. Convención de nombrado de paquetes

El paquete de Bitdefender Security for Mail Servers se denomina considerando el esquema siguiente:

### 3.2.1. Convención Linux

Los paquetes de Linux son nombrados de acuerdo con las siguientes reglas.

```
Bitdefender-Security-Mail-{ver}-{os}-{arch}.{pkg}.run
```

| Variable | Descripción |
|---|---|
| {ver} | Esta es la versión del paquete. Por ejemplo, 2.1-1 es la versión 2, subversión 1, construcción del paquete 1. |
| {os} | El sistema operativo es Linux, con compilador GCC 4.x. |
| {arch} | La arquitectura contiene un procesador clase. i586 y amd64 son las actuales versiones. |
| {pkg} | Esto representa el nombre del paquete de herramientas de administración. Es `rpm` para el Administrador de Red Hat, `deb` para Debian y `ipk` para IPKG. |

### 3.2.2. Convención FreeBSD

Hay dos paquetes de FreeBSD, a saber:

```
bitdefender-common-{ver}.tbz bitdefender-mail-{ver}.tbz
```

Esta es la versión *{ver}* del paquete. Por ejemplo, 2.1_1 es versión 2, subversión 1, construcción del paquete 1.

# 4. Instalación de paquetes

En este capítulo se explica cómo instalar Bitdefender en un sistema operativo tipo Unix como Linux o FreeBSD. Es bastante sencillo: obtener el paquete deseado, comprobar su integridad e instalarlo.

## 4.1. Obteniendo Bitdefender Security for Mail Servers

El paquete puede ser descargado desde los servidores de Bitdefender o se puede encontrar en medio de distribución diferentes, tales como CD-ROM. Cuando la descarga de los servidores de Bitdefender, se le pide que rellene un formulario y recibirá un correo electrónico en la dirección que he proporcionado en este formulario. El e-mail contiene la ubicación de descarga.

Los paquetes de Linux vienen en tres sabores:

- `rpm` para distribuciones que utilizan el administrador de paquetes de RedHat
- `deb` para distribuciones que utilizan el sistema de paquetes Debian Linux
- `ipk` para cualquier otra distribución que utilice IPKG (Itsy Package Management System)

Los paquetes de FreeBSD son `tbz` archivos comprimidos (.tar.bz), adecuados para FreeBSD desde la versión 5.

### 4.1.1. Repositorios de software de Bitdefender

Para hacer nuestros productos más accesibles, Bitdefender ofrece sus propios repositorios de software `deb` y `rpm`.

Para añadir el repositorio de Bitdefender en una distribución basada en Degbian, siga los siguientes pasos:

1. Añada la clave de repositorio de Bitdefender a la lista de las claves de confianza de **apt** ejecutando los siguientes comandos:

```
$ wget http://download.bitdefender.com/repos/deb/bd.key.asc
```

```
# apt-key add bd.key.asc
```

2. Añada la siguiente línea al archivo `/etc/apt/sources.list`:

```
deb http://download.bitdefender.com/repos/deb/ bitdefender  \ no
```

3. Refresque su caché **apt** ejecutando los siguientes comandos:

```
$ apt-get update
```

or

```
$ aptitud actualización
```

Para añadir el repositorio de Bitdefender a una distribución basada en RedHat, siga los siguientes pasos:

1. Install the Bitdefender-repo package:

```
$ rpm -i http://download.bitdefender.com/repos/rpm/    \ bitdefen
```

2. Actualice la caché de **yum**:

```
$ yum update
```

# 4.2. Instale el paquete

Hay un método común de instalación para `rpm`, `deb` y `ipk`, al igual que varios métodos para FreeBSD.

## 4.2.1. Instalar los paquetes de Linux

Los paquetes deben instalarse utilizando los siguientes comandos:

```
# sh Bitdefender-Security-Mail-{ver}-{os}-{arch}.{pkg}.run
```

Esto desempaquetar los paquetes de Bitdefender, según el tipo de paquete, e instalarlos usando el gestor de paquetes. Los paquetes contienen los archivos de Bitdefender (motores, núcleo, etc), instalar y desinstalar los scripts.

Veamos algunos ejemplos.

Para instalar Bitdefender Security for Mail Servers basada en una distribución RedHat tiene que ejecutar el siguiente comando:

```
# sh Bitdefender-Security-Mail-{ver}-{os}-{arch}.rpm.run
```

Si ha configurado su sistema para usar el repositorio de software de Bitdefender, puede instalar Bitdefender Security for Mail Servers con su yum preferido front-end **yum**. Por ejemplo:

```
# yum install Bitdefender-Mail
```

Para instalar Bitdefender Security for Mail Servers basada en una distribución Debian tiene que ejecutar el siguiente comando:

```
# sh Bitdefender-Security-Mail-{ver}-{os}-{arch}.deb.run
```

Si ha configurado su sistema para usar el repositorio de software de Bitdefender, puede instalar Bitdefender Security for Mail Servers con su yum preferido front-end **apt**. Por ejemplo:

```
# apt-get install bitdefender-mail
```

La versión `ipk` del archivo, instalará las herramientas **ipkg** en el sistema y las utilizará para instalar los paquetes `.ipk`.

Para instalar Bitdefender Security for Mail Servers en cualquier distribución Linux, usando **ipkg**, tiene que ejecutar el siguiente comando:

```
# sh Bitdefender-Security-Mail-{ver}-{os}-{arch}.ipk.run
```

## Parámetros adicionales

Para usuarios no tan impacientes, el archivo autoextraible proporciona algunos parámetros de línea de comandos, descritos en la siguiente tabla:

| Parámetro | Descripción |
|---|---|
| `--ayuda` | Imprime los mensajes de ayuda cortos. |
| `--información` | Esto imprimirá la información del archivo, como el título, el directorio objetivo por defecto, el script incrustado para ejecutarse tras el desempaquetado, el método de compresión utilizado, el tamaño descomprimido, la fecha de empaquetado. |
| `--lista` | Esta opción imprimirá el contenido del archivo incrustado. Los archivos listados son motores, binarios del programa, documentación incrustada, el script de instalación y desinstalación junto con su tamaño y sus permisos. |
| `--comprobar` | Esta es una de las opciones más útiles, porque permite al usuario verificar la integridad de los paquetes, como se ha dicho. La integridad se comprueba comparando el md5 checksum incrustado (generado durante el empaquetado) con uno calculado en el momento de la comprobación. El comando de salida será el siguiente:<br>`MD5 checksums are OK. All good.`<br>Si no, se mostrará un mensaje de error, mostrando los checksum almacenado y calculado no coincidentes, de la siguiente manera:<br>`Error in MD5 checksums: XY` |
| `--confirme` | Se le preguntará al usuario que confirme cada paso durante el proceso de instalación. |
| `--keep` | Por defecto, el contenido del archivo se extrae a un directorio temporal, que será eliminado después de salir del instalador. Añadiendo este parámetro al script, no se eliminará el directorio. |

| Parámetro | Descripción |
|---|---|
| `--Directorio` *Destino* | Puede especificar otro directorio para extraer el archivo, si no desea utilizar el nombre predeterminado. Tenga en cuenta que este directorio destino no será eliminado. |
| `--desinstalar` | Ejecute el script de desinstalación incrustado en lugar del instalador normal. |

## 4.2.2. Instala los paquetes de FreeBSD

Los paquetes deben instalarse utilizando los siguientes comandos:

```
# sh Bitdefender-Security-Mail-{ver}-{os}-{arch}.tbz.run
```

Esto desempaquetar los paquetes de Bitdefender, según el tipo de paquete, e instalarlos usando el gestor de paquetes. Los paquetes contienen los archivos de Bitdefender (motores, núcleo, etc), instalar y desinstalar los scripts.

### Parámetros adicionales

Para usuarios no tan impacientes, el archivo autoextraible proporciona algunos parámetros de línea de comandos, descritos en la siguiente tabla:

| Parámetro | Descripción |
|---|---|
| `--ayuda` | Imprime los mensajes de ayuda cortos. |
| `--información` | Esto imprimirá la información del archivo, como el título, el directorio objetivo por defecto, el script incrustado para ejecutarse tras el desempaquetado, el método de compresión utilizado, el tamaño descomprimido, la fecha de empaquetado. |
| `--lista` | Esta opción imprimirá el contenido del archivo incrustado. Los archivos listados son motores, binarios del programa, documentación incrustada, el script de instalación y desinstalación junto con su tamaño y sus permisos. |
| `--comprobar` | Esta es una de las opciones más útiles, porque permite al usuario verificar la integridad de los paquetes, como se ha dicho. La integridad se comprueba comparando el md5 checksum |

| Parámetro | Descripción |
|---|---|
| | incrustado (generado durante el empaquetado) con uno calculado en el momento de la comprobación. El comando de salida será el siguiente:<br>`MD5 checksums are OK. All good.`<br>Si no, se mostrará un mensaje de error, mostrando los checksum almacenado y calculado no coincidentes, de la siguiente manera:<br>`Error in MD5 checksums: XY` |
| `--confirme` | Se le preguntará al usuario que confirme cada paso durante el proceso de instalación. |
| `--keep` | Por defecto, el contenido del archivo se extrae a un directorio temporal, que será eliminado después de salir del instalador. Añadiendo este parámetro al script, no se eliminará el directorio. |
| `--Directorio` *Destino* | Puede especificar otro directorio para extraer el archivo, si no desea utilizar el nombre predeterminado. Tenga en cuenta que este directorio destino no será eliminado. |
| `--desinstalar` | Ejecute el script de desinstalación incrustado en lugar del instalador normal. |

## 4.2.3. Instala el paquete de idioma

Tiene la posibilidad de elegir el idioma a la hora de instalar. Los mensajes de ayuda, error, etc serán mostrados de acuerdo a su elección.

Para instalar el paquete de idioma en su equipo, debe ejecutar el siguiente comando:

```
# sh Bitdefender-Security-Mail-langpack-{ver}-{os}-\ {arch}.{pkg}.
```

Detecta automáticamente el idioma local del sistema a través de la variable de entorno LANG.

Los archivos de localización de idioma se almacenarán en el siguiente directorio: `/opt/Bitdefender/share/locale/[lang]/`.

Un enlace apuntando a `/opt/Bitdefender/share` se hará como `/usr/share/bitdefender`.

De todos modos, si está insatisfecho con el idioma elegido, puede configurar esta opción, estableciendo otro idioma. Esto puede hacerse ya sea cambiando el valor de la variable LANG o mediante el uso de una clave de configuración junto con herramienta **bdsafe**.

Este es el comando que debe ejecutar si decide utilizar la herramienta **bdsafe**.

```
# bdsafelang LL_CC.UTF-8
```

`LL` significa código de idioma `(ISO 639)` y `CC` para el código de país `(ISO 3166)`. Por ejemplo, si quiere establecer el idioma en Rumano, ejecute el siguiente comando:

```
# bdsafelang ro_RO.UTF-8
```

***Important***
Su terminal debe soportar la codificación **UTF-8**.

Si no instala el pack de idioma en primer lugar, puede instalarlo a través del gestor de paquetes en cualquier momento.

## 4.3. El instalador

Después de desempaquetar el archivo, se ejecutará el instalador. Es un instalador basado en texto, creado para ejecutarse en diferentes configuraciones. Su objetivo es instalar los paquetes extraídos de su ubicación y de hacer la primera configuración de Bitdefender Security for Mail Servers, mientras le pide algunas preguntas. Para aceptar la configuración predeterminada, el instalador ofrece (que es lo recomendado), pulse la tecla `ENTER` cuando se le solicite.

En primer lugar, el *Acuerdo de Licencia* en la pantalla. Le invitamos a leer el contenido completo pulsando el bar `ESPACIO` para ir a la página siguiente o `ENTER` para una línea cada vez. Para continuar el proceso de instalación, debe leer y aceptar este Acuerdo de licencia, por, literalmente, escribiendo la palabra `aceptar` cuando se le solicite. Si escribe cualquier otra cosa o nada, significará que usted no está de acuerdo con el Acuerdo de Licencia y el proceso de instalación se detendrá.

Después se le preguntará que agentes de integración desea instalar. Puede elegir uno o más de esta lista.

1. CommuniGate Pro
2. Courier
3. Postfix
4. qmail
5. Sendmail-Milter
6. SMTP Proxy - funciona con cualquier Agente de Transferencia de Correo

Please enter the corresponding numbers, when prompted, separated by empty spaces. For example, to install the integration agents for *Sendmail Milter* or *qmail*, enter `3` or `4`.

La siguiente cuestión se refiere a la característica RBL. Se le pedirá que especifique el servidor DNS y uno o más servidores RBL.

En este punto, el instalador ha adquirido toda la información necesaria y comenzará el proceso de instalación. Básicamente, instalará los motores, los binarios y la documentación y realizará la configuración post-instalación. Esta es una lista de sus acciones en su sistema Linux o FreeBSD:

- Crea el usuario y grupo `bitdefender` y le asigna el directorio de instalación.
- Instala las páginas de manual y configura la `RUTA MANUAL` de acuerdo a las mismas.
- Anexa la ruta a las librerías Bitdefender al fichero de configuración del cargador de librerías dinámicas.
- Crea un enlace simbólico al directorio de configuración en `/etc`.
- Integra Bitdefender en las secuencias de comando init del sistema.
- Bitdefender Security for Mail Servers está puesto en marcha.

# 5. Desinstalar

Si necesita desinstalar Bitdefender Security for Mail Servers, hay varios métodos para hacerlo, depende del tipo de paquete.

## 5.1. Desinstalar el paquete rpm

Para desinstalar Bitdefender Security for Mail Servers en una distribución basada en un gestor de paquetes `rpm`, debe ejecutar los siguientes comandos:

```
# rpm -e Bitdefender-mail # rpm -e Bitdefender-common
```

## 5.2. Desinstalar el paquete deb

Para desinstalar Bitdefender Security for Mail Servers utilizando **dpkg**, en una distribución basada en un gestor de paquetes `deb`, debe ejecutar los siguientes comandos:

```
# dpkg -r Bitdefender-mail # dpkg -r Bitdefender-common
```

```
# dpkg -r Bitdefender-antispam # dpkg -r Bitdefender-common
```

## 5.3. Desinstalar el paquete ipk

Para desinstalar Bitdefender Security for Mail Servers con **ipkg**, hay que ejecutar los siguientes comandos:

```
# ipkg-cl remove bitdefender-mail # ipkg-cl remove bitdefender-com
```

***Note***

El comando **ipkg** debe ejecutarse desde la siguiente ubicación: `/opt/ipkg/bin/`

## 5.4. Desinstalar el paquete tbz

Para desinstalar Bitdefender Security for Mail Servers también puede utilizar el comando **pkg_delete**, ejecutando los siguientes comandos:

```
# pkg_delete bitdefender-mail-{ver} # pkg_delete -r bitdefender-co
```

***Note***
Reemplace {ver} con la versión del paquete devuelta por el comando **pkg_info**.

O, utilizando **pkg_deinstall**, parte de sysutils/portupgrade, ejecute el siguiente comando:

```
# pkg_deinstall  bitdefender-mail  bitdefender-common
```

## Desinstalación alternativa

También puede desinstalar el producto de esta manera:

```
# Bitdefender-Security-Mail-{ver}-{os}-{arch}.{pkg}\ .run -- desin
```

# Iniciando

# 6. Iniciar y Apagar

Bitdefender Security for Mail Servers deben integrarse en los scripts de inicio del sistema, a fin de iniciar en la inicialización del sistema y parar en sistema cerrado. Una vez integrado, el servidor estará protegido todo el tiempo, ya que todos los servicios de Bitdefender estará listo y funcionando. Normalmente, no hay necesidad de que el usuario inicie manualmente o dejar de Bitdefender, pero hay tareas administrativas cuando dichas acciones sean necesarias. Normalmente, no hay necesidad de que el usuario inicie manualmente o dejar de Bitdefender, pero hay tareas administrativas cuando dichas acciones sean necesarias.

***El comando bd(8)***

El programa **bd(8)** incluido en los programas de Bitdefender, desempeña el papel de los guiones de inicio. Entre los muchos parámetros que apoya, no son el estándar `inicio`, `stop`, `reinicie`, con acciones obvias. La ubicación estándar del programa es `/opt/Bitdefender/bin/bd`, en el caso de una norma recta de avance de la instalación. Si selección un directorio de instalación diferente, por favor utilice la ruta correcta cuando llame a este programa.

**bd(8)** es enlazado simbólicamente, por el programa de instalación, al directorio de inicio específico del sistema, como `/etc/init.d/bd` (para scripts de inicio del sistema V type) o `/etc/rc.d/rc.bd` (para scripts de inicio del tipo BSD). Entonces, de acuerdo con su distribución, los siguientes comandos son idénticos, haciendo lo mismo de la misma manera. Por ejemplo, iniciarán Bitdefender.

```
# /opt/Bitdefender/bin/bd start
  - or -
# /etc/init.d/bd start
  - or -
# /etc/rc.d/rc.bd start
  - or -
# servicio bd start
```

Por conveniencia, en este documento siempre nos referimos al programa utilizando la primera forma, pero recuerde que puede utilizar todas las formas presentadas a continuación. Utilice la que mejor se ajuste a sus necesidades.

## 6.1. Inicio

Con el fin de iniciar Bitdefender Security for Mail Servers, tiene que ejecutar el siguiente comando (para formas alternativas, por favor, mire la nota anterior).

```
# /opt/Bitdefender/bin/bd start
```

El resultado será similar a la pantalla proporcionada como ejemplo a continuación. Tenga en cuenta que cuantos más componentes tenga instalados, habrá más lineas de salida correspondientes.

```
* Starting bdregd  ...                                  [ ok ]
* Starting bdlogd  ...                                  [ ok ]
* Starting bdscand  ...                                 [ ok ]
* Starting bdmaild  ...                                 [ ok ]
* Starting bdlived  ...                                 [ ok ]
* Starting bdmond  ...                                  [ ok ]
* Starting bdsmtpd  ...                                 [ ok ]
```

Por favor, espere a que se inicien todos los servicios. El script le devolverá al shell cuando todos los procesos se hayan iniciado. Si hay cualquier error mientras se inicializan, estos serán reportados.

## 6.2. Apagar

Con el fin de apagar Bitdefender Security for Mail Servers, tiene que ejecutar el siguiente comando (para formas alternativas, por favor mire la nota anterior).

```
# /opt/Bitdefender/bin/bd stop
```

La salida será similar a la siguiente pantalla, proporcionada como ejemplo. Tenga en cuenta que si tiene más componentes instalados y ejecutándose, habrá más lineas de salida correspondientes.

```
* Stopping bdsmtpd  ...                                 [ ok ]
* Stopping bdmond  ...                                  [ ok ]
* Stopping bdlived  ...                                 [ ok ]
* Stopping bdscand  ...                                 [ ok ]
```

```
* Stopping bdmaild  ...                                  [ ok ]
* Stopping bdlogd  ...                                   [ ok ]
* Stopping bdregd  ...                                   [ ok ]
```

Los procesos se apagaran en orden inverso al inicio. Por favor espere hasta que todos los servicios se detengan. El script le devolverá al shell cuando no haya más procesos en ejecución. Si hay algún error durante el apagado, serán reportados.

## 6.3. Reiniciar

Se puede realizar un simple reinicio de todos los servicios de Bitdefender ejecutando el siguiente comando (para formas alternativas, por favor consulte la nota anterior).

```
# /opt/Bitdefender/bin/bd restart
```

La salida es similar a las descritas anteriormente.

```
* Stopping bdsmtpd  ...                                  [ ok ]
* Stopping bdmond  ...                                   [ ok ]
* Stopping bdlived  ...                                  [ ok ]
* Stopping bdscand  ...                                  [ ok ]
* Stopping bdmaild  ...                                  [ ok ]
* Stopping bdlogd  ...                                   [ ok ]
* Stopping bdregd  ...                                   [ ok ]
* Starting bdregd  ...                                   [ ok ]
* Starting bdlogd  ...                                   [ ok ]
* Starting bdscand  ...                                  [ ok ]
* Starting bdmaild  ...                                  [ ok ]
* Starting bdlived  ...                                  [ ok ]
* Starting bdmond  ...                                   [ ok ]
* Starting bdsmtpd  ...                                  [ ok ]
```

Los procesos se apagaran en orden inverso, después se iniciarán. Por favor espere hasta que todos los servicios se detengan y se inicien. El script le devolverá al shell cuando se complete la acción. Si hay algún error en el apagado o inicio, serán reportados.

# 7. Estado de salida de Bitdefender

Puesto que todos sus componentes son daemons, Bitdefender funciona en segundo plano, con poca o ninguna salida incluso en absoluto. Una fuente de información sobre las acciones de Bitdefender son los registros, si está habilitado. Pueden obtenerse informes instantáneos en tiempo real utilizando las herramientas integradas de estado e informes estadísticos.

## 7.1. Estado del Proceso

Una breve descripción de todos los procesos en ejecución y sus process-id (PID) estará disponible ejecutando el siguiente comando.

```
# /opt/Bitdefender/bin/bd status
```

***La invocación del comando bd(8)***
Un breve debate sobre diferentes formas de los comandos de invocación **bd(8)** se pueden encontrar en Chapter 6 "*Iniciar y Apagar*" (p. 26).

***Salida en sistemas no NPTL***
En sistemas no NPTL, la salida es ligeramente diferente. En lugar de mostrar solamente un hilo, se muestran todos los PID de todos los hilos. Deberá ver las múltiples ID de proceso para hilos menores.

## 7.2. Información Básica

Utilizando la consola de texto, dispondrá de más información sobre el estado actual de Bitdefender con el siguiente comando:

```
# /opt/Bitdefender/bin/bd info
```

***La invocación del comando bd(8)***
Un breve debate sobre diferentes formas de los comandos de invocación **bd(8)** se pueden encontrar en Chapter 6 "*Iniciar y Apagar*" (p. 26).

***Registro de Bitdefender***
Debido a que esta información se almacena en el interior del Registro de Bitdefender, el daemon **bdregd** debe estar en ejecución para poder ver todo. Si no, solamente se mostrará una pequeña parte.

Se mostrará la siguiente información:

- La versión actual de Bitdefender Security for Mail Servers, junto con un poco de información del sistema.
- Estado de la cuarentena.
- Versión de los Componentes Centrales Agentes de Integración de BitDefender instalados.
- El número de firmas, cuando Bitdefender comprobó las actualizaciones de firmas de virus por última vez y cuando actualizó sus firmas.

## 7.3. Informe Estadístico

Los informes estadísticos sobre la actividad de Bitdefender, pueden obtenerse al ejecutar el siguiente comando:

```
# /opt/Bitdefender/bin/bd stats
```

***La invocación del comando bd(8)***
Un breve debate sobre diferentes formas de los comandos de invocación **bd(8)** se pueden encontrar en Chapter 6 “*Iniciar y Apagar*” (p. 26).

# 8. Integración MTA

After Bitdefender Security for Mail Servers has been installed, you have to integrate it in your Mail Transfer Agent. This means you have to redirect the email traffic through the Bitdefender integration agents, for each message to be scanned. To do so, use the bdsafe(8) command.

```
# bdsafe agent integrate [MTA]
```

Esto automáticamente integrará el agente de Bitdefender en la instalación de MTA. Deberá considerar activarlo utilizando el comando:

```
# bdsafe agent enable [MTA]
```

El Agente de Transferencia de Correo puede ser uno de los siguientes:

- cgate
- courier
- milter
- postfix
- qmail
- smtp

# 9. Configuración Básica

## 9.1. Ver Configuración

Después de haber instalado Bitdefender Security for Mail Servers puede ser una buena idea para comprender cómo funcionan las políticas de seguridad. La primera cosa a recordar es que las políticas de seguridad se aplican a grupos.

Por defecto, se trata de un único grupo, conocido como `Todos`, que contiene la lista completa de los usuarios, tanto de los remitentes y receptores. Al mismo tiempo, hay un grupo especial, el valor `predeterminado` de grupo, que especifica los valores implícitos, si no se especifica de otro modo en un grupo determinado.

***Note***
For detailed information about adding and editing groups, see Section 10.1.1 "*Añadiendo y Editando Grupos*" (p. 35)and, of course, the bdsafe(8) manual pages.

Naturalmente, la segunda cosa a realizar es ver la configuración de seguridad por defecto. Ejecute este comando como root.

```
# bdsafegroup configure Default
```

***Note***
For detailed information about the default settings, see Section 10.1.3 "*Configuración Predeterminada*" (p. 39).

## 9.2. Editar Configuración

Puede personalizar algunos grupos para cubrir sus necesidades, cambiando su configuración. De esta manera, la nueva configuración tendrá mayor prioridad sobre las predeterminadas. Por ejemplo, supongamos que desea agregar un grupo llamado `Secretario`. Ejecute este comando como root.

```
# bdsafegroup insert Secretary \ recipient:my_secretary@example.co
```

```
          #
```

```
bdsafe
group
priority
Secretary
4
```

***Note***

La prioridad del grupo será `4`. Para entender lo que la prioridad del grupo es todo esto, por favor vea el Section 10.1.4 "*Prioridad de Grupo*" (p. 44).

Y quiere que su secretaria nunca pierda un correo, incluso cuando parezca spam. El comando **bdsafe** para ignorar el spam para que el grupo `Secretario` es el siguiente.

```
# bdsafe group configure Secretary \ antispam actions ignore
```

O quizás quiera activar el filtro para caracteres asiáticos con el fin de cortar la cantidad de spam originada en el Este. Ejecute este comando como root.

```
# bdsafemail antispam charsets \ asian enable
```

Para comprobar el estado de la configuración del componente daemon de correo, ejecute esta línea.

```
# bdsafemail
```

***Note***

Para una descripción completa de la configuración de Bitdefender, debe consultar las páginas del manual.

# Modo Avanzado

# 10. Configuración

Una vez que Bitdefender Security for Mail Servers se ha instalado e integrado en el agente de transporte de correo, que funciona. Pero hay algunas configuraciones para afinar su instalación que a usted le debe interesar.

## 10.1. Administración de Grupos

El componente de administración de grupo de Bitdefender se utiliza para gestionar los usuarios y los ajustes como los grupos de una manera muy flexible. Puede integrarse con facilidad con cualquier aplicación que requiera esta característica. Le presentamos unos comandos introductorios. Para obtener información detallada, consulte las páginas de manual bdsafe(8).

### 10.1.1. Añadiendo y Editando Grupos

Los usuarios se definen en función de su dirección de correo electrónico, ya que son vistos por el servidor interno. Algunos usuarios definen un grupo. La parte buena es que puede especificar varias configuraciones para cada grupo, como acciones del antivirus, plantillas que se usarán para notificaciones, etc.

Hay dos grupos especiales: `Todos` y `defecto` El grupo `Todos` concentra la configuración para todos los usuarios, como se esperaba, y el grupo `defecto` especifica la configuración implícita, si no se definen en un determinado grupo.

Tendremos que crear un nuevo, añadir algunos usuarios y aplicar algunas configuraciones.

Primero, se ha de crear un nuevo grupo. Vamos nombre que `MiGrupo` y agregar un usuario identificado por su dirección de correo electrónico: `user1@domain.com`. Después podrá añadir más. Abra una terminal y ejecute el siguiente como root.

```
# bdsafegroup insert MyGroup sender:user1@example.com
```

Debemos aclarar algunas cosas, antes de proceder al siguiente paso. El comando **bdsafe** es el principal herramienta de configuración de Bitdefender. Sería bueno tener una mirada en la página del manual bdsafe(8), para tener una idea acerca de sus opciones y su uso.

En segundo lugar, el opción de `remitente` identificará los usuarios sólo como remitentes de correo electrónico. Si usted necesita para identificarlos como receptores, cambiar a los `beneficiarios`.

En este punto, podemos listar los grupos y usuarios para comprobar si los comandos previos funcionaron. He aquí el comando que debe ejecutar.

```
# bdsafegroup list MyGroup
```

Añadamos un usuario receptor.

```
# bdsafegroup insert MyGroup recipient:user2@example.com
```

Ahora, tenemos un grupo y algunos usuarios dentro del grupo. Vamos a cambiar las acciones antivirus para `desinfectar; cuarentena`. Tenemos que usar el mismo comando bdsafe(8). Tenga en cuenta el método utilizado para la cadena de escapar de la cáscara.

```
# bdsafe group configure MyGroup antivirus actionsonvirus \
   'disinfect;quarantine'
```

O, quizás, quiera modificar el umbral de spam para el mismo grupo.

```
# bdsafe group configure MyGroup antispam aggressivity 9
```

Utilice el grupo `Predeterminado`: por defecto, los pies de e-mail no suelen estar anexados. Este es el comando.

```
# bdsafegroup configure Default addfooters N
```

Siguiente, puede utilizar la característica de continuar correo, activando el envío del mensaje a otro receptor. Para esto, ejecute este comando como root.

```
# bdsafe group configure GROUP_NAME \ smtpforward smtpip [Direcció
```

Ocasionalmente, puede querer eliminar el grupo.

```
# bdsafegroup remove MyGroup
```

## 10.1.2. Integración con el servidor LDAP

El proceso de creación de los grupos pueden ser fácilmente simplificado al integrar la Bitdefender Security for Mail Servers con un servidor LDAP (Lightweight Directory Access Protocol). El comando **bdsafe**se puede utilizar para acceder y grupos de importación y de los usuarios del servidor LDAP.

Para acceder al servidor LDAP respectivo, debe seguir los siguientes pasos:

1. 
```
#

    bdsafe
    ldap
    configure
    server
    "ldap://example.test.ro:8000"
```

   Este comando establecerá la dirección del servidor LDAP respectivo. La argumento de `url` debe seguir la sintaxis: `ldap://server:port`.

2. 
```
# bdsafeldap configure basedn \ "ou=Test,ou=Test Team,dc=example
```

   Este comando establecerá el nivel más alto del árbol de directorio LDAP. El argumento reemplazable representa el distinguido nombre de la entrada LDAP (ver RFC 1779 - Una Representación de Cadena o Nombres Distinguidos para más detalles).

3. 
```
#

    bdsafe
    ldap
    configure
    user
```

```
"test\example1"
```

Este comando se utiliza para establecer el nombre de usuario de LDAP.

Para los servidores de Active Directory, el usuario también puede tener el sintaxis `domain\user`. Either quote user names or just escape the backslash.

4.

```
#

bdsafe
ldap
configure
passwd
set
```

Este comando se utiliza para establecer la contraseña de LDAP. Tras ejecutarlo, escriba la contraseña.

Para importar un grupo desde su respectivo servidor LDAP, debe seguir los siguientes pasos:

1.

```
#

bdsafe
ldap
group
list
```

Este comando se utiliza para mostrar todos los grupos LDAP.

2.

```
#
```

```
bdsafe
ldap
group
list
"Group_Name"
```

Se mostrarán los usuarios del grupo `Group_Name`.

3.

```
#

bdsafe
ldap
group
import
"Group_Name"
"senders"
```

El comando se utiliza para añadir automáticamente un grupo idéntico al del servidor LDAP. En los ejemplos, los miembros del grupo se añaden como remitentes. También pueden ser añadidos como receptores.

## 10.1.3. Configuración Predeterminada

Para ver la configuración de seguridad actual, ejecute este comando como root.

```
# bdsafegroup configure Default
```

La salida será similar a una de las siguientes.

```
Configuration for 'addfooters', group 'Default':
addfooters = 'Y'

Configuration for 'smtpforward', group 'Default':
```

```
enable   = 'N'
when     = 'BeforeScan'
smtphelo = ''
smtpfrom = ''
smtprcpt = ''
smtpip   = '127.0.0.1'
smtpport = ''

Configuration for 'antivirus', group 'Default':
enable               = 'Y'
addheaders           = 'Y'
headername           = 'X-BitDefender-Scanner'
actionsonriskware    = 'copy-to-quarantine;reject'
actionsonsuspected   = 'copy-to-quarantine;reject'
actionsonvirus       = 'copy-to-quarantine;reject'
pipeprogram          = ''
pipeprogramarguments = ''

Configuration for 'antispam', group 'Default':
enable               = 'Y'
addheaders           = 'Y'
modifysubject        = 'Y'
aggressivity         = '0'
actions              = 'move-to-quarantine'
whitelist            = '/opt/BitDefender/etc/as_wlist'
blacklist            = '/opt/BitDefender/etc/as_blist'
headername           = 'X-BitDefender-Spam'
stampheadername      = 'X-BitDefender-SpamStamp'
headertemplateham    = '/opt/BitDefender/share/templates/ham.tpl'
headertemplatespam   = '/opt/BitDefender/share/templates/spam.tpl'
subjecttemplate      = '/opt/BitDefender/share/templates/subject.tpl'
usebwfilter          = 'Y'
usebayesfilter       = 'Y'
useheurfilter        = 'Y'
useimgfilter         = 'Y'
usemultifilter       = 'Y'
usepbayesfilter      = 'Y'
userblfilter         = 'Y'
useurlfilter         = 'Y'
usesignfilter        = 'Y'
pipeprogram          = ''
pipeprogramarguments = ''
```

```
Configuration for 'contentfilter', group 'Default':
enable         = 'Y'
rules          = '/opt/BitDefender/etc/cf/Default-cf.conf'
maxrules       = '1000'
administrator  = ''
smtpserver     = ''
```

Cada configuración se explica en la siguiente tabla.

| *Configuración* | *Valor* |
|---|---|
| AddFooters | Y si está habilitada, N si está desactivado. Añade un nuevo pie a todos los correos o no. |
| SmtpForward/Enable | Y si reenvía correos a otro servidor de correo, N si el reenvío SMTP está desactivado. |
| SmtpForward/When | Muestra si los mensajes de correo van a ser reenviados a otro servidor de correo antes o después del análisis. |
| SmtpForward/SMTP_HELO | Muestra el protocolo de comandos del otro servidor de correo HELO. |
| SmtpForward/SMTP_FROM | Muestra el protocolo de comandos CORREO DE del otro servidor de correo. |
| SmtpForward/SMTP_RCPT_TO | Muestra el protocolo de comandos RCPT TO del otro servidor de correo. |
| SmtpForward/SMTP_IP | Muestra la dirección IP del otro servidor de correo. |
| SmtpForward/SMTP_PORT | Muestra el puerto del otro servidor de correo. |
| SmtpForward/Activar | Y si el módulo antivirus está activado, N si está desactivado. |
| Antivirus/AddHeaders | Y si está habilitada, N si está desactivado. Añade un nuevo encabezado a todos los correos o no. |

| *Configuración* | *Valor* |
|---|---|
| Antivirus/HeaderName | Muestra el encabezado del antivirus predeterminado. |
| Antivirus/ActionsOnRiskware | Lista las acciones a realizar cuando se encuentra un mensaje de riesgo. |
| Antivirus/ActionsOnSuspected | Lista las acciones a realizar cuando se encuentra un mensaje sospechoso. |
| Antivirus/ActionsOnVirus | Lista las acciones a realizar cuando se encuentra un mensaje infectado con virus. |
| Antivirus/PipeProgram | Muestra la ruta completa al programa para canalizar el correo. |
| Antivirus/PipeProgramArguments | Muestra el argumento correspondiente al programa pipe acepta. |
| Antispam/Enable | Y si el módulo antispam está activado, N si el módulo antispam está desactivado. |
| Antispam/AddHeaders | Y si está habilitada, N si está desactivado. Añade un nuevo encabezado a todos los correos o no. |
| Antispam/ModifySubject | Y si está habilitada, N si está desactivado. Specifies whether the subject of the email message should be modified conforming to the Subject template field or not. |
| Antispam/Aggressivity | Configura la nivel de agresividad antispam. Escala va de 0 (confianza mínima en la puntuación antispam devuelto por los filtros de Bitdefender hasta 9 (máxima confianza). |
| Antispam/Actions | Lista las acciones a realizar cuando se encuentra un mensaje de spam. |
| Antispam/Lista blanca | Muestra la ruta al archivo de configuración de la lista blanca. |

| *Configuración* | *Valor* |
|---|---|
| Antispam/BlackList | Muestra la ruta al archivo de configuración de la lista negra. |
| Antispam/StampHeaderName | Muestra el encabezado predeterminado de spam. |
| Antispam/HeaderTemplateHam | Muestra la ruta al archivo de plantilla del encabezado ham. |
| Antispam/HeaderTemplateSpam | Muestra la ruta al archivo de plantilla del encabezado spam. |
| Antispam/SubjectTemplate | Muestra la ruta al archivo de plantilla del asunto. |
| Antispam/Engines/UseBWFilter | Y si el filtro de lista negra/blanca del antispam está activado, N si está desactivado. |
| Antispam/Engines/UseBayesFilter | Y si el filtro Bayesiano antispam está activado, N si está desactivado. |
| Antispam/Engines/UseHeurFilter | Y si el filtro heurístico antispam está activado, N si está desactivado. |
| Antispam/Engines/UseIMGFilter | Y si el filtro de imágenes antispam está activado, N si está desactivado. |
| Antispam/Engines/UseMultiFilter | Y si el multi-filtro antispam está activado, N si está desactivado. |
| Antispam/Engines/UsePBayesFilter | Y si el filtro antispam Bayesiano pre-entrenado está activado, N si está desactivado. |
| Antispam/Engines/UseRblFilter | Y si el filtro antispam RBL (Real-time Blackhole List) está activado, N si está desactivado. |
| Antispam/Engines/UseURLFilter | Y si el filtro URL antispam está activado, N si está desactivado. |
| Antispam/Motores/UseURLFilter | Y si el filtro de firmas antispam está activado, N si está desactivado. |

| Configuración | Valor |
|---|---|
| Antispam/PipeProgram | Muestra la ruta completa al programa para canalizar el correo. |
| Antispam/PipeProgramArguments | Muestra el argumento correspondiente al programa pipe acepta. |
| ContentFilter/Activar | Y si el filtrado de contenido está activado, N si está desactivado. |
| ContentFilter/Reglas | Muestra la ubicación del archivo de configuración del filtrado de contenido. |
| ContentFilter/MaxRules | Muestra el máximo número de reglas que pueden cargarse desde el archivo de configuración del filtrado de contenido. |
| ContentFilter/Administrador | Muestra el usuario sea notificado acerca de bloquear o permitir mensajes de correo electrónico basados en el análisis de su contenido. |
| ContentFilter/SMTPServer | Muestra el nombre del host y el puerto en caso de que quiera reenviar correos basados en el análisis de su contenido a otro servidor de correo. |

La configuración de seguridad predeterminada se aplica al grupo Todos y a cualquier nuevo grupo.

## 10.1.4. Prioridad de Grupo

El atributo de prioridad de grupo, cuando se utiliza correctamente, puede ser un instrumento muy útil. Al mismo tiempo, si no se entiende completamente, puede causar algunas incidencias.

Veamos un ejemplo. Spongamos que ha creado siete grupos: Marketin, HR, Secretario, Administrador, Técnico, Finanzas, Dangerous Además de estos grupos, recuerda que ya están lidiando con el grupo Todos, que contiene la lista completa de los usuarios, tanto de los remitentes y receptores, y un grupo especial, el defecto una.

Para cada grupo configura algunas opciones personalizadas: una política antispam relajada para los grupos `Secretaria`, `Admin` y `Marketing` y una más agresiva para los grupos `RH`, `Finanzas` y `Técnico`. Además, necesitará una colección de virus y mensajes de spam para sus test de seguridad y establecer Bitdefender para ignorar el malware y los mensajes ilícitos para el grupo `Peligroso`.

Cada grupo es creado con una prioridad específica. Por ejemplo, el grupo `Secretario` fue creado con prioridad `4`.

***Note***

Recuerde que el grupo `Todos` tiene por defecto la prioridad `1` (la prioridad más alta).

En aras de la discusión, supongamos que la situación de la prioridad de grupo es la siguiente.

| *Grupo* | *Prioridad* |
|---|---|
| `Todos` | 1 |
| `Dangerous` | 2 |
| `Marketing` | 3 |
| `Secretaria` | 4 |
| `Admin` | 5 |
| `HR` | 6 |
| `Técnica` | 7 |
| `Finanzas` | 8 |

En este caso, la primera política de seguridad a aplicar será la correspondiente al grupo `Todos`, pongamos una que desinfecte virus y borre los mensajes de spam. La segunda, que debe aplicarse es la política que corresponde a el grupo `Dangerous`, etc.

¿Que opina sobre sus mensajes de spam y su colección de archivos infectados con virus? Usted recibirá casi nada, porque el directiva de grupo `Todos` se aplica en primer lugar.

Para cambiar esta situación, usted tiene que fijar el `1` prioridad para el grupo`Dangerous`. Para esto, ejecute este comando como root.

```
# bdsafegroup priority Dangerous 1
```

El orden de prioridad de los grupos será el siguiente.

| Grupo | Prioridad |
|---|---|
| Dangerous | 1 |
| Todos | 2 |
| Marketing | 3 |
| Secretaria | 4 |
| Admin | 5 |
| HR | 6 |
| Técnica | 7 |
| Finanzas | 8 |

Naturalmente, sería una buena idea cambiar la prioridad del grupo `Todos` a `8`, para no comprometer las otras políticas de seguridad. Ejecute este comando como root.

```
# bdsafegroup priority All 8
```

El orden de prioridad de los grupos será el siguiente.

| Grupo | Prioridad |
|---|---|
| Dangerous | 1 |
| Marketing | 2 |
| Secretaria | 3 |
| Admin | 4 |
| HR | 5 |
| Técnica | 6 |
| Finanzas | 7 |
| Todos | 8 |

Tenga en cuenta que es lógico que los grupos `Marketing, Secretaria` y `Admin`, con una política de seguridad antispam relajada, tengan prioridad sobre los grupos `RH, Técnico` y `Finanzas`, con una política más agresiva.

***Más de las páginas del manual***
Como los anteriores, estos son simples ejemplos. Por favor vea las páginas del manual bdsafe(8) para obtener información detallada.

## 10.2. Configuración Antivirus

Bitdefender antivirus detecta no sólo virus, sino también otras aplicaciones potencialmente maliciosas como software de riesgo (programas que pueden ser ejecutados o mal utilizados por otros ejemplares de malware) y los archivos sospechosos de contener malware (posible; por lo general son presentados al laboratorio para su posterior análisis AV).

Puede personalizar su configuración antimalware. Mediante el uso de comando **bdsafe**, puede elegir las acciones a realizar en cada tipo de malware.

- accionesenvirus
- accionesenriskware
- accionesensospechosos

Por ejemplo, si desea eliminar (o mover a la cuarentena, cuando no se puede eliminar) cada objeto sospechoso, ejecute esta línea como root.

```
# bdsafe group configure GROUP_NAME \ antivirus actionsonsuspected
```

***Orden de acciones***
No todas las acciones están disponible en cualquier orden; por ejemplo, no puede establecer como primera acción Eliminar y como segunda Desinfectar: ¡No tiene sentido!

Ahora, veamos la lista completa de posibles acciones.

**Desinfectar**

Para eliminar el malware de un adjunto infectado (o cualquier otro componente en un correo que pueda ser utilizado para enviar malware). Si tiene éxito, el correo pasa al siguiente plugin (si lo hubiera) o se reenvía. De otro modo, se ejecutará la siguiente acción.

**Eliminar**

Para eliminar un adjunto u otro componente del correo que contenga malware. Si tiene éxito, el correo pasa al siguiente plugin (si lo hubiera) o se reenvía. De otro modo, se ejecutará la siguiente acción.

Cuando el correo se elimina completamente, se generará un reemplazo para hacer conocer al destinatario que ha ocurrido.

**Mover a cuarentena**

Para mover el correo a la cuarentena. Si la acción falla, se escribirá un mensaje de error en el registro.

Tras ejecutarse esta acción, el correo será eliminado (la acción predeterminada) o rechazado.

**Copiar a cuarentena**

Para copiar el correo a la cuarentena. Si la acción falla, se escribirá un mensaje de error en el registro.

**Eliminar (acción predeterminada)**

Envíe el mensaje al agente de transporte de correo (MTA) para dejar el correo. Esta es la acción predeterminada. Por lo tanto, la acción final siempre será **Drop**, a menos que decida lo contrario.

Esta acción prohíbe el paso del correo. MTA no devolverá ninguna respuesta al remitente.

**Rechazar**

Para enviar el mensaje al agente de transporte de correo (MTA) para rechazar el correo.

Esta acción prohíbe el paso del correo. Sin embargo, MTA devolverá un mensaje de rechazo.

**Omitir**

Para enviar el mensaje al agente de transporte de correo (MTA) para reenviar el correo.

**Pipe to programa**

Para el tubo electrónico a un programa determinado.

***Utilizando la línea de comandos***

Todas estas acciones también se pueden configurar mediante la herramienta **bdsafe**. Para una descripción completa de la configuración, debe consultar las páginas del manual bdsafe(8).

Por ejemplo, para todos los tubos riskwares al programa **submit.sh**, ejecute el siguiente comando como root.

```
# bdsafe group configure GROUP_NAME \ antivirus actionsonrisk
```

## 10.3. Configuración Antispam

Bitdefender Antispam emplea sorprendentes innovaciones tecnológicas y filtros antispam estándares en la industria para impedir que el spam llegue a su bandeja de entrada.

En nuestro campo, interpretación o ejecución, las altas tasas de detección y muy pocos “positivos falsos”. Para alcanzar esta meta, hemos empaquetado conjuntamente potentes filtros antispam. Estos son los filtros antispam en orden de paso.

**Filtro Multipropósito**

El filtro Multipropósito, es un nombre genérico para GTUBE (un test antispam) y dos filtros especializados: el filtro Charset y el filtro de Sexualidad explícita.

GTUBE, el Test Genérico para Correo Masivo no Solicitado, es un test antispam similar al test antivirus EICAR. El test consiste en introducir una cadena especial de 68-byte en el cuerpo del mensaje de un e-mail con el fin de ser detectado como spam. Su rol es comprobar la funcionalidad del producto para ver si los filtros están correctamente instalados y detectan el spam entrante.

El filtro Charset puede ser instruido para detectar mensajes escritos en otros idiomas (por ejemplo idiomas asiáticos o Cirílico) y marcarlos como spam. Esto es útil cuando el usuario está seguro de que no va a recibir correo en estos idiomas.

La ley exige que todos los estadounidenses anuncio sexualmente explícito e-mails serán marcados como tales, con “sexualmente explícito” en su materia. El filtro Sexualmente explícito puede detectar y marcar estos mensajes como spam directamente.

***Note***

GTUBE es el primer filtro en entrar en acción, mientras que los filtros especializados van tras el filtro de lista negra / lista blanca.

**Filtro de lista Negra / lista Blanca**

El filtro de lista negra / lista blanca puede ser muy útil cuando el usuario quiere bloquear mensajes entrantes de un remitente concreto (lista negra), o cuando el usuario quiere asegurarse de que todos los mensajes de una migo o newsletter llegan a su buzón, sea cual sea su contenido. El filtro de la lista de negro/lista

blanca se llama a menudo “Lista Amigos/Spammers”. Se puede definir listas de *permitir* o *niegan* tanto para individuales de correo electrónico, o los nombres de dominio completos (por ejemplo, todo el correo desde cualquier empleado de bigcorporation.com).

***Añadir amigos a la lista blanca***
Le recomendamos agregar los nombres y las direcciones de correo de sus amigos al Lista blanca. Bitdefenderno bloquea los mensajes provenientes de este listado; de esta manera, al agregar amigos se asegura que los mensajes legítimos llegarán a su bandeja de entrada.

Las dos listas son archivos de texto plano, conteniendo una entrada por línea. You can find these text files (`as_wlist` and `as_blist`) in this location: `/opt/BitDefender/etc` The entries may be usual email addresses or domain names, respecting the following format.

| *Formato* | *Descripción* |
|---|---|
| `user@domain.com` | Este formato solo coincidirá con el usuario especificado del dominio especificado. |
| `user@domain.*` | El usuario mencionado de cualquier dominio cuyo nombre comience por el texto especificado, coincidirá. |
| `user@*.com` | El usuario de cualquier dominio con un sufijo `.com` (por ejemplo) coincidirá. |
| `*@domain.com` | Esto hará coincidir a todos los usuarios del dominio especificado. |
| `*@domain.*` | Todos los usuarios de todos los dominios comenzando con el texto mencionado, coincidirán. |
| `*.com` | Esto hará coincidir a todos los usuarios de cualquier dominio con el sufijo `.com` (por ejemplo). |
| `user@*` | El usuario especificado, de cualquier dominio, coincidirá. |
| `user*` | Esto hará coincidir a todos los usuarios cuyos nombres comiencen por el texto mencionado, no importa el dominio. |

***Important***
Los cambios no se harán efectivos hasta que reinicie Bitdefender

**Filtro RBL**

RBL es sinónimo de lista “tiempo real Negro” o “Lista Blackhole tiempo real” La aplicación de Bitdefender utiliza el protocolo DNSBL y servidores RBL para filtrar el spam basado en la reputación del servidor de correo remitente como spam.

La dirección del servidor de correo se extrae del encabezado del correo y se comprueba para su validación. Si la dirección pertenece a una clase privada (`10.0.0.0/8` o `192.168.0.0/16`) o no es relevante, será ignorado.

La comprobación DNS se realiza en el dominio `d.c.b.a.rbl.ejemplo.com`, donde `d.c.b.a` es la dirección IP del servidor invertida y `rbl.ejemplo.com` es el servidor RBL. Si la DNS responde que el dominio es válido, significa que la IP está listada en el servidor RBL y que se ha proporcionado una puntuación de servidor. Esta puntuación puede tener valores desde`0` a `100`, de acuerdo con la confianza del servidor (nivel de confianza), la cual es libre de configurar.

Se consultarán todos los servidores RBL introducidos en la lista y se determinará una puntuación media a partir de la puntuación obtenida en cada uno de ellos. Al alcanzar `100`, hay más consultas se realizan.

Finalmente, se calcula una puntuación spam desde las puntuaciones de los servidores RBL y se añade a la puntuación spam global del e-mail.

Puede configurar con facilidad los servidores de nombres RBL desde el daemon de Correo, ejecutando este comando.

```
# bdsafe mail antispam rbl nameservers [add|remove] [host]
```

También puede configurar los servidores RBL para el daemon de Correo, ejecutando el siguiente comando.

```
# bdsafe mail antispam rbl servers [add|remove] host:[weight]
```

El valor para el parámetro `weight` puede oscilar entre `0` (nivel de confianza mínimo) y `100` (nivel de confianza máximo).

**Filtro de Imágenes**

Algunos mensajes incluyen imágenes adjuntas, disponemos del filtro de imágenes para detectarlas y compararlas con una base de datos de imágenes de spam conocidas, la cual es mantenida y actualizada por nuestro laboratorio.

El nuevo filtro de imágenes combina técnicas antiguas de CBIR (Content Based Image Retrieval) con un nuevo filtro especialmente diseñado para las imágenes

llamado SID (Spam Image Distance). También aprende histogramas (gráficos que muestran el número de píxeles de cada color dentro de una imagen o área) de las imágenes spam y las identifica rápidamente para el usuario. El filtro de Imágenes se entrena en los Laboratorios BitDefender y se actualiza varias veces al día para conseguir un ratio de detección sumamente preciso.

Para obtener más información sobre el filtro de imágenes, consulte el libro blanco Fighting Image Spam.

**Filtro URL**

Casi todo el spam enlaza a un sitio web: si quieren que compremos un Rolex barato o introduzcamos nuestro usuario y contraseña para una web falsa de un banco, ellos tienen un enalce. El filtro URL detecta estos enlaces y los comprueba en una base de datos creada y mantenida (con actualizaciones) por nuestro laboratorio. Si un mensaje de enlaces a un sitio “prohibido”, las probabilidades son altas de que es spam.

**Filtro Bayesiano**

Sabemos que no todos nuestros usuarios estarán de acuerdo con nosotros al calificar un mensaje como spam o legítimo. Por ejemplo, un doctor hablando sobre Viagra con sus pacientes, seguramente necesite personalizar sus filtros. Esta es la razón por la que hemos añadido el filtro Bayesiano.

Cada usuario puede *entrenar* que con el ejemplo, y hacerlo saber qué mensajes son spam y los mensajes son de fiar (a partir de ejemplos concretos en el buzón del usuario). Tras el suficientes aprendizaje, el filtro Bayesiano se adapta a los mensajes legítimos y spam que el usuario recibe normalmente y se convierte en un potente factor en el proceso de decisión.

Puede entrenar el filtro bayesiano con ejemplos de spam, ejecutando el siguiente comando.

```
# bdsafe bayes spam [file1] [file2] [dir1] [dir2]
```

Veamos un ejemplo.

```
# bdsafe bayes spam /home/test/viagra.eml /home/test/porn
```

Puede entrenar con facilidad el filtro bayesiano con ejemplos, ejecutando el siguiente comando.

```
# bdsafe bayes ham [file1] [file2] [dir1] [dir2]
```

Puede crear una copia de seguridad del diccionario del filtro bayesiano, ejecutando el siguiente comando.

```
# bdsafe bayes backup [directory]
```

Para restaurar el diccionario del filtro bayesiano, ejecute el siguiente comando.

```
# bdsafe bayes restore [directory]
```

Para restablecer el diccionario del filtro bayesiano, ejecute el siguiente comando.

```
# bdsafe bayes reset [noask]
```

El parámetro `noask` se utiliza para evitar que **bdsafe** nos pida confirmación.

**Filtro Bayesiano Pre-entrenado**

Mientras que el filtro Bayesiano es entrenado por el usuario, este filtro es pre-entrenado por los Laboratorios Antispam de Bitdefender y actualizado periódicamente.

Puede ayudar a mejorar el filtro pre-entrenado enviando mensajes spam a nuestros Laboratorios Antispam. El proceso de envío funciona de la siguiente manera:

1. A spam e-mail is delivered to a user
2. The user forwards the e-mail as an attachment to a predefined POP3 e-mail account that Bitdefender periodically checks
3. Bitdefender recupera el e-mail y lo añade al diccionario Bayesiano

***Important***
Los e-mails recuperados por Bitdefender se borrarán del buzón de entrada.

Para configurar los envíos de spam, tiene que editar el registro de Bitdefender. Siga estos pasos:

1. Activar/desactivar el módulo de envío ejecutando el siguiente comando:

```
# bdsaferegistry setkey \ $BDMLD/SpamSubmit/Enable Y/N
```

2. Establezca el host POP3:

```
# bdsaferegistry setkey  $BDMLD/SpamSubmit/Host [host_address
```

3. Activar/desactivar cifrado SSL:

```
#
    bdsafe
    registry
    setkey
    $BDMLD/SpamSubmit/UseSSL Y/N
```

4. Si es necesario, escriba los nombres de usuario de las cuentas de POP3 para que el spam y ham se envían:

```
# bdsaferegistry setkey \ $BDMLD/SpamSubmit/SpamUser [user_na
```

```
# bdsaferegistry setkey \ $BDMLD/SpamSubmit/HamUser [user_nam
```

5. Introduzca las contraseñas para las cuentas POP3 (si se requiere):

```
# bdsaferegistry setkey \ $BDMLD/SpamSubmit/SpamPass [passwor
```

```
# bdsaferegistry setkey \ $BDMLD/SpamSubmit/HamPass [password
```

6. Establezca el intervalo de tiempo en que Bitdefender comprobará la cuenta de e-mail:

```
# bdsaferegistry setkey \ $BDMLD/SpamSubmit/Timeout [seconds]
```

***Important***
Los mensajes de spam deben ser reenviados como adjuntos a e-mail que no excedan los 8MB.

**Filtro NeuNet**

Cuando creamos reglas de detección, nuestros analistas antispam consideran que mensajes de spam tenemos disponibles. Aunque hay millones de ellos, es imposible considerar cada uno a fondo. Es la razón por la que hemos creado un potente filtro utilizando una Red Neuronal (un concepto tomado prestado del campo de la inteligencia artificial).

La característica más importante de la red Neural (NeuNet) es que tenemos *entrenado* en los laboratorios de Antispam, que le permite ver una gran cantidad de mensajes de spam. Al igual que un niño en la escuela, se ha *aprendido* para distinguir entre el spam y los correos electrónicos de fiar, y su formidable ventaja es que se puede reconocer el spam nueva percepción de similitudes (a menudo muy sutil) entre los mensajes que ha aprendido. Este enfoque (tanto reactivo como *proactivo*) es similar a la heurística utilizada por los productos antivirus.

Una vez instalado Bitdefender Security for Mail Servers todos estos filtros antispam están habilitados. Por supuesto, usted puede configurar el número deseado de filtros activos, utilizando el comando**bdsafe**. Por ejemplo, para activar/desactivar el filtro de imagen, ejecute la línea siguiente como root.

```
# bdsafegroup configure \ MyGroup antispam useimgfilter [value]
```

***Note***
El nuevo valor puede ser `Y`, para habilitar el filtro, o `N`, para desactivarlo.

Para una descripción completa de la configuración de antispam, debe consultar las páginas del manual bdsafe(8).

### 10.3.1. X-Junk-Score de cabecera para la integración CommuniGate Pro

Cuando se integra con CommuniGate Pro, Bitdefender puede agregar el encabezado X-Junk-Score para filtrar e-mails. CommuniGate Pro utiliza el valor de la cabecera X-Junk-Score para llevar a cabo determinadas acciones en los tratados e-mails

***Note***
Para obtener más información acerca del encabezado X-Junk-Score, por favor consulte la documentación CommuniGate Pro.

Para habilitar la cabecera X-Junk-Score, ejecute el comando siguiente:

```
#
    bdsafe
    group
    configure
    GROUP_NAME
    antispam
    cgatecompat Y
```

Para aplicar los cambios de configuración, ejecute el comando siguiente:

```
# bdsafereloadsettings
```

## 10.4. Filtro de Contenido

A veces sólo necesita bloquear o permitir mensajes de correo electrónico basado en el análisis de su contenido, en lugar de otros criterios. Bitdefender ofrece soporte para este tipo de operaciones.

Para crear, modificar o eliminar las reglas de filtrado de contenidos que tiene que ejecutar uno de los comandos siguientes bdsafe.

```
# bdsafe group configure GROUP_NAME contentfilter add \ {priority}
```

| Argument | Valor |
|---|---|
| tipo | encabezado, cuerpo, nombre-apego, tipo de apego, tamaño de apego, mailsize |
| condición | existe, !existe!, partido, partido, mayor que, !mayor que! |
| valor | un número positivo (de bytes), una expresión regular |
| acción | ignorar, sueltar, rechazar, reemplazar, copia a la cuarentena, mover a cuarentena |
| suscripción | ninguno, administrador, administrador, remitente, destinatarios |

El comando anterior agrega una regla de contenido nuevo filtro.

```
# bdsafe group configure GROUP_NAME contentfilter modify \ {rule_p
```

| Argument | Valor |
|---|---|
| field_name | prioridad, habilitado, nombre, tipo, header_name, condición, valor, acción, notificar |

El comando anterior modifica una regla, campo por campo.

```
# bdsafe group configure GROUP_NAME contentfilter dump \ {rule_pri
```

El comando anterior muestra todas las reglas existentes para el grupo especificado. Si añade un número como argumento que la regla con la prioridad número se mostrará solamente.

```
# bdsafe group configure GROUP_NAME contentfilter delete \ {rule_p
```

El comando anterior borra la regla con la prioridad número especificado.

```
# bdsafe group configure GROUP_NAME contentfilter enable \ {boolea
```

El comando anterior activa/desactiva el filtrado de contenido para un grupo determinado. Si añade un número como argumento que la regla con la prioridad número se activa/desactiva solamente.

```
# bdsafe group configure GROUP_NAME contentfilter priority \ {old_
```

El comando anterior cambia la prioridad de una regla determinada.

```
# bdsafe group configure GROUP_NAME contentfilter rules \ {path_to_
```

El comando anterior muestra el contenido del grupo de configuración de filtro ubicación del archivo. Si agrega un argumento `path_to_file`, el comando establece el archivo de contenido del grupo de configuración del filtro a la ubicación especificada.

```
# bdsafe group configure GROUP_NAME contentfilter maxrules \ {numb
```

El siguiente comando, establece el máximo número de reglas que pueden ser cargadas desde el archivo de configuración del filtro de contenido del grupo.

```
# bdsafe group configure GROUP_NAME \ contentfilter htmldisarm Y
```

El commmand anterior permite desarmar el código HTML de función para un grupo. Esta característica está diseñada para eliminar el código potencialmente malicioso como JavaScript o Visual Basic de e-mails con contenido HTML.

## 10.4.1. Ejemplos

Veamos algunos ejemplos para ilustrar lo que ofrece el potente filtro de contenido.

1. 
```
# bdsafe group configure GROUP_NAME \ contentfilter add 0 MyRule
```

   Esto agregará la regla del filtro de contenido, el nombre `MiRegla` con prioridad `0` (la más importante) a GROUP_NAME. La regla dice: cuando la palabra `porno` se encuentra dentro de la parte de sujeción de la cabecera, el correo respectivo será dado de baja y nadie será notificado.

2. `# bdsafe group configure GROUP_NAME \ contentfilter add 1 Salari`

Esto agregará la regla del filtro de contenido, el nombre `Salario` con `1` prioridad a GROUP_NAME. Cuando se aplica esta regla significa que los correos electrónicos que contienen en sus palabras del cuerpo como `salary, salaries, salarry, salariess, salariu` se abandonarse y el administrador será notificado.

La lección a aprender es la siguiente: si es un deber que los e-mails que contengan información sensible (como datos salariales, informes salariales personales) sean filtrados en consecuencia, simplemente establezca una regla para ellos. Sería una buena idea el utilizar expresiones regulares. La siguiente tabla puede proporcionarle algunos ejemplos.

| *Ejemplo* | *Descripción* |
|---|---|
| `Honou?r` | Usted puede usar esto para coincidir con `Honor` o `Honour`. El signo de interrogación hace que la señal anterior en la expresión regular opcional. |
| `Dr[iau]nk` | Usted puede usar esto para coincidir con `Drink` o `Drank` o `Drunk`. Mediante el uso de este tipo de expresión regular (clase de caracteres) a uno de varios personajes será igualada solamente. |
| `[0-9]\sMAR\s200[5-8]` | Usted puede usar esto para igualar `5 MAR 2005` o `3 MAR 2008` o `9 MAR 2007` y así sucesivamente. Mediante el uso de un guión en el interior de una clase de caracteres uno fuera de un rango especificado de caracteres será igualada solamente. El señal `\s` coincidirá con un espacio. |
| `Is+ues*` | Usted puede usar esto para igualar `Isue` o `Issue` o `Issues` o `Issssuess` y así sucesivamente. El señal `+` coincidirá con una o varias veces el testigo anterior. El señal `*` coincidirá con cero o más veces el testigo anterior. |

| Ejemplo | Descripción |
|---|---|
| `^[0-9]+EUR` | Usted puede usar esto para coincidir `30 EUR` o `35EUR` o `023213 EUR` o cualquier cadena que comience con un dígito, seguido por cadena `EUR`. El signo `^` signo representa el inicio de la cadena a coincidir. |
| `[^\s]*@example.com` | Usted puede usar esto para coincidir `noreply@example.com` o `news@example.com` o `blabla@example.com` y así sucesivamente. El signo `^` entre paréntesis coincide con cualquier carácter que no sea el siguiente muestra. En el ejemplo antes mencionado, `[^\s]*` coincidirá con cualquier carácter que no sea espacio en blanco. |
| `^List-I[dD]:\s.*example.com` | Usted puede usar esto para coincidir `List-Id: aNYstring example.com` o `List-ID: example.com`, etc El signo `^` signo representa el inicio de la cadena a coincidir. El señal `\s` coincidirá con un espacio. El `[dD]` expresión significa o bien `d` o `D` será igualado. El expresión `.*` significa cualquier signo será duplicada. |

**Note**
No olvidarse de escapar con una barra invertida los metacaracteres (los paréntesis cuadrados o redondos, la barra invertida, símbolo de intercalación, el signo del dólar, plazo, el símbolo de la barra vertical, el signo de interrogación, el asterisco, el signo más).

3.
```
# bdsafe group configure GROUP_NAME \ contentfilter add 2 BigMai
```

Esto agregará la regla del filtro de contenido, el nombre `Bigmail` con `2` prioridad a GROUP_NAME. Cuando se aplica esta regla significa que si el tamaño de un cierto apego es mayor de 10000 bytes, el correo electrónico con el archivo adjunto correspondiente será dado de baja y nadie será notificado.

4. ```
   # bdsafe group configure GROUP_NAME \ contentfilter modify 0 "pr
   ```

   Esto cambiará el `MiRegla` (prioridad `0`) de la prioridad viejo `0` para nueva prioridad `3`. El nuevo nombre de esta regla será "regla porno".

5. ```
   # bdsafe group configure GROUP_NAME \ contentfilter priority 1 0
   ```

   Esto cambiará la regla de `Salario` de GROUP_NAME de prioridad viejo `1` para nueva prioridad `0` (la regla más importante, sino que se aplicará en primer lugar).

6. ```
   # bdsafe group configure GROUP_NAME \ contentfilter dump
   ```

   Esto mostrará una lista de las reglas de filtrado de contenido de GROUP_NAME junto con sus prioridades.

7. ```
   # bdsafe group configure GROUP_NAME \ contentfilter delete 4
   ```

   Esto eliminará la regla del filtro de contenido de NOMBRE_GRUPO con prioridad `4`.

8. ```
   # bdsafe group configure GROUP_NAME \ contentfilter enable N 4
   ```

   Esto desactivará la regla del filtro de contenido de NOMBRE_GRUPO con prioridad `4`.

## 10.5. Daemon de Log de BitDefender

The BitDefender Logger Daemon (**bdlogd**) allows you to get a full picture of the others demons activity, as it receives logging messages from the other modules and passes them to the logger plugins.

Either a local socket (Unix domain socket) or a TCP/IP socket will be used to implement communication among different modules of Bitdefender while the communication among the Logger Daemon and its plugins is based on API (Application Programming Interface).

**bdlogd** was designed with a plugins parallel execution philosophy in mind. In short, this means that each plugin will run on its own individual thread. The result is that the slower plugins will no longer disturb the faster ones (like filelog).
   ```

To manage the configuration of the Logger Daemon and the associated plugins you will use the **bdsafe** command. You will be provided below with a list of common settings for **bdlogd**.

The general syntax for the **bdlogd** daemon and plugins configuration is the following one:

```
# bdsafe logger configuration [parameters ...]
```

```
# bdsafe logger plugin configuration [parameters ...]
```

## The BasePath

To specify the fully-qualified name of a directory from which **bdlogd** will attempt to load plugins, run the following line as root:

```
# bdsafe logger basepath [value]
```

## 10.5.1. The Logger Plugins

The BitDefender Logger Daemon supports the following plugins:

- Plugin de Registro de archivo
- Plugin SMTP
- Plugin SNMP

### Plugin de Registro de archivo

The **bdlogd** receives messages from the other modules and send them to the other plugins, for instance the filelog plugin. By default, the filelog plugin settings are the following:

- bdlived.info=`/opt/Bitdefender/var/log/update.log`
- bdmaild.info=`/opt/Bitdefender/var/log/mail.log`
- *.error=`/opt/Bitdefender/var/log/error.log`
- bdlived.error=`/opt/Bitdefender/var/log/update.log`
- *.license=`/opt/Bitdefender/var/log/license.log`
- bdmaild.virus=`/opt/Bitdefender/var/log/virus.log`
- bdmaild.spam=`/opt/Bitdefender/var/log/spam.log`

It means that, for example, all error-related information, coming from all Bitdefender daemons, will be found in this location: `/opt/Bitdefender/var/log/error.log`.

However, you can fully customize the daemon and message type and also the file paths where the file logger writes the messages, by using the **bdsafe** command. In order to do this, please run the following line as root:

```
# bdsafe logger file path message_type [value]
```

The `message_type` argument must follow the syntax: `daemon.type`.

`daemon`
: It can take the following values: * (i.e. all daemons), bdmaild, bdfiled, bdlogd, bdscand, bdmond, bdlived

`tipo`
: It can take the following values: * (i.e. all types), info, error, license, debug, virus, spam

You can also enable or disable the entire filelog plugin or just a certain type of message. In order to do this, run these commands as root.

```
# bdsafe logger file disable message_type
```

```
# bdsafe logger file enable message_type
```

***Note***
Para una descripción completa de la configuración de registro de archivo, debe consultar las páginas del manual bdsafe(8).

## El plug-in de registro SMTP

Una de las principales características de las plugins **bdlogd** es el hecho de que son fácilmente y extremadamente configurable, mediante el uso del comando **bdsafe** . Ciertamente, el plugin de registro SMTP no hace excepciones a la característica antes mencionada. Usted puede averiguar el estado de plugin, activarlo/ desactivarlo, establezca un tiempo de espera de conexión, los remitentes y receptores de alerta, seleccione una plantilla o sólo un encabezado, etc.

Veamos algunos ejemplos.

Si desea conocer el estado de registro de SMTP plugin (habilitar / deshabilitar el plugin o sólo para un cierto tipo de mensajes) ejecuta la línea siguiente como root.

```
# bdsafe logger smtp status message_type
```

The `message_type` argument must follow the syntax: `daemon.type`.

`daemon`
: Puede tomar los siguientes valores: *(es decir, todos los demonios), bdmaild, bdfiled, bdlogd, bdscand, bdmond, bdlived, bdsmtpd.

`tipo`
: It can take the following values: * (i.e. all types), info, error, license, debug, virus, spam

Para enviar una notificación a los destinatarios de un correo electrónico infectado, ejecute este comando.

```
# bdsafe logger smtp alertrecv value
```

***Note***
Para una descripción completa de la configuración de registro SMTP, debe consultar las páginas del manual bdsafe(8).

## The SNMP log plugin

By using the **bdsafe** command, you can get the SNMP log plugin status, enable /disable it, set the port number where notification will be sent, set a connection timeout, etc.

Por ejemplo, para establecer el número de puerto donde se enviará la notificación, ejecute este comando como root.

```
# bdsafe logger snmp port value
```

***Note***
Para una descripción completa de la configuración de registro, debe consultar las páginas del manual bdsafe(8).

## 10.6. Cuarentena

The Quarantine is a special directory (or directories), unavailable for common users, where infected or suspected files or emails are to be isolated for a future purpose. Some BitDefender Daemons (**bdmaild**, **bdfiled** and **bdmond**) add files to Quarantine. The administrator can list and search these files, delete, restore or resend all files that match the given pattern by using the **bdsafe** command.

Para encontrar información sobre los directorios de Cuarentena, ejecute el siguiente comando como root.

```
# bdsafe quarantine status [quarname]
```

Si se especifica el parámetro opcional `quarname`, **bdsafe** mostrará la información solamente en ese directorio.

Para mostrar todos los archivos del directorio `quarname`, ejecute la siguiente linea.

```
# bdsafe quarantine list [quarname]
```

Buscar en la Cuarentena es muy fácil. Todo lo que tiene que hacer es ejecutar la siguiente linea.

```
# bdsafe quarantine search [quarname] [field] [pattern]
```

El parámetro `field` puede tener uno de los siguientes valores:

- remitente
- recipiente
- asunto
- uuid

***Note***
Puede utilizar un comodín (*) con el parámetro `pattern` (excepto para uuid).

Para el directorio de cuarentena específico y copiar, mover o eliminar todos los archivos que encajen con un patrón específico, ejecute el siguiente comando.

```
# bdsafe quarantine copy [quarname] [field] [pattern]
```

```
# bdsafe quarantine move [quarname] [field] [pattern]
```

```
# bdsafe quarantine delete [quarname] [field] [pattern]
```

El parámetro `field` puede tener uno de los siguientes valores:

- remitente
- recipiente
- asunto
- uuid

***Note***
Puede utilizar comodín (*) con el parámetro `pattern`.

En el caso de que desee reenviar todos los archivos que encajen con el patrón dado a través del servidor SMTP, ejecute la siguiente linea.

```
# bdsafe quarantine resend [quarname] \ [field] [pattern] server[:
```

The optional `crlfmagic` parameter can take any value. The effect of addind this parameter is the following one: **bdsafe** will actively replace all end-of-line sequences in the file with `\r\n`.

Para manejar la configuración de la Cuarentena, ejecute el siguiente comando.

```
# bdsafe quarantine configure [quarname] [parameter] [value]
```

`parameter` puede tener uno de los siguientes valores:

**maxentries**
Se refiere al número máximo de archivos permitido en la Cuarentena.

En este caso, el parámetro `value` debe ser un entero positivo.

**maxsize**
Se refiere al tamaño máximo permitido para la Cuarentena.

In this case, the `value` parameter must be a string describing the maximum size of the Quarantine directory. For example, `1m512k` specifies that the maximum size is 1.5 megabytes (`g` is for gigabytes, `m` for megabytes, `k` for kilobytes and `b` for bytes).

**ttl**

Time-to-live (ttl) se refiere al tiempo determinado que, cuando se agota, hace que el correo sea descartado de la Cuarentena.

In this case, the `value` parameter must be a string describing the maximum amount of time a file can remain in Quarantine before being deleted. For example, `1w2d` specifies that the maximum amount of time a file may remain in the quarantine is one week and two days (`w` is for weeks, `d` for days, `h` for hours, `m` for minutes, `s` for seconds).

# 11. Integración con Terceros

Con el lanzamiento de Bitdefender Security for Mail Servers SDK, los usuarios avanzados tienen la posibilidad de escribir plug-ins y scripts que se integren con el producto.

Para más información, por favor consulte el archivo `bdsms-sdk.tar.gz` ubicado en el directorio `opt/Bitdefender/share`.

# 12. Registro del Producto

El producto incluye un número de registro que le permite evaluarlo durante treinta días. Al final del periodo de prueba, si desea seguir utilizando el producto, necesitará proporcionar una nueva licencia.

Para comprobar el estado de la licencia, utilice el siguiente comando.

```
# bdsafe license mail
```

Se le presentará el tipo de licencia, estado, el número de usuarios cubiertos y el tiempo restante de validez.

Si dispone de una nueva licencia, el siguiente comando realizará el registro del daemon instalado.

```
# bdsafe license mail ABCDE12345ABCDE12345
```

# 13. Testing Bitdefender

Para asegurar que Bitdefender realmente funciona, puede probar la eficiencia de su antivirus y antispam utilizando métodos de prueba estándar. Básicamente, enviará un e-mail especial a alguna cuenta a través del servidor de correo. Recibirá los resultados (e-mail desinfectado, notificaciones o e-mail marcado como SPAM).

***Enviando el e-mail a Otra Cuenta***
El parámetro `$USER` se utiliza para enviar el correo electrónico a su cuenta corriente en la máquina local. Si desea enviar los mensajes de correo electrónico de prueba a otro destinatario a algún servidor de correo remoto, reemplácelo con una dirección de correo electrónico real, pero tenga cuidado de los correos electrónicos serán clasificados como infectados.

## 13.1. Prueba de Antivirus

You can verify that the Bitdefender Antivirus component works properly by the help of a special test file, known as the *EICAR Standard Anti-virus Test* file. EICAR stands for the *European Institute of Computer Anti-virus Research*. This is a dummy file, detected by antivirus products.

There is no reason to worry, because this file is not a real virus. All that `EICAR.COM` does when executed is display the text `EICAR-STANDARD-ANTIVIRUS-TEST-FILE` and exit.

No incluimos este archivo en el paquete de instalación para evitar generar falsas alarmas a aquellos usuarios de Bitdefender u otros antivirus. Sin embargo, el archivo puede ser creado utilizando cualquier editor de texto, siempre que el archivo se guarde en formato estándar MS-DOS ASCII y sea 68 bits de longitud. También podría ser de 70 bytes si el editor pone un CR/LF al final. El archivo debe contener únicamente la siguiente línea:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Copy this line and save the file with any name and `.COM` extension, for example `EICAR.COM`. You can keep the `EICAR.COM` in a safe place and periodically test the server protection.

***recursos online EICAR***
Puede visitar la página web EICAR en http://eicar.com/, lea la documentación y descargue el archivo desde una de las ubicaciones en la página web http://eicar.com/anti_virus_test_file.htm.

### 13.1.1. Adjunto de e-mail Infectado

Para probar la eficiencia de la protección e-mail, cree un e-mail con su agente de correo favorito, adjunte el archivo `EICAR.COM` y envíeselo a usted mismo a través de su servidor de correo. En breve recibirá el e-mail desinfectado, los e-mails de notificación que se supone que han de llegarle, el administrador de correo y, si está configurado, e-mails que informan al remitente y al destinatario sobre los virus encontrados.

Uso de la **uña** programa, disponible en muchas distribuciones de Linux, enviar el correo electrónico se puede hacer de la siguiente manera. De forma segura puede reemplazar **uñas** con **mutt**, o cualquier otro comando que acepta datos adjuntos.

```
$ echo "EICAR test file." | nail -s EICAR -a EICAR.COM  $USER
```

Si su programa de correo no soporta adjuntos, puede utilizar el siguiente comando, donde el cuerpo del e-mail es el contenido del archivo `EICAR.COM` (ya que es un archivo ASCII). Después de haber explorado el correo completo, Bitdefender les resultará infectado, desinfectar y notifique al administrador de correo y, eventualmente, el emisor y el receptor.

```
$ mail -s EICAR $USER < EICAR.COM
```

### 13.1.2. Archivo Adjunto Infectado

Para probar la eficiencia del componente Empaquetador MIME de Bitdefender, cree un archivo que contenga el archivo `EICAR.COM`, adjúntelo en un e-mail enviado a si mismo a través del servidor de correo. Por ejemplo, **gzip** el `EICAR.COM` y adjuntar el archivo resultante.

```
$ gzip  --best EICAR.COM $ echo "EICAR test archive." | nail -s EI
```

En breve recibirá el e-mail desinfectado, los e-mails de notificación que se supone que han de llegarle, el administrador de correo y, si está configurado, e-mails que informan al remitente y al destinatario sobre los virus encontrados.

## 13.2. Prueba de Antispam

Usted puede verificar que el componente Antispam de Bitdefender funciona correctamente con la ayuda de una prueba especial, conocido *GTUBE*. GTUBE representa la prueba *Genérica para el correo electrónico masivo no solicitado*. GTUBE proporciona una prueba mediante la cual se puede verificar que Bitdefender filtro está instalado correctamente y detecta el spam entrante.

***recursos online GTUBE***
Puede visitar la página web de GTUBE en http://gtube.net/, leer la documentación y descargar la muestra del mensaje en formato RFC-822 desde la página web.

El test consiste en introducir la siguiente cadena de texto 68 bytes en el cuerpo de un mensaje de correo, en una sola línea:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Al analizar el mensaje, Bitdefender debería marcarlo como spam.

El uso de cualquier **correo** programa, usted puede poner a prueba Bitdefender con el siguiente comando. Tienes que crear un archivo, llamado `GTUBE`, que contiene la cadena anterior en una línea. Ejecute el siguiente comando.

```
$ nail -s GTUBE $USER < GTUBE
```

En breve recibirá el e-mail marcado como SPAM. El `sujeto` y `X-BitDefender-Spam` cabeceras serán:

```
Subject:  [SPAM] GTUBE [SPAM]
X-BitDefender-Spam:  Yes (100)
```

# 14. Actualizaciones

Bitdefender was designed with capabilities for automatic update. At present, the risk of getting infected is high, both because new viruses appear and because the existing ones keep on spreading. Email communication, which is more and more used, has become a final factor in spreading infections from one user to another. This is why your antivirus must be kept up-to-date, by periodically checking the Bitdefender servers for new updates.

The Bitdefender update process is realized by Live! Update, a daemon which connects periodically to the Bitdefender update server and checks whether new virus definitions, antispam updates and product upgrades are available. In case there are any, the daemon will download only the changed files, executing an incremental update and saving bandwidth.

To find out the current configuration settings for the global proxy and the Live! Update service, run the following command.

```
# bdsafe live
```

## 14.1. Actualizaciones automáticas

Bitdefender Security for Mail Servers is configured to update automatically each hour, through the **bdlived** module. In case of a necessary update, before the specified interval expires, the daemon can be signaled to execute the update routine, manually. To trigger the on-demand check, one can issue the following command.

```
# bdsafe live forceupdate
```

***Note***
A minimum of five minutes must elapse from the last forced update.

### 14.1.1. Time Interval Modification

To modify the time interval you will have to run the command bellow. You can change the update interval to the desired value, in seconds. The new value must be an integer between 3600 (seconds, 1 hour) and 86400 (seconds, 24 hours).

```
# bdsafe live checkinterval [new_value]
```

## 14.1.2. Live! Update Proxy Configuration

If a proxy server is to be used to connect to the Internet, you can set/get your proxy server address and port by using the following command.

```
# bdsafe live globalproxy host [new_host]
```

Whitout the optional `[new_host]` parameter, this command displays the current proxy host only, in case there is a proxy host. To change the host, you must add the `[new_host]` parameter, following this syntax: `host[:port]`

However, you have to enable proxy usage by this command.

```
# bdsafe live globalproxy enabled Y
```

In order to deactivate the use of a proxy, run the following:

```
# bdsafe live globalproxy enabled N
```

For proxy servers that require authentication, the server administrator can set the user domain, name and the associated password via the following commands:

```
# bdsafe live globalproxy user [new_user]
```

```
# bdsafe live globalproxy domain [new_domain]
```

```
# bdsafe live globalproxy password [new_password]
```

The BitDefender Live! Daemon does not immediately load the settings modified via the **bdsafe** command. So, a good idea would be to run the following command, to apply the configuration changes.

```
# bdsafelive reloadsettings
```

## 14.2. Actualización Manual

Se trata de archivo .zip del servidor de actualizaciones que contienen las actualizaciones de los motores de análisis y las firmas de virus: `cumulative.zip`.

- `cumulative.zip` se publica el lunes de cada semana e incluye todas las firmas de virus y actualizaciones de los motores de análisis hasta la fecha de publicación.

Para actualizar el producto manualmente, siga los siguientes pasos:

1. **Descargue el archivo de la actualización.** Por favor descargue el archivo `cumulative.zip` y guárdelo en el disco cuando se le solicite.
2. **Extraer las actualizaciones.** Extraiga contenidos del archivo zip en el directorio `/opt/Bitdefender/var/lib/scan/Plugins/`, sobrescribiendo los archivos existentes con los nuevos, si fuese necesario.
3. **Establezca el dueño y los permisos del archivo.** Después de extraer el archivo zip, **debe** establecer el dueño y los permisos adecuados, ejecutando los siguientes comandos.

```
# chownbitdefender:bitdefender \ /opt/Bitdefender/var/lib/Plugin
# chmod 644 /opt/Bitdefender/var/lib/Plugins/*
```

4. **Reiniciar Bitdefender.** Once updated, Bitdefender should be restarted, using the following command.

```
# /opt/Bitdefender/bin/bdrestart
```

## 14.3. PushUpdate

Una Actualización Forzada (PushUpdate) es una actualización ordenada lanzada por los servidores de Bitdefender en situaciones inminentes, cuando una actualización puntual puede evitar que el servidor deje pasar e-mails infectados.

El disparador es un correo electrónico, enviado a la dirección que usted tiene que especificar en http://www.bitdefender.es/site/Products/pushUpdates/ . Bitdefender, mientras que el filtrado de los mensajes de correo electrónico, lo reconocerá y se iniciará el proceso de actualización.

## 14.4. Patches and New Product Versions

Since the Live! Update module can update automatically only the virus definitions and some of the core libraries used by Bitdefender, there is a small tool that can be used to update the whole Bitdefender installation.

BitDefender Swiss Army kniFE, **bdsafe(8)**, the multipurpose tool, can be used to keep Bitdefender up to date by applying various patches that might appear after the product was released. It can be run directly by the system administrator to list, search, install or uninstall patches or it can be installed as a cron job to automatically install patches as soon as they are released.

Patches are released to correct any bugs found or to add new features and they are grouped in the following categories: **CRITICAL**, **SECURITY**, **NORMAL**.

- Patches are labeled **CRITICAL** when they affect the normal behavior of the product. For example, if a new kernel is released, preventing the **bdcored** module to accomplish its job, then a **CRITICAL** patch will be released, correcting this issue.
- A patch is labeled **SECURITY** when it has the role of correcting any security related issue. For example, if there is a bug which might permit an attacker to gain access to emails scanned by Bitdefender, then a **SECURITY** patch will be released to fix this issue. As opposed to **CRITICAL** patches, which affect Bitdefender's normal behavior, **SECURITY** patches can fix the bugs that will not normally occur in a friendly environment, if such one exists.
- Patches labeled **NORMAL** are usually released to fix minor (cosmetic) bugs or to add some new features. For example, if Bitdefender incorrectly formats an email header, a **NORMAL** patch will be released to fix this minor issue.

New product versions may bring new features and functionalities. It is recommended to install upgraded versions when they become available.

Administrators are notified about releases of new patches and new product versions via automated e-mails, as well as through the Bitdefender Remote Admin interface. Notifications contain all the relevant information regarding the release, such as new features, bug fixes and installation instructions.

# Administración Remota

# 15. Bitdefender Remote Admin

Bitdefender Security for Mail Servers can be configured remotely by using a web browser under any operating system. In order to do this, it is necessary to install on the server side the Bitdefender Remote Admin module.

Bitdefender Remote Admin is an intuitive management interface. This management tool for UNIX-based product helps you remotely configure any settings in a single interface and lets you check the current status of the product (detailed statistics and update information).

When installing Bitdefender Remote Admin, you will be asked to enter a bind address for the Remote Admin server. For security reasons, by default, Bitdefender Remote Admin listens for incoming connections on `127.0.0.1 (port 8139)` and allows incoming connections from `127.0.0.1` only, as well. If you want to be able to remotely configure Bitdefender, set the address to `0.0.0.0:8139` (listening on all interfaces).

To see the existing Remote Admin socket, run the following command:

```
#
/opt/BitDefender/bin/bdsafe registry getkey /BDUX/Radmin/Ho
```

To set a new value for this socket, run the command:

```
# /opt/BitDefender/bin/bdsafe registry setkey /BDUX/Radmin/Host \
```

Before you use port number `8139`, make sure the port is not used by another application:

```
#
netstat -anpe | grep 8139
```

Also as part of the installation you can set a password for the default `administrator` account. If you choose not to, the default password `admin` will be used.

Once the installation is completed, use the `bdcertgen.sh` script located in `/opt/BitDefender/bin/` to indicate your domain name and generate an openssl certificate file. It is highly recommended to enable ssl (secure sockets layer) connections when using remote administration, so make sure you have the Net::SSLeay perl module installed.

To start Bitdefender Remote Admin, run the following command:

```
#
/opt/BitDefender/bin/bdradmin start
```

After any modification to the configuration, you have to manually restart Bitdefender Remote Admin by running the following command:

```
#
/opt/BitDefender/bin/bdradmin restart
```

## 15.1. Iniciando

Once you have setup Bitdefender Remote Admin, you can remotely configure almost all Bitdefender settings. All you have to do is open your favorite web-browser and point it to the following location, for the standalone module: http://your.domain.name:8139. The following login form will appear:


**Iniciar Sesión**

To login for the first time, use the default user account.

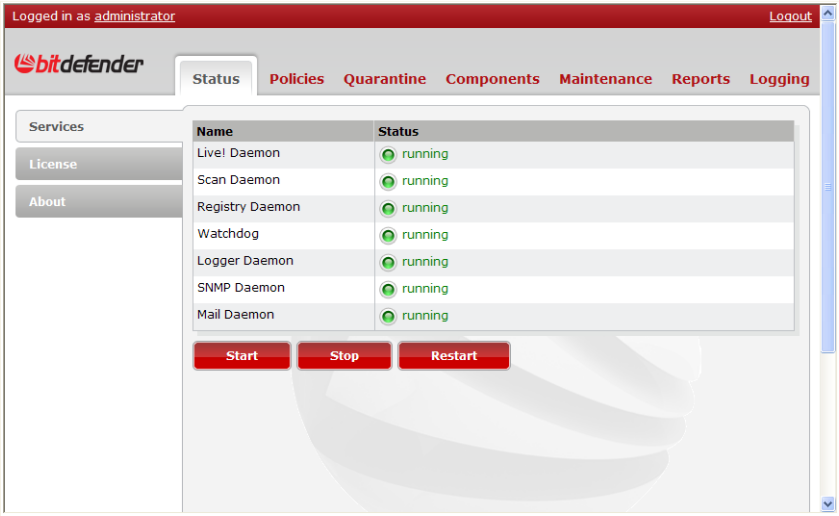
***Note***
To change the default password, after logging in click **administrator** on the upper left-hand corner of the interface and type the new password in the provided textboxes.

The following sections of this document describe how to configure Bitdefender using Bitdefender Remote Admin.

# 15.2. Estado

## 15.2.1. Servicios

Para abrir esta sección, vaya a **Estado** y seleccione **Servicios**.



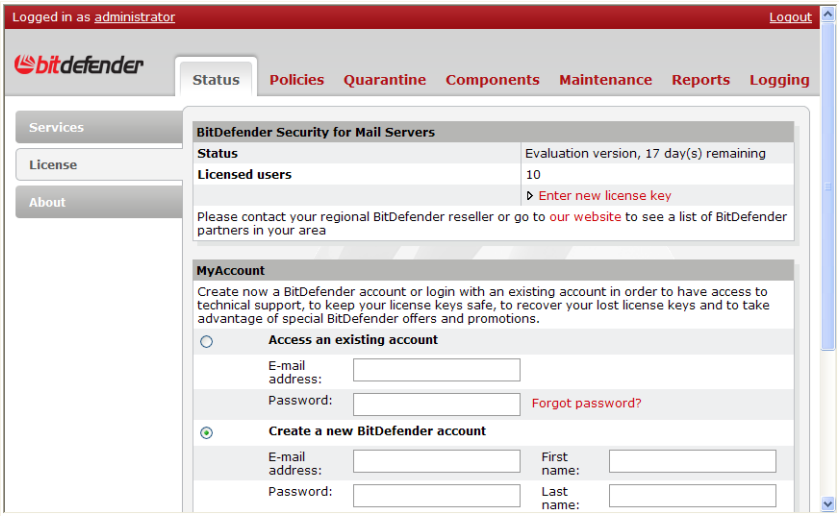

**Servicios**

Here you can see a list of all Bitdefender services and their current status. You can start, stop or restart the services by clicking the corresponding buttons.

***Note***
These actions are not performed instantly, a couple of seconds may be required for them to finish.

## 15.2.2. Licencia

Para abrir esta sección, vaya a **Estado** y seleccione **Licencia**.




**Licencia**

Here you can check the license status and register Bitdefender.

Click **Enter new license key**, type the license key in the corresponding textbox and click **Apply** to perform the registration process. If you mistype the license key, the message **Invalid key** will be displayed and you will have to type it again.

You can also create a Bitdefender account or login to an existing one to have access to technical support, keep your license keys safe, recover your lost license keys and take advantage of special offers and promotions.

Para crear una cuenta de Bitdefender, seleccione **Crear una nueva cuenta BitDefender** e introduzca la información solicitada.Los datos que introduzca aquí serán confidenciales.

- **E-mail** - introduzca su dirección de correo.
- **Contraseña** - introduzca una contraseña para su cuenta de Bitdefender.

***Note***
La contraseña debe contener 4 caracteres como mínimo.

- **Repetir contraseña** - introduzca de nuevo la contraseña especificada anteriormente.
- **Nombre** - introduzca su nombre.
- **Apellidos** - introduzca sus apellidos.
- **País** - introduzca el país en el que reside.

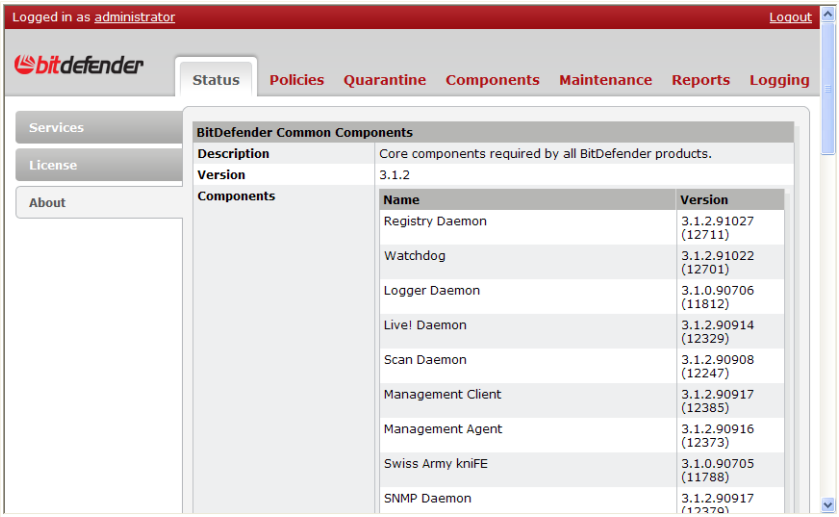
Haga clic en **Aplicar** para finalizar.

***Note***
Utilice la dirección indicada y contraseña para iniciar sesión en su cuenta http://myaccount.bitdefender.com.

To successfully create an account you must first activate your email address. Check your email address and follow the instructions in the email sent to you by the Bitdefender registration service.

## 15.2.3. Acerca de

Para abrir esta sección, vaya a **Estado** y seleccione **Sobre**.

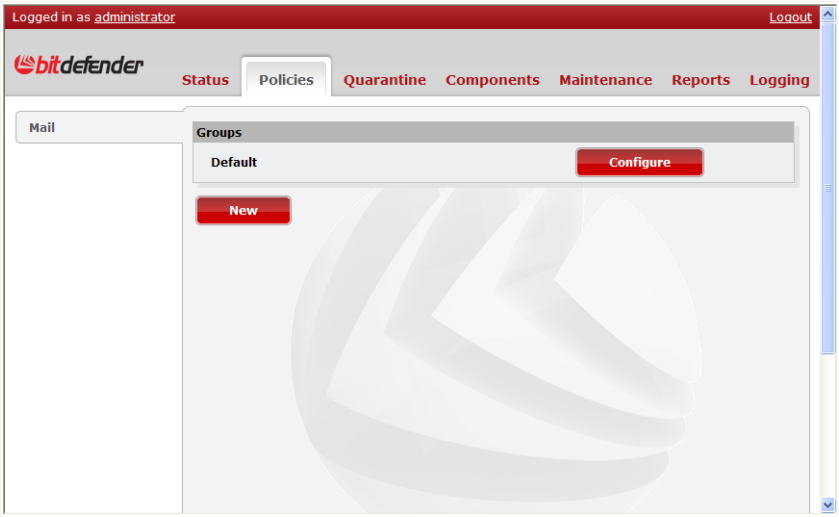



**Acerca de**

This section displays a short description, the version number and the list of components for every Bitdefender product installed.

## 15.3. Políticas

Cuando se trata de las políticas de seguridad que desea permanecer organizado, trabajar de manera más eficiente y en menos tiempo. Para gestionar fácilmente grupos y hacer cumplir las políticas de seguridad del grupo ir a **Políticas** y seleccione **Mensajes**.



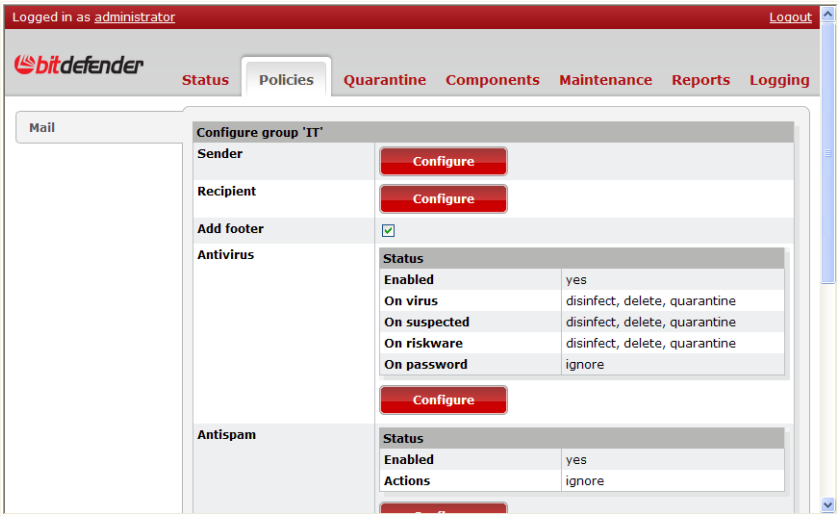

**Políticas**

La lista de grupos se muestra en esta ventana en orden de prioridad. Para cambiar la prioridad de un grupo, simplemente arrástrelo hacia arriba o hacia abajo en la lista y colóquela en la posición deseada.

Para crear un grupo nuevo, haga clic en **Nueva**, introduzca el nombre del grupo y haga clic en **Añadir** para guardar el nuevo grupo. Para eliminar un grupo, haga clic en el botón correspondiente **Eliminar** a la misma.

## 15.3.1. Configurar políticas de grupo

Puede editar las políticas de seguridad para un grupo haciendo clic en el botón correspondiente **Configurar** a ese grupo.




**Configurar Políticas**

Los ajustes actuales se muestran para el grupo seleccionado. Puede administrar los remitentes y los destinatarios incluidos en el grupo, configure el Antivirus, Antispam, Filtro de Contenido y Continuar correo.

## Administrando los Grupos

- **Remitente** - para editar la lista de remitentes de correo electrónico incluidas en el grupo, haga clic en el botón correspondiente **Configurar**.

  Aquí puede ver la lista de remitentes actualmente asignadas al grupo. Para añadir una nueva dirección de correo al grupo, haga clic en el botón **Nuevo** , introduzca la dirección (se aceptan comodines) y haga clic en **Añadir**. Para eliminar un remitente de la lista, seleccione la casilla correspondiente y haga clic en **Eliminar**. Haga clic en **Aceptar** para guardar los cambios en el grupo.

- **Destinatario** - para editar la lista de destinatarios de correo electrónico incluidas en el grupo, haga clic en el botón correspondiente **Configurar**.

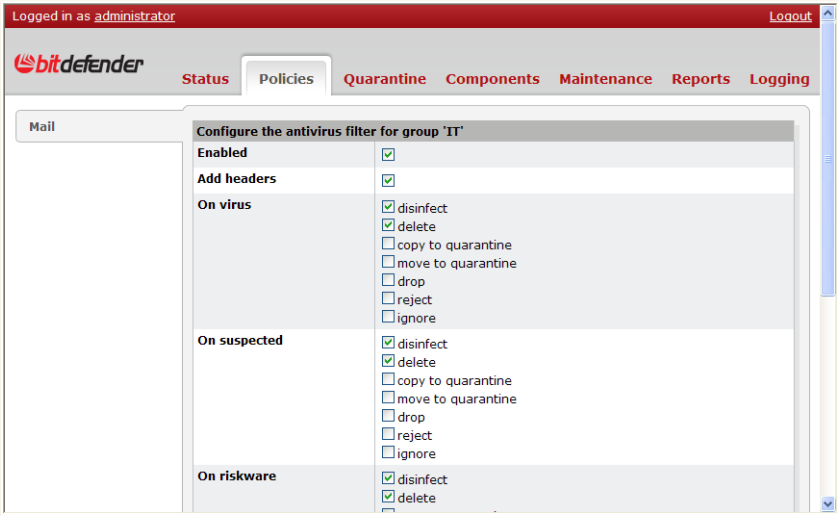
  Aquí se puede ver la lista de recepients actualmente asignadas al grupo. Para añadir una nueva dirección de correo al grupo, haga clic en el botón **Nuevo** , introduzca la dirección (se aceptan comodines) y haga clic en **Añadir**. Para eliminar

un destinatario de la lista, seleccione la casilla correspondiente y haga clic en **Eliminar**. Haga clic en **Aceptar** para guardar los cambios en el grupo.

**Añadir pie de página** - seleccione la casilla de verificación para habilitar la visualización de un mensaje en el pie de página de los correos electrónicos que informa a los destinatarios que el mensaje ha sido escaneados por Bitdefender.

## Antivirus

La configuración del módulo Antivirus se visualiza en esta sección. Para editar la configuración, haga clic en **Configura**.




**Antivirus**

- Para activar el análisis antivirus de los correos electrónicos, active la casilla de verificación correspondiente.
- Bitdefender Security for Mail Servers puede agregar un encabezado a los correos electrónicos digitalizados. Para habilitar encabezados, seleccione la casilla correspondiente.
- Seleccione las casillas de verificación junto a las acciones que desee tener sobre los **virus, objetos sospechosos** y **riskware** :

**Desinfectar**

Elimine el malware de un adjunto infectado (o cualquier otro componente en un correo que pueda ser utilizado para enviar malware). Si tiene éxito, el correo pasa al siguiente plugin (si lo hubiera) o se reenvía. De otro modo, se ejecutará la siguiente acción.

**Eliminar**

Elimina un adjunto u otros componentes del correo que contengan malware. Si tiene éxito, el correo pasa al siguiente plugin (si lo hubiera) o se reenvía. De otro modo, se ejecutará la siguiente acción.

Cuando el correo se elimina completamente, se generará un reemplazo para hacer conocer al destinatario que ha ocurrido.

**Mover a Cuarentena**

Mover el correo a la cuarentena. Si la acción falla, se escribirá un mensaje de error en el registro.

Tras ejecutarse esta acción, el correo será eliminado (la acción predeterminada) o rechazado.

**Copiar a la cuarentena**

Copiar el correo a la cuarentena. Si la acción falla, se escribirá un mensaje de error en el registro.

**Eliminar (acción predeterminada)**

Envíe el mensaje al agente de transporte de correo (MTA) para dejar el correo. Esta es la acción predeterminada. Por lo tanto, la acción final siempre será **Drop**, a menos que decida lo contrario.

Esta acción prohíbe el paso del correo. MTA no devolverá ninguna respuesta al remitente.

**Rechazar**

Envíe el mensaje al agente de transporte de correo (MTA) para rechazar el correo.

Esta acción prohíbe el paso del correo. Sin embargo, MTA devolverá un mensaje de rechazo.

**Omitir**

Envíe el mensaje al agente de transporte de correo (MTA) para reenviar el correo.

- Seleccione las casillas de verificación junto a las acciones que desee tomarse contraseña **archivos adjuntos protegidos**:

**Copiar a la cuarentena**

Copiar el correo a la cuarentena. Si la acción falla, se escribirá un mensaje de error en el registro.

**Mover a Cuarentena**

Mover el correo a la cuarentena. Si la acción falla, se escribirá un mensaje de error en el registro.

Tras ejecutarse esta acción, el correo será eliminado (la acción predeterminada) o rechazado.

**Eliminar (acción predeterminada)**

Envíe el mensaje al agente de transporte de correo (MTA) para dejar el correo. Esta es la acción predeterminada. Por lo tanto, la acción final siempre será **Drop**, a menos que decida lo contrario.

Esta acción prohíbe el paso del correo. MTA no devolverá ninguna respuesta al remitente.

**Rechazar**

Envíe el mensaje al agente de transporte de correo (MTA) para rechazar el correo.

Esta acción prohíbe el paso del correo. Sin embargo, MTA devolverá un mensaje de rechazo.

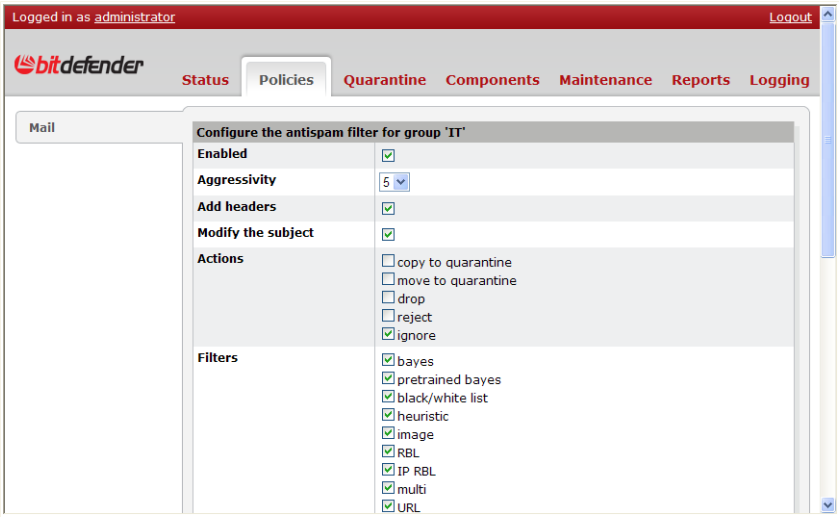
**Omitir**

Envíe el mensaje al agente de transporte de correo (MTA) para reenviar el correo.

Para guardar los cambios, haga clic en **Aceptar**.

## *Antispam*

La configuración de antispam se muestran en esta sección Para editar la configuración, haga clic en **Configura**.




**Antispam**

- Para activar el filtro antispam, seleccione la casilla correspondiente.
- Para establecer el nivel de la **agresividad** antispam, utilice la correspondiente lista desplegable. La escala va de `0` (confianza mínima en la puntuación antispam devuelto por los filtros de Bitdefender hasta `9` (máxima confianza). Elegir `0` podría aumentar la cantidad de correos electrónicos no solicitados, mientras que la elección `9` podría aumentar la cantidad de falsos positivos.
- **Añadir encabezados** agregará nuevas cabeceras de todos los mensajes (por defecto `X-BitDefender-Spam`). La cabecera SpamStamp, por defecto `X-BitDefender-SpamStamp`, es un encabezado de retroalimentación especial, utilizado por los especialistas de Bitdefender Antispam como retroalimentación, cuando los falsos negativos y positivos se someten a spam_submission@bitdefender.com.
- Seleccione **Modificar el asunto** para modificar el asunto de los mensajes de correo electrónico que se ajusten a la `Asunto` de la plantilla.
- Seleccione las acciones a realizar por el filtro antispam:
  - Copiar a Cuarentena
  - Mover a la Cuarentena

- Descartar
- Rechazar
- Omitir

- Cada uno de los filtros antispam se puede activar o desactivar individualmente. Marque las casillas de verificación correspondientes a los filtros que quiere permitir.
  - Filtro Bayes
  - Filtro Bayes pre-entrenado
  - Filtro Lista blanco/negro
  - Filtro Heurístico
  - Filtro de imágenes
  - Filtro RBL
  - Filtro IP RBL
  - Filtro de usos múltiples (juegos de caracteres asiáticos y cirílicos)
  - Filtro URL
  - El Filtro de Firmas
  - Filtro fuzzy
  - Filtro SURBL
  - Filtro SQMD

- Uso de los cuadros de texto proporcionados, puede añadir los amigos y los spammers a la **Lista Blanca** y respectivamente. **lista Negro**. Las entradas pueden ser puntos de venta habituales de correo electrónico o nombres de dominio (una entrada por línea), respetando el siguiente formato:

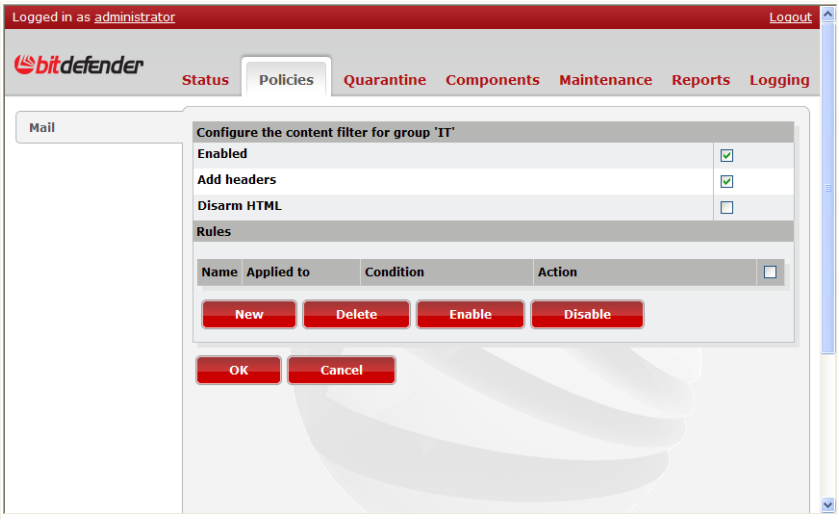
| *Formato* | *Descripción* |
|---|---|
| `user@domain.com` | Este formato solo coincidirá con el usuario especificado del dominio especificado. |
| `user@domain.*` | El usuario mencionado de cualquier dominio cuyo nombre comience por el texto especificado, coincidirá. |
| `user@*.com` | El usuario de cualquier dominio con un sufijo `.com` (por ejemplo) coincidirá. |
| `*@domain.com` | Esto hará coincidir a todos los usuarios del dominio especificado. |
| `*@domain.*` | Todos los usuarios de todos los dominios comenzando con el texto mencionado, coincidirán. |
| `*.com` | Esto hará coincidir a todos los usuarios de cualquier dominio con el sufijo `.com` (por ejemplo). |

| Formato | Descripción |
|---|---|
| user@* | El usuario especificado, de cualquier dominio, coincidirá. |
| user* | Esto hará coincidir a todos los usuarios cuyos nombres comiencen por el texto mencionado, no importa el dominio. |

Para guardar los cambios, haga clic en **Aceptar**.

## Filtro de Contenido

La configuración de filtro se mostrará en esta sección Para editar la configuración, haga clic en **Configura**.




**Filtro de contenido**

Para activar el filtro de contenido o añadir un encabezado a los mensajes filtrados marque las casillas de verificación correspondientes.

Para quitar el código potencialmente malicioso de mensajes de correo electrónico con contenido HTML, seleccione la casilla de verificación **Desarmar HTML** .

El contenido de las reglas de filtrado se enumeran por orden de prioridad conforme a las **Reglas**. Para cambiar la prioridad de una regla, simplemente arrástrelo hacia arriba o hacia abajo en la lista y colóquela en la posición deseada.

Seleccione una regla y haga clic en **Eliminar** para eliminarla, **Activar** / **Desactivar** para activar / desactivar, o **Editar** para configurar los parámetros de la regla.

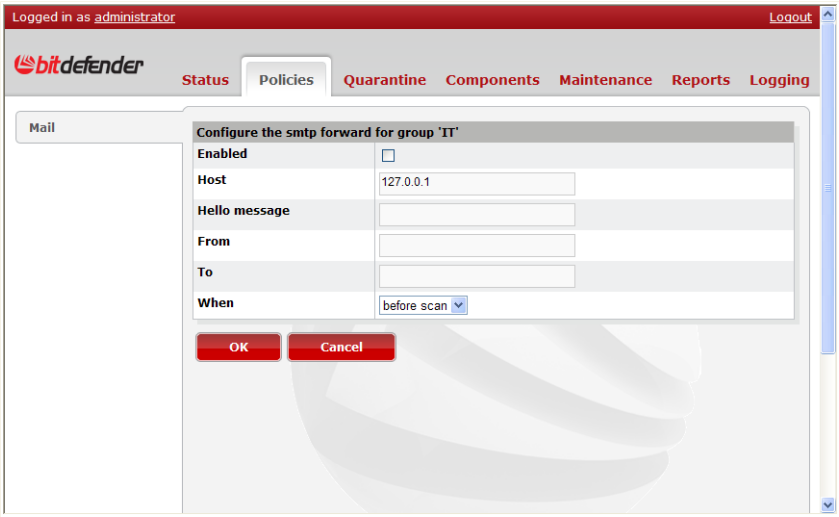
Para crear una nueva regla de filtrado de contenido, haga clic en **Nuevo** y siga estos pasos:

1. Introduzca el nombre de la regla.
2. Seleccione el tipo de regla Esto indicará la parte del correo electrónico del filtrado de contenidos regla se aplicará a:. la cabecera, el cuerpo, el tamaño de archivo adjunto de correo o el (nombre, tipo o tamaño).
3. Seleccione quienes recibirán una notificación de Bitdefender cuando un mensaje que coincida con la regla se detecta: nadie (no se envía la notificación), el administrador, el recepient o el remitente.
4. Establecer la fórmula de la regla. El tipo de regla aparecerá automáticamente en el cuadro de texto **Si**. Seleccione una expresión de la contigua lista desplegable e introduzca un valor para él en el cuadro de texto. Para completar la fórmula, seleccione una acción de la lista a **continuación** desplegable: ignorar, eliminar, rechazar, cambiar, copiar a cuarentena o mover en cuarentena.
5. Haga clic en **Aceptar** para guardar la regla.

Para guardar los cambios, haga clic en **Aceptar**.

## *Reenviar SMTP*

La configuración de continuar correo se mostrará en esta sección Para editar la configuración, haga clic en **Configura**.




**Reenviar SMTP**

Para habilitar el reenvío de mensajes a otro destinatario, seleccione la casilla de verificación correspondiente.

A continuación, especifique la información necesaria:

- IP/ Nombre del host
- Mensaje de Hola
- Desde - el remitente
- A - la cuenta de destino
- Cuando - seleccione de la lista desplegable si desea que los mensajes que se envían antes o después de ser escaneados

Para guardar los cambios, haga clic en **Aceptar**.

Una vez que haya terminado de configurar las políticas de un grupo, haga clic en **Aplicar** para aplicar los cambios.

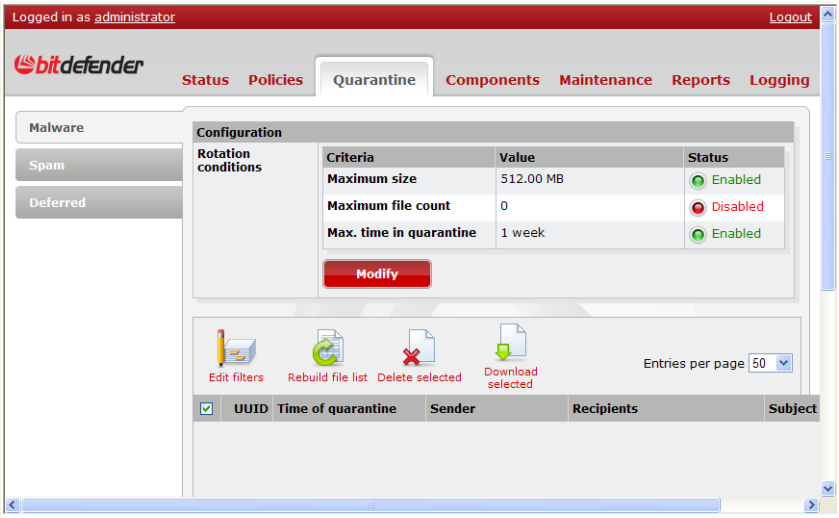
# 15.4. Cuarentena

La Cuarentena es un directorio especial, no disponible para usuarios comunes, donde los archivos o correos electrónicos sospechosos son aislados para una comprobación futura.

***Quarantined objects are safe***
Cuando un virus está aislado en cuarentena no puede hacer daño alguno, al no poder ejecutar o leerlo.

## 15.4.1. Cuarentena de malware

Para abrir esta sección, vaya a **Cuarentena** y seleccione **Malware**.




**Cuarentena de malware**

La Cuarentena de Malware es el directorio en donde los archivos infectados o sospechosos son aislados del sistema. La configuración de la cuarentena, estado y contenidos son mostrados en esta ventana.

Puede editar las **Condiciones de Rotación de la Cuarentena de malware** haciendo clic en el botón **Modificar** y editar las cajas de texto correspondientes a los siguientes criterios:

- **Tamaño máximo**`k`, `m` or `g` after the number you can set the size in Kilobytes, Megabytes or Gigabytes respectively.
- **Tamaño máximo de archivo**
- **Maximum time in quarantine**`m`, `h`, `d` or `w` after the number you can set the time period in minutes, hours, days or weeks respectively.

To disable a condition, type `0` in its corresponding box. Click the **Apply** button to save the changes.

El contenido de la cuarentena esta listado en la parte inferior de la ventana. Para cada ítem se proporciona el UUID, tiempo en cuarentena, remitentes, destinatarios y sujetos. Puede utilizar las siguientes herramientas para navegar fácilmente y administrar la cuarentena:

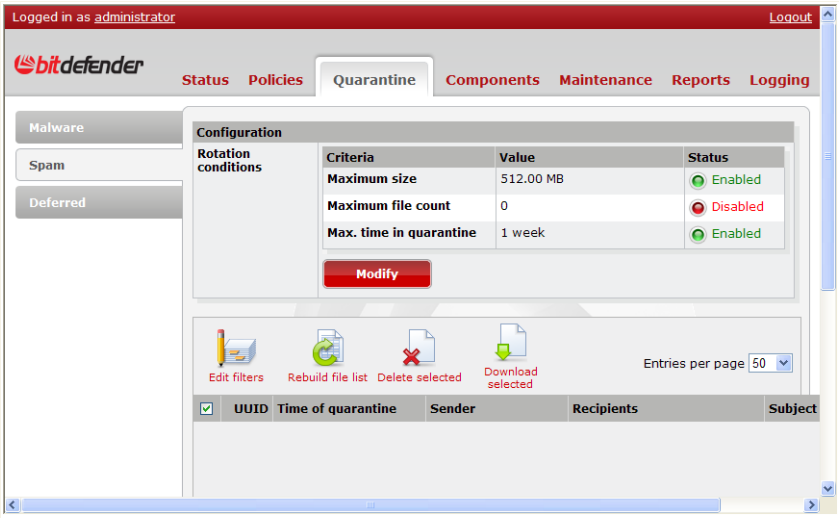
- **Edit filters** - helps you filter the list of displayed items using the following criteria:
  - **Tamaño**
  - **Time of quarantine**
  - **Original file name**
  - **Dirección IP**
  - **Estado**
  - **Remitente**
  - **Destinatarios**
  - **Asunto**
  - **Infection** - filter items based on infection information:
    - **Virus**
    - **Estado**
    - **Acción realizada**
    - **Objeto infectado**

  Select the filtering options and click **Apply** to use them on the list.
- **Rebuild the list** - refresh the list of quarantined files.
- **Delete selected** - remove the selected items from the quarantine.

- **Download selected** - select quarantine items and download them to a location of your choice.
- You can choose how many items are to be displayed per page by selecting a number from the **Entries per page** drop-down list.

## 15.4.2. Cuarentena de spam

Para abrir esta sección, vaya a **Cuarentena** y seleccione **Spam**.




**Cuarentena de spam**

Aquí es donde se encuentran los mensajes de spam. La configuración de la cuarentena, estado y contenidos son mostrados en esta ventana.

Puede editar las **Condiciones de Rotación de la Cuarentena de Spam** haciendo clic en el botón **Modificar** y editar las cajas de texto correspondientes a los siguientes criterios:

- **Tamaño máximo**`k`, `m` or `g` after the number you can set the size in Kilobytes, Megabytes or Gigabytes respectively.
- **Tamaño máximo de archivo**

- **Maximum time in quarantine**`m`, `h`, `d` or `w` after the number you can set the time period in minutes, hours, days or weeks respectively.

To disable a condition, type `0` in its corresponding box. Click the **Apply** button to save the changes.

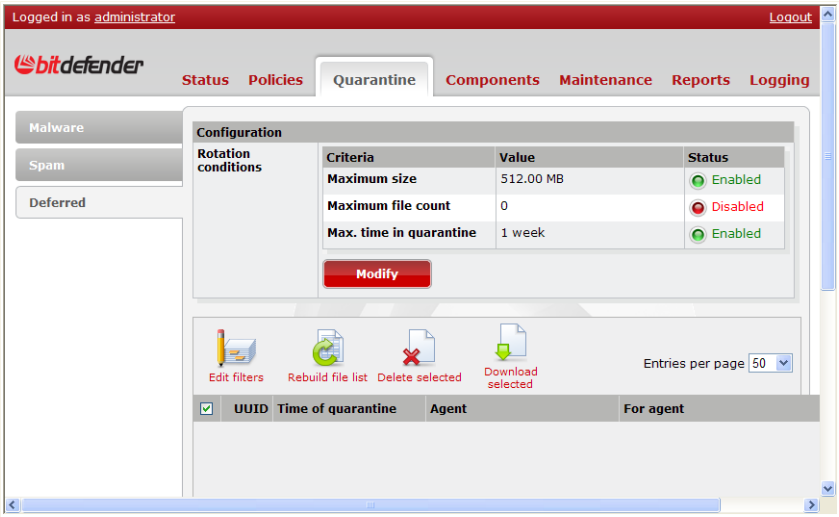
El contenido de la cuarentena esta listado en la parte inferior de la ventana. Para cada ítem se proporciona el UUID, tiempo en cuarentena, remitentes, destinatarios y sujetos. Puede utilizar las siguientes herramientas para navegar fácilmente y administrar la cuarentena:

- **Edit filters** - helps you filter the list of displayed items using the following criteria:
  - **Tamaño**
  - **Time of quarantine**
  - **Original file name**
  - **Dirección IP**
  - **Remitente**
  - **Destinatarios**
  - **Asunto**
  - **Stamp spam**

  Select the filtering options and click **Apply** to use them on the list.
- **Rebuild the list** - refresh the list of quarantined files.
- **Delete selected** - remove the selected items from the quarantine.
- **Download selected** - download the selected quarantine items to a location of your choice.
- You can choose how many items are to be displayed per page by selecting a number from the **Entries per page** drop-down list.

## 15.4.3. Deferred Quarantine

Para abrir esta sección, vaya a **Cuarentena** y seleccione **Diferido**.




**Deferred Quarantine**

The Deferred Quarantine is an isolated directory storing all the objects that may cause process crashing (for instance, malformed archives or zip-bombs). The quarantine settings, status and contents are displayed in this window.

Puede editar las **Condiciones de Rotación de la Cuarentena diferidos** haciendo clic en el botón **Modificar** y editar las cajas de texto correspondientes a los siguientes criterios:

- **Tamaño máximo**`k`, `m` or `g` after the number you can set the size in Kilobytes, Megabytes or Gigabytes respectively.
- **Tamaño máximo de archivo**
- **Maximum time in quarantine**`m`, `h`, `d` or `w` after the number you can set the time period in minutes, hours, days or weeks respectively.

To disable a condition, type `0` in its corresponding textbox. Click the **Apply** button to save the changes.

El contenido de la cuarentena esta listado en la parte inferior de la ventana. Para cada ítem se proporciona el UUID, tiempo en cuarentena, nombre original del archivo

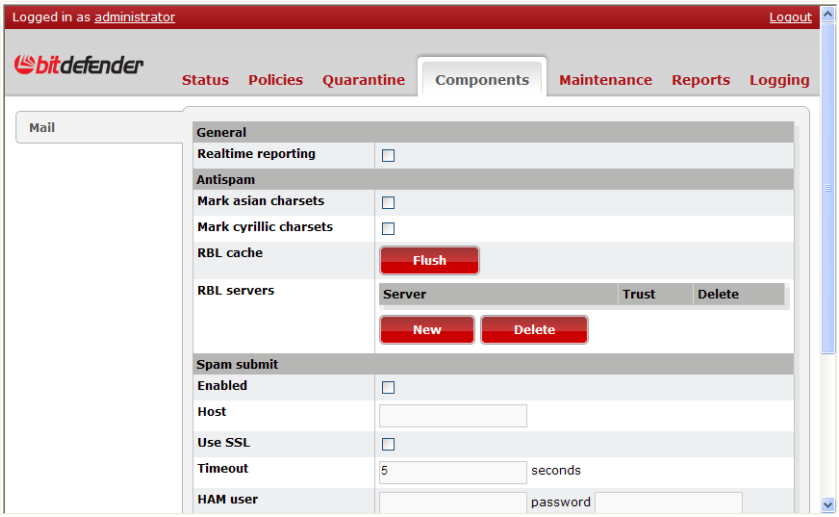
y tamaño. Puede utilizar las siguientes herramientas para navegar fácilmente y administrar la cuarentena:

- **Edit filters** - helps you filter the list of displayed items using the following criteria:
  - **Tamaño**
  - **Time of quarantine**
  - **Original file name**
  - **Agentebdmond**
  - **For agent**

  Select the filtering options and click **Apply** to use them on the list.
- **Rebuild the list** - refresh the list of quarantined files.
- **Delete selected** - remove the selected items from the quarantine.
- **Download selected** - download the selected quarantine items to a location of your choice.
- You can choose how many items are to be displayed per page by selecting a number from the **Entries per page** drop-down list.

## 15.5. Componentes

Para abrir esta sección, vaya a **Componentes** y seleccione **Mensajes**.




**Componentes**

To allow sending anonymous reports about the viruses and spam found on your server to the Bitdefender Lab, select the **Realtime reporting** checkbox. This way you can help Bitdefender identify new viruses and spam and find quick remedies for them.

## 15.5.1. Antispam

Para marcar los mensajes redactados con caracteres asiáticos o cirílicos como spam, seleccione las casillas de verificación correspondientes.

Para borrar la caché de RBL, haga clic en el botón **Flush**.

Los servidores RBL que están configuradas actualmente se enumeran en **servidores RBL**.

Para añadir un nuevo servidor - haga clic en **Nuevo** yintroduzca un nombre de servidor y el nivel de confianza (un valor entre 0 y 100) en el campo de texto correspondiente. Haga clic en **Añadir** para añadir el servidor a la lista.

## 15.5.2. Envío de Spam

Al permitir a los usuarios enviar mensajes de spam a la Lab de Bitdefender le puede ayudar a mejorar el filtro Bayesiano pre capacitado.

Para utilizar esta función, debe configurar la configuración:

- Para activar envíos de spam, seleccione la casilla de verificación correspondiente
- Escriba el host POP3
- Para activar /desactivar SSL, seleccione la casilla de verificación correspondiente
- Establezca el intervalo de tiempo en que Bitdefender comprobará las cuentas de e-mail:
- Introduzca el nombre de usuario y, si es necesario, la contraseña para los cuentas de usuario SPAM y HAM

## 15.5.3. SMTP

Para la integración del Proxy SMTP tiene que especificar la siguiente información de cara a permitir a Bitdefender analizar todo el tráfico de mensajes de correo:

- La dirección del servidor SMTP real y puerto utilizado por Bitdefender para enviar los correos electrónicos. Por defecto, la dirección es `127.0.0.1` y el puerto es `10025` .
- El puerto de Bitdefender escuchará. De forma predeterminada, el puerto es `25`.
- El tiempo de espera de conexión especifica cuánto tiempo esperará los datos entrantes Bitdefender en una conexión ya establecida antes de cerrarla.

  Escriba el valor temporal en segundos. Por ejemplo, si escribe 60 y los datos no se transmiten a través de la conexión ya establecida durante 60 segundos, Bitdefender cancelará la conexión. Cuando el valor es `0`, sin tiempo de espera de conexión se hace cumplir.
- Los hilos representan el número máximo de conexiones entrantes simultáneas Bitdefender será capaz de manejar. Si el valor introducido es negativo, todas las conexiones entrantes serán rechazadas. Cuando el valor es `0`, sin límite de hilos se hace cumplir.
- The maximum size of the email messages that will pass through the SMTP Proxy. If a message size surpasses this limit, the email message will be rejected. When the value is `0`, no size limit is enforced. All the files, regardless of their size, will be scanned.

### Redes

Esta sección contiene las redes de Bitdefender mensajes de correo electrónico de relés. Debe agregar la dirección IPv4 en formato con puntos a la lista para instruir Bitdefender para aceptar mensajes de correo electrónico procedentes de estas direcciones, independientemente de su destino.

El **Nuevo** botón permite agregar un dominio a la vez. Para cada dominio existe la opción de eliminarlo al seleccionar la casilla de verificación y haga clic en **Eliminar** .

### Dominios

Los dominios de transmisión de Bitdefender se utiliza para aceptar emails sobre se configuran en esta sección. Por ejemplo, si su servidor de correo electrónico se encarga de correos electrónicos para los dominios *company1.com* y*company2.com*, debe introducir los dos dominios en esta sección. Si tiene subdominios, debe especificar explícitamente como *subdomain1.company3.com* , *subdomain2.company3.com* , etc

El **Nuevo** botón permite agregar un dominio a la vez. Para cada dominio existe la opción de eliminarlo al seleccionar la casilla de verificación y haga clic en **Eliminar** .

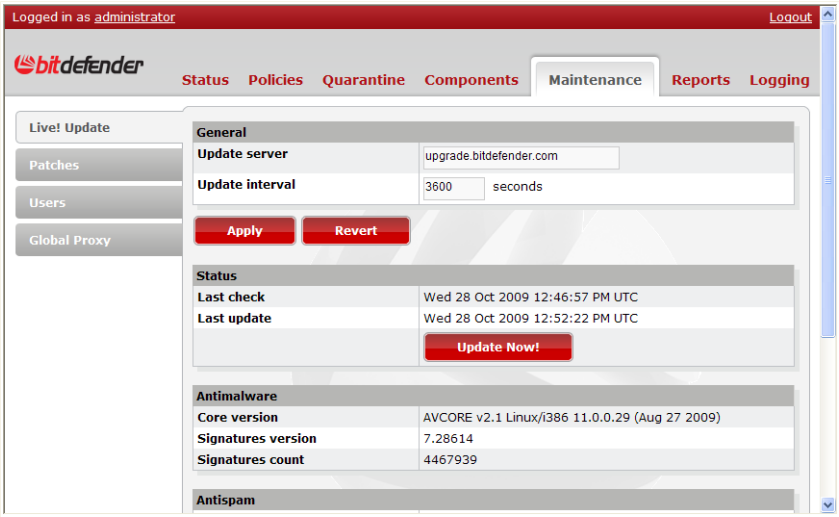
### Escuche en línea el

Se puede establecer un límite a las interfaces de Bitdefender escuchar, especificados por su dirección IP. Para añadir una dirección, haga clic en **Nuevo**, rellene el cuadro de texto y haga clic en **Añadir**. Para eliminar una dirección, seleccione la casilla correspondiente y haga clic en el botón**Eliminar** .

## 15.6. Mantenimiento

### 15.6.1. Live! Update

To open this section, go to **Maintenance** and select **Live! Update**.




**Live! Update**

The Live! Update window provides information regarding the general update settings and update status, the malware signatures version and number of signatures and the Bitdefender Remote Admin version.

The default update server is http://upgrade.bitdefender.com and the default update interval is 1 hour. To use a different server or set a different time interval between updates, enter the new information in the corresponding textbox and click **Apply**.

Click the **Update Now!** button to trigger an automatic check and, possibly, update (if there are any updates on the server).

## 15.6.2. Parches

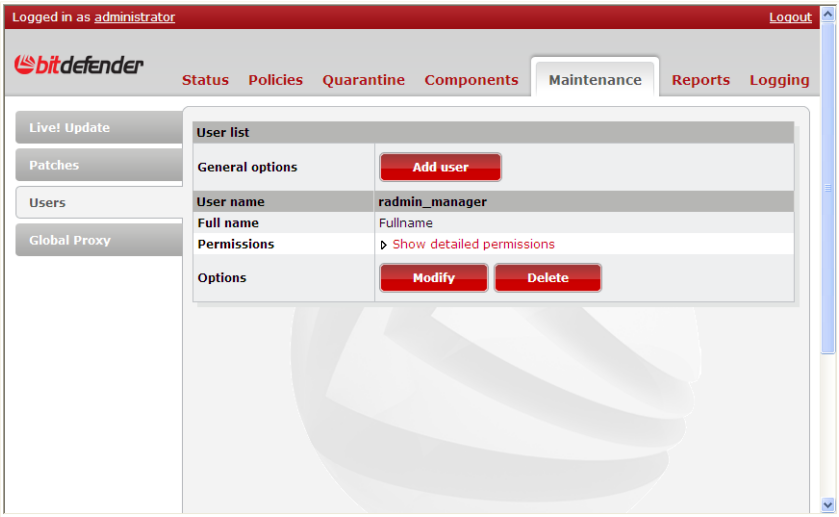
To open this section, go to **Maintenance** and select **Patches**. Patches might appear after the product is released. This is where you are provided with a list of available patches and a short description for each of them.

Choose which patches to install by selecting the checkbox next to them and click the **Update** button to start installing the selected patches.

***Important***
It is highly recommended to install product patches as soon as they are available.

## 15.6.3. Usuarios

Para abrir esta sección, vaya a **Mantenimiento** y seleccione **Usuarios**.

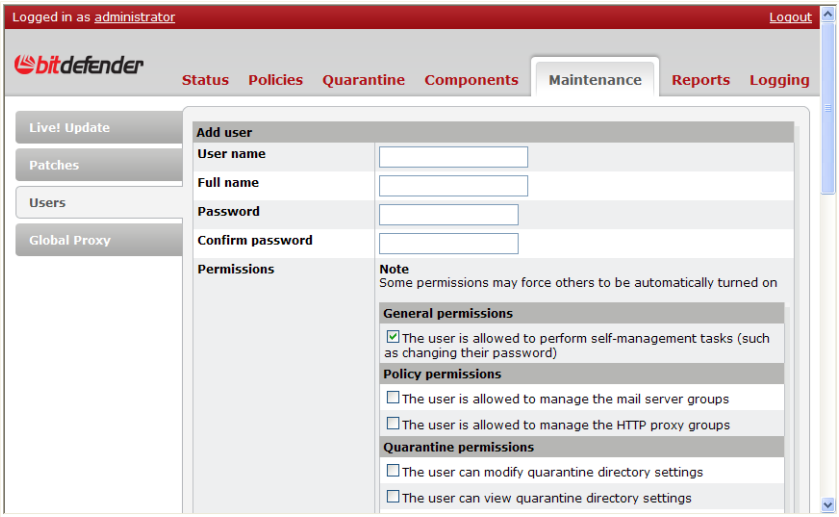



**Usuarios**

This is where you can create and manage Bitdefender Remote Admin user accounts.

Existing users appear in the user list. To view the permissions of a user, click **Show detailed permissions**. To edit the credentials or permissions for a user, click the **Modify** button next to that user. To remove a user, click the **Delete** button.

To create a new user, click **Add user**.

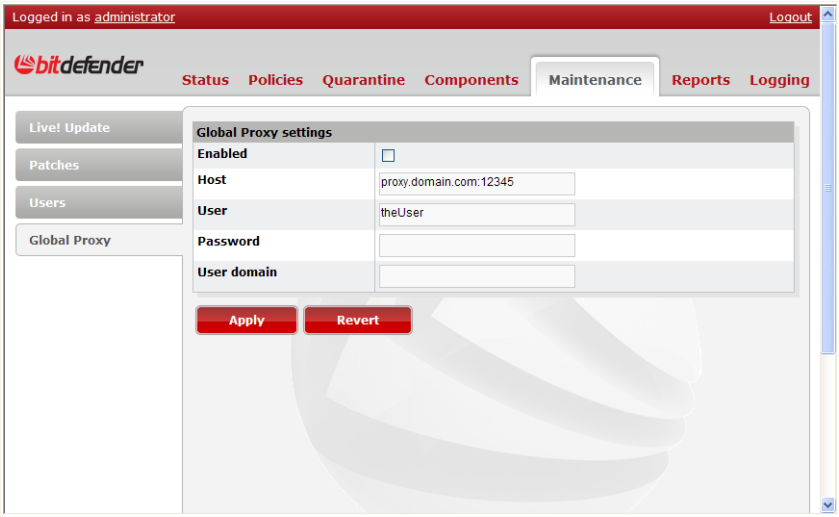



**Añadir nuevo usuario**

Fill in the necessary account information: the user name, the user's full name and account password and set the permissions by selecting their corresponding checkboxes. Click the **Add user** button to finish.

## 15.6.4. Global Proxy

Para abrir esta sección, vaya a **Mantenimiento** y seleccione **Proxy global**.




**Global Proxy**

Aquí es dónde puede introducir la configuración del servidor proxy.

Si utiliza un servidor proxy para conectarse a Internet, seleccione la casilla **Activado**.

Enter the server address and port in the **Host** textbox. If authentication is required, you also have to enter the user name, password and domain in the corresponding textboxes.

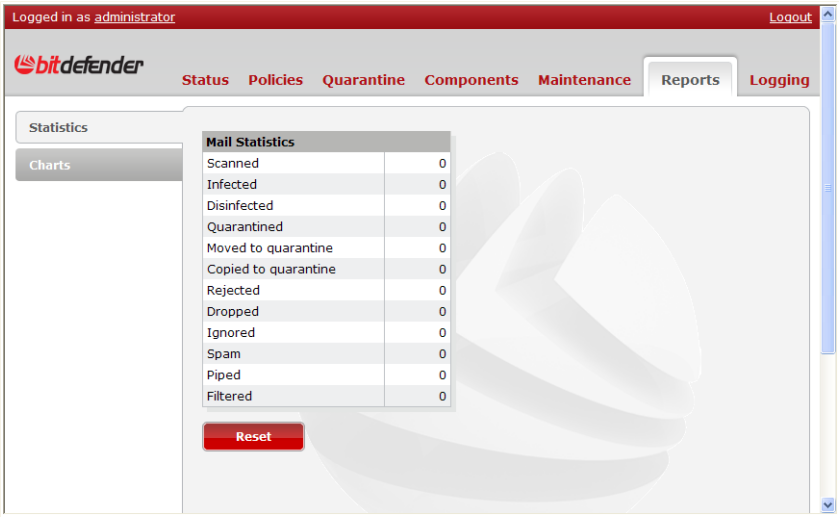
Haga clic en **Aplicar** para guardar la configuración.

# 15.7. Informes

This section offers the possibility to obtain statistical data regarding product activity as well as showing helpful charts for information related to memory consumption and daemons activity.

## 15.7.1. Estadísticas

Para abrir esta sección, vaya a **Informes** y seleccione **Estadísticas**.



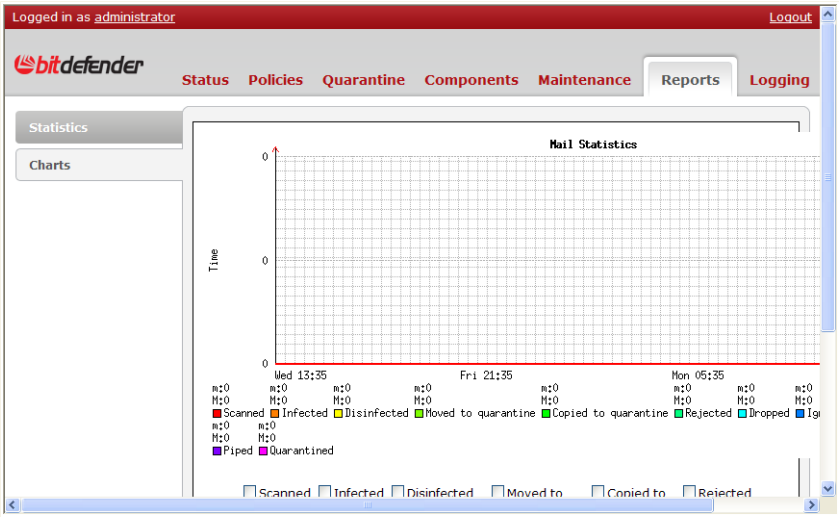

**Estadísticas**

La tabla de informe estadístico se puede acceder en esta sección. Aquí puede encontrar información sobre los objetos analizados en cuanto a su situación y de las medidas adoptadas:. analizado, infectado, desinfectado, en cuarentena, rechazado, ignorado, correo no deseado, abandonado, hilo, filtrado.

Use the **Reset** button to clear the statistics.

## 15.7.2. Gráficos

Para abrir esta sección, vaya a **Informes** y seleccione **Gráficos**.




**Gráficos**

Here you can find two types of charts which you can select from the **Chart type** drop-down list:

- Resource Usage - provides information related to memory consumption and daemons activity
- Mail Statistics - provides information regarding actions taken on scanned objects

You can set which daemons' activity and which actions are to be displayed by selecting the corresponding checkboxes.

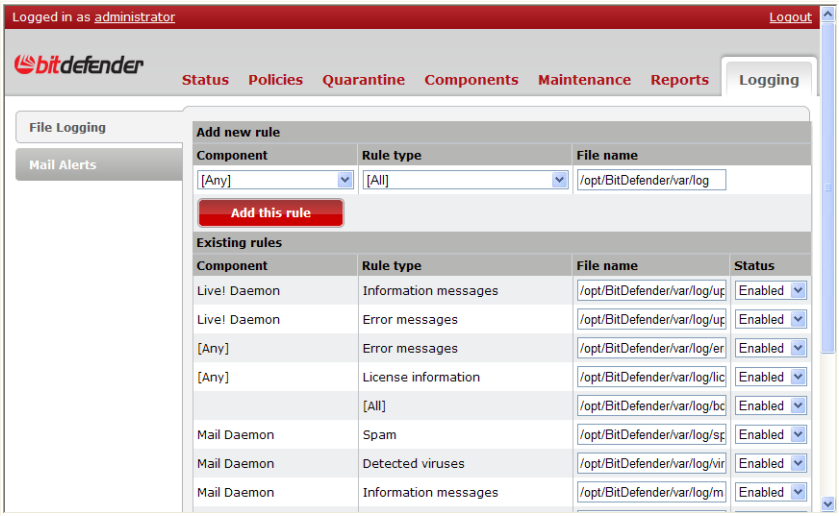
The charts can be customized by selecting different sizes from the **Chart size** drop-down list and different time intervals from the **Interval** drop-down list.

# 15.8. Registro en Log

This section allows the customization of the logging process, realized by the Bitdefender logging module.

## 15.8.1. Registro de Archivo

Para abrir esta sección, vaya a **Registro** y seleccione **Registro de archivos**.




**Registro de Archivo**

By default, you will be provided with a list of logging rules. For each rule you can see the component (daemon) it applies to, the rule type, the location of the log file and the status. Enable/disable a rule by selecting the status from the corresponding drop-down list.

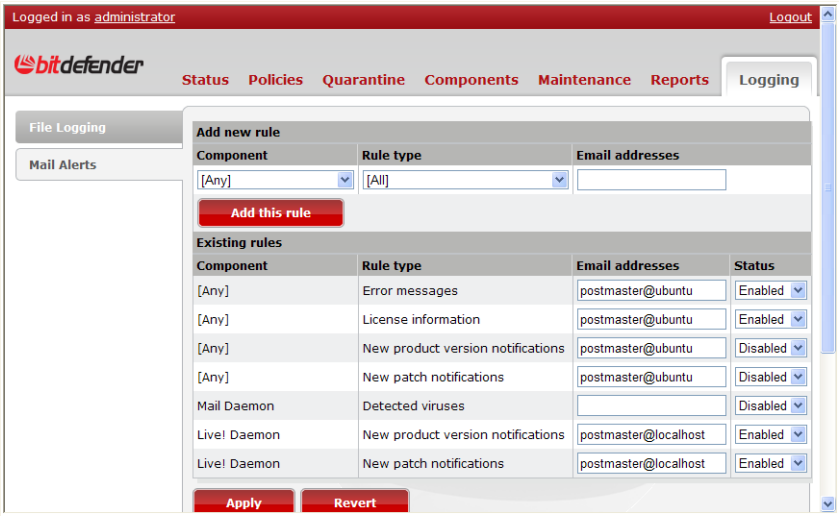
Let's say you enable the **Error messages** for **[Any]** component rule.This means that all error-related information, coming from all Bitdefender daemons, will be found in this location: `/opt/Bitdefender/var/log/error.log`. Of course, you can easily modify the location by editing the **File name** textbox.

Si quiere añadir una regla nueva, seleccione el componente (daemon) al que se aplica y el tipo de regla desde las listas desplegables correspondientes, escriba la ubicación del archivo en el cuadro de texto **Nombre de archivo** y haga clic en **Añadir esta regla**.

To complete the setup, click the **Apply** button. To use the default rule set, click the **Revert** button.

## 15.8.2. Alertas por Correo

Para abrir esta sección, vaya a **Registro** y seleccione **Alertas por Correo**.




**Alertas por Correo**

Las alertas por correo son simples mensajes enviados por Bitdefender al administrador del sistema para informarle de eventos especiales ocurridos o a los partners para comunicarles mediante un mensaje que se ha encontrado malware.

By default, you will be provided with a list of logging rules. For each rule you can see the component (daemon) it applies to, the rule type, the email address and the status. Enable/disable a rule by selecting the status from the corresponding drop-down list.

If you want to add a new rule, select the component it applies to and the rule type from the corresponding drop-down lists, type the email address(es) the alerts should be sent to into the **Email addresses** textbox and click **Add this rule**.

To complete the setup, click the **Apply** button. To use the default rule set, click the **Revert** button.

# 16. SNMP

## 16.1. Introducción

The SNMP (Simple Network Management Protocol) support of Bitdefender consists of two implementations: a SNMP daemon and a Logger plugin.

The SNMP daemon is a custom implementation of a **snmpd** service. It exports a minimal set of features to allow interrogation of Bitdefender.

The second implementation, the Logger plugin, is just another module besides the file logger, real-time virus and spam report module or mail notification module. It receives the same Bitdefender events information as the others Logger Plugins and it sends them to some remote host running the SNMP trap server, which, in its turn, will process them (send to syslog, etc.).

## 16.2. The SNMP Daemon

As stated before, this is a daemon which allows the user to interrogate the Bitdefender settings.

One popular tool to do SNMP queries is **snmpget**, part of the **net-snmp** package. Each command must follow this syntax:

```
# snmpget -v 1 -Cf -c [community] [hostname] [OID]
```

Let's take an example. Suppose that you want to find out the number of scanned objects on `JohnDoe` server. Simply run this command.

```
# snmpget -v 1 -Cf -c initial JohnDoe \ 1.3.6.1.4.1.22446.1.1.1.1.
```

Below you will find the complete list of the OIDs.

| *Tipo* | *OID* |
|---|---|
| **Analizado** | 1.3.6.1.4.1.22446.1.1.1.1.1.1 |
| **Infectados** | 1.3.6.1.4.1.22446.1.1.1.1.1.2 |
| **Desinfectados** | 1.3.6.1.4.1.22446.1.1.1.1.1.3 |

| Tipo | OID |
|---|---|
| En quarentena | 1.3.6.1.4.1.22446.1.1.1.1.1.4 |
| Dropped | 1.3.6.1.4.1.22446.1.1.1.1.1.5 |
| LastUpdate | 1.3.6.1.4.1.22446.1.1.1.2.1 |
| LastCheck | 1.3.6.1.4.1.22446.1.1.1.2.2 |
| CheckSecs | 1.3.6.1.4.1.22446.1.1.1.2.3 |
| License/Type | 1.3.6.1.4.1.22446.1.1.1.3.1.1 |
| License/Count (user) | 1.3.6.1.4.1.22446.1.1.1.3.1.2 |
| License/Count (domain) | 1.3.6.1.4.1.22446.1.1.1.3.1.3 |
| bdregd | 1.3.6.1.4.1.22446.1.1.3.1.1 |
| bdmond | 1.3.6.1.4.1.22446.1.1.3.1.2 |
| bdscand | 1.3.6.1.4.1.22446.1.1.3.1.3 |
| bdmaild | 1.3.6.1.4.1.22446.1.1.3.1.4 |
| bdlogd | 1.3.6.1.4.1.22446.1.1.3.1.5 |
| bdlived | 1.3.6.1.4.1.22446.1.1.3.1.6 |
| bdsmtpd | 1.3.6.1.4.1.22446.1.1.3.1.7 |
| bdmilterd | 1.3.6.1.4.1.22446.1.1.3.1.8 |

## 16.3. The Bitdefender Logger Plugin

The Bitdefender Logger receives messages from various Bitdefender components and presents them to the user in various formats. It can log the messages to a file, forward them by email to a designated address or, using this plugin, it can send them to a SNMP server.

### 16.3.1. Requisitos

You will need a working SNMP server installed on the same or on some other machine. Please take a look at the Troubleshooting section below, because there are some glitches you have be aware of.

You will also need the following MIB files present in the `mibs` directory we have talked about before: `BITDEFENDER-ALERTS-MIB.txt`, `BITDEFENDER-NOTIFY-MIB.txt` and `BITDEFENDER-TRAP-MIB.txt`.

Regarding the SNMP protocol version, you can use `1`, `2c` or `3` with the following notes.

- Alerts of the `TRAP` type can be sent using the SNMP protocol versions `1` `2c` and `3`.
- Alerts of the `INFORM` type can be sent using the SNMP protocol versions `2c` and `3`.
- Protocol `3` needs the user and offers authentication and encryption.
- Protocols `1` and `2c` need no user, they use the `community` string, which is `public` by default.

## 16.3.2. Configuración

The messages sent to the SNMP server are received by the **snmptrapd** daemon. We need to configure it. But first, please make sure the SNMP services are not running.

We need a username for the SNMP version 3 protocol. If you want to use version 1 or 2c, you do not need the user and you can skip the following paragraphs.

Let's use the same `bitdefender` username as above. Make sure there is this line in the `/etc/snmp/snmpd.conf` file.

```
rwuser bitdefender
```

Thus we specify that this user who is not yet defined will have read and write access. Add this line at the end of the `/var/net-snmp/snmptrapd.conf` file and remember the passwords should be longer than 8 characters. If the file does not exist, just create it.

```
createUser -e 0xBD224466 bitdefender MD5 <authpass> DES <privpass>
```

If you plan to use the `INFORM` alerts, without need for the EngineID, you will have to add an user without specifying the EngineID. The user defined in the line above will not work, so add a new one.

```
createUser bitdefender_inform MD5 <authpass> DES <privpass>
```

Let's stop a while and explain this line. You are free to change anything in it with the only condition to reflect the changes in the Bitdefender configuration.

`-e 0xBD224466`
: This is the EngineID. It is mandatory for alerts of the `TRAP` type and optional for the `INFORM` type. The alert type should be specified in `/BDUX/LoggerDaemon/Plugins/SNMP/AlertType` registry key.

  The EngineID must also be specified in the Bitdefender registry at the `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityEngineID` key. If not used (it is optional when the alerts type is `INFORM`), the `SecurityEngineID` key must be empty.

`bitdefender`
: This is the user to create for authenticated SNMP v3. The same name should be declared in the `/etc/snmp/snmpd.conf` (please read above) and in the `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityName` registry key.

`MD5`
: The authentication protocol (`MD5` or `SHA1`) used for authenticated SNMP v3. The same value must be found in `/BDUX/LoggerDaemon/Plugins/SNMP/AuthProto` registry key.

<authpass>
: Set the authentication pass phrase used for authenticated SNMP v3 messages. The same value must be found in the `/BDUX/LoggerDaemon/Plugins/SNMP/AuthProtoPass` registry key.

`DES`
: Set the privacy protocol (`DES` or `AES`) used for encrypted SNMP v3 messages. The same value must be found in the `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityPrivProto` registry key.

<privpass>
: Set the privacy pass phrase used for encrypted SNMP v3 messages. The same value must be found in the `/BDUX/LoggerDaemon/Plugins/SNMP/SecurityPrivProtoPass` registry key.

This line will be replaced with another one, with encrypted passwords, when the **snmptrapd** daemon is started.

One more thing: you do not need to use all the parameters specified above for SNMP v3. You can use the authentication without encryption (the `SecurityLevel` key is

authNoPriv) or no authentication and no encryption (the SecurityLevel key is noAuthNoPriv). You have to modify the createUser line accordingly.

This would be the user. Now, let's get back to the /etc/snmp/snmpd.conf file and add some more lines. You might find them already in your file, but commented out. Uncomment them and set the correct values.

```
# trapsink: A SNMPv1 trap receiver
trapsink  localhost

# trap2sink: A SNMPv2c trap receiver
trap2sink  localhost

# informsink: A SNMPv2c inform (acknowledged trap) receiver
informsink  localhost public

# trapcommunity: Default trap sink community to use
trapcommunity  public

# authtrapenable: Should we send traps when authentication
#                 failures occur
authtrapenable  1
```

I think this is the moment to start the **snmpd** and **snmptrapd** daemons. If you get an error, please review the configuration.

## 16.3.3. Usabilidad

Now you can test the SNMP server. Here are some commands you may start with. The first one will send the TRAP alert that should be logged on syslog. Please note we use the EngineID.

```
# snmptrap-e 0xBD224466 -v 3 -m ALL -u bitdefender -l authPriv
           -a MD5 -A <authpass> -x DES -X <privpass> localhost 42
           coldStart.0
```

Another command sends an INFORM alert. In this case, there is no need to specify the EngineID and the user you have created must not have the EngineID. In our examples, we have created the bitdefender_inform user for this purpose. The alert will be logged on the syslog too.

```
# snmpinform-v 3 -m ALL -u bitdefender_inform -l authPriv -a MD5
            -A <authpass> -x DES -X <privpass> localhost 42
            coldStart.0
```

If you do not want to use the SNMP version 3 protocol, you can use the other two supported: 1 and 2c. In this case you do not need the username, all you have to know is the community string. This is `public` by default. For example, for version 2c, use this command.

```
# snmptrap-c public -v 2c -m ALL localhost 42 coldStart.0
```

If everything is all right and Bitdefender is properly configured (that means the registry keys fit the SNMP server configuration), all you have to do is to enable the plugin (if not already enabled) and try it by sending emails through the MTA. You will shortly see the report on the syslog of the machine running the SNMP server.

## 16.4. Resolución de Problemas

Due to some newly found bug in the net-snmp package, the `TRAP` feature does not work for net-snmp version 5.2.2 or newer with the SNMP version 3 protocol (but it works in version 5.2.1). This bug will hopefully be fixed by the net-snmp team soon.

For more information, please see the discussion from the following thread: http://sourceforge.net/mailarchive/forum.php?thread_id=9098786&forum_id=4959.

# Obtener Ayuda

# 17. Soporte

## 17.1. Support department

As a valued provider, BitDefender strives to offer its customers an unparalleled level of fast and accurate support. The Support Center listed below is continually updated with the newest virus descriptions and answers to common questions, so that you obtain the necessary information in a timely manner.

At BitDefender, dedication to saving customers' time and money by providing the most advanced products at the fairest prices has always been a top priority. Moreover, we think that a successful business is based on good communication and a commitment to excellence in customer support.

You are welcome to ask for support at support@bitdefender.com any time. For a prompt response, please include in your email as many details as you can about your Bitdefender, about your system and describe the problem as accurately as possible.

## 17.2. On-line help

### 17.2.1. Bitdefender Knowledge Base

The Bitdefender Knowledge Base is an online repository of information about Bitdefender products. It stores, in an easily accessible format reports on the results of the ongoing technical support and bug fixing activities of the Bitdefender support and development teams, along with more general articles about virus prevention, the management of Bitdefender solutions and detailed explanations, and many other articles.

The Bitdefender Knowledge Base is open to the public and freely searchable. This wealth of information is yet another way to provide Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Knowledge Base, as bug fix reports, workaround cheatsheets or informational articles to supplement product help files.

Puede acceder a Bitdefender Knowledge Base en cualquier momento desde la siguiente dirección http://www.bitdefender.es/businesshelp.

## 17.2.2. Bitdefender Unix Servers Mailing List

The Bitdefender mailing lists bring the latest information regarding security, offer on-line technical support and provide valuable feedback. They are grouped in the following categories.

- Technical Support.
- Product Announcements: bug-fixes, new features or versions, etc.
- Community feedback.

### Subscribe and Unsubscribe

In order to join the Bitdefender mailing lists, please undertake the following steps:

- Send a blank message to unix-mailservers-subscribe@bitdefender.com with the subject line `subscribe`.
- Confirm your subscription, validate your email address, by redirecting or forwarding the received email from Bitdefender to the same address, while leaving the message body unchanged.

To unsubscribe from the mailing list, send an empty mail with the subject `unsubscribe` to unix-mailservers-unsubscribe@bitdefender.com, and follow the received instructions.

### Submit a message

To post a message in the list, compose a new message and send it to unix-mailservers@bitdefender.com, with a subject line describing your topic and including all details in your message.

Below are the guidelines and rules of the Bitdefender discussion list:

- The official language of BitDefender mailing lists is English.
- Messages must be plain text, instead of HTML or Rich Text.
- All mails should have a short descriptive Subject line, specifying the product you are referring to.
- Necessary details must be included in the messages so that other list members can fully understand the situation.
- The posts may be moderated by the BitDefender Customer Service Department, if the message does not conform to standard and common-sense policies.

## 17.3. Online Forum

You can also visit our online forum. Please log in to take benefit of the fruitful discussions in the forum.

## 17.4. Información de Contacto

Efficient communication is the key to a successful business. For the past 10 years Bitdefender has established an indisputable reputation in exceeding the expectations of clients and partners, by constantly striving for better a communication. Please do not hesitate to contact us regarding any issues or questions you might have

### 17.4.1. Direcciónes

Departamento de ventas: comercial@bitdefender.es
Centro de soporte:http://www.bitdefender.es/businesshelp
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://www.bitdefender.es

### 17.4.2. Oficinas de Bitdefender

Las oficinas de Bitdefender están lista para responder a cualquier pregunta sobre sus áreas de operación, tanto comerciales como de asuntos generales. Sus direcciones y contactos están listados a continuación.

#### Norte América

**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
Web de AutoAyuda: http://www.bitdefender.de/site/KnowledgeBase/showMain/2/

## Reino Unido e Irlanda

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

## 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

# Apéndices

# A. Supported antivirus archives and packs

Bitdefender scans inside the most common types of archives and packed files, including, but not limited to the following.

## Supported archive types

Ace
Arc
Arj
bzip2
Cab
Cpio (clean+delete)
Gzip (clean+delete)
Ha
Imp
Jar
MS Compress
Lha (lzx)
Rar (including 3.0)
Rpm (clean+delete)
Tar (clean+delete)
Z
Zip (clean+delete)
Zoo

## Installation packers

Inno (Inno Installer)
Instyler
VISE (viza.xmd)
InstallShield (ishield.xmd)
Nullsoft Installer (NSIS)
Wise Installer

## Mail archives

Dbx (Outlook Express 5, 6 mailboxes)
Mbx (Outlook Express 4 mailbox)
Pst (Outlook mailboxes, supports clean and delete)
Mime (base64, quoted printable, plain) supports clean and delete
Mbox (plain mailbox - Linux and Netscape)
Hqx (HQX is a format used for mail attachments on Mac)
Uudecode
Tnef (a Microsoft format in which some properties of the attachments are encoded, and which can contain scripts)

## Supported packers

ACProtect / UltraProtect
PELock NT

ASPack (all versions)
Bat2exec (1.0, 1.2, 1.3, 1.4, 1.5, 2.0)
Yoda's Cryptor
CExe
Diet
DxPack
Dza
Patcher
ECLIPSE
Exe32Pack (1.38)
ExePack
ExeStealth
JdProtect
Lzexe
Mew
Molebox (2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.8)
Morphine
Neolite
PC/PE Shrinker 0.71
PCPEC
PE Crypt 32 (1.02 (a,b,c)
PE PACK\CRYPT
PeBundle
pecompact (up to 1.40 beta 3)
PeDiminisher
Pencrypt (3.1, 4.0a, 4.0b)
PePack (all versions)
Perplex
PeShield
PeSpin
Petite (all versions)
Pex
PhrozenCrew PE Shrinker (0.71)
PkLite
PKLITE32 (1.11)
Polyene
RelPack
Rjcrush (1.00, 1.10)
Shrinker (3.3, 3.4)
VgCrypt
Stpe
Telock (all versions)
T-pack
Ucexe
UPolyx
UPX (all versions)
WWPACK32 (1.0b9, 1.03, 1.12, 1.20)
Wwpack (3.01, 3.03, 3.04, 3.04PU, 3.05, 3.05PU)
Xcomor (0.99a, 0.99d, 0.99f (486), 0.99h, 0,99i)

## Otros

Chm (contains html which can be infected)
Iso (CD images)
Pdf
Rtf
Mso (contains compressed OLE2 files, this way macros are saved in case a Doc is saved as html)
Swf (extracts certain fields that contain various commands; these are scanned by other plug-ins, for ex: SDX)
Bach (extracts debug.exe scripts on the basis of heuristic methods)
Omf (object file)

# B. Alert templates

All alerts can be customized. Bitdefender provides a template mechanism to generate the alert messages. These templates are plain text files containing the desired notice and certain variables, keywords, which will be replaced with their proper values during the alert generation.

## B.1. Variables

The variables and their meaning are described in the table below.

| *Variable* | *Descripción* |
|---|---|
| `${BitDefender}` | This variable will be replaced with the *BitDefender* string. |
| `${RealSender}` | El remitente del mensaje de correo electrónico, tomada de el comando SMTP `CORREO DE:` |
| `${RealReceivers}` | Los destinatarios del mensaje de correo electrónico, tomada de el comando SMTP `RCPT DE:` |
| `${HeaderSender}` | El remitente del correo electrónico, desde el encabezado del e-mail `De:` |
| `${HeaderReceivers}` | Los receptores del mensaje, de la encabezados por email `Para:` y `Cc:`. |
| `${Subject}` | The subject of the alert email. |
| `${Object}` | The object containing the malware. |
| `${Action}` | The action taken on the object. |
| `${Virus}` | The virus name. |
| `${Status}` | The status of the object, namely `Infected`, `Suspected`, `Unknown`. |
| `${Days}` | The remaining period until key expiration. |

***The variable ${BitDefender}***
It is mandatory to include the variable `${BitDefender}` in your custom template. If it is not found, the module will use the built-in template instead.

Estas variables se pueden combinar de cualquier forma dentro de las listas de objetos con el fin de generar una plantilla a medida, sin importar el idioma. De forma predeterminada, las plantillas se almacenan en el directorio `/opt/Bitdefender/share/templates/language`. Para todos los idiomas soportados, hay entradas subdirectorio, como `en`, `ro`, `de`, `fr`, `hu`, `es`. Dentro de los subdirectorios de idiomas, se encuentran los archivos de plantilla, sugerente nombre.

En cuanto a las alertas por correo, las plantillas involucradas son las siguientes: `MailServerAlert.tpl`, `KeyHasExpiredAlert.tpl`, `KeyWillExpireAlert.tpl`, `ReceiverAlert.tpl` and `SenderAlert.tpl`.

***El nombre de la plantilla***
Usted no tiene que mantener el nombre de archivo predeterminado o ubicación. Lo único obligatorio es que se refieren en consecuencia dentro del Registro de Bitdefender, bajo su tecla correspondiente.

# B.2. Resultados de las muestras

Buscando en los archivos antes mencionado, se podría confundirse acerca de la estructura. Estos son los valores por defecto para el idioma Inglés y los posibles resultados al generar los pies de página.

## B.2.1. Alerta MailServer

Esta es la alerta que el administrador de correo recibirá cuando un mensaje es infectado. Las variables que pueden ser utilizadas son las siguientes.

- `${RealSender}`
- `${RealReceivers}`
- `${HeaderSender}`
- `${HeaderReceivers}`
- `${Subject}`
- `${Object}`
- `${Action}`
- `${Virus}`
- `${Status}`
- `${BitDefender}`

La plantilla predeterminada es la siguiente:

```
Subject: System info

${BitDefender} found an infected object in a message:

Real sender: ${RealSender}
Real receivers: ${RealReceivers}
From: ${HeaderSender}
To: ${HeaderReceivers}
Subject: ${Subject}
Virus: ${Virus}
http://www.bitdefender.com/vfind/?q=${virus}
Object: ${Object}
Status: ${Status}
Action: ${Action}

Thank you for choosing ${BitDefender}
http://www.bitdefender.com/
```

Este expandirá el siguiente mensaje (proporcionado como un ejemplo).

```
Subject: System info

BitDefender found an infected object in a message:

Real sender: <sender@example.com>
Real receivers: <receiver@example.com>
From: The Sender <sender@example.com>
To: The Receiver <receiver@example.com>
Subject: klez
Virus: Win32.Klez.A@mm
http://www.bitdefender.com/vfind/?q=Win32.Klez.A@mm
Object: /tmp/bdnp.milter.qf2aqW=>[Subject: klez]
Status: Infected
Action: Deleted

Thank you for choosing BitDefender
http://www.bitdefender.com/
```

## B.2.2. Envía alerta

This is the alert the sender of the original email will receive when an infected message he has sent is found. Variables that could be used:

- ${RealReceivers}
- ${HeaderReceivers}
- ${Subject}
- ${Object}
- ${Action}
- ${Virus}
- ${Status}
- ${BitDefender}

La plantilla predeterminada es la siguiente:

```
Subject: Virus Warning!

${BitDefender} found an infected object
in a message that was sent from your address

Real receiver: ${RealReceivers}
To: ${HeaderReceivers}
Subject: ${Subject}
Virus: ${Virus}
http://www.bitdefender.com/vfind/?q=${virus}
Object: ${Object}
Status: ${Status}
Action: ${Action}

For more information about ${BitDefender}
please visit http://www.bitdefender.com/
```

Este expandirá el siguiente mensaje (proporcionado como un ejemplo).

```
Subject: Virus Warning!

BitDefender found an infected object
in a message that was sent from your address

Real receivers: <receiver@example.com>
To: The Receiver <receiver@example.com>
Subject: klez
Virus: Win32.Klez.A@mm
http://www.bitdefender.com/vfind/?q=Win32.Klez.A@mm
Object: /tmp/bdnp.milter.qf2aqW=>[Subject: klez]
```

```
Status: Infected
Action: Deleted

For more information about BitDefender
please visit http://www.bitdefender.com/
```

## B.2.3. Receptor de alerta

This is the alert the receiver of the original email will get when an infected message having reached him is found. Variables that could be used:

- ${RealSender}
- ${HeaderSender}
- ${Subject}
- ${Object}
- ${Action}
- ${Virus}
- ${Status}
- ${BitDefender}

La plantilla predeterminada es la siguiente:

```
Subject: Virus warning!

${BitDefender} found an infected object
in a message addressed to you:

Real sender: ${RealSender}
From: ${HeaderSender}
Subject: ${Subject}
Virus: ${Virus}
http://www.bitdefender.com/vfind/?q=${virus}
Object: ${Object}
Status: ${Status}
Action: ${Action}

For more information about ${BitDefender}
please visit http://www.bitdefender.com/
```

Este expandirá el siguiente mensaje (proporcionado como un ejemplo).

```
Subject: Virus warning!

BitDefender found an infected object
in a message addressed to you:

Real sender: <sender@example.com>
From: The Sender <sender@example.com>
Subject: klez
Virus: Win32.Klez.A@mm
http://www.bitdefender.com/vfind/?q=Win32.Klez.A@mm
Object: /tmp/bdnp.milter.qf2aqW=>[Subject: klez]
Status: Infected
Action: Deleted

For more information about BitDefender
please visit http://www.bitdefender.com/
```

## B.2.4. KeyWillExpire Alert

This is the alert the system administrator will receive when the license key is about to expire. Variables that could be used:

- `${Days}`
- `${BitDefender}`

La plantilla predeterminada es la siguiente:

```
Subject: Registration info

Your ${BitDefender} license will expire in ${Days} days!

http://www.bitdefender.com
```

## B.2.5. KeyHasExpired Alert

This is the alert the system administrator will receive when the license key has expired. The variables that could be used are the next ones.

- `${BitDefender}`

La plantilla predeterminada es la siguiente:

```
Subject: Registration Error

Your ${BitDefender} license has expired!

http://www.bitdefender.com
```

# C. Plantillas pie de página

Bitdefender apoya una personalización completa de los pies de página se adjuntan a los mensajes de correo electrónico e indicando si están limpios o infectados, así como información adicional detallada acerca de la infección. Estos pies son configurables por el usuario: basado en plantillas, que incluyen varias palabras clave, llamadas *variables*, que será sustituido por Bitdefender notificar módulo con sus valores correspondientes.

## C.1. Variables

The variables and their meaning are described in the table below.

| *Variable* | *Descripción* |
|---|---|
| `${BitDefender}` | This variable will be replaced with the *BitDefender* string. |
| `${begin}`, `${end}` | Estos son los marcadores de la frontera lista de objetos. Múltiples listas de objetos están permitidos, siempre que no se imbricados. |
| `${object}` | El archivo u objeto encontrado infectados o sospechosos de estar infectados. |
| `${status}` | The status of the object, namely `Infected`, `Suspected`, `Unknown`. |
| `${virus}` | The virus name. If you want to know more about the reported virus, use the Virus Encyclopedia. |
| `${action}` | Las medidas adoptadas por el objeto, a saber `desinfectado`, `eliminado`, `cuarentena`, `bandonado`, `Rechazado` , `ignorado`. Normalmente `Abandonado` y `Rechazado` nunca debe aparecer, ya que este tipo de mensajes se pierden. |

***The variable ${BitDefender}***
Es obligatorio incluir variables `${BitDefender}` en su plantilla personalizada. Si no se encuentra, el módulo usará la plantilla integrada en su lugar.

Estas variables se pueden combinar de cualquier forma dentro de las listas de objetos con el fin de generar una plantilla a medida, sin importar el idioma. De forma predeterminada, las plantillas se almacenan en el directorio

`/opt/Bitdefender/share/templates/language`. Para todos los idiomas soportados, hay entradas subdirectorio, como `en`, `ro`, `de`, `fr`, `hu`, `es`. Dentro de los subdirectorios de idiomas, se encuentran los archivos de plantilla, sugerente nombre.

En cuanto a los pies de página de correo electrónico, la plantilla en cuestión es `bd.tpl`.

***El nombre de la plantilla***
Usted no tiene que mantener el nombre de archivo predeterminado o ubicación. Lo único obligatorio es que se refieren en consecuencia dentro del Registro de Bitdefender, bajo su tecla correspondiente.

# C.2. Resultados de las muestras

Buscando en el archivo antes mencionado, se podría confundirse acerca de la estructura. Estos son los valores por defecto para el idioma Inglés y los posibles resultados al generar los pies de página.

***Codificación de texto***
Para evitar resultados extraños de salida, el texto debe ser escrito utilizando el conjunto de caracteres sin formato ASCII, ya que no hay conversión de codificación charset.

La plantilla predeterminada es la siguiente.

```
------------------------------------------------------------
This mail was scanned by ${BitDefender}
For more information please visit http://www.bitdefender.com

${begin:virus}
Found virus:
        Object: ${object}
        Name:   ${virus}
        Status: ${status}
        Action: ${action}

${end}
------------------------------------------------------------
```

## C.2.1. Limpio

Cuando el mensaje está limpio, el pie de página como se indica a continuación.

```
------------------------------------------------------------
This mail was scanned by BitDefender
For more informations please visit http://www.bitdefender.com
------------------------------------------------------------
```

## C.2.2. Omitidos

Cuando un correo electrónico infectado se encuentra y la acción fue ignorar ese objeto, el resultado es el siguiente.

```
------------------------------------------------------------
This mail was scanned by BitDefender
For more information please visit http://www.bitdefender.com

Found virus:
        Object: (MIME part)=>(application)=>word/W97M.Smac.D
        Name:   W97M.Smac.D
        Status: Infected
        Action: Ignored
------------------------------------------------------------
```

## C.2.3. Desinfectados

Por último, cuando un correo infectado fue encontrado y limpiado, el resultado será el siguiente.

```
------------------------------------------------------------
This mail was scanned by BitDefender
For more information please visit http://www.bitdefender.com

Found virus:
        Object: (MIME part)=>(application)=>word/W97M.Story.A
        Name:   W97M.Story.A
        Status: Infected
        Action: Disinfected
------------------------------------------------------------
```

# Glosario

**ActiveX**

ActiveX is a model for writing programs so that other programs and the operating system can call them. The ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

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

**Actualizar**

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 de actualización que le permite comprobar manualmente si hay actualizaciones, o bien hacer una actualización automática del producto.

**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.

**Archivo Comprimido**

Disco, cinta o directorio conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

**Archivo de informe**

Es un fichero que lista las acciones ocurridas. BitDefender mantiene un archivo de informe que incluye la ruta analizada, las carpetas, el número de archivos comprimidos y no comprimidos analizados, así como cuántos archivos infectados o sospechosos se encontraron.

**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**

Es una brecha de seguridad dejada intencionalmente por los diseñadores o los administradores. La motivación no es siempre maléfica; algunos sistemas operativos funcionan con unas cuentas privilegiadas, concebidas para el uso de los técnicos del service o para los responsables con el mantenimiento del producto, de parte del vendedor.

**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.

**Descargar**

Para copiar información (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.

**E-mail**

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

**Elementos en 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**

Es la abreviatura de Navegador Web, una aplicación que se utiliza para ubicar y visualizar páginas web. Los dos navegadores más populares son Netscape Navigator y Microsoft Internet Explorer. Ambos son navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos pueden mostrar información multimedia: sonido e imágenes, aunque requieren 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.

Muchos sistemas operativos utilizan extensiones de nombres de archivo, por ejemplo, Unix, VMS y MS-DOS. Normalmente son de una a tres letras (algunos viejos SO no soportan más de tres). Por ejemplo "c" para código fuente C, "ps" para PostScript, o "txt" para texto plano.

**Falso positivo**

Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho 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 añadir a otros programas.

**Heurístico**

Un método basado en reglas para identificar nuevos virus. Este método de análisis no se basa en firmas de virus específicas. La ventaja de un análisis heurístico es que no le engaña una nueva variante de un virus existente. Sin embargo, puede que informe ocasionalmente de códigos sospechosos en programas normales, generando el llamado "falso positivo".

**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.

**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 con aplicaciones que pueden parecer un virus, y por consiguiente, no genera falsas alarmas.

**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.

**Protocolo de Control de Transmisión/Protocolo de Internet** (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.

**Protocolo de Internet** (IP)

Un protocolo enrutable dentro del protocolo TCP/IP que es responsable del direccionamiento IP, el enrutamiento y el fragmentado y re-ensamblado de los paquetes IP.

**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.

**Ruta**

Las rutas exactas de un archivo en un equipo. Esta suma de información 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.

**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 viene de la historia de la Ilíada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como oferta de paz. Pero después de que los troyanos arrastraran el caballo dentro de las murallas de su ciudad, los soldados griegos salieron del vientre hueco del caballo y abrieron las puertas de la ciudad, permitiendo a sus compatriotas entrar y capturar 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 hallado en un disco fijo o en una disquetera. Al intentar de relanzar el sistema desde un disco infectado con un virus de boot, el virus se instalará activo en la memoria. Cada vez que usted trate de relanzar el sistema desde este punto en adelante, tendrá el virus activo en la memoria.

**Virus de macro**

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

Estas aplicaciones permiten introducir un macro en un documento y también que el 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.