



PANDA **CLOUD OFFICE PROTECTION**

Guía Avanzada de Administración



Aviso de copyright

© Panda Security 2013. Todos los derechos reservados.

Ni la documentación, ni los programas a los que en su caso acceda, pueden copiarse, reproducirse, traducirse o reducirse a cualquier medio o soporte electrónico o legible sin el permiso previo por escrito de Panda Security, C/ Gran Vía Don Diego López de Haro, 4, 48001, Bilbao (Bizkaia) España.

Marcas registradas

Windows Vista y el logo de Windows son marcas o marcas registradas de Microsoft Corporation en los EEUU y/o otros países. Otros nombres de productos son marcas registradas de sus respectivos propietarios.

© Panda Security 2013. Todos los derechos reservados.

PCOP-650



¿A quién va dirigida esta guía?	9
Introducción	9
La protección	10
La instalación	11
Seguridad desde la nube & Inteligencia Colectiva	11
¿Qué es "la nube"?	11
¿Qué es la Inteligencia Colectiva?	12
¿Cómo es la detección con la Inteligencia Colectiva?	12
Tecnología Anti-Exploit	12
Información y consultas	13
Información, consultas y servicios	13
Otros productos y servicios	15
Requisitos y URLs necesarias	16
Requisitos de los equipos	16
URL's necesarias	16
Conceptos clave	17
Acceso a la consola Web	25
La consola Web	25



Preferencias	26
Gestión de licencias	28
Tipos de clientes	28
Alertas relacionadas con las licencias	29
Anulación de licencias	30
Añadir licencias mediante código de activación	31
Gestión de cuentas	33
Introducción a la gestión de cuentas	33
Delegar la gestión de una cuenta	34
Unificar cuentas	35
Creación y gestión de usuarios	39
Tipos de permisos	40
Permiso de control total	41
Permiso de administrador	43
Permiso de monitorización	45
Configuración de la protección	45
Introducción	45
Perfil por defecto	47
Crear / Copiar un perfil	48
Crear un perfil	48



Copiar un perfil	49
Configuración general del perfil	50
Pestaña <i>Principal</i>	50
Pestaña Actualizaciones	51
Pestaña Análisis programados	53
Pestaña <i>Alertas</i>	54
Pestaña <i>Aplica a</i>	54
Edición de perfil - opciones avanzadas	58
Configuración de la protección antivirus	60
Pestaña <i>Archivos</i>	61
Pestaña <i>Correo</i>	61
Pestaña <i>Web</i>	62
Análisis locales	63
Opciones avanzadas antivirus - protección de archivos	64
Opciones avanzadas antivirus - protección de correo	65
Configuración de la protección firewall	66
Introducción a la configuración del firewall	66
Administración del firewall desde cliente	67
Administración centralizada del firewall	68
Configuración del control de dispositivos	71
Para activar el control de dispositivos	72



Configuración de la protección para servidores Exchange	73
Introducción	73
Protección antivirus para servidores Exchange	74
Protección anti-spam para servidores Exchange	78
Configuración del control de acceso a páginas Web	81
Denegar el acceso a páginas Web.....	82
Denegar el acceso a páginas de categoría desconocida	82
Creación de grupos	84
Asignar equipos a un grupo	85
Instalación de la protección	86
Recomendaciones previas a la instalación	86
Instalación rápida	87
Casos de instalación	88
Modos de instalación	89
Desinstalación de otras protecciones	92
Desinstalación automática	92
Desinstalación manual.....	93
Estado de la protección	93
Introducción	93
Licencias y detecciones.....	94



Control de accesos a páginas Web	98
Análisis programados	99
Monitorización de los equipos	104
Introducción	104
Equipos protegidos	105
Equipos desprotegidos	107
Detalle de equipos	108
Acceso remoto a los equipos	109
Comportamiento de las herramientas de acceso remoto	111
Búsqueda de equipos desprotegidos.....	113
Visualización y resultado de la búsqueda	114
Cuarentena	116
Archivos excluidos del análisis	118
Informes	119
Tipos de informes	119
Generar informes	121
Visualizar informes	123
Desinstalación	124
Tipos de desinstalación	124
Desinstalación local	125



Desinstalación centralizada	125
Desinstalación remota	127
Solución de Problemas – Preguntas Frecuentes	131
Solución de problemas	131
Preguntas frecuentes	131
Anexo 1: línea de comandos para operaciones básicas remotas	151
Instalación	151
Verificación de la instalación de la protección	156
Desinstalar Panda Cloud Office Protection	157
Actualización del fichero de firmas	160
Actualizar la configuración	160
Obtener la fecha de los ficheros de firmas	160
Obtener el estado del Antivirus, Firewall y el Control de dispositivos	163
Anexo 2: Proceso de despliegue de la protección	168
El agente de administración	168
Funcionalidad Peer To Peer (P2P)	169
Proxy dinámico	172
Proxy estático	174
Despliegue de Panda Endpoint Agent	175
Despliegue de Panda Endpoint Protection	194
Anexo 3: Descubrimiento automático de equipos	203
Datos a tener en cuenta a la hora de crear una tarea de búsqueda	203



Panda Cloud Office Protection

Secuencia de acciones de la tarea de búsqueda y correspondencia con el estado de la tarea	205
Casos en los que el servidor puede NO tener constancia de la finalización de una tarea de descubrimiento	209
Anexo 4: Panda Cloud Office Protection para Linux	211
Prerrequisitos	211
Instalación	215
Despliegue	216
Procesos	216
Comunicación a través de proxy	218
Análisis	220
Lanzamiento manual de análisis	223
Informes de detección	224
Actualizar a versión superior de Panda Cloud Office Protection (Upgrades)	225
Desinstalación	226



¿A quién va dirigida esta guía?

Esta Guía Avanzada de Administración está dirigida a administradores de red que desean mantener la red informática de su empresa libre de virus y otras amenazas. La guía profundiza en los aspectos de instalación, configuración y monitorización de la protección, y añade información de utilidad sobre aspectos como el control de los equipos mediante herramientas de acceso remoto.

En los anexos se detallan las operaciones realizables bajo línea de comandos, el árbol de despliegue de la protección, las preguntas frecuentes y diversos ejemplos con recomendaciones de instalación en función de diferentes necesidades.

Toda la información presente en esta guía complementa el resto de la documentación básica que puede usted encontrar en el área de documentación de producto, en

<http://www.pandasecurity.com/spain/enterprise/downloads/docs/product/managedprotection/>, especialmente en las ayudas web y en las guías de administración básica.



NOTA IMPORTANTE

Para obtener información acerca de la protección en equipos con sistema operativo Windows 2000, Windows XP 32bits SP0 / SP1, Windows XP 64bits, Windows Server 2003 32bits SP0, Windows Server 2003 R2 32bits SP0, Windows Server 2003 64bits o Windows Server 2003 R2 64 bits, consulte la [Guía Avanzada de Administración para versiones anteriores a las 6.0](#) en el área de documentación del producto.

Esperamos que esta guía avanzada de administración le resulte útil.

Introducción

Panda Cloud Office Protection es una solución completa de seguridad concebida para que usted pueda proteger su red informática y gestionar la seguridad de manera sencilla y en modo on line. La protección que proporciona neutraliza [spyware](#), [trojanos](#), [virus](#) y cualquier otra amenaza dirigida contra sus equipos.

Sus principales características son:



Panda Cloud Office Protection

- ☁ Máxima protección para PCs, portátiles y servidores.
- ☁ Fácil de instalar, gestionar y mantener a través de su consola Web.
- ☁ Gestión y organización basada en perfiles de protección y grupos de equipos.

El centro de gestión de Panda Cloud Office Protection es la consola Web, desde donde usted podrá:

Configurar la protección, distribuirla e instalarla en los equipos.

Monitorizar el estado de la protección en los equipos.

Extraer informes sobre el estado de la seguridad y las amenazas detectadas.

Gestionar las detecciones realizadas y saber en todo momento qué se ha detectado, cuándo y en qué equipo.

Configurar la cuarentena de elementos sospechosos.

Si desea disfrutar de otros servicios, como la protección de correo electrónico Panda Cloud Email Protection, el servicio de seguridad para el tráfico Web Panda Cloud Internet Protection o la auditoría de malware on line bajo demanda MalwareRadar, haga clic en el menú **Otros productos** y seleccione el botón correspondiente.

La protección

De acuerdo con las necesidades de protección de sus equipos, usted podrá crear [perfiles](#) y determinar cuál será el comportamiento de la protección ([antivirus](#), [firewall](#), [control de dispositivos](#), [servidores Exchange](#) y [control de accesos a páginas Web](#)) para el perfil que está creando. A continuación, podrá asignar dicho perfil a los [grupos](#) de equipos que quiere proteger.



La protección para servidores Exchange solo podrá activarla si ha adquirido licencias de Panda Cloud Office Protection Advanced

Configuración de la protección

Usted puede configurar la protección instalada en los equipos antes o después de la instalación, pero es recomendable que dedique un tiempo a analizar en profundidad cuáles son las necesidades de protección de su red.



Estas necesidades pueden variar de unos equipos a otros o también pueden ser las mismas para todos ellos. En consecuencia, podrá necesitar crear perfiles nuevos o le bastará con la configuración por defecto que Panda Cloud Office Protection proporciona.

La instalación

Antes de instalar la protección, le invitamos a consultar las [recomendaciones previas a la instalación](#), donde encontrará información importante sobre cuestiones que tienen que ver con el proceso de instalación y desinstalación.

A lo largo de todo el proceso de configuración e instalación de la protección, usted será quien decidirá qué equipos desea proteger, con qué tipo de protección y de qué manera desea instalar dicha protección en los equipos.

Esperamos que todas las indicaciones que encontrará a lo largo de esta ayuda le resulten útiles.

Seguridad desde la nube & Inteligencia Colectiva

¿Qué es "la nube"?

La computación en la nube (*Cloud computing*) es una tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.

Panda Cloud Office Protection se sirve de la nube conectándose a los servidores de Inteligencia Colectiva y así proteger su PC desde el primer momento, aumentando la capacidad de detección y evitando penalizar el rendimiento del equipo. Ahora todo el conocimiento está en la nube y, gracias a Panda Cloud Office Protection, puede usted beneficiarse de ello.



¿Qué es la Inteligencia Colectiva?

La Inteligencia Colectiva es una plataforma de seguridad creada por Panda Security que ofrece un alto nivel de protección en tiempo real, aumentando exponencialmente la capacidad de detección de Panda Cloud Office Protection.

¿Cómo es la detección con la Inteligencia Colectiva?

La Inteligencia Colectiva consta de servidores que clasifican y procesan de forma automática toda la información que la comunidad de usuarios proporciona sobre las detecciones que se han producido en sus equipos.

Panda Cloud Office Protection realiza consultas a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección y sin afectar negativamente al consumo de recursos de los equipos.

Cuando un nuevo ejemplar de malware es detectado en el equipo de un miembro de la comunidad de usuarios, Panda Cloud Office Protection se encarga de enviar la información necesaria a los servidores de Inteligencia Colectiva alojados en la nube, de forma totalmente automática y anónima.

La información es procesada por dichos servidores, entregando una solución no sólo al usuario afectado, sino también al resto de usuarios de la comunidad, en tiempo real. De ahí el nombre de Inteligencia Colectiva.

Sin lugar a dudas, en el contexto actual de crecimiento continuo del malware, la Inteligencia Colectiva y los servicios alojados y servidos desde la nube vienen a complementar a las actualizaciones tradicionales para afrontar con éxito y anticipación la enorme cantidad de amenazas que surgen en la actualidad.

Tecnología Anti-Exploit

Panda Security ha desarrollado una nueva tecnología, denominada Anti-Exploit, que refuerza sus soluciones de seguridad de manera muy importante y que posibilita



detectar virus que ninguna otra compañía de seguridad está detectando.

La tecnología Anti-Exploit detecta y neutraliza el malware que explota vulnerabilidades de día cero (Java, Adobe , MS Office ..) como Blackhole o redkit antes de que infecte el ordenador.

La clave es utilizar las tecnologías heurísticas con gran capacidad de detección. Para ello, la nueva protección Anti-Exploit de Panda Cloud Office Protection Advanced analiza el comportamiento de los exploits en lugar de su morfología.

Panda Cloud Office Protection Advanced utiliza múltiples sensores para enviar información a la [Inteligencia Colectiva](#) sobre el comportamiento de archivos sospechosos que intentan explotar vulnerabilidades de día 0 para infectar equipos informáticos.

Esta información permite actualizar constantemente las tecnologías proactivas incluidas en los productos de Panda Security mediante actualizaciones en caliente en [la nube](#).

En definitiva, Panda Cloud Office Protection Advanced detecta y neutraliza este tipo de malware antes de que se haya identificado y antes incluso de que se haya creado, protegiendo a los usuarios frente a nuevas variantes de malware.

Información y consultas

Información, consultas y servicios

Junto a los productos, Panda Security pone a su disposición ayudas y documentación con la que podrá ampliar información, resolver dudas, acceder a las últimas actualizaciones y beneficiarse de otros servicios. Además, usted podrá estar al tanto de la actualidad y las novedades sobre seguridad informática. Visite la Web de Panda Security y acceda a toda la información que necesita.



Enlaces de interés

- [Página principal](#): Toda la información de Panda Security a su disposición.
- [Documentación](#): Encontrará la documentación actualizada de los productos y otras publicaciones de interés.
- [Soporte técnico](#): Resuelva sus dudas sobre infecciones, [virus](#), productos y servicios de Panda Security a cualquier hora del día y cualquier día del año, con información y ayuda continua y completamente actualizada.
- [Software de evaluación](#): Panda Security le proporciona software de evaluación para que usted pruebe gratuitamente el producto que desee.
- [Productos](#): Consulte las características de todos los productos de Panda Security. También puede adquirirlos y probarlos sin compromiso.

Servicios de Panda Cloud Office Protection

Panda Cloud Office Protection es sinónimo de protección permanente contra todo aquello que amenace la seguridad de su red informática. Con Panda Cloud Office Protection, será usted quien estará al tanto en todo momento del estado de la seguridad de sus equipos y quien dispondrá cuándo, cómo y de qué manera protegerlos. Todo ello de forma sencilla.

Además de esta ayuda en la que encontrará la información que necesita para sacar el máximo rendimiento a su protección, Panda Security le proporciona otros servicios. Son valores añadidos al producto que usted ha adquirido y que le permitirán contar, desde el primer momento, con el asesoramiento y la última tecnología que, en materia de seguridad, Panda Security aplica a sus productos.

Los servicios que ofrece Panda Cloud Office Protection son:

- [Actualizaciones diarias del archivo de identificadores](#).
- [Soporte técnico especializado](#) tanto telefónico como vía e-mail.
- Actualización general de Panda Cloud Office Protection: nuevas características, mejoras en su capacidad de detección, etc.
- Documentación: Acceso a la [Guía avanzada de administración](#).



Otros productos y servicios

Desde la consola Web de Panda Cloud Office Protection, usted puede acceder a otros productos y servicios que le permitirán, entre otras cosas, realizar auditorías de seguridad y extremar las medidas de seguridad sobre el correo electrónico.

Servicios

Haga clic en el vínculo **Servicios**, situado en la parte inferior de la consola Web. Desde la ventana **Servicios**, podrá enviar sugerencias a Panda Security y acceder al área de ayudas en la Web, donde encontrará las respuestas a las dudas que pueda tener sobre Panda Cloud Office Protection y todo el resto de información y utilidades que Panda Security pone a su disposición.

Auditorías MalwareRadar

En la pantalla principal de la consola Web, haga clic en la pestaña **Otros servicios**. Si desea realizar una auditoría de malware en su red informática, puede hacerlo mediante MalwareRadar. Se trata de un servicio de auditoría on line bajo demanda que detecta y desinfecta [malware](#), especialmente el de última generación, que puede pasar desapercibido para los sistemas de protección tradicionales.

Para iniciar la auditoría, haga clic en el botón **Acceder a MalwareRadar**.

Limpieza de correo electrónico

Como propietario de licencias de Panda Cloud Email Protection, puede poner en marcha el sistema de limpieza de correo electrónico basado en la nube, de mínimo impacto sobre sus equipos y máxima fiabilidad. Haga clic en la pestaña **Otros productos** y utilice el botón correspondiente para acceder a la consola Web de Panda Cloud Email Protection, desde la que poner en marcha las medidas de limpieza.

Si no dispone de licencias, puede acceder a la página de registro y probar la versión de evaluación.



Gestión de la seguridad para el tráfico Web

Panda Cloud Internet Protection garantiza la seguridad de los accesos a Internet y una gestión correcta del tráfico Web de su red corporativa. Utilice el botón correspondiente para acceder a la versión de prueba.

Si dispone de licencias, utilice el botón correspondiente para acceder a la consola. En caso contrario, puede acceder a la versión de prueba haciendo clic en la pestaña **Otros productos** y utilizando el botón correspondiente.

Requisitos y URLs necesarias

Requisitos de los equipos

Panda Cloud Office Protection ha sido concebido como la solución óptima para proteger su red informática, pero para poder extraer todo su potencial y disfrutar al máximo de sus funcionalidades, los equipos que intervienen en el proceso de acceso, instalación, configuración y despliegue de la protección han de reunir una serie de requisitos.

Si desea conocer al detalle los requisitos correspondientes a los diferentes equipos, haga clic [aquí](#). Encontrará toda la información necesaria además de accesos rápidos y directos a todo lo que necesita saber sobre Panda Security y sus productos.

URL's necesarias

Para acceder a los servidores de Panda Cloud Office Protection y poder descargar las actualizaciones, es necesario que al menos uno de los equipos de la subred tenga acceso a una serie de páginas web. Haga clic [aquí](#) para acceder al listado de URL's necesarias.



Nota: Es necesario que habilite los puertos (intranet del cliente) TCP 18226 y UDP



21226 para una correcta comunicación entre los agentes de administración de Panda Cloud Office Protection.

Conceptos clave

Adaptador de red

El adaptador de red permite la comunicación entre los diferentes aparatos conectados entre sí y también permite compartir recursos entre dos o más equipos. Tienen un número de identificación único.

Adware

Programa que automáticamente ejecuta, muestra o baja publicidad al PC, una vez instalado o mientras se está utilizando.

Agente

Agente encargado de las comunicaciones entre los equipos administrados y los servidores de Panda Cloud Office Protection, y de la gestión de los procesos locales.

Análisis heurístico genético

El análisis heurístico genético analiza los elementos sospechosos del software malintencionado en base a unos "genes digitales" representados por unos pocos cientos de características de cada archivo que es analizado.

Así se determina el potencial que el software detectado tiene para llevar a cabo acciones maliciosas o dañinas cuando se ejecuta en un ordenador, y si se trata de un virus, un spyware, un troyano, un gusano, etc.



Antivirus

Programas cuya función es detectar y eliminar virus informáticos y otras amenazas.

Archivo de identificadores

Es el fichero que permite a los antivirus detectar las amenazas. También es conocido con el nombre de Fichero de Firmas.

Broadcast

Area lógica en una red de equipos en la que cualquiera de ellos puede transmitir directamente a otro equipo en el dominio broadcast sin precisar ningún dispositivo de encaminamiento.

Consola Web de cliente

Mediante la consola Web, usted puede configurar, distribuir y gestionar la protección a todos los ordenadores de su red. También podrá conocer en todo momento el estado de la seguridad de su red informática, y obtener e imprimir los informes que desee.

Cuarentena

La cuarentena es la situación en la que se almacenan contenidos sospechosos de ser maliciosos o no desinfectables, así como el spyware y herramientas de hacking detectadas.

Dialer

Se trata de un programa que marca un número de tarificación adicional (NTA) usando el módem. Los NTA son números cuyo coste es superior al de una llamada nacional.

Dirección IP



Número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Dirección MAC

Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia identificación MAC determinada.

Firewall

También conocido como cortafuegos. Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.

Funcionalidad Peer To Peer (P2P)

La red Peer to Peer (P2P) es una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Es una forma legal de compartir archivos de forma similar a como se hace en el e-mail o mensajería instantánea, sólo que de una forma más eficiente.

En el caso de Panda Cloud Office Protection, la funcionalidad Peer To Peer reduce además el consumo de ancho de banda de la conexión a Internet, dando prioridad a que los equipos que ya han actualizado un archivo desde Internet lo compartan con otros que también necesitan actualizarlo. Así se evitan los accesos masivos a Internet y los consiguientes colapsos.

Funcionalidad Proxy

Esta funcionalidad permite el funcionamiento de Panda Cloud Office Protection en equipos sin acceso a Internet, realizándose los accesos a través de otro agente instalado en una máquina de su misma subred.



Grupo

En Panda Cloud Office Protection, un grupo es un conjunto de equipos informáticos a los que se aplica el mismo perfil de configuración de la protección. En Panda Cloud Office Protection existe un grupo inicial o grupo por defecto *-Default-* en el que se pueden incluir todos los ordenadores a proteger. También se pueden crear grupos nuevos.

Herramienta de distribución

Una vez descargada de Internet al PC administrador e instalada en éste, la herramienta de distribución permite instalar y desinstalar a distancia las protecciones en los equipos seleccionados.

Herramienta de hacking

Programa que puede ser utilizado por un hacker para causar perjuicios a los usuarios de un ordenador (pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.).

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

Identificador del agente de administración

Número único o GUID (*Globally Unique IDentifier*) que identifica a cada agente de administración de Panda Cloud Office Protection.

Joke

No es un virus, sino bromas de mal gusto que tienen por objeto hacer pensar a los usuarios que han sido afectados por un virus.



Lista negra

Lista de equipos a los que no se distribuye la protección. En el caso de que el equipo que está en la lista negra tenga aún la protección instalada, ésta no se actualizará. También figurarán en situación de lista negra los grupos de equipos caducados o aquéllos cuyo número máximo de instalaciones permitido haya sido superado.

Malware

Es un término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware tiene como objetivo infiltrarse en dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas.

Nodo

Un nodo es un punto de intersección o unión de varios elementos que confluyen en el mismo lugar. Aplicado a las redes informáticas, cada uno de los equipos de la red es un nodo y, si la red es Internet, cada servidor constituye también un nodo.

Nube

La computación en la nube (Cloud computing) es una tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.

Panda Endpoint Protection

Nombre que recibe la protección que Panda Cloud Office Protection distribuye e instala en los equipos de la red.

Perfil

Un perfil es una configuración específica de la protección. Este perfil es posteriormente



asignado a un grupo o grupos y aplicado a todos los equipos que forman parte de dicho grupo o grupos.

Phishing

Intento de conseguir información confidencial de un usuario de forma fraudulenta. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

Proceso local

Los procesos locales son los encargados de realizar tareas necesarias para la correcta implantación y administración de la protección en los equipos.

Protocolo

Sistema utilizado para la interconexión entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Un servidor proxy actúa como un intermediario entre una red interna (por ejemplo, una intranet) y una conexión externa a Internet. De esta forma, se puede compartir una conexión para recibir ficheros desde servidores Web.

Puerto

Punto de acceso a un ordenador o medio a través del cual tienen lugar las transferencias de información (entradas / salidas) del ordenador con el exterior y viceversa (vía TCP-IP).



Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los propios normalmente). Este tipo de software no es malicioso en sí mismo, pero es utilizado por los piratas informáticos para esconder evidencias y utilidades en los sistemas previamente comprometidos.

Existen ejemplares de malware que emplean rootkits con la finalidad de ocultar su presencia en el sistema en el que se instalan.

Servidor Exchange

Es un servidor de correo de la compañía Microsoft. El servidor Exchange almacena los correos electrónicos entrantes y/o salientes y gestiona la distribución de los mismos en las bandejas de entrada configuradas para ello.

Para conectarse al servidor y descargar el correo electrónico que haya llegado a su bandeja los usuarios han de tener instalado en su PC un agente de correo electrónico.

Servidor SMTP

Servidor que utiliza el protocolo SMTP -o protocolo simple de transferencia de correo- para el intercambio de mensajes de correo electrónicos entre los equipos.

Spyware

Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal y utilizarla posteriormente.



Topología de red

Cadena de comunicación que los nodos que conforman una red usan para comunicarse.

Troyanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario.

Red pública

Una red de este tipo es propia de cyberlocales, aeropuertos, etc. Conlleva limitación de su nivel de visibilidad y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Red de confianza

Este tipo de red generalmente es de oficina o casera. El equipo es perfectamente visible para el resto de equipos de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

Variable de entorno

Cadena compuesta por información del entorno, como la unidad, la ruta de acceso o el nombre de archivo, asociada a un nombre simbólico que pueda utilizar Windows. La opción Sistema del Panel de control o el comando set del símbolo del sistema permiten definir variables de entorno.

Virus

Programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.



Acceso a la consola Web

La consola Web

Para acceder a la consola Web:

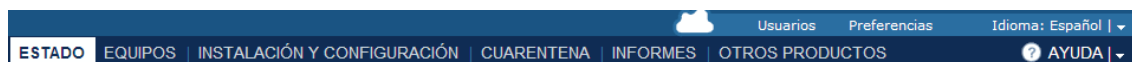
Introduzca Login Email y Contraseña.



Nota: En el caso de que su periodo de licencia haya caducado, podrá renovarla poniéndose en contacto con su distribuidor o comercial habitual.

Acepte los términos y condiciones del **Acuerdo de Licencia** (sólo se le solicitará la primera vez que acceda a la aplicación).

Después se mostrará la ventana principal de la consola Web. Desde esa ventana, usted podrá acceder a las áreas de **Estado**, **Equipos**, **Instalación y configuración**, **Cuarentena**, **Informes** y **Otros servicios**.



Mediante la opción **Salir**, usted puede cerrar la sesión. También puede seleccionar el idioma en el que desea visualizar la consola Web, utilizando el desplegable **Idioma** situado junto al idioma activo.

Para crear nuevos usuarios y asignarles permisos de acceso y privilegios de gestión de la consola Web, haga clic en [Usuarios](#).

Para establecer la configuración general de su consola Web, haga clic en [Preferencias](#).

Si desea acceder a la ayuda, conocer las últimas novedades de Panda Cloud Office Protection o consultar la Guía Avanzada de Administración, seleccione la opción



correspondiente en el menú desplegable **Ayuda**.

Utilice también este menú si lo que desea es acceder al Acuerdo de Licencia o saber qué versión de la protección está utilizando en su parque informático.

Menú Acerca de

Este menú muestra información sobre:

- La versión de la consola Web.
- La última versión de Panda Endpoint Protection instalada en el parque informático.
- La última versión del [agente](#) instalada en el parque informático.
- Si el cliente tiene varios equipos y en cada uno de ellos hay instalada una versión diferente de la protección, este menú **Acerca de** mostrará la versión más reciente de todas ellas.
- Si el cliente no ha instalado la protección en ningún equipo, se muestra la última versión disponible de la protección, es decir, la que será instalada en los equipos.

Preferencias

Desde esta ventana, usted puede establecer configuraciones generales que afectarán a su consola Web.

Opciones generales

Si desea que la guía de inicio rápido se muestre cada vez que acceda a la consola, marque la casilla **Mostrar guía de inicio rápido al entrar**.

Vista por defecto

Elija la manera en que se mostrarán los equipos: por nombre o por IP. Marque la opción deseada.



Restricciones de grupo

Seleccione esta opción si desea limitar el número de instalaciones y la fecha de caducidad de los [grupos](#). Para ello, marque la casilla correspondiente.

Acceso remoto

Utilice esta sección para introducir las credenciales con las que accederá a los equipos a través de las diferentes herramientas de acceso remoto.

Estas credenciales serán propias de cada usuario, es decir, usuarios diferentes de la consola de administración podrán incluir credenciales diferentes de acceso a los equipos.

Si desea eliminar el acceso remoto a sus equipos a su proveedor de servicio, desmarque la opción **Permitir a mi proveedor de servicios iniciar conexión remota a mis equipos**.

Acceso remoto desde la consola de Panda Cloud Partner Center

En el caso de que el acceso a la consola se produzca desde una consola de Panda Cloud Partner Center, las credenciales que introduzca el usuario que acceda por primera vez, serán las mismas que utilizarán otros usuarios de la consola de Panda Cloud Partner Center que intenten acceder con posterioridad.

Cada usuario que acceda desde la consola de Panda Cloud Partner Center tendrá la posibilidad de cambiar las credenciales, pero dicho cambio afectará al resto de usuarios.

Gestión automática de archivos sospechosos

Utilice esta opción si desea que los archivos sospechosos sean enviados al laboratorio para su estudio. De esta forma, en caso de infección se podrá proporcionar una respuesta en el menor tiempo posible y acelerar la distribución de la protección adecuada.



Gestión de cuentas

Si es usted un usuario con [permisos de control total](#), podrá acceder a las funcionalidades de [gestión de cuentas](#). Para ello, haga clic sobre el vínculo **Gestionar cuentas**.

Lista negra de equipos

Usted puede elaborar una lista de equipos a los que no quiere distribuir la protección y añadir o eliminar equipos de esta lista. También figurarán en la lista negra los equipos de los grupos caducados o aquéllos cuyo número máximo de instalaciones permitido haya sido superado.

Los equipos no protegidos también aparecerán en esta lista negra. Visite el apartado [equipos desprotegidos](#) para saber más sobre ellos.

Gestión de licencias

Tipos de clientes

Clientes suscriptores

Son aquéllos que contratan licencias sin fecha de caducidad. Si es usted cliente suscriptor, podrá ver en el apartado **Licencias** de la ventana [Estado](#) el texto *"Periodo de validez: Permanente"*. **No tendrá que preocuparse por la fecha de caducidad de su licencia.**

Clientes no suscriptores

Son aquéllos que contratan licencias con fecha de caducidad. Si es usted cliente no suscriptor, podrá ver en el apartado **Licencias** de la ventana [Estado](#) el texto *"Periodo de validez: 00/00/0000 "*.



Alertas relacionadas con las licencias

Usted dispone de una serie de licencias de Panda Cloud Office Protection. De acuerdo con sus necesidades, podrá [instalar las protecciones](#) en los equipos, [desinstalarlas](#), eliminar equipos de la lista de equipos protegidos, añadir equipos a dicha lista, etc.

La utilización que haga de sus licencias tiene su reflejo en el número de licencias disponibles.




Las licencias pueden ser utilizadas indistintamente en equipos con sistema operativo Windows o Linux.

Actualización del número de licencias

Si usted:

 **Instala la protección en un equipo** ▶ Se resta una licencia del total de licencias disponibles.

 **Elimina un equipo de la lista de equipos protegidos** ▶ Se suma una licencia al total de licencias disponibles.

 **Disminuye en X unidades el número de licencias contratadas** ▶ Se envía a lista negra un número de equipos igual a aquél en que se supera al número de licencias contratadas.

Alerta por fecha de caducidad de licencias contratadas

En el área de notificaciones, aparecerán diferentes avisos en función de la proximidad de la fecha de caducidad (menos de 60 días), si se ha superado dicha fecha o si estas caducidades dejarían menos licencias disponibles de las usadas actualmente.



***Nota:** En ambos casos podrá usted renovar la licencia poniéndose en contacto con su distribuidor habitual o comercial. Panda Cloud Office Protection se lo recordará mediante un mensaje en la ventana [Estado](#). Una vez concluido el plazo de 60 días, dispondrá de otros 15*



días de gracia para realizar la renovación. Superado este tiempo, la renovación no será posible.

Lista negra

Un equipo puede ser introducido en la [lista negra](#) de forma manual o de manera automática, al tratar de instalar en él la protección cuando se ha superado el número de instalaciones permitidas o cuando la licencia ha caducado.

La inclusión automática también se produce al superar las restricciones impuestas a un grupo, restricciones que usted puede configurar en la ventana [Preferencias](#).

La inclusión de un equipo en la lista negra implica que dicho equipo no se actualiza y que la información procedente de él no es tenida en cuenta a ningún efecto de las estadísticas, [informes](#) y análisis realizados por Panda Cloud Office Protection. Sin embargo, la licencia del equipo no se sumará al total de licencias consumidas sino que se restará del mismo.



Nota: La exclusión de equipos de la lista negra sólo será posible cuando existan licencias disponibles y cuando el equipo que se desea excluir haya sido integrado en la lista negra de forma manual.

Anulación de licencias

En el caso de varios mantenimientos, esta pantalla le mostrará la fecha de caducidad de licencias más próxima en el tiempo, el número de licencias que es necesario anular y la advertencia de, que una vez transcurrida la fecha de caducidad, los equipos afectados por la anulación se enviarán automáticamente a la **lista negra**.

Usted puede elegir entre anular el número de licencias que necesita de entre los primeros equipos a los que se instaló la protección o de entre los últimos. Utilice para ello el desplegable **Anular licencias de** y haga clic en el botón **Aplicar**. Se mostrarán en el listado tantos equipos como licencias sea necesario liberar.



Equipos afectados

Esta es la pestaña por defecto, en la que se muestra la lista de equipos cuyas licencias se anularán y que, por tanto, dejarán de estar administrados.

Esta pestaña distribuye la información en cuatro columnas: **Equipo**, **Grupo**, **Fecha de instalación** e **Inserción**. Esta última columna mostrará el término **Automático** si el equipo proviene de la selección que usted ha hecho en el desplegable **Anular licencias de**, o **Manual** si el equipo proviene de la pestaña **Equipos administrados**. Seleccione la casilla correspondiente a los equipos cuyas licencias desea anular y, a continuación, haga clic en **Excluir**.

Mediante el desplegable **Opciones**, puede refinar la búsqueda de equipos, especificando periodos de tiempo en los que se instaló protección en los equipos y obtener así listados diversos.

Equipos administrados

Esta pestaña muestra los equipos que usted administra. Si desea añadir alguno de ellos a la lista de equipos afectados, marque la casilla correspondiente y haga clic en **Agregar** y el equipo pasará a la lista de equipos afectados, donde mostrará en la columna **Inserción** el término **Manual**.

Finalmente, cuando haya transcurrido la fecha de caducidad, desde la lista de equipos afectados se enviarán a la lista negra tantos equipos como licencias haya sido necesario anular.

Añadir licencias mediante código de activación

Mediante esta funcionalidad, será usted quien decida cuándo ampliar sus licencias.



Desde su consola Web, podrá acceder al formulario de **Activación de licencias** y activar el servicio de manera sencilla y rápida, utilizando el código de activación que le fue proporcionado por Panda Security o su distribuidor en el momento de la compra.

Siga los siguientes pasos:

Haga clic en **Añadir más licencias**, en la ventana **Estado**. Se mostrará la ventana **Activación de licencias**.

Introduzca el código de activación.

Haga clic en **Aceptar**.



Nota: *El proceso de añadir licencias no es inmediato, por lo que puede que transcurra un tiempo hasta que las licencias añadidas se muestren en la sección **Licencias** de la ventana **Estado**.*

En caso de error, consulte el apartado [Errores posibles al añadir licencias](#).

Errores posibles al añadir licencias

Al introducir el código de activación, pueden aparecer los siguientes errores:



El código de activación introducido no es válido / no existe

Asegúrese de haber introducido correctamente todos los dígitos.



El código de activación introducido ya está en uso

Se trata de un código de activación que ya ha sido usado. En este caso, póngase en contacto con su distribuidor o comercial habitual para poder adquirir un código nuevo.



No se puede realizar la operación

Es posible que las características de los servicios/licencias que usted ha contratado no




permitan la utilización de la funcionalidad de ampliación de licencias.

Este error también se reportará cuando un cliente de Panda Cloud Office Protection intente añadir licencias introduciendo un código de activación de Panda Cloud Office Protection Advanced en la consola cliente y viceversa.

Otros errores

Una vez introducido con éxito el código de activación, puede darse el siguiente error:

 *No se ha podido dar de alta la solicitud*

Este error tiene lugar cuando el proceso falla por un motivo desconocido. Por favor, vuelva a intentarlo y si no consigue realizar la activación, contacte con el soporte técnico de Panda Security.

Gestión de cuentas

Introducción a la gestión de cuentas

Si es usted un usuario con [permisos de control total](#), puede acceder a las funcionalidades de gestión de cuentas que Panda Cloud Office Protection pone a su disposición: delegar la gestión de una cuenta y unificar cuentas. A ambas opciones se accede desde la pantalla **Gestión de cuentas** (*Preferencias / Gestionar cuentas*).

Delegar la gestión de una cuenta

Por medio de esta funcionalidad, usted permitirá que la seguridad de sus equipos sea gestionada por otro cliente. Para ver más información sobre esta opción, consulte el apartado [Delegar la gestión de una cuenta](#).

Unificar cuentas

Cuando existen varias cuentas de cliente, se pueden unificar en una y posibilitar así la



gestión centralizada de la seguridad de los equipos. Para ver más información sobre esta opción, consulte el apartado [Unificar cuentas](#).

Delegar la gestión de una cuenta

Si desea delegar la gestión de la seguridad de sus equipos en un partner, puede hacerlo mediante la funcionalidad **Delegar servicio**. El partner en quien usted delega tendrá acceso a su consola.

➡ **Nota:** Para delegar la gestión de su cuenta en un partner, usted necesitará el identificador de Panda Security de dicho partner.

Siga los siguientes pasos:

Haga clic en **Gestionar cuentas** de la ventana **Preferencias**. Se mostrará la ventana **Gestión de cuentas**.

En el apartado **Delegar seguridad a su proveedor de servicio** introduzca el identificador del partner que gestionará la seguridad de los equipos.

Para confirmar que desea proceder a la delegación, haga clic en **Delegar**.

➡ **Nota:** El proceso de delegación de gestión no es inmediato, por lo que puede que transcurra un tiempo hasta que sus datos sean accesibles para el partner especificado.

En caso de error, consulte el apartado [Errores posibles al delegar la gestión de una cuenta](#).

Errores posibles al delegar la gestión de una cuenta


Al tratar de activar la funcionalidad de delegación del servicio, pueden aparecer los siguientes errores:

☁ *El identificador introducido no es válido. Por favor, revíselo e introdúzcalo de nuevo.*



Panda Cloud Office Protection

Por favor, asegúrese de haber introducido correctamente todos los dígitos del identificador del partner.

 *No dispone de licencias para realizar esta operación. Contacte con su distribuidor o comercial habitual para renovarlas.*

Si sus licencias han caducado, no podrá acceder a la funcionalidad de delegación de servicio.


Por favor, contacte con su distribuidor o comercial habitual para renovar sus licencias.

 *No puede realizar esta operación. Consulte con su distribuidor o comercial habitual.*

Es posible que las características de los servicios/licencias que usted contrató no permitan la utilización de la funcionalidad de delegación de servicio.

Por favor, consulte a su distribuidor o comercial habitual.

Otros errores

 *Ha ocurrido un error y no se ha podido dar de alta la solicitud. Por favor, inténtelo de nuevo.*

Este error tiene lugar cuando el proceso falla por un motivo desconocido. Por favor, vuelva a intentarlo y si no consigue realizar la activación del servicio, contacte con el soporte técnico de Panda Security.

Unificar cuentas

¿Qué es la unificación de cuentas?

Si usted posee varias cuentas de cliente y desea unificarlas para gestionarlas de manera centralizada, puede hacerlo mediante la funcionalidad de unificación de cuentas. De esta manera, podrá gestionar todas sus cuentas desde una sola consola Web.



➡ **Nota Importante:** Antes de proceder a la unificación de cuentas, es importante comprender cuáles son las consecuencias de ello. Por favor, consulte el apartado [Consecuencias de la unificación de cuentas](#).

¿Cómo se realiza la unificación de cuentas?

Básicamente el proceso consiste en traspasar los datos de una cuenta-origen (cuenta A) a una cuenta-destino (cuenta B). Esta cuenta-destino ha de encontrarse activa.

Para unificar las cuentas:

Acceda a la consola Web de la cuenta-origen (cuenta A), la que será dada de baja.

Haga clic en **Gestionar cuentas** en la ventana **Preferencias**. Se mostrará la ventana **Gestión de cuentas**.

Seleccione **Unificar**.

Introduzca **Login Email** y **Contraseña** de la cuenta-destino (cuenta B), a la que se trasladará la información procedente de la cuenta A. Estos datos le fueron proporcionados en el mensaje de bienvenida cuando creó la cuenta.

Si está seguro de que desea unificar las cuentas, haga clic en **Unificar**.

➡ **Nota:** El proceso de traspaso de datos no es inmediato, por lo que puede que transcurra un tiempo hasta que pueda comprobarlo en la consola Web de su cuenta B.

En caso de error, consulte el apartado [Errores posibles en el proceso de unificación de cuentas](#).

¿Qué información se traslada en el proceso de unificación de cuentas?

La unificación de cuentas implica el traslado de información sobre los equipos gestionados desde la cuenta A.



A continuación, se detalla la información que se trasladará:

Todos los mantenimientos activos y no caducados, es decir, la información sobre las licencias activas, sus fechas de inicio y caducidad, tipo de licencia, etc.

Perfiles de configuración. Todos los perfiles de configuración de las protecciones de la cuenta-origen. En el caso de que en la cuenta-destino exista un perfil con el mismo nombre (por ejemplo, *Perfil Comercial*), el perfil procedente de la cuenta-origen será "renombrado" mediante un sufijo numérico (*Perfil Comercial-1*).

➡ **Nota:** *El perfil por defecto -perfil Default- de la cuenta-origen se traspasará a la cuenta-destino, pero será considerado como un perfil más y perderá la marca de perfil por defecto.*

Grupos de equipos. Todos los grupos de equipos. En el caso de grupos de igual nombre, el funcionamiento será similar al aplicado para los perfiles en el punto anterior.

➡ **Nota:** *El grupo por defecto -grupo Default- de la cuenta-origen se traspasará a la cuenta-destino, pero será considerado como un grupo más y perderá la marca de perfil por defecto.*

Información de las protecciones activas y de las que se encuentran en situación de lista negra.

Informes y estadísticas de detección.

Todos los elementos en cuarentena, incluyendo los elementos excluidos de cuarentena y los restaurados.

Los **usuarios** de la consola Web (con sus correspondientes permisos), excepto el usuario por defecto -*Default*-.


Errores posibles en el proceso de unificación de cuentas

Al tratar de acceder al formulario **Gestión de cuentas**, pueden producirse los siguientes errores:


☁ *El Login Email y/o contraseña no son correctos*



Por favor, asegúrese de haber introducido correctamente todos los caracteres.

 *No se puede realizar la operación*


Es posible que las características de los servicios/licencias que usted ha contratado no permitan la utilización de la funcionalidad de unificación de cuentas. Por favor, consulte con su distribuidor o comercial habitual.

 *No dispone de licencias para realizar esta operación*


Si sus licencias han caducado, no podrá acceder a la funcionalidad de unificación de cuentas. Por favor, contacte con su distribuidor o comercial habitual para renovar sus licencias.

 *La cuenta especificada tiene una fusión en curso*


En el caso de que la cuenta B (cuenta-destino) que usted ha especificado esté inmersa en otro proceso de unificación, será necesario aguardar a que dicho proceso termine para poder comenzar el suyo.

 *La cuenta con la que ha iniciado sesión supera el número permitido de equipos*

El proceso de unificación de cuentas sólo es posible si la cuenta A (cuenta-origen) tiene menos de 10.000 equipos asociados.

 *Las cuentas implicadas en la unificación pertenecen a versiones diferentes de Panda Cloud Office Protection*

Para que la unificación de las cuentas A y B se lleve a cabo de manera correcta, es necesario que ambas pertenezcan a la misma versión de Panda Cloud Office Protection. Es improbable que las cuentas pertenezcan a diferentes versiones, salvo en situaciones de actualización de versión.

 *No se ha podido dar de alta la solicitud*

Cuando haya fallado el proceso por un motivo desconocido, por favor, vuelva a intentarlo y si no consigue realizar la unificación de cuentas, contacte con el soporte técnico de Panda Security.

Consecuencias de la unificación de cuentas

Antes de proceder a la unificación de cuentas, es **MUY IMPORTANTE** que tenga en cuenta las consecuencias que ello conlleva:



Panda Cloud Office Protection

Los **servicios asociados** a la cuenta A **dejarán de estar activos** y la cuenta será eliminada. Obviamente, el acceso a la consola Web de la cuenta A será denegado.

En la consola Web de la cuenta B, se mostrarán los datos e informaciones sobre los equipos gestionados desde la cuenta A. Para comprobarlo, tan sólo tiene que acceder a la consola Web de la cuenta B.

Se producirá la **reasignación automática** de las protecciones instaladas en los equipos gestionados desde la cuenta A, pasando a ser gestionados desde la cuenta B. **No será necesario reinstalar las protecciones.**

➡ **Nota:** *El proceso de traspaso de datos no es inmediato, por lo que puede que transcurra un tiempo hasta que pueda comprobarlo en la consola Web de su cuenta B.*

En caso de error, consulte el apartado [Errores posibles en el proceso de unificación de cuentas](#).

Creación y gestión de usuarios

Si la opción por defecto que Panda Cloud Office Protection le ofrece no se ajusta a las necesidades de protección de su red informática, usted puede optar por crear nuevos usuarios y asignarles [diferentes tipos de permisos](#), en función de lo que desea que gestione cada usuario.

En la ventana principal de la consola Web, haga clic en **Usuarios**.

La ventana **Usuarios** distribuye la información en tres columnas: **Nombre**, **Permisos** y **Estado**. A medida que usted vaya creando usuarios, éstos aparecerán en el listado, junto al tipo de permisos que les haya otorgado y su estado (activado o desactivado).



Usted puede necesitar crear nuevos usuarios y asignarles diferentes permisos de gestión y control de grupos. Con Panda Cloud Office Protection puede hacerlo de forma sencilla.



Nota: El usuario por defecto que muestra Panda Cloud Office Protection no se puede eliminar y sólo se pueden modificar sus comentarios. La aplicación lo muestra en el listado como **Nombre (Usuario por defecto)**.

Haga clic en **Crear nuevo usuario** para acceder a la ventana **Usuarios - Edición**. Complimente los campos **Usuario** (nombre de usuario), **Login Email**, **Contraseña** y **Repetir contraseña**.

Puede añadir información adicional si lo desea, utilizando para ello la caja de texto **Comentarios**.

En **Grupos** seleccione el grupo o grupos sobre los que el usuario administrador y de monitorización podrá actuar, de acuerdo con el permiso que usted le haya asignado. El usuario con permiso de control total podrá actuar sobre todos los grupos.

Haga clic en **Aceptar**.

En la ventana principal **Usuarios**, compruebe que el usuario ha sido creado y que su nombre, permiso y estado aparecen correctamente en el listado.

Si desea eliminar alguno de los usuarios de la lista, seleccione la casilla correspondiente y haga clic en **Borrar**.

Tipos de permisos

En Panda Cloud Office Protection se han establecido tres tipos de permisos. En función del permiso que se asigne a un usuario, éste podrá realizar mayor o menor número de



acciones que afectarán o bien a todos o a algunos equipos y grupos.

Las acciones que el usuario podrá llevar a cabo afectan a diferentes aspectos de configuración básica y avanzada de la protección, y van desde la creación y modificación de sus propias credenciales de usuario y la configuración y asignación de perfiles a grupos y equipos, hasta la generación y obtención de diferentes tipos de informes, entre otros.

Los permisos existentes son:



[Permiso de control total](#)



[Permiso de administrador](#)



[Permiso de monitorización](#)

Seleccione el tipo de permiso cuyas especificaciones desee consultar. Le resultarán de utilidad para asignar funciones a los diferentes integrantes de sus equipos de trabajo y obtener el máximo rendimiento de todas las funcionalidades que Panda Cloud Office Protection ha preparado para su seguridad.

Permiso de control total

Gestión de usuarios

El usuario puede:

Ver todos los usuarios creados en el sistema.

Eliminar usuarios.

Gestión de grupos y equipos

El usuario puede:

Crear y eliminar grupos.



Gestionar la configuración de los perfiles de protección de todos los grupos.

Asignar equipos a los grupos.

Mover equipos de un grupo a otro.

Editar el campo **Comentarios** en la pantalla [Detalle de equipos](#).

Acceso remoto a cualquier equipo.

Gestión de perfiles e informes

El usuario puede:

Copiar perfiles y ver todas las copias realizadas de todos los perfiles.

Configurar análisis programados de rutas específicas para cualquier perfil.

Visualizar informes (informes inmediatos, no programados), de cualquier grupo.

Crear tareas de envío de informes programados sobre cualquier grupo

Visualizar todas las tareas de envío de informes.

Búsqueda de equipos desprotegidos

El usuario puede:

Configurar tareas de búsqueda de equipos desprotegidos.

Visualizar y/o eliminar cualquiera de las tareas creadas.

Desinstalación de la protección

El usuario puede:

Configurar tareas de desinstalación de protecciones.

Visualizar y/o eliminar cualquiera de todas las tareas creadas.



Gestión de licencias y cuentas

El usuario puede:

Utilizar la opción de [Ampliar licencias mediante código de activación](#).

Utilizar la opción de [Unificar cuentas](#).

[Delegar la gestión de su cuenta](#) en un partner.

Permiso de administrador

Las acciones que el usuario con permiso de administrador puede llevar a cabo y que tienen que ver con gestión de usuarios, equipos, grupos, configuración y desinstalación de la protección, sólo son aplicables a equipos o grupos sobre los que el usuario administrador tenga permiso o que hayan sido creados por él.

Gestión de usuarios

El usuario puede:

Modificar sus propias credenciales.

Crear usuarios.

Búsqueda de equipos desprotegidos

El usuario puede:

Crear tareas de búsqueda para que equipos de los grupos sobre los que se tienen permisos realicen la búsqueda.

Visualizar y/o eliminar cualquiera de las tareas de búsqueda de equipos creadas, pero sólo desde equipos pertenecientes a grupos sobre los que tenga permiso.



Gestión de grupos y equipos

El usuario puede:

Crear grupos y gestionar la configuración de los perfiles de los grupos sobre los que tiene permiso.

Eliminar los grupos sobre los que tiene permisos.

Editar el campo **Comentarios** de los equipos sobre los que tenga permisos, en la pantalla [Detalle de equipos](#).

Acceso remoto a aquellos equipos que pertenezcan a grupos sobre los que tenga permiso.

Desinstalación de protecciones

El usuario puede:

Configurar tareas de desinstalación de protecciones en equipos o grupos sobre los que tenga permiso.

Visualizar y/o eliminar tareas de desinstalación, pero sólo en equipos pertenecientes a grupos sobre los que tenga permiso.

Gestión de perfiles e informes

El usuario puede:

Crear perfiles nuevos y visualizarlos.

Crear copias de perfiles sobre los que tiene permiso y visualizarlos.

Configurar análisis programados de rutas específicas para perfiles sobre los que tenga permiso o hayan sido creados por él.

Visualizar informes (informes inmediatos, no programados) que incluyan grupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos que aparezcan en el informe.

Crear tareas de envío de informes programados sobre grupos sobre los que tenga



permisos

Visualizar las tareas de envío de informes que incluyan grupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos que aparezcan en el informe. En caso contrario no podrá visualizar la tarea de envío de informes.

Permiso de monitorización

El usuario puede:

Modificar sus propias credenciales.

Ver y monitorizar la protección de los grupos que se le asignen.

Visualizar los perfiles asignados a grupos sobre los que tenga permiso.

Visualizar las tareas de búsqueda de equipos protegidos realizadas desde equipos pertenecientes a grupos sobre los que tenga permiso.

Visualizar las tareas de desinstalación de los grupos sobre los que tiene permiso.

Visualizar informes (informes inmediatos) de grupos sobre los que tenga permisos.

Visualizar las tareas de envío de informes que incluyan grupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos que aparezcan en el informe. En caso contrario no podrá visualizar la tarea de envío de informes.

Configuración de la protección

Introducción

La protección que Panda Cloud Office Protection proporciona está pensada para ser instalada y distribuida en la red informática de su empresa. En consecuencia, la protección a instalar varía en función del tipo de equipos a proteger y de las diferentes necesidades que usted tiene en cuanto a seguridad.



Panda Cloud Office Protection

Usted puede configurar la protección antes o después de la instalación. Para ello debe crear un [perfil](#) y después asignarlo al grupo o grupos a los que desea aplicarlo.

➡ **IMPORTANTE:** A lo largo de esta ayuda se describe el proceso de configuración de las diferentes protecciones partiendo de la creación desde cero de un perfil (**Instalación y Configuración / Perfiles / Crear nuevo perfil /...**).

No obstante, la configuración de las protecciones de los perfiles puede modificarse en cualquier momento, por lo que para perfiles ya existentes los pasos a seguir serán (**Instalación y Configuración / Perfiles / Nombre del perfil /** y a continuación realizar las modificaciones en la ventana **Edición de perfil**)

➡ En el caso de esta ayuda, se ha optado por explicar el proceso de configuración como paso previo a la instalación de la protección en los equipos.



A la hora de asignar perfiles a los grupos creados, las opciones son varias: un mismo perfil se puede aplicar a varios grupos, cada grupo puede tener un perfil diferente o se puede dar el caso de que sólo se necesiten un único perfil y un único grupo.



Al crear un perfil usted configurará el comportamiento que la protección tendrá para ese perfil específico, esto es, determinará qué tipo de análisis se realizarán y sobre qué elementos, y cada cuánto tiempo se actualizará la protección.

Antes de acceder a la opción **Instalación** es necesario crear los perfiles que se necesitan y configurar cuál será el comportamiento de la protección en cada perfil. A continuación se crearán los grupos de equipos necesarios, asignándoles el perfil que se desee, con lo que dicho perfil se aplicará a todos los equipos que formen parte del grupo.

➡ *Si usted no necesita crear ningún perfil ni grupo adicional a los que Panda Cloud Office Protection proporciona por defecto, acceda al menú **Instalación y Configuración** y seleccione el grupo **Default**. Después seleccione el modo de instalación que desea utilizar para instalar la protección en los equipos.*

Perfil por defecto

Seleccione la opción **Perfiles** para acceder a la ventana **Perfiles del programa de instalación**. Esta ventana muestra los perfiles existentes.

La primera vez que acceda a ella, se mostrará el perfil por defecto **-Default-** e información sobre las protecciones que tiene asociadas (antivirus, firewall, control de dispositivos, servidores Exchange y control de acceso a páginas Web).

La protección para servidores Exchange y el control de acceso a páginas Web irán desactivadas por defecto, y sólo las podrán activar los clientes que dispongan de licencias de Panda Cloud Office Protection.

➡ *Esta protección para servidores Exchange es aplicable a las versiones 2003, 2007, 2010 y 2013*



Si en algún momento usted quiere modificar la configuración de este perfil, haga clic sobre el nombre del perfil. Accederá a la ventana **Edición de perfil**. Realice las modificaciones que desee y utilice la opción **Guardar**.

Si posteriormente desea restaurar la configuración original del perfil, hágalo mediante la opción **Restaurar configuración por defecto** de la ventana **Edición de perfil**.

Crear / Copiar un perfil

Crear un perfil

Si usted necesita crear perfiles nuevos, a medida que los cree se mostrarán en la ventana **Perfiles del programa de instalación** junto al perfil **Default** ya existente, acompañados de información sobre las protecciones que incluyen.

Después podrá modificar en cualquier momento la configuración de un perfil haciendo clic sobre su nombre y accediendo a la ventana **Edición de perfil**, tal y como se ha explicado para el perfil por defecto.

Si se intenta asignar a un perfil un nombre ya utilizado para otro, se mostrará un mensaje de error.

Permisos necesarios

Si usted no puede visualizar el perfil que ya existe con dicho nombre es porque seguramente no disponga de permiso para ello. Para más información, consulte el apartado [Tipos de permisos](#).

Para crear el perfil haga clic sobre el vínculo **Crear nuevo perfil**, y accederá a la ventana **Edición de perfil**. Desde aquí podrá [configurar el perfil nuevo](#).

Configuración del perfil



La configuración de un perfil se estructura en las siguientes secciones: General, Antivirus, Firewall, control de dispositivos y protección para servidores Exchange (esta protección solo se podrá configurar si usted dispone de licencias de Panda Cloud Office Protection Advanced).

Todo el proceso de configuración del perfil se describe con detalle a lo largo de las siguientes secciones:

[Configuración general del perfil](#)

[Configuración de la protección antivirus](#)

[Configuración de la protección firewall](#)

[Configuración del control de dispositivos](#)

[Configuración de la protección para servidores Exchange](#)

Copiar un perfil

Panda Cloud Office Protection le ofrece la posibilidad de realizar copias de perfiles existentes. Esto resulta útil cuando usted prevea que la configuración básica de un perfil que ya ha creado es susceptible de ser aplicada a otros equipos.

De esta manera en lugar de crear dicha configuración básica cada vez, podrá copiar el perfil para después personalizarlo y adaptarlo a las circunstancias concretas de protección que necesite.

Para utilizar esta opción de copia de perfil haga clic en el menú **Instalación y configuración > Perfiles** y accederá a la pantalla **Perfiles del programa de instalación**. Seleccione el perfil o perfiles que desea copiar -hasta un máximo de diez- y haga clic en el botón **Copiar**.

Una vez copiado el perfil, éste se mostrará con el nombre *Copia de<Nombre_perfil>*, y usted podrá renombrarlo haciendo clic sobre él e introduciendo el nombre en la



pantalla **Edición de perfil**.



En el caso del perfil Default, es posible hacer una copia de él, pero el perfil copiado no tendrá la condición de perfil por defecto ni será asignado automáticamente a ningún equipo. El perfil Default original será siendo el predeterminado.

La copia de perfil será posible en función del tipo de permiso del que usted disponga. Para más información, consulte el apartado [Tipos de permisos](#).

Configuración general del perfil

En esta parte de la configuración se seleccionan opciones de tipo general de la configuración del perfil, por lo que es importante tener claro qué tipo de perfil se desea, en función de los equipos en los que se va a instalar la protección con el perfil asignado.

Para acceder a la configuración, haga clic en el menú **Instalación y Configuración / Perfiles / Crear nuevo perfil**.

Pestaña *Principal*

Por medio de las opciones que aparecen en esta pestaña podrá dar un nombre al perfil que está creando y activar la actualización automática del motor de la protección y del [archivo de identificadores](#). Marque la casilla correspondiente para activarlos.

También podrá añadir una descripción adicional que le sirva para identificar el perfil y seleccionar el idioma en el que se instalará la protección. Haciendo clic sobre el vínculo **Opciones avanzadas** accederá a la ventana [Edición de perfil-Opciones avanzadas](#).



Pestaña Actualizaciones

Puede utilizar las opciones que encontrará en esta pestaña para realizar la configuración automática de la actualización tanto del motor de la protección como del [archivo de identificadores](#).

Equipos con sistema operativo Linux

En el caso de los equipos con sistema operativo Linux, no es posible configurar la periodicidad de la actualización automática del archivo de identificadores. Se hará siempre cada 4 horas.

Actualización automática del motor de la protección

En primer lugar marque la casilla de activación de las actualizaciones.

Utilice el desplegable para establecer cada cuánto tiempo desea que se busquen nuevas actualizaciones.

Si lo desea, podrá establecer la fecha en la que tendrán lugar las actualizaciones automáticas y la franja horaria. Se permite seleccionar:

El día o los días de la semana en los que se quiere realizar la actualización.



- ☒ Realizar las actualizaciones sólo en las siguientes fechas:

Los siguientes días de la semana ▼

☐ Lunes

☐ Jueves

☐ Domingo

☐ Martes

☐ Viernes

☐ Miércoles

☐ Sábado

El intervalo de días del mes en los que se realizará la actualización.

- ☒ Realizar las actualizaciones sólo en las siguientes fechas:

Los siguientes días del mes ▼

Primer día: 1 ▼

Último día: 31 ▼

El intervalo de fechas en los que se realizará la actualización.

- ☒ Realizar las actualizaciones sólo en las siguientes fechas:

Los siguientes días ▼

Desde: 

Hasta: 

Y, para terminar, marque la casilla si desea permitir que los equipos afectados por las actualizaciones -estaciones de trabajo, servidores o ambos- se reinicien cuando el proceso termine.

Haga clic en **Aceptar**.

Es recomendable que reinicie el equipo tan pronto como se muestre un mensaje en este sentido, aunque es posible que no sea necesario hacerlo hasta pasados varios



días después de la actualización.

Equipos con sistema operativo Linux

En el caso de los equipos con sistema operativo Linux no es posible realizar una actualización automática, por lo que cuando exista una nueva versión de la protección ésta deberá instalarse de nuevo en los equipos.

Cuando transcurran 7 días desde que exista una versión de la protección superior a la que los equipos tienen instalada, los equipos con sistema operativo Linux aparecerán como "desactualizados" en la ventana **Estado**, momento en el que el administrador podrá proceder a instalar la versión superior en los equipos.

Actualización automática del archivo de identificadores

Marque la casilla para activar la actualización automática.

Seleccione en el desplegable la periodicidad con la que desea que se realice la búsqueda de actualizaciones.

Haga clic en **Aceptar**.

Pestaña Análisis programados

Si selecciona la pestaña **Análisis programados** podrá crear tareas de análisis, periódicas, puntuales o inmediatas y determinar si afectarán a todo el PC o a determinados elementos del mismo.

También puede optar por programar análisis exclusivos del correo electrónico o especificar las rutas concretas en las que se encuentran las carpetas o archivos que desee analizar.



Pestaña *Alertas*

Aquí podrá usted configurar las alertas que se mostrarán cuando se detecte malware en los equipos, intentos de intrusión o dispositivos no permitidos y si estas alertas serán de tipo local, por correo, o de las dos maneras.

La diferencia entre ambas está en que la alerta local se mostrará en el equipo o equipos en los que se produjeron las detecciones, mientras que si opta usted por activar la alerta por correo, cada equipo en el que se produce la detección enviará una alerta en forma de mensaje de correo electrónico a la cuenta o cuentas habilitadas.

Para ello:

En primer lugar, active la checkbox **Enviar alerta por correo**.

Cumplimente el campo **Asunto del mensaje**.

Introduzca la dirección de correo y especifique el servidor SMTP que se utilizará para enviar las alertas. En el caso de que el servidor requiera autenticación, introduzca el usuario y la contraseña necesarios.

Haga clic en **Aceptar**.

Pestaña *Aplica a*

Cuando usted asigne el perfil que está creando a algún grupo o grupos, éstos aparecerán listados aquí.

Configurar análisis programados



Si selecciona la pestaña **Análisis programados** podrá crear tareas de análisis, periódicas, puntuales o inmediatas y determinar si afectarán a todo el PC o a determinados elementos del mismo.

También puede optar por programar análisis exclusivos del correo electrónico o especificar las rutas concretas en las que se encuentran las carpetas o archivos que desee analizar.

A medida que usted vaya creando tareas de análisis, éstas se irán añadiendo en el listado principal de la pestaña **Análisis programados** de la ventana **Edición de perfil**, desde donde podrá editarlas o eliminarlas.

Pasos a seguir para la configuración de los análisis

Haga clic en el botón Nuevo para acceder a la ventana Edición de perfil – Nueva tarea de análisis.

Siga los siguientes pasos:

Nombre: indique el nombre con el que quiere identificar el análisis que va a programar.

Tipo de análisis: seleccione el tipo de análisis que va a crear (inmediato , programado, o periódico).



Análisis inmediato: una vez configurado el análisis, éste tendrá lugar en el momento en que se produzca la conexión del equipo con el servidor de Panda Cloud Office Protection y se constate que se ha producido alguna modificación en la configuración de la protección.



Análisis programado: el análisis tendrá lugar en la hora y fecha que usted determine en **Fecha de comienzo** y **Hora de comienzo**.



Análisis periódico: determine **Fecha y hora de comienzo**, y seleccione en el desplegable **Repetición** la periodicidad que desea adjudicar al análisis.

Analizar: seleccione la opción que desea:

Todo el PC

Discos duros

Correo electrónico (análisis no aplicable en equipos con sistema operativo Linux)

Otros elementos

Utilice esta opción para analizar elementos concretos almacenados (archivos, carpetas,...) tendrá que introducir la ruta en la que se encuentra el elemento a analizar. El formato de la ruta ha de empezar por `\\`, (letra):\
Ejemplos:

* `\\carpeta1\carpeta2`

* `c:\carpeta1\carpeta`

El número máximo de rutas a analizar que podrá introducir por cada perfil es de diez. En función del permiso que usted posea podrá establecer rutas específicas de análisis. Para más información, consulte el apartado [Tipos de permisos](#).

En Linux se deben seleccionar rutas en formato Linux. *Ejemplo:* `/root/documents`



Fecha de comienzo: indique la fecha de realización del análisis.

Hora de comienzo: especifique la hora del análisis, teniendo en cuenta si la hora es la marcada por el equipo (local) o por el servidor de Panda Cloud Office Protection.

Repetición: en el caso de que el análisis sea del tipo periódico, especifique aquí la periodicidad del mismo (diaria, semanal o mensual).

Opciones avanzadas de análisis

A esta pantalla se accede a través del vínculo **Opciones avanzadas** de la pantalla **Edición de perfil - nueva tarea de análisis**. En ella podrá configurar aspectos complementarios de los [análisis programados](#) con anterioridad.

Siga los siguientes pasos:

Seleccione en opciones generales si desea activar el análisis de archivos comprimidos.

Seleccione el software malintencionado que desea analizar.

Puede analizar todo por defecto y permitir excluir extensiones, carpetas o archivos. En este caso utilice los botones **Añadir**, **Vaciar** y **Eliminar** para conformar la lista de exclusiones.

Equipos con sistema operativo Linux

En la configuración avanzada de los análisis nuevos que se creen, no todas las opciones están disponibles en Linux.



Estas son las opciones avanzadas de análisis soportadas en Linux:

- Analizar archivos comprimidos.
- Analizar virus (siempre está activa).
- Analizar sospechosos.

El análisis de hacking tools y programas potencialmente no deseados estará siempre activo, sin embargo, las exclusiones no.

➡ *Por favor, tenga en cuenta que en Linux no hay protección en tiempo real. El método para proteger los equipos pasa por la realización de análisis bajo demanda o la [programación de análisis periódicos](#).*

Edición de perfil - opciones avanzadas

A esta ventana se accede haciendo clic sobre el vínculo **Opciones avanzadas**, en la pestaña **Principal** de la ventana **Edición de perfil**.

Aquí usted puede especificar aspectos que tienen que ver con la instalación de la protección en los equipos, así como con la conexión de éstos a Internet y a los servidores de Panda Cloud Office Protection. También podrá configurar opciones relacionadas con la cuarentena de los archivos sospechosos.

Instalación

Especifique en qué directorio quiere instalar la protección. Panda Cloud Office Protection muestra por defecto una ruta que usted puede modificar.

En el caso de los equipos con sistema operativo Linux, la instalación se realiza en un directorio por defecto que no puede ser modificado.



Conexión a Internet

Establezca cuál es la conexión a Internet del equipo, si ésta se realiza a través de proxy, y si se requiere una autenticación para dicho proxy.

En el caso de los equipos con sistema operativo Linux, esta configuración de la conexión a Internet es necesario hacerla desde el equipo mediante la línea de comandos.

Conexión con la Inteligencia Colectiva

El administrador podrá desactivar los análisis con la inteligencia Colectiva. Es recomendable mantener activa esta opción si desea disfrutar de toda la protección que la Inteligencia Colectiva proporciona.

En el caso de los equipos con sistema operativo Linux, no es posible desactivar la conexión con la Inteligencia Colectiva, por lo que siempre que los equipos estén conectados a Internet la protección instalada en ellos se alimentará de la Inteligencia Colectiva.

Opciones de conexión con el servidor

Determine cada cuánto tiempo desea que el equipo envíe información a los servidores de Panda Cloud Office Protection acerca del estado de la protección instalada. Modifique, si así lo desea, el número de horas que la aplicación muestra por defecto, pero siempre en un intervalo entre 12 y 24.

Usted también puede especificar el equipo a través del cuál desea que se centralicen las conexiones con el servidor de Panda Cloud Office Protection. Para ello, marque la casilla y haga clic en el botón **Seleccionar**. En la pantalla **Selección de equipo** elija el equipo o búsquelo mediante el botón **Buscar**. A continuación haga clic en **Aceptar**.

Requisitos del equipo que se utilizará para realizar las conexiones con el servidor



Conexión a internet.

Mínimo de 128 MB de RAM.

Deberá ser un [equipo protegido](#) (equipo perteneciente al listado de equipos protegidos) y además deberá disponer de una versión de agente 5.04 o superior.

No puede hallarse en situación de [lista negra](#).

No deberá llevar más de 72 horas sin conectarse con el servidor.

Opciones de cuarentena

Los archivos que se encuentran en situación de cuarentena son analizados hasta determinar si suponen una amenaza o no. En caso de no ser una amenaza, usted puede optar por restaurarlos, utilizando para ello la opción **Restaurar** de la ventana **Cuarentena** e indicando la ruta del directorio en el que se restaurarán.

Desinstalación

Utilice esta sección si desea establecer una contraseña de desinstalación. Le será requerida cuando usted desee desinstalar la protección de aquellos equipos a los que se aplique el perfil que está creando. Esta opción no está disponible para equipos con sistema operativo Linux.

Configuración de la protección antivirus

Para acceder a la configuración, haga clic en el **menú Instalación y Configuración / Perfiles / Crear nuevo perfil / Antivirus**.

Mediante las pestañas **Archivos**, **Correo y Web** usted puede configurar el comportamiento general de la protección permanente Antivirus para el perfil que está creando.



Pestaña *Archivos*

Aquí puede usted configurar el comportamiento básico de la protección antivirus en lo que a la protección de archivos se refiere. La protección permanente no se aplica a los equipos con sistema operativo Linux.

Seleccione la casilla Activar protección permanente de archivos.

A continuación, marque la casilla correspondiente si desea que la protección de archivos incluya a los archivos comprimidos.

Seleccione los tipos de malware que desea que sean detectados por la protección.



La detección de virus se encontrará activa siempre que la protección de archivos lo esté.

A continuación seleccione si desea que se bloqueen acciones maliciosas y la detección de archivos sospechosos en función de su comportamiento.

Si desea profundizar en esta configuración, haga clic en Opciones avanzadas. Accederá a la ventana [Opciones avanzadas Antivirus - Protección de Archivos](#).

Pestaña *Correo*

En esta ventana usted puede configurar cuál va a ser el comportamiento de la protección antivirus del perfil que está creando, en lo que a correo electrónico se refiere.

Si desea profundizar en la configuración de dicho comportamiento, haga clic en **Opciones avanzadas**. Accederá a la ventana [Opciones avanzadas Antivirus - Protección de Correo](#)



Active la protección permanente de correo y la de archivos comprimidos si desea que la protección se aplique también a este tipo de archivos.

Seleccione el tipo de malware que desea detectar. Marque la casilla correspondiente.

Haga clic en **Aceptar**.

Pestaña *Web*

Desde aquí puede configurar el funcionamiento de la protección para la navegación Web. De esta manera evitará verse afectado por malware o phishing procedente de páginas Web.

Esta protección va desactivada por defecto. Para activarla, siga los siguientes pasos:

Marque la casilla para activar la protección permanente para navegación Web.

Si desea activar la detección de phishing en las páginas Web, marque la casilla correspondiente.

La detección de virus se encuentra activada por defecto.

En el panel Detecciones por tipo de la ventana **Estado** se contabilizarán las detecciones realizadas en URLs con phishing dentro de la categoría **Phishing**, y las de URLs con malware dentro de la categoría **Otros**.

Estas detecciones también se muestran en:



- El reporte de detección.
- En los informes.

Las detecciones de URL con Phishing se contabilizan como Phishing y las de URL con malware se contabilizan dentro de la categoría **Otros**. Cualquier phishing o malware detectado por esta protección, será bloqueado.

Las detecciones de malware y phishing reportadas por la protección de navegación Web no se contabilizan como categorías bloqueadas.



La protección por URL analiza los puertos 80 para http, 443 para https y 8080 para proxy. Si se usa otro puerto distinto no serán inspeccionados.

Análisis locales

Panda Endpoint Protection es el nombre de la protección que Panda Cloud Office Protection despliega e instala en los equipos. Una vez instalada, usted puede acceder a las diferentes opciones de análisis mediante el menú contextual de windows o desde el menú contextual de la propia protección.

Análisis contextual sobre un elemento seleccionado

Seleccione una carpeta, unidad, archivo o cualquier otro elemento analizable y haga clic sobre él con el botón derecho. A continuación, aparecerá el menú contextual de windows, donde podrá seleccionar la opción **Analizar con Panda Endpoint Protection**.

Inmediatamente se lanza el análisis del elemento. Este análisis puede ser detenido y reanudado con posterioridad. Cuando finaliza muestra el resultado del análisis y le da la posibilidad de imprimir o exportar el informe y guardarlo en la ubicación que desee.

Análisis locales desde Panda Endpoint Protection



Análisis optimizado

Al seleccionar esta opción, Panda Endpoint Protection examinará las carpetas del PC donde suele ocultarse el malware, para poder detectar y eliminar las amenazas en el menor tiempo posible.

Otros análisis

Al hacer clic en esta opción dispondrá de las siguientes dos opciones:

Analizar todo mi PC

Esta opción analizará de forma exhaustiva todos los elementos de su PC: todas las unidades de disco, la memoria, etc. La duración de este análisis dependerá de la cantidad de datos almacenados en su PC, así como de las características de su equipo.

Analizar otros elementos...

Esta opción es la más adecuada cuando sólo quiere analizar algún archivo concreto, alguna carpeta, etc. Es decir, le permite analizar sólo aquello que le interesa en un momento concreto, sin tener que realizar un análisis completo del PC. Una vez seleccionada esta opción, localice las carpetas o archivos que desee analizar y haga clic en **Comenzar**.



Nota importante: Asegúrese de que su PC está conectado a Internet antes de comenzar el análisis para garantizar la máxima capacidad de detección.

Aparte de estos análisis, que puede realizar cuando desee, Panda Endpoint Protection le protege también de forma permanente analizando todos los archivos que usted abre o ejecuta en cada momento, y neutralizando las posibles amenazas.

Opciones avanzadas antivirus - protección de archivos

En esta pantalla usted puede configurar con detalle la protección antivirus que desea para un perfil, en lo que a la protección de archivos se refiere.



Analizar todos los archivos cuando se crean o modifican

Puede hacerlo en base a un criterio general para todo tipo de archivos. Esto quiere decir que todos los archivos serán analizados en el momento en que se crean o modifican.

Aunque esta opción no supone en sí un aumento de la protección, lo que sí propicia es rapidez, entendida ésta como la inmediatez que supone analizar los archivos en el mismo momento en que son creados o modificados.

La alternativa es analizar solo aquéllos archivos con determinado tipo de extensión. Para ello, podrá excluir del análisis las extensiones, carpetas o archivos que usted indique.

Exclusiones

En cada uno de los casos utilice los botones **Añadir**, **Eliminar** y **Vaciar** para conformar la lista de elementos (extensiones, carpetas, archivos) a excluir de los análisis.

Cuando haya finalizado, haga clic en **Aceptar** para guardar los cambios.

Opciones avanzadas antivirus - protección de correo

Para mantener un nivel óptimo de seguridad en sus equipos informáticos, resulta fundamental protegerlos de las amenazas que puedan llegar a través de sistemas de correo electrónico.

Panda Cloud Office Protection le permite configurar con detalle la protección antivirus de correo para cada perfil. Puede hacerlo de manera general para todos los archivos recibidos o según la extensión de los mismos.



En cada uno de los casos utilice los botones **Añadir**, **Eliminar** y **Vaciar** para conformar la lista de exclusiones.

Cuando haya finalizado, haga clic en **Aceptar** para guardar los cambios.

Configuración de la protección firewall

Introducción a la configuración del firewall

Para acceder a la configuración, haga clic en el menú Instalación y Configuración / Perfiles / Crear nuevo perfil / Firewall.

Lo primero que debe usted hacer a la hora de configurar la protección del firewall es decidir si los usuarios pertenecientes al grupo al que se aplique este perfil configurarán el firewall desde sus equipos o si será usted como Administrador quien se encargue de ello.

Permitir al usuario establecer la configuración del firewall

Si decide que sea así, seleccione la opción que permite que la configuración del firewall la establezca el usuario de cada equipo.

En este caso consulte la sección [Administración del firewall desde cliente](#).

Establecer la administración centralizada del firewall

Si, por el contrario, prefiere que la configuración se realice desde la [consola Web](#), será usted, como [Administrador](#), quien establezca las limitaciones, bloqueos, permisos, en definitiva, la configuración del firewall que se aplicará a los equipos que usted elija.



Panda Cloud Office Protection

Si opta por este método de administración centralizada del firewall desde la consola web, mantenga la opción por defecto **Aplicar la siguiente configuración al firewall**.

También tendrá que establecer sin la configuración de la protección firewall se aplicará también a servidores y/o estaciones Windows. Utilice para ello las casillas correspondientes.

A continuación podrá realizar todo el proceso de configuración a través de las opciones que encontrará en las pestañas [General](#), [Programas](#), [Prevención de intrusiones](#) y [Sistema](#).

Administración del firewall desde cliente

El usuario de Panda Endpoint Protection podrá acceder a la configuración del firewall siempre y cuando haya sido autorizado para ello por el administrador de Panda Cloud Office Protection, tal y como se ha comentado en el apartado [Introducción a la configuración del firewall](#).

Mediante la configuración del firewall desde Panda Endpoint Protection el usuario no sólo filtra las conexiones que entran y salen del ordenador cuando éste se conecta a Internet, sino que también interviene en las conexiones establecidas entre su equipo y otros equipos de la red con los que puede intercambiar archivos y compartir carpetas e impresoras, entre otras cosas.

Cada vez que un programa intente conectarse a Internet desde el equipo del usuario (conexiones salientes), o cuando se produzca un intento de conexión desde el exterior al PC del usuario (conexiones entrantes), Panda Endpoint Protection le preguntará a usted si desea autorizar dicha conexión. Para ello utilizará mensajes emergentes mediante los que usted podrá autorizar o no las conexiones y configurar aspectos relativos a las mismas.

Si usted desea denegar o autorizar permanentemente la conexión en cuestión, puede hacerlo seleccionando la opción correspondiente en el mensaje emergente.



*En el caso de las conexiones salientes, si marca la opción **Activar asignación automática de permisos**, Panda Endpoint Protection no le preguntará si autoriza las conexiones y las realizará de manera automática.*

De este modo, a medida que el usuario asigne permisos y concrete la configuración, obtendrá un control total de las conexiones que se establezcan desde su ordenador a la red local e Internet, y viceversa.

Acceso a la configuración de firewall en Panda Endpoint Protection

El acceso a las opciones de configuración del firewall en Panda Endpoint Protection se



realiza haciendo clic en el icono en la ventana principal.

Administración centralizada del firewall

Activar el firewall

Haga clic en el menú Instalación y Configuración / Perfiles / Crear nuevo perfil / Firewall.

Seleccione la casilla Aplicar la siguiente configuración al firewall.

Seleccione si desea aplicar la configuración del firewall a estaciones y/o servidores Windows.

Marque la casilla correspondiente al tipo de red al que se conectará. La configuración será más restrictiva si se trata de una ubicación pública y más flexible si la ubicación es de confianza.

Red pública

Una red de este tipo es propia de cyberlocales, aeropuertos, etc. Conlleva limitación de su nivel de visibilidad y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Red de confianza



Este tipo de red generalmente es de oficina o casera. El equipo es perfectamente visible para el resto de equipos de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

Haga clic en **Aceptar**.

Conexión de programas a la Red

Haga clic en el menú Instalación y Configuración / Perfiles / Crear nuevo perfil / Firewall/ Programas.

Active las reglas de TelefónicaMovistarPanda. Se trata de unas reglas predefinidas para las aplicaciones más comunes, y que le pueden facilitar al administrador de la red las tareas de configuración. Pueden ser modificadas, pero no eliminadas.

Añada programas y asígneles permisos de comunicación. Para ello haga clic en **Añadir**.

Modifique o elimine los programas añadidos, mediante los botones **Configurar** y **Eliminar**.

Decida si quiere permitir o denegar el acceso a comunicaciones para los que no exista una regla determinada. Utilice para ello la lista desplegable **Acción**

Los permisos pueden ser

 Permitir entrantes y salientes

El programa se podrá conectar a la red (Internet y redes locales) y también permitirá que otros programas o usuarios se conecten con él. Existen ciertos tipos de programas que requieren este tipo de permisos para funcionar correctamente: programas de intercambio de archivos, aplicaciones de chat, navegadores de Internet, etc.



Permitir salientes

El programa se podrá conectar a la red, pero no aceptará conexiones externas por parte de otros usuarios o aplicaciones.

Permitir entrantes

El programa aceptará conexiones externas de programas o usuarios procedentes de Internet, pero no tendrá permisos de salida.

No permitir ninguna conexión

El programa no podrá acceder a la red.

Prevención de intrusiones

Haga clic en el menú Instalación y Configuración / Perfiles / Crear nuevo perfil / Firewall/ Prevención de intrusiones

Usted puede configurar aquí cuál será el comportamiento de la protección firewall en cada perfil, en lo que a prevención de intrusiones se refiere.

Seleccione las casillas correspondientes y haga clic en **Aceptar**.

Reglas de sistema

Haga clic en el menú Instalación y Configuración / Perfiles / Crear nuevo perfil / Firewall/ Sistema.

¿Qué son las reglas de sistema?

Mediante las reglas de sistema usted puede establecer reglas de conexión que afectarán a todo el sistema, y que son prioritarias con respecto a las reglas configuradas anteriormente para la [conexión de los programas a la red](#).



A medida que usted vaya creando reglas de sistema, éstas aparecerán en el listado. El orden de las reglas en la lista no es aleatorio, es decir, su aplicación va en orden descendente, por lo que al desplazar una regla hacia arriba o abajo modificará la prioridad en su aplicación.

Creación de reglas de sistema

Active las reglas de TelefónicaMovistarPanda. Se trata de unas reglas predefinidas que le pueden facilitar las tareas de configuración.

Para añadir reglas de sistema haga clic en el botón **Añadir**. Accederá a la ventana **Edición de perfil-nueva regla de sistema**, donde podrá seleccionar la acción que desea denegar o permitir al sistema, elegir cuál será la dirección de la comunicación para dicha acción, y la red que se utilizará.

También puede determinar el protocolo, puerto, y los PCs a los que se aplicará la regla, especificando su dirección IP, su dirección MAC o ambas.

Para modificar o eliminar alguna de las reglas y permisos establecidos, utilice los botones **Configuración** y **Eliminar**.

Configuración del control de dispositivos

Dispositivos de uso común como las llaves USB, los lectores de CD/DVD, dispositivos de imágenes y Bluetooth pueden constituir también una vía de infección para los equipos cuya seguridad usted desea preservar.

La opción de configuración del control de dispositivos le permite determinar cuál será el comportamiento de este tipo de protección para el perfil que está creando. Para ello, seleccionará el dispositivo o dispositivos que desea autorizar y le asignará un nivel de utilización.



Notificaciones

Según cómo sea la configuración para los dispositivos, se mostrará un aviso advirtiéndolo de ello.

Dispositivos no permitidos

Cuando la protección detecte que se ha conectado al equipo un dispositivo cuyo uso no esté permitido por el perfil de seguridad que usted ha aplicado para ese equipo, se mostrará un aviso al respecto advirtiéndolo al usuario que no tiene permiso para acceder a dicho dispositivo.

Dispositivos con permiso de solo lectura

El dispositivo conectado se mostrará con normalidad en el directorio Mi PC del equipo. Al hacer doble clic sobre la unidad, se mostrará un aviso advirtiéndolo de que el usuario no tiene permiso para escribir en el dispositivo.

Para activar el control de dispositivos

En la ventana Edición de perfil seleccione Perfiles / Control de dispositivos.

Marque la casilla Activar el control de dispositivos.

A continuación puede elegir en el desplegable correspondiente el nivel de autorización que desea aplicar al dispositivo que le interesa configurar.

En el caso de las llaves USB y las unidades CD/DVD puede elegir entre *Permitir* o *Permitir lectura*. Para Bluetooth, los dispositivos de imágenes y los modems USB las opciones son *Permitir* y *No permitir*.



Haga clic en **Aceptar** para guardar la configuración del control de dispositivos.

Configuración de la protección para servidores Exchange

Introducción

Si usted dispone de las licencias correspondientes, desde su consola Web podrá activar la protección de Panda Cloud Office Protection para servidores Exchange y aplicarla a cualquier servidor Exchange que esté administrando.

➡ *Esta protección para servidores Exchange es aplicable a las versiones 2003, 2007 y 2010.*

La protección para servidores Exchange que ofrece Panda Cloud Office Protection Advanced está compuesta por las siguientes unidades:

Antivirus

Analiza en busca de Virus, Herramientas de hacking y programas potencialmente no deseados sospechosos, con destino a buzones situados en el servidor Exchange, así como el acceso a sus buzones y carpetas públicas.

Para saber más sobre esta protección, consulte [Antivirus para la protección de servidores Exchange](#).

Anti-spam

Esta unidad se encarga de detectar y detener el spam.

Para saber más sobre esta protección, consulte [Protección anti-spam para servidores Exchange](#).



Monitorización de la protección para servidores Exchange

Al igual que sucede con el resto de protecciones que ofrece Panda Cloud Office Protection Advanced (antivirus, firewall, control de dispositivos) el estado de la protección para servidores Exchange se mostrará en la ventana [Equipos](#), además de en los diferentes [informes](#) que Panda Cloud Office Protection Advanced proporciona.

Las detecciones reportadas por la protección para servidores Exchange serán visibles en:

La ventana [Estado](#), dentro de la sección **Detecciones por origen**, junto al resto de detecciones aportadas por las diferentes protecciones integradas en Panda Cloud Office Protection Advanced.

El [listado de detecciones](#).

Los [informes](#) de detección, informe ejecutivo e informe ejecutivo extendido.

Protección antivirus para servidores Exchange

Protección de buzones

Para acceder a la configuración de la protección Antivirus para servidores Exchange, haga clic en el menú **Instalación y Configuración / Perfiles / Crear nuevo perfil / Servidores Exchange / pestaña Antivirus**.

Aquí puede usted configurar el comportamiento básico de la protección Antivirus en lo que a protección de buzones de correo electrónico se refiere.

Protección de buzones

Active la casilla de verificación **Activar protección de buzones**.



Al activar la protección de buzones, podrá mantener libres de software malintencionado los correos electrónicos almacenados en los buzones de correo administrados por su servidor Exchange. De esta manera aumentará su seguridad y evitará el robo de datos y la pérdida de información.

En la sección **Software malintencionado a detectar** marque los elementos que desea detectar.

En las versiones anteriores a Microsoft Exchange 2013, existe una API de detección de virus que ofrece las funciones para el análisis de la protección de buzones.

En Exchange 2013 para interceptar el tráfico entre buzones se ha desarrollado un nuevo interceptador que recoge el tráfico entre buzones por SMTP (protocolo para la transferencia simple de correo electrónico).

Modelo de actuación de la protección Antivirus de Buzones

En buzones se actuará sobre el elemento concreto que se ha detectado como malware o sospechoso, no sobre el mensaje completo (por ejemplo, si se detecta malware en un fichero adjunto, se actúa sobre el propio fichero adjunto).

Las actuación se realiza de la siguiente forma:

Se realiza sobre el fichero en concreto la acción por defecto de la plataforma, determinada por el laboratorio: Desinfectar, Borrar, Mover a cuarentena...

Se notifica al usuario introduciendo un security_alert.txt.

Cuando se restaure de cuarentena, el correo se restaura al buzón de los destinatarios. Si se produce algún problema en esta restauración, se restaura directamente a la



carpeta Lost&Found, dejando un fichero con el nombre del elemento insertado en cuarentena.

Modelo de actuación de la protección Antivirus de buzones en Exchange 2013

La actuación en la protección de buzones de Exchange 2013 será equivalente a la actuación existente en la protección de transporte. La actuación será:

En caso de detectar malware o sospechosos los correos completos irán siempre a cuarentena.

Estos mensajes se mantienen en cuarentena un tiempo máximo:

Clasificación	Tiempo	Acción transcurrido el tiempo
Malware	7 días	Borrar
Sospechoso	14 días	Restaurar

Cuando un mensaje se mueve a cuarentena, se envía una notificación a los destinatarios del correo con el asunto original, avisando de que el correo ha sido bloqueado y de que contacte con su administrador si desea recuperar el mensaje.

Cuando se restaure de cuarentena, el correo se restaura al buzón de los destinatarios. Si se produce algún problema en esta restauración, se restaura directamente a la carpeta Lost&Found, dejando un fichero con nombre del asunto del mensaje. Este fichero contiene el mensaje completo.



Protección de transporte

Para acceder a la configuración de la protección Antivirus para servidores Exchange, haga clic en el menú **Instalación y Configuración / Perfiles / Crear nuevo perfil / Servidores Exchange / pestaña Antivirus**.

Aquí puede usted configurar el comportamiento básico de la protección Antivirus en lo que a protección de transporte se refiere.

Protección de transporte

Active la casilla de verificación **Activar protección de transporte**.

Al activar la protección de transporte asegurará que los correos electrónicos que circulen a través de sus servidores Exchange lo hagan con total seguridad y libres de virus y malware.

En la sección **Software malintencionado a detectar** marque los elementos que desea detectar.

Modelo de actuación de la protección Antivirus de Transporte

En la protección de transporte se actúa sobre el correo completo de la siguiente forma:

En caso de detectar malware o sospechosos se mueven los correos completos a cuarentena, independientemente de la acción que se debe realizar. Estos mensajes se mantienen en cuarentena el tiempo establecido por Panda Security.

Cuando un mensaje se mueve a cuarentena, se envía una notificación a los destinatarios del correo con el asunto original avisando de que el correo ha sido



movido a cuarentena y que contacte con su administrador si desea recuperar el mensaje.

Cuando se restaure de cuarentena, el correo se restaura al buzón de los destinatarios. Si se produce algún problema en esta restauración, se restaura directamente a la carpeta Lost&Found, dejando un fichero con nombre del asunto del mensaje. Este fichero contiene el mensaje completo.

Análisis inteligente de buzones

Si elige activar esta opción, la protección aprovechará los momentos de menor actividad de sus servidores Exchange para analizar en profundidad todos los correos electrónicos que almacenan.

Además de realizar el análisis en la franja horaria que menor impacto pueda tener en el normal funcionamiento de los servidores, solo serán analizados aquellos correos electrónicos que no lo hayan sido con anterioridad y que contengan archivos adjuntos.

Al desactivar la protección de buzones se deshabilita el análisis inteligente de buzones.

Modelo de actuación en las detecciones reportadas por los análisis en Background

La actuación en la protección de background es igual a la de buzones.



Los análisis en background no están disponibles para Exchange 2013.

Protección anti-spam para servidores Exchange

La eliminación del correo basura -spam- de los servidores Exchange es una labor que requiere de mucho tiempo de dedicación. El spam no solo supone un gran peligro de estafa, sino que además es una enorme pérdida de tiempo que usted no tiene por qué



soportar.

Para solucionar esta situación puede utilizar la protección anti-spam para servidores Exchange que le ofrece Panda Cloud Office Protection Advanced. Así conseguirá optimizar su tiempo de trabajo y aumentar la seguridad de sus servidores Exchange.

Para activar o desactivar esta protección, utilice la casilla de verificación **Detectar spam**.

Acción para mensajes de spam

Las acciones a llevar a cabo son:

Dejar pasar el mensaje

Se añadirá la etiqueta *Spam* al Asunto de los mensajes. Esta será la opción configurada por defecto.

Mover el mensaje a...

Será necesario especificar la dirección de correo electrónico a la que se moverá el mensaje, con la etiqueta *Spam* añadida en el *Asunto*.

Borrar el mensaje

Marcar con SCL (Spam Confidence Level)

¿Qué es SCL?

SCL -*Spam Confidence Level*- es una escala de valores comprendidos entre el 0 y el 9 que se aplican a los mensajes de correo electrónico susceptibles de ser spam. Para ello se analizan su cabecera, asunto y contenido.

El valor 9 se asigna a los mensajes que con total probabilidad son spam. El 0 es el



valor que se aplica a los mensajes que no son spam.

Este valor SCL se puede utilizar para marcar los mensajes que posteriormente serán tratados en función de un umbral configurable en Active Directory: Panda Cloud Office Protection Advanced marca el mensaje con el valor SCL correspondiente y le permite pasar.

A continuación será el Administrador, en función del umbral determinado en el Active Directory, quien seleccione la acción que finalmente se realizará con el mensaje.

Direcciones y dominios permitidos y denegados

Utilizando los botones **Añadir**, **Eliminar** y **Vaciar**, usted puede configurar listas de direcciones y dominios cuyos mensajes no serán analizados por la protección anti-spam (*lista blanca*) o, por el contrario, otra lista de dominios y direcciones cuyos mensajes serán interceptados por la protección y eliminados (*lista negra*).

Añadir: utilice este botón para seleccionar de una en una las direcciones y/o dominios que desea incluir en la lista.

Eliminar: utilice este botón si desea eliminar alguna de las direcciones y/o dominios.

Vaciar: si desea eliminar toda la lista de direcciones, haga clic en este botón.

A la hora de configurar las listas es importante tener en cuenta lo siguiente:

Si un dominio se encuentra en la lista negra y una dirección perteneciente a dicho dominio se encuentra en la lista blanca, se permitirá dicha dirección, pero no el resto de direcciones del dominio.



Si un dominio se encuentra en la lista blanca y una dirección perteneciente a dicho dominio se encuentra en la lista negra, dicha dirección no será aceptada, pero sí el resto de direcciones de dicho dominio.

Si un dominio (por ejemplo: domain.com) se encuentra en la lista negra y un subdominio de este (ej: mail1.domain.com) se encuentra en la lista blanca, se permitirán direcciones de dicho subdominio, pero no el resto de direcciones del dominio o de otros subdominios diferentes.

Si un dominio se encuentra en la lista blanca también se considerarán incluidos en la lista blanca todos sus subdominios.

Configuración del control de acceso a páginas Web

Para acceder a la configuración, haga clic en el menú Instalación y Configuración / Perfiles / Crear nuevo perfil y seleccione Control de acceso a páginas Web.

Si es usted un cliente nuevo que acaba de adquirir la versión más reciente del producto, esta opción estará activada por defecto.

Si su versión del producto no es la más reciente, deberá activar esta funcionalidad en la consola Web. Para ello deberá activar la casilla **Activar monitor de accesos a páginas Web**.

Con esta protección podrá restringir el acceso a determinadas categorías web y configurar URLs a las que autorizará o restringirá el acceso. Esto contribuirá a la optimización del ancho de banda de su red y a la productividad de su negocio.



Denegar el acceso a páginas Web

Las páginas Web se agrupan por categorías. Usted tan solo tendrá que seleccionar las categorías a las que desea denegar el acceso, y podrá modificar las categorías seleccionadas siempre que lo desee.

En la ventana **Edición de perfil**, marque la casilla que activa el monitor de accesos a páginas Web.

Seleccione las categorías a las que quiere denegar el acceso.



Cuando desde el equipo se intente acceder a una página Web que pertenece a una categoría bloqueada mediante protocolo HTTPS, se mostrará un aviso al respecto.

Recuerde que puede configurar la aparición o no de estos avisos desde la pestaña **Alertas** en la [configuración general del perfil](#).

Denegar el acceso a páginas de categoría desconocida

En el caso de páginas no categorizadas, puede optar por denegar el acceso también. Para ello no tiene más que activar la casilla correspondiente.

Es importante que tenga en cuenta que en el caso de Intranets o Webs de tipo interno que se conectan a través de los puertos 80 u 8080 puede suceder que se clasifiquen como pertenecientes a una categoría desconocida y, por tanto, se deniegue el acceso a ellas con el consiguiente perjuicio para los usuarios.

Por eso es conveniente que analice a fondo cual es la situación de estas conexiones antes de activar esta opción, aunque siempre puede optar por mantener activada la denegación de acceso a páginas de categoría desconocida y "rescatar" las páginas Web que necesita mediante su inclusión en la lista de direcciones y dominios permitidos.



Modificación de las categorías permitidas/denegadas y actualización en los equipos

Cuando se modifiquen las categorías a las que se desea restringir o permitir el acceso, transcurrirá un **plazo máximo de 4 horas** hasta que los equipos recojan la nueva configuración.

Durante este intervalo de tiempo el comportamiento del control de acceso a páginas Web será el anterior a la modificación.

No obstante, si fuera necesario forzar la actualización siempre puede hacerlo desde cada uno de los equipos en los que está instalada la protección. Para ello, haga clic en el icono de la protección situado en la barra de tareas, junto al reloj de Windows, y a continuación seleccione la opción **Actualizar**.

Lista de direcciones y dominios permitidos o denegados

Por otra parte, también podrá especificar listas de páginas Web a las que siempre se permitirá o denegará el acceso. Es lo que se denomina lista blanca (acceso permitido) o lista negra (acceso denegado).

Podrá modificar ambas listas en cualquier momento en función de sus necesidades.

Introduzca en la caja de texto la URL del dominio o dirección.

Haga clic en **Añadir**.

Utilice los botones **Eliminar** y **Vaciar** para modificar la lista en función de sus necesidades.

Finalmente, haga clic en **Aceptar** para guardar la configuración.



Una vez finalizada la configuración, en la ventana **Estado** podrá ver [un resumen de los accesos realizados a páginas Web](#) así como detalle de los mismos.

Base de datos de URLs accedidas desde los equipos

Cada uno de los equipos recopila en una base de datos información sobre las URL a las que se ha accedido desde él.

Esta base de datos solo se puede consultar en local, es decir, desde el propio equipo, durante un plazo de 30 días.

Los datos almacenados en la base de datos son:

Identificador del usuario.

Protocolo (http o https).

Dominio.

URL

Categorías devueltas por Commtouch.

Acción (Permitir/denegar).

Fecha de acceso.

Contador acumulado de accesos por categoría y dominio.

Creación de grupos

Panda Cloud Office Protection le permite reunir en un grupo una serie de equipos y aplicar a todo el grupo el mismo perfil de protección.

Haga clic en **Instalación y configuración > Grupos** para abrir la ventana principal



Grupos. A medida que usted vaya creando grupos y asociándolos a un perfil, los grupos aparecerán aquí, con su nombre y perfil.

Esta ventana estructura la información en cuatro columnas: **Nombre, Perfil, Número máximo de instalaciones, y Caducidad.** Estas dos últimas sólo serán visibles siempre y cuando usted haya seleccionado la opción **Permitir asignar restricciones a los grupos** en la ventana [Preferencias](#).

La aplicación muestra por defecto el grupo y el perfil **Default**. *Ninguno de ellos se puede eliminar.*

Haga clic en **Crear nuevo grupo** para acceder a la ventana **Edición de grupo**. Introduzca el nombre del grupo en el cuadro de texto correspondiente.

En la lista desplegable **Perfil** seleccione el perfil que desea asignar al grupo.



*Si ha seleccionado usted la opción **Permitir asignar restricciones a los grupos** en la ventana **Preferencias** podrá seleccionar la fecha de caducidad y el número máximo de instalaciones del grupo, utilizando para ello las casillas correspondientes.*

Asignar equipos a un grupo

Una vez asignado nombre y perfil al grupo nuevo, puede usted seleccionar los equipos que desea que formen parte de dicho grupo en la pestaña **Equipos disponibles**.

Para ello:

Seleccione los equipos que desea asignar y haga clic en **Asignar**

Haga clic en la pestaña **Equipos integrantes**, y compruebe que los equipos seleccionados han sido asignados y el grupo se ha creado correctamente.



Panda Cloud Office Protection

Si desea mover algún equipo o equipos de un grupo a otro, selecciónelo y elija el grupo en la lista desplegable **Mover equipos seleccionados al grupo**. A continuación haga clic en **Mover**.

Haga clic en **Aceptar** y la aplicación le mostrará la ventana principal **Grupos**. El grupo que usted acaba de crear aparecerá con su nombre y perfil en el listado.

Si quiere eliminar algún grupo, seleccione la casilla del grupo que desea borrar y haga clic en **Borrar**.

➡ **Nota:** *Tenga en cuenta que al eliminar un grupo se perderán definitivamente los datos relativos al mismo.*

Instalación de la protección

Recomendaciones previas a la instalación

Requisitos que deben cumplir los diferentes equipos

Independientemente del modo de instalación que vaya a utilizar, es recomendable consultar los [requisitos](#) que los diferentes equipos afectados por la instalación deben reunir.

Existencia de otras protecciones instaladas en los equipos


Es muy importante que antes de instalar Panda Cloud Office Protection en los equipos se asegure usted de que no hay instalado otro antivirus o solución de seguridad. Algunos de ellos serán detectados y desinstalados automáticamente por el instalador de Panda Cloud Office Protection.

Puede consultar una lista de los antivirus que Panda Cloud Office Protection desinstala automáticamente haciendo click [aquí](#).

Si el suyo no estuviera en la lista, desinstálelo manualmente:

 En Windows XP: Panel de Control > Agregar o quitar programas



 En Windows Vista o superiores: Panel de Control > Programas y características > Desinstalar

Configuración de exclusiones en la protección de archivos para servidores con Exchange Server

Con el fin de que no se produzcan interferencias entre los servidores de Panda Cloud Office Protection y Exchange, en servidores en los que se va a instalar o ya se ha instalado Panda Cloud Office Protection es necesario excluir una serie de carpetas del análisis de la protección de archivos.

Para más información, acuda al [centro de soporte técnico](#).

 *Si usted dispone de licencias de Panda Cloud Office Protection las exclusiones ya se habrán realizado por defecto.*

Instalación rápida

Si usted no necesita crear perfiles ni grupos diferentes a los que Panda Cloud Office Protection le proporciona por defecto —ambos se denominan **Default**— puede optar por realizar una instalación rápida de la protección.

Aunque tendrá que elegir entre [instalar mediante el programa de instalación](#) o [mediante la herramienta de distribución](#), al no tener que crear perfiles ni grupos adicionales el proceso de instalación será más breve.

Modificación del perfil Default

Si necesita modificar la configuración del perfil Default, siga los siguiente pasos:

En la ventana **Perfiles del programa de instalación**, haga clic en el nombre del perfil *Default*.



Panda Cloud Office Protection

Desde la ventana **Edición de perfil** podrá acceder a la configuración de la protección para [antivirus](#), [firewall](#), [control de dispositivos](#), [servidores exchange](#) y [acceso a páginas Web](#).

Seleccione el idioma de la protección, y haga clic en **Aceptar**.



*Si posteriormente desea restaurar el perfil Default, puede hacerlo con el botón **Restaurar configuración por defecto**.*

Casos de instalación

Instalación en equipos sin protección previa instalada

Acceda a la consola web e introduzca su Login Email y contraseña.

Cree un [perfil nuevo](#) (o utilice el [perfil por defecto](#), según sus necesidades).

Configure el comportamiento de la [protección antivirus](#), [protección firewall](#), [control de dispositivos](#) para el perfil nuevo. Si dispone de licencias de Panda Cloud Office Protection Advanced también podrá configurar la protección para servidores Exchange.

[Cree un grupo](#) (opcional).

Instale la protección. Utilice para ello el [modo de instalación](#) que mejor se adapte a sus necesidades y a las características de su red informática.

Instalación en equipos con protección previa instalada

El proceso de instalación es similar al caso anterior, pero es muy importante que antes de instalar la protección de Panda Cloud Office Protection en los equipos se asegure usted de que no hay instalado otro [antivirus](#) o solución de seguridad. Para ello consulte las [Recomendaciones previas a la instalación](#).



➡ *En la mayoría de los casos de instalación de la protección y desinstalación de protecciones previas, el número de reinicios que el proceso exige es de 1, y nunca será superior a 2.*

Modos de instalación

Instalar la protección mediante el instalador

Descarga del instalador

➡ *Antes de descargar el instalador, consulte los requisitos que los equipos deben cumplir.*

Seleccione el sistema operativo para el que va a descargar el instalador.

➡ *Tanto en Linux como en Windows el instalador es el mismo para plataformas de 32 y de 64 bits.*

A continuación especifique el grupo en el que se integrarán los equipos a los que instalará la protección.

Haga clic en **Descargar**.

En el área de Instalación y configuración, haga clic en **Utilizar programa de instalación** y a continuación en **Descargar programa de instalación**.

En el cuadro de diálogo de descarga de archivo seleccione **Guardar**, y una vez la descarga haya finalizado ejecute el archivo desde el directorio en el que lo haya guardado. El asistente le guiará a lo largo del proceso de instalación.

Distribuya la protección al resto de equipos de la red. Para ello puede utilizar sus propias herramientas o bien instalarlo manualmente.



Generar URL de instalación

Utilice esta opción si lo que desea es lanzar la instalación desde cada equipo. Simplemente copie la URL de instalación para el sistema operativo que necesite, y después acceda a ella desde cada uno de los equipos a los que tenga acceso y a los que desee instalar la protección.

Envío del enlace por correo

Haga clic en **Enviar por correo**. Automáticamente los usuarios recibirán un email con el enlace de descarga (recibirán el link de instalación para sistemas operativos Linux y para sistemas operativos Windows). Al hacer clic en cualquiera de los enlaces, se iniciará la descarga del instalador.

Instalar la protección mediante la herramienta de distribución

Descarga de la herramienta de distribución

Es importante que antes de descargar la herramienta de distribución, compruebe los [requisitos que debe reunir el equipo](#).

La [herramienta de distribución](#) le permite instalar y desinstalar la protección de forma centralizada en los equipos de la red con sistema operativo Windows, evitando así la intervención manual de los usuarios a lo largo del proceso.



Recuerde que, en el caso de que desee desinstalar la protección, se le solicitará que introduzca la contraseña que usted estableció para el perfil de configuración correspondiente.

En Instalación y configuración, haga clic en Descargar herramienta de distribución.

En el cuadro de diálogo de descarga de archivo seleccione **Guardar**, y cuando la descarga haya finalizado ejecute el archivo desde el directorio en el que lo haya



guardado. El asistente le guiará a lo largo del proceso de instalación.

Una vez instalada la herramienta de distribución de Panda Cloud Office Protection, es necesario abrirla para poder desplegar la protección en los equipos. A continuación se mostrará la ventana principal desde la que usted podrá instalar y desinstalar las protecciones.

Instalación de la protección

A la hora de seleccionar los equipos en los que instalar la protección, la herramienta de distribución le permite hacerlo en base a dos criterios: por dominios, o por IP/nombre de equipo.

Por dominios

Haga clic en Instalar protecciones.

Haga clic en **Por dominios**.

Especifique el grupo en el que desea agrupar los equipos (opcional).

Localice en el árbol los equipos a los que desea distribuir la protección, y marque la casilla correspondiente.

Opcionalmente, puede indicar un nombre de usuario y contraseña con privilegios de administrador en los equipos seleccionados.

Es aconsejable utilizar una contraseña de administrador de dominio. De este modo, no tendrá que indicar el nombre de usuario y la contraseña de cada equipo.

Por IPs o nombre de equipo

Haga clic en Por IPs o nombre de equipo.




Especifique el grupo en el que desea agrupar los equipos (opcional).


Indique los equipos a los que desea distribuir la protección.

Puede introducir los nombres de los equipos, sus direcciones IP o rangos de IP, separando estos datos con comas.

Haga clic en **Añadir** para sumarlos a la lista, y en **Eliminar** para suprimirlos.

 Ejemplo de IP individual: 127.0.0.1

 Ejemplo de nombre de equipo: EQUIPO03

 Ejemplo de rango de IP: 192.0.17.5-192.0.17.145

Opcionalmente, puede indicar un nombre de usuario y contraseña con privilegios de administrador en los equipos seleccionados.

Es aconsejable utilizar una contraseña de administrador de dominio. De este modo, no tendrá que indicar el nombre de usuario y la contraseña de cada equipo.

Para obtener información más detallada sobre la tarea, active el **Log de eventos** (menú **Ver**)

Instalación mediante otras herramientas

Si usted utiliza habitualmente herramientas de distribución de archivos propias puede utilizarlas para distribuir la protección.

Desinstalación de otras protecciones

Desinstalación automática

Al iniciarse el proceso de instalación, Panda Cloud Office Protection detecta muchas de



Panda Cloud Office Protection

las otras soluciones de seguridad existentes, y, acto seguido, las desinstala automáticamente.



Antes de instalar Panda Cloud Office Protection es necesario cerrar el resto de aplicaciones que se estén utilizando.

Puede consultar una lista de los antivirus que Panda Cloud Office Protection desinstala automáticamente haciendo click [aquí](#). Si el suyo no estuviera en la lista, desinstálelo manualmente.

Desinstalación manual



En Windows XP

Panel de Control > Agregar o quitar programas



En Windows Vista o Windows 7

Panel de Control > Programas y características > Desinstalar

A continuación, proceda a la instalación de Panda Cloud Office Protection.

Estado de la protección

Introducción

La ventana **Estado** es la primera que se muestra una vez que se accede a la consola.

Aquí puede ver cuál es el [número de licencias](#) que posee, cuáles están caducadas y cuáles están próximas a estarlo. También puede, si lo desea, activar más licencias.

Por otra parte, se le muestran en dos paneles el [número de detecciones](#) realizadas por la



Panda Cloud Office Protection

protección instalada en los diferentes equipos, agrupadas [por tipo](#) o [por origen](#).

Accesos a páginas Web

Si dispone de licencias de Panda Cloud Office Protection Advanced habrá podido configurar el [control de acceso a páginas Web](#) en el apartado de configuración de los diferentes perfiles de protección.

De acuerdo con la configuración realizada, en esta ventana **Estado** podrá ver los porcentajes de acceso a páginas Web que se han producido y obtener detalles sobre ello.



Si no dispone de licencias pero quiere probar o comprar Panda Cloud Office Protection Advanced, contacte con su distribuidor o comercial habitual.

Análisis programados y listado de detecciones

Si desea ver la lista de análisis programados, haga clic en el vínculo [Análisis programados](#).

Para obtener más información sobre las detecciones, haga clic en el vínculo [Listado de detecciones](#).

Licencias y detecciones

El área **Estado** se estructura en tres secciones: **Notificaciones**, **Licencias** y **Detecciones**.

Notificaciones

Este área sólo se mostrará cuando existan cuestiones que pueden ser de su interés, tales como la existencia de versiones nuevas del producto o avisos sobre incidencias técnicas, mensajes informativos acerca del estado de sus licencias, o cuestiones



críticas que requieran especialmente su atención.

La caducidad de las licencias supone que sus equipos dejan de estar protegidos, por lo que es recomendable que adquiera más licencias contactando con su distribuidor o comercial habitual.

Licencias

Aquí podrá usted ver el número de licencias de Panda Cloud Office Protection Advanced o de Panda Cloud Office Protection Advanced que haya contratado y cuál es su periodo de validez. Si desea más información acerca del control y la gestión de licencias, consulte el apartado [Gestión de licencias](#).



Cada cliente sólo puede disponer de licencias de un tipo, bien licencias de Panda Cloud Office Protection o de Panda Cloud Office Protection Advanced.

En este apartado también aparecerá la información sobre las licencias que usted posea de Panda Cloud Email Protection y/o Panda Cloud Internet Protection, protecciones para la [limpieza del correo electrónico y seguridad del tráfico web](#).

En caso de que disponga de más de dos mantenimientos de Panda Cloud Office Protection o de alguno de Panda Cloud Email Protection o Panda Cloud Internet Protection, podrá acceder al detalle de los mismos haciendo clic en el vínculo **Ver detalles**.

Si un mantenimiento caducara en menos de 30 días y, una vez caducado, el número de licencias consumidas superara al número de licencias contratadas que restan por consumir, usted podrá utilizar la opción de anulación de licencias. Para ello, haga clic en el vínculo **Gestionar la anulación de licencias** y accederá a la ventana **Anulación de licencias**.

Si es usted un usuario con permiso de control total, puede anular licencias de los equipos que usted seleccione. Si opta por esta opción, los equipos afectados por la



anulación de su licencia dejarán de estar protegidos y, una vez transcurrida su fecha de caducidad, pasarán automáticamente a la situación de **lista negra**.

Listado de licencias

Esta pantalla muestra la información en dos pestañas. En una de ellas se detalla la información sobre las licencias de Panda Cloud Office Protection o Panda Cloud Office Protection Advanced y en la otra la referente a otras protecciones.

En el caso de Panda Cloud Office Protection / Panda Cloud Office Protection Advanced, los datos se muestran en cuatro columnas: **Fecha de caducidad**, **Contratadas** (número total de licencias contratadas), **Tipo** (tipo de licencias), y **Unidades** (detalla la protección contratada: antivirus, firewall, control de dispositivos, exchange server y/o control de accesos a páginas Web).

En el caso de otros productos, se detalla el producto del que se trata, la fecha de caducidad de las licencias y su número.

A medida que las diferentes licencias vayan caducando, desaparecerán del listado.

Detecciones

Esta sección consta de dos paneles que muestran cuál es el estado de la protección antivirus que usted ha instalado en los equipos, en función del tipo y el origen de las detecciones.

En la gráfica de detecciones por tipo, las detecciones de Linux se añaden en la categoría apropiada. En caso de no poder identificar la categoría, se añadirán al contador **Otros**.

En la gráfica de detecciones por origen, las detecciones de Linux se suman al contador



de **Sistema archivos**.

Para conocer qué detecciones se han encontrado durante un periodo de tiempo determinado, seleccione una opción dentro de la lista desplegable **Periodo**, y haga clic en **Aplicar**.

Detecciones por tipo

Le mostrará las detecciones de cada tipo de amenaza encontradas. Además, se mostrarán también datos sobre el número de bloqueos de intentos de intrusión, de dispositivos, de operaciones peligrosas y de *tracking cookies*. En el caso de las URL, las consideradas como malware se incluyen en la categoría **Otros**, y las consideradas como phishing o fraude en la categoría **Phishing**.

Detecciones por origen

Le informará sobre el origen de las detecciones.

Se incluirán las detecciones reportadas por:

Sistema de archivos

Correo

Web (detección de páginas Web correspondientes a malware y/o phishing)

Firewall

Control de dispositivos (bloqueos de llaves USB, lectores de CD/DVD, dispositivos de imágenes y Bluetooth o accesos denegados a dichos dispositivos)

Exchange Server (detecciones realizadas en servidores Exchange)

Para ampliar los gráficos haga clic en ellos. También puede imprimirlos si así lo desea.

Si desea ver la lista de [análisis programados](#), haga clic en el vínculo **Análisis**



programados.

Para obtener más información sobre las detecciones, haga clic en el vínculo **Listado de detecciones**.



El listado de detecciones mostrará el detalle de las detecciones correspondientes a los últimos siete días.

Control de accesos a páginas Web

Si usted dispone de licencias de Panda Cloud Office Protection Advanced podrá ver en este panel la información correspondiente a las páginas Web a las que se ha accedido desde los diferentes equipos de su red.

La configuración de estas categorías la habrá realizado previamente en la [configuración del control de acceso a páginas Web](#).

Como puede observar, la información se presenta en forma de gráfico coloreado con los colores asignados a las diferentes categorías. Cada porción del gráfico detalla el porcentaje de accesos a la categoría en cuestión.

Si hace clic en el gráfico, éste se ampliará.

Si utiliza el link **Ver detalle de accesos a páginas Web** situado en la parte inferior del panel, accederá a la ventana **Accesos a páginas Web**.

En la ventana **Accesos a páginas Web**, en primer lugar seleccione si desea que se le muestren los datos correspondientes a los últimos siete días, últimas 24 horas o último mes. Haga clic en **Aplicar**.



La información resultante se muestra en cuatro paneles:

Top 10 de Categorías más accedidas

Top 10 de Equipos que más acceden

Top 10 de Categorías más bloqueadas

Top 10 de Equipos con más accesos bloqueados

Si lo que desea es ver el listado completo de categorías accedidas y bloqueadas o el de equipos con accesos a páginas Web, utilice el link **Ver listado completo**.

Equipos que más acceden/con más accesos bloqueados

Si hace clic en el nombre de un equipo se mostrarán todos los accesos que desde el equipo seleccionado se han permitido o denegado a las diferentes categorías.

Categorías más accedidas/bloqueadas

Si hace clic en el nombre de una categoría, se mostrarán los accesos que se han permitido o denegado a páginas Web de esa categoría para todos los equipos.


Puede exportar los resultados utilizando la opción **Exportar a excel o .csv**.


Análisis programados

Desde esta ventana usted puede conocer en todo momento qué tareas de análisis programados se han creado para los diferentes perfiles de configuración, y acceder a los resultados de dichas tareas. Para acceder a esta ventana, haga clic en el vínculo **Análisis programados** de la ventana **Estado**.


La información se estructura en cuatro columnas:



 **Nombre.** Muestra el nombre de la tarea de análisis programado. Si hace clic sobre el nombre de la tarea, podrá acceder a la vista de resultados del análisis programado.

 **Perfil.** Indica el perfil de configuración al que pertenece el análisis programado.

 **Periodicidad.** Detalla el tipo de análisis (periódico, inmediato, programado).


 **Estado tarea.** En esta columna se utilizan una serie de iconos para indicar el estado de la tarea de análisis (*En espera, En curso, Finalizada con éxito, Finalizada con error, Finalizada por timeout*). Puede usted ver la lista de iconos situando el cursor sobre la opción **Leyenda**.


Resultados de tareas de análisis programados


En esta ventana se muestra un listado de los equipos que se encuentran involucrados en tareas de análisis, salvo que la tarea se encuentre en situación de *En espera*.


Si se trata de un análisis de tipo periódico, usted podrá elegir entre las opciones **Ver resultados del último análisis** o **Ver resultados de análisis anteriores**.

Los datos se muestran en seis columnas:


 **Equipo.** Indica cuál es el equipo involucrado en la tarea. Este equipo aparecerá con su nombre o con su [dirección IP](#), según lo que haya seleccionado usted en la ventana [Preferencias](#).

 **Grupo.** El grupo al que pertenece el equipo.

 **Estado.** En esta columna se utilizan una serie de iconos para indicar el estado del equipo involucrado en la tarea (*Error, Analizando, Finalizando, Tiempo de espera superado*). Puede usted ver la lista de iconos situando el cursor sobre la opción **Leyenda**.

 **Detecciones.** Se muestra el número de detecciones realizadas durante la tarea. haga clic sobre el número y accederá al [listado de detecciones](#).

 **Fecha de comienzo.** Indica la fecha y hora de comienzo de la tarea.

 **Fecha de fin.** Indica la fecha y hora de finalización de la tarea.



Si desea consultar la [configuración de los análisis programados](#) para el perfil de protección al que pertenece el equipo, haga clic en el vínculo **Ver configuración**.

Equipos con sistema operativo Linux

En los equipos con sistema operativo Linux, la protección permite hacer análisis bajo demanda y programados. A la hora de seleccionar los elementos a analizar, el comportamiento de la protección es el siguiente:

 **Todo el PC.** Analizará todos los discos duros.

 **Discos duros.** Analizará todos los discos duros.

 **Correo.** No analizará nada dado que en Linux no se analizan carpetas de correo.

 **Otros elementos.** Permite seleccionar rutas en formato Linux.

Ejemplo: /root/documents

Para saber más acerca de los análisis programados, consulte la sección [Opciones avanzadas de análisis](#).

Listado de detecciones

Mediante la monitorización de detecciones, usted puede realizar búsquedas en su red informática para saber cuándo han sido amenazados los equipos, qué tipo de amenaza ha sido detectada, y qué acción ha sido puesta en marcha.

Utilice el desplegable **Opciones** para activar el filtro que le permitirá buscar equipos en función del grupo al que pertenezcan y del tipo de detección realizada.



Panda Cloud Office Protection

Seleccione el tipo de amenaza detectada o el origen de la detección. También puede optar por seleccionar **Todas las detecciones**.

Haga clic en **Buscar**.

Resultado de la búsqueda

La columna **Equipo** muestra el listado de los equipos analizados, denominándolos por su nombre o por su IP. Si usted desea cambiar el modo en el que se nombran, puede hacerlo desde **Preferencias > Vista por defecto**.

En la columna **Grupo** se detalla el grupo al que pertenece el equipo.

La columna **Nombre** le indica cómo se llama la amenaza detectada, y la columna **Tipo** proporciona información acerca del tipo de amenaza y/o dispositivo bloqueado (llaves USB, unidades de CD/DVD, Bluetooth, dispositivos de imágenes,...). En el caso de las URLs se especifica si se trata de URL categorizada como malware o como phishing.

Ocurrencias indica el número de veces que se ha producido la detección.

Finalmente, **Acción** indica qué medidas ha llevado a cabo Panda Cloud Office Protection para bloquear el ataque, y en **Fecha** usted podrá ver la fecha y hora exactas en que fue detectada la amenaza.



El listado de detecciones muestra el detalle de las detecciones correspondientes a los últimos siete días.



*Como norma general a toda la ventana **Monitorización de detecciones**, al situar el cursor sobre cualquiera de los equipos del listado de búsquedas aparece una etiqueta amarilla con información ampliada sobre la detección seleccionada.*



➡ *En el caso de equipos con sistema operativo Linux, los valores que se muestran en los detalles de la detección son los mismos que se muestran para la protección permanente de los equipos con sistema operativo Windows.*

Por último, puede usted obtener más detalles de la detección. Para ello haga clic en el signo [+] situado junto al nombre o IP de cualquiera de los equipos, y accederá a la ventana **Detalles de detección**.

Las detecciones reportadas por los análisis en background de la protección Exchange (Exchange 2007 / Exchange 2010), se muestran en el detalle de detección como "Notificado por: Análisis inteligente de buzones".

➡ *En los servidores Exchange 2003 no se puede diferenciar que se ha detectado en background y aparecen igual que las detecciones de buzones ("r;Notificado por: Protección Exchange Server ").*

En algunos casos podrá acceder a la información que Panda Security ofrece en su página web sobre determinadas amenazas. Para ello, haga clic en el vínculo **Ver descripción**.

Exportar el listado

La lista de detecciones obtenida se puede exportar, bien en formato excel o en CSV.

Para ello, haga clic sobre el icono correspondiente junto al texto **Exportar a**.


Ambos formatos incluyen una cabecera que especifica la fecha y hora en que se ha emitido el archivo, un resumen de los criterios de búsqueda utilizados, y el detalle del listado, incluyendo la dirección IP origen de la infección o infecciones detectadas.



Monitorización de los equipos

Introducción

Desde la consola Web usted puede ver cuál es el estado de los equipos. En el caso de equipos a los que se ha distribuido la protección, puede monitorizar en todo momento el estado de la misma. Para ello, Panda Cloud Office Protection utiliza dos listas de equipos:

 Lista de [equipos protegidos](#)

 Lista de [equipos desprotegidos](#)

Cada lista ofrece una visión general del estado de la protección en los equipos que la integran, pero además también permiten conocer al detalle si la protección se ha instalado correctamente, si se ha producido algún error durante el proceso de instalación, si se encuentra a la espera de reinicio y cuál es su nivel de actualización, por ejemplo.

Para acceder a las listas de equipos protegidos y desprotegidos utilice la pestaña **Equipos**. A continuación se mostrará la pantalla **Equipos**, que tiene dos pestañas: **Protegidos** y **Desprotegidos**.

Seleccione la pestaña correspondiente. Podrá realizar búsquedas de equipos y exportar la lista a formato excel o csv. En ambos casos, al hacer clic sobre el nombre de un equipo accederá a la ventana de detalle del equipo.

Acceso remoto a los equipos

Tanto en la pestaña de **Equipos Protegidos** como en la de **Equipos Desprotegidos**, se indican los equipos en los que se ha instalado previamente alguna herramienta de control remoto, de tal manera que usted, en función de los permisos que posee, puede utilizar dicha herramienta para acceder a ellos desde su consola de administración.



No se podrá acceder remotamente a los equipos desprotegidos que se encuentren en alguno de los siguientes estados:

- Equipo descubierto
- Equipo desinstalado

Si el equipo tiene varias herramientas de acceso remoto instaladas y sitúa el cursor sobre el icono que aparece en la columna **Acceso remoto**, podrá ver con detalle qué herramientas de acceso remoto hay instaladas en el equipo. Haga clic sobre el icono para acceder al equipo.

Si el equipo dispone de varias herramientas de VNC instaladas, (RealVNC, UltraVNC, TightVNC), sólo podrá acceder remotamente a través de una de ellas, siguiendo la siguiente prioridad:

- RealVNC
- UltraVNC
- TightVNC

Si desea conocer cómo es el proceso de instalación de las herramientas de acceso remoto en los equipos, haga clic en el vínculo que encontrará dentro del recuadro informativo de color azul. Para más información, visite el apartado [Acceso remoto a los equipos](#).

Equipos protegidos

La lista de equipos protegidos le permite conocer el estado en el que se encuentra la protección instalada en los equipos de su red informática.

Búsqueda de equipos




Panda Cloud Office Protection

Puede elegir que se le muestren todos los equipos protegidos, utilizando para ello el botón **Mostrar todos**, o puede utilizar el desplegable **Opciones** y activar el filtro que le permitirá buscar equipos en función del estado en el que se encuentra la protección instalada en ellos: activada, desactivada, con error, pendiente de reinicio, etc.


Pero esta herramienta de búsqueda también es muy útil para conocer qué equipos no disponen de la versión actualizada del archivo de identificadores o disponer de un listado de los que, por alguna razón, no se han conectado con el servidor de Panda Cloud Office Protection en las últimas 48 horas.


Seleccione el estado que le interesa en el desplegable **Estado del equipo**, y haga clic en **Buscar**.


La información resultante de la búsqueda se presenta en cinco columnas:

 La columna **Equipo** muestra el listado de los equipos analizados, denominándolos por su nombre o por su IP. Si hay diferentes equipos con igual nombre y dirección IP, se mostrarán como equipos diferenciados en la consola web siempre y cuando tanto su [dirección MAC](#) como su [identificador del agente de administración](#) sean diferentes.

Si usted desea cambiar el modo en el que se nombran, puede hacerlo en **Preferencias > Vista por defecto**.

 Las columnas **Actualización Protección**, **Actualización Identificadores**, y **Protecciones** utilizan una serie de iconos para indicar el estado de actualización de las protecciones y la situación general de la protección en sí. Sitúe el cursor sobre el icono para visualizar la información.

 En **Última conexión** podrá ver la fecha y hora exactas de la última conexión del equipo con el servidor de actualizaciones.

 **Acceso remoto**. Si esta columna muestra un icono, indica que el equipo tiene instalada alguna herramienta de acceso remoto. Si solo es una, haciendo clic sobre el icono podrá acceder a la herramienta y, una vez introducidas las credenciales correspondientes, acceder al equipo.

Si el equipo tiene instaladas varias herramientas de acceso remoto, al situar el cursor sobre el icono se mostrarán dichas herramientas y podrá elegir cuál de ellas desea utilizar para acceder al equipo.



Si sitúa el cursor sobre el nombre de un equipo, se mostrará una etiqueta amarilla con información sobre la dirección IP del equipo, el grupo al que pertenece y el sistema operativo que tiene instalado.

Equipos desprotegidos

En esta pantalla usted podrá ver cuáles son los equipos que se encuentran desprotegidos.


Un equipo puede figurar como desprotegido cuando está en proceso de instalación/desinstalación de la protección o cuando al instalar o desinstalar se ha producido algún error.


Búsqueda de equipos

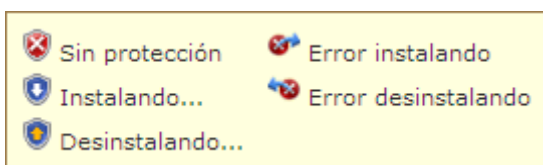
Puede elegir que se le muestren todos los equipos desprotegidos, utilizando para ello el botón **Mostrar todos**, o puede utilizar el desplegable **Opciones** para activar el filtro que le permitirá buscar equipos que se encuentran desprotegidos debido a diferentes razones.

Seleccione el estado que le interesa en el desplegable **Estado del equipo**, y haga clic en **Buscar**.

La información resultante de la búsqueda se presenta en cinco columnas:

 La columna **Equipo** muestra el listado de los equipos analizados, denominándolos por su nombre o por su IP. En el supuesto de que el nombre del equipo no se conozca, se mostrará la cadena *Desconocido*.

 La columna **Estado** muestra cuál es la situación de la protección. Para ello utiliza una serie de iconos:



En la columna **Detalle** se especifica el motivo por el cuál el equipo se encuentra en determinado estado. Por ejemplo, si muestra el estado *Error instalando*, en **Detalle** se puede mostrar el código del error producido. Si, por el contrario, la columna **Estado** muestra *Sin protección*, **Detalle** mostrará la explicación *Protección desinstalada*.

Última conexión. Muestra la fecha y hora en que tuvo lugar la última conexión con el equipo.

Acceso remoto. Si esta columna muestra un icono, indica que el equipo tiene instalada alguna herramienta de acceso remoto. Si solo es una, haciendo clic sobre el icono podrá acceder a la herramienta y, una vez introducidas las credenciales correspondientes, acceder al equipo.

Si el equipo tiene instaladas varias herramientas de acceso remoto, al situar el cursor sobre el icono se mostrarán dichas herramientas y podrá elegir cuál de ellas desea utilizar para acceder al equipo.

Detalle de equipos

Si desea acceder a los detalles de protección de un equipo concreto, haga clic en dicho equipo. A continuación se mostrará la ventana **Detalles de equipo protegido**, con información sobre el estado de las protecciones instaladas en el equipo.

Utilice el campo **Comentario** si desea añadir información adicional que le pueda ayudar a identificar el equipo. Si es usted un usuario con permiso de monitorización no podrá acceder a este campo. Para más información, consulte el apartado [Tipos de permisos](#).

Para añadir el equipo a la lista negra haga clic en **Añadir a lista negra**. Para eliminarlo de la base de datos utilice el botón **Eliminar de la base de datos**.



Exportar el listado

La lista de equipos obtenida tras realizar una búsqueda se puede exportar, bien en formato excel o en CSV.

Para ello, haga clic sobre el icono correspondiente junto al texto **Exportar a**.

Ambos formatos incluyen una cabecera que especifica la fecha y hora en que se ha emitido el archivo, un resumen de los criterios de búsqueda utilizados, y datos sobre el equipo, grupo al que pertenece, versión del archivo de identificadores y de la protección, sistema operativo, y dirección IP.

Acceso remoto a los equipos

La funcionalidad de acceso remoto a los equipos resulta muy útil cuando usted desea acceder a los equipos de su red desde su consola de administración sin necesidad de trasladarse.



El control remoto de los equipos solo es posible para los equipos con sistema operativo Windows

Panda Cloud Office Protection le permite acceder a los equipos utilizando alguna o algunas de las herramientas de acceso remoto siguientes:



TeamViewer



RealVNC



UltraVNC



TightVNC



LogmeIn



En la ventana **Equipos** se mostrarán mediante un icono los equipos que tienen instalada alguna de estas herramientas de acceso remoto. Si solo es una, haciendo clic sobre el icono podrá acceder a la herramienta y, una vez introducidas las credenciales correspondientes, acceder al equipo.

Puede introducir las credenciales desde la propia ventana de equipos o desde la de [Preferencias](#).

Si el equipo tiene instaladas varias herramientas de acceso remoto, al situar el cursor sobre el icono se mostrarán dichas herramientas y podrá elegir cuál de ellas desea utilizar para acceder al equipo.

En el apartado [Comportamiento de las herramientas de acceso remoto](#) encontrará información sobre cada una de las herramientas.



En el caso de que el equipo tenga más de una herramienta VNC instalada, solo se podrá acceder a través de una de ellas, siendo la prioridad de acceso la siguiente:

1-RealVNC

2-UltraVNC

3-TightVNC

Dependiendo de si usted posee [permiso de control total](#) o de [administrador](#), podrá utilizar el acceso remoto para acceder a más o menos equipos. Si su permiso es de [monitorización](#), no podrá acceder a ninguno y el icono de la columna **Acceso remoto** aparecerá deshabilitado.

Cómo obtener acceso remoto

Acceso desde la ventana Equipos



La primera vez que accede a la ventana **Equipos** se mostrará un aviso indicándole que sus equipos no disponen de acceso remoto instalado.

Si desea instalarlo utilice el vínculo que se le mostrará en el aviso.

Acceso remoto desde la ventana **Detalles de equipo**

Desde la ventana **Detalles de equipo** también podrá utilizar el acceso remoto, siempre y cuando el equipo seleccionado tenga alguna de las herramientas de acceso remoto instalada. Si es así, haga clic en el icono de la herramienta de acceso remoto que desee usar para ello.

Para poder tener acceso remoto, deberá instalar en sus máquinas una de las soluciones de control remoto soportadas: TightVNC, UltraVNC, RealVNC, TeamViewer, LogMeIn.

En el caso de las herramientas VNC se seguirá la misma prioridad comentada anteriormente para el caso de que el equipo tenga instaladas más de una de estas herramientas.

Comportamiento de las herramientas de acceso remoto

Herramientas VNC

Estas herramientas sólo se podrán utilizar para acceder a equipos que estén en la misma red local que la del cliente.

Dependiendo de la configuración de autenticación de las herramientas, es posible que se pueda acceder a ellas sin necesidad de incluir credenciales de acceso remoto en la consola, o, por el contrario, tenga que configurar únicamente el password de acceso remoto o tanto el usuario como la password para poder conectar remotamente.

Para que al administrador pueda acceder a sus equipos a través de estas



herramientas, debe permitir la ejecución del applet de Java en su propio equipo, en caso contrario, el acceso a los equipos, no funcionará correctamente.

TeamViewer

Esta herramienta se podrá utilizar para acceder a equipos que se encuentren fuera de la red local del cliente.

Para acceder a los equipos a través de TeamViewer solo será obligatorio introducir la password de los equipos, el campo "usuario" puede dejarse en blanco.



La password que hay que incluir para acceder a un equipo a través de TeamViewer, es la password de TeamViewer del equipo o la password configurada para el acceso no presencial, y no la password de la cuenta de cliente de TeamViewer.

Es recomendable disponer de la misma password de TeamViewer en todos los equipos, ya que cada usuario de la consola de Panda Cloud Office Protection sólo puede incluir una password para el acceso remoto a sus equipos a través de TeamViewer.

El equipo del administrador (equipos a través del cual se accede a la consola), deberá disponer de TeamViewer instalado (no es suficiente disponer de TeamViewer en modo ejecutor en dicho equipo).

LogMeIn

Esta herramienta se podrá utilizar para acceder a equipos que se encuentren fuera de la red local del cliente.

Para acceder a los equipos a través de LogMeIn, será necesario incluir el usuario y la password de la cuenta de LogMeIn.



Búsqueda de equipos desprotegidos

Con el fin de facilitar y mejorar la labor del administrador a la hora de monitorizar la protección instalada en los equipos, Panda Cloud Office Protection permite establecer tareas de búsqueda y detección de equipos desprotegidos.

Esta labor de búsqueda se puede realizar incluso cuando el administrador no se encuentra dentro de la red que se quiere monitorizar, es decir, el administrador puede, desde una ubicación remota, ver en todo momento en su consola información actualizada tanto de equipos protegidos como desprotegidos.



La búsqueda de equipos desprotegidos no está disponible para equipos con sistema operativo Linux.



Si necesita o desea ejecutar de forma simultánea búsquedas de equipos desprotegidos y tareas de desinstalación remota de las protecciones, consulte el apartado [Compatibilidad de tareas de gestión remota](#).

Establecer tareas de búsqueda de equipos desprotegidos

En la ventana principal de la consola web, haga clic en **Instalación y configuración**. A continuación, en el menú de la izquierda seleccione la opción **Búsqueda**. Accederá a la pantalla **Búsqueda de equipos desprotegidos**.

Para establecer una tarea de búsqueda, haga clic en **Nueva búsqueda**. A continuación, en la pantalla **Edición de búsqueda** podrá delimitar qué equipo será el encargado de realizar la búsqueda -utilice el botón **Seleccionar**.

El alcance de la búsqueda se definirá en función de que usted decida realizarla en la subred del equipo encargado de llevar a cabo la búsqueda, en rangos de direcciones IP



determinados, o en dominios concretos.

Requisitos del equipo que realiza la búsqueda

Para poder llevar a cabo la tarea de búsqueda, el equipo encargado de ello tiene que reunir una serie de requisitos.

Ha de disponer de conexión a Internet y haberse conectado durante las últimas 72 horas con el servidor de Panda Cloud Office Protection

Debe estar debidamente protegido con la versión 5.05 o superior de Panda Cloud Office Protection

Debe estar operativo y no podrá encontrarse en situación de lista negra ni realizando tareas de desinstalación remota.



Es importante que compruebe que el equipo no tiene configurada una tarea de desinstalación remota. Para más información, consulte el apartado [Compatibilidad entre tareas de gestión remota](#).

Debe ser un equipo con sistema operativo Windows.

Deber ser un equipo con sistema operativo Windows.

Para conocer más acerca de cómo se muestran los resultados de las búsquedas una vez que han finalizado, consulte el apartado [Visualización y resultado de la búsqueda](#).

Visualización y resultado de la búsqueda

Las búsquedas creadas aparecerán listadas en la pantalla **Búsqueda de equipos desprotegidos**, desde donde podrá también eliminar las tareas si así lo desea, utilizando para ello el botón **Eliminar**.

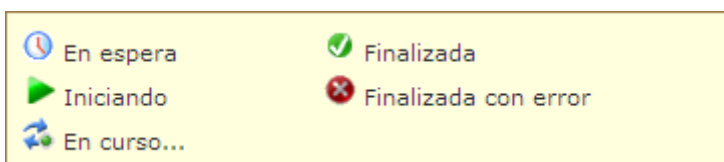


Las tareas en estado **Iniciando** o **En curso** no se pueden eliminar.

En esta pantalla la información se organiza en las siguientes columnas:

Nombre: muestra el nombre que se ha dado a la búsqueda cuando se ha creado.

Estado: indica mediante iconos el estado en que se encuentra la tarea de búsqueda.



Descubiertos: detalla el número de equipos desprotegidos encontrados.

Fecha creación: fecha en que se creó la tarea de búsqueda.

Creado por: usuario que creó la tarea de búsqueda.

Según el permiso del que usted disponga podrá crear, visualizar o eliminar tareas de búsqueda de equipos desprotegidos. Para más información, consulte el apartado [Tipos de permisos](#).

Resultado de las búsquedas

Si hace clic sobre el nombre de una búsqueda, accederá a una pantalla donde se le ofrecerán detalles acerca del resultado obtenido por la búsqueda seleccionada.

Al hacer clic el nombre de una búsqueda de las que aparecen en la pantalla **Búsqueda de equipos desprotegidos** accederá a la pantalla **Resultado de la búsqueda**. Aquí se mostrarán los equipos desprotegidos que se han descubierto tras ejecutar la tarea de búsqueda correspondiente.



Además del nombre de la búsqueda, sus fechas de inicio y fin y el estado, esta pantalla también proporcionará información cuando durante la ejecución de la búsqueda se haya producido algún error.



*En el caso de que la tarea esté en estado **En espera**, la fecha de inicio mostrará un guión (-). Lo mismo sucederá con la fecha de fin si la tarea no ha finalizado.*

Si desea consultar la configuración de la tarea de búsqueda, utilice el vínculo **Ver configuración**.

Cuarentena

Panda Cloud Office Protection almacena en situación de cuarentena aquellos contenidos sospechosos de ser maliciosos o aquellos no desinfectables, así como el spyware y herramientas de hacking detectadas.

Una vez que los elementos sospechosos han sido enviados para su análisis, se pueden producir tres situaciones:



Si se comprueba que **los elementos son maliciosos**, son desinfectados y posteriormente restaurados a su ubicación original, siempre y cuando exista desinfección para ello.



Si se comprueba que los elementos son maliciosos y no existe manera de desinfectarlos, son eliminados.



Si se comprueba que **no se trata de elementos perjudiciales**, son restaurados directamente a su ubicación.

En los equipos Linux, ni los elementos sospechosos ni el malware detectado se envían a cuarentena.



El malware detectado será desinfectado o eliminado y sobre los sospechosos se informa, pero no se realiza ninguna acción.

En la ventana principal de la consola web, haga clic en **Cuarentena** para abrir la ventana del mismo nombre. La ventana se estructura en dos secciones: una zona de búsqueda y otra para mostrar el listado de elementos resultantes de dicha búsqueda.

En la zona de búsqueda usted puede filtrar los elementos que desea visualizar en función de cuatro características:

Motivo

Seleccione en la lista desplegable **Motivo** el tipo de archivos que desea buscar. Los archivos se clasifican en función de la razón o motivo por la que fueron puestos en cuarentena.

Por defecto, se muestran los elementos que se han enviado a cuarentena por ser considerados sospechosos.

Grupo

Una vez seleccionado el tipo de archivos que desea buscar, seleccione en qué grupo de equipos desea centrar la búsqueda.

Fecha

Seleccione el periodo de tiempo que desea.

Haga clic en **Buscar**.



Si desea restaurar algún elemento, marque la casilla correspondiente, haga clic en **Restaurar** y responda afirmativamente al mensaje de confirmación. A continuación, el elemento desaparecerá del listado de búsqueda y podrá usted encontrarlo en la pestaña **Archivos excluidos del análisis**.

Si lo que quiere es eliminar alguno de los elementos encontrados, seleccione la casilla correspondiente, haga clic en **Eliminar** y responda afirmativamente al mensaje de confirmación.

➡ *En el caso de que existan varios elementos que contengan el mismo tipo de malware, al restaurar o eliminar uno de ellos se restaurarán o eliminarán todos.*

➡ *Al situar el cursor sobre cualquiera de los elementos del listado de búsqueda, aparece una etiqueta amarilla con información sobre dicho elemento.*

➡ *La columna **Equipo** muestra el nombre del equipo o su IP, en función de lo que usted seleccione en la opción **Vista por defecto**, en **Preferencias**.*

Archivos excluidos del análisis

Cuando usted selecciona un elemento en la ventana [Cuarentena](#) y opta por restaurarlo, el elemento en cuestión desaparece de **Archivos en cuarentena** y pasa a figurar como archivo excluido del análisis (**Cuarentena / Archivos excluidos del análisis**).

De igual manera que usted ha decidido excluir elementos de la cuarentena, puede también devolverlos a dicha situación. Para ello, marque la casilla del elemento que desea devolver y haga clic en **Deshacer exclusión**. A continuación acepte el mensaje de confirmación.




El elemento seleccionado desaparecerá del listado de exclusiones, y volverá a aparecer en el listado de archivos en cuarentena cuando sea detectado de nuevo.


Informes


Tipos de informes

Ejecutivo


Información que incluye:

 Resumen del estado de las protecciones instaladas y las detecciones realizadas en las últimas 24 horas, últimos 7 días, o último mes.


 Listas *top 10* de equipos con malware detectado y ataques bloqueados, respectivamente.

 Listas *top 10* de equipos con dispositivos bloqueados.


 Información sobre el estado de las licencias contratadas.

 Detalle del número de equipos que se encuentran en proceso de instalación de la protección en el momento de generar el informe (se incluyen los equipos con error en la instalación).

Si usted dispone de licencias de Panda Cloud Office Protection Advanced, en el informe se mostrará la cifra de spam detectado así como las listas *top 10* de:

 Categorías más accedidas

 Equipos que más acceden

 Equipos que han accedido a categorías prohibidas y a los cuales se les han bloqueado el acceso a URLs.


Equipos con sistema operativo Linux


En el caso del informe ejecutivo, para los equipos con sistema operativo Linux se indica si tienen los ficheros de firmas actualizados y si la protección está actualizada o no.



De estado

Información que incluye:

 Proporciona una visión general del estado de las protecciones y sus actualizaciones en el momento de solicitar el informe.

 Detalle del número de equipos que se encuentran en proceso de instalación de la protección en el momento de generar el informe (se incluyen los equipos con error en la instalación).


Equipos con sistema operativo Linux


En el informe de estado se indica si los equipos con sistema operativo Linux tienen los ficheros de firmas actualizados y si la protección está actualizada o no.

Además se muestra el estado de las protecciones. Dado que en los equipos con Linux no hay protecciones permanentes sino que se dispone de la protección a través de análisis bajo demanda y programados, el estado de la protección deberá ser correcto y se mostrará el icono verde siempre y cuando se haya instalado correctamente la protección.

De detección

Información que incluye:

 Ofrece la evolución de las detecciones realizadas en las últimas 24 horas, últimos 7 días, o último mes.

 Detalla el equipo, grupo, tipo de detección, número de veces (ocurrencia) de la detección, acción realizada y la fecha en que se produjo la detección.

Equipos con sistema operativo Linux

En el informe de detección en los equipos con sistema operativo Linux se muestran las detecciones realizadas por los análisis bajo demanda o programados.



Generar informes

Con Panda Cloud Office Protection puede obtener informes sobre el estado de la seguridad en su red informática y las detecciones realizadas en un determinado periodo de tiempo.

Además, puede usted también seleccionar el contenido que aparecerá en el informe, si quiere que la información sea detallada, y si desea acompañarla de gráficas. Todo ello de manera rápida y sencilla.

En la ventana principal de la consola web, haga clic en **Informes**. Se abrirá la ventana **Informes**, que se estructura en dos secciones: en una de ellas podrá seleccionar cuál será el contenido y el alcance del informe, y en la otra programar el envío del informe por correo.

Contenido del informe

En primer lugar, seleccione el [tipo de informe](#) que desea generar.

Seleccione el intervalo que desea que refleje el informe (últimas 24 horas, últimos 7 días, o último mes).

Según el tipo de informe de que se trate, podrá seleccionar que se muestren diferentes informaciones.

Alcance del informe

En el árbol situado bajo **Alcance del informe**, seleccione el grupo o grupos que se incluirán en el informe.



Marque la casilla **Todos** si necesita seleccionar todos los grupos existentes.

Si no necesita programar el envío del informe haga clic en **Generar informe**. El informe se generará al momento y aparecerá en la lista de informes de la parte izquierda de la pantalla.

Programar envío por correo

Si lo necesita, puede programar el envío por correo del informe a los usuarios que usted decida y utilizando determinados formatos.

La frecuencia con la que podrá programar los informes es:

Mensual

Semanal

Diario

Primer día del mes

Podrá programar hasta 27 tareas de envío de informes. Una vez alcanzado dicho valor necesitará eliminar alguna de ellas para crear más.



Para poder programar tareas de envío de informes es necesario contar con el permiso necesario. Por favor, consulte la sección [Tipos de permisos](#).

Si, por el contrario, no necesita programar el envío de sus informes, el número de informes que podrá guardar es ilimitado. Podrá acceder de nuevo a un informe haciendo clic en el nombre del mismo en la lista que aparecerá en la parte izquierda de la ventana **Informes**.

Para programar la tarea de envío por correo, siga los siguientes pasos:




Puede optar entre programar envíos diarios, semanales, mensuales o establecer como fecha de envío el primer día de cada mes.

A continuación seleccione el formato en que desea enviar el informe y cumplimente los campos referidos a destinatario, copia y asunto.

Para finalizar con la generación del informe y la configuración de su envío programado, haga clic en **Guardar**. El informe aparecerá en la lista de informes de la parte izquierda de la pantalla, y se enviará en la fecha establecida.

Visualizar informes

Una vez generado el informe, utilizando los controles de navegación usted podrá desplazarse por sus páginas, realizar búsquedas en él y exportarlo en un formato diferente.

Para exportar el informe, haga clic en el icono  seleccione en la lista desplegable el formato que desea.



*Para poder exportar los informes en Internet Explorer hay que tener desmarcada la casilla **No guardar las páginas cifradas en el disco** en el apartado **Seguridad** de la pestaña **Opciones avanzadas** (**Herramientas** > **Opciones de Internet**).*

Haga click en  para actualizar la vista del informe.

Si desea imprimir el informe previamente ha de exportarlo. Una vez exportado, puede imprimirlo desde el archivo descargado.



La primera vez que desee imprimir un informe (solo disponible en Internet Explorer) se solicitará la instalación de un control ActiveX de SQLServer.



Desinstalación

Tipos de desinstalación

La desinstalación de las protecciones puede realizarse de diferentes maneras.

Desinstalación local

Si usted desea realizar la desinstalación de manera local, tendrá que hacerlo de manera presencial desde cada uno de los equipos, desde la opción correspondiente del panel de control del sistema operativo.

Desinstalación centralizada

La desinstalación de la protección de forma centralizada en varios equipos a la vez se realiza mediante la [herramienta de distribución](#). Esta herramienta se descarga y ejecuta en el equipo desde el que lanzará el proceso de desinstalación que afectará a los equipos seleccionados.

Desinstalación remota

Existe también el método de desinstalación remota, que se utiliza para desinstalar la protección desde una consola web situada en una ubicación diferente a aquella en la que se encuentran los equipos afectados. Para ello se configuran tareas de desinstalación y se especifica cuáles serán los equipos afectados.



En caso de ser necesario, tanto en el método de desinstalación local como en el centralizado se le requerirá que introduzca la contraseña que usted estableció en su día para el perfil de configuración de la protección correspondiente. La desinstalación protegida con contraseña no es aplicable a equipos con sistema operativo Linux.

Seleccione el método de desinstalación sobre el que desea más información:

 [Desinstalación local](#)

 [Desinstalación centralizada](#)

 [Desinstalación remota](#)



Desinstalación local

La desinstalación de las protecciones se realiza desde cada equipo en el que fueron instaladas.

 En Windows XP

Panel de Control > Agregar o quitar programas

 En Windows Vista o Windows 7

Panel de Control > Programas y características > Desinstalar

Desinstalación centralizada

En la ventana principal de la consola web, haga clic en **Instalación y configuración** y, a continuación, en la opción **Desinstalación** del menú situado a la izquierda de la ventana. Seleccione **Desinstalación centralizada**. Accederá a la pantalla **Desinstalación centralizada**.



***IMPORTANTE:** antes de descargar e instalar la herramienta de distribución, consulte los [requisitos que debe reunir el equipo](#) desde el que se realizará el despliegue.*

Descarga e instalación de la herramienta de distribución

En la ventana principal de la consola web, haga clic en **Instalación y configuración** y, a continuación, en la opción **Desinstalación** del menú situado a la izquierda de la ventana. Seleccione **Desinstalación centralizada (herramienta de distribución)**.

En el cuadro de diálogo de descarga de archivo seleccione **Guardar**, y cuando la descarga haya finalizado ejecute el archivo desde el directorio en el que lo haya guardado. El asistente le guiará a lo largo del proceso de instalación.



Panda Cloud Office Protection

Una vez instalada la herramienta de distribución es necesario abrirla para poder desinstalar la protección de los equipos. Se mostrará la ventana principal desde la que usted podrá desinstalar las protecciones:



Desinstalación por dominios

Abra la herramienta de distribución.

En la ventana principal, haga clic en **Desinstalar**.

Localice en el árbol los equipos a los que desea desinstalar la protección, y marque la casilla correspondiente.

Si fuera necesario, se le solicitará que introduzca [la contraseña que usted estableció para el perfil de configuración](#) correspondiente.

Indique el nombre de usuario y contraseña con privilegios de administrador si en su



momento lo estableció para los equipos seleccionados.

Si desea que durante el proceso de desinstalación se eliminen los elementos en cuarentena, y que al finalizar dicho proceso los equipos se reinicien, marque la casilla correspondiente.

Desinstalación por IP o nombre de equipos

Abra la herramienta de distribución.

En la ventana principal de la herramienta de distribución, haga clic en **Desinstalar**.

Indique los equipos a los que desea desinstalar la protección. Puede introducir los nombres de los equipos, sus direcciones IP o rangos de IP, separando estos datos con comas.

Si fuera necesario, se le solicitará que introduzca [la contraseña que usted estableció para el perfil de configuración](#) correspondiente.

Indique el nombre de usuario y contraseña con privilegios de administrador si en su momento lo estableció para los equipos seleccionados.

Si desea que durante el proceso de desinstalación se eliminen los elementos en [cuarentena](#), y que al finalizar dicho proceso los equipos se reinicien, marque la casilla correspondiente.

Desinstalación remota

Creación de tareas de desinstalación remota



Con la desinstalación remota es posible desinstalar la protección desde la consola web de forma sencilla y eficaz, y sin necesidad de desplazarse hasta el lugar donde se encuentran los equipos. Este tipo de desinstalación supone, por tanto, un abaratamiento en costes y desplazamientos.



Esta opción no está disponible para equipos con sistema operativo Linux

El proceso se inicia con la creación de tareas de desinstalación, y continúa con la configuración de estas tareas. Para ello el administrador seleccionará el grupo y los equipos del grupo a los que afectará la desinstalación, y, finalmente, podrá comprobar cuáles han sido los resultados del proceso de desinstalación y acceder a detalles sobre cada uno de ellos.

Pasos para crear una tarea de desinstalación remota

En la ventana principal de la consola web, haga clic en **Instalación y configuración** y, a continuación, en la opción **Desinstalación** del menú situado a la izquierda de la ventana.

Seleccione Desinstalación remota. Accederá a la pantalla Desinstalación remota.



Para establecer tareas de desinstalación el usuario debe poseer permiso de control total o administrador. Para más información, consulte el apartado Tipos de permisos.

Para establecer una tarea de desinstalación, haga clic en **Nueva desinstalación**.

A continuación, en la pantalla **Edición de desinstalación** podrá nombrar la tarea y seleccionar en el desplegable **Grupo** el grupo en el que están los equipos cuya protección quiere desinstalar. Los grupos mostrados serán aquellos sobre los que usted tenga permisos.



Si selecciona la opción Reiniciar los equipos al finalizar la desinstalación recuerde que es importante guardar toda la información que se esté utilizando en dichos equipos.

Si el grupo seleccionado tiene aplicado un perfil de configuración para el que en el momento de su creación se adjudicó una contraseña de desinstalación, introdúzcala en la caja de texto **Contraseña**.

Seleccione los equipos en el listado de equipos que se muestran en la pestaña **Equipos disponibles**, y haga clic en Agregar. Al seleccionarlos, pasarán a la pestaña **Equipos seleccionados**.


Para [ver el desarrollo de la desinstalación remota y sus resultados](#), acuda de nuevo a la pantalla **Desinstalación remota**.


Visualización y resultado de la desinstalación remota







Visualización de las desinstalaciones

Las tareas de desinstalación aparecerán listadas en la pantalla **Desinstalación remota**, desde donde podrá también eliminarlas si así lo desea, utilizando para ello el botón **Eliminar**.

En esta pantalla la información se organiza en las siguientes columnas:

 **Nombre:** muestra el nombre que se ha dado a la tarea de desinstalación cuando se ha creado.


 **Estado:** indica mediante iconos el estado en que se encuentra la tarea de desinstalación.


 En espera	 Finalizada
 Iniciando	 Cancelada
 En curso...	 Finalizada con error



Panda Cloud Office Protection

 - **Protecciones desinstaladas:** detalla el número de protecciones desinstaladas.

 **Fecha creación:** fecha en que se creó la tarea de desinstalación.

 **Creado por:** usuario que creó la tarea de desinstalación.


Según el permiso del que usted disponga podrá crear, visualizar o eliminar tareas de desinstalación de protecciones. Para más información, consulte el apartado [Tipos de permisos](#).

Si desea ver los detalles de alguna de las desinstalaciones, haga clic sobre el nombre de la desinstalación y accederá a la pantalla [Resultado de la desinstalación](#).

Resultado de la desinstalación remota


Al hacer clic el nombre de una desinstalación de las que aparecen en la pantalla **Desinstalación remota** accederá a la pantalla **Resultado de la desinstalación**.

Además del nombre y las fechas de comienzo y final de la desinstalación, esta pantalla también proporcionará información sobre los equipos afectados por la desinstalación y el estado en el que ésta se encuentra.

 *En el caso de que la tarea esté en estado **En espera**, la fecha de inicio mostrará un guión (-). Lo mismo sucederá con la fecha de fin si la tarea no ha finalizado.*


Si desea consultar la configuración de la tarea de desinstalación, utilice el vínculo **Ver configuración**.

Compatibilidad entre tareas de búsqueda de equipos desprotegidos y desinstalación remota

 Si un equipo está involucrado en una tarea de desinstalación (*En espera, Iniciando, o En curso*), **no es posible** crear otra tarea de desinstalación sobre él ni



seleccionarlo como equipo desde el que lanzar [búsquedas de equipos desprotegidos](#).

 Si un equipo está ejecutando una tarea de descubrimiento de equipos desprotegidos, **no es posible** crear una tarea de desinstalación sobre él.

Solución de Problemas – Preguntas Frecuentes

Solución de problemas

Para cualquier duda o consulta, puede acceder a la página de soporte técnico, donde encontrará un listado con los códigos de error más comunes de Panda Cloud Office Protection, e información actualizada sobre todos ellos. Haga clic [aquí](#) o introduzca la siguiente URL en su navegador de Internet:

<http://www.pandasecurity.com/spain/enterprise/support/card?id=50032&idIdioma=1&idSolucion=147&idProducto=124>

Preguntas frecuentes

¿Cómo se accede a la consola web de Panda Cloud Office Protection?

La gestión de Panda Cloud Office Protection se realiza en modo online, utilizando la consola web. Para acceder a ella, siga los siguientes pasos:

Acceda a la siguiente URL: <https://managedprotection.pandasecurity.com>

Introduzca los datos de Login Email y Contraseña.

Acepte los términos y condiciones del Acuerdo de Licencia (sólo se le solicitará la primera vez que acceda a la aplicación).

Una vez haya iniciado sesión en la consola web, se mostrará la pestaña **Estado**.

Mediante la opción **Salir** usted puede cerrar la sesión. También puede seleccionar el idioma en el que desea visualizar la consola web, utilizando el desplegable situado junto al idioma activo.



¿Qué es un perfil?

La configuración de Panda Cloud Office Protection está basada en la creación de perfiles y grupos de máquinas a los que se asignarán determinadas políticas.

Una política es un conjunto de configuraciones que son aplicables a uno o más grupos de máquinas. Todas las máquinas que pertenezcan a un mismo grupo tendrán asignada la misma política.

Pasos para configurar un perfil

Acceda a la consola web.

Dentro de la pestaña **Configuración**, seleccione la opción **Perfiles** de la parte izquierda de la consola web.

Se visualizará cada uno de los perfiles creados, además del perfil por defecto (Default). Una vez se selecciona un perfil, en el panel de la izquierda se mostrarán las secciones correspondientes a cada perfil: General, Antivirus, Firewall, Control de dispositivos.

¿Cuáles son los requisitos de instalación de Panda Cloud Office Protection?

Para instalar Panda Cloud Office Protection es necesario que los equipos implicados en el proceso de instalación reúnan una serie de requisitos.

Esto afecta tanto a los equipos a los que se va a instalar la protección como al equipo desde el que se realizará el despliegue de dicha protección.

También se deben cumplir unas condiciones para poder acceder a la consola web. Puede conocer con detalle cuáles son todos estos requisitos en el apartado [Requisitos del](#)



[sistema](#).

¿Qué comprobaciones se deben realizar antes de instalar Panda Cloud Office Protection?

Antes de instalar Panda Cloud Office Protection es muy recomendable realizar una serie de comprobaciones mínimas, que están relacionadas con la existencia de otras protecciones instaladas en los equipos, la compatibilidad Panda Cloud Office Protection-AdminSecure, o la recomendación de mantener cerradas otras aplicaciones mientras se instala Panda Cloud Office Protection.

Todos estos consejos están debidamente detallados en el apartado [Recomendaciones previas a la instalación de la protección](#).

¿Cuáles son los componentes de Panda Cloud Office Protection?

Panda Cloud Office Protection está compuesto por cuatro componentes principales:

- La consola web.
- La unidad antivirus
- La unidad firewall.
- El control de dispositivos.
- La protección para servidores Exchange.
- El control de acceso a páginas Web.

La consola web

La consola web permite la gestión de la protección del parque informático.



La unidad antivirus

La instalación de la unidad antivirus se realiza desde la consola Web y se compone de las siguientes protecciones:

- Archivos: protección permanente que monitoriza los accesos a disco.
- Correo (sólo estaciones): protección para correo electrónico
- Web: protección para navegación Web.

La unidad firewall

La unidad firewall monitoriza todas las conexiones de red, bloqueando o permitiendo el acceso en función de las reglas configuradas. Incorpora detección y bloqueo de intrusiones IDS y ataques de virus de red, que son los que los trojanos aprovechan para propagarse. Esta protección permite al administrador configurar el modo de funcionamiento de la misma.

Administración centralizada (desde la consola web): el administrador define la configuración que se va a aplicar en las máquinas administradas. Esta configuración se realiza desde la consola web.

Administración desde cliente (desde el icono de Panda Endpoint Protection): el usuario final de la protección es la persona encargada de realizar la configuración del firewall. Para facilitar esta tarea de configuración al usuario, se incluyen una serie de reglas predefinidas por Panda que establecen los permisos para las aplicaciones más comunes.

Se podrán crear nuevas reglas o modificar las existentes desde las opciones de configuración del firewall.



El control de dispositivos

Dispositivos de uso común como las llaves USB, los lectores de CD/DVD, dispositivos de imágenes, Bluetooth y módems pueden constituir también una vía de infección para los equipos cuya seguridad usted desea preservar.

La opción de configuración del control de dispositivos le permite determinar cuál será el comportamiento de este tipo de protección para el perfil que está creando. Para ello, seleccionará el dispositivo o dispositivos que desea autorizar y le asignará un nivel de utilización.

Protección para servidores Exchange

Los correos electrónicos, ya sean los que circulan por la red interna de la empresa como los procedentes del exterior pueden contener malware y son una fuente de spam.

Gracias a la protección para servidores Exchange se puede prevenir esta situación, evitando infecciones y la sobrecarga debida al exceso de tráfico de spam.

Control de Acceso a páginas web

Con esta protección es posible restringir el acceso a determinadas categorías web y configurar URLs a las que autorizar o denegar el acceso. Esto contribuirá a la optimización del ancho de banda de su red y a la productividad de su negocio.

¿Qué es el agente de administración de Panda Cloud Office Protection?

El agente de administración es un elemento que será distribuido a cada uno de los equipos que usen los servicios de Panda Cloud Office Protection. Una vez instalado, desencadena la instalación de la protección en los equipos.

Consta principalmente de tres funciones:



- Comunicar los procesos locales de las máquinas con los servidores de Panda Cloud Office Protection.
- Comunicar los procesos locales de las máquinas con otros agentes.
- Comunicar a otros agentes con los servidores de Panda Cloud Office Protection (funcionalidad proxy).

Toda la información referente al agente y sus principales funciones está disponible en el apartado [Proceso de despliegue de la protección](#).

¿En qué consisten las funcionalidades P2P y Proxy implementadas en Panda Cloud Office Protection?

Sistema P2P

Los procesos locales de instalación y actualización (procesos walupg y walupd*) de Panda Cloud Office Protection cuentan con cierta lógica que les permite ser capaces de detectar si los ficheros de instalación o actualización necesarios se encuentran disponibles en otro agente de la red.

De este modo, en el momento de instalar o actualizar, se obtendrán estos ficheros del equipo de la red en lugar de descargarlos desde Internet. Esta lógica se denomina sistema P2P, y su objetivo fundamental es reducir el consumo de ancho de banda de la conexión a Internet.

Los procesos locales de instalación y de actualización son, respectivamente:

walupg: proceso local de instalación y actualización de protecciones.



Panda Cloud Office Protection

walupd: proceso encargado de la actualización de archivos de identificadores.

Funcionamiento

Cuando una máquina se ha descargado un fichero de Internet podrá servirlo a otras máquinas, evitando que éstas tengan que conectarse a Internet de forma directa.

Una vez que la máquina termina de actualizar el archivo de identificadores de virus o la protección, envía información por broadcast al resto de máquinas, informando de los ficheros que tiene disponibles.

Cuando una máquina necesite un fichero, primero intentará obtenerlo por P2P. Si no es posible, entonces intentará obtenerlo de Internet.



Para que una máquina pueda servir ficheros a otras utilizando el sistema de P2P, deberá tener al menos 128 MB disponibles de RAM.

Proxy

El agente de Panda Cloud Office Protection está dotado de la funcionalidad Proxy. Esta funcionalidad permite el funcionamiento de Panda Cloud Office Protection en equipos sin acceso a Internet, realizándose los accesos a través de otro agente instalado en una máquina que sí dispone de conexión a Internet.



Para poder actuar como proxy para otros agentes, una máquina debe cumplir los siguientes requisitos: disponer de conexión directa a Internet, y disponer al menos de 128 MB de RAM. Además, el equipo no puede estar en lista negra y debe haber concluido completamente la secuencia de instalación.

Este sistema sólo se intentará utilizar una vez que se haya determinado que no es posible el acceso directo a Internet.



Funcionamiento

El agente detecta que no puede acceder a Internet, y lanza una petición broadcast para localizar las máquinas que pueden servirle como proxy.

Se almacenará el listado de máquinas obtenidas (hasta un máximo de 10 máquinas) en el fichero Proxy.dat.

La siguiente vez que el agente necesite acceder a Internet y no pueda hacerlo de forma directa, tomará la primera máquina del listado disponible en el archivo Proxy.dat, y la utilizará para salir a Internet.

Cada petición a la lista Proxy.dat se realizará a una maquina distinta, de manera rotativa, para no utilizar siempre la misma máquina.

Además, los proxys tienen un indicador de disponibilidad. En el momento en que no se pueda contactar con un agente de la lista de proxys, la disponibilidad del mismo disminuye. Inicialmente el valor de disponibilidad es de 3, y al llegar a cero, esa máquina se eliminará de la lista de Proxy.dat.

Proxy estático

Si deseamos que todos los accesos a Internet se hagan a través de un equipo concreto decidido por el administrador, en lugar de por equipos determinados de forma dinámica, el agente de comunicaciones admite la posibilidad de especificar que máquina deseamos que actúe como Proxy.

La máquina que actúe como 'Proxy estático' debe cumplir los siguientes requisitos:



Debe tener un agente instalado versión 6.0 o superior.

Debe tener acceso directo a Internet

Disponer de al menos 128 MB de memoria.

Debe haber comunicado con el servidor en las últimas 72 horas

Además, el equipo no puede estar en lista negra y debe haber concluido completamente la secuencia de instalación de la protección.

Si en algún momento el equipo que se estableció para que actuara como proxy estático dejara de cumplir alguno de los requisitos necesarios para ejercer como tal, se desactivará en la consola la configuración del proxy estático, desapareciendo el nombre del equipo que estaba configurado y se mostrará un mensaje indicándole cuál de dichos requisitos se incumple.

Usted podrá seleccionar otro equipo para que realice las funciones de proxy estático.

Si un equipo deja de ser proxy estático por haber sido incluido en la lista negra, una vez que deje de pertenecer a dicha lista, si se desea que actúe de proxy estático será necesario configurarlo de nuevo para que transiten por él todas las comunicaciones con el servidor.

La configuración del proxy estático se realiza en el apartado **Proxy/Repositorio** de las **Opciones avanzadas** de la pestaña **Principal** de la configuración general del perfil.

¿Cómo se instala Panda Cloud Office Protection mediante el instalador?

La instalación de Panda Cloud Office Protection se inicia con la instalación del agente de administración (.msi), quien descarga la protección para, a continuación, desencadenar su instalación en los equipos.



Panda Cloud Office Protection

Panda Cloud Office Protection le ofrece dos maneras de distribuir la protección a sus equipos utilizando el programa de instalación:

Descarga del archivo de instalación en el equipo del administrador para después realizar la instalación en el resto de equipos de la red.

Envío del enlace del archivo de instalación a cada equipo por correo electrónico para que cada usuario lo descargue y ejecute de forma manual.

Descarga del instalador

➡ *Antes de descargar el instalador, consulte los [requisitos](#) que los equipos deben cumplir.*

Seleccione el sistema operativo para el que va a descargar el instalador.

➡ *Tanto en Linux como en Windows el instalador es el mismo para plataformas de 32 y de 64 bits.*

A continuación especifique el grupo en el que se integrarán los equipos a los que instalará la protección.

Haga clic en **Descargar**

En el área de Instalación y configuración, haga clic en Utilizar programa de instalación y a continuación en Descargar programa de instalación.

En el cuadro de diálogo de descarga de archivo seleccione **Guardar**, y una vez la descarga haya finalizado ejecute el archivo desde el directorio en el que lo haya guardado. El asistente le guiará a lo largo del proceso de instalación.

Distribuya la protección al resto de equipos de la red. Para ello puede utilizar sus propias herramientas o bien instalarlo manualmente.



Generar URL de instalación

Utilice esta opción si lo que desea es lanzar la instalación desde cada equipo. Simplemente copie la URL de instalación para el sistema operativo que necesite, y después acceda a ella desde cada uno de los equipos a los que tenga acceso y a los que desee instalar la protección.

Envío del enlace por correo

Haga clic en **Enviar por correo**. Automáticamente los usuarios recibirán un email con el enlace de descarga (recibirán el link de instalación para sistemas operativos Linux y para sistemas operativos Windows). Al hacer clic en cualquiera de los enlaces, se iniciará la descarga del instalador.

¿Cómo se instala Panda Cloud Office Protection mediante la herramienta de distribución?

La herramienta de distribución de Panda Cloud Office Protection le permite instalar la protección de una forma centralizada, evitando así la intervención manual de los usuarios a lo largo del proceso.

Descarga de la herramienta de distribución

Acceda a la consola web.

Seleccione la pestaña **Configuración**.

haga clic en **Instalación** en el menú de la parte izquierda.

En **Tipo de instalación**, seleccione el **Grupo** a instalar del menú desplegable. Esta selección determinará el grupo al que se van a incorporar las máquinas que se van a instalar, y por lo tanto, la política o perfil que se le va a aplicar.

Haga clic en el enlace **Descargar herramienta de distribución**

Seleccione **Guardar** en la ventana de descarga del archivo Wadistributiontool.msi.

Una vez la descarga haya finalizado, ejecute el archivo Wadistributiontool.msi desde el directorio en el que lo haya guardado. El asistente le guiará a lo largo del proceso de



instalación.

Instalación de la protección

Acceda a **Inicio, Programas, Panda Distribution tool** o bien desde el acceso directo del Escritorio.

Una vez en la consola de la herramienta, seleccione **Instalar protecciones**. Se abrirá la pantalla llamada **Instalación de protecciones**, que permitirá distribuir la protección de dos modos:

Distribución por Dominios

Introduzca el grupo en el que se desea que se incluyan los equipos que se van a instalar. Esta selección marcará la política de configuración que se va a aplicar a estos equipos.

Dentro del árbol de red, seleccione los dominios o equipos sobre los que se quiere instalar.

Utilice un usuario y contraseña con permisos de administrador para realizar la instalación. El nombre de usuario deberá introducirse con formato dominio\usuario.

Una vez introducidos los datos, pulse la opción **Instalar**, para generar las tareas de instalación.

Distribución por direcciones IP o nombre de equipo

Introduzca el grupo en el que se desea que se incluyan los equipos que se van a instalar. Esta selección marcará la política de configuración que se va a aplicar a estos equipos.



Panda Cloud Office Protection

En este paso, añada los nombres de los equipos a instalar, o las direcciones IP de los mismos, separadas por comas. También es posible seleccionar rangos de IPs (usar el símbolo "-" para los rangos (ej: 172.18.15.10 – 172.18.15.50)).

Utilice un usuario y contraseña con permisos de administrador para realizar la instalación. El nombre de usuario se deberá introducir con formato dominio\usuario

Pulse **Instalar**, para generar las tareas de instalación.

Verifique desde la consola que la tarea de instalación se ha completado con éxito. A partir de entonces, comenzará la instalación de la protección, de forma completamente transparente.

Reinicie el equipo si así lo solicita.

Toda la información sobre la instalación de Panda Cloud Office Protection está disponible en el apartado [Instalación de la protección](#).

¿Es posible instalar Panda Cloud Office Protection en una red protegida con Panda AdminSecure?

Antes de instalar Panda Cloud Office Protection en equipos que tienen instalada la protección distribuida desde AdminSecure, es necesario desactivar la opción Instalaciones Automáticas de AdminSecure, porque en caso contrario, cuando el agente de AdminSecure detecta que Panda Cloud Office Protection ha sido instalado, procede a desinstalarlo e instalar de nuevo la protección de AdminSecure.

En función de la versión de AdminSecure de que se trate, los comportamientos son dos:

Si la versión de AdminSecure es posterior a AdminSecure 4.02 SP2, la desinstalación de Panda Cloud Office Protection se realizará de manera automática mediante el desinstalador que incorpora AdminSecure.



Panda Cloud Office Protection

Si la versión de AdminSecure es anterior a AdminSecure 4.02 SP2, no existe la posibilidad de desinstalación automática, con lo que la protección de AdminSecure se instalará independientemente de que Panda Cloud Office Protection también lo esté, produciéndose efectos no deseados.

Al desactivar la opción Instalaciones Automáticas en AdminSecure, se puede optar por desactivarla para todos los equipos o hacerlo únicamente para aquéllos equipos en los que se va a instalar Panda Cloud Office Protection.

Es decir, lo que en realidad se está configurando es cuáles serán los equipos en los que no se instalará automáticamente la protección de AdminSecure, o, lo que es lo mismo, qué equipos serán la excepción a la regla de instalación automática definida por AdminSecure.

[Para desactivar la opción Instalaciones Automáticas en AdminSecure:](#)

En la consola de AdminSecure, seleccione **Configurar > Instalaciones automáticas**.

Haga clic en **Configurar excepciones**, y utilice el botón **Añadir** para seleccionar los equipos que quedarán excluidos del proceso de instalación.

[¿Cómo se puede incluir un equipo en situación de lista negra?](#)

La inclusión de un equipo en situación de lista negra puede hacerse de manera manual o automática.

[Inclusión manual](#)

Utilice las opciones de que dispone en la ventana **Preferencias**.



Inclusión automática

Un equipo es incluido automáticamente en la lista negra cuando se intenta instalar en él protección cuya licencia ha caducado, o para la que se ha superado el número máximo de instalaciones permitidas.

Las consecuencias de esto son que el equipo no será actualizado ni la información proveniente de él será tomada en cuenta en los informes y estadísticas que Panda Cloud Office Protection obtenga.

¿Cómo se puede restaurar un equipo que está en situación de lista negra?

Para restaurar este equipo y extraerlo de la situación de lista negra, es necesario poseer licencias disponibles.

Si el equipo que se desea restaurar ha sido incluido en la lista negra de manera manual, bastará con seleccionarlo y aplicarle la opción **Restaurar** en la ventana **Preferencias**.

¿Por qué no se recibe información de un equipo que se encontraba en lista negra y ha sido restaurado?

Si se restaura un equipo y transcurren unos días sin que éste envíe información al servidor, puede ser debido a que aún no se haya comprobado la validez del usuario.

Transcurridos un máximo de 5 días, el equipo comenzará a enviar de nuevo información.



¿Por qué aparecen equipos desactualizados tras una actualización de Panda Cloud Office Protection?

En ocasiones, tras una actualización de versión de Panda Cloud Office Protection, en la pestaña **Equipos**, columna **Actualización Protección**, aparecen equipos con la protección desactualizada.

Uno de los motivos por los que se puede producir esta situación se debe a que la opción **Actualizaciones automáticas del perfil de los equipos** se encuentra desactivada.

Solución

Active las actualizaciones automáticas del perfil de los equipos de la red que muestren el error. Para ello, siga los pasos que se indican a continuación:

Acceda a la pestaña **Instalación y Configuración**.

Seleccione la opción **Perfiles** del panel de la izquierda.

Haga clic en uno de los equipos del listado que se encuentre desactualizado.

Edite el perfil de las máquinas desactualizadas y seleccione la pestaña **Actualizaciones**.

Compruebe en la sección **Actualización automática** que la opción **Activar actualizaciones automática del archivo de actualizaciones** se encuentra habilitada.

Certifique que la opción **Activar actualización automática del motor** se encuentra activada dentro de la sección **Actualización del motor de la protección**.



Haga clic en **Aceptar**.

Una vez habilitadas las actualizaciones automáticas, compruebe que, al cabo del período configurado, el motor de la protección se actualiza correctamente.

¿Cuál es el comportamiento de Panda Cloud Office Protection a la hora de acceder a la nube?

Las máquinas necesitan tener acceso a Internet para que la protección pueda acceder a la nube. Para ello, en caso de ser necesario, es recomendable que el Administrador configure el Proxy en la consola Web de Panda Cloud Office Protection.

Aún así, en el caso de que dicha configuración no se realice, la protección intentará acceder a Internet utilizando para ello la siguiente lógica:

La protección intentará salir con la **configuración establecida en la consola Web** para las actualizaciones.

En caso de no existir dicha configuración o no poder acceder a Internet con ella, la protección intentará salir con la **configuración establecida por el usuario en la alerta local**, si alguna vez se hubiera introducido dicha configuración.

En caso de no existir dicha configuración o no poder acceder a Internet con ella, se realizará un **intento de conexión directa**.

En caso de no poder acceder a Internet directamente, se **probará con la configuración establecida en Internet Explorer** (valores de Proxy y Puerto configurados en este navegador).



En caso de no poder acceder a Internet con dicha configuración y sólo en el caso en el que esté configurado un proxy en Internet Explorer, se mostrará un cuadro de diálogo en el que podrá introducir los datos del Proxy.

Para probar la conexión a Internet, la protección realizará una consulta http a la siguiente URL:

<http://proinfo.pandasoftware.com/connectiontest.html>

Para realizar las consultas a la nube, la protección accederá a la siguiente URL:

<http://cache2.pandasecurity.com>

Según el tipo de análisis que se desea realizar ¿cómo es el acceso de Panda Cloud Office Protection a la nube?

Si desea desactivar los análisis contra la nube, puede hacerlo desde la consola de administración, en el menú **Instalación y configuración > Perfiles >** seleccionar el perfil a editar > Sección **General > Pestaña Principal > Opciones avanzadas >** marcar la opción **Desactivar los análisis con la Inteligencia Colectiva**.

No obstante, es recomendable no desactivarlo si desea disfrutar de toda la protección que la Inteligencia Colectiva proporciona.

Panda Cloud Office Protection ofrece acceso a la nube en los siguientes tipos de análisis:

Análisis de usuario

Cualquier tipo de análisis lanzado desde el icono del oso en la área de notificaciones o desde el menú contextual (análisis lanzado mediante la opción Analizar que aparece al



seleccionar un elemento con el botón derecho del ratón)

Análisis programados

Cualquier tipo de análisis lanzado desde la consola Web de Panda Cloud Office Protection

Análisis background

Análisis programados por Panda que tienen como objetivo analizar las zonas del PC donde habitualmente se ubica el malware.

Análisis de Memoria

Este análisis se realiza tras la actualización de los ficheros de firmas.

Se analizará todo lo existente en memoria en cada momento, usando el conocimiento de las cachés para no lanzar consultas contra nube para elementos ya consultados anteriormente.

Se ha implementado un mecanismo de control de análisis de forma que no se solape la ejecución de un análisis con el siguiente:

No se lanzará un nuevo análisis de memoria si ya existe uno en ejecución.

¿Cada cuánto tiempo comunican los equipos a los servidores de Panda Cloud Office Protection el estado de la protección instalada?

El mensaje de estado está programado para enviarse cada X horas (el número x de horas lo puede especificar en la ventana **Edición de perfil – Opciones**



avanzadas), pero solo se enviará siempre y cuando se haya producido alguna variación en el estado de la protección con respecto a la situación anterior. Si no ha habido cambio alguno el mensaje se envía una vez al día.

Si lo desea, usted puede modificar el número de horas que la aplicación muestra por defecto, pero siempre en un intervalo entre 12 y 24. Si, por ejemplo, especifica 14, el mensaje de estado de la protección se enviará a los servidores de Panda Cloud Office Protection cada 14 horas.

El envío del mensaje de estado es independiente de que usted haya seleccionado o no un equipo a través del cuál realizar las conexiones con el servidor.

Una vez creada una tarea de análisis inmediato desde la consola web de Panda Cloud Office Protection, ¿cuánto tarda el endpoint en reconocerla y aplicarla?

Las tareas de análisis se crean desde la ventana Edición de perfil, en la pestaña Análisis programados. Para ello:

Haga clic en el botón **Nuevo** para acceder a la ventana **Edición de perfil – Nueva tarea de análisis**.

Nombre: indique el nombre con el que quiere identificar el análisis que va a programar.

Tipo de análisis: seleccione el tipo de análisis que va a crear (en este caso, inmediato).

Una vez configurado el análisis inmediato, éste tendrá lugar en el momento en que se produzca la conexión del equipo con el servidor de Panda Cloud Office Protection (cada 4 horas, como máximo) y se constate que se ha producido alguna modificación en la configuración de la protección.



El informe de las detecciones realizadas se envía una vez finalizado el análisis inmediato.

Anexo 1: línea de comandos para operaciones básicas remotas

Las operaciones básicas que se van a poder realizar son:

1. Instalación remota.
2. Verificación remota de la correcta Instalación.
3. Desinstalación.
4. Actualización de los ficheros de firmas.
5. Actualización de políticas o configuraciones.
6. Ejecución de análisis inmediatos: completos, de correo, etc.
7. Obtención de la fecha de última actualización del fichero de firmas
8. Obtención de la información del estado del Antivirus y del firewall

Instalación

Paso previo. Descarga del paquete de Instalación

Antes de lanzar la instalación debemos obtener el paquete de Instalación de Panda Cloud Office Protection: WaAgent.msi. Este paquete de instalación podrá estar ubicado en el repositorio de las soluciones SaaS de Remote Desktop Management para el cliente concreto sobre el que estemos realizando la instalación.

Opciones en la descarga del paquete de instalación



El paquete de instalación utilizado, puede ser uno genérico o uno específico para el cliente y para el cliente y perfil de seguridad.

Según la opción seleccionada, la línea de comando utilizada deberá complementarse con parámetros específicos o no. Las Opciones de descarga son:

Descargar el paquete desde una cuenta cualquiera de cliente y para el perfil DEFAULT. Posteriormente en la instalación podremos pasar como parámetro el Identificado del cliente y el identificador del grupo con un perfil de seguridad para ese cliente.

De esta forma estaremos indicando a que cliente pertenece la protección instalada y a que perfil de seguridad y grupo.

Descargar para cada cliente, su propio paquete de instalación. En este caso, no es necesario indicar el identificador del cliente.

Descargar para cada cliente y por cada grupo con su perfil de seguridad, su propio paquete de instalación. En este caso, no es necesario indicar ni el identificador del cliente, ni el grupo al que pertenece el equipo.

Pasos para la descarga del paquete de instalación (WaAgent.msi)

Accedemos a la cuenta de cliente específica a través de la consola web de cliente de Panda Cloud Office Protection.



Panda Cloud Office Protection



Accedemos a la sección de **Instalación y Configuración**. Vamos a descargar el paquete de instalación de este cliente para el grupo Default, que pertenece al perfil de seguridad default, es decir, antimalware y firewall centralizado.



Descargamos el paquete de instalación y lo guardamos en local.



[Instalación](#)
[Perfiles](#)
[Grupos](#)
[Búsqueda](#)
[Desinstalación](#)

Instalación de las protecciones

Para instalar las protecciones en los equipos de su red, simplemente decida en qué grupo quiere que se añadan los equipos y el modo de instalación.

Grupo

Seleccione a qué grupo desea añadir los equipos cuando se instalen las protecciones.

Grupo:

Idioma: Inglés Perfil: DEFAULT [¿Qué es un grupo?](#)

Modo de instalación

Puede instalar las protecciones en sus equipos mediante la herramienta de distribución, o bien mediante el programa de instalación.

Programa de instalación

Utilice el programa de instalación para instalar manualmente o mediante sus propias herramientas las protecciones en los equipos de su red.

☒ Utilizar programa de instalación

Puede descargar el programa de instalación y ejecutarlo en cada uno de los PCs a proteger.

[Descargar programa de instalación](#)

Si lo prefiere, puede enviar por correo a los usuarios de su red el link de acceso al programa de instalación para que éstos lo ejecuten en su puesto.

Enlace directo:
<http://pcop800rascaeaconsole.cloudapp.net/Console/v8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST={95C2837E-018B-4E9C-808D-A9C1DE8EA7D4}&GROUP=DEFAULT>
Enviar por email: [Enviar por email](#)

Pasos de Instalación

Paso 1.

Descargar el paquete de instalación en los desktops a proteger.

Paso 2.

Ejecutar la sentencia de instalación en el directorio donde se ha descargado el paquete de instalación.

```
msiexec /i "WaAgent.msi" /qn <GROUP> <GUID> <ALLOWREBOOT>
```

Los parámetros opcionales son:



Panda Cloud Office Protection

<GROUP> El grupo y por tanto el perfil de seguridad del equipo dentro del parque del cliente.

El msi ya tendrá un valor asignado en la descarga, este valor se puede sobrescribir indicando el parámetro GROUP.


<GUID> Identificador del cliente al que pertenece el equipo donde se está realizando la instalación.


El msi ya tendrá un valor asignado en la descarga, este valor se puede sobrescribir indicando el parámetro GUID.


El GUID se obtiene en la sección de Instalación y configuración de la consola web de gestión, como parámetro CUST en el acceso directo al paquete de instalación


Programa de instalación

Utilice el programa de instalación para instalar manualmente o mediante sus propias herramientas las protecciones en los equipos de su red.

 [Utilizar programa de instalación](#)

 Puede descargar el programa de instalación y ejecutarlo en cada uno de los PCs a proteger.

 [Descargar programa de instalación](#)

 Si lo prefiere, puede enviar por correo a los usuarios de su red el link de acceso al programa de instalación para que éstos lo ejecuten en su puesto.

Enlace directo:
<http://pcop800rascaeaconsole.cloudapp.net/Console/v8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST={95C2837E-018B-4E9C-808D-A9C1DE8EA7D4}&GROUP=DEFAULT>

Enviar por email: [Enviar por email](#)



<ALLOWREBOOT>. Permitirá indicar si el instalador de la protección puede o no reiniciar la máquina, en caso de que se requiera, una vez haya finalizado.

ALLOWREBOOT=TRUE → Permite el reinicio.

ALLOWREBOOT=FALSE → No permite el reinicio

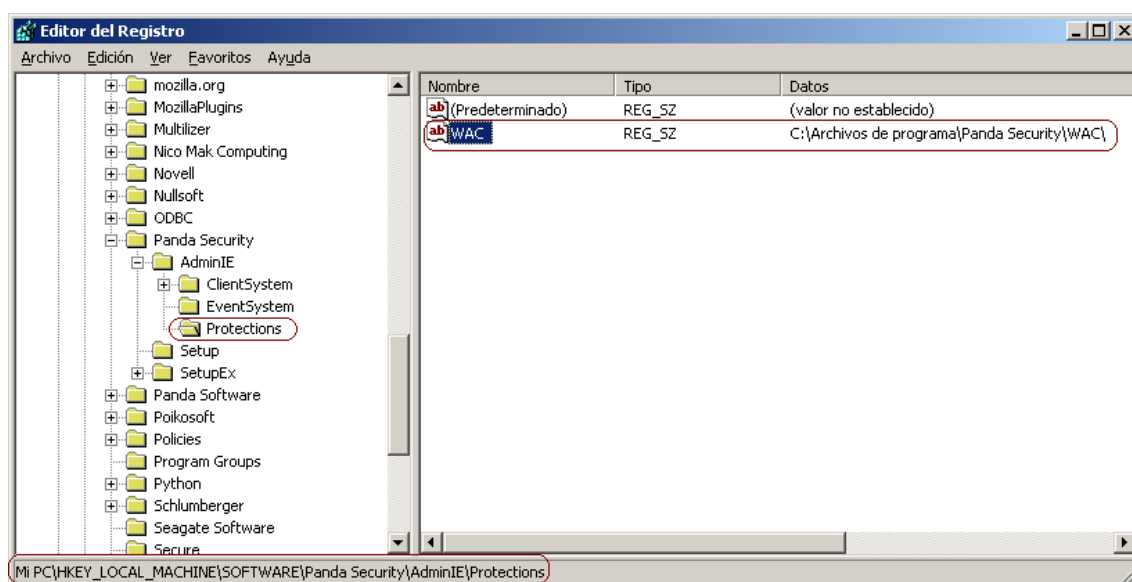
Ejemplos

```
msiexec /i " WaAgent.msi" GROUP=GROUP_ONLYAV GUID={81729831} /qn
```

Verificación de la instalación de la protección

La comprobación de que en el equipo se encuentra instalada la protección de Panda Cloud Office Protection, se realiza mediante consultar de la entrada del registro.

HKLM\Software\Panda Security\AdminIE\Protections





Panda Cloud Office Protection

Paso 1.

Comprobar la existencia de la entrada

HKLM\Software\Panda Security\AdminIE\Protections

Si existe, ir a paso 2. Si no existe, entonces la protección no está instalada

Paso 2.

Obtener el valor de WAC.

Los datos asociados a este valor, representa la ubicación de la instalación de la protección.

Si existe y no es vacío, entonces la protección está instalada.

Si no existe o es vacío, entonces la protección no está instalada.

Desinstalar Panda Cloud Office Protection

Para desinstalar Panda Cloud Office Protection de una máquina debemos desinstalar primero el agente y luego la protección.

Pasos para la desinstalación

Paso 1.

El comando de desinstalación del agente se obtiene mediante consulta al registro del valor UnPath de la clave



Panda Cloud Office Protection

HKLM\SOFTWARE\Panda Security\SetupEx\AdminIE.

Paso 2.

Ejecución de la desinstalación del agente de forma silenciosa:

<valor de UnPath de HKLM\SOFTWARE\Panda Security\ SetupEx\AdminIE > /qn
PASS=<Contraseña>

Sólo será necesario utilizar el parámetro PASS en caso de haber configurado una contraseña de desinstalación en el perfil.

Paso 3.

El comando de desinstalación de la protección se obtiene mediante consulta al registro del valor **UnPath** de la clave **HKLM\SOFTWARE\Panda Software\Setup**.

Paso 4.

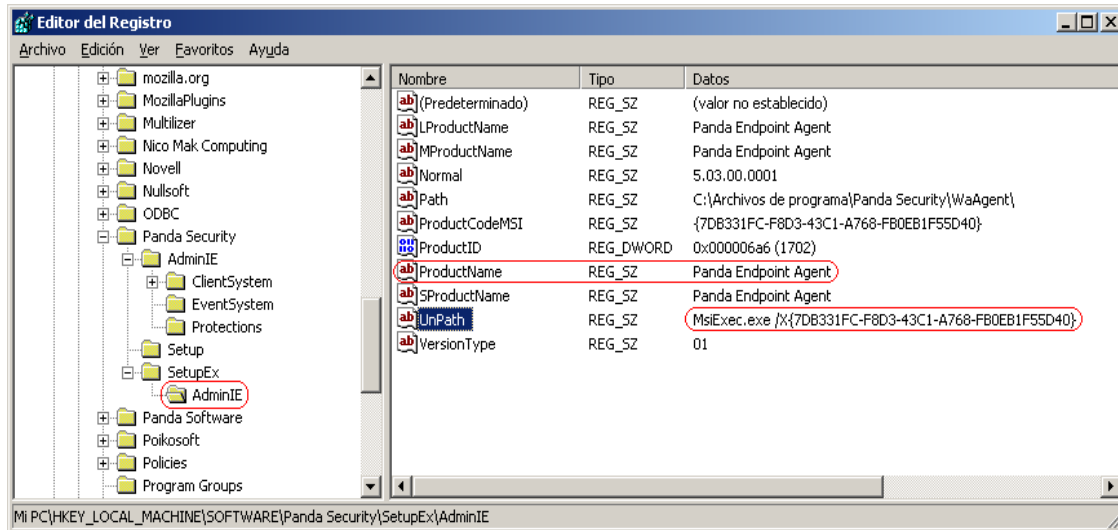
Ejecución de la desinstalación de la protección de forma silenciosa:

<valor de UnPath de HKLM\SOFTWARE\Panda Software\Setup> > /qn
PASS=<Contraseña>

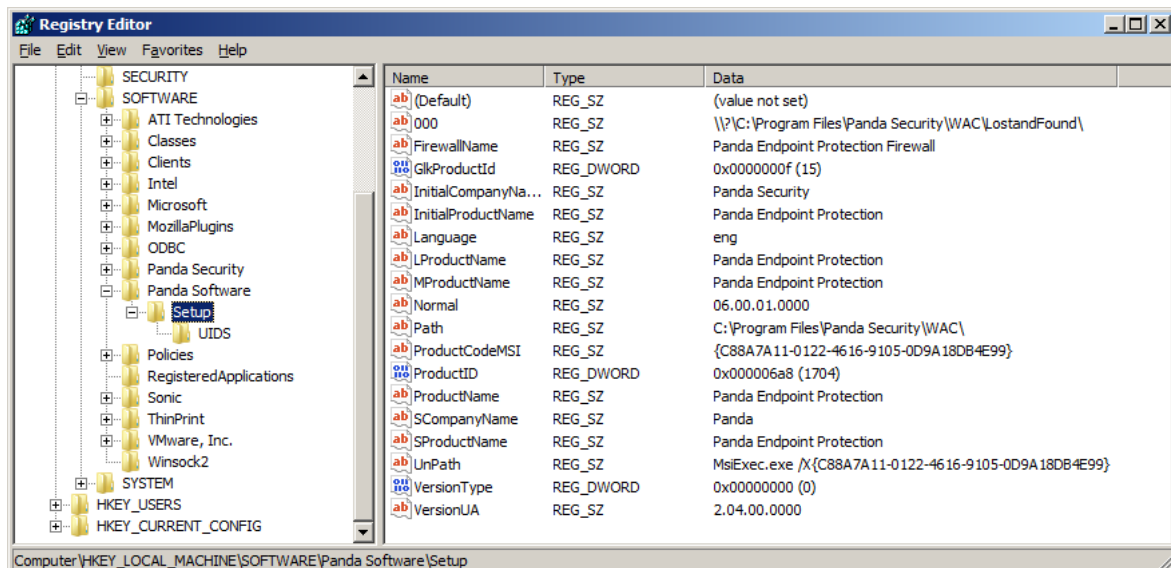
Sólo será necesario utilizar el parámetro PASS en caso de haber configurado una contraseña de desinstalación en el perfil.



Ejemplo



MsiExec.exe /X{7DB331FC-F8D3-43C1-A768-FB0EB1F55D40} /qn





[MsiExec.exe /X{C88AtAA-0122-4616-9105-0D9A18D84E99} /qn](#)

Actualización del fichero de firmas

La actualización del fichero de firmas se realiza mediante el proceso local [WalUpd](#).

Pasos para la actualización de los ficheros de firmas

```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng  
WAPLPMNG.exe WALUPD -force
```

Actualizar la configuración

Si se realiza algún cambio en el perfil de seguridad del grupo al que pertenece el equipo protegido, esta actualización se propagará al puesto, cuando este realice una consulta al servidor. Sin embargo, es posible forzar la actualización de la configuración mediante el proceso local [WalConf](#).

Pasos para la actualización de la configuración

```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng  
WAPLPMNG.exe WALCONF -force
```

```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng  
WAPLPMNG walscan -T:<FILENAME> -P:WAC -A:START
```

Obtener la fecha de los ficheros de firmas



La determinación de si la protección se encuentra actualizada con los últimos ficheros de firmas, se elabora en el backend de Panda Cloud Office Protection.

El agente envía al servidor su última fecha de actualización y ésta se contrasta con la fecha de los últimos ficheros de firmas publicados.

En esta sección se explica el mecanismo para la obtención de la última fecha de actualización de los ficheros de firmas en el equipo.

Es importante tener presente que esta información, junto con otra información del estado real de la protección, se actualiza continuamente en el equipo en un fichero denominado **WALTEST.DAT**.

Este fichero tiene formato de fichero XML por lo que puede tratarse como tal para analizar sintácticamente su contenido en busca de la información que nos interese (ver [Anexo 1](#)).

En la sección **<PavsigDate>** encontramos la información relativa a la fecha del último catálogo de fichero de firmas utilizado para actualizar.

Necesitamos, por tanto, recuperar este fichero y realizar un tratamiento de su contenido en búsqueda del tag **<PavsigDate>**

Pasos para obtener la fecha de los ficheros de firmas

Paso 0.

Previamente a la obtención de la información, se recomienda lanzar la actualización de los ficheros de firmas expuesta en el apartado número 4. Posteriormente actualizar la información del fichero waltest.dat lanzando el proceso local waltest.



```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng  
WAPLPMNG.exe WALUPD -force  
WAPLPMNG waltest -force  
(Update the file WALTEST.DAT)
```

Paso 1.

Posicionarnos en el directorio del proceso local Waltest y recuperar el fichero waltest.dat.

```
CD %ProgramFiles%\Panda Security\WaAgent\WalTest  
(find the file: WALTEST.DAT)
```

Paso 2.

Búsqueda del tag "<PavSigDate>". Para ello, podemos utilizar un programa que nos permita analizar sintácticamente ficheros XML, para lo cual será necesario renombrar el fichero waltest.dat a XML, o bien podemos utilizar el comando de DOS FindString que nos permite buscar cadenas en ficheros.

Aquí vamos a explicar la forma de obtener esa información mediante el comando FindString

```
FindStr "<PavSigDate>" waltest.dat  
(find tag <PavSigDate>)  
)
```



Obtendremos una información similar a la siguiente:

```
<PavSigDate>2012-03-23 12:25:43</PavSigDate>
```

En este ejemplo, la fecha del último catálogo utilizado para actualizar es "2012-03-23 12:25:43".

Obtener el estado del Antivirus, Firewall y el Control de dispositivos

Esta información se encuentra, junto con otra información del estado real de la protección, y se actualiza continuamente en el fichero denominado WALTEST.DAT.

Como ya se ha indicado en el punto anterior, este fichero tiene formato de fichero XML por lo que puede tratarse como tal para analizar sintácticamente su contenido en busca de la información que nos interese.

En la sección <AVSTATUSINFO> encontramos la información relativa al estado de cada una de las protecciones del antivirus. Cada sección <JOBID> hace referencia a cada protección y la información disponible es:

<IsInstalled> Protección instalada

<IsStarted> Esta ejecutándose.

<IsActivated> Esta activada desde configuración



Los valores y significados de los JobIDs son:

JobID	Significado
2	Protección de archivos (file resident)
4	Protección de correo (mail resident)
64	Protección Firewall
256	Device Control
512	Protección de transporte en servidores Exchange.
1024	Protección de buzones en servidores Exchange.
2048	Protección antispam en servidores Exchange.
4096	Monitorización de URLs.
8192	Protección antimalware en navegación web.

Pasos para obtener información del estado de la protección

Paso 0.

Previamente, aunque no sea necesario, se recomienda lanzar la actualización del fichero waltest.dat, ejecutando para ello, el proceso local WalTest.



```
CD %ProgramFiles%\Panda Security\WaAgent\WasLpMng  
WAPLPMNG waltest -force  
(Update the file WALTEST.DAT)  
CD %ProgramFiles%\Panda Security\WaAgent\WalTest
```

Paso 1.

Posicionarnos en el directorio del proceso local Waltest y recuperar el fichero waltest.dat.

```
CD %ProgramFiles%\Panda Security\WaAgent\WalTest  
(find the file: WALTEST.DAT)
```

Paso 2.

Obtener la información que deseemos.

```
FindStr "<JobID> <IsInstalled> <IsStarted> <IsActivated>" waltest.dat  
(find info in the file WALTEST.DAT)
```

Obtendremos una información similar a la siguiente:

```
<AVStatusInfo><JobStatusInfo><JobInfo><JobID>2</JobID>
```



```
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>4</JobID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>64</JobID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>256</JobID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
</JobStatus></JobStatusInfo>
```

En este ejemplo vemos lo siguiente:

Residente de ficheros (JobID = 2): Instalado, ejecutándose y activo.

Residente de correo (JobID = 4): Instalado, ejecutándose y activo.

Firewall (JobID = 64): Instalado, ejecutándose y activo.

Device Control (JobID = 256): Instalado, ejecutándose y activo.



Formato WALTEST.DAT. <AVSTATUSINFO>

```
<AVProducts><AVProduct><AVID><AVName>WAC</AVName>
<AVVersion>6.00.12.0000</AVVersion>
</AVID><PendingUpgrade>>false</PendingUpgrade>
<PavSigDate>2012-03-23 12:25:43</PavSigDate>
<MUID>69c87ea1-90d4-463d-999a-89302d311e26</MUID>
<AVStatusInfo><JobStatusInfo><JobInfo><JobID>2</JobID>
<UnitID>1</UnitID>
</JobInfo><JobStatus><IsInstalled>>true</IsInstalled>
<IsStarted>>true</IsStarted>
<IsActivated>>true</IsActivated>
<IsStatusCoherence>true</IsStatusCoherence>
<ReqConform>0</ReqConform>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>4</JobID>
<UnitID>1</UnitID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
<IsStatusCoherence>true</IsStatusCoherence>
<ReqConform>0</ReqConform>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>64</JobID>
<UnitID>2</UnitID>
```




```
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
<IsStatusCoherence>true</IsStatusCoherence>
<ReqConform>0</ReqConform>
</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>256</JobID>
<UnitID>8</UnitID>
</JobInfo><JobStatus><IsInstalled>true</IsInstalled>
<IsStarted>true</IsStarted>
<IsActivated>true</IsActivated>
<IsStatusCoherence>true</IsStatusCoherence>
<ReqConform>0</ReqConform>
</JobStatus></JobStatusInfo></AVStatusInfo></AVProduct></AVProducts></TestReport>
```

Anexo 2: Proceso de despliegue de la protección

Antes de entrar al detalle de los archivos, claves de registro, directorios y carpetas que se crean al desplegar la protección en los equipos, se ofrece información acerca del agente de administración, la funcionalidad P2P, la funcionalidad Proxy, y tiempos de instalación de la protección.

Todos ellos son aspectos a tener en cuenta para conocer con más detalle el proceso de despliegue.

El agente de administración

El agente es el encargado de las comunicaciones entre los equipos administrados y los servidores de PCOP. Se encarga de "hablar" con los agentes de los diferentes equipos



de su mismo grupo y de las descargas de programas de instalación desde Internet.

Al ejecutar el instalador del agente se lanza el proceso de instalación de PCOP, a lo largo del cuál se realizarán diferentes tareas, como la descarga de las configuraciones, la instalación de las protecciones, la actualización del archivo de identificadores, etc.

Como elemento fundamental en el diálogo entre los diferentes equipos, el agente es imprescindible para la puesta en práctica de la funcionalidad P2P, que se describe en el siguiente apartado.

Funcionalidad Peer To Peer (P2P)

Básicamente, consiste en una funcionalidad de tipo P2P que reduce el consumo de ancho de banda de la conexión a Internet, dando prioridad a que los equipos que ya han actualizado un archivo desde Internet lo compartan con otros que también necesitan actualizarlo. Así se evitan los accesos masivos a Internet y los consiguientes colapsos.

La funcionalidad P2P es de gran utilidad en el despliegue de PCOP a la hora de descargarse el programa de instalación. Cuando una de las máquinas ha descargado de Internet el programa de instalación, las otras tienen conocimiento de ello por medio de sus respectivos agentes de comunicación, que han sido activados y han puesto en marcha el proceso de instalación de PCOP .

En lugar de acceder a Internet acceden a la máquina que posee el programa de instalación y lo cogen directamente de ella. A continuación se realiza la instalación.

Pero esta funcionalidad es muy útil también en el caso de actualizaciones del motor de la protección y del archivo de identificadores, y se implementa en los dos procesos locales que necesitan descargar ficheros de Internet, WalUpd y WalUpg.



La activación se hace en los ficheros de configuración de estos procesos:

```
WALUPD.ini
```

```
[GENERAL]
```

```
UPDATE_FROM_LOCAL_NETWORK=1
```

```
WALUPG.ini
```

```
[GENERAL]
```

```
UPGRADE_FROM_LOCAL_NETWORK=1
```

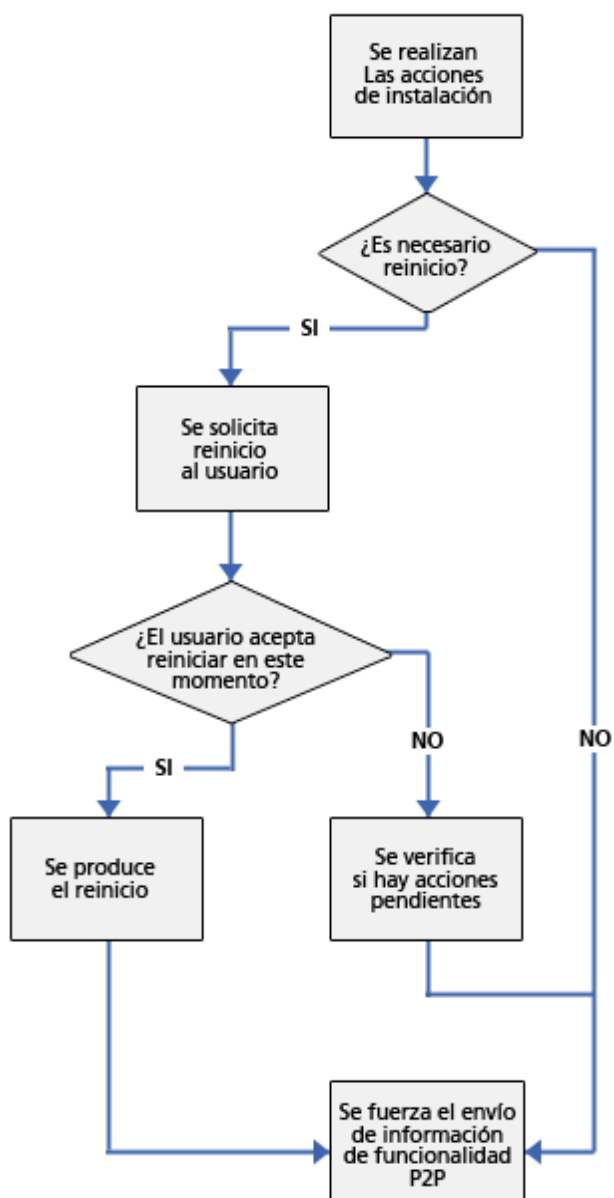
La funcionalidad P2P funciona de forma independiente en cada uno de estos procesos locales, pudiendo estar activo únicamente en uno de ellos.

Las bases del funcionamiento de la funcionalidad P2P son las siguientes

Cuando una máquina termina de actualizar los ficheros de firmas o alguna protección (o el propio agente) envía por broadcast la información de los ficheros que tiene disponibles al resto de máquinas de la red.

En cuanto al envío de la información EN WALUpg, en caso de ser necesario algún reinicio después de la instalación/actualización de las protecciones, si el usuario opta por no reiniciar el equipo inmediatamente sino más tarde, la información de la funcionalidad P2P se enviará de forma inmediata en lugar de esperar al reinicio.

El funcionamiento se muestra en el siguiente diagrama:



Las máquinas que reciben el mensaje guardarán la información que han recibido para utilizarla cuando la necesiten.



Si una máquina necesita algún fichero, antes de intentar descargarlo de Internet comprobará si puede obtenerlo de otra máquina. Si es así enviará un mensaje a la máquina que lo tiene disponible para solicitárselo. El fichero se recibirá de forma asíncrona y se esperará un tiempo máximo a recibirlo antes de reintentar.

La máquina que tiene el fichero recibirá un mensaje de solicitud y como respuesta enviará un mensaje con el fichero.

La máquina que pidió el fichero lo recibirá y podrá proseguir con la actualización o upgrade.

➡ *Para que una máquina pueda servir ficheros a otras a través de la funcionalidad P2P debe tener al menos 128 MB de RAM.*

Proxy dinámico

El agente guarda una lista con información de equipos en la red que tengan agentes que son capaces de enviar mensajes a Internet. Estos agentes se denominan Proxys.

➡ *Para poder actuar como proxy para otros agentes, una máquina debe cumplir los siguientes requisitos: disponer de conexión directa a Internet, y disponer al menos de 128 MB de RAM. Además, el equipo no puede estar en lista negra y debe haber concluido completamente la secuencia de instalación*

Cuando la lista de proxys está vacía o ninguno de los agentes que están en ella responde (Disponibilidad = 0), el agente envía un mensaje por broadcast a la subred preguntando ¿quién es Proxy? para que estos le respondan y pueda mandar mensajes a Internet a través de ellos.



Mientras realiza la espera por datos de la lista de proxys válidos, el módulo del Proxy no atenderá peticiones de otros mensajes.

La lista de proxys tendrá un valor asociado para cada Proxy con el número de intentos que se permiten fallar en la comunicación con otro agente antes de invalidar ese agente como proxy.

Por defecto el número de veces será 3, y cuando este valor alcance 0 se entenderá que ese agente no es válido como proxy. Si en algún momento todos los proxys de la lista son inválidos se entiende que la lista es no válida en su conjunto y se comenzará la búsqueda de proxys, lanzando un mensaje "¿quién es proxy?".

Puede ocurrir que el mensaje se envíe correctamente a un proxy de la lista, pero que éste al intentar mandar el mensaje a Internet descubra que ya no tiene conexión.

En ese caso el agente remoto repetirá la secuencia aquí descrita reenviando el mensaje a un proxy de su lista, pero además enviará por TCP al agente del que le llegó el mensaje otro de tipo "Yo no soy Proxy", para indicarle que lo borre de su lista porque ya no tiene conexión a Internet.

Este proceso se repetirá hasta que el mensaje se envíe correctamente a Internet o hasta que pase por un número máximo de proxy sin conseguir enviarse, en cuyo caso se perderá.

Se puede configurar el número de proxys por los que puede pasar un mensaje. Por defecto sólo se enviará a 1, y si falla el envío desde ése se perderá el mensaje.

Dentro del mensaje se guarda la lista de proxys por los que ha pasado, de modo que no se envíe dos veces al mismo proxy sin conexión a Internet.



Proxy estático

Si deseamos que todos los accesos a internet se hagan a través de un equipo concreto decidido por el administrador, en lugar de por equipos determinados de forma dinámica, el agente de comunicaciones admite la posibilidad de especificar que máquina deseamos que actúe como Proxy.

La máquina que actúe como 'Proxy estático' debe cumplir los siguientes requisitos:

Debe tener un agente instalado versión 6.0 o superior.

Debe tener acceso directo a Internet

Disponer de al menos 128 MB de memoria.

Debe haber comunicado con el servidor en las últimas 72 horas

Además, el equipo no puede estar en lista negra y debe haber concluido completamente la secuencia de instalación

Si en algún momento el equipo que se estableció para que actuara como proxy estático dejara de cumplir alguno de los requisitos necesarios para ejercer como tal, se desactivará en la consola la configuración del proxy estático, desapareciendo el nombre del equipo que estaba configurado y se mostrará un mensaje indicándole cuál de dichos requisitos se incumple.

Usted podrá seleccionar otro equipo para que realice las funciones de proxy estático. Si un equipo deja de ser proxy estático por haber sido incluido en la lista negra, una vez que deje de pertenecer a dicha lista, si se desea que actúe de proxy estático será necesario configurarlo de nuevo para que transiten por él todas las comunicaciones con el servidor.

Cuando el agente tenga que realizar un acceso a Internet en primer lugar intentará



comunicarse utilizando el 'proxy estático'.

Si la comunicación con el Proxy estático no es posible, se intentará llevar a cabo el acceso a internet siguiendo la secuencia de comunicaciones habitual.

Si tiene una configuración válida almacenada, intentará la comunicación utilizando dicha configuración.

En caso contrario, intentará comunicarse mediante conexión directa a Internet.

Si tampoco consigue la conexión directa, lo intentará a través de otro equipo 'proxy dinámico', cuyo funcionamiento se ha detallado en el apartado anterior.

Cuando el equipo que está actuando como proxy recibe una petición de acceso a internet intentará realizar la conexión de forma directa. Si la conexión se realiza con éxito enviará la respuesta obtenida al agente que solicitó la conexión.

La configuración del proxy estático se realiza en el apartado Proxy/Repositorio de las Opciones avanzadas de la pestaña Principal de la configuración general del perfil.

Despliegue de Panda Endpoint Agent

Módulos principales de la arquitectura

Panda Endpoint Agent está formado por cuatro componentes principales:

Agente de administración



Panda Cloud Office Protection

Procesos Locales

Watchdog

Planificador de tareas (scheduler)

Árbol de carpetas y entradas de registro de Panda Endpoint Agent

En el diagrama siguiente AdminIEClientPath es la ruta raíz donde se han instalado los módulos.



Panda Cloud Office Protection

- [-] Panda Security
 - [-] WaAgent
 - [-] Common
 - [-] DATA
 - [-] Cfg
 - WAC
 - Scans
 - [-] Scheduler
 - config
 - [-] WAHost
 - [-] Data
 - Catalog
 - WalConf
 - WalLnChr
 - WalPsEvt
 - WalQtine
 - WalReport
 - WalScan
 - WalSNet
 - WalSysCf
 - WalSysIn
 - WalSysUd
 - WalTask
 - WalTest
 - [-] WalUpd
 - [-] Data
 - Catalog
 - Files
 - [-] WalUpg
 - [-] Data
 - Catalog
 - Files
 - WAPWInst
 - [-] WasAgent
 - Data
 - [-] WasLpMng
 - config
 - WASWD



WasAgent – carpeta raíz de instalación de Panda Endpoint Agent.

Common – carpeta donde se guardan los ficheros de uso común, como WalAgApi.dll, librerías de núcleo, etc. Durante la ejecución de los procesos locales se creará en esta carpeta una subcarpeta "Data"

Scheduler – carpeta donde se guardan los ficheros del planificador de tareas.

Scheduler\Config – carpeta donde se guardan los ficheros de tokens para el planificador de tareas.

WalHost – carpeta donde se guardan los ficheros del servicio del agente de administración. Durante la ejecución de los procesos locales se puede crear en esta carpeta una subcarpeta "Data"

WalConf – carpeta donde se guardan los ficheros del proceso local WalConf.

WalTest – carpeta donde se guardan los ficheros del proceso local WalTest.

WalLnChr – carpeta donde se guardan los ficheros del proceso local WalLnChr.

WalPsEvt – carpeta donde se guardan los ficheros del proceso local WalPsEvt.

WalQtine – carpeta donde se guardan los ficheros del proceso local WalQtine.



WalReport – carpeta donde se guardan los ficheros del proceso local WalReport.

WalScan – carpeta donde se guardan los ficheros del proceso local WalScan.

WalSNet – carpeta donde se guardan los ficheros del proceso local WalSNet.

WalSysCf – carpeta donde se guardan los ficheros del plugin WalSysCf.

WalSysIn – carpeta donde se guardan los ficheros del plugin WalSysIn

WalSysUd – carpeta donde se guardan los ficheros del plugin WalSysUd

WalTask – carpeta donde se guardan los ficheros del plugin WalTask.

WalUpd – carpeta donde se guardan los ficheros del proceso local WalUpd. Durante la ejecución del proceso local se creará en esta carpeta una subcarpeta "Data"

WalUpg – carpeta donde se guardan los ficheros del proceso local WalUpg. Durante la ejecución del proceso local se creará en esta carpeta una subcarpeta "Data"

WAPWInst – carpeta donde se guardan los ficheros del proceso que supervisa la instalación.

WasAgent – carpeta raíz de instalación del agente de administración. Al ejecutarse el agente se creará en esta carpeta una subcarpeta "Data"

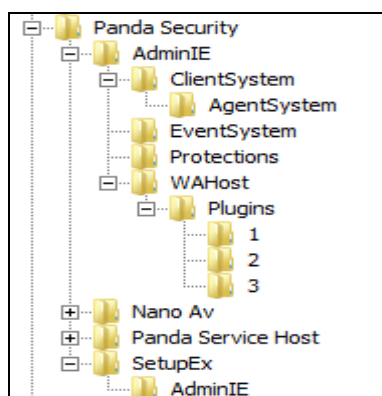


Panda Cloud Office Protection

WasLpMng – carpeta donde se guardan los ficheros del gestor de procesos locales.

WasLpMng\Config – carpeta donde se guardan los ficheros de tokens para el gestor de procesos locales.

Árbol de Entradas de registro de Windows



Panda Security se refiere a la clave del registro de Windows

HKEY_LOCAL_MACHINE\SOFTWARE\Panda Security\

AdminIE

carpeta dentro de la cual se crean todas las entradas de registro propias de PCOP.

ClientSystem



Panda Cloud Office Protection

Clave de registro que contiene entradas de Panda Endpoint Agent. Estas entradas son:

- `InstallPath` - Contiene el directorio raíz en el que se ha instalado Panda Endpoint Agent (lo que arriba se denominaba "AdminIEClientPath")

EventSystem

Contiene la configuración del sistema de eventos.

Protections

Contiene información sobre la protección.

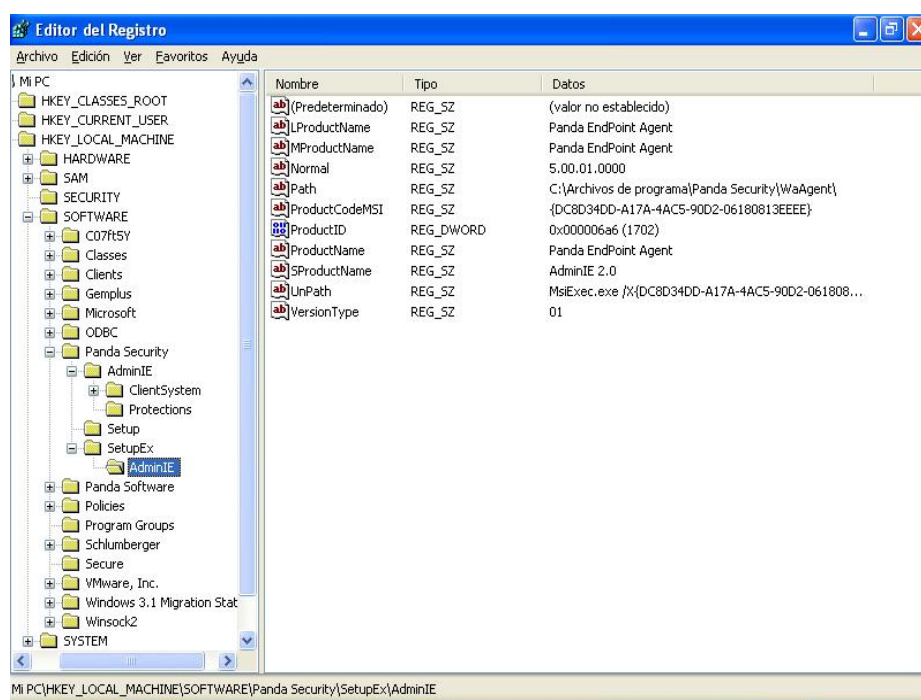
WAHost

Contiene la configuración del servicio del agente de administración.

SetupEx

carpeta dentro de la cual se crean todas las entradas de registro que serán utilizadas por los instaladores que emplean el Agente.

- `AdminIE` - clave de registro que contiene todas las entradas de Panda Endpoint Agent empleadas por los instaladores. Dichas entradas aparecen reflejadas en la siguiente captura:



El agente durante su ejecución creará la clave "AgentSystem" debajo de "ClientSystem". Dentro de esa clave se crearán diversas entradas. El instalador no se tiene que preocupar de nada salvo de borrar la clave "AgentSystem" y sus entradas en la desinstalación.

Distribución de ficheros

Toda máquina administrada lleva instalado el agente de administración. Junto con el agente se instalan también los procesos locales.

A continuación se presentan todas las rutas y ficheros del agente de administración y los procesos locales:



Agente de administración

El Agente se instala en <AdminIEClientPath>\WasAgent

- WasAgent.conf
- WasAgent.dll
- WaPIRes.exe
- WAInterface.dll
- Wa_AGPRX.dat
- LPTokens.dat
- INTEGRA.dat
- INTEGRA.bak (se genera durante la instalación, no se distribuye)
- AgentSystem.DAT
- proxy.dat (se genera durante la instalación, no se distribuye)

Durante la ejecución del agente se crea dentro de esta carpeta la subcarpeta "Data", con los siguientes ficheros:

- MsiExec.log
- WasAgent.log
- WaHost.log
- WapWinst.log
- Counters.ini



Panda Cloud Office Protection

Así mismo se creará la clave de registro "AgentSystem" debajo de "ClientSystem". Dentro de esa clave se crearán las entradas:

- Value1
- Value2
- Value3

Si la conexión a Internet se debe hacer a través de proxy, al solicitar al usuario los datos para realizar la conexión estos se almacenarán en el fichero AgentSystem.dat dentro de la carpeta <AdminIEClientPath>\WasAgent.

Todo debe ser borrado en la desinstalación.

Proceso local WalConf

Se instala en < AdminIEClientPath >\WalConf

- WalConf.ini
- WalConf.dll

Durante la ejecución de este proceso local se creará el siguiente fichero:

Walconf.log

Proceso local WalLnChr

Se instala en < AdminIEClientPath >\WalLnChr

- WalLnChr.dll



Durante la ejecución de este proceso local se crearán el siguiente fichero:

WalLnchr.log

Proceso local WalQtine

Se instala en < AdminIEClientPath >\WalQtine

- WalQtine.ini

- WalQtine.dll

Durante la ejecución de este proceso local se creará el siguiente fichero:

WalQtine.log

Proceso local WalReport

Se instala en < AdminIEClientPath >\WalReport

- WalReport.dll

- WalReport.ini

Durante la ejecución de este proceso local se creará el siguiente fichero:

- WalReport.log

Proceso local WalScan

Se instala en < AdminIEClientPath >\WalScan

- WalScan.dll



- WalScan.ini

Durante la ejecución de este proceso local se creará el siguiente fichero:

WalScan.log

Proceso local WalTest

Se instala en < AdminIEClientPath >\WalTest

- WalTest.dll
- WalTest.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- WalTest.dat
- WalTest.log
- Waltestlt.dat
- Waltestdf.dat

Proceso local WalUpd

Se instala en < AdminIEClientPath >\WalUpd

- WalUpd.dll
- WalUpd.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:



- Counters.ini
- WalUpd.log

También se generará el subdirectorio Data que contendrá el subdirectorio Catalog que podrá llegar a disponer de los siguientes ficheros:

- WEB_GUID
- WEB_CATALOG
- LAST_GUID
- LAST_CATALOG
- LOCAL_CATALOG
- RUMOR_TABLE
- LOCAL_CATALOG.TMP

y el subdirectorio Files que contendrá de manera temporal los ficheros necesarios para realizar actualizaciones necesarias.

Proceso local WalUpg

Se instala en < AdminIEClientPath >\WalUpg

- WalUpg.dll
- WalUpg.ini
- PavGenUn.exe



- Settings.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- Counters.ini
- WalUpg.dat
- WalUpg.log
- WAUPGTD.dat
- WAC_Installer.log
- Agent_Installer.log

También se generará el subdirectorio Data que contendrá el subdirectorio Catalog que podrá llegar disponer de los siguientes ficheros:

- WEB_GUID
- WEB_CATALOG
- LAST_GUID
- LAST_CATALOG
- LOCAL_CATALOG
- RUMOR_TABLE
- LOCAL_CATALOG.TMP
- INSTALLED_PRODUCTS.TMP

y el subdirectorio Files que contendrá de manera temporal los instaladores necesarios para realizar las instalaciones/actualizaciones de los productos.



Proceso local WalSNet

Se instala en < AdminIEClientPath >\WalSNet

- WalSNet.dll
- WalSNet.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- WALNet.log
- WALNET.dat

Plugin WalTask

Se instala en < AdminIEClientPath >\WalTask

- WalTask.dll
- WalTask.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- WalTask.log
- SCAN_TASKS.DAT

Plugin WalSysCf

Se instala en < AdminIEClientPath >\WalSysCf

- WalSysCf.dll



- WalSysCf.dat

Durante la ejecución de este proceso local se crearán el siguiente fichero:

- WalSysCf.log

Plugin WalSysUd

Se instala en < AdminIEClientPath >\WalSysUd

- WalSysUd\WalSysUd.dll

Gestor de procesos locales

Se instala en < AdminIEClientPath >\WasLpMng

- WapLpMng.exe
- WasLpMng.dll
- Config\Plugins.tok (en el subdirectorio config)
- WapLpmng.ini
- WasLpmng.ini

Durante el proceso de instalación se crearán los ficheros

- WapLpmng.log
- WasLpmng.log



Planificador de tareas

Se instala en < AdminIEClientPath >\Scheduler

- PavAt.exe
- PavSched.dll
- PavAt3Api.dll
- Config\tokens.tok (en el subdirectorio config)

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- Pavsched.cfg (generado durante el proceso de instalación)
- Tasklist.lst (se genera durante la instalación, no se distribuye)

Servicio principal

Se instala en < AdminIEClientPath >\WAHost

- WAHost.exe
- WAHostClnt.dll

Librerías comunes

Se instala en < AdminIEClientPath >\Common



APIcr.dll

AVDETECT.INI

DATA

libxml2.dll

MiniCrypto.dll

PavInfo.ini

pavsddl.dll

Platforms.ini

pskalloc.dll

PSLogSys.dll

pssdet.dll

psspa.dll

putczip.dll

puturar.dll

putuzip.dll

WalAgApi.dll

WalCount.dll

WALLMIInf.dll

WALMNAPI.dll

WALOSInf.dll

WALRVNCInf.dll

WALTVNCInf.dll

WALTVWRInf.dll



WALUtils.dll

WalUtils.ini

WALUVNCInf.dll

WaPrxRepos.dll

WaPrxRepos.Ini

WCheckReq.dll

Durante su ejecución se creará la subcarpeta "Data" dentro de ésta, que contendrá las políticas propias de la protección para que estén disponibles cuando esta se instale.

Así mismo se crearán los siguientes ficheros:

- PavInfo
- WalUtils.log
- WALMNAPI.log
- WALLMIInf.log
- WALRVNCInf.log
- WALTVNCInf.log
- WALUtils.log
- WALTVWRInf.log
- WALUVNCInf.log

Servicios

Panda Endpoint Agent crea el servicio siguiente:



- WAHost.exe

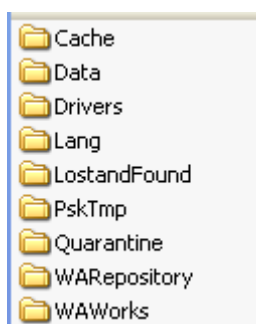
Los servicios se instalan llamando al ejecutable con la opción "-RegServer", y se desinstalan con la opción "-UnregServer"

Despliegue de Panda Endpoint Protection

Estructura de directorios de Panda EndPoint Protection

El usuario puede elegir la ruta donde desea instalar el producto. Por defecto la ruta de instalación es la siguiente:

%PROGRAMFILES%\Panda Security\WAC\



InstallPath

Ruta de instalación de Panda EndPoint Protection. Contiene los ficheros necesarios para el funcionamiento de Panda EndPoint Protection.

Cache: Contiene los ficheros de firmas locales.

Data: Contiene los ficheros de datos de la tecnología de análisis por comportamiento.



Drivers: Contiene binarios que se usan en la instalación / desinstalación de las unidades.

NNSNahs: Binarios para la instalación del driver intermediate del Firewall.

PSINDvct: Binarios para la instalación del driver de la tecnología Device Control.

Lang: Contiene los diccionarios con los diferentes idiomas.

LostandFound: Contiene los elementos restaurados de la cuarentena, cuando han sido movidos por las protecciones de correo, o cuando no se han podido restaurar en su ruta original.

Quarantine: Los elementos que se han movido a cuarentena.

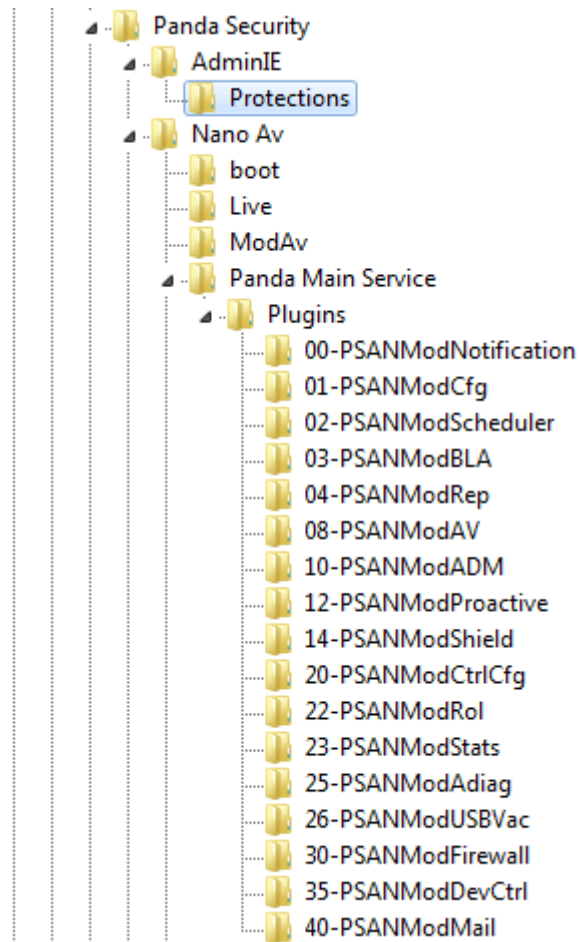
PskTmp: Ficheros temporales de configuración creados durante los análisis.

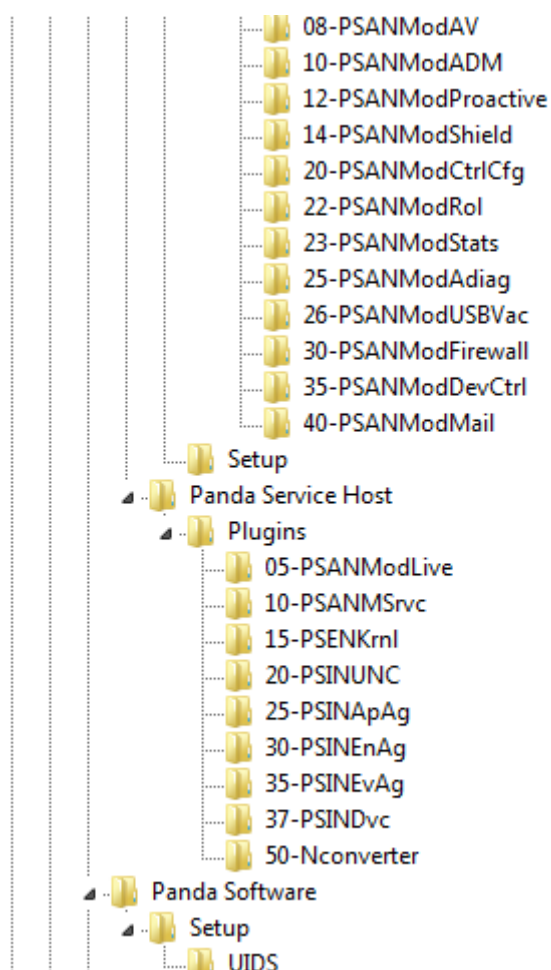
Entradas de registro

Entradas del registro en Panda Software



Panda Cloud Office Protection





Panda Security: Clave en HKEY_LOCAL_MACHINE\Software\Panda Security bajo la que se encuentran las claves y valores de la protección.

AdminIE\Protections: Clave donde se encuentra el valor WAC que indica donde está instalado el cliente.

Nano Av\Boot: Mantenido por compatibilidad con versiones anteriores. Actualmente no se utiliza.



Panda Cloud Office Protection

Nano AV\ModAV: Mantenido por compatibilidad con versiones anteriores. Actualmente no se utiliza.

Nano Av\Live: Clave donde se encuentra el valor DownloadFolder en el que se indica la carpeta de descargas del cliente

Nano Av\Panda Main Service: Clave donde se guardan los valores de carga de plugins del módulo principal del antivirus.

Nano Av\Setup: Contiene el Path de instalación de la protección

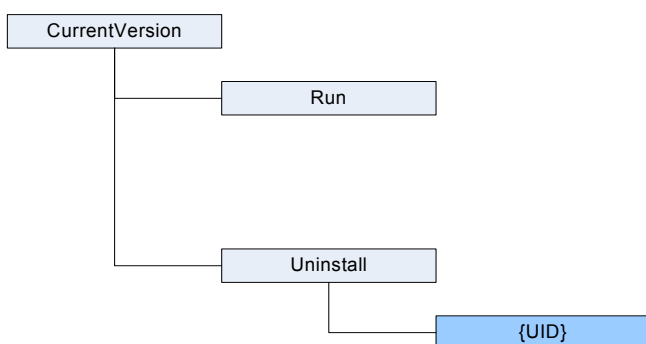
Panda Service Host: Contiene los plugins que se cargan en el servicio: sistema de actualización, el sistema principal del antivirus, el motor, el sistema de interceptación de ficheros y procesos, sistema de configuración del device control, firewall.

Panda Software\Setup: (nombre, versión, ID, ruta de instalación, etc).

Entradas del registro en Windows\CurrentVersion

En este apartado se podrán ver las entradas de registro que Panda EndPoint Protection crea dentro de la clave:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion



CurrentVersion

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

Run

Clave del sistema donde está la ruta a aquellas aplicaciones lanzadas al inicio.

Uninstall

Clave del sistema donde se almacena información relativa a los desinstaladores de los productos instalados en el sistema.

Panda Universal Agent Endpoint: Clave con información necesaria para la desinstalación del producto.

Entradas del registro en Services

Services

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services



NNSALPC: Driver del firewall.

NNSHTTP: Driver del firewall.

NNSIDS: Driver del firewall.

NNSNAHS: Driver del firewall.

NNSPICC: Driver del firewall.

NNSPIHS: Driver del firewall.

NNSPOP3: Driver del firewall.

NNSPROT: Driver del firewall.

NNSPRV: Driver del firewall.

NNSSMTP: Driver del firewall.

NNSSTRM: Driver del firewall.

NNSTLSC: Driver del firewall.

NNSHTTPS: Driver del firewall.

PRKPAVPROC: Driver usado para análisis de Rootkits.

PSBOOT.SYS: Driver que se encarga de operaciones a reinicio.

PSINAflt: Filtro de interceptación.

PSINDvct: Driver de Device Control.

DVCTPROV.sys: Driver de Device Control

PSINFile: Driver de interceptación de ficheros.

PSINKNC: Driver de interceptación de kernel.

PSINProc: Driver de interceptación de procesos.



PSINProt: Driver protector (escudo, KRE).

PSKMAD: Driver de análisis de memoria.

Servicios

PSUAService: Servicio de control y gestión de tareas en las diferentes sesiones.

NanoServiceMain: Servicio principal del cliente para todas las protecciones.

CLOUDUPDATEREX: Servicio encargado de tareas de Upgrade.

Procesos

Aparte de los servicios mostrados en el punto anterior, los siguientes procesos pueden estar ejecutados en la máquina:

bspatch.exe

Proceso usado en el parcheo de los ficheros de firmas.

PAV2WSC.exe

Proceso usado para la actualización del estado del antivirus en el Windows Security Center.

PSANCU.exe

Proceso usado para realizar tareas de configuración durante la instalación y durante los upgrades del cliente.



PSINanoRun.exe

Proceso usado durante la instalación y upgrades del cliente.

PSNCSysAction.exe

Proceso que realiza las tareas de activación / desactivación del driver intermediate NNSNahs del firewall.

PSUAMain.exe

Proceso correspondiente a la traybar.

PSUNMain.exe

Proceso correspondiente interfaz del cliente.

Setup.exe

Proceso correspondiente a tareas de instalación y upgrades.

WAScanner.exe

Proceso que gestiona las tareas de análisis de background configuradas desde la consola web.



Anexo 3: Descubrimiento automático de equipos

Panda Cloud Office Protection dispone de un sistema de descubrimiento de equipos, que permite que el administrador pueda tener una visión general de cuáles son los equipos de su red que no se encuentran protegidos.

Este sistema se basa en la configuración y ejecución de tareas de búsqueda, que se llevan a cabo desde un "equipo descubridor", que ha de reunir una serie de requisitos para poder actuar como tal.

Datos a tener en cuenta a la hora de crear una tarea de búsqueda

Se realizará una única ejecución por tarea de búsqueda.

La ejecución de la tarea de búsqueda comenzará una vez que el equipo descubridor se descargue la orden de descubrimiento desde el servidor de Panda Cloud Office Protection. Existirá, por tanto, un margen de tiempo entre la creación de la tarea y la ejecución de la misma.

Se podrá forzar el comienzo inmediato de la tarea si se realiza una actualización a través de la opción **Actualizar** del menú contextual de la protección en el equipo descubridor.

En caso contrario podrán pasar hasta un máximo de 4 horas antes de que comience a ejecutarse la tarea.

Es posible definir varias tareas de búsqueda para un mismo equipo descubridor. En esta caso las tareas se irán ejecutando de forma secuencial, en el orden en que se han



definido.

Si se produce un reinicio de la máquina durante la ejecución de una tarea de descubrimiento, la tarea se ejecutará de nuevo a los 5 minutos del arranque. Previamente se validará contra el servidor que la tarea de descubrimiento sigue vigente.

Al configurar la tarea de búsqueda, es necesario proporcionar la siguiente información

Nombre de la tarea (de 50 caracteres como máximo)

No se permitirá crear tareas con el mismo nombre dentro del mismo cliente.

No se permitirá la introducción de los siguientes caracteres en el nombre de las tareas
<, >, ", ', &

Equipo desde donde se lanzará la tarea de descubrimiento de equipos ('equipo descubridor'), seleccionándolo de la lista de equipos protegidos.

Se podrá limitar el alcance del barrido de la red, eligiendo una de las siguientes opciones:

La **subred del equipo** que realiza el descubrimiento (opción seleccionada por defecto).

Uno o varios **rangos de direcciones IP (IPv4)** introducidos por el usuario. Si se introducen rangos con direcciones IP en común se realizará el descubrimiento una única vez.

Uno o varios **dominios** introducidos por el usuario.



Requisitos que debe reunir el equipo descubridor

Tener instalado el agente y la protección, y estar integrado correctamente en el servidor de Admin IE.

Tener una versión de agente 5.05 o superior.

No deberá estar en lista negra.

Deberá haberse conectado durante las últimas 72 horas con el servidor de AdminIE.

No deberá estar realizando una tarea de desinstalación, el equipo no podrá estar en ninguno de los siguientes estados en una tarea de desinstalación:

En espera

Iniciando

Desinstalando

Debe disponer de conexión a Internet, ya sea directamente, o a través de otros equipos (funcionalidad 'proxy')

A medida que se van sucediendo las acciones de la tarea de búsqueda, Panda Cloud Office Protection mostrará el estado en el que se encuentra la tarea.

Secuencia de acciones de la tarea de búsqueda y correspondencia con el estado de la tarea

El usuario ordenará la ejecución desde la Consola para Clientes, de una tarea de descubrimiento de equipos, a partir de un equipo que ya cuenta con la protección



instalada ('Equipo descubridor').

Estado de la tarea: En espera

El 'Equipo descubridor' se descargará la orden de descubrimiento del servidor. El servidor tendrá constancia de esta acción y modificará el estado de la tarea.

Estado de la tarea: Iniciando

El 'Equipo descubridor' recalculará la prioridad de la nueva tarea, junto con las tareas que ya estuviesen a la espera de ser ejecutadas. Esperará a que le llegue el turno, según la lógica de prioridades.

Estado de la tarea: Iniciando

El 'Equipo descubridor' comprobará que cumple con los requisitos para poder ejecutar la tarea.

Estado de la tarea: Iniciando

Se enviará un mensaje al servidor indicando el comienzo de la ejecución de la tarea.

Estado de la tarea: En curso

El 'Equipo descubridor' realizará el barrido de la red, en busca de equipos.



Estado de la tarea: En curso

Secuencia de la tarea de búsqueda

Obtener la lista de máquinas

Por IP (Rangos de IP y Subred)

Se hace un ping a cada IP mediante el protocolo ICMP

Se espera la respuesta a los ping

Se intenta resolver el nombre de las IPs que responden

Por dominio

Se enumeran los equipos pertenecientes al dominio

Determinar si las máquinas que tenemos en la lista tienen el agente instalado

Se envía un mensaje al agente

Se espera respuesta

Generar lista de equipos y enviar los resultados al servidor

Resultados de la tarea de búsqueda

El equipo descubridor enviará siempre al servidor el listado completo de equipos no protegidos descubiertos, aunque no haya sufrido modificación con respecto al listado enviado anteriormente por el mismo equipo.



El listado de equipos descubiertos contendrá:

Equipos sin agente instalado.

Equipos integrados en otro cliente.

No hay forma de comunicar con agentes de otros clientes, por lo tanto, no se recibirá respuesta y se asumirá que el equipo no está protegido.

Equipos con agente inferior a 5.05.

El agente de estos equipos no está preparado para responder a los mensajes de descubrimiento, y por lo tanto se considerarán como equipos no protegidos.

Equipos que tienen agente 5.05 ó superior pero que no hayan respondido al mensaje de descubrimiento durante el tiempo establecido. El tiempo de espera de la respuesta será= 3 seg (Factor de espera) * Número de equipos que han respondido a petición del protocolo ICMP (ping)+30 seg (margen de seguridad).

NOTA: Los equipo en lista negra (siempre y cuando tengan agente 5.05 o superior y estén integrados en clientes) no se considerarán equipos no protegidos descubiertos, y por lo tanto NO se incluirán en el listado de equipos descubiertos.

Detalle de los equipos no protegidos

De cada 'Equipo descubierto', se obtendrá:

Dirección IP, siempre.

Nombre de equipo, si el 'Equipo Descubridor' fue capaz de resolverlo.



Casos en los que el servidor puede NO tener constancia de la finalización de una tarea de descubrimiento

Caso 1

La tarea se encuentra en situación de "En espera", "Iniciando" o "En curso", y el equipo distribuidor se desinstala, elimina de la base de datos o es enviado a lista negra durante la ejecución de la tarea.

Consecuencias

El 'equipo descubridor' no podrá informar al servidor sobre el resultado de dicha tarea.

En cuanto el servidor tenga constancia de que el "equipo descubridor" ha sido eliminado, desinstalado* o enviado a lista negra, la tarea de descubrimiento pasará a estado "Finalizado con error".

***NOTA:** se considerará que el "equipo descubridor" ha sido desinstalado en cuanto envíe el mensaje de fin de desinstalación, es decir, en cuanto termine de desinstalar la protección.*

Además, si el 'Equipo Descubridor' ha sido eliminado:

Se eliminará su nombre de la pantalla de configuración de la tarea de descubrimiento, y se mostrará un error que indique que el equipo ha sido eliminado.

Al eliminar el equipo, también se eliminará la información del grupo al que pertenecía dicho equipo, por lo tanto, los usuarios monitorizadores o administradores con permiso sobre dicha tarea (con permiso sobre el grupo del "Equipo Descubridor"),



dejarán de visualizarla.

Caso 2

La tarea se encuentra en estado "En espera", "Iniciando" o "En curso", y el equipo descubridor es enviado a lista negra y posteriormente restaurado.

Consecuencias

El equipo continuará con la tarea que tenía pendiente, y por lo tanto, el estado de la tarea podrá cambiar, podrá pasar de 'Finalizado con Error' a 'Finalizada', siendo éste el único cambio de estado posible.

Si el 'equipo descubridor' tiene algún problema de comunicación durante la ejecución de la tarea, no podrá informar al servidor sobre el estado y los resultados de dicha tarea.

La tarea no actualizará su estado, y se mantendrá en el estado en el que estaba ("En espera" "Iniciando" o "En Curso") hasta que sea eliminada.

Si se produce algún error durante la ejecución de la tarea, (tarea en estado "En espera", "Iniciando" o "En curso"): la tarea se mantendrá en el estado en el que estaba ("En espera" "Iniciando" o "En Curso") hasta que sea eliminada.

Ante la **interrupción de la tarea**, el comportamiento será el siguiente:

Si una vez iniciado el descubrimiento de equipos y, antes de que finalice, se apagase el 'Equipo descubridor' por cualquier motivo (a voluntad del usuario o fortuitamente), al volver a arrancar el equipo, el agente:

Chequeará contra el servidor la vigencia de la tarea.



En caso de seguir vigente, relanzará de nuevo el descubrimiento desde el principio

En caso de no seguir vigente, por haberse superado el tiempo máximo de existencia de una tarea, abortará el descubrimiento.

Esperará 5 minutos a partir del reinicio del equipo para relanzar la tarea de descubrimiento.

Anexo 4: Panda Cloud Office Protection para Linux

Prerrequisitos

El sistema debe cumplir los siguientes requisitos:

Debe estar instalada la utilidad "lsb_release" (en RedHat y Debian).

Esta utilidad se utiliza para determinar la distribución de Linux en que se está ejecutando el instalador.

En Debian se debe descargar e instalar el paquete:

lsb-release_3.2-23.2squeeze1_all.deb

Dependencias de la protección PavSL (todas las distribuciones)

La protección PavSL necesita de la instalación de las siguientes librerías para su correcto funcionamiento:

libsoup-2.4.so.1 (HTTP client/server library for GNOME)



libmccrypt.so.4 (MCrypt - encryption functions)

libz.so.1 (zlib compression and decompression library)

Revisar sobre el directorio `/opt/PCOPAgent/PCOPScheduler/pavsl-bin/` que están todas las dependencias de la "PavSL":

```
# ldd libPskcomms.so
```

En caso de SUSE/OpenSUSE de x64 si hay problemas aplicar el siguiente "workaround":

Instalar (si no lo está) la ligsoup-2_4-1-32bit. Por ejemplo:

```
# zypper install ligsoup-2_4-1-32bit
```

Instalar (si no lo está) la libgthread-2_0-0-32bit. Por ejemplo:

```
# zypper install libgthread-2_0-0-32bit
```

Desinstalar la libmccrypt y la mccrypt:

```
# zypper rm libmccrypt
```

```
# zypper rm mccrypt
```



Instalar "libmccrypt-2.5.8-109.1.2.i586.rpm". Descargar e instalar si no lo está ya.

AT/CRON correctamente instalados y habilitados (TODAS DISTRIBUCIONES):

Se debe revisar en los servicios del sistema que están correctamente instalados y activados los servicios de AT y CRON.

Workaround para el "atd" (en suse y opensuse)

Las acciones para solucionar que el "atd" no arranque de forma automática en openSUSE son las siguientes:

Alterar el fichero: /etc/sysconfig/atd

```
ATD_BATCH_INTERVAL = "60"
```

```
ATD_LOADAVG = "0.8"
```

Alterar el fichero /lib/systemd/system/atd.service para transformarlo en:

```
# cat /lib/systemd/system/atd.service
```

```
[Unit]
```

```
Description=Execution Queue Daemon
```

```
After=syslog.target
```



[Service]

Type=forking

EnvironmentFile=-/etc/sysconfig/atd

ExecStart=/usr/sbin/atd -b \${ATD_BATCH_INTERVAL} -l \${ATD_LOADAVG}

[Install]

WantedBy=multi-user.target

Recargar el demonio, arrancarlo, comprobar el status y...

```
# chkconfig --add atd
```

```
# systemctl --system daemon-reload
```

```
# systemctl enable atd.service
```

```
# systemctl start atd.service
```

```
# systemctl status atd.service
```

atd.service - Execution Queue Daemon

Loaded: loaded (/lib/systemd/system/atd.service; disabled)

Active: active (running) since Fri, 05 Oct 2012 12:14:52 -0500; 1s ago

Process: 20851 ExecStart=/usr/sbin/atd -b \${ATD_BATCH_INTERVAL} -l \${ATD_LOADAVG} (code=exited, status=0/SUCCESS)

Main PID: 20852 (atd)

CGroup: name=systemd:/system/atd.service

└─ 20852 /usr/sbin/atd -b 60 -l 0.8



Reiniciar el equipo para que a partir de esos momentos lo tenga en cuenta cada vez que arranca:

```
# reboot
```

Tras reinicio verificar el estado del servicio:

```
# systemctl status atd.service
```

Instalación

Para instalar la protección de forma que se integre correctamente en el servidor de PCOP es necesario descargar el instalador desde la consola, tal y como se ha comentado en el apartado [Modos de instalación](#).

El nombre del instalador descargado es "LinuxWAAgent.run".

Después de descargar el instalador es necesario darle permiso de ejecución. Se puede hacer desde el explorador de archivos o ejecutando el comando;

```
# chmod +x LinuxWAAgent.run
```

A continuación se puede ejecutar el instalador. Para que funcione correctamente la instalación se debe hacer como root. Para hacerla se puede hacer doble click sobre el instalador desde el explorador de ficheros o se puede ejecutar desde un terminal el siguiente comando:



```
# ./LinuxWAAgent.run
```

El instalador descomprime los ficheros y a continuación ejecuta un shell script, `post_install.sh`, que se encarga de las tareas de post instalación, tales como: escribir ficheros de configuración, lanzar procesos etc...

Cuando termina la instalación deben estar en ejecución los siguientes procesos:

PCOP_AgentService

PCOPScheduler

Se puede comprobar el estado de los procesos ejecutando el comando:

```
# ps aux | grep PCOP
```

Despliegue

Cuando el producto se instala se crean en disco las siguientes carpetas y ficheros:

Carpeta del agente `/opt/PCOPAgent`

Carpeta de configuración `/etc/PCOPLinux`

Fichero `pcopagent` en la carpeta `/etc/init.d`

Procesos



Panda Cloud Office Protection

Como se ha comentado anteriormente, cuando la protección de Panda Cloud Office Protection está instalada en el equipo normalmente habrá en ejecución dos procesos, PCOP_AgentService y PCOPScheduler.

Estos procesos se ejecutan como daemon y se lanzan automáticamente cuando se inicia el sistema operativo.

Se ha comprobado que al enviar el mensaje de integración si la integración falla, ya sea porque el mensaje no se puede enviar o porque el servidor devuelve un error de integración, el proceso PCOP_AgentService se detiene y no se hacen nuevos reintentos de integración hasta que el proceso se inicie de nuevo.

Para detener de forma manual los procesos se puede ejecutar el comando

```
# /opt/PCOPAgent/Stop-PCOP-Agent
```

Para iniciar de nuevo los procesos se debe ejecutar el comando

```
# /etc/init.d/pcopagent start
```

Para su funcionamiento el producto deberá tener acceso a los siguientes dominios de Internet, tanto para comunicaciones HTTP como HTTPS.

mp-agents-inst.pandasecurity.com

mp-agents-sync.pandasecurity.com

mp-agents-async.pandasecurity.com



Estos dominios podrían cambiar en futuras versiones del producto.

Es importante que tenga presente los requisitos que los diferentes equipos deben reunir y las URLs a las que es necesario que tengan acceso. En el apartado [Requisitos y URLs necesarias](#) encontrará la información más actualizada al respecto.

Comunicación a través de proxy

Si la salida a Internet es a través de proxy es necesario configurar el producto para que utilice el proxy adecuado. Para ello se puede editar directamente el fichero proxy.conf indicando los datos del proxy en formato

```
proxy:port:user:password
```

Hay dos instancias de este fichero:

```
/opt/PCOPAgent/proxy.conf
```

Contiene la configuración utilizada por el agente para enviar los mensajes al servidor de PCOP.

```
/opt/PCOPAgent/Common/Binaries/PcopSigUpdater-bin/proxy.conf
```

Contiene la configuración utilizada por el proceso encargado de la actualización de ficheros de firmas.



También es posible establecer la configuración de forma más visual, ejecutando el script proxyConf.sh desde la carpeta /opt/PCOPAgent o desde la carpeta /opt/PCOPAgent/Common/Binaries/PcopSigUpdater-bin, en función del fichero de configuración de proxy que se quiera modificar.

En comunicaciones a través de proxy el único tipo de autenticación que se soporta es la autenticación básica.

Validación de usuario

Cuando el usuario no es válido o el equipo está en lista negra, Panda Cloud Office Protection no podrá operar normalmente, es decir, no se podrán enviar mensajes al servidor ni se actualizarán los ficheros de firmas.

En este caso únicamente se podrá validar de nuevo el usuario de forma periódica para recuperar el funcionamiento normal en caso de que el usuario vuelva a estar en estado válido de nuevo.

Actualización de ficheros de firmas

Para permitir la actualización de ficheros de firmas debe estar permitido el acceso a siguientes dominios:

<http://acs.pandasoftware.com>

<http://cloudav.downloads.pandasecurity.com>

<http://cloudav.updates.pandasecurity.com>

Estos dominios podrían cambiar en futuras versiones del producto. En el apartado [Requisitos y URLs necesarias](#) encontrará la información más actualizada al respecto.



Análisis

En consola, al igual que el agente de Windows, se pueden configurar análisis inmediatos, programados y periódicos para cada perfil, pero en el caso de Linux no está disponible aún el análisis de correo electrónico.

Análisis bajo demanda

En la configuración del perfil se pueden añadir análisis inmediatos, en los cuales se puede configurar el tipo de análisis que se soportan:

- De toda la máquina
- De los discos duros
- De otros elementos

Si selecciona "otros elementos" podrá añadir rutas a analizar, siguiendo la sintaxis de rutas de Linux.



Edit profile - New scan job

Profile: suse_server

Scan job details

Name:

Scan type:

Scan:

Path:

[Advanced settings](#)

Los análisis bajo demanda se lanzarán inmediatamente después de descargarse la configuración del mismo, que podría llegar a tardar un máximo por defecto de 4h.

Análisis programados

En la configuración del perfil se pueden añadir análisis programados, en los cuales se puede configurar el tipo de análisis que se soportan:

- De toda la máquina
- De los discos duros
- De otros elementos

Se puede configurar la fecha del análisis y la hora local de lanzamiento.

Si selecciona "otros elementos" podrá añadir rutas a analizar, siguiendo la sintaxis de



rutas de Linux.

Los análisis programados se lanzarán en el día y hora programada pero después de descargarse la configuración del mismo, que podría llegar a tardar un máximo por defecto de 4h.

Análisis periódicos

En la configuración del perfil se pueden añadir análisis periódicos, en los cuales se puede configurar el tipo de análisis que se soportan:

- De toda la máquina
- De los discos duros
- De otros elementos

Si selecciona "otros elementos" podrá añadir rutas a analizar, siguiendo la sintaxis de rutas de Linux.

Se puede configurar la fecha donde se quiere que comience la ejecución de estos análisis así como la hora local de lanzamiento. Además en este tipo de análisis se puede configurar la periodicidad del mismo:

- Diario
- Semanal
- Mensual

Los análisis periódicos se lanzarán en el día y hora programados, con la periodicidad programada, pero deberá previamente descargarse la configuración del mismo, que



podría llegar a tardar un máximo por defecto de 4h.

Lanzamiento manual de análisis

Es posible lanzar tareas de análisis de forma manual desde el equipo. Para ello se utilizará la protección PAVSL.

Para realizar un análisis y desinfección de ficheros, los parámetros que acepta el producto son los siguientes:

```
Pavsl.sh -cmp -heu -rpt [log] -noglk -prx [http(s)://user:password@maquina:puerto]  
[samples_path]
```

Donde:

Parámetro *cmp*: indica si se quiere entrar a recorrer o no ficheros comprimidos o empaquetados para analizar los elementos que contiene.

Parámetro *heu*: indica si se quiere realizar el análisis con tecnología heurística o no.

Parámetro *rpt*: indica el path donde se generará un fichero de log con los resultados del análisis.

Parámetro *noglk*: indica que se desea realizar el análisis sin consultar a la nube.

Parámetro *prx*: este parámetro va a ser la cadena de conexión necesario en caso de que exista un proxy para conectarse a internet. El formato debe ser el siguiente:

http://user:password@máquina:puerto

o

https://user:password@máquina:puerto



Parámetro *samples_path*: indica el path del fichero o directorio (y subdirectorios que contenga) que se quiere analizar. Para múltiples paths de análisis, estos deberán de estar entre comillas y separados por coma ("path","path"). En caso de paths con espacios en blanco deberán estar "escapados" al estilo de la Shell de Linux (\) y entre comillas (") tanto si es un análisis de un path simple o múltiple.

Algunos ejemplos de uso son:

```
pavsl.sh -cmp -heu -rpt /tmp/log /home/user/cebos
```

```
pavsl.sh -cmp -heu -rpt /tmp/log "/home/user/cebos"," /home/user/cebos2"
```

```
pavsl.sh -cmp -heu -rpt /tmp/log "/home/user/cebos \virus"
```

```
pavsl.sh -cmp -heu -rpt /tmp/log "/home/user/cebos \virus","/home/user/malware"
```

Si se desea que las detecciones realizadas por el análisis manual se envíen al servidor es necesario que el log se genere en la carpeta /opt/PCOPAgent/Common/DATA/ScansLogs y que el nombre del fichero es de la forma SCAN_XXXX.log, siendo XXXX un número de 4 dígitos.

Por ejemplo:

```
pavsl.sh -cmp -heu -rpt /opt/PCOPAgent/Common/DATA/ScansLogs/SCAN_2000.log  
/home/user/cebos
```

Informes de detección

La función de este proceso es la de recoger de las protecciones la información sobre las detecciones realizadas.



Panda Cloud Office Protection

Panda Cloud Office Protection

c_m400 | Log out

Users Preferences Language: English

STATUS COMPUTERS INSTALLATION AND SETTINGS QUARANTINE REPORTS OTHER SERVICES

HELP

> Status > List of detections

List of detections

<<Back

Find computer: Find Show all Options

Export to:

Page 1 of 7 1-20 of 125 items Items per page 20 View

	Computer	Group	Name	Type	Instances	Action	Date
[+]	OPENSUSE64ESP8	suse_workstation	Panda.SpywareB.TestFile	Spyware	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.HackingTool.Test...	Hacking Tool	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.VirusND.TestFile	Virus	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.Adware.TestFile	Adware	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Generic.Malware	Dialer	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.Virus.TestFile	Virus	1	Disinfected	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Generic.Malware	Trojan	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.SecurityR.TestFile	Security Risk	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.SpywareNB.TestFile	Spyware	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.Joke.TestFile	Joke	1	Deleted	3/26/2013 1:17:59 PM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.SpywareB.TestFile	Spyware	1	Deleted	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.HackingTool.Test...	Hacking Tool	1	Deleted	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.VirusND.TestFile	Virus	1	Deleted	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.Adware.TestFile	Adware	1	Deleted	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Generic.Malware	Dialer	1	Deleted	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.Virus.TestFile	Virus	1	Disinfected	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Generic.Malware	Trojan	1	Deleted	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.SecurityR.TestFile	Security Risk	1	Deleted	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.SpywareNB.TestFile	Spyware	1	Deleted	3/26/2013 9:20:03 AM
[+]	OPENSUSE64ESP8	suse_workstation	Panda.Inks.TestFile	Inks	1	Deleted	3/26/2013 9:20:03 AM

Por defecto, los mensajes de reporte, si hay detecciones, se envían cada 6h y se pueden ver en consola cliente, en la ventana **Estado** → **Lista de detecciones**, al igual que sucede con el sistema operativo Windows.

Actualizar a versión superior de Panda Cloud Office Protection (Upgrades)

Panda Cloud Office Protection no dispone de una funcionalidad de actualización de versión automática.



Si desea actualizar la versión de Panda Cloud Office Protection es necesario acceder a la consola para descargar la nueva versión y ejecutar el instalador de forma manual en el equipo.

No es necesario desinstalar previamente Panda Cloud Office Protection, ya que el instalador es capaz de actualizar a partir de una versión anterior.

Desinstalación

Panda Cloud Office Protection no dispone de un script de desinstalación por lo que para eliminarlo del sistema es necesario realizar de forma manual las siguientes acciones:

1. Parar los procesos.

Para ello ejecutar el comando:

```
/opt/PCOPAgent/Stop-PCOP-Agent
```

2. Eliminar la carpeta /opt/PCOPAgent y su contenido.
3. Eliminar la carpeta /etc/PCOPLinux y su contenido.
4. Eliminar el servicio. La forma de hacer esta tarea depende de la distribución:

SUSE

```
chkconfig --del pcpagent
```



Debian / Ubuntu

`update-rc.d -f pcopagent remove`

5. Eliminar el fichero `/etc/init.d/pcopagent`.