gestión de **dispositivos en la nube**

GUÍA DE ADMINISTRACIÓN

panda

euskaltel

Contenidos

1. Prólogo

¿A quién va dirigida esta guía?

Iconos

1.1. Introducción

Esta guía contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto **Panda Systems Management**.

1.2. ¿A quién está dirigida esta guía?

El objetivo de esta guía es procurar información técnica sobre el producto al personal miembro del departamento de IT encargado que ofrecer servicios de soporte a los equipos y dispositivos en las empresas, y lo hace desde dos posibles entornos:

- Desde el departamento de IT de la empresa que desea profesionalizar el soporte técnico interno que ofrece al resto de la compañía.
- Desde el proveedor de servicios gestionados (MSP) que actualmente ofrece soporte técnico presencial o remoto, reactivo o proactivo, a sus cuentas de clientes.

1.3. Iconos

Aclaraciones e información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.

Sugerencias y recomendaciones.

Consejo importante de cara a un uso correcto de las opciones de **Panda Systems Management.**

Consulta en otro capítulo o punto del manual.

2. Introducción

Características principales

Perfil de usuario

Componentes principales

Principales actores

2.1. Introducción

Panda Systems Management es una solución **basada en la Nube** que **monitoriza y administra remotamente** dispositivos, destinada a departamentos de IT que quieren ofrecer un servicio profesional y minimizar su impacto en las tareas del usuario. **Panda Systems Management** incrementa la eficiencia a través de una gestión de dispositivos centralizada y sencilla, favoreciendo a su vez la automatización de tareas. De esta forma, los costes generales invertidos en dar servicio a cada cliente se ven reducidos ya que **Panda Systems Management**:

- Es un servicio alojado en la nube, por lo que requiere nula infraestructura adicional en las instalaciones del partner y en la cuenta del cliente.
- Tiene una curva de aprendizaje muy suave para los técnicos de soporte, por lo que su valor es apreciable desde el primer momento.
- Es una herramienta accesible desde cualquier lugar y en cualquier momento, lo que facilita las guardias no presenciales del equipo técnico y evita desplazamientos, gracias al control remoto de dispositivos.
- Permite la automatización de tareas que se lanzan de forma automática como respuesta a alertas programadas, previniendo los fallos antes de que se produzcan.

Panda Systems Management favorece la colaboración entre los técnicos encargados de ofrecer soporte y minimiza o evita completamente el tiempo dedicado a interactuar con el usuario para determinar las causas de los problemas.

2.2. Características principales de Panda Systems Management.

Las características principales de Panda Systems Management son:

Característica	Descripción
Solución basada íntegramente en la Nube	No precisa infraestructura adicional en el cliente o en el MSP / departamento de IT. Permite gestionar todos los dispositivos en cualquier momento y desde cualquier lugar.
Gestión mediante agente para dispositivos compatibles	Agente extremadamente ligero para dispositivos compatibles con Windows, Linux, macOS, Android e iOS.
Gestión sin agente	Gestión simple con ayuda del protocolo SNMP y plantillas de configuración, para aquellos dispositivos donde no sea posible la instalación del agente (impresoras, routers, switches, scanners, centralitas, etc). Gestión de servidores VMware ESXi (VMware vSphere Hypervisor 4.1, 5.0, 5.5 y 6.0), Gestión de servidores Microsoft Hyper-V en Window Server.
Detección automática de dispositivos	El agente instalado en un solo dispositivo puede detectar otros equipos conectados a la misma red e iniciar su instalación desatendida.

Característica	Descripción
Auditorías programadas y extraordinarias	Seguimiento de todos los cambios implementados en el dispositivo (hardware, software y sistema).
Gestión de licencias de software	Seguimiento de las licencias de software utilizadas.
Alertas y monitorización	Controla del uso de CPU, memoria y disco, servicios, colas, gráficos de rendimiento, alertas en panel, etc. Aplicable a cualquier dispositivo y en tiempo real. Monitores recomendados de rápida configuración.
Monitorización de las aplicaciones más comunes	Monitoriza las aplicaciones más comunes, como Exchange, SQL y IIS, los servicios de Backup, dispositivos de red, etc., gracias a los monitores disponibles gratuitamente en la **ComStore** del producto.
Creación de scripts y tareas rápidas	Crea o descargar scripts previamente configurados de la **ComStore** en línea y lánzalos de forma programada, o como respuesta automática a una alerta. Todo ello con un solo clic.
Gestión de parches	Automatiza el despliegue de actualizaciones y parches para el software instalado.
Despliegue de software	Despliega de forma centralizada el software en equipos Windows, Linux, Mac e iOs de la red.
Políticas	Establece configuraciones comunes en los dispositivos gestionados. Accede a políticas recomendadas para acelerar la gestión del entorno IT.
Acceso remoto	Gestor de tareas, transferencia de archivos, editor del registro, línea de comandos, visualizador de eventos del sistema, etc. Todas estas herramientas integradas permiten solucionar los problemas sin que el proceso de resolución impacte en el trabajo de los usuarios.
Control remoto	Acceso compartido al escritorio del usuario o control total. Compatible con cortafuegos y Network Address Translation (NAT).
Gestión remota de dispositivos de red	Accede a las herramientas de administración incorporadas en los dispositivos de red, impresoras y otros equipos que no admiten la instalación del agente PCSM. De esta manera el administrador puede gestionar desde su puesto todos los dispositivos de la red.
Comunicación segura	Todas las comunicaciones entre los agentes y el **Servidor Systems Management** están cifradas (SSL).
Control de acceso al servicio	Máxima seguridad en el inicio de sesión a la **Consola** de administración, mediante la autenticación en dos fases y otros recursos que limitan el acceso de los dispositivos al Servidor **Systems Management.**
Informes	Envío por correo de informes programados o extraordinarios. Facilita detalles sobre las tareas ejecutadas y quién las lanza, además de datos sobre el uso de los recursos realizado por los usuarios.
Entorno colaborativo	Sistema de tickets que gestiona la asignación, el estado y la documentación de las incidencias. Facilita la creación de históricos de intervención con notas asociadas a los dispositivos y mejora la comunicación en vivo con el usuario mediante el servicio de mensajería.

Característica	Descripción
Registro de actividad	Almacena toda la actividad de los administradores en la Consola.
ComStore	Amplía las capacidades de la plataforma, al seleccionar y descargar los componentes necesarios en cada momento. Todos los complementos se ofrecen de forma gratuita.
Gestión de dispositivos móviles (MDM)	Compatible con iOS y Android, permite monitorizar y gestionar móviles y tablets, establecer configuraciones y políticas de uso, geolocalizar los dispositivos y evitar la pérdida de datos en caso de robo del terminal.

Tabla 1: listado de características de Panda Systems Management

2.3. Perfil de usuario de Panda Systems Management.

Los usuarios de **Panda Systems Management** son profesionales con un perfil técnico medio-alto, ya que se trata de una herramienta orientada al mantenimiento diario de dispositivos informáticos sometidos a un régimen constante de uso y cambio de configuración. Sin embargo, en **Panda Systems Management** se distinguen dos grandes grupos de usuarios:

- **Técnicos pertenecientes al departamento de IT de la empresa**

Son técnicos subcontratados o pertenecientes a la plantilla de la empresa, que ofrecen un servicio de soporte a los dispositivos y usuarios de la propia compañía. Este escenario contempla la existencia de una estructura distribuida de oficinas, a las cuales los técnicos deberán acceder con herramientas de monitorización y acceso remoto, así como usuarios desplazados o que desarrollan su labor fuera de la oficina y son susceptibles de sufrir problemas en sus dispositivos.

- **Técnicos pertenecientes a un proveedor de servicios gestionados (MSP)**

Se trata de personal técnico perteneciente a empresas que ofrecen un servicio profesional a clientes que han decidido externalizar o subcontratar el departamento de IT.

2.4. Componentes principales de Panda Systems Management.

- **Consola de administración**

Se trata de un portal Web accesible a través de un navegador compatible, desde cualquier lugar y en cualquier momento, con una simple conexión a Internet.

La mayor parte de las actividades diarias de seguimiento y monitorización se realizarán desde este portal Web y a través del navegador.

Es un recurso accesible únicamente por los técnicos encargados de ofrecer soporte.

- **Agente**

Es un pequeño programa de 6'5 megabytes de tamaño en su versión Windows, que se instala en cada uno de los dispositivos compatibles a administrar. Una vez desplegado el agente, el técnico de soporte podrá acceder a través de la Consola.

En el caso de que no sea posible la instalación del agente en el dispositivo (impresoras, switches, servidores ESXi etc), Panda Systems Management permite recoger datos de estado y mostrarlos en la consola con ayuda del protocolo SNMP. Para más información, consulta la sección Administración de dispositivos no compatibles con el Agente del Capítulo 5: Dispositivos.

El agente admite dos modos de ejecución:

- **Modo usuario / monitor**: es la forma de ejecución normal del agente PCSM y está diseñada para pasar inadvertida al usuario del dispositivo durante la mayor parte del tiempo.
- **Modo administrador**: el agente PCSM también es utilizado por el administrador para acceder a los dispositivos de la red, previa introducción de unas credenciales válidas.

Instala el agente en todos los dispositivos que deseas administrar y también en aquéllos que utilizarán los técnicos para la administración los recursos de la infraestructura IT.

- **Servidor**

El servicio de la consola y todos los procesos que recogen, sincronizan y redirigen los mensajes y los flujos de información generados por los agentes, junto a la base de datos que los almacenan, residen en una granja de servidores alojados en la Nube, online las 24 horas del día.

La información de estado que fluye desde cada uno de los dispositivos administrados hacia el servidor **Systems Management** está muy optimizada, de forma que el impacto en la red del cliente y la latencia son inapreciables. Esta información se ordena y consolida en el servidor para mostrarse como un flujo de eventos que permitirá diagnosticar e incluso anticipar eficazmente los problemas de los dispositivos administrados.

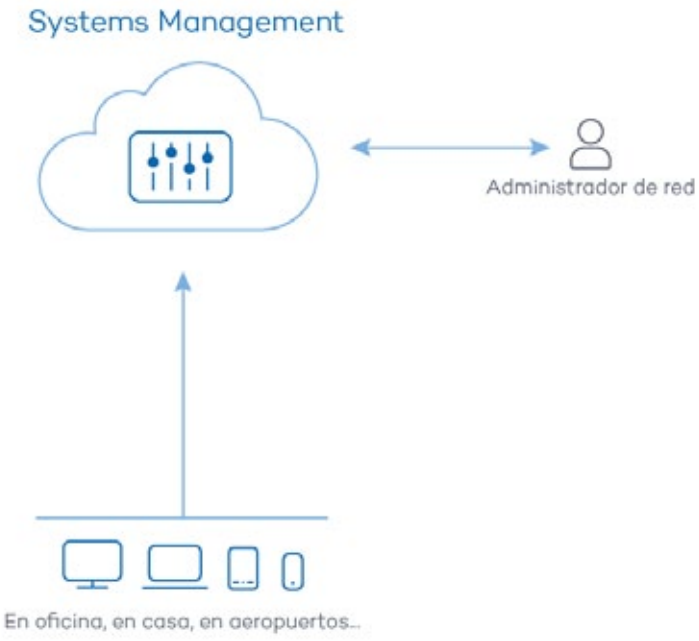


Figura 1: esquema básico de funcionamiento Panda Systems Management

2.5. Principales actores de Panda Systems Management.

- **Administrador de IT / Administrador / Proveedor de servicios gestionados / MSP / Departamento de IT /Técnico de soporte / Equipo técnico**

Son las personas que tienen acceso a la consola de **Panda Systems Management**, independientemente del nivel de privilegios asociado a las credenciales suministradas.

Se trata de personal técnico perteneciente al departamento IT de la empresa que adopta **Panda Systems Management** para administrar sus propios equipos, o personal del MSP que accede a los dispositivos de clientes para su administración y monitorización.

- **Cuenta de administración Panda Systems Management / Cuenta de administración principal**

A cada empresa que adquiera el producto **Panda Systems Management** se le entregará una cuenta de administración principal con los máximos privilegios, capaz de gestionar todos los recursos del producto.

Consulta el Capítulo 16: Cuentas de usuario y roles para crear nuevos usuarios y roles que delimiten el acceso de los técnicos de sistemas a recursos clave de Panda Systems Management.

Consulta el Capítulo 20: Seguridad y control de acceso al servicio Panda Systems Management para configurar la autenticación de dos fases.

Cada cuenta de administración principal pertenece a una instancia del producto estanca e independiente. Así, todas las configuraciones de un cliente de **Panda Systems Management** y todos los dispositivos administrados por éste, no serán accesibles ni visibles por otras cuentas de administración.

- **Cuenta de cliente / Cliente**

Es un contrato firmado entre el proveedor de servicios gestionados y una empresa que acude a él con la intención de externalizar el mantenimiento de la infraestructura informática.

- **Usuario**

Persona que utiliza uno o más dispositivos y requiere soporte técnico directo del MSP o departamento de IT.

- **Dispositivo**

Equipo informático con rol de cliente o servidor, que lleva instalado un agente o es gestionado de forma indirecta con ayuda del protocolo SNMP.

3. Jerarquía de niveles en la consola

3.1. Jerarquía de niveles para la consola de administración

Panda Systems Management separa la administración de los dispositivos en tres entidades / niveles de agrupación, para reutilizar y limitar procedimientos establecidos por el personal técnico en la consola y así agilizar y afinar su administración. Del nivel más general al más particular son las siguientes:

- Nivel Cuenta.
- Nivel Zona.
- Nivel Dispositivo.

Figura 2: jerarquía de niveles

3.2. Nivel Cuenta

¿Qué es?

El Nivel Cuenta es la entidad de agrupación más general, **siendo además única por cada MSP / departamento de IT**. Reúne automáticamente todos los dispositivos administrados por el MSP / departamento de IT pertenecientes a sus clientes y usuarios, y que estén ya integrados en **Panda Systems Management**.

Ámbito

Las acciones en este nivel afectan a todos los dispositivos integrados en el sistema, aunque el ámbito podrá ser limitado a un subconjunto de los equipos mediante filtros y grupos descritos en el Capítulo 6: Filtros y grupos.

Acceso

Haz clic en el menú general **Cuenta** para acceder a los recursos de la entidad.

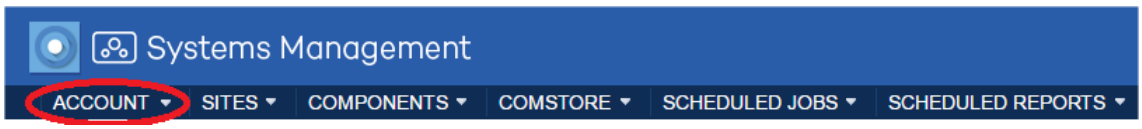


Figura 3: acceso al menú general Cuenta

Funcionalidad

El Nivel Cuenta tiene la capacidad de ejecutar acciones de forma global. Así, es posible obtener listados con el estado de todos los dispositivos administrados, informes consolidados relativos al sistema y acciones sobre todos o parte de los dispositivos registrados.

Configuración

La configuración del Nivel Cuenta aglutina una serie de parámetros muy heterogéneos que se tratan en varios capítulos a lo largo de esta guía. A continuación, se indica una lista completa de todas las opciones incluidas en el menú general **Ajustes, Configuración de cuenta** y una breve reseña de cada una.

Parámetro	Descripción
Política de contraseñas	Establece políticas de contraseñas. Para más información, consulta el Capítulo 20: Seguridad y control de acceso al servicio **Panda Systems Management**.
Control de acceso	Establece controles de acceso avanzados a la consola y al servicio. Para más información, consulta el Capítulo 20: Seguridad y control de acceso al servicio **Panda Systems Management**.
Potencia nominal	Establece el consumo en vatios de cada tipo de dispositivo para poder calcular su coste mensual. Para más información, consulta el Capítulo 5: Dispositivos.
Recurso asignado a los tickets de usuario final	Indica la cuenta a la que los usuarios envían los tickets que se abren directamente desde el agente. Para más información, consulta el Capítulo 14: Ticketing.
Variables	Variables que se pasan a los scripts ejecutados en los dispositivos. Para más información, consulta el Capítulo 11: Componentes y la ComStore.
Campos personalizados	Redefine el nombre de las etiquetas utilizadas para mostrar el resultado de los scripts ejecutados en los dispositivos. Para más información, consulta el Capítulo 11: Componentes y la ComStore.
Configuración personalizada de agente	Define el comportamiento de los agentes instalados relativo al rol de "agente de conexión". Para más información, consulta el Capítulo 5: Dispositivos.
Credenciales de despliegue de agentes	Establece las credenciales para la instalación remota del agente. Para más información, consulta el Capítulo 5: Dispositivos.
Credenciales SNMP	Establece los parámetros de conexión por defecto del protocolo SNMP aplicables a los dispositivos de la red a gestionar, y que no son compatibles con el agente de **Panda Systems Management.**
Credenciales ESXi	Establece los parámetros de conexión por defecto para gestionar servidores ESXi.
Configuración de las actualizaciones de agentes	Impide o permite la actualización automática de los agentes ya instalados.

Parámetro	Descripción
Configuración de correo	Configura la cuenta origen y la respuesta para los mails enviados por el servidor **Panda Systems Management** a los administradores del servicio.
Destinatarios de correo	Configura las cuentas de correo que recibirán alertas, informes, resúmenes con los nuevos componentes añadidos a la ComStore o actualizaciones y avisos de nuevos dispositivos administrados en la cuenta por **Panda Systems Management.**
Actualizar variables de Zona	Variables que se pasan a los scripts ejecutados en los dispositivos.
Certificado push de Apple	Configuración del certificado necesario para administrar dispositivos móviles Apple. Para más información, consulta el Capítulo 17: Gestión de dispositivos móviles.
Restablecer presentación columnas	Restaura la configuración inicial para mostrar los datos básicos de los dispositivos administrados. Para más información, consulta el Capítulo 5: Dispositivos.

Tabla 2: configuración del nivel Cuenta

3.3. Nivel Zona

¿Qué es?

El Nivel Zona es la entidad de agrupación inmediatamente inferior al Nivel Cuenta y está formada por grupos que contienen dispositivos pertenecientes a una misma delegación / oficina / red. De esta manera, una empresa que tenga varios centros de trabajo o redes independientes generalmente establecerá una zona por cada una de ellas. Cada uno de estas zonas agruparán dispositivos con una configuración de conectividad específica.

La lista de zonas es accesible desde el menú general **Zonas**.

Cada zona lleva integrada la configuración de conexión a Internet de los dispositivos que la forman, accesible desde la barra de pestañas **Configuración** en la consola. Las configuraciones son añadidas al Agente **Systems Management** que el usuario del dispositivo instalará en su equipo, aplicándose de forma automática y sin intervención del administrador.

Ámbito

Los procedimientos ejecutados en el Nivel Zona afectan a todos los dispositivos que pertenecen a la agrupación, si bien algunas acciones podrán ser limitadas a un subconjunto de equipos mediante filtros y grupos, descritos en el Capítulo 6: Filtros y grupos.

A diferencia del Nivel Cuenta, que es único, el administrador podrá crear tantas agrupaciones de tipo zona como considere oportuno.

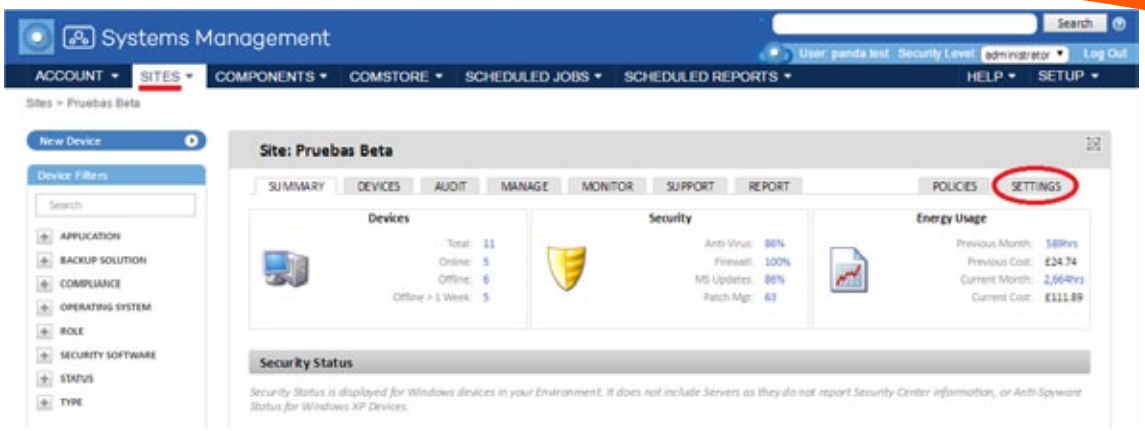


Figura 4: acceso al menú general Zonas, Configuración

Pertenencia

La pertenencia de un dispositivo administrado a una zona u otra, queda determinada por la instalación del agente, aunque desde la consola es posible mover equipos entre zonas, una vez instalado el agente en el dispositivo del usuario.

> ***Descarga el agente directamente desde la página de la zona elegida de forma que, al instalarse en el dispositivo del usuario, éste se agregará de automáticamente a la zona en cuestión en la consola. Para más información, consulta el Capítulo 5: Dispositivos.***

> ***Para minimizar las tareas en la fase de distribución, se recomienda primero crear una zona en la consola de administración y después descargar el agente desde ésta, de forma que la pertenencia de los dispositivos gestionados a la zona creada sea automática.***

Funcionalidad

El Nivel Zona ejecuta acciones sobre todos los dispositivos que la forman.

Configuración

La configuración del Nivel Zona aglutina una serie de parámetros muy heterogéneos que se tratan en varios capítulos a lo largo de esta guía.

> ***Los parámetros definidos en el nivel Zona tienen prioridad sobre los definidos en el nivel Cuenta.***

Para acceder a la configuración de una zona, en el menú general **Zonas** elige la zona indicada y haz clic en la pestaña **Configuración**,

A continuación, se incluye una lista completa con todas las opciones y una reseña indicando si son tratados en capítulos posteriores

Parámetro	Descripción
General	Información general de la zona: **Nombre**, identificador interno (**UID**), **Descripción** y **Tipo** de dispositivos albergados en la zona.
Potencia nominal	Establece el consumo en vatios de cada tipo de dispositivo para poder calcular el coste mensual. Para más información, consulta el Capítulo 5: Dispositivos.
Proxy	Establece la configuración de proxy para las redes de usuarios que no tengan conexión directa con Internet. Para más información, consulta el Capítulo 5: Dispositivos.
Configuración de agente personalizada	Define el comportamiento de los agentes instalados relativos al rol de "agente de conexiones". Para más información, consulta el Capítulo 5: Dispositivos.
Subredes adicionales para el descubrimiento de subredes	Los agentes con el rol de nodo de red asignado ejecutan barridos de la red a la que pertenecen por defecto, en busca de dispositivos sin administrar. Añade aquí las subredes adicionales que serán exploradas.
Credenciales de despliegue del agente	Establece las credenciales para la instalación remota del agente. Para más información, consulta el Capítulo 5: Dispositivos.
Credenciales SNMP	Establece los parámetros de conexión por defecto del protocolo SNMP aplicables a los dispositivos de la red a gestionar, y que no compatibles con el agente **Systems Management.**
Credenciales ESXi	Establece los parámetros de conexión por defecto para gestionar servidores ESXi.
Destinatarios de correo	Configura las cuentas de correo que recibirán alertas, informes y avisos de nuevos dispositivos en la zona administrados por **Panda Systems Management.**
Cachés locales	Asigna el rol de caché a un dispositivo. Así, se ahorrará ancho de banda en los despliegues de software. Para más información, consulta el Capítulo 13: Distribución e instalación centralizada de software.
Recurso asignado a los tickets de usuario final	Indica la cuenta a la que los usuarios envían los tickets abiertos directamente desde el agente. Para más información, consulta el Capítulo 14: Ticketing.
Variables	Variables que se pasan a los scripts ejecutados en los dispositivos. Para más información, consulta el Capítulo 11: Componentes y la ComStore.
Credenciales	Establece las credenciales para ejecutar el despliegue de software. Para más información, consulta el Capítulo 13: Distribución e instalación centralizada de software.

Parámetro	Descripción
Campos personalizados	Redefine el nombre de las etiquetas utilizadas para mostrar el resultado de los scripts ejecutados en los dispositivos. Para más información, consulta el Capítulo 11: Componentes y la ComStore.

Tabla 3: configuración del Nivel Zona

3.4. Nivel Dispositivo

¿Qué es?

Es la representación lógica en la consola para un único dispositivo gestionado. Los Niveles Dispositivo se crean automáticamente, ya que se añade uno por cada equipo del cliente con un agente instalado, o gestionado de forma indirecta con ayuda del protocolo SNMP.

Ámbito

Todas las acciones ejecutadas en este nivel afectan únicamente al dispositivo seleccionado.

Funcionalidad

El Nivel Dispositivo tiene la capacidad de ejecutar acciones sobre un equipo particular.

4. Elementos básicos de la consola

Menú general

Barra de pestañas / Barra de listados

Barra de iconos / Barra de acciones

Panel de grupos y filtros

Paneles de control

4.1. Instalación

La consola de administración está estructurada de forma intuitiva y visual para que la mayor parte de los recursos queden a un clic de distancia, minimizando el tiempo de navegación.

El objetivo es disponer de una herramienta visualmente limpia, rápida de utilizar y cómoda, que evite en lo posible las recargas de página completas y que ofrezca una curva de aprendizaje muy poco pronunciada y corta para el departamento de IT; Así, partners y administradores podrán entregar valor a sus clientes desde el primer momento.

Los elementos básicos de la consola a los que se hace referencia a lo largo de esta guía son:

4.2. Menú general

Es el menú accesible desde cualquier punto de la consola. Consta de ocho entradas:

Figura 5: menú general

Elementos

Menú	Descripción
Cuenta	Acceso al Nivel Cuenta.
Zonas	Acceso al Nivel Zonas.
Componentes	Acceso a los componentes descargados disponibles para el administrador.
ComStore	Repositorio de componentes creados por **Panda Security** que extienden la funcionalidad de **Panda Systems Management.**
Tareas programadas	Listado de tareas activas y terminadas.
Informes programados	Listado de informes configurados y ya generados.
Centro de ayuda	Centro de ayuda con enlaces a recursos de **Panda Security**
Ajustes	Acceso a los datos de la Cuenta de administración principal, así como a los recursos para crear nuevos roles y usuarios. Para más información, consulta el Capítulo 16: Cuentas de usuario y roles.

Tabla 4: entradas del menú general

4.3. Barra de pestañas / Barra de listados

La barra de pestañas, también llamada barra de listados, permite el acceso a las herramientas de la consola que generan listados consolidados en pantalla, con información del estado de los dispositivos que pertenecen al nivel accedido. La barra de pestañas también permite acceder a herramientas para crear y visualizar configuraciones.

Este recurso varía ligeramente en función del nivel desde el que se accede a ella (Nivel Zona, Nivel Cuenta o Nivel Dispositivo para un dispositivo concreto) ofreciendo por tanto un ámbito de administración distinto.

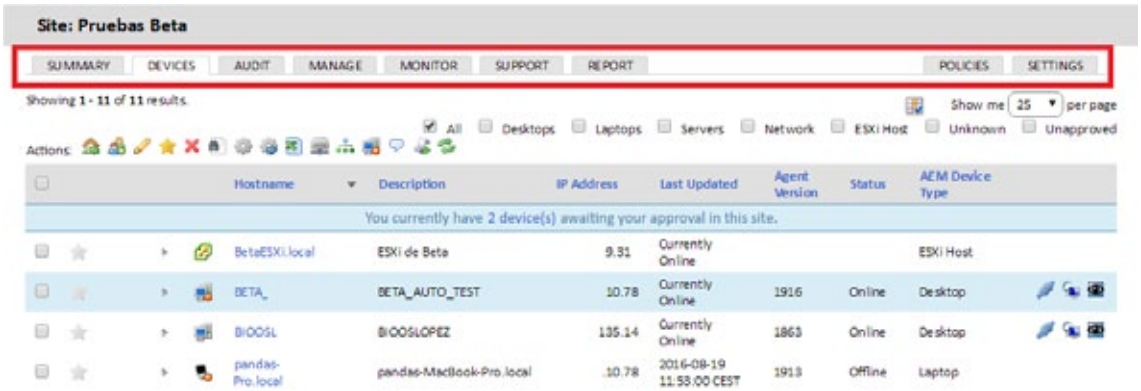


Figura 6: barra de pestañas / listados

4.3.1 Elementos

Pestaña	Accesible desde (Nivel)	Descripción
Resumen	Zona, Dispositivo	Información de estado.
Panel de control	Cuenta	Panel de control general.
Dispositivos	Zona	Listado de dispositivos accesibles con información asociada.
Auditoría	Cuenta, Zona, Dispositivo	Listado del inventariado del hardware, software y licencias.
Administrar	Cuenta, Zona, Dispositivo	Listado de parches aplicados y pendientes de instalar, software en los dispositivos y listados con los dispositivos descubiertos en la red y gestionados por **Panda Systems Management**.
Supervisar	Cuenta, Zona, Dispositivo	Listado de alertas generadas por monitores o tareas terminadas.
Soporte	Cuenta, Zona, Dispositivo	Listado de tickets generados
Informe	Cuenta, Zona, Dispositivo	Listado y generación bajo demanda de Informes.

Pestaña	Accesible desde (Nivel)	Descripción
Políticas	Cuenta, Zona, Dispositivo	Listado y generación de políticas, explicadas en el Capítulo 8: Políticas.
Configuración	Zona	Configuración asociada a la zona.
Dispositivos eliminados	Cuenta	Listado de dispositivos desinstalados.

Tabla 5: entradas de la barra de pestañas / listados

El ámbito de la barra de pestañas se refiere al nivel en curso. De este modo, si accedes a la barra de pestañas en el Nivel Cuenta se matrará la información consolidada de todos los dispositivos; si accedes en el Nivel Zona se mostrará información consolidada de los dispositivos que participan de la zona; si accedes en el Nivel Dispositivo, solo se mostrará información de ese dispositivo en particular.

4.4. Barra de iconos / Barra de acciones

La barra de iconos o barra de acciones permite el acceso a acciones que modifican el estado de los dispositivos**.** Esta barra no existe en el menú general **Cuenta** de forma directa y varía ligeramente si se accede a ella desde el menú general **Zonas** o desde un dispositivo particular, ya que se adapta al ámbito de administración.

Su ámbito de acción será el formado por la selección manual de dispositivos marcados dentro de una zona.

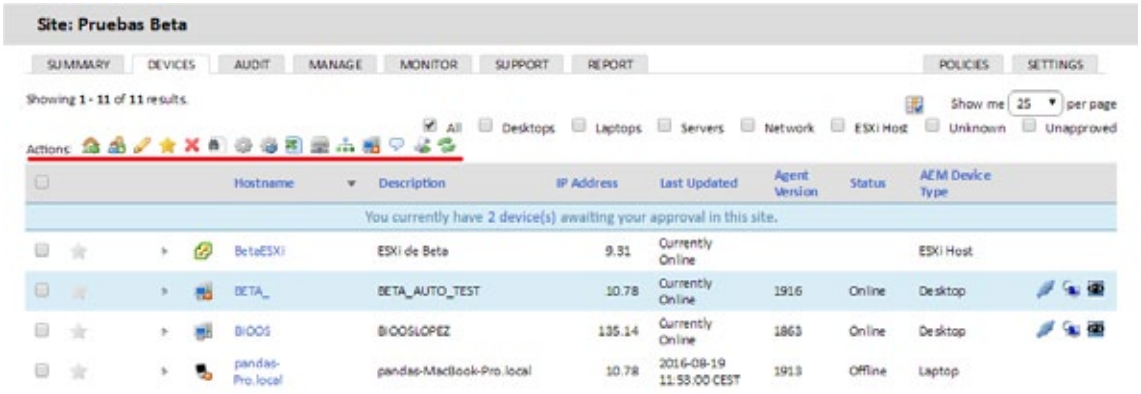


Figura 7: barra de iconos

4.4.1 Elementos

Icono	Accesible desde (Nivel)	Descripción
Mover dispositivo(s) a una zona diferente	Zona, Dispositivo	Mueve los dispositivos seleccionados a otra zona.

Icono	Accesible desde (Nivel)	Descripción
Añadir dispositivo(s) a un grupo	Zona, Dispositivo	Añade el o los dispositivos seleccionados a un grupo.
Editar descripción de dispositivos seleccionados	Zona	Añade notas y campos personalizados a los dispositivos seleccionados que podrán ser utilizados por los filtros.
Activar dispositivo(s) como favoritos	Zona	Marca como favoritos dispositivos para su acceso rápido desde **Resumen / Dashboard**.
Eliminar dispositivo(s)	Zona, Dispositivo	Borra un dispositivo de una zona. El agente se desinstalará y el equipo dejará de ser administrado y se añadirá a la pestaña **Dispositivos eliminados** del menú general Cuenta.
Solicitar auditoria de dispositivo(s)	Zona, Dispositivo	Fuerza el lanzamiento de una auditoria. Para más información, consulta el capítulo 12: Auditoria de activos.
Programar una tarea	Zona, Dispositivo	Crea tareas programadas para una fecha posterior. Para más información, consulta el capítulo 11: Componentes y la ComStore.
Ejecutar una tarea rápida	Zona, Dispositivo	Ejecuta en el momento una tarea ya creada. Para más información, consulta el capítulo 11: Componentes y la ComStore.
Descargar CSV	Zona	Descarga del listado de dispositivos de la zona.
Añadir/eliminar como caché local	Zona, Dispositivo	Marca al dispositivo como caché para acelerar la descarga e instalación de componentes y la distribución de software en los equipos de la red.
Network node settings	Zona, Dispositivo	Marca al dispositivo como nodo de red para facilitar los despliegues de **Panda Systems Management** y la comunicación con el servidor.
Activar privacidad	Zona, Dispositivo	Impide el acceso remoto por parte del administrador a los dispositivos si no es con la aprobación manual del usuario.
Enviar un mensaje a los dispositivos seleccionados	Zona, Dispositivo	Envía un mensaje a los dispositivos seleccionados.
Programar informes seleccionados	Zona	Programa un informe para una fecha posterior.
Mostrar dispositivo(s) en el mapa de Google	Dispositivo	Geolocaliza los dispositivos en el mapa.
Código QR	Dispositivo	Código QR asociado al dispositivo para su inventariado en papel.

Icono	Accesible desde (Nivel)	Descripción
Actualizar la vista actual	Zona, Dispositivo	Vuelve a cargar el listado de dispositivos mostrad o el dispositivo particular.

Tabla 6: entradas de la barra de iconos

> ***Para ejecutar acciones sobre dispositivos en el Nivel Cuenta, crea un filtro de cuenta o grupo de zona con los equipos seleccionados. El Nivel Cuenta no muestra la barra de iconos a no ser que se seleccionen dispositivos a través de un filtro o un grupo.***

4.5. Panel de grupos y filtros

En la parte izquierda de la consola se encuentran varios paneles con grupos de diversos tipos:

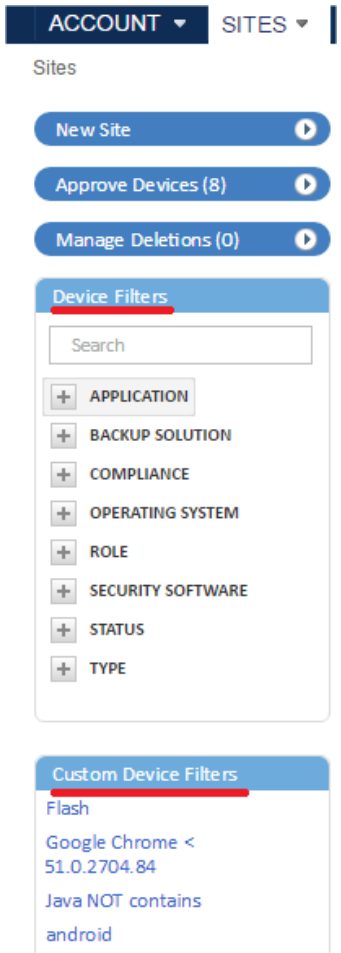


Figura 8: panel lateral con las herramientas de agrupación y filtrado

- **Filtro de dispositivos**: Filtros pre configurados para facilitar la localización de los dispositivos.
- **Filtros de zona / Filtros de cuenta**: Filtros de dispositivos creados por el administrador en el Nivel Zona o Nivel Cuenta respectivamente.
- **Grupo de dispositivos de zona / Grupos de dispositivos**: Grupos de dispositivos creados por el administrador en el Nivel Zona o Nivel Cuenta respectivamente.
- **Grupos de zonas**: disponibles únicamente en el Nivel Cuenta, son agrupaciones de varias zonas.

4.6. Paneles de control

Los paneles de control (Dashboards) reflejan el estado de un conjunto de dispositivos. Existen cuatro tipos.

4.6.1 Estado de la seguridad

Accesible desde el menú general **Cuenta,** refleja el estado de la seguridad de todos los dispositivos gestionados.

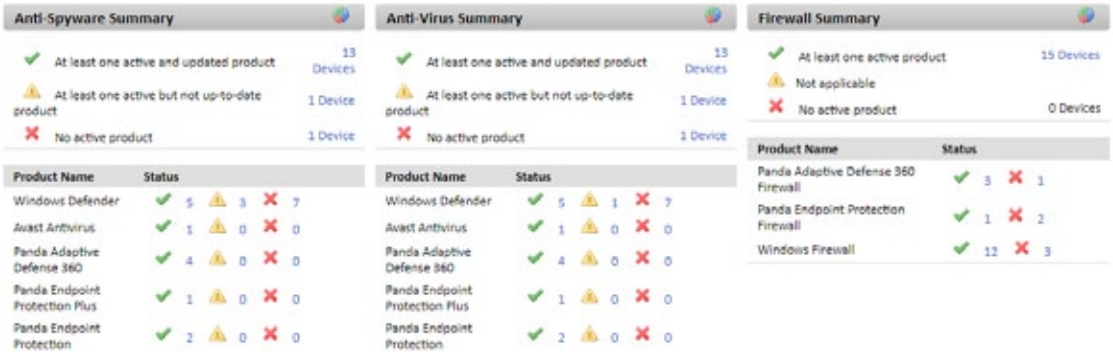


Figura 9: panel de control de seguridad

4.6.2 Panel de control del Nivel Cuenta

Desde el menú general **Cuenta** haz clic en el menú de pestañas **Panal de control** y en **Panel de control de cuenta**.

Reúne información general del estado del parque de dispositivos: notificaciones, tareas, alertas, etc.

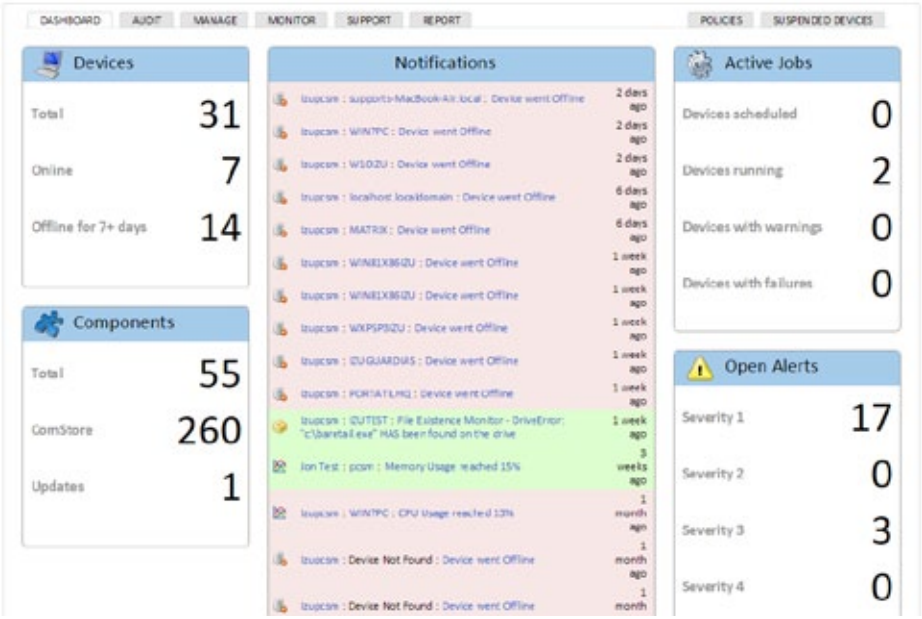


Figura 10: panel de control del Nivel Cuenta

4.6.3 Resumen (Zona)

Desde el menú general **Zonas,** selecciona una zona y haz clic en el menú de pestañas **Resumen**. Refleja el estado de todos los dispositivos que pertenecen a la agrupación. Habrá un panel de control resumen por cada una de ellas.

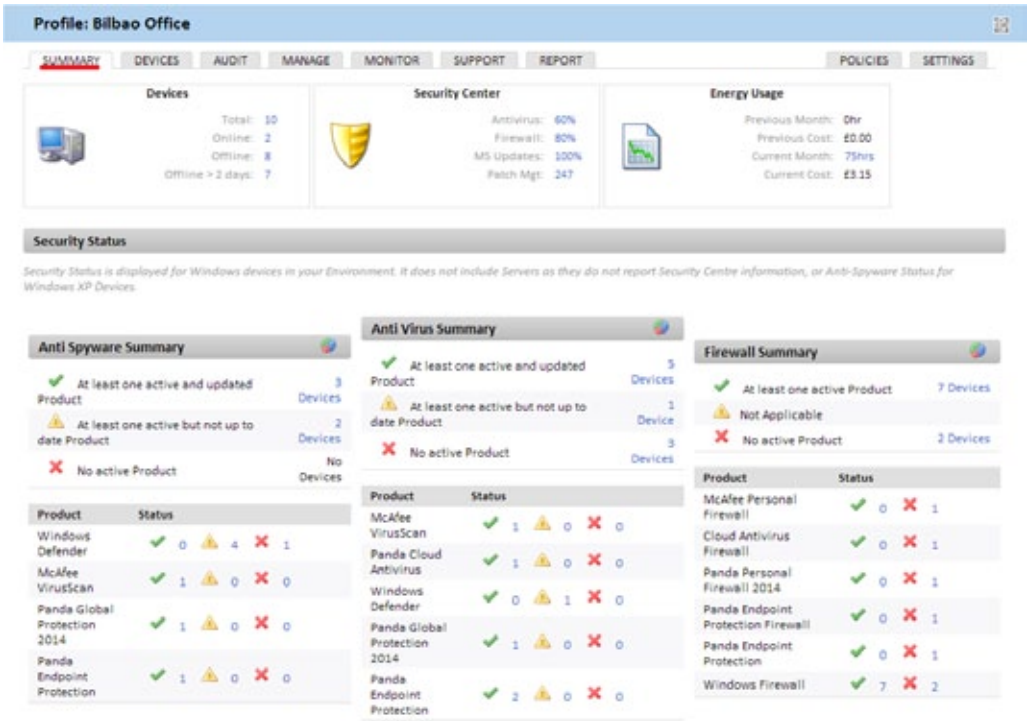


Figura 11: panel de control del Nivel Zona

4.6.4 Resumen (Dispositivo)

Accesible desde un dispositivo. Refleja su estado y habrá tantos como dispositivos administrados.

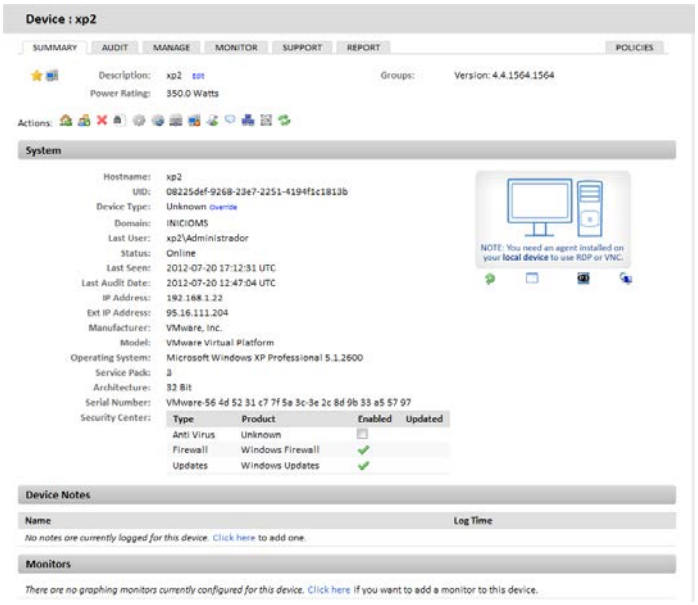


Figura 12: panel de control del Nivel Dispositivo

5. Despliegue y administración de dispositivos

Preparativos para agregar dispositivos

Envío del agente por email

Descarga directa del agente

Instalación en plataformas Android e iOS

Administración de servidores ESXi

Administración de servidores Hyper-V

Aprobación de dispositivos

Configuración de un agente de conexiones

Configuración de un nodo de red

Gestión de dispositivos

Visualización de la información de los dispositivos

Gestión del consumo de los dispositivos

5.1. Introducción

Consulta el Apéndice B para determinar las plataformas compatibles con la instalación del Agente.

En un entorno administrado por **Panda Systems Management,** un dispositivo es un equipo informático accesible desde la consola web para su gestión y mantenimiento remotos.

Todos los dispositivos gestionados por **Panda Systems Management** son emisores y receptores de información que el servidor recoge, cataloga y muestra en tiempo real y de forma ordenada en la consola.

El servidor PCSM y los dispositivos se comunican de tres maneras posibles:

- De forma directa instalando el agente en plataformas compatibles. En este escenario los agentes tienen salida a Internet para comunicarse con el servidor sin intermediarios.
- Indirectamente a través de un proxy para aquellos dispositivos que no tengan acceso a Internet de forma directa. Consulta más adelante en este capítulo para configurar un proxy.
- De forma indirecta a través del protocolo SNMP o de otros protocolos propietarios (ESXi).

Para dispositivos en los que no sea posible la instalación del agente, otro equipo con el agente desplegado y con el rol Nodo de red asignado puede hacer de pasarela y comunicarse con el dispositivo mediante protocolos auxiliares.

De esta forma, el nodo de red recibe los comandos del servidor convirtiéndolos a un protocolo que el dispositivo sin agente instalado pueda entender. En la respuesta del equipo gestionado, el mismo nodo de red deshace los cambios para hacer llegar la información del dispositivo no compatible al Servidor.

5.2. Preparativos para agregar dispositivos a Panda Systems Management

Antes de agregar un dispositivo a Panda Systems Management es necesaria cierta información básica:

- Zona de pertenencia del agente.
- Información de conexión.

Zona de pertenencia del agente

Para mantener ordenados todos los dispositivos administrados, éstos deben ser agrupados por zonas dentro de la consola. En plataformas de escritorio (Windows, Linux y macOS) la zona a la que pertenecerá el dispositivo se establece automáticamente al instalar el agente generado desde la

propia zona. De esta forma se evita la asignación manual de dispositivos a zonas como parte del despliegue de Panda Systems Management en los equipos de la red.

Para plataformas móviles (tablets y smartphones) la zona a la que pertenece el agente se debe de introducir manualmente con un fichero de configuración suministrado mediante correo electrónico. Consulta el apartado **Instalación del agente en plataformas Android e iOS** más adelante en este mismo capítulo.

Información de conexión

Además de la pertenencia a la zona designada por el administrador, el agente recién instalado en el dispositivo de usuario requiere información de salida a Internet para comunicarse con el servidor.

En gran parte de las infraestructuras TI de las empresas, solo es necesaria una configuración básica TCP/IP marcada por el propio sistema operativo instalado en el dispositivo del usuario, que el agente utilizará de forma normal en sus comunicaciones. Para esquemas de red que requieren servidores proxy para acceder a Internet, el agente necesitará información de conexión.

Los datos de configuración de proxy pueden ser introducidos:

- **Manualmente en cada agente instalado**: con el botón de la derecha del ratón haz clic en el icono de Panda Systems Management dentro del área de notificaciones del escritorio, selecciona **Configuración** en el menú desplegable y haz clic en la pestaña **Red**. Introduce los datos del proxy en los campos mostrados.
- **Globalmente en cada zona**: desde el menú general **Zonas** elige la zona a la que pertenecerá el dispositivo recién instalado y selecciona la barra de pestañas **Configuración** para introducir los datos necesarios en la sección **Proxy.** Una vez suministrada la configuración, todos los agentes que se instalen desde esta zona llevarán la información de proxy introducida.

5.3. Envío del agente PCSM por email

Para enviar el paquete de instalación del agente PCSM:

- Desde el menú general **Zonas,** elige la zona donde residirán los equipos a gestionar.
- Haz clic en barra de pestañas **Dispositivos** y en el botón **Añadir un dispositivo**. Se mostrarán en un diálogo todas las plataformas compatibles con el agente: Windows, macOS, Linux, iOS y Android, además de los dispositivos gestionables sin agente (dispositivos de red, impresoras y servidores ESXi).

- Introduce las direcciones de correo de los usuarios que manejan los dispositivos a administrar, separadas por el carácter ";". Dependiendo de la plataforma, el usuario recibirá un email con el agente en un adjunto (Windows, macOS y Linux) o con un link para su descarga desde la tienda de aplicaciones Google Play o Apple Store.

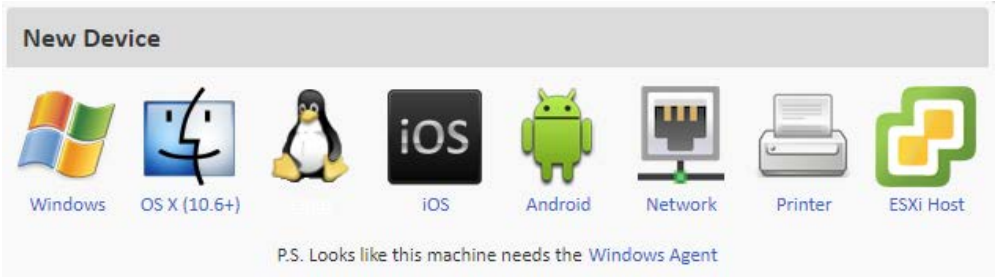


Figura 13: plataformas compatibles con Panda Systems Management

Para enviar un email con la URL de descarga del paquete de instalación Windows, macOS o Linux mediante el cliente de mensajería instalado en el equipo del administrador, haz clic en el link **enviar el enlace desde su cliente de correo electrónico en cambio**:

Figura 14: link para el envío del agente PCSM mediante el cliente de correo instalado en el equipo

5.4. Descarga directa del agente PCSM

El administrador puede descargar el agente desde la consola para luego distribuirlo de forma manual o con programas de instalación centralizada, como Active Directory. Para ello, se sigue el mismo procedimiento de los puntos anteriores, pero haz clic en el icono de la plataforma.

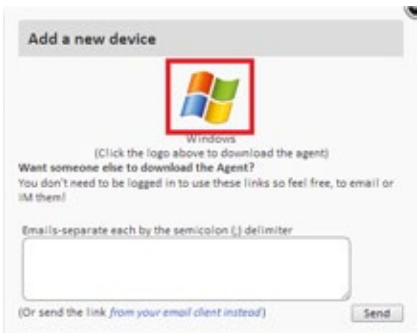


Figura 15: descarga directa del agente PCSM

Las plataformas móviles sin modificar (rooteo / jailbreak) solo permiten la descarga de aplicaciones desde la tienda asociada. Por esta razón, la única forma certificada disponible para el envío del agente en tablets y smartphones es mediante un mail con la URL de la aplicación publicada en la tienda de aplicaciones asociada al terminal.

5.5. Instalación remota

La instalación del agente en redes con muchos dispositivos es un proceso largo y tedioso si se ejecuta en cada uno de los equipos de forma independiente. En este escenario, se puede agilizar el despliegue con la funcionalidad de instalación remota:

- Envía del agente al primer dispositivo Windows o macOS de la red mediante cualquiera de los métodos descritos anteriormente.
- Designa el agente instalado como nodo de red (con escaneo de red).
- Lanza un descubrimiento de equipos en la red:
  - Desde la consola (Windows y macOS).
  - Desde el propio agente instalado (solo Windows).
- Instala de forma remota los agentes:
  - Desde la consola (Windows y macOS).
  - Desde el propio agente instalado (solo Windows).

5.5.1 Designa el agente instalado como nodo de red (con escaneo de la red)

Para descubrir dispositivos conectados a la red, es necesario designar el rol "nodo de red" a uno de los equipos con el agente **Systems Management** instalado. Consulta más adelante en este capítulo para asignar el rol nodo de red a un dispositivo.

5.5.2 Efectúa un descubrimiento de equipos en la red desde la consola

Para descubrir dispositivos en la red es necesario lanzar una auditoria del equipo designado como nodo de red (con escaneo de la red). Para ello, en el menú general **Zonas, Dispositivos** selecciona el dispositivo y en la barra de iconos haz clic sobre el icono de los catalejos  .

Por defecto, el descubrimiento se limitará a los dispositivos conectados en la misma subred a la que pertenece el equipo con el rol Nodo de red. Para ampliar el rango de exploración:

- Desde el menú general **Zonas**, haz clic en el menú de pestañas **Configuración**.
- En la sección **Subredes adicionales para el descubrimiento de redes** introduce los rangos de IPs que serán explorados.
- Para limitar el número total de direcciones IP analizadas por cada subred haz clic en el menú general **Ajustes**, menú de pestañas **Configuración de cuenta**, sección **Configuración**

personalizada del agente y establece los valores **Límite de subred** y **Límite del escaneo de red.**

Requisitos de descubrimiento de dispositivos

Para que un equipo de la red sea descubierto por un dispositivo con el rol Nodo de red se tiene que cumplir:

- **Si el nodo de red escanea la subred a la que pertenece**: el equipo candidato a ser descubierto tiene que responden al ping.
- **Si el nodo de red escanea otras subredes distintas a las que pertenece**:
  - El equipo candidato a ser descubierto tiene que responden al ping.
  - El equipo candidato a ser descubierto tiene que aceptar conexiones TCP en cualquiera de los puertos / protocolos siguientes: 22 – SSH, 80 – HTTP, 8080 – HTTP, 443 – HTTPS.

5.5.3 Instala de forma remota los agentes desde la consola

- Transcurridos un máximo de 15 minutos desde el descubrimiento de la red, en el menú general **Zonas,** menú de pestañas **Auditoría,** selecciona **Red** en el botón de selección para mostrar los equipos descubiertos agrupados por su tipo.
- Selecciona los dispositivos a instalar y haz clic en el icono **Administrar equipos.**
- Elige el tipo de agente a instalar en el dialogo mostrado.
- Introduce las credenciales necesarias en los dispositivos de destino para poder efectuar la instalación del agente. Puesto que la instalación remota de un agente es un proceso que crea servicios en el dispositivo, es necesario suministrar credenciales de administrador o equivalentes. La configuración de la cuenta del dominio que se utilizará se indica en la pestaña **Configuración** de la zona a la que pertenecen los dispositivos a instalar. En el apartado **Credenciales de implementación de agentes** se indicarán el nombre de usuario y la contraseña de administrador del dominio.

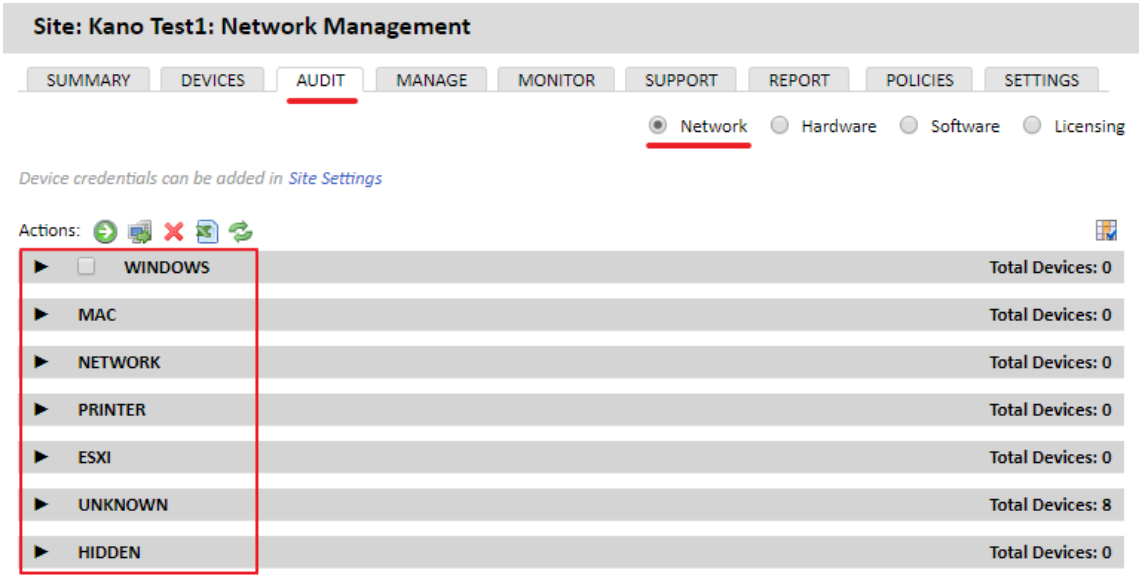


Figura 16: descubrimiento de equipos

Un agente instalado solo puede distribuir otros compatibles con su plataforma; de esta manera, un agente Windows distribuirá el agente a dispositivos compatibles con el sistema operativo de Microsoft, y un agente macOS distribuirá agentes a dispositivos Apple.

5.5.4 Descubrimiento de equipos en la red desde el agente instalado (procedimiento alternativo)

Para desplegar el agente PCSM directamente desde un equipo Windows ya integrado en Panda Systems Management haz clic en el icono de descubrimiento y después lanza un descubrimiento de dispositivos.

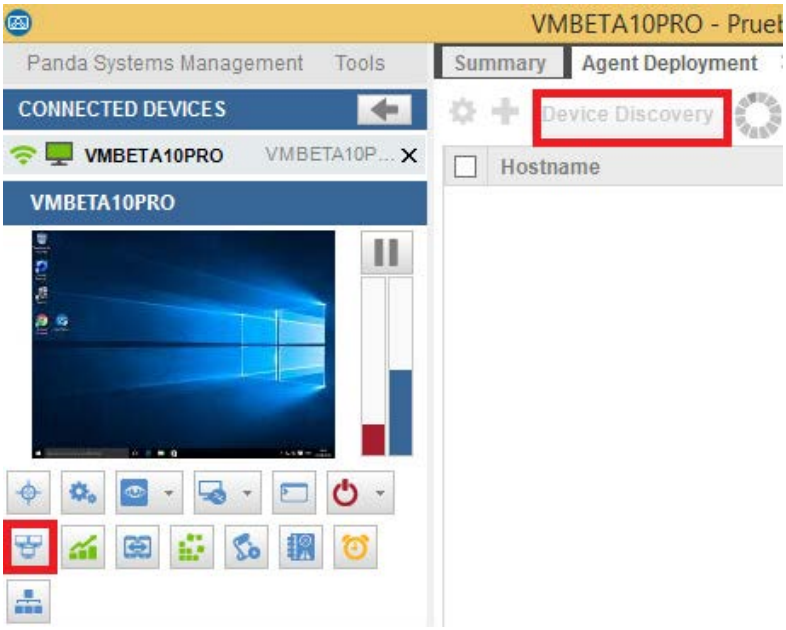


Figura 17: descubrimiento de dispositivos desde el agente PCSM

El agente mostrará todos los equipos conectados a la misma subred y además indicará si ya tienen un agente **Systems Management** instalado y su versión. Una vez que el proceso haya terminado, selecciona los equipos que recibirán el agente y haz clic en el icono **+.**

Antes de iniciar el despliegue propiamente dicho, se muestra una ventana donde podrás introducir las credenciales de usuario necesarias para poder instalar el agente y crear los servicios necesarios en los equipos de destino.

5.6. Instalación del agente en plataformas Android e iOS

Para administrar dispositivos móviles desde la consola **Systems Management** es necesario:

- Activa las funcionalidades MDM.
- Importa el certificado en la consola (solo dispositivos iOS).

- Envía por email la URL de descarga del agente PCSM.
- Asocia el dispositivo a la zona.

Activa las funcionalidades MDM de la consola

Para poder interactuar con los dispositivos móviles desde la consola habilita las funcionalidades MDM importando el componente gratuito **Mobile Device Management** directamente desde la **Comstore**.

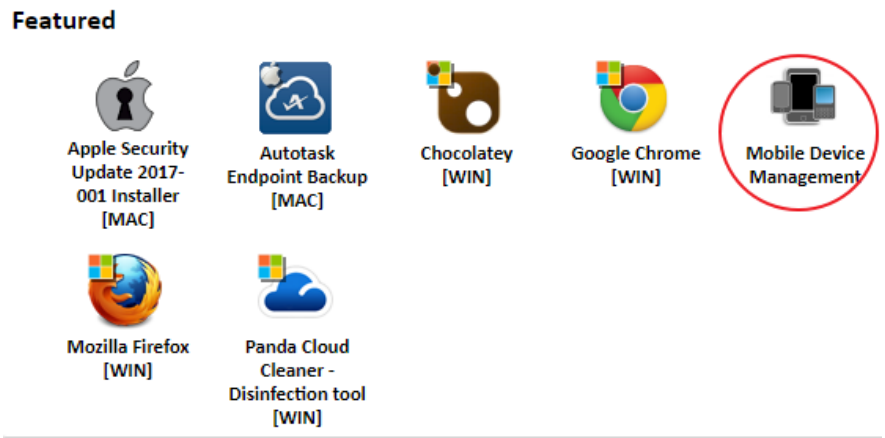


Figura 18: componente Mobile Device Management

> ***Aunque el componente Mobile Device Management se ofrece sin cargo extra, cada dispositivo móvil con un agente instalado contará como una licencia de dispositivo normal a los efectos del cómputo global de licencias adquiridas.***

Una vez agregado el componente, aparecerán las plataformas iOS y Android en la pestaña **Añadir un dispositivo**.

Importa el certificado en la consola para dispositivos basados en iOS

Es necesario incorporar en la consola el certificado generado por Apple para que los dispositivos iOS puedan conectar con el servidor.

> ***La importación del certificado de Apple es un proceso de obligado cumplimiento una sola vez por cada Cliente / Partner que vaya a administrar uno o más dispositivos de usuario basados en iOS.***
>
> ***La instalación del certificado es un requisito impuesto por Apple para garantizar la integridad, autenticidad y confidencialidad de las comunicaciones entre el servidor y el dispositivo de usuario.***

Para importar el certificado:

- En el menú general **Ajustes, Configuración de cuenta** al final de la página se muestra la configuración de certificados para Apple.

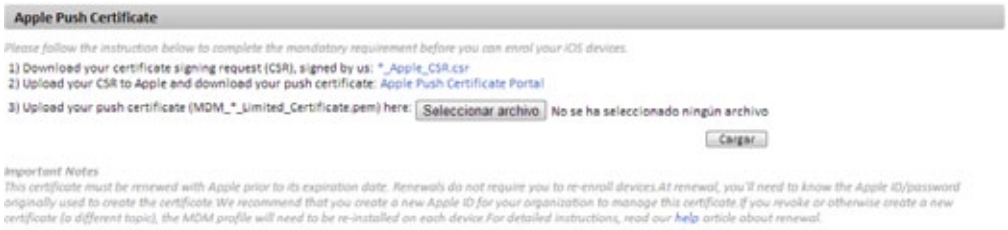


Figura 19: pantalla de carga del certificado

- Exportar la petición de firma de certificado (CSR) firmado por Panda Security (**_Apple_CSR.csr*).
- Importar el fichero CSR en el portal *Apple Push Certificate Portal*.

Para acceder al portal Apple *Push Certificate Portal,* es necesario disponer de una cuenta de Apple de cualquier tipo. Si quieres crear un nuevo juego de credenciales visita https://appleid.apple.com/, haz clic en **Crea un ID de Apple** y sigue las instrucciones en pantalla.

Con las credenciales preparadas visita la página https://identity.apple.com/pushcert, haz clic en **Create Certificate** y sigue las instrucciones en pantalla. Deberás cargar el fichero CSR descargado en el paso anterior.

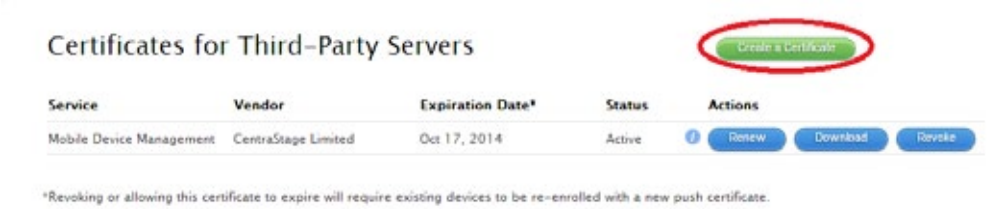


Figura 20: creación de un nuevo certificado en el portal de Apple

Descarga un nuevo fichero .PEM con el certificado de Apple.

Figura 21: descarga del certificado del portal de Apple

Carga el nuevo fichero .PEM obtenido del *Apple Push Certificate Portal* en la consola. Se mostrará la siguiente pantalla:

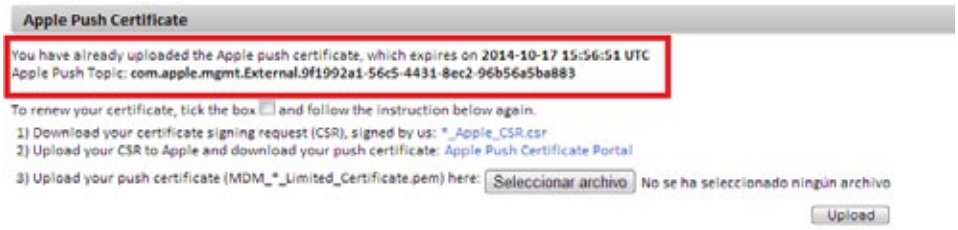


Figura 22: carga del certificado en la consola PCSM concluida

Envía por email la URL de descarga

Debido a las restricciones de seguridad, el cliente únicamente recibirá un correo con un link de descarga directa desde la *Apple Store* o Google *Play* y un fichero. MDM que es el que contiene la información de la zona a la que quedará asociado el dispositivo.

Puesto que la descarga del agente se realiza desde la tienda de aplicaciones certificada para cada plataforma móvil (Google Play o Apple Store), la información de pertenencia a la zona no forma parte del paquete descargado ya que de otro modo cambiaría de contenido. Para ello, se utiliza el fichero. MDM suministrado en el email.

Asocia el dispositivo a la zona

Los agentes de iOS y Android ya instalados en el dispositivo del cliente necesitan de un proceso manual que los vincule con la zona elegida. El proceso de vinculación se puede realizar de dos formas:

- **Opción 1: Capturando el código QR con la cámara del dispositivo.**

En un PC con la consola mostrando la zona que contendrá al dispositivo móvil del usuario, haz clic en el icono de código QR para ampliarlo, situado en la parte superior derecha de la ventana.

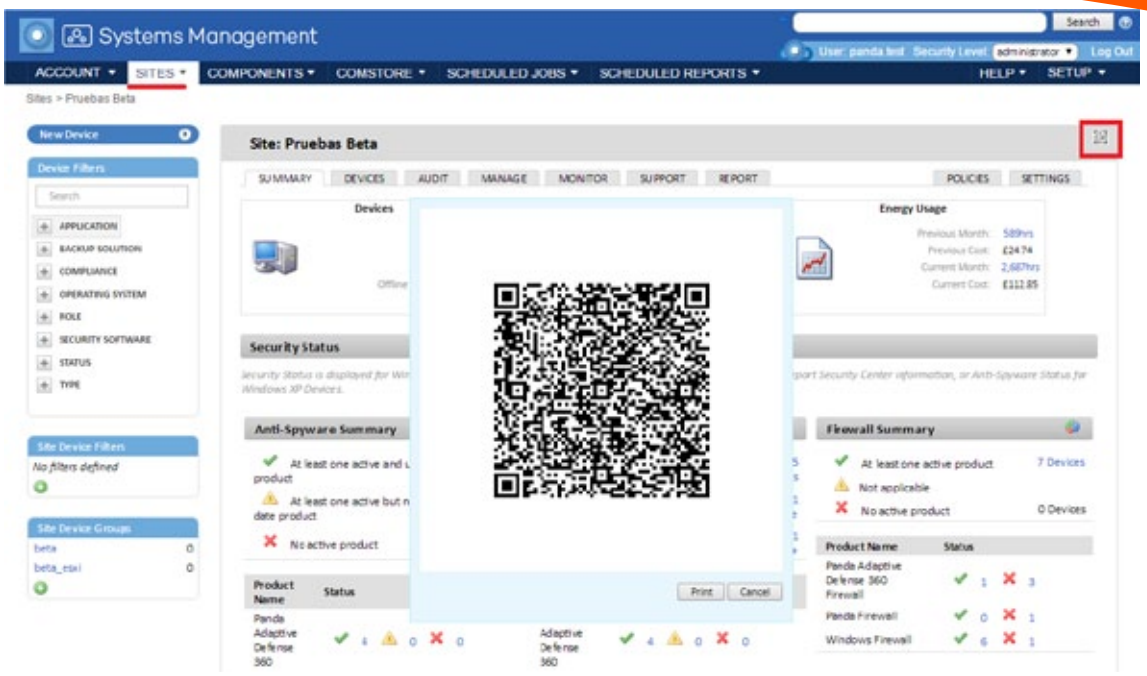


Figura 23: generación de código QR

En el dispositivo móvil del usuario, tocar el icono de la rueda para lanzar la cámara y enfocarla hacia el código QR de la pantalla.

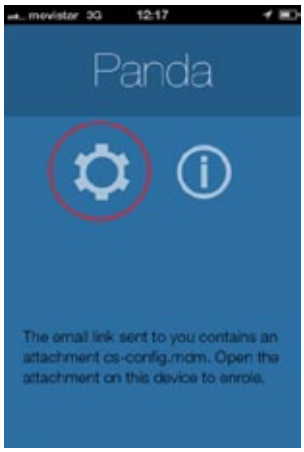


Figura 24: agente PCSM en el dispositivo movil

Una vez interpretado el código, el agente mostrará **Connected** en el dispositivo del usuario y el dispositivo se mostrará en la consola.

- **Opción 2: Importando en el agente el fichero. MDM enviado en el mensaje de correo.**

Si el móvil no incorpora cámara puedes abrir el fichero. MDM desde el propio mensaje de correo haciendo clic sobre el mismo. Una vez cargado, el agente mostrará **Connected** en el dispositivo y se mostrará en la consola.

Solo se soporta la importación del fichero MDM desde el cliente de correo nativo del terminal.

5.7. Administración de dispositivos mediante el protocolo SNMP

Aunque no es estrictamente necesario, se recomienda al administrador familiarizarse con los conceptos básicos del protocolo SNMP (OID, MIB, NMS etc) así como disponer de un navegador MIB para poder explorar la estructura de OIDs del dispositivo a gestionar. Se recomienda el programa Mibble, accesible en su página Web.

Panda Systems Management permite gestionar dispositivos que no admiten la instalación de software mediante el protocolo SNMP, tales como impresoras routers, switches, scanners, centralitas etc.

Para administrar dispositivos de red en **Panda Systems Management**:

- Agrega dispositivos de red
- Asigna un equipo nodo de red al dispositivo

5.7.1 Agrega dispositivos de red

Agrega dispositivos de forma individual

- En el menú general **Zonas** haz clic en la zona donde residen los dispositivos a gestionar.
- En la barra de pestañas **Dispositivos** haz clic en **Añadir un dispositivo** y elige **Impresora** o **Dispositivo de red.**

La consola muestra una ventana donde es necesario introducir la información relevante del dispositivo.

Agrega varios dispositivos de red a la vez

- En la pestaña **Auditoría,** selecciona **Red.** Se mostrarán todos los dispositivos descubiertos y agrupados por su tipo. Los grupos **Red**, **Impresora** y **Desconocido** contienen los dispositivos que no son compatibles con el agente PCSM.

- Selecciona los dispositivos de red a integrar y haz clic en el botón . Se mostrará una ventana donde introducir la información necesaria para poder gestionar el dispositivo nuevo:
  - **Desplegar desde**: selecciona el nodo de red asignado al dispositivo
  - **Tipo de dispositivo**: determina el tipo de dispositivo que aparecerá en la consola
  - **Definir credenciales**: selecciona la configuración de credenciales SNMP creada en la sección **Credenciales SNMP** de la pestaña **Configuración** en el Nivel zona o en la pestaña **Ajustes, Configuración de cuenta** en el Nivel Cuenta,

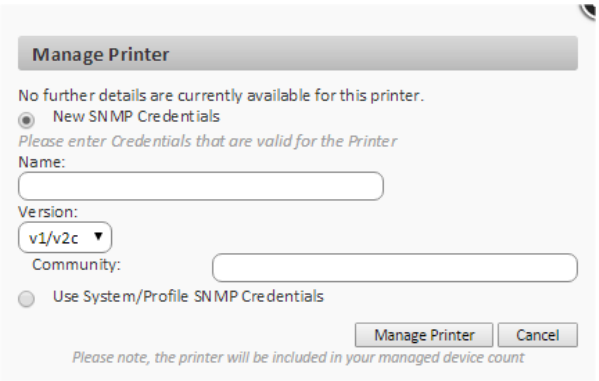


Figura 25: ventana de credenciales para gestionar un dispositivo por SNMP

Cada dispositivo añadido a la consola consume una licencia del total de licencias contratadas por el cliente.

5.7.2 Asigna un equipo nodo de red al dispositivo

Debido a la imposibilidad de instalar un agente PCSM en routers, switches y otros dispositivos de red, es necesario que un equipo independiente haga de puente entre el servidor **Systems Management** y el propio dispositivo a administrar. Este equipo requiere la asignación del rol Nodo de red.

Asigna un nodo de red a un único dispositivo no compatible con el agente PCSM:

- Haz clic en el menú general **Zonas**, selecciona la zona a la que pertenece el dispositivo a administrar y haz clic en el menú de pestañas **Resumen**.
- Haz clic en el link **Editar** del campo **Nodo de red**. Se mostrará un desplegable con todos los nodos de red accesibles. Selecciona uno de ellos y haz clic en **Guardar**.

Asigna un equipo nodo de red a varios dispositivos

- Haz clic en el menú general **Zonas** y selecciona la zona donde residen los dispositivos.
- Selecciona los equipos a asignar y haz clic en el icono de la barra de acciones.
- Selecciona en el desplegable la entrada **Asignar nodo de red**. Se mostrará una ventana donde elegir un nodo de red entre todos los disponibles.

5.8. Administración de servidores ESXi

Los servidores ESXi son sistemas que utilizan un kernel Linux especialmente modificado y simplificado para la ejecución del hypervisor del fabricante, que será el encargado de dar el servicio de virtualización a todas las máquinas virtuales alojadas. Los sistemas ESXi no son compatibles con el agente PCSM, ya que su único objetivo es ejecutar las máquinas virtuales creadas con el menor impacto posible en los recursos del servidor.

La administración de servidores ESXi en **Panda Systems Management** se realiza a través de un agente PCSM instalado en una máquina Windows. Este agente se conectará con el servidor ESXi a gestionar y recogerá toda la información necesaria para enviarla al Servidor PCSM y mostrarla en la consola de administración.

Es importante distinguir entre la administración del servidor ESXi y de las máquinas virtuales que alberga. La gestión del servidor ESXi permite administrar los recursos de la máquina física y el hypervisor, mientras que la administración de las diferentes máquinas virtuales permite gestionar el estado de los recursos virtualizados para una máquina virtual concreta. Para este caso es necesario instalar un agente PCSM de la misma forma que si se tratara de una maquina física.

5.8.1 Agrega un servidor ESXi de forma individual

- En el menú general **Zonas** elige la zona donde residen los equipos a gestionar
- En la barra de pestañas **dispositivos** haz clic en **Añadir un dispositivo.** Se mostrará en un diálogo las plataformas admitidas.
- Haz clic en el icono ESXi.
- Introduce los datos necesarios para la comunicación con el servidor ESXi.

Puesto que los servidores ESXi no son compatibles con el agente PCSM, es necesario que un agente PCSM de la red actúe de pasarela (Nodo de red). Para ello, hay que suministrar las credenciales de conexión apropiadas.

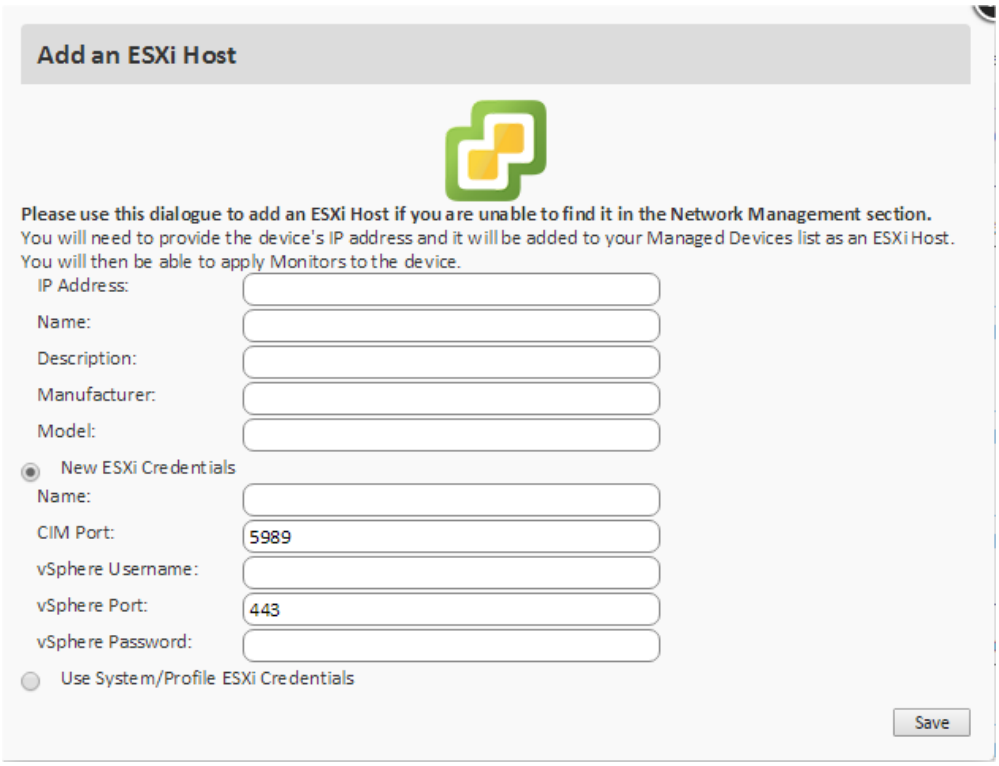


Figura 26: pantalla de conexión con el servidor ESXi

Para definir un juego de credenciales específico para conectar con el servidor ESXi, haz clic en **Nuevas credenciales ESXi.** Para heredar la configuración establecida en el Nivel Cuenta o Nivel Zona, haz clic en **Utilizar credenciales EXSi de Cuenta/Zona**.

Las credenciales del servidor ESXi se definen de forma particular para el servidor ESXi a integrar o heredan la configuración general establecida a nivel global en menú general **Cuenta, Ajustes** o a nivel de zona, seleccionando la zona apropiada y haciendo clic en la barra de pestañas **Configuración**.

Para más información, consulta el Capitulo 3 Jerarquía de niveles en la Consola.

5.8.2 Agrega varios servidores ESXi a la vez

En la barra de pestañas **Administrar** se muestran todos los dispositivos descubiertos en la red. Filtra el listado por **Otros** o utiliza el campo **Buscar** para localizar el servidor ESXi a agregar.

Una vez localizado, haz clic en el icono de **Manage device**  y a continuación en ESXi como tipo de dispositivo. Se presentará un formulario equivalente al mostrado en el punto anterior donde introducir las credenciales necesarias para que un agente PCSM de la red se conecte con el servidor ESXi y extraiga la información de monitorización y estado.

5.8.3 Asigna un equipo nodo de red al dispositivo ESXi

Debido a la imposibilidad de instalar un agente PCSM en los servidores ESXi, es necesario que un equipo independiente haga de puente entre el servidor **Systems Management** y el propio dispositivo a administrar. Este equipo requiere la asignación del rol Nodo de red. Para asignar un nodo de red a un servidor ESXi sigue los pasos mostrados en el punto 5.7.2.

5.9. Administración de servidores Hyper-V

Los servidores Hyper-V son sistemas Windows Server con el rol Hyper-V configurado, de forma que puedan ejecutar el subsistema hypervisor de Microsoft para alojar máquinas virtuales.

Debido a que **Panda Systems Management** es directamente compatible con la familia de servidores Windows Server, no es necesario ejecutar ningún procedimiento distinto al detallado en el apartado **Agregar dispositivos compatibles con el agente** para sistemas Windows. Una vez instalado el agente PCSM, se podrá auditar el servidor Hyper-V y las máquinas virtuales que albergue.

5.10. Aprobación de dispositivos

Como paso adicional, el administrador del servicio puede requerir una aprobación manual a la hora de integrar un nuevo equipo con el agente recién desplegado. Este proceso es necesario para controlar qué dispositivos se agregan al servicio, sobre todo en aquellos entornos donde el instalador del agente es accesible de forma libre dentro de la empresa (unidad mapeada o recurso compartido).

La configuración de la aprobación manual de dispositivos se encuentra en el menú general **Ajustes, Configuración de cuenta,** apartado **Control de acceso.**

Una vez activada la aprobación manual de equipos, éstos irán apareciendo en la sección **Dispositivos eliminados** dentro de la zona elegida, según vayan siendo instalados los agentes. El administrador entonces podrá aprobar aquellos dispositivos que quiera integrar en el servicio.

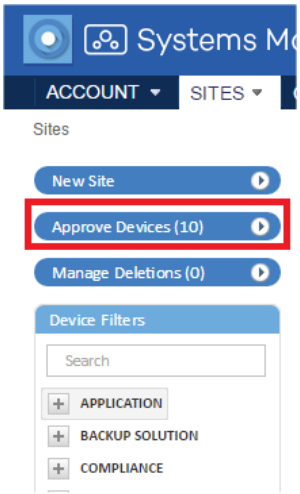


Figura 27: botón de dispositivos pendientes de aprobación

Aunque los dispositivos no sean aprobados, entrarán a formar parte de los procesos de inventariado y será posible acceder a ellos por escritorio remoto.

> ***Los equipos no aprobados seguirán consumiendo licencias.***
>
> ***Los equipos no aprobados no podrán recibir tareas ni componentes desplegados.***

Cuando un equipo esté pendiente de aprobación, aparecerá un mensaje en el listado de dispositivos en la zona a la que pertenece.

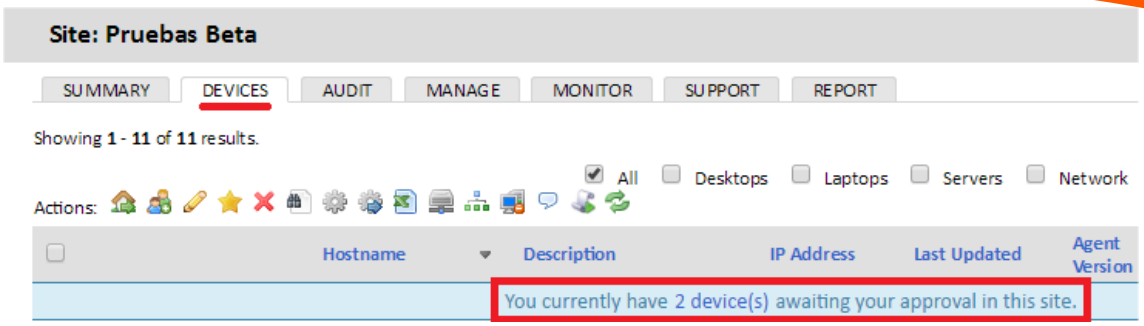


Figura 28: mensaje de dispositivo pendiente de aprobación

5.11. Configuración de un agente de conexiones

Un agente de conexiones, también conocido como Broker de conexiones, es un dispositivo Windows con un agente instalado encargado de realizar un conjunto de tareas adicionales orientadas a minimizar el tráfico de red del cliente, así como a facilitar la conectividad del escritorio remoto en sus dispositivos vecinos.

Por defecto, en cada segmento de red del cliente habrá un agente promocionado de forma automática al rol de agente de conexiones. Éste será el encargado de mantener la comunicación de forma centralizada entre el servidor y los dispositivos administrados para minimizar el uso de ancho de banda en la red.

Si se observan dificultades para establecer una sesión de escritorio remoto con los dispositivos en un segmento de red, reinicia el equipo que tenga el rol "agente de conexiones" y vuelve a intentarlo.

5.11.1 Asignar el rol de agente de conexiones a un dispositivo

Aunque la promoción de un equipo a agente de conexiones es un proceso automático según las características de cada dispositivo (tiempo que permanece encendido, ancho de banda disponible, potencia de CPU etc.), en algunos casos es posible que convenga promocionar manualmente un dispositivo en concreto de la red.

Procura asignar el rol de agente de conexiones a un dispositivo de tipo servidor en cada segmento de red, de forma que sea un equipo con suficientes recursos y que permanezca siempre en servicio.

Para ello, accede a la configuración del agente que tomará el rol de agente de conexiones haciendo clic con el botón de la derecha del ratón y seleccionando **Configuración, Preferencias.**

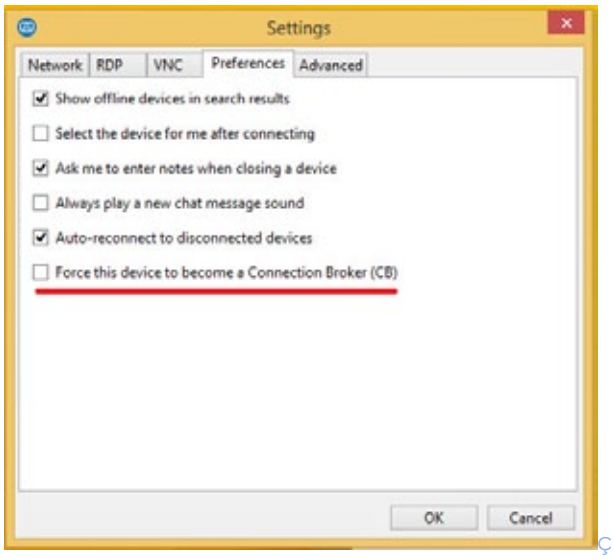


Figura 29: ventana de configuración del agente de conexiones en el agente PCSM

5.11.2 Desactivar el uso de agente de conexiones

Debido a que las tareas de un agente PCSM promocionado a agente de conexiones requieren una serie de recursos de la CPU del dispositivo y de la red local del cliente que pueden no estar disponibles, es posible desactivar completamente esta funcionalidad desde el menú general **Ajustes, Configuración de cuenta** en **Configuración de agente personalizada** o desde la propia zona, **Configuración** para desactivar la funcionalidad en una zona concreta.

5.12. Configuración alternativa de los parámetros del agente

Excepto Límite de subred, estos parámetros solo deben ser modificados por petición expresa del departamento de Soporte de Panda Security. Cualquier modificación puede resultar en la pérdida de conexión de los agentes administrados.

Para especificar los parámetros que gobiernan la conexión del agente PCSM haz clic en el menú general **Ajustes, Configuración de cuenta, Usar configuración alternativa para agente.** Dentro de la sección **Configuración de agente personalizada,** puedes configurar:

Campo	Descripción
Dirección de canal de control	Uso restringido al departamento de Soporte de **Panda Security.**
Puerto 1 de canal de control	Uso restringido al departamento de Soporte de **Panda Security.**
Dirección de servicio Web:	Uso restringido al departamento de Soporte de **Panda Security.**

Campo	Descripción
Dirección de servidor de túnel:	Uso restringido al departamento de Soporte de **Panda Security.**
Límite de la subred	Limita al número indicado (0-65535) el rango de escaneo de dispositivos del nodo de red dentro de un segmento de red. Introduciendo el valor 0 se impide el escaneo de dispositivos en la red.
Límite del escaneo en la red	Limita al número indicado (0-1024) el número de dispositivos escaneados por el agente dentro de su subred. Introduciendo el valor 0 se impide el escaneo de dispositivos en la red.

Tabla 7: parámetros de configuración de las conexiones utilizadas por el agente PCSM

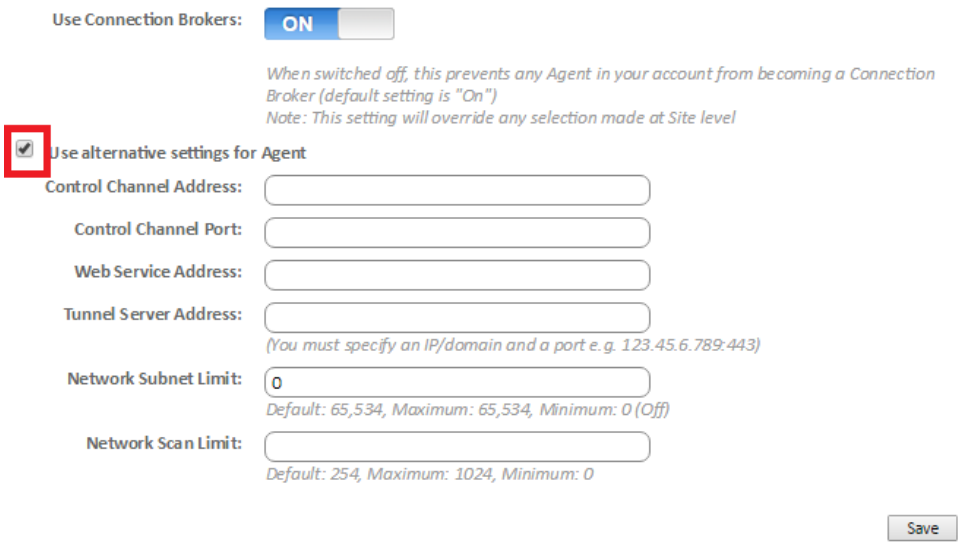


Figura 30: ventana de configuración de conexiones utilizadas por el agente PCSM

5.13. Configuración de un nodo de red

Un nodo de red es un dispositivo con un agente **Systems Management** instalado que ejecuta funciones adicionales en la red del cliente relativas al descubrimiento de equipos y a la gestión de dispositivos vía SNMP.

5.13.1 Requisitos para configurar un nodo de red

- Solo los dispositivos con rol de servidor, puesto de trabajo o portátil pueden ser nominados al rol Nodo de red.
- El dispositivo tiene que tener instalado un sistema operativo Windows, macOS o Linux compatible con el agente PCSM.

Solo los sistemas operativos Windows y macOS pueden ejecutar exploraciones de red para descubrir equipos.

- El dispositivo tiene que tener instalado un agente PCSM.

5.13.2 Asignación del rol Nodo de red

En el menú general **Zonas, Dispositivos** selecciona el dispositivo que será designado con el rol de nodo de red. Para ello, selecciona un dispositivo con la casilla de selección, haz clic en la barra de iconos y selecciona **Nodo de red**.

Una vez que el dispositivo ha adoptado el nuevo rol, su icono cambia a .

5.13.3 Tipos de nodo de red

Existen dos tipos de nodos de red:

Con exploración de la red

Estos nodos permiten descubrir los dispositivos cercanos o conectados al mismo segmento de red.

Cada vez que se ejecute una auditoría del equipo con el rol nodo de red y exploración de red, el agente lanzará un broadcast de descubrimiento de dispositivos, mostrando los encontrados en la pestaña **Auditoria, Red**.

Además, los equipos con el nodo de red asignado están habilitados para enviar y recibir comandos SNMP que permiten gestionar dispositivos que no admiten la instalación de un agente **Systems Management**.

Sin exploración de la red

Estos dispositivos simplemente están habilitados para enviar y recibir comandos SNMP y no buscan en la red otros equipos.

5.14. Gestión de dispositivos.

Panda Systems Management ofrece varias funcionalidades para acceder a los dispositivos integrados en el producto, dependiendo de si son compatibles con el agente PCSM o no.

5.14.1 Dispositivos compatibles con el agente PCSM

Para gestionar equipos compatibles con el agente PCSM:

- Haz clic en el menú general **Zonas**, selecciona la zona donde reside el dispositivo y haz clic en el dispositivo a gestionar.
- En el menú de pestañas **Resumen** se muestran varios iconos que permiten acceder al equipo.

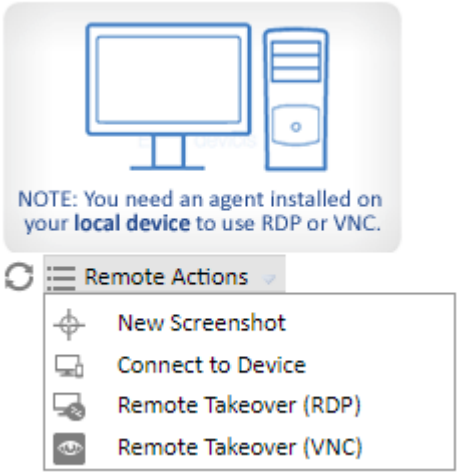


Figura 31: acceso a las herramientas de acceso remoto

Actualizar	Actualiza la captura del escritorio del dispositivo.
Nueva captura de pantalla	Descarga una captura del escritorio del dispositivo.
Conectar con dispositivo	Establece una conexión con el agente local al dispositivo seleccionado.
Toma de control de un remoto (RDP)	Conexión remota al escritorio del dispositivo mediante el protocolo RDP.
Toma de control de un remoto (VNC)	Conexión remota al escritorio del dispositivo mediante el protocolo VNC.

Tabla 8: tipos de acceso remoto a los dispositivos

Acceso a los recursos de los dispositivos remotos administrados

Para ejecutar ciertos comandos sobre un equipo concreto:

- Haz clic en la opción **Conectar dispositivo** de la pestaña **Resumen** del dispositivo. Se abrirá el agente PCSM instalado con las credenciales adecuadas.
- Una vez conectado al dispositivo las opciones de control y acceso remoto serán accesibles tanto a través de los iconos como de los menús.

Las opciones disponibles que no impiden al usuario seguir trabajando con el dispositivo son:

- **Captura de pantalla remota**: visualización rápida de mensajes de error.
- **Pestaña de servicios de Windows**: acceso a parada, arranque y reinicio de servicios sin necesidad de acceder al escritorio remoto.
- **Sesión de pantalla compartida**: escritorio remoto compartido. El usuario ve lo que el técnico está haciendo en su dispositivo.
- **Shell de comandos**: línea de comandos DOS remota.
- **Implementación del agente**: lanza el despliegue del Agente en la LAN.
- **Administrador de tareas**: acceso al administrador de tareas sin necesidad de acceder al escritorio remoto.
- **Transferencia de archivos**: acceso completo al sistema de ficheros del dispositivo con posibilidad de transferir ficheros entre el equipo del usuario y el del administrador, mover ficheros, crear y borrar carpetas y renombrar elementos.
- **Información de unidad**: obtiene información sobre todas las unidades locales y de red conectadas al dispositivo, con la posibilidad de añadir nuevas rutas de red o borrarlas.
- **Editor del registro**: accede a la herramienta de Regedit sin necesidad de conectar con el escritorio remoto.
- **Tareas rápidas**: lanza tareas en el dispositivo.
- **Visor de eventos**: accede al visor de sucesos sin necesidad de conectar con al escritorio remoto.
- **Wake Up**: arranca de forma remota un dispositivo de la red mediante el envió de un "magic packet" por parte de un equipo que este en la misma subred.

Las opciones que interrumpen el trabajo del usuario con el dispositivo son:

- **RDP de Windows**: acceso al escritorio remoto por RDP. Implica el cierre de la sesión del usuario.
- **ShutDown / Reboot:** reinicio del equipo.

5.14.2 Dispositivos no compatibles con el agente PCSM

Routers, switches, centralitas o impresoras son dispositivos de red no compatibles con el agente PCSM, pero que incorporan servicios más o menos estandarizados para su administración. Estos servicios tienen el inconveniente de poderse utilizar únicamente desde dentro de la red corporativa de la organización.

Es una práctica habitual configurar un equipo accesible desde el exterior que haga las veces de proxy cuando el administrador no está directamente conectado a la red de la organización y quiere gestionar este tipo de dispositivos. **Panda Systems Management** automatiza esta operación

utilizando los equipos con el rol Nodo de red asignado, evitando la redirección de puertos manual en los routers corporativos o la contratación y configuración de VPNs de acceso.

Con **Panda Systems Management** el equipo del administrador puede establecer conexiones Telnet, SSH, HTTP u otros protocolos contra el dispositivo a gestionar, independientemente de donde se encuentren. El equipo Nodo de red gestiona las peticiones del administrador y recoge los resultados, entregándolos en tiempo real al equipo del técnico IT.

La administración de un equipo a través de un nodo de red sigue este proceso:

- El agente Systems Management del administrador crea un túnel entre su equipo y el dispositivo Nodo de red. Este túnel tiene en el extremo del administrador la dirección 127.0.0.1 en un puerto asignado por el agente PCSM de forma aleatoria. El túnel es gestionado por el servidor Systems Management y atraviesa los cortafuegos perimetrales de la organización, así como el cortafuegos personal del equipo Nodo de red.
- El administrador ejecuta una aplicación cliente de administración y la conecta a la dirección local asignada por el agente PCSM 127.0.0.1 {puerto}.
- El tráfico con destino a la dirección 127.0.0.1:puerto del equipo del administrador se enruta por el túnel y el rol nodo de red dentro de la red de la organización lo recibe.
- El Nodo de red recoge los datos recibidos y los reenvía al servicio instalado en el dispositivo remoto a gestionar (HTTP, SSH, Telnet u otros).
- El servicio del equipo remoto a gestionar recoge las peticiones del administrador, las procesa y las devuelve al Nodo de red.
- El Nodo de red enruta la respuesta por el túnel establecido para entregarla a la aplicación conectada en el 127.0.0.1:puerto en el equipo del administrador.

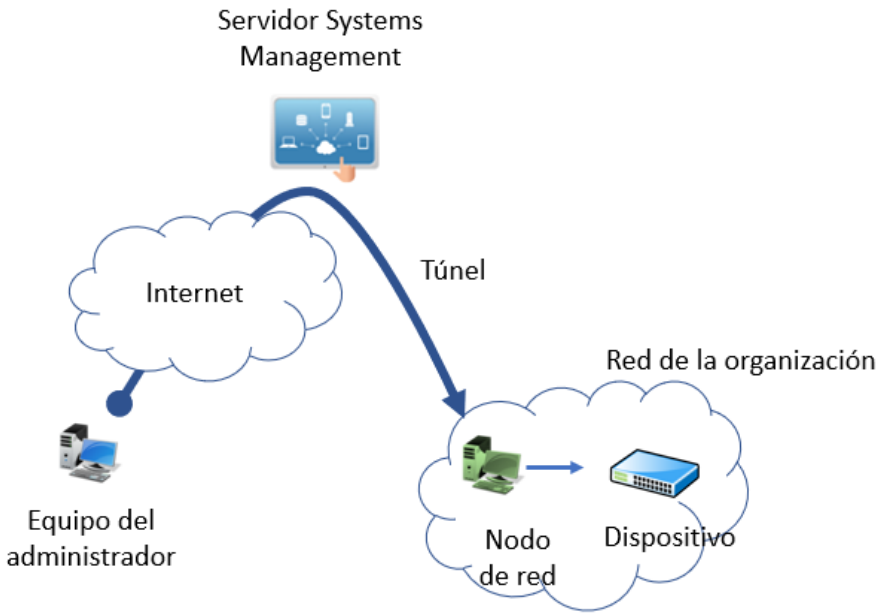


Figura 32:esquema general de conexión entre el equipo del administrador hasta el nodo de red a través del túnel

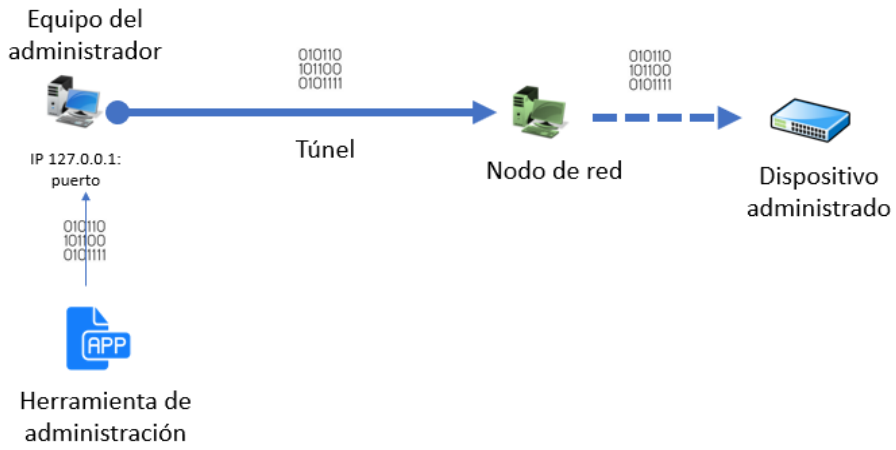


Figura 33: esquema de acceso de la herramienta de administración al dispositivo administrado

Para acceder a un dispositivo de red mediante HTTP:

- Es necesario que el dispositivo a administrar incorpore un servidor web que recoja la petición y presente una interface de gestión web.
- Desde el agente PCSM selecciona el dispositivo a gestionar.
- Haz clic en el icono y selecciona del desplegable **Connect (HTTP)**
- Haz clic en la casilla **Open browser automatically**. El equipo del administrador debe de tener un navegador instalado.
- Se completará automáticamente el campo URL con la IP del dispositivo a acceder. Si el servidor web del dispositivo no escucha en el puerto predeterminado HTTP (80) indica el nuevo puerto separado por dos puntos.
- En la sección **VIA** selecciona el nodo de red que actuará de intermediario entre el equipo del administrador y el dispositivo a gestionar.
- Haz clic en el botón **Iniciar.**

Para acceder a un dispositivo de red mediante SSH

- Es necesario que el dispositivo a administrar incorpore un servidor de línea de comandos remota compatible con el protocolo telnet o ssh, encargado recoger las peticiones y presentar los resultados.
- Desde el agente PCSM selecciona el dispositivo a gestionar.
- Haz clic en el icono y selecciona del desplegable **Connect (Telnet/SSH)**.
- Haz clic en la casilla **Open PuTTY automatically**. El programa Putty tiene que estar instalado en el equipo del administrador.
- Se completará automáticamente el campo URL con la IP del dispositivo a acceder y el puerto. Si el servidor telnet / ssh del dispositivo no escucha en el puerto predeterminado telnet (21) / ssh (22) indica el nuevo puerto en la caja de texto.
- En la sección **VIA** selecciona el nodo de red que actuará de intermediario entre el equipo del administrador y el dispositivo a gestionar.
- Haz clic en el botón **Iniciar.**

Para acceder a un dispositivo de red mediante una aplicación de terceros.

- Desde el agente PCSM selecciona el dispositivo a gestionar.
- Haz clic en el icono  y selecciona del desplegable **Connect (Custom Tunnel**).
- Para ejecutar la herramienta de administración de forma automática una vez establecido el túnel haz clic en la casilla **After connected, run the following program**. El programa tiene que estar instalado en el equipo a administrar.
- Indica en el campo URL la IP del dispositivo a acceder y el puerto de servicio de administración. Es necesario que el dispositivo incorpore un servidor compatible con la herramienta de administración elegida por el técnico de IT, capaz de entender las peticiones, procesarlas y devolver el resultado.
- En la sección **VIA** selecciona el nodo de red que se utilizará de intermediario entre el equipo del administrador y el dispositivo a gestionar.
- Haz clic en el botón **Iniciar.**

El túnel entre el equipo del administrador y el Nodo de red se establece en un único puerto local, por lo tanto, solo es necesario que la herramienta de gestión se comunique con el servicio de administración a través de un único puerto. Servicios que utilicen protocolos que establecen varios canales simultáneos de comunicación no funcionarán.

5.15. Visualización de la información de los dispositivos

Para acceder al Nivel Dispositivo asociado a cada equipo, desde el menú general **Zonas**, selecciona la zona a la que pertenece el dispositivo y haz clic en la pestaña **Dispositivos** y después en el equipo a visualizar. Se mostrará la siguiente información de carácter general.

Dependiendo del tipo de dispositivo (servidor, puesto de trabajo o teléfono móvil / tablet, dispositivo de red o servidor ESXi) algunas entradas podrán cambiar o no estar disponibles.

La información mostrada se divide en cinco apartados:

- Información general del dispositivo.
- Información de sistema.
- Notas del administrador.
- Información de actividad.
- Información de rendimiento.

Información general del dispositivo

Campo	Descripción	Disponible en
Descripción	Texto editable descriptivo del dispositivo. Inicialmente contiene su nombre.	Todos los dispositivos.
Grupos	Grupos a los que pertenece el dispositivo.	Todos los dispositivos.
Versión	Versión del agente instalado	Windows, Linux, macOS, Android, iOS.
Potencia nominal	En función del tipo de dispositivo se le asignará un consumo por defecto. Consulta más adelante en este capítulo la gestión del consumo de los dispositivos administrados.	Windows, Linux, macOS, ESXi.
Campo personalizado	Este campo permite definir etiquetas descriptivas por dispositivo. La diferencia con el campo **Descripción** es que **Campo personalizado** es accesible desde scripts ejecutados en los dispositivos, siendo una forma visual de integrar el resultado de la ejecución de un script en la consola. Para más información, consulta el Capítulo 11: Componentes y la ComStore.	Todos los dispositivos.

Tabla 9: información general del dispositivo

Información de sistema

Campo	Descripción	Disponible en
Nombre del host	Nombre del dispositivo.	Windows, Linux, macOS, ESXi, Network Device.
Nodo de red	Nombre del equipo asociado al dispositivo que tiene asignado el rol Nodo de red. Los equipos que tengan un agente PCSM instalado mostrarán la entrada **localhost** ya que no requieren la asignación de un nodo de red para su monitorización y gestión.	Windows, Linux, macOS, ESXi, Network Device
UID	Identificador interno del dispositivo.	Windows, Linux, macOS, ESXi, Network Device
Tipo de dispositivo	Tipo del dispositivo (Desconocido, Automático, Escritorio, Portátil, Servidor, Smartphone, Tablet, Network Device, ESXi Host).	Todos los dispositivos. Los servidores Hyper-V se muestran como Servidor.
Dominio	Dominio Windows al que pertenece el dispositivo.	Windows, Linux, macOS.
Versión de Hyper-V	Versión interna del Windows Server	Windows Server con el rol Hyper-V activado

Campo	Descripción	Disponible en
Ultimo usuario	Ultimo usuario que hizo login en el dispositivo.	Windows, Linux, macOS.
Estado	Estado (online, offline).	Windows, Linux, macOS, ESXi.
Visto por última vez	Fecha de la última vez que el servidor accedió al dispositivo.	Windows, Linux, macOS, ESXi, Android, iOS.
Último reinicio	Fecha de la última vez que se reinició el dispositivo	Windows, Linux, macOS
Fecha de la última auditoría	Fecha de la última vez que se realizó una auditoria de software y hardware. Para más información, consulta el Capítulo 12: Auditoria de activos.	Windows, Linux, macOS, ESXi, Android, iOS.
Creado en fecha	Fecha de alta del dispositivo en el sistema.	Windows, Linux, macOS, ESXi, Android, iOS, Network Device.
Dirección IP	Dirección IP local del dispositivo.	Windows, Linux, macOS, ESXi, Android, iOS, Network Device.
Ext. de dirección IP	Dirección IP del router o dispositivo que conecta a Internet al dispositivo.	Windows, Linux, macOS, ESXi, Android, iOS, Network Device.
IP(s) adicionales	Alias de IP.	Windows, Linux, macOS, ESXi, Android, iOS.
Credenciales ESXi	Configuración de acceso que aplica al servidor ESXi, definida en la pestaña **Configuración** de la zona. Para más información sobre los detalles de configuración del Nivel Cuenta y Nivel Zona, consulta el capítulo 4.	ESXi
Fabricante		Windows, Linux, macOS, ESXi, Android, iOS.
Modelo		Windows, Linux, macOS, ESXi, Android, iOS.
Sistema operativo		Windows, Linux, macOS, ESXi, Android, iOS.
Service Pack		Windows, Linux, macOS.
Etiqueta Servicio / Recurso	Cadena de texto para la identificación del servidor.	ESXi.
IMEI	Código de identificación del terminal móvil.	Android, iOS.
ICCID	Identificador de la tarjeta SIM.	Android, iOS.

Campo	Descripción	Disponible en
Operador	Compañía que suministra el servicio de telefonía.	Android, iOS.
Número	Número de teléfono.	Android, iOS.
Información GPS	Coordenadas obtenidas por GPS.	Android, iOS.
Imágenes	Numero de imágenes tomadas de las máquinas virtuales albergadas en el servidor ESXi.	ESXi.
Información del invitado	Información de cada máquina virtual albergada en el servidor ESXi o Hyper-V. (**Nombre del host, Nombre del invitado, Sistema operativo, Estado**). Esta información solo es accesible si se instala un agente PCSM en cada máquina virtual.	ESXi.
Arquitectura	32 o 64 bits.	Windows, Linux, macOS.
Número de serie		Windows, Linux, macOS.
Centro de seguridad	Estado de los recursos de protección instalados en el dispositivo.	Windows, Linux, macOS.
Credenciales SNMP	Configuración SNMP que aplica al dispositivo, definida en la pestaña **Configuración** de la zona. Para más información sobre los detalles de configuración del Nivel Cuenta y Nivel Zona, consulta el capítulo 4.	Network Device.

Tabla 10: información del sistema

Algunos de los campos llevan un link de búsqueda en Google para facilitar información acerca del fabricante, marca o modelo del dispositivo.

Notas del administrador

En esta sección el administrador puede agregar recordatorios, comentarios, así como procedimientos de resolución de problemas recurrentes del dispositivo para facilitar la colaboración con otros administradores

Registro de actividad

Muestra las acciones ejecutadas sobre el dispositivo. Esta información es un resumen de la información mostrada en el menú de pestañas **Informe**, al seleccionar el combo **Actividad**.

Para llegar directamente a esta pantalla haz clic en el link **más…** situado al final del listado.

Type	Name	Started	Ended	Status
	VNC Remote Takeover by panda.test	2014-10-28 16:22:53 CET	2014-10-28 16:23:13 CET	
	VNC Remote Takeover by panda.test	2014-10-28 16:21:38 CET	2014-10-28 16:22:34 CET	
	Screenshot by panda.test	2014-04-03 09:08:55 CEST	2014-04-03 09:08:55 CEST	
	Screenshot by panda.test	2014-04-03 09:06:43 CEST	2014-04-03 09:06:43 CEST	
more...				

Figura 34: registro de actividad

Rendimiento

La consola muestra tres gráficos de líneas con el uso de la CPU, memoria y disco duro. También se indica el tiempo que el dispositivo lleva en funcionamiento.

- **Consumo de disco (una línea en la gráfica por cada disco instalado en el dispositivo).**

Figura 35: gráfica de consumo de disco

- **Consumo de memoria.**

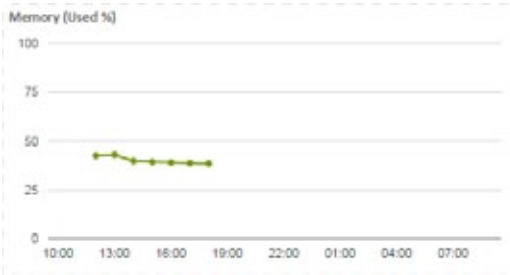


Figura 36: gráfica de consumo de memoria

- **Consumo de CPU.**

Figura 37: gráfica de consumo de CPU

- **Tiempo que el dispositivo ha estado encendido en el día.**

Figura 38: tiempo desde que el dispositivo está en funcionamiento

- **Escala**

Define el intervalo de tiempo mostrado en las gráficas:

- 24 horas
- 1 semana
- 1 mes

5.16. Gestión del consumo de los dispositivos

Panda Systems Management automatiza el seguimiento del consumo de los dispositivos administrados. Para ello, es necesaria cierta configuración inicial que, aunque en gran medida ya viene completada por defecto, puede requerir ajustes posteriores. Se recomienda afinar los valores asignados por defecto para los consumos reales de los dispositivos gestionados con el objeto de obtener el gasto más cercano a la realidad de cada país / parque informático.

El ciclo completo de la gestión del consumo se divide en tres apartados:

- Especificación del tipo de dispositivo.
- Especificación del consumo por tipo de dispositivo.
- Visualización del consumo general.

5.16.1 Especificación del tipo de dispositivo

Panda Systems Management distingue cuatro grandes grupos de dispositivos relativos al nivel de consumo:

- Desktop
- Laptop
- Server
- Others

El sistema asigna de forma automática el tipo que mejor encaje con cada dispositivo administrado, En caso de error cámbialo en el Nivel Dispositivo asociado al dispositivo, en la pestaña **Resumen**.

5.16.2 Especificación del consumo por tipo de dispositivo

Por defecto, el sistema asigna consumos distintos para un portátil, un teléfono móvil o un servidor. Estos valores son medias calculadas según equipos con configuraciones hardware típicas.

- Para cambiar los valores calculados en todas las zonas administradas: haz clic en el menú general **Ajustes,** menú de pestañas **Configuración de cuenta,** sección **Potencia Nominal** y asigna los vatios consumidos por cada tipo de dispositivo.
- Para cambiarlos los valores calculados en una zona concreta, haz clic en la pestaña **Configuración** de la zona seleccionada.

Como el coste de la electricidad varía enormemente entre países e incluso regiones, también es posible especificar el coste por Kwh.

5.16.3 Visualización del consumo general

Para obtener el consumo de cada dispositivo haz clic en la columna **Coste,** en el listado de dispositivos de la zona.

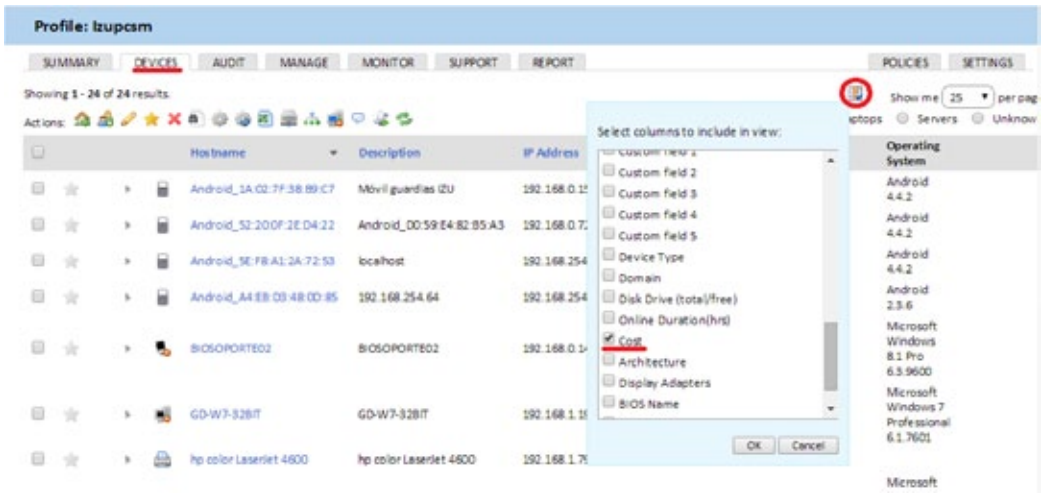


Figura 39: pantalla de edición de los campos de información mostrados en el listado de dispositivos

6. Filtros y grupos

Definición de grupos y filtros

Tipos de grupos y filtros

Grupos

Filtros

6.1. Definición de grupos y filtro

Los grupos y filtros son recursos para generar agrupaciones de dispositivos similares a las zonas, pero de una forma más ágil y dinámica. Así, mientras en la creación de una zona se consideran propiedades de los dispositivos de marcado aspecto estático, como la pertenencia a una cuenta de cliente concreta o a una delegación, los grupos y filtros están diseñados para ser modificados con agilidad atendiendo a características o criterios temporales de los dispositivos.

6.2. Tipos de grupos y filtros

Se soportan varios tipos de grupos / filtros:

- **Grupos de dispositivos de zona / Filtros de zona**: son agrupaciones creadas dentro de una zona determinada y solo pueden contener dispositivos que pertenecen a la zona seleccionada.
- **Grupos de dispositivos / Filtros de cuenta**: son agrupaciones creadas en el Nivel Cuenta y pueden contener dispositivos que pertenecen a una, varias o todas las zonas.
- **Grupos de zonas:** creados en el Nivel Cuenta, son agrupaciones de zonas completas.

Los filtros y los grupos pueden ser agrupaciones de dispositivos inter-zona: dependiendo del nivel donde se generen, pueden abarcar dispositivos de una o de varias zonas.

6.3. Grupos

Los grupos son agrupaciones de dispositivos estáticas. La pertenencia de un dispositivo a un grupo es manual por asignación directa del administrador. Un dispositivo puede pertenecer a más de un grupo.

6.4. Filtros

Los filtros son agrupaciones de dispositivos dinámicas. La pertenencia de un dispositivo a un filtro se determina de forma automática cuando el dispositivo en cuestión cumpla con las condiciones de pertenencia al filtro que se haya configurado en administrador. Un dispositivo puede pertenecer a más de un filtro.

6.4.1 Filtros predefinidos

Panda Systems Management incorpora un conjunto de filtros predefinidos que ordenan y localizan los dispositivos dados de alta en el servicio.

Los filtros listados a continuación se refieren a los dispositivos administrados por Panda Systems Management, es decir, solo muestran dispositivos previamente integrados en la consola de administración.

Los dispositivos predefinidos se agrupan en:

- **Aplicación**: contiene filtros para aplicaciones tales como Adobe Flash, Java, Microsoft Office etc.
- **Solución de Backup**: contiene filtros para soluciones de backup tales como Backup Exec, StorageCraft, Veeam.
- **Atención**: contiene filtros que muestran los dispositivos que requieren atención por parte del administrador debido a falta de memoria, antivirus deshabilitado, reinicios pendientes etc.
- **Sistema Operativo**: contiene filtros para mostrar los dispositivos gestionados según el sistema operativo instalado.
- **Rol**: contiene filtros para localizar servidores según su función.
- **Software de seguridad**: contiene filtros para filtrar dispositivos según la solución de seguridad instalada.
- **Estado**: contiene filtros para localizar dispositivos según su estado (encendido, apagado, Nodo de red etc).
- **Tipo**: contiene filtros para localizar dispositivos según su tipo (servidores ESXi, dispositivos de telefonía móvil, tablets etc)

A continuación, se ofrece una descripción detallada de cada filtro implementado.

Categoría	Nombre del filtro	Uso
Aplicación	Adobe Flash	Muestra los dispositivos con el plugin Adobe Flash instalado.
	Box.Net	Muestra los dispositivos que tienen la aplicación Box.net instalada.
	Dropbox	Muestra los dispositivos que tienen la aplicación Dropbox instalada.
	Google Chrome	Muestra los dispositivos que tienen el navegador Google Chrome instalado.
	Java	Muestra los dispositivos que tienen el framework Java instalado.
	Mozilla Firefox	Muestra los dispositivos que tienen el navegador Mozilla Firefox instalado.
	SQL Express	Muestra los dispositivos que tienen la base de datos personal Microsoft SQL Express instalada.
Solución de Backup	Acronis TrueImage	Muestra los dispositivos que tienen instalado el sistema de backup de ficheros.
	Ahsay	Muestra los dispositivos que tienen instalado el sistema de backup de ficheros.
	Backup Exec	Muestra los dispositivos que tienen instalado el sistema de backup de ficheros.

Categoría	Nombre del filtro	Uso
	StorageCraft	Muestra los dispositivos que tienen instalado el sistema de backup de ficheros.
	Veeam	Muestra los dispositivos que tienen instalado el sistema de backup de ficheros.
Atención	< 2 GB de espacio libre	Muestra los dispositivos con menos de 2 Gigabytes de espacio libre en alguno de sus discos duros.
	< 2 GB de memoria	Muestra los dispositivos con menos de 2 Gigabytes de memoria RAM libre.
	Antivirus desactivado	Muestra los dispositivos con el antivirus deshabilitado.
	Sin MS Office	Muestra los dispositivos que no tienen el paquete de ofimática Microsoft Office instalado.
	Necesita Reinicio	Muestra los dispositivos que tienen un reinicio pendiente para completar algún proceso, como la instalación de parches de seguridad o similares.
	Dispositivos suspendidos	Muestra los dispositivos que han entrado en estado de suspensión.
Sistema Operativo	Todos los Sistemas Operativos de Estaciones	Muestra los dispositivos de tipo sobremesa.
	Todos los Sistemas Operativos de Servidores	Muestra todos los dispositivos de tipo servidor.
	Apple iOS	Muestra los dispositivos con sistema operativo iOS (tablets y teléfonos móviles).
	Google Android	Muestra los dispositivos con sistema operativo Android (tablets y teléfonos móviles).
	Linux	Muestra todos los equipos con sistema operativo Linux.
	MS Win 10	Muestra los dispositivos con sistema operativo Microsoft Windows 10.
	MS Win 7	Muestra los dispositivos con sistema operativo Microsoft Windows 7.
	MS Win 8	Muestra los dispositivos con sistema operativo Microsoft Windows 8.
	MS Win Server 2003	Muestra los dispositivos con sistema operativo Microsoft Windows 2003.
	MS Win Server 2008	Muestra los dispositivos con sistema operativo Microsoft Windows 2008.
	MS Win Server 2012	Muestra los dispositivos con sistema operativo Microsoft Windows 2012.
	MS Win Server 2016	Muestra los dispositivos con sistema operativo Microsoft Windows 2016

Categoría	Nombre del filtro	Uso
	MS Win XP	Muestra los dispositivos con sistema operativo Microsoft Windows XP.
	Mac OSX	Muestra los dispositivos con sistema operativo macOS.
Rol	Servidores DHCP	Muestra los dispositivos que hacen de servidor DHCP en la red.
	Servidores DNS	Muestra los dispositivos que hacen de servidor DNS en la red.
	Controladores de Dominio	Muestra los dispositivos que hacen de servidor de dominio en la red.
	Servidores Exchange	Muestra los dispositivos que hacen de servidor de correo con Exchange en la red.
	Servidores Hyper-V	Muestra los dispositivos que hacen de host para máquinas virtuales en la red, basados en la tecnología Microsoft Hyper-V.
	Servidores web IIS	Muestra los dispositivos que hacen de servidor web con Internet Information Server en la red.
	Servidores SQL	Muestra los dispositivos Microsoft SQL Server o Microsoft SQL Server Express en la red.
	Servidores Sharepoint	Muestra los dispositivos que hacen de servidor Sharepoint en la red.
	Servidores WSUS	Muestra los dispositivos que hacen de servidor de actualizaciones WSUS en la red.
Software de seguridad	AVG	Muestra los equipos con software de seguridad instalado.
	Avira	Muestra los equipos con software de seguridad instalado.
	ESET	Muestra los equipos con software de seguridad instalado.
	McAfee	Muestra los equipos con software de seguridad instalado.
	Panda	Muestra los equipos con software de seguridad instalado.
	Sophos	Muestra los equipos con software de seguridad instalado.
	Symantec	Muestra los equipos con software de seguridad instalado.

Categoría	Nombre del filtro	Uso
	Trend Micro	Muestra los equipos con software de seguridad instalado.
	Webroot	Muestra los equipos con software de seguridad instalado.
Estado	**Visto por última vez > 30 días**	Muestra los dispositivos que no han sido contactados por un periodo superior a los 30 días.
	Nodo de red	Muestra los equipos que tiene el rol de nodo de red. Consulta el Capítulo 5 para más información sobre el rol de Nodo de red.
	Offline > 1 Week	Muestra los dispositivos apagados o no accesibles desde hace más de una semana.
	Dispositivos de sobremesa Offline	Muestra los dispositivos de tipo sobremesa apagados o no accesibles.
	Dispositivos Offline	Muestra todos los dispositivos apagados o no accesibles.
	Dispositivos Servidor Offline	Muestra los dispositivos de tipo servidor apagados o no accesibles.
	Dispositivos de sobremesa Online	Muestra los dispositivos de tipo sobremesa encendidos y accesibles.
	Dispositivos Online	Muestra todos los dispositivos encendidos y accesibles.
	Dispositivos Servidor Online	Muestra los dispositivos de tipo servidor encendidos y accesibles.
	Reinicio > 30 Días	Muestra los equipos que no han sido reinicios por un periodo superior a los 30 días.
Tipo	**Todos los Dispositivos**	Muestra todos los dispositivos gestionados por PCSM.
	Todos los Portátiles	Muestra todos los dispositivos de tipo portátil gestionados por PCSM.
	Todos los Móviles	Muestra todos los teléfonos móviles gestionados por PCSM.
	Todos los dispositivos de red	Muestra todos los dispositivos de red gestionados por PCSM. Para más información acerca de los dispositivos de red consulta el capítulo 5
	Todas las impresoras de red	Muestra todas las impresoras instaladas en la red y gestionados por PCSM.
	ESXi	Muestra los hosts ESXi (servidores ESXi) gestionados por PCSM.
	Servidores físicos	Muestra todos los servidores físicos (no virtualizados).
	Máquinas virtuales	Muestra todos los servidores virtualizados gestionados por PCSM.

Tabla 11: listado de filtros predefinidos

Los filtros predefinidos no son editables.

6.4.2 Construcción de filtros

Un filtro está formado por uno o más atributos, relacionados entre sí mediante operaciones lógicas AND / OR. Un dispositivo entrará a formar parte del filtro si cumple con los valores especificados en los atributos del filtro.

El esquema general de un filtro se compone de dos bloques:

- **Nombre del filtro:** se recomienda que sea descriptivo, indicando las características comunes de los dispositivos agrupados (p. ej. "Servidores Microsoft Exchange", "Workstations con poco espacio de disco").
- **Criterio**: selecciona los atributos que serán comprobados por cada dispositivo y su valor. Por cada atributo puedes especificar varios valores, que serán evaluados según la relación AND / OR especificada entre ellos. De la misma manera, puedes especificar varios atributos en un mismo filtro relacionados entre sí por AND / OR.

El bloque criterio se descompone en tres partes:

- **Atributo**: indica la característica del dispositivo que formará parte de la condición de pertenencia al filtro. Los principales atributos están enumerados y clasificados más abajo.
- **Condición**: establece el modo de comparación del contenido del atributo del dispositivo con el valor de referencia que establezca el administrador.
- **Valor**: contenido del atributo. Dependiendo del atributo el campo valor cambiará para permitir entradas de tipo fecha, literales, etc.

A continuación, se indican los distintos valores disponibles para cada línea de condición criterio:

Atributo	Condición	Valor
String	Está vacío – No está vacío, Contiene – No contiene, Comienza con – No comienza con, Termina con – No termina con	Cadena de caracteres. Utilizar % como comodín para representar cualquier número de caracteres
Integer	Mayor – Mayor o igual que, Menor – Menor o igual que, Entre inclusivo, Entre exclusivo	Numérico.
Binary	Enabled / Disabled	
Date	Antes – Después de, Más viejo de 30/60/90 días	Intervalo de fechas
Selección	Is a member of, is not a member of	Grupos disponibles

Tabla 12: tipos de dato para los atributos de los filtros

Para especificar diferentes valores en un mismo atributo, haz clic en el símbolo **+** situado a la derecha del campo valor. Se desplegará un nuevo control y un botón **AND / OR** que permitirá elegir la relación: dos valores relacionados con **AND** requerirán que el dispositivo examinado contenga en ese atributo un valor coincidente con los dos campos. Dos valores relacionados con **OR** requerirán que el dispositivo examinado contenga en ese atributo al menos un valor compatible con los dos campos.

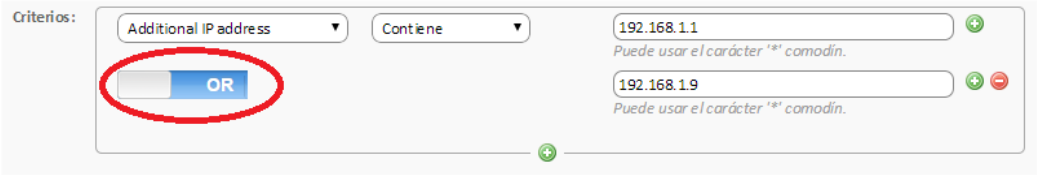


Figura 40: operación lógica OR entre dos atributos

Finalmente, para desarrollar filtros más complejos que permitan examinar varios atributos de los dispositivos añade más bloques criterio. Para ello haz clic en el símbolo **+** inferior y repite la operativa descrita anteriormente: el nuevo bloque criterio se relacionará con el anterior mediante lógica **AND / OR**.

A continuación, se detallan los atributos disponibles a la hora de confeccionar un bloque criterio:

Atributo	Descripción
Actualización de Windows (Sí/No)	Filtra los dispositivos con el motor Windows Update activado o desactivado.
Adaptador de pantalla	Filtra por el nombre, la marca y modelo de la tarjeta gráfica instalada en el dispositivo.
Adaptador de red	Filtra por la marca y modelo de la tarjeta de red instalada en el dispositivo.
Antivirus (Si / No)	Filtra los dispositivos que tienen el antivirus activado o desactivado.
Archivo del controlador del dispositivo conectado	Filtra por el campo **Archivo del controlador** de los dispositivos USB externos conectados al equipo. Para más información, consulta el Capítulo 12: Auditoria de activos.
Arquitectura	Filtra dispositivos con arquitectura 32 bits o 64 bits.
CPU	Filtra por la marca y modelo de la CPU instalada en el dispositivo.
Capacidad de disco	Filtra por el tamaño del disco duro conectado.

Atributo	Descripción
Capacidad de disco libre	Filtra por el espacio libre del disco duro conectado.
Clase	
Controlador del dispositivo conectado modificado	Filtra por el campo **Última modificación del archivo del controlador** de los dispositivos USB externos conectados al equipo. Para más información, consulta el Capítulo 12: Auditoria de activos.
Descripción	Filtra por el campo **Descripción** del dispositivo. Para más información, consulta el Capítulo 5: Dispositivos.
Descripción de la zona	Filtra por el campo **Descripción** de la zona al que pertenece el dispositivo.
Descripción del disco	Filtra por la cadena de descripción de los dispositivos de almacenamiento interno conectados al equipo.
Dirección IP	
Dirección IP adicional	Filtra por alias de IP.
Dirección IP externa	Filtra por la dirección IP con la que se conecta el dispositivo al servidor.
Dirección MAC	
Dispositivos administrados	Sin uso.
Dispositivos de OnDemand	Sin uso.
Dominio	Filtra por el dominio en redes Microsoft al que pertenece el dispositivo.
La zona es OnDemand	Sin uso.
Estado – Online/Offline	
Estado – Puerto de red OK	Sin uso.
Estado – Suspendido	
Fabricante	Empresa que ensambló el dispositivo.
Fabricante del controlador del dispositivo conectado	Filtra por el campo **Fabricante del controlador** de los dispositivos USB externos conectados al equipo. Para más información, consulta el Capítulo 12: Auditoria de activos.

Atributo	Descripción
Favorito	Filtra por los dispositivos marcados como favoritos.
Fecha de lanzamiento de BIOS	
Fecha de la última visualización	Fecha en la que el dispositivo fue visto por última vez por el servidor.
Firewall (Sí/No)	Filtra los dispositivos que tienen el cortafuegos activado o desactivado.
Grupo de dispositivos de zona	Filtra por el nombre del grupo de dispositivo de zona al que pertenece el dispositivo.
Grupos de dispositivos	Filtra por el nombre del grupo de dispositivos al que pertenece el dispositivo.
Memoria	Filtra por la cantidad de memoria instalada en el dispositivo.
Modelo	
Monitor de SNMP	Filtra por los agentes con el rol de agente de red.
Monitor / pantalla	
Necesita reinicio	Filtra por los dispositivos que tengan pendiente un reinicio para completar tareas de instalación de programas, actualización de componentes u otros.
Nombre de BIOS	
Nombre del controlador del dispositivo conectado	Filtra por el campo **Nombre del controlador** de los dispositivos USB externos conectados al equipo. Para más información, consulta el Capítulo 12: Auditoria de activos.
Nombre del dispositivo conectado	Filtra por el campo **Nombre** de los dispositivos USB externos conectados al equipo. Para más información, consulta el Capítulo 12: Auditoria de activos.
Nombre del host	
Nombre del servicio	
Nombre del parche (instalado)	Filtra por el nombre de un parche instalado.
Nombre de la zona	Filtra por el nombre de la zona a la que pertenece el dispositivo.

Atributo	Descripción
Nombre / versión del controlador del dispositivo conectado	Filtra por el campo driver **Nombre del controlador/versión del controlador** de los dispositivos USB externos conectados al equipo. Para más información, consulta el Capítulo 12: Auditoria de activos.
Número de serie	Filtra por el número de serie del dispositivo.
Paquete de software	Filtra por un paquete de software instalado en el dispositivo.
Paquete/versión de software	Paquete de software y versión instalada.
Personalizar el campo 1-10	Filtra por el contenido del campo personalizado referido (del 1 al 10). Para más información, consulta el Capítulo 5: Dispositivos.
Placa madre	Filtra por el fabricante, marca y modelo de la placa madre del dispositivo.
Puerto del dispositivo conectado	Filtra por el campo **Nombre del puerto** de los dispositivos USB externos conectados al equipo. Para más información, consulta el Capítulo 12: Auditoria de activos.
Nombre del servicio mostrado al usuario	
Service Pack	
Sistema Operativo	
Tipo de dispositivo	Filtra por el tipo de dispositivo: Desconocido, Escritorio, Portátil, Servidor, Smartphone, Tablet, Impresora, Network Device, ESXi Host
Tipo de dispositivo conectado	
Versión de BIOS	
Versión de software	Filtra por la versión de un paquete de software instalado en el equipo.
Versión del agente	
Versión del controlador del dispositivo conectado	Filtra por el campo driver versión de los dispositivos USB externos conectados al equipo. Para más información, consulta el Capítulo 12: Auditoria de activos.

Atributo	Descripción
Última auditoría	Fecha en la que se realizó la última auditoría de hardware / software en el dispositivo. Para más información, consulte el Capítulo 12: Auditoria de activos.
Ultimo reinicio	Filtra los equipos cuyo último reinicio ocurrió en periodos de tiempo determinados.
Último usuario	Filtra por el último usuario logeado en el dispositivo.

Tabla 13: listado de atributos

7. Gestión eficiente de dispositivos

Diferencias entre zonas, grupos y filtros

Enfoque general y estructura de ordenación de dispositivos

Visualización rápida de la información de los dispositivos

7.1. Introducción

La distribución en la consola de los dispositivos administrados en un MSP con múltiples cuentas de cliente o en un departamento de IT con varias delegaciones, afecta a la eficiencia de forma importante: muchos procedimientos y acciones pueden configurarse para ser ejecutadas sobre gran cantidad de dispositivos siguiendo una correcta combinación de zonas, grupos y filtros.

7.2. Diferencias entre zonas, grupos y filtros

A continuación, se describen las ventajas y limitaciones de las tres formas de agrupación soportadas.

7.2.1 Zonas

Ventajas

- Asocian una misma configuración de salida a Internet para el agente a todos los dispositivos: ahorra la configuración manual del agente dispositivo por dispositivo en local.
- Asocian información de contacto vía email para el envío de informes, alertas, tickets etc.
- Tienen acceso a la barra de pestañas y a la Barra de iconos con lo que permiten la ejecución de acciones y la visualización de listados e informes consolidados, abarcando a todos los dispositivos de la zona de forma cómoda y rápida.

Limitaciones

- Un dispositivo concreto solo puede pertenecer a una única zona.
- No es posible generar zonas dentro de zonas.

7.2.2 Grupos y filtros

Ventajas

- Los grupos / filtros permiten crear subconjuntos de dispositivos dentro de una única zona o incluso de diferentes zonas.
- Un dispositivo puede pertenecer a varios grupos / filtros.

Inconvenientes

- Los grupos / filtros tienen funcionalidad limitada ya que se pierde el acceso a la barra de pestañas, con lo que no es posible la generación de listados con información consolidada de los miembros pertenecientes al grupo o filtro.
- El acceso a los informes es limitado, es decir, solo se generan informes que contienen información de un único dispositivo.

Los grupos / filtros son a los efectos zonas dentro de zonas (tantas como queramos) pero con acceso limitado a la funcionalidad de informes consolidados y a la barra de pestañas.

7.3. Enfoque general y estructura de ordenación de dispositivos.

Se aplican las siguientes normas de carácter general:

- **Agrupa los dispositivos en zonas para separar los dispositivos de cuentas de cliente distintas.**

Las zonas no imponen ningún tipo de limitación en la generación de informes o listados consolidados y permiten aplicar configuraciones a todos los dispositivos de una zona.

- **Crea grupos de dispositivos para agrupar dispositivos de hardware / software / configuración / uso similar**

Por ejemplo, configura grupos de dispositivos para segregar dispositivos por departamentos dentro de una misma cuenta de cliente con necesidades similares (software utilizado, requisitos generales, acceso a impresoras, etc.) o con roles muy diferenciados (Servidores vs Workstations).

- **Crea filtros para buscar equipos con estados comunes dentro de una zona**

Utiliza filtros para establecer búsquedas rápidas y automáticas que permitan localizar condiciones anómalas o que caigan fuera de umbrales predeterminados (poco disco libre, poca memoria física instalada, software no permitido, etc.) de forma proactiva, o para buscar equipos con características concretas.

No se deberían utilizar de forma general filtros para agrupaciones de carácter estático.

- **Crea grupos en el Nivel Cuenta para agrupar zonas**

En el caso existir cuentas de cliente o delegaciones muy similares en las características y variedad de dispositivos, es posible agruparlas en un mismo grupo creado en el Nivel Cuenta para acelerar su gestión.

- **Asocia grupos y filtros en el Nivel Cuenta a perfiles técnicos.**

Si el tamaño del MSP es medio-alto, llegará un momento en que tenderá a la especialización de su personal técnico. De esta forma, habrá técnicos que solo administren cierto tipo de dispositivos concretos, como servidores de correo Exchange o estaciones de trabajo Windows XP, por ejemplo. Un grupo o filtro de tipo Cuenta ayuda a localizar y agrupar estos equipos sin tener que ir zona a zona en su búsqueda. Para completar el escenario descrito, crea y configura roles y nuevas cuentas de usuario, según se describe en el Capítulo 16: Cuentas de usuario y roles.

7.4. Visualización rápida de la información de los dispositivos

Para disponer de la información más relevante de los dispositivos, la consola de administración muestra listados tabulados de equipos con campos de información configurables por el administrador.

Para configurar la información mostrada en cualquier listado de dispositivos haz clic en el icono  . Este icono es accesible desde cualquier listado de dispositivos (zonas, grupos o filtros). Las opciones a elegir son las siguientes:

Campo	Descripción
UID	Identificador interno del dispositivo.
Zona	Nombre de la zona a la que pertenece el dispositivo.
Nombre del host	Nombre del dispositivo.
Descripción	
Dirección IP	Dirección IP local del dispositivo.
Suplem. IP	Alias de IP.
Ext. Dirección IP	Dirección IP del router o dispositivo que conecta a Internet al dispositivo.
Último usuario	Último usuario que hizo login en el dispositivo.
Grupo	
Creado en fecha	Fecha de alta del dispositivo en el sistema.
Última actualización	Fecha de la última vez que el servidor accedió al dispositivo.
Auditado por última vez	Fecha de la última vez que se realizó una auditoria de software y hardware. Para más información, consulta el Capítulo 12: Auditoria de activos.
Nombre de la sesión	Sin uso actualmente.
Favorito	Marca el dispositivo como favorito para un rápido acceso en los dashboards del sistema.
Modo privacidad	Modo de privacidad del dispositivo.
Versión del agente	Versión menor del agente.
Versión del agente	Versión del agente completa.
Versión de la pantalla	El dispositivo es capaz de conectar al servicio Web para la descarga del branding, componentes, actualizaciones etc.
Monitor de SNMP	El agente tiene el rol agente de red activado.
Estado	Estado (Online, Offline). El estado Online indica que el agente es capaz de conectar con el canal de control (Control Channel) para enviar los latidos (keep alives).
Modelo	
Sistema operativo	
Service Pack	
Número de serie	

Campo	Descripción
Placa madre	
CPU	Marca, modelo y velocidad de la CPU.
Memoria	Cantidad de memoria instalada.
Direcciones MAC	
Personalizar el campo 1-10	Contenido de los campos personalizados definidos. Para más información, consulta el Capítulo 11 Componentes y la ComStore.
Tipo de dispositivo	Tipo del dispositivo (estación de trabajo, portátil, Tablet, teléfono móvil, impresora, network device, ESXi host).
Dominio	Dominio Windows al que pertenece el dispositivo.
Unidad de disco (total/libre)	Tamaño total y consumido de las unidades de almacenamiento instaladas en el dispositivo.
Duración Online (horas)	
Coste	Coste asociado al dispositivo según su consumo. Para más información, consulta el Capítulo 5: Dispositivos.
Arquitectura	32 o 64 bits.
Adaptadores de pantalla	Marca y modelo de la tarjeta gráfica instalada en el dispositivo.
Nombre de BIOS	Marca y modelo de la BIOS.
Fecha de lanzamiento de BIOS	
Versión de BIOS	
Último reinicio	Fecha del ultimo reinicio del dispositivo
Necesita reinicio	Indica si el equipo requiere un reinicio para completar el proceso de instalación

Tabla 14: listado de campos disponibles en la pestaña dispositivos

Una vez configurada la vista, haz clic en el título de las columnas para establecer el criterio de ordenación que más convenga.

8. Los 8 primeros pasos para comenzar a usar Panda Systems Management

Crea y configura la primera zona

Instalación del agente

Comprueba el listado de dispositivos de la zona y filtrado básico

Inventariado de hardware, software y licencias

Gestiona los parches

Crea monitores

ComStore

Accede a los recursos de los dispositivos remotos administrados

8.1. Introducción

En este capítulo se resumen los pasos necesarios para poner en funcionamiento **Panda Systems Management** con un dispositivo gestionado basado en Windows.

8.1.1 Estado actual de la puesta en marcha de Panda Systems Management

Para determinar si se ha completado el proceso de puesta en marcha del servicio, la consola de administración muestra de forma gráfica el estado del despliegue del servicio en la red del cliente.

Para ver el estado del despliegue haz clic en el menú general **Zonas**. En la parte inferior de la ventana se muestra un asistente de tres pasos, indicado además el estado de cada uno de los pasos:

- Paso 1: despliegue del agente en los dispositivos.
- Paso 2: aplicación monitores por defecto.
- Paso 3: ejecución de auditorías, gestión de parches, configuración de políticas.

Estos tres pasos son contemplados en detalle más adelante en este mismo capítulo.

8.2. Crea y configura la primera zona

Determina si crear una nueva zona o reutilizar una ya en uso, dependiendo de los criterios de ordenación que utilices. De forma general, una nueva cuenta de cliente se corresponderá con una zona nueva.

En el menú general **Zonas** haz clic en **Nueva zona** y rellena la información necesaria, teniendo en cuenta que el campo **Descripción** podrá ser utilizado por filtros que hagan referencia al contenido de este campo.

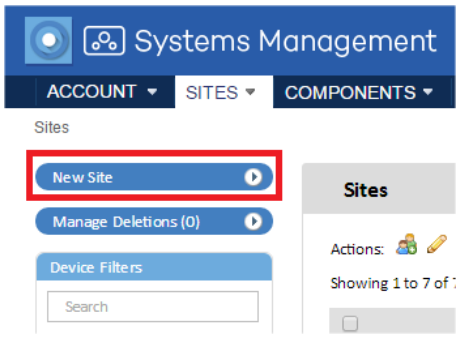


Figura 41: botón para crear una zona

Si los dispositivos de la zona requieren información adicional de Proxy HTTP para acceder a Internet, esta información puede ser suministrada aquí o más adelante.

Una vez creada la zona, configúrala a través de la pestaña **Configuración**. Esta configuración será incorporada en el agente a instalar en cada dispositivo administrable.

8.3. Instala el agente Systems Management

El agente a instalar en los dispositivos del cliente requiere cierta información básica para poder funcionar:

- La zona a la que va a pertenecer.
- La información mínima para poder acceder a Internet y conectarse con el servidor.

La zona a la que pertenecerá el agente queda automáticamente establecida al iniciar la descarga o el envío desde la propia zona. Para ello, desde el menú general **Zonas**, selecciona la zona recién creada y haz clic en el botón **Nuevo dispositivo.**

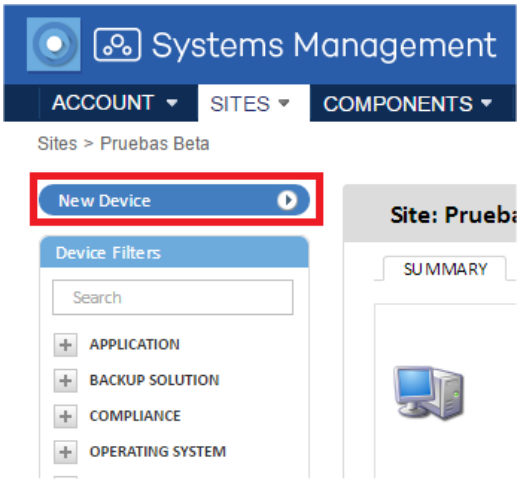


Figura 42: botón para integrar un dispositivo

La información de salida a Internet fue indicada en el paso anterior al crear la zona o en la barra de pestañas **Configuración,** de forma que el agente que se descarga ya contendrá dicha información.

El agente se descara de tres maneras:

- Envío del agente por email.
- Envío por email de la URL de descarga.
- Descarga directa.

8.4. Comprueba el listado de dispositivos de la zona y filtrado básico.

Marca los equipos como favoritos para acceder a ellos de forma rápida más adelante, ordena los listados, o fíltralos por el rol del dispositivo y dimensiona el listado para mostrar más o menos elementos.

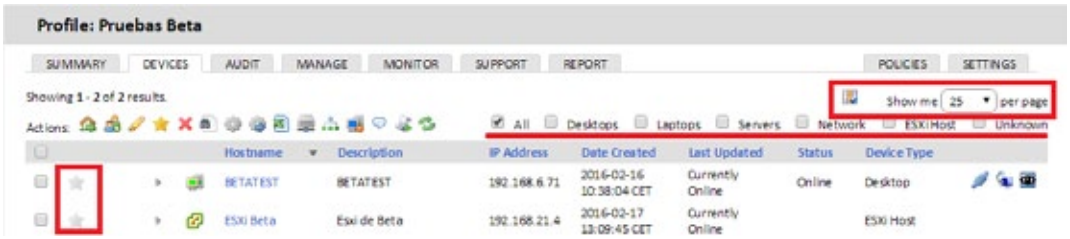


Figura 43: configuración del listado de equipos

8.5. Inventariado de hardware, software y licencias.

En la barra de pestañas **Auditoría** tienes toda la información de inventariado de los dispositivos que pertenecen a la zona. Accede desde el Nivel Dispositivo para mostrar la información relativa al dispositivo de forma más detallada. Para más información, consulta el Capítulo 12: Auditoría de Activos.

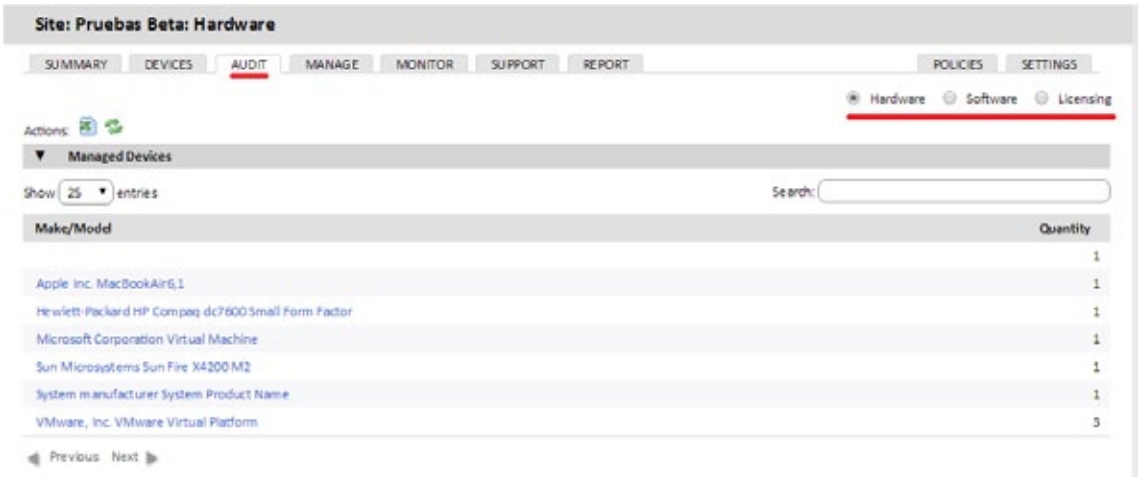


Figura 44: pantalla de inventario hardware

8.6. Gestión de parches

Desde la barra de pestañas **Administrar** aprueba los parches que no han sido instalados en los dispositivos administrados o ejecuta un rollback para desinstalarlos.

Mediante la barra de pestañas **Políticas**, aplica los parches en los dispositivos de la zona y determina el comportamiento posterior de dichos dispositivos. Crea una política de **Windows**

Update o **Gestión de parches para** configurar otros parámetros adicionales. Consulta el Capítulo 15: Gestión de parches y el Capítulo 9: Políticas.

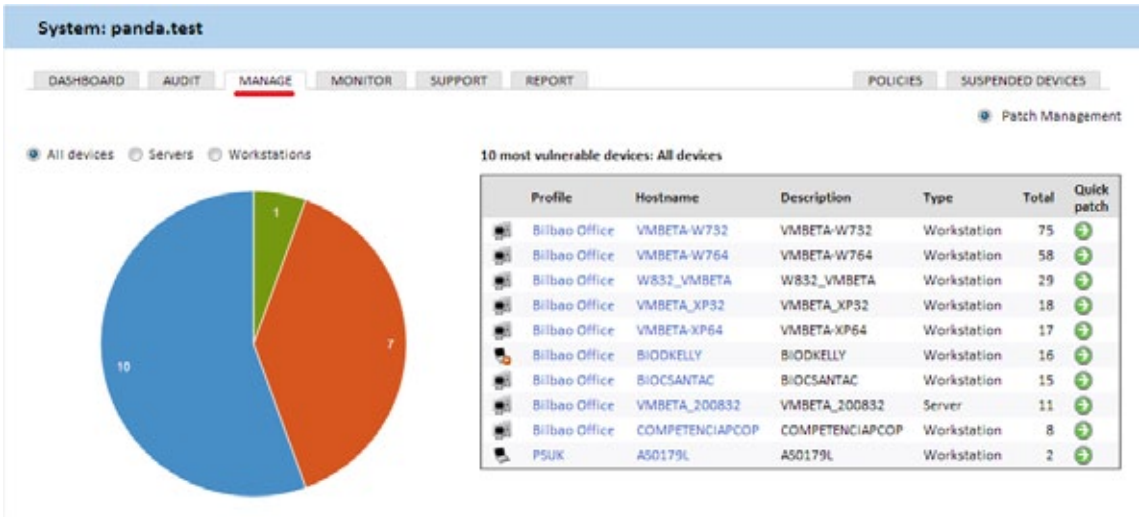


Figura 45: ventana de gestión de parches

8.7. Crea monitores

Para implementar mecanismos de monitorización en los dispositivos de la red, **Panda Systems Management** requiere la instalación y configuración de monitores. Los monitores son los componentes encargados de notificar al **Servidor PCSM** cuando los dispositivos no cumplen con ciertas condiciones establecidas durante un determinado intervalo de tiempo.

Panda Systems Management configura de forma automática ciertos monitores dependiendo del tipo de dispositivo que se haya añadido a la consola de administración. De esta manera el administrador no necesita invertir tiempo extra en configurar un conjunto básico de monitores que le muestren el estado de los dispositivos.

Además, existen monitores disponibles para su importación que permiten sacar el máximo partido desde el primer minuto.

Para añadir monitores adicionales, desde el menú general **Cuenta** o desde una zona concreta en la barra de pestañas **Políticas** haz clic en **Añadir políticas de la zona**.

En el tipo de política elige supervisión.

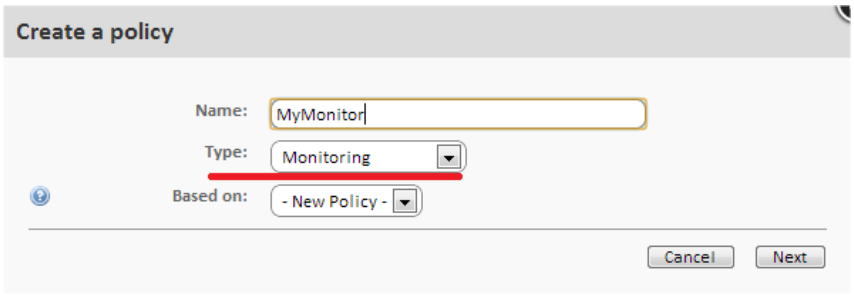


Figura 46: ventana de creación de políticas

Añade un destino (uno o varios grupos o filtros) y un monitor. Al añadir un monitor se mostrará un asistente de cuatro pasos donde especificar la configuración necesaria.

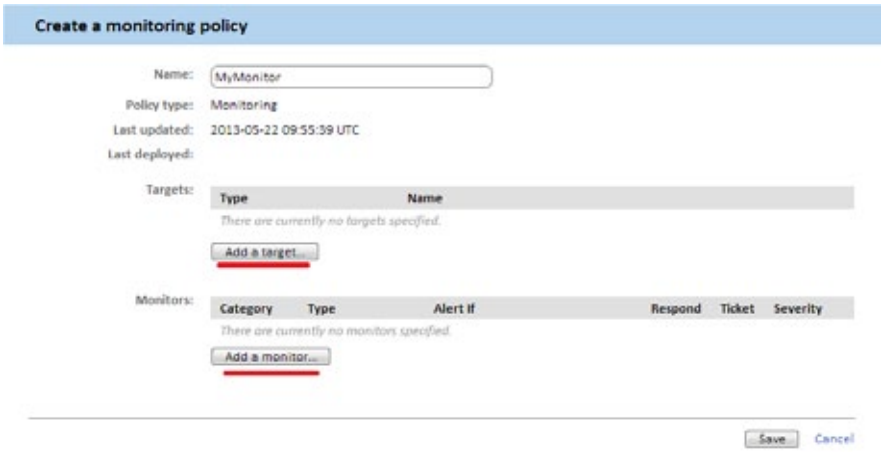


Figura 47: ventana de configuración de políticas

Para más información sobre monitores, consulta el Capítulo 10: Monitorización.

8.8. ComStore

La ComStore es un repositorio que componentes prediseñados que extiende la funcionalidad de **Panda Systems Management** y permite la instalación de software de terceros de forma centralizada.

Para utilizar un componente descárgalo de la **ComStore:** selecciona el componente y haz clic en **Comprar**. El componente se incorporará al apartado **Mis componentes**.

Todos los componentes de la ComStore son gratuitos.

Bajo **Mis componentes** en el menú general **Componentes** aparecerán los componentes ya descargados y utilizables.

Dependiendo del tipo de componente, podrá ser ejecutado como una tarea o como respuesta a una alerta generada por un monitor.

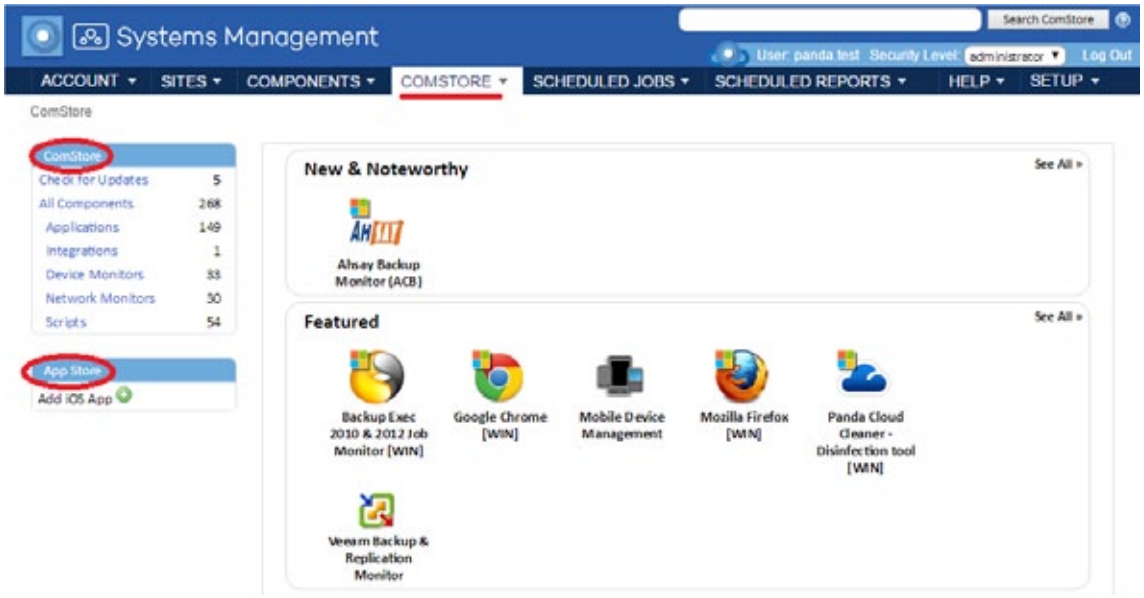


Figura 48: sección Comstore

Dentro de la zona correspondiente, en la barra de pestañas **Dispositivos** selecciona los dispositivos a los que aplicará el componente que has adquirido. A continuación, selecciona si deseas programar una tarea (**Programar una tarea**) o ejecutarlo de forma inmediata (**Ejecutar una tarea rápida**).

Para más información sobre componentes, despliegue y desarrollo consulta el Capítulo 11: Componentes y la ComStore. Para más información sobre instalación de aplicaciones en equipos Windows, Mac, Linux, tablets y móviles iOS consulta el Capítulo 13: Distribución e instalación centralizada de software. Para obtener un listado de los componentes publicados por Panda Security en la ComStore junto a una descripción y explicaciones de su uso consulta el Apéndice C

8.9. Acceso a los recursos de los dispositivos remotos administrados

A pesar de que la mayor parte de las operaciones cotidianas se pueden desempeñar desde la consola, en ocasiones es necesario acceder directamente al dispositivo.

Para acceder a un dispositivo mediante el agente PCSM:

- Instala el agente en el dispositivo del técnico que facilitará el soporte remoto.
- Selecciona la zona a la que pertenece el dispositivo.

- Haz clic en el icono  para desplegar el menú de contexto del dispositivo, o haz clic sobre el nombre del equipo y haz clic en el icono  de la pantalla **Detalles**.
- Selecciona **Conectar con dispositivo**. El agente PCSM se maximizará y se conectará de forma automática al dispositivo.
- Una vez conectado al dispositivo, quedarán accesibles todas las opciones de control y acceso remoto tanto a través de los iconos como de los menús.

Las opciones disponibles que no impiden al usuario seguir trabajando con el dispositivo son:

- **Captura de pantalla remota**: visualización rápida de mensajes de error.
- **Pestaña de servicios de Windows**: acceso a parada, arranque y reinicio de servicios sin necesidad de acceder al escritorio remoto.
- **Sesión de pantalla compartida**: escritorio remoto compartido. El usuario ve lo que el técnico está haciendo en su dispositivo.
- **Shell de comandos**: línea de comandos DOS remota.
- **Implementación del agente**: lanza el despliegue del agente PCSM en la LAN.
- **Administrador de tareas**: accede al administrador de tareas sin necesidad de conectar con el escritorio remoto.
- **Transferencia de archivos**: accede al sistema de ficheros completo del dispositivo con posibilidad de transferir ficheros entre el equipo del usuario y el del administrador, mover ficheros, crear y borrar carpetas y renombrar elementos.
- **Información de unidad**: obtiene información sobre todas las unidades locales y de red conectadas al dispositivo, con la posibilidad de añadir nuevas rutas de red o borrarlas.
- **Editor del registro**: accede a la herramienta de Regedit sin necesidad de conectar con el escritorio remoto.
- **Tareas rápidas**: lanza tareas en el dispositivo gestionado.
- **Visor de eventos**: accede al visor de sucesos sin necesidad de conectar con el escritorio remoto.
- **Wake Up**: envía al resto de dispositivos dentro del mismo segmento de LAN un "magic packet" para encenderlos remotamente.

Las opciones que interrumpen el trabajo del usuario con el dispositivo son:

- **RDP de Windows**: accede al escritorio remoto por RDP, lo que implica el cierre de la sesión del usuario.
- **ShutDown / Reboot:** reinicia del equipo.

9. Políticas

Definición de política

Creación de una política de cuenta

Administrar políticas

Distribuir políticas

Tipos de políticas

9.1. Definición de políticas

Las políticas implementan acciones específicas de gestión o resolución que se repiten a intervalos regulares durante un tiempo determinado, o actúan al producirse determinadas condiciones, en uno o varios dispositivos administrados.

Las políticas son contenedores o plantillas de configuraciones formadas por:

- **Destinos**: agrupaciones de dispositivos que se verán afectados por la política.
- **Servicios**: según el tipo de la política, el agente ejecutará una serie de acciones concretas en cada dispositivo.

Las políticas pueden crearse en los tres niveles disponibles dependiendo del número de dispositivos y su pertenencia a un mismo cliente o a varios:

- **Políticas de cuenta**: define un comportamiento aplicable a Grupos de dispositivos, Grupos de zonas o Filtros de cuenta.
- **Políticas de zona**: define un comportamiento aplicable a Filtros de zona o Grupos de dispositivos de zona.
- **Políticas de dispositivo**: define un comportamiento aplicable a un dispositivo concreto.

9.2. Creación de políticas

Para crear una política:

- Determina el ámbito o nivel de la política en función de los dispositivos que va a afectar.
- Para crear una política de cuenta haz clic en el menú general **Cuenta**, menú de pestañas **Políticas** y haz clic en el botón **Nueva política de cuenta** situado en la parte inferior de la ventana.
- Para crear una política de zona haz clic en el menú general **Zonas**, elige una de las zonas creadas, haz clic en el menú de pestañas **Políticas** y en el botón **Nueva política de zona** situado en la parte inferior de la ventana.
- Para crear una política de dispositivo haz clic en el menú general **Zonas**, elige una de las zonas creadas, selecciona el dispositivo al que se asignará la política, haz clic en la pestaña **Monitorizar** y en el botón **Añadir un monitor** situado en la parte inferior de la ventana.

En el nivel de dispositivo solo es posible añadir políticas de tipo monitor. Consulta el capítulo 10 para mas información sobre como crear una politica de tipo monitor.

- Indica el nombre de la política, su tipo y si está basada en otra política ya existente, para agilizar su creación.
- Introduce los datos necesarios para configurar la política según el tipo de política elegida. Consulta más adelante en este capítulo para conocer los tipos de políticas soportados por **Panda Systems Management**.
- Añade los grupos o filtros para configurar el destino de la política definido, dependiendo de su nivel (Cuenta, Zona, Dispositivo).

9.3. Administrar las políticas creadas

Debido a que las políticas se pueden crear en los tres niveles, puede ser difícil determinar sobré qué agrupaciones de dispositivos se está aplicando una política concreta, incluso si se están produciendo problemas de solapamiento entre varias políticas creadas en distintos niveles.

9.3.1 Gestión de políticas a nivel Cuenta

Haz clic en el menú general **Cuenta** y menú de pestañas **Políticas.** Se mostrará una ventana con todas las políticas creadas en el nivel cuenta y su información asociada:

- **Nombre**: nombre de la política.
- **Destinos**: agrupaciones de dispositivos destinatarios de la política.
- **Tipo**: clase de política, consulta más adelante en este capítulo para conocer un listado de políticas implementadas en **Panda Systems Management**.
- **Activado**: activa o desactiva la política.

Además, se incluyen cinco controles adicionales:

- **Editar modificación**: modifica la política heredada del nivel **Cuenta**. Solo se muestra en políticas de tipo Patch Management definidas en el nivel **Cuenta** y gestionadas en el nivel **Zona**. Consulta el capítulo 15 para conocer más sobre la herencia de políticas.
- **Desplegar cambios**: despliega la política a todos los dispositivos marcados como destino.
-  : permite visualizar los dispositivos que recibirán la política.
- **Activado (para esta zona)**: activa o desactiva la política en toda la zona o cuenta.
- **Borrar**  : elimina la política.

9.3.2 Dispositivos afectados por la política

Haz clic sobre el icono  para mostrar la pantalla **Asociaciones de la política** con un listado de dispositivos que cumplen con el filtro seleccionado:

- **Exclusiones de zonas**: zonas excluidas de la aplicación de la política.
- **Zonas activadas manualmente**: zonas incluidas de forma manual en la política.

- **Todos los dispositivos**: dispositivos asociados a la política.
- **Dispositivos incluidos**: dispositivos que tienen actualmente aplicada la política.
- **Dispositivos excluidos**: dispositivos actualmente excluidos de la aplicación de la política.

9.4. Distribuir políticas

Una vez creada la política, se agregará una línea en la pantalla de políticas de la zona seleccionada.

Para distribuir la política haz clic en el botón **Forzar cambios**. Con esta acción, la política será distribuida de forma inmediata en todos los dispositivos afectados, comenzando su ejecución.

9.5. Tipos de políticas

Hay ocho tipos de políticas que se resumen a continuación:

9.5.1 Agente

Determina la apariencia del agente, así como las opciones de funcionalidad que son accesibles para el usuario.

Opciones del modo privacidad

- **Activar modo privacidad**: al activar el modo privacidad se establece una confirmación para que el usuario que utiliza el dispositivo pueda aceptar o denegar los intentos de acceso remoto por parte del administrador. Con el modo de privacidad activado todas las herramientas de gestión remota de dispositivos (escritorio remoto, pantallazos, línea de comandos remota, gestión de servicios etc.) requerirán de la confirmación del usuario antes de poder ser utilizadas con éxito.

> *Si está establecido el modo de privacidad, únicamente el usuario será capaz desde retirarlo desde el menú desplegable del agente instalado en su dispositivo.*

- **Permitir conexiones cuando no hay ningún usuario que haya iniciado la sesión: c**on el modo de privacidad activado, habilita al administrador la conexión a aquellos dispositivos donde el usuario no esté presente para validar la conexión.
- **Solo solicitar permiso para Herramientas restringidas:** configura el modo de privacidad de tal manera que el cliente solo recibe solicitudes de confirmación cuando el administrador intenta acceder al escritorio remoto, bien de forma interactiva o tomando pantallazos. El resto de herramientas de gestión remota no requieren de la configuración del usuario para poder ser utilizadas por el administrador.

Opciones del servicio

- **Instalar servicio únicamente**: oculta el icono en el área de notificaciones, situada junto al reloj del sistema operativo (Windows) 

de forma que el usuario no puede acceder a las ventanas de configuración.
- **Desactivar tareas entrantes**: impide la ejecución de tareas en el dispositivo.
- **Desactivar soporte de entrada**: deshabilita el acceso remoto al dispositivo.
- **Desactivar auditorías:** los dispositivos seleccionados no envían datos de auditoría hardware / software.

Opciones de política de agentes

- **Desactivar las opciones de privacidad:** elimina el acceso del usuario a las opciones de privacidad accesibles desde el menú de opciones del agente.

> *No es posible desactivar la privacidad si ya está activada: la única forma de desactivarla es mediante las opciones del agente.*

- **Desactivar menú de configuraciones**: el usuario no puede acceder al menú contextual del agente.
- **Desactivar opción de salir**
- **Desactivar la pestaña Tickets**: desactiva la pestaña de tickets en el agente.
- **Modo de navegación Agente**: permite establecer el modo de ejecución del agente.
  - **Desactivado**.
  - **Usuario**: el agente no muestra la ventana de Soporte y por tanto impide el login para entrar en el Modo administrador.
  - **Admin**: el agente se ejecuta de forma completa.

9.5.2 ESXi

Permite crear y asignar monitores a servidores ESXi que vigilan el rendimiento, almacén de datos y la temperatura.

> *Consulta el Capítulo 10: Monitorización para obtener más información.*

9.5.3 Ventana de mantenimiento de la monitorización

Permite definir un intervalo de tiempo en el cual las alertas generadas en los dispositivos no producen notificaciones de email ni tickets.

Email y tickets son acciones de respuesta de políticas. Estas quedarán suprimidas mientras una política Ventana de mantenimiento de la monitorización esté activa, sin embargo, otras acciones de respuesta como la ejecución de componentes seguirán ejecutándose.

Esta política se utiliza cuando el departamento de IT realiza intervenciones alargadas en el tiempo sobre la infraestructura de IT; durante este tiempo el sistema de alertas puede generar ruido innecesario que no debe ser tenido en cuenta.

9.5.4 Administración de dispositivos móviles

Establece condiciones de uso de dispositivos basados en la plataforma iOS (tablets y teléfonos móviles). Con esta política es posible restringir el uso de estos dispositivos.

Consulta el Capítulo 17: Gestión de dispositivos móviles para obtener más información.

9.5.5 Supervisión

Añade procesos de monitorización de los recursos de los dispositivos.

Consulta el Capítulo 10: Monitorización para obtener más información.

9.5.6 Gestión de parches

Descarga y aplica parches de software.

Consulta el Capítulo 15: Gestión de parches para obtener más información.

9.5.7 Energía

Configura las opciones de ahorro de energía de los dispositivos que las soporten.

Figura 49: configuración de las políticas de energía

9.5.8 Actualización de Windows

Integra las opciones disponibles en un Servidor WSUS en la consola PCSM para configurar las más comunes, relativas a la Gestión de parches para sistemas Microsoft.

Consulta el Capítulo 15: Gestión de parches para obtener más información.

10. Monitorización

10.1. Introducción

La monitorización es un tipo de política dedicada a la detección de fallos en los dispositivos de los usuarios de forma desatendida. De esta manera, el administrador de IT puede configurar monitores en los dispositivos de usuario que le adviertan de situaciones anómalas y lancen de forma automática alertas o secuencias de script para resolverlas, todo ello sin intervención humana.

10.2. Composición de un monitor

Un monitor se compone de cuatro grupos de configuraciones:

- **Tipo del monitor**: indica su funcionalidad.
- **Detalles del monitor**: parámetros del monitor que describen en qué condiciones desencadenará una respuesta.
- **Respuesta**: acciones automáticas que el monitor puede desencadenar. Se soportan dos tipos de respuesta:
  - Ejecución de componentes.
  - Envío de emails.
- **Ticket**: generación de tickets (Consulta el Capítulo 14: Ticketing).

10.3. Creación manual de monitores

Al igual que las políticas, la creación manual de monitores tiene lugar en los tres niveles disponibles, dependiendo de los dispositivos que vayan a ser monitorizados:

- Desde el menú general **Cuenta**, barra de pestañas **Políticas** haz clic en **Nueva política de cuenta.**
- Desde una zona concreta en la barra de pestañas **Políticas,** haz clic en **Nueva política de zona**.
- Desde un dispositivo concreto en la barra de pestañas **Supervisar,** haz clic en el selector **Monitores.**

10.3.1 Pasos para la creación de un monitor

1 Elige el tipo de política

Al tratarse de un monitor, el tipo de política siempre será **Supervisión**

2 Añade un destino

Añade un grupo o filtro de destino y el monitor asociado.

Una política puede tener más de un monitor asociado.

Al añadir un monitor se muestra un asistente de cuatro pasos, donde se especifica la configuración necesaria.

3 Elige el tipo de monitor

Indica el tipo de monitor que se añadirá a la política según sean los recursos objeto de monitorización en el dispositivo del usuario.

Nombre del monitor	Función	Disponible en
Monitor de estado en línea	Comprueba si el dispositivo está online.	Windows, Mac, Linux, ESXi, Dispositivos de red.
Monitor de CPU	Controla el consumo de CPU.	Windows, Mac, Linux.
Monitor de memoria	Controla el consumo de memoria.	Windows, Mac, Linux.
Monitor de componentes	Lanza un componente de monitorización de la **ComStore** o diseñado por el administrador.	Windows, Mac, Linux.
Monitor de procesos	Controla el estado de un proceso concreto.	Windows, Mac, Linux.
Monitor de servicio	Controla el estado de un servicio concreto.	Windows.
Monitor de registro de eventos	Supervisa el visor de sucesos.	Windows.
Monitor de Software	Supervisa el software que se instala o desinstala del dispositivo.	Windows.
Monitor del centro de seguridad	Controla el estado del Centro de Seguridad del sistema operativo.	Windows.
Monitor de uso del disco	Controla el consumo de disco duro.	Windows.

Nombre del monitor	Función	Disponible en
Monitor del tamaño de carpeta	Controla el tamaño de ficheros y carpetas.	Windows, macOS, Linux.
Patch monitor	Controla la instalación de las actualizaciones programadas con el módulo Patch Management de Panda Systems Management.	Windows
Ping monitor	Monitoriza la conectividad de dispositivos mediante el protocolo ICMP y comprueba el buen funcionamiento de la red.	Windows
SNMP Monitor	Monitoriza dispositivos de red compatibles con el protocolo SNMP.	Windows, macOS, Linux, dispositivos de red
SNMP Throughput Monitor	Comprueba el consumo de ancho de banda en los dispositivos de la red para detectar condiciones de cargas extremas o fallos.	Dispositivos de red
WMI Monitor	Monitoriza dispositivos Windows a través del motor WMI (Windows Management Instrumentation) para acceder a contadores internos del sistema operativo, tales como memoria consumida, colas de procesos, interrupciones y muchos otros.	Windows
Windows performance monitor	Monitoriza ciertos contadores del sistema operativo asociados a procesos en ejecución para generar alertas si caen por debajo de los umbrales establecidos.	Windows
Printer monitor	Monitoriza el estado de los consumibles de la impresora, generando alertas cuando caen por debajo del umbral establecido.	Impresoras de red

Tabla 15: listado de monitores disponibles

4 Configura el monitor

Según su función, cada tipo de monitor necesita de una configuración ligeramente diferente, de modo que este paso varía según el tipo de monitor elegido.

De forma general, se requieren los siguientes datos:

- **Condiciones de generación de alertas**: configuración complementaria del monitor y condiciones que se tienen que cumplir para que desencadene una respuesta.
- **Información de las alertas**: indica la prioridad de la alerta que se generará (**Critico**, **Alto**,

Moderado, **Bajo**, **Información**).

- **Resolución automática**: indica el tiempo que tiene que transcurrir para que una alerta se considere como resuelta de forma automática.

5 Establece la respuesta del monitor

Indica la respuesta que se desencadenará cuando se alcanzan los límites definidos en el paso 4.

- **Ejecutar el siguiente componente**: se mostrarán en el desplegable los componentes importados desde **ComStore** o desarrollados por el administrador.
- **Enviar correo electrónico a los siguientes destinatarios**: permite especificar los destinatarios de los correos, el asunto, el formato y el contenido del mensaje. La casilla **Destinatarios** por defecto permite enviar los correos a las cuentas definidas en la barra de pestañas **Configuración de la zona** a la que pertenece el monitor creado y a las definidas a nivel global en el menú general **Cuenta, Ajustes**.

6 Generación de tickets

Activa la creación automática de tickets como respuesta generada por el monitor al alcanzar los límites definidos en el paso 4.

- **Usuario asignado**: asigna a un técnico los tickets que el monitor genere.
- **Gravedad**: genera el ticket con la severidad indicada.
- **Notificación de correo electrónico de ticket**: genera un mail de notificación a la cuenta de correo del técnico asignado.
- **Desactivar resolución automática de tickets**: evita que el ticket se dé por resuelto de forma automática cuando se deja de producir la alerta que lo generó.

10.4. Importar monitores de la Comstore

Para acelerar la tarea de configurar monitores para los dispositivos que forman la infraestructura IT de la organización, Panda Security ofrece a través de la Comstore más de 50 políticas de monitorización preconfiguradas y listas para ser asignadas.

Para importar una política de monitorización de la **ComStore**:

- Haz clic en el menú general **Comstore**, menú lateral **Políticas de monitorización.** Se mostrará un listado de todas las políticas disponibles.
- Haz clic en el botón **Añadir a políticas de cuenta** de las políticas que quieres importar.
- Haz clic en el botón **Añadir un destino** para agregar grupos o filtros de dispositivos que recibirán la política. Consulta el Capítulo 10 para conocer más sobre crear y monitorizar políticas.
- Haz clic en el botón **Guardar.**
- Si quieres que la política se aplique de forma inmediata, haz clic en el botón **Desplegar cambios.**

10.5. Importar y exportar una política de monitorización

10.5.1 Importar políticas de monitorización

- Haz clic en el menú general **Cuenta**, pestaña **Políticas** para importar una política en el nivel de cuenta, o haz clic en el menú general **Zonas**, selecciona una zona y haz clic en el menú de pestañas **Políticas** para importar una política en una zona determinada.
- En el listado de políticas creadas, haz clic en botón **Importar** situado en la parte inferior de la pantalla**.** Se mostrará una ventana para elegir el fichero. pcy, que contendrá la definición de la política a importar.

10.5.2 Exportar políticas de monitorización

Para exportar como un fichero de tipo Pcy una política de tipo monitor ya configurada:

- Edita la política a exportar. Para ello haz clic en su nombre.
- Haz clic en botón **Exportar** situado en la parte inferior de la pantalla**.** Se mostrará una ventana para elegir el nombre del fichero. Pcy, que contendrá la definición de la política a exportar y la ruta donde se descargará el fichero.

10.6. Monitorización de impresoras

Panda Systems Management agrega de forma automática monitores pre configurados en el momento en que los dispositivos se incorporan a la plataforma de administración. En el caso de las impresoras, al añadir a la consola un dispositivo de este tipo aparecerá un nuevo monitor en la pestaña **Políticas** de la zona.

El monitor de impresoras detecta si los consumibles instalados (papel, tóner, tintas etc.) descienden por debajo de cierto umbral configurable para poder anticipar su reposición.

10.7. Creación de monitores SNMP

Aunque no es estrictamente necesario, se recomienda al administrador familiarizarse con los conceptos básicos del protocolo SNMP (OID, MIB, NMS etc.) así como disponer de un navegador MIB para poder explorar la estructura de OIDs del dispositivo a gestionar. El navegador MIB gratuito Mibble se encuentra disponible en su página Web.

La configuración de monitores SNMP es ligeramente diferente al resto ya que requiere cumplir con una serie de condiciones asociados a la tecnología SNMP.

10.7.1 Parámetros a monitorizar

La gran mayoría de dispositivos compatibles con SNMP publican en su MIB una cantidad de información detallada de su estado, mediante la cual es posible recuperar muchos parámetros del funcionamiento del dispositivo, como, por ejemplo:

- Consumo de los recursos internos del dispositivo (memoria, almacenamiento interno, CPU etc.).
- Ancho de banda consumido.
- Temperatura interna del dispositivo.
- Información descriptiva del fabricante y dispositivo (modelo, versión, última actualización del firmware, etc.).
- Detección de errores específicos mediante códigos de error.
- Cambios en la configuración del dispositivo.
- Cambios de estado en los dispositivos: bocas activadas o desactivadas en un switch mediante STP, líneas disponibles en una centralita, etc.

Cualquier dato publicado en la MIB del dispositivo es susceptible de ser leído e interpretado por **Panda Systems Management**, si bien será necesario recurrir a la documentación del fabricante para poder localizar la información que resulte de interés. De la misma forma, es necesario conocer las unidades de medida de los datos publicados y establecer los límites que, una vez superados, servirán para determinar que el dispositivo está ante un fallo inminente y requerirá atención por parte del departamento técnico.

10.7.2 Pasos para la creación de monitores SNMP

Para monitorizar un dispositivo SNMP:

1 Prepara de los dispositivos a monitorizar

Prácticamente todos los dispositivos conectados a una red de datos pueden ser monitorizados mediante SNMP. Para ello, habilita este protocolo en la configuración del dispositivo y anota la Comunidad a la que pertenece (por defecto suele ser *Public*)

En algunos dispositivos también es necesario configurar la versión del protocolo SNMP que se va a utilizar (v1/v2) y las direcciones IP desde donde el dispositivo monitorizado recibirá las peticiones SNMP. En este caso, la dirección IP será la del dispositivo con un Agente **Systems Management** instalado y designado como Nodo de red.

Una vez activado el soporte SNMP en el dispositivo a monitorizar determina qué OIDs será necesario supervisar. Los dispositivos compatibles con SNMP vuelcan periódicamente información de su estado interno en la estructura MIB. De esta manera, es necesario consultar la documentación del proveedor para conocer los nodos OID de la estructura MIB que contienen la información y anotarlos.

Otra forma de obtener los nodos OID es navegar la estructura MIB con el navegador Mibble o un software equivalente.

2 Designa un dispositivo con un Agente Systems Management instalado como Nodo de red

Consulta el capítulo 5 Dispositivos para obtener información acerca de cómo designar a un agente el rol de Nodo de red.

Se recomienda testear la comunicación en el puerto 161 para los protocolos TCP y UDP entre el agente con el rol Nodo de red y el dispositivo a monitorizar, en ambas direcciones.

3 Agrega el dispositivo de red a la Consola de administración

Consulta el capítulo 5 Dispositivos para más información sobre como añadir a la consola de administración dispositivos no compatibles con la instalación del **Agente Systems Management.**

4 Crea una política de monitorización SNMP

Las OIDs que **Panda Systems Management** leerá del dispositivo se establecen mediante monitores SNMP creados y configurados por el administrador, o mediante políticas ya publicadas en la **ComStore**.

Para crear una política de monitorización SNMP:

- Determina el nivel de la política a crear (Cuenta, Zona, Dispositivo).
- Haz clic en el menú de pestañas **Políticas** asociado al nivel elegido (Cuenta o Zona). Para crear un monitor en el nivel Dispositivo haz clic en el menú de pestañas **Monitorizar** y elige **Monitores** en el botón de selección situado arriba a la derecha de la ventana**.**
- Haz clic en el botón **Nueva política de cuenta** (nivel Cuenta)**, Nueva política de zona** (Nivel Zona) o **Añadir un monitor (Nivel Dispositivo)**
- Introduce un nombre de política y elige en el desplegable **Monitorización.**
- Si se trata de una política de zona o de cuenta haz clic en el botón **Añadir un destino** para definir el rango de aplicación de la política.
- Haz clic en el botón **Añadir un monitor** y selecciona **Monitor SNMP**. Se mostrará el asistente de configuración.
- Indica en el campo **OID SNMP del objeto a monitorizar** la cadena OID que se corresponde al parámetro del dispositivo a monitorizar.
- En **Configuración de las alertas** indica las condiciones que se tienen que cumplir para considerar que el dispositivo está funcionando de forma errónea. Para controlar que el dispositivo no esté respondiendo a las peticiones de SNMP activa la casilla **Genera alerta si el OID no responde.**
- En **Transformar resultado** establece correspondencias entre los valores que envía el dispositivo al servidor Systems Management y cadenas de texto o datos numéricos que serán mostrados en la consola de administración. Las alertas serán generadas tomando como referencia los valores originales, pero en la consola PCSM se mostrarán los datos transformados para facilitar su lectura.

- Para facilitar la lectura de los resultados, indica el tipo de formato del dato recogido en **Formato de datos**.
- En **Información de las alertas** indica la importancia de la alerta.
- En **Resolución automática** indica si la alerta se resolverá de forma automática transcurrido un intervalo de tiempo a definir.

5 Importa una política de monitorización SNMP (opcional)

En la **ComStore** se incluyen políticas para monitorizar los dispositivos de red más comunes. Para utilizar uno de estos componentes:

- Haz clic en el menú general **Comstore**, **Políticas de monitorización**.
- Haz clic en el botón **Añadir a políticas de cuenta** asociada a la política seleccionada.
- Configura la política en la ventana mostrada (destinatario de la política y configuración de otros parámetros del monitor).

Los componentes SNMP de Panda Systems Management permiten leer el estado interno de los dispositivos administrados no compatibles con el Agente. No se soporta la escritura en la MIB de los dispositivos o la recepción de traps SNMP.

10.8. Creación de monitores ESXi

Los servidores ESXi requieren un tipo de monitor específico y diferente al usado para monitorizar dispositivos compatibles con el Agente PCSM.

10.8.1 Pasos para la creación de un monitor ESXi

1 Elige el tipo de política ESXi

La creación de políticas ESXi está soportada desde el Nivel Cuenta y el Nivel Zona. No es posible crear una política ESXi desde el Nivel Dispositivo.

2 Añade un destino

Selecciona los grupos o filtros de dispositivos que recibirán el monitor, y después el tipo de monitor que quieres añadir a la política.

Al añadir un monitor se mostrará un asistente de cuatro pasos donde se especifica la configuración necesaria.

3 Elige el tipo de monitor

Indica el tipo de monitor que se añadirá a la política según sean los recursos objeto de monitorización en el servidor ESXi.

Nombre del Monitor	Función
Monitor de CPU de ESXi	Controla el consumo de CPU del servidor ESXi.
Monitor de memoria de ESXi	Controla el consumo de memoria del servidor ESXi.
Monitor de almacén de datos de ESXi	Controla el consumo de espacio en los diferentes almacenes de datos del servidor ESXi.
Monitor de sensor de temperatura de ESXi	Controla la temperatura del servidor ESXi.
Monitor de ventilador de ESXi	Controla el correcto funcionamiento de los ventiladores del servidor.
Monitor de estado del disco de ESXi	Controla el buen funcionamiento de los discos duros instalados y los fallos del sistema RAID. Este monitor requiere proveedores CIM para su funcionamiento.
Monitor de fuente de alimentación de ESXi	Controla el buen funcionamiento de la fuente de alimentación del servidor ESXi.
Monitor de estado Online	Comprueba el estado del servidor ESXi.

Tabla 16: listado de monitores compatibles con servidores ESXi

4 Configura el monitor

La configuración de un monitor ESXi es equivalente a la empleada con dispositivos compatibles con el Agente PCSM, mostrada anteriormente en este mismo capítulo.

5 Establece la respuesta del monitor

La configuración de la respuesta de un monitor ESXi es equivalente a la empleada con dispositivos compatibles con el Agente PCSM, mostrada anteriormente en este mismo capítulo.

> ***No se puede ejecutar un componente de la ComStore como respuesta a un evento generado por un monitor ESXi.***

6 Generación de tickets

La generación de tickets es equivalente a la mostrada en dispositivos compatibles con el Agente PCSM, mostrada anteriormente en este mismo capítulo.

11. Componentes y la ComStore

11.1. Definición de componente

Los componentes son extensiones de la plataforma **Panda Systems Management** que añaden funcionalidades adicionales de monitorización y resolución de problemas al agente PCSM.

Según su autoría, los componentes se dividen en dos tipos:

- Componentes desarrollados por el administrador o equipo de IT en la empresa que utiliza **Panda Systems Management** como herramienta de gestión y resolución remota de incidencias.
- Componentes desarrollados por **Panda Security** y ofrecidos a todos los clientes de forma gratuita a través de la ComStore.

11.1.1 Componentes desarrollados por el administrador

Se dividen en tres tipos según su objetivo, comportamiento y forma de ejecución:

- **Aplicaciones**

Estos componentes facilitan el despliegue de software en la red del cliente. Para más información, consulta el Capítulo 13: Distribución e instalación centralizada de software.

Se trata de scripts que se ejecutan por lo general una única vez o de forma puntual y pueden llevar asociados ficheros externos, que en el caso de componentes de instalación se trataría del propio software a instalar en el dispositivo del usuario.

- **Monitores**

Las políticas de tipo monitor llevan asociado siempre un componente que es el que realiza la monitorización propiamente dicha en el dispositivo del usuario. **Panda Systems Management** incorpora de base varios monitores que controlan muchos aspectos del dispositivo, como puede ser el consumo de CPU o de disco duro; sin embargo, es posible que el administrador requiera controlar algún aspecto que no esté cubierto inicialmente por la plataforma. En este caso será necesario añadir un componente de tipo monitor a la política.

- **Scripts**

Son pequeños programas, desarrollados en lenguaje de script, que se ejecutan en el dispositivo del cliente de forma puntual a través de una tarea o periódicamente según la programación indicada en el programador de tareas.

A continuación, se incluye una tabla a modo de resumen con los tipos de componentes desarrollados por el administrador:

Tipo de componente	Se ejecuta desde	Se ejecuta cada	Objetivo
Aplicaciones	Tarea rápida o tarea programada.	En el momento o cuando se indique en el calendario.	Despliegue e instalación de software centralizada. Para más información, consulta el Capítulo 13: Distribución e instalación centralizada de software.
Monitores	Política de zona o Política de cuenta.	60 segundos (fijo).	Monitorización de dispositivos.
Scripts	Tarea rápida o tarea programada.	En el momento o cuando se indique en el calendario.	Ejecución de aplicaciones desarrolladas por el administrador.

Tabla 17: listado de tipos de componentes

Monitores, aplicaciones y scripts son prácticamente idénticos en lo que a estructura interna se refiere. El tipo de componente únicamente determina cómo se integra en la consola PCSM. De esta manera, en la creación de una tarea solo se listarán los componentes de tipo script o aplicación, y en la creación de una política de tipo monitor solo aparecerán los componentes de tipo monitor creados por el administrador.

11.1.2 Componentes desarrollados por Panda Security: ComStore

ComStore es un canal de publicación de componentes desarrollados y certificados por **Panda Security** para los usuarios de **Panda Systems Management.** El objetivo de la **ComStore** es facilitar el acceso a los componentes y su posterior integración en el espacio de trabajo del equipo de IT.

Todos los componentes publicados en la ComStore son gratuitos y se ofrecen sin ningún tipo de limitación a los clientes de Panda Systems Management.

11.2. Uso de componentes en la plataforma

11.2.1 Integración de componentes en la plataforma

Para que un componente pueda ser utilizado por el administrador, tiene que ser incorporado en la plataforma **Panda Systems Management**.

Agregar un componente desde la ComStore

En el menú general **ComStore** se encuentra el repositorio de componentes desarrollados y certificados por **Panda Security** disponibles para todos los clientes de **Panda Systems Management**.

Para añadir un componente de la **ComStore** a la **Lista de Componentes:**

- Haz clic en el componente. Se mostrará una ventana con su descripción, fecha de publicación, valoración y comentarios de otros administradores que han usado ese componente.
- Haz clic en el botón **Comprar** y el componente se añadirá a la **Lista de Componentes**.

Búsqueda de componentes en la ComStore

La búsqueda de componentes se realiza mediante el panel de la izquierda donde quedan clasificados los componentes que **Panda Security** añade a la **ComStore** de forma equivalente a como se clasifican en la **Lista de Componentes** de la ventana **Componentes**. Además, se ofrece una herramienta de búsqueda en la parte superior derecha con la cual el administrador puede buscar por el nombre del componente.

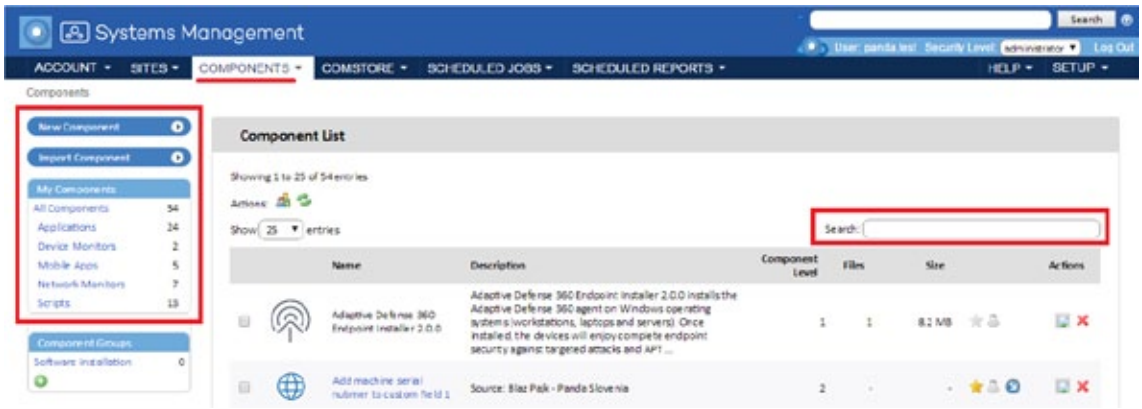


Figura 50: herramientas de búsqueda de componentes

Importar un componente

Haz clic en **Añadir componente** en el menú general **Componentes.**

Únicamente se admiten componentes exportados previamente por la consola PCSM. Para exportar un componente a disco es necesario hacer clic en el icono de la flecha del listado de componentes.

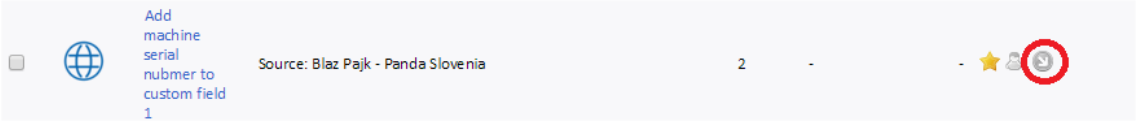


Figura 51: icono para exportar una componente

Clasificación y ordenación de los componentes integrados

Haz clic en el menú general **Componentes** para ver los componentes que el administrador ha incorporado a la plataforma.

En la zona **Mis componentes** se clasifican de forma automática los componentes ya incorporados según su funcionalidad en seis categorías:

- Todos los componentes
- Aplicaciones
- Aplicaciones administradas
- Extensiones
- Monitores
- Scripts

Además, el administrador tiene la posibilidad de crear nuevos grupos de componentes con la herramienta de agrupación de componentes situada debajo de la **Lista de Componentes.**

Figura 52: creación de nuevos grupos de componentes

Para crear un grupo de componentes:

- Haz clic en el menú general **Componentes**.
- Haz clic en el icono para mostrar una ventana donde dar un nombre al grupo.
- Indica un nombre y haz clic en el botón **Guardar**
- Selecciona los componentes que quieres agrupar y haz clic en el icono
- Se mostrará una ventana donde se listan los grupos de componentes creados previamente. Elige un grupo para añadir los componentes seleccionados.

Actualización de componentes.

Periódicamente, **Panda Security** distribuye actualizaciones de los componentes publicados en la ComStore. Estas actualizaciones se agrupan en la sección **Buscar Actualizaciones** de la ComStore.

Esta sección muestra todos los componentes de la **ComStore** que han sido actualizados desde que el administrador de la red los integró en **Mis componentes**. Haz clic en el botón **Actualizar todo** para actualizar la versión de los componentes añadidos en **Mis componentes.**

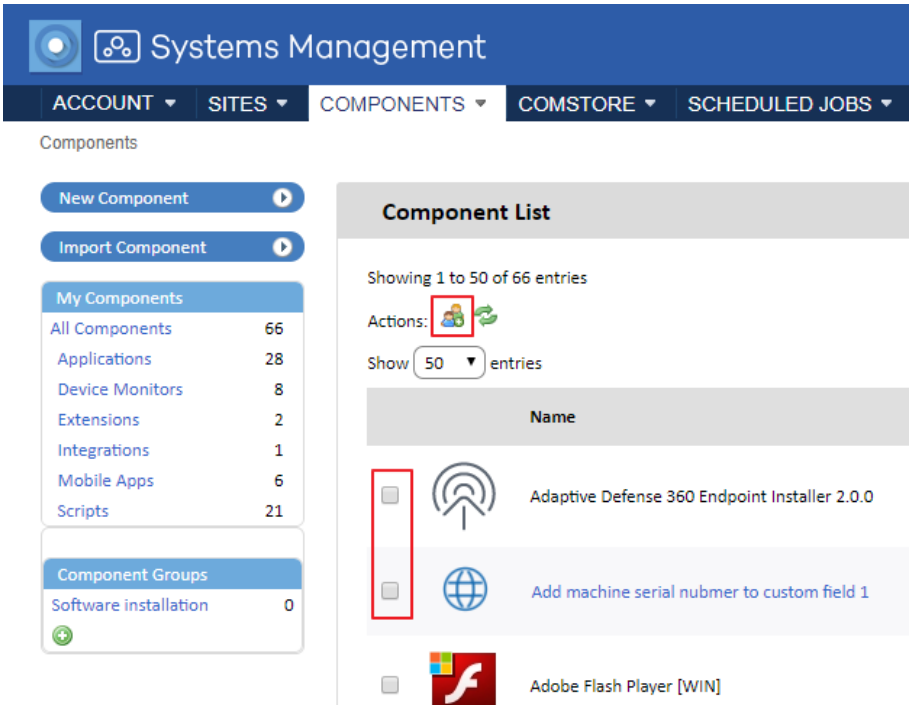


Figura 53: agrega componentes a un grupo

La opción Buscar Actualizaciones, libera al administrador de la tarea de buscar manualmente los componentes que integró desde la ComStore para comprobar si han sido actualizados. Actualizar componentes únicamente actualiza los componentes en Mis componentes, no los despliega de forma automática en los dispositivos del cliente. Para desplegar las actualizaciones, es necesario ejecutar una tarea inmediata o una tarea programada.

Adicionalmente, los administradores pueden recibir un correo semanal informativo con una lista de todos los componentes publicados en la ComStore desde el ultimo envío del correo, así como de las actualizaciones de los componentes que aparezcan en la sección Mis Componentes.

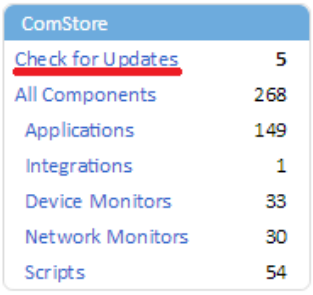


Figura 54: actualización de componentes global

Para habilitar el envío de este correo ve al menú general Ajustes, Configuración de cuenta y habilita Componentes de la ComStore en Destinatarios de correo.

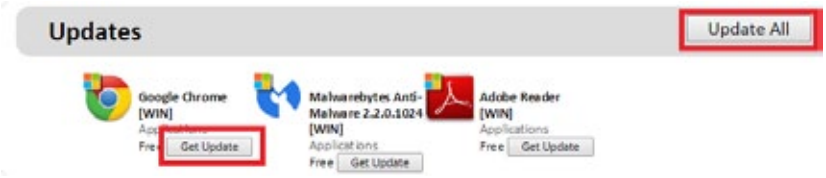


Figura 55: actualización de componentes individual

11.2.2 Lanzamiento de componentes desde una tarea rápida

Los componentes de tipo Script o Aplicación incorporados a la consola PCSM pueden ser lanzados desde una tarea rápida. Las tareas rápidas son tareas que se lanzan en los dispositivos de la red de forma puntual y en el momento.

Para que los componentes integrados en **Panda Systems Management** puedan ser ejecutados como tareas rápidas:

- Haz clic en el menú general **Componentes**.
- En el listado de componentes integrados, haz clic en el icono del componente.

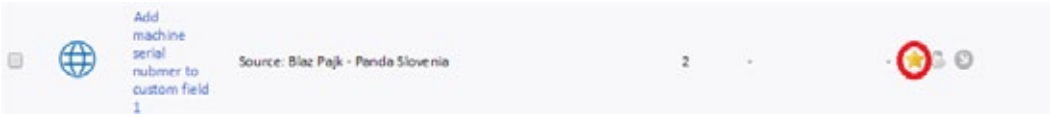


Figura 56: activación de un componente ya integrado

De esta forma, el administrador puede agregar múltiples componentes a su espacio de trabajo, pero activar solo aquellos que considere oportuno.

Para configurar una tarea rápida:

- Selecciona los equipos sobre los cuales será lanzado y haz clic en el icono accesible desde la Barra de iconos.
- El icono de tarea rápida se encuentra disponible en la Barra de iconos del Nivel Cuenta, en el Nivel Zona y en el Nivel Dispositivo. De esta forma, es posible lanzar una tarea rápida a todos los dispositivos de uno o más zonas, a varios equipos de una misma zona o en un único dispositivo, respectivamente.
- Selecciona del desplegable el componente a ejecutar. Solo se mostrarán aquellos componentes que han sido previamente activados mediante el icono .

Pestaña Tareas Programadas

Una vez lanzada la tarea rápida, se podrá recoger el resultado desde la pestaña **Tareas Programadas**, donde se muestran tanto las tareas activas como las tareas completadas.

Tareas activas

Muestra una lista de todas las tareas que están pendientes de ejecución. Se muestra también una barra de herramientas que permite el filtrado de las tareas mostradas.

Tareas completadas

Muestra todas las tareas completadas junto a un código de error que permite conocer el resultado de la tarea.

11.2.3 Lanzamiento de componentes desde una tarea programada

Las tareas programadas son equivalentes a las tareas rápidas, excepto por su ejecución retrasada en el tiempo y/o repetitiva. De esta manera, es necesario indicar información adicional en la creación de la tarea, como, por ejemplo, cuándo será lanzado o en qué periodo, cuántas veces se tiene que repetir antes de que la tarea programada se dé por concluida, etc.

Para configurar una tarea programada:

- Desde la Barra de iconos del Nivel Cuenta, Zona o Dispositivo apropiado haz clic en el icono de tarea programada  .
- Indica la configuración completa de la tarea:
  - Ciclo de ejecuciones.
  - Selección del componente.
  - Vencimiento de la tarea.
  - Alertas.
  - Envío por correo de la salida de la tarea programada.

Ciclo de ejecuciones

Para establecer el ciclo de ejecuciones haz clic en **Cronograma - Hacer clic**. Dependiendo del tipo de repetición elegida (diariamente, semanalmente, etc.) en el cuadro de la derecha se habilitarán nuevas opciones para detallar con exactitud las fechas de ejecución.

Selección del componente

Haz clic en el link **Añadir componente** para seleccionar el componente a ejecutar. Solo se mostrarán los componentes que han sido activados previamente mediante el icono  .

Vencimiento de la tarea

indica la fecha en la cual la tarea deja de repetirse y se da por concluido.

Además, permite establecer el requisito previo de tener abierta una sesión interactiva en los dispositivos afectados por la tarea programada para su ejecución.

Alertas

Para configurar la generación de alertas si se cumple alguna de las condiciones indicadas, haz clic en las casillas apropiadas. En el apartado **Destinatarios de la tarea** se pueden indicar las direcciones de correo adicionales que recibirán las alertas.

Envío por correo de la salida de la tarea programada

Envía un correo electrónico a las cuentas definidas en la configuración de la cuenta y de la zona con el código de error devuelvo por la tarea programada.

Consulta el capítulo 3 para más información sobre la configuración de cuenta y zona

11.3. Desarrollo de componentes

El desarrollo de componentes permite al administrador crear nuevos procesos que se ejecutan en los dispositivos de los usuarios y que añaden funcionalidad extra a la plataforma **Panda Systems Management**.

Aunque por defecto **Panda Systems Management** ofrece el repositorio de componentes **ComStore** que extiende sus funcionalidades de base, es posible que sea necesario desarrollar componentes específicos para realizar tareas muy concretas en los dispositivos del usuario, o extender la capacidad de monitorización ofrecida a aquellos dispositivos que no soporten la instalación de un agente **Systems Management**.

De este modo, **Panda Systems Management** se presenta como una plataforma de gestión y monitorización remota extensible, que se adapta muy fácilmente a las necesidades particulares de cada cliente.

11.3.1 Requisitos necesarios para el desarrollo de componentes

Para el desarrollo de componentes de carácter general, se necesitan conocimientos básicos de programación en uno de los lenguajes de scripting soportados:

Lenguaje	Incluido de serie en	Proveedor
Batch	Todas las versiones de Windows	Microsoft
Visual Basic Script	Windows 98 y superiores Windows NT 4.0 Option Pack y superiores	Microsoft

JavaScript (Jscript)	Windows 98 y superiores Windows NT 4.0 Option Pack y superiores	Microsoft
Powershell	Windows 7	Microsoft
Python	macOS 10.3 (Panther)	Python Software Foundation
Ruby	Ninguno	Yukihiro Matsumoto
Groovy	Ninguno	Pivotal & Groovy Community
Unix (Linux, Mac OSX)	Linux, Mac OSX	Variable

Tabla 18: listado de lenguajes soportados en el desarrollo de componentes

Además, es necesario que el intérprete asociado al lenguaje de scripting elegido se encuentre instalado y funcionando en el dispositivo del usuario.

Algunos intérpretes como Python o Groovy requieren de su instalación, por lo que el funcionamiento de componentes escritos en estos lenguajes no está garantizado en equipos Windows recién instalados.

Como paso previo a la ejecución de un componente desarrollado en un lenguaje no soportado directamente por el dispositivo del usuario, se recomienda ejecutar una tarea de distribución automática del intérprete. La distribución de software se trata en el Capítulo 13: Distribución e instalación centralizada de software.

11.4. Creación de un componente de tipo monitor

11.4.1 Presentación y objetivo del componente

A continuación, se detallan los pasos para crear un Monitor y distribuirlo en los dispositivos de una zona concreta.

El objetivo del componente es monitorizar de forma fácil y sencilla la cuarentena del producto de seguridad **Panda Endpoint Protection**. La cuarentena almacena los ficheros sospechosos de ser malware y también los ficheros detectados como virus, por esta razón resulta de interés para el administrador saber cuántos elementos hay en cuarentena en todo momento.

El ejemplo muestra además lo simple que resulta adaptar e integrar nuevos monitores para otras soluciones software.

A continuación, se muestra un resumen de las características del componente.

Dispositivos afectados	Todos los dispositivos Windows 7 de la zona Home.
Lenguaje del script	Visual Basic Script
Periodicidad del envío de información	Cada 10 minutos se notifica si los elementos de la cuarentena se incrementaron.
Acciones de Panda Systems Management	Envío de correo con el resultado de la monitorización al administrador. Generación de alerta automática.

Tabla 19: características del componente a desarrollar

Uno de los problemas a afrontar es que, si bien el agente ejecutará el script cada 60 segundos de forma automática, éste solo enviará información cada 10 minutos.

11.4.2 Elementos necesarios

Para seguir este ejemplo, es necesaria una licencia de **Panda Endpoint Protection** o **Panda Adaptive Defense 360** y el agente instalado en un dispositivo, aunque, dado que los elementos introducidos en cuarentena por **Panda Endpoint Protection / Panda Adaptive Defense 360** son ficheros en una carpeta concreta del dispositivo, en este ejemplo puede usarse con cualquier otra carpeta del sistema.

Panda Endpoint Protection es una solución Cloud de seguridad, integral y fácil de utilizar que aprovecha todo el potencial de la Inteligencia Colectiva para proporcionar máxima protección en tiempo real contra el spam y las amenazas conocidas a PCs, servidores, portátiles y servidores Exchange

El componente está desarrollado en Visual Basic Script y por tanto necesitará el intérprete `Wscript.exe` o `Cscript.exe` instalado previamente en el dispositivo del usuario. Este intérprete está incluido de serie en todos los sistemas Windows.

11.4.3 Protocolo de comunicación entre el componente y el Servidor

Prácticamente todos los componentes van a necesitar información del servidor y enviar de vuelta el resultado de su ejecución. El servidor PCSM y el componente se comunican a través de ciertas variables de entorno creadas en el dispositivo. El propio agente PCSM crea estas variables de forma automática al lanzar un componente, aunque también es usual que sea el propio script el que cree variables de entorno de forma manual para el envío de respuestas al servidor, que recogerá e incorporará a la consola.

En este caso se requerirán tres variables de entorno.

Nombre Variable	Dirección	Objetivo
PCOP_PATH	**Lectura**	El script recupera del servidor la ruta donde Panda Endpoint Protection almacena la cuarentena en el dispositivo de cada usuario.
Result	**Escritura**	Envío de datos al servidor cada 10 minutos por la salida estándar.
Errorlevel	**Escritura**	Código de error del script. Si es 0 el Servidor interpreta la monitorización como correcta y no recoge datos de la salida estándar. Si es 1 **Panda Systems Management** interpreta la monitorización como errónea, recoge los datos de la salida estándar (variable `Result`) y los procesa.

Tabla 20: variables de entorno requeridas

La configuración necesaria para ejecutar el componente en el dispositivo del cliente será la ruta de la carpeta a monitorizar. Esta ruta podría ir fijada en el código fuente del script, pero en este ejemplo se tomarán los valores que el administrador haya indicado en la consola; de esta manera, se añade un mayor grado de flexibilidad al componente.

El `Errorlevel` le indicará al servidor si tiene que procesar la respuesta del script (variable `Result`) o no: si el número de ficheros en cuarentena no ha variado o es menor (vaciado de cuarentena), se enviará un `Errorlevel 0`. Por el contrario, si el número de ficheros se ha incrementado, entonces se enviará un 1 y se escribirá en la salida estándar (variable `Result`) cierta información. Para que el servidor interprete correctamente la salida estándar y pueda extraer el contenido de la variable `Result` del componente, hay que adaptarse al siguiente formato:

```
Linea 1: <-Start Result->
Linea 2: Result=(datos a enviar)
Linea 3: <-End Result->
```

Si el lenguaje de script elegido es Batch, es necesario añadir el símbolo ^ delante de cada carácter "<" o ">". Por ejemplo: ^<-Start Result-^>.

`Result` será la variable de donde el servidor extraerá los datos al terminar la ejecución del componente. El string que quede a la derecha del "=" es el contenido que el servidor almacenará y procesará.

11.4.4 Esquema de funcionamiento general.

1 Carga del componente de tipo monitor en la plataforma Panda Systems Management.

- En el menú general **Componentes**, haz clic en **Añadir Componente**.
- Selecciona **Monitores** en la categoría del script.

- Selecciona en la sección **script** el lenguaje de scripting a utilizar, en este ejemplo VBScript.

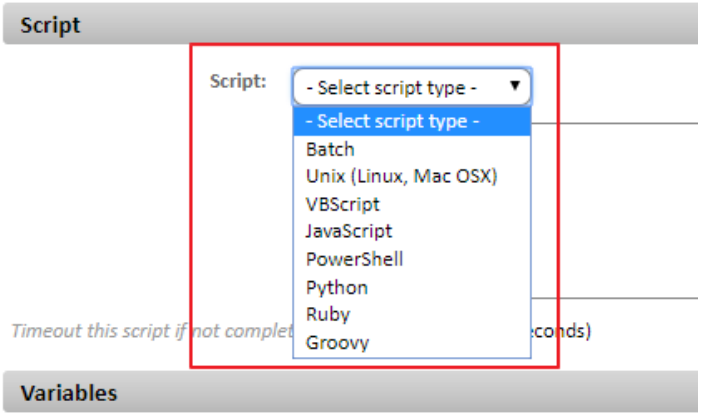


Figura 57: listado de motores de script compatibles con Panda Systems Management

- Establece el tiempo máximo de ejecución del componente. Pasado ese tiempo, el agente interrumpirá su ejecución.

> ***Se recomienda desarrollar componentes muy ligeros, que tarden muy poco tiempo en ejecutarse.***

- Establece las variables de entrada y salida, en este ejemplo `PCOP_PATH` contendrá la ruta donde se encuentra la carpeta de cuarentena de **Panda Endpoint Protection**. `Result` contendrá la salida del script.

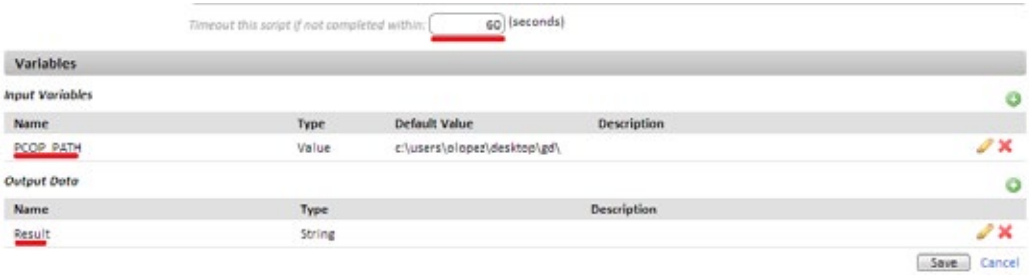


Figura 58: variables de entrada y salida del componente

- Haz clic en **Salvar** para agregar el componente al repositorio.

2 Distribución del monitor mediante políticas de cuenta o políticas de zona

- En el caso del desarrollo de un monitor, es necesaria la creación de una política de zona o política de cuenta de tipo **Supervisión**.

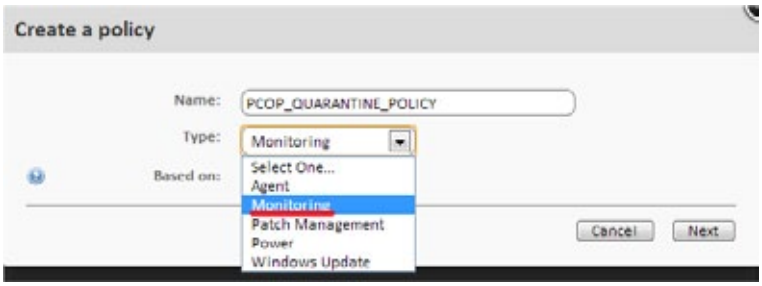


Figura 59: selección del tipo de politica Supervisión

- Añade el destino Windows 7 y un monitor de tipo **Monitor de Componentes**.

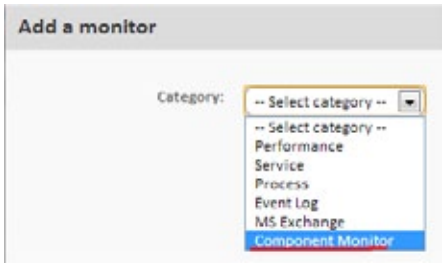


Figura 60: selección del tipo de monitor

- Selecciona el componente recién creado y salva.

Figura 61: selección del componente previamente desarrollado

- Indica la severidad de la alerta que **Panda Systems Management** creará cuando el monitor devuelva una condición de error y si esta alerta se auto resuelve por sí misma al cabo de un tiempo o, por el contrario, se resuelve de forma manual por el administrador (N/A).
- Para que el servidor genere un correo cuando se detecten nuevos elementos en la cuarentena, define una respuesta de tipo email con la dirección de correo del destinatario. El contenido de la variable de respuesta `Result` será copiada en el correo que se envía al administrador.

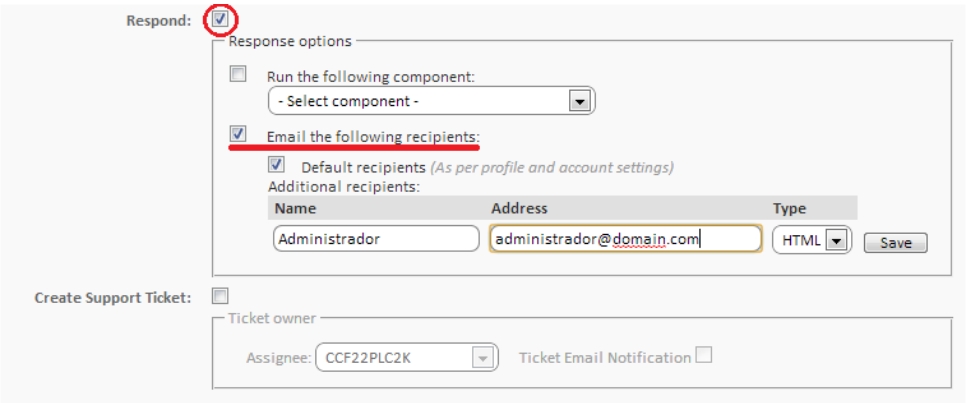


Figura 62: configuracion de la respuesta del monitor

- Una vez creado el monitor, se añadirá una línea en la pantalla de políticas, accesible desde el menú general **Cuenta**, pestaña **Políticas** o desde el menú general **Zona**, seleccionando la zona, en la pestaña **Políticas**, dependiendo del nivel donde se creó la política.

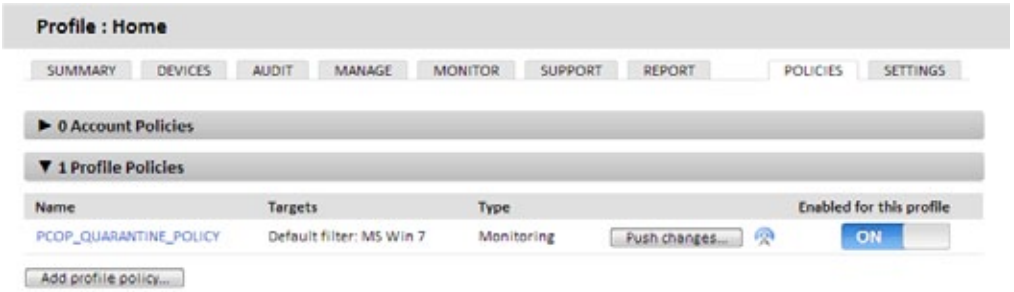


Figura 63: listado de políticas asociadas en la zona

- Haz clic en el botón **Forzar cambios** para distribuir la política entre los dispositivos asignados y comenzar su ejecución.

3 Creación de variables de entorno y ejecución del componente cada 60 segundos.

Una vez distribuido el monitor en los dispositivos, éste se ejecutará cada 60 segundos. Para ello, se invoca el intérprete de script asociado, se leen las variables de entorno necesarias y se escribe la respuesta adecuada.

> *El código fuente completo del script se encuentra en el Apéndice A.*

En la línea 24 lee la variable de entorno `PCOP_PATH` y obtiene un objeto de tipo `FileSystemObject` que apunta a la carpeta de la cuarentena.

```
23      Set WshSysEnv = WshShell.Environment("PROCESS")
24      Set objFolder = objFSO.GetFolder(WshSysEnv("PCOP_PATH"))
```

Las líneas 25 a 30 controlan si la variable de entorno está definida. Si la variable no fue definida, se devuelve un error en la variable `Result` y se termina la ejecución con `Errorlevel 1` (línea 34).

```
25      if err.number <> 0 then
26          'PCSM didn't send the environment variable
27          err.clear
28          WScript.Echo "<-Start Result->"
29          WScript.Echo "Result=PCOP_PATH variable not defined on PCSM console or path not found"
30          WScript.Echo "<-End Result->"
31          Set WshShell = nothing
32          Set WshSysEnv = nothing
33          Set objFolder = nothing
34          WScript.Quit(1)
```

En las líneas 44-51 se escribe en el Registro del dispositivo el número de elementos de la carpeta monitorizada. Puesto que el script se ejecuta cada 60 segundos, pero se quiere realizar la comparación cada 10 minutos, se almacenan 10 entradas en el registro con el valor registrado cada 60 segundos.

```
44      While Err.Number=0 And n < 10
45          iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor" & n))
46          If err.number<>0 then
47              WshShell.RegWrite "HKLM\Software\Panda Security\Monitor" & n, colFiles.count, "REG_SZ"
48          Else
49              n=n+1
50          End If
51      Wend
```

La ejecución de componentes en el dispositivo del usuario es "atómica": no se conserva el estado entre dos ejecuciones sucesivas del mismo script. Si se requiere de varias ejecuciones de un mismo script para generar un resultado válido, los estados intermedios deberán ser guardados en los dispositivos y leídos en cada ejecución del componente.

Se recomienda utilizar el registro para almacenar el estado entre dos o más ejecuciones del componente dentro de un dispositivo, aunque también pueden utilizarse ficheros temporales.

Cuando el contador es igual a 9, (10 anotaciones en el Registro, 10 minutos) se compara el valor inicial con el final (línea 57). Si es mayor en las líneas 59, 60 y 61 se envía la diferencia y se termina el script con `Errorlevel 1`.

Terminado el último ciclo, se borran todas las entradas del registro (Líneas 64-66) y se copia la última entrada como la primera para continuar con el proceso.

```
54      If n=9 Then
55          iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor0"))
56          iCountNow= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor9"))
57          if iCountPast < iCountNow then
58              'there is more items in the folder, it updates the registriy and sends an alert
59              WScript.Echo "<-Start Result->"
60              WScript.Echo "Result=" & iCountNow - iCountPast & " new items in PCOP quarantine"
61              WScript.Echo "<-End Result->"
62              bHit=true
63          end if
64          For n=0 To 9
65              WshShell.RegDelete("HKLM\Software\Panda Security\Monitor" & n)
66          Next
67          WshShell.RegWrite "HKLM\Software\Panda Security\Monitor0", colFiles.count, "REG_SZ"
68
69      end if
```

4 Envío cada 10 minutos de la salida estándar y procesamiento en la plataforma Panda Systems Management

Si el script termina la ejecución con `Errorlevel 0`, la respuesta no es tenida en cuenta por el servidor; si termina con `Errorlevel 1`, el servidor leerá la salida estándar en busca de la variable `Result` entre las cadenas `"<-Start Result->"` y `"<-End Result->"`. Con esta información realizará las acciones configuradas en la definición del monitor.

11.4.5 Cómo utilizar variables globales

Si el desarrollo de nuevos scripts es frecuente, es muy probable encontrarnos en la situación de querer utilizar datos comunes en todos ellos, como pueden ser rutas a carpetas concretas en los discos duros del usuario, letras de unidades de red compartidas en servidores o incluso credenciales comunes para ejecutar ciertas tareas.

Una posible solución es incorporar en cada script todos los datos que se necesiten, de tal forma que si la información cambia habría que actualizar manualmente todos los scripts desarrollados y volverlos a distribuir entre los dispositivos.

La opción más conveniente, sin embargo, es definir variables globales a Nivel Zona o Cuenta para que puedan ser utilizados por los scripts de forma directa.

Define las variables y su contenido en el menú general **Cuenta, Configuración** o menú **Zona, Configuración**, que será directamente accesible desde los scripts diseñados cuando se ejecuten en los dispositivos de los usuarios.

En el caso de almacenar información sensible como usuarios y contraseñas, marca la casilla **Enmascarar valor** para sustituir el contenido de la variable por asteriscos en la consola.

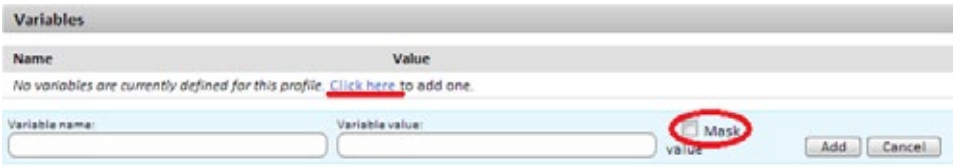


Figura 64: casilla para ocultar información sensible

Al hacer la distribución de los scripts, el servidor enviará el contenido de las variables al agente, que se encargará de crear variables de entorno en el dispositivo de usuario fácilmente accesibles por los scripts diseñados.

11.4.6 Etiquetas y campos personalizados

En el paso 2 del ejemplo se indicaba qué tareas tienen que desencadenarse en el servidor cuando el resultado de componente es "error"; en este caso, se mandaba un correo al administrador informando del cambio de estado del dispositivo.

Este enfoque es correcto en el caso de un dispositivo que cumple una condición de error o excepción, y el administrador quiere ser informado de ello sin necesidad de tener que consultar la consola cada cierto tiempo. Sin embargo, puede ser necesario simplemente visualizar el estado de un dispositivo sin atender a condiciones de error. Para ello, será necesario publicar los datos de interés en la consola.

Para este escenario, el componente utilizará los campos personalizados de la consola que aparecen en la barra de pestañas **Resumen** del Nivel Dispositivo de cada dispositivo y en los listados de dispositivos, añadiendo la columna necesaria tal y como se explica en el Capítulo 5: Dispositivos.

Figura 65: localización de los campos personalizados en la ventana Resumen del dispositivo

La etiqueta **Campo personalizado 1** y sucesivas (hasta 10), se pueden renombrar a nivel global para todos los dispositivos que administre el partner independientemente de la zona a la que pertenezcan, o se puede definir al nivel de la zona concreta:

- En el Nivel Cuenta en el menú general **Cuenta**, **Configuración**.
- En el Nivel Zona en la barra de pestañas **Configuración**.

De esta forma en el Nivel Dispositivo o en el listado de dispositivos de la zona aparecerá el nombre de etiqueta elegido en vez de **Campo personalizado X.**

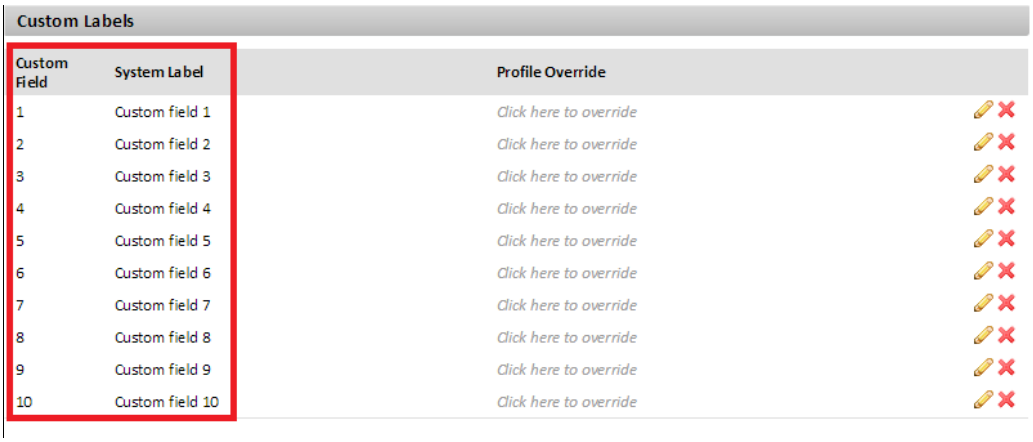


Figura 66: configuración del cambio de etiqueta de los campos personalizados

El contenido de los campos personalizados se toma de las ramas del registro de cada dispositivo, indicadas a continuación:

```
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom1
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom2
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom3
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom4
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom5
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom6
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom7
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom8
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom9
HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom10
```

Cada una de las ramas indicadas podrá contener una cadena de caracteres de hasta 255 caracteres.

Un componente podrá escribir libremente en las ramas del registro indicadas, de forma que el agente las leerá al lanzar una auditoría automática (cada 24 horas) o manual (bajo demanda) y enviará la información al servidor, que se encargará de mostrarla en la consola. Además, el agente procederá al borrado de esta información en el registro del dispositivo una vez leída y enviada al servidor.

11.5. Creación de un componente de tipo Script

Para crear un componente de tipo script se sigue el mismo proceso que en un componente de tipo monitor:

- En el menú general **Componentes**, haz clic en **Añadir Componente**.
- Elige el tipo script.
- La pantalla de configuración del componente solo difiere de la de monitores en la zona de recogida de información: no se pueden definir variables de salida, pero en su lugar se permite buscar cadenas en la salida estándar (`stdout`) o salida de error (`stderr`) para activar condiciones de aviso en la consola.

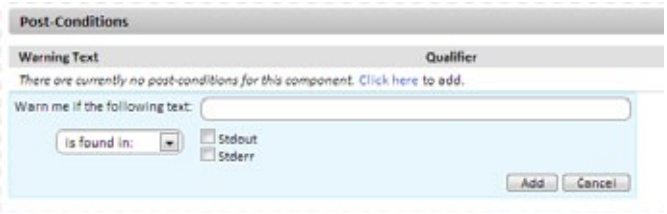


Figura 67: variables de salida estándar y error

- Para utilizar un componente de tipo script, haz clic en el icono para marcarlo como favorito en la lista de componentes. Así aparecerá en los listados de **tareas rápidos** y **tareas programadas**.

11.6. Modificación de componentes

Los componentes importados o agregados desde la **ComStore** no son directamente modificables; **Panda Systems Management** únicamente permite modificar de forma directa los componentes que haya desarrollado el administrador.

Para modificar un componente importado o agregado desde la **ComStore** y ajustarlo a las necesidades del parque informatico a administrar:

- En el menú general **Componentes**, haz clic en el icono de los documentos para copiar el componente.
- Se abrirá la pantalla de edición del componente, donde puedes cambiar el script de comandos asociado, el nombre y otras características.
- Para editar posteriormente un componente ya copiado haz clic en el nombre. Si un componente no permite hacer clic en el nombre es que no ha sido previamente copiado.

12. Auditoría de activos

Auditoria de hardware

Auditoria de software

Auditoria de licencias

Auditoria de servicios

Auditoria de cambios

12.1. Introducción

Panda Systems Management te ayuda a catalogar todos tus activos hardware y software. El módulo de auditoria de activos supervisa la aparición de nuevos dispositivos y programas instalados en ellos, al tiempo que realiza un control de licencias para el software de pago.

La pestañada **Auditoria** está disponible en los tres niveles soportados (Cuenta, Zona y Dispositivo) mostrando información mas detallada o genérica según el nivel seleccionado.

- Para acceder a las funcionalidades de auditoría en el Nivel **Cuenta** haz clic en el menú general **Cuenta**, menú de pestañas **Auditoría.**
- Para acceder a las funcionalidades de auditoría en el Nivel **Zona** haz clic en el menú general **Zonas**, selecciona una zona y haz clic en el menú de pestañas **Auditoría.**
- Para acceder a las funcionalidades de auditoría en el Nivel Dispositivo haz clic en el menú general **Zonas**, selecciona una zona, selecciona un dispositivo y haz clic en el menú de pestañas **Auditoría.**

La información de la pestaña Auditoría se actualiza cada 24 horas de forma automática, o bajo demanda haciendo clic en el icono de los catalejos, en la barra de iconos.

La información suministrada se agrupa en cinco secciones accesibles desde la parte superior derecha de la ventana **Auditoria**, haciendo clic en el botón de selección apropiado:

- **Hardware**: dispositivos encontrados en la red del cliente, hardware instalado, etc.
- **Software**: software encontrado en los dispositivos con un agente instalado.
- **Licencias**: información de las licencias de software consumidas.
- **Servicios**: muestra los servicios instalados en los equipos Windows y su estado de ejecución.
- **Cambios**: registro de cambios de software, hardware y del sistema.

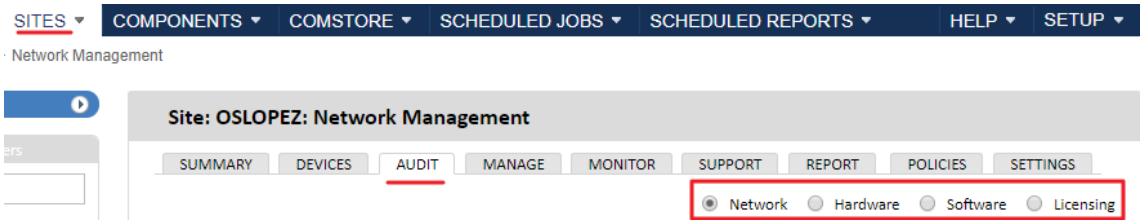


Figura 68: pantalla de auditoría

Accesibilidad de la información según el nivel seleccionado

Dependiente del nivel seleccionado (Cuenta, Zona o Dispositivo) seran accesibles ciertas secciones. A continuacion se muestra una tabla con los tipos de informacion accesibles según el nivel selecionado.

Sección / Nivel	Cuenta	Zona	Dispositivo
Hardware	SI	SI	SI
Software	SI	SI	SI
Licencias	SI	SI	NO
Servicios	NO	NO	SI
Registro de cambios	NO	NO	SI

Tabla 21: funcionalidad de auditoria según el nivel seleccionado

12.2. Auditoria de hardware

12.2.1 Nivel Cuenta

Muestra las plataformas (modelos) del hardware utilizado en los dispositivos gestionados en toda la cuenta. La plataforma de un dispositivo coincide con la marca y modelo de la placa madre en dispositivos personalizados o clónicos, y con la marca y modelo comercial en dispositivos fabricantes que ensamblan PCs y dispositivos.

Además, se muestra el número de dispositivos encontrados que coinciden con la plataforma.

Haz clic en cada plataforma para mostrar los dispositivos gestionados por **Panda Systems Management** que coincidan con el criterio seleccionado.

12.2.2 Nivel Zona

Muestra toda la información del hardware administrado en la red del cliente, separado en dos secciones:

Dispositivos administrados

Contiene un listado de los dispositivos que son gestionados por **Panda Systems Management** en el parque, agrupados por su modelo.

Haz clic en el modelo para mostrar el listado de dispositivos agrupados.

Dispositivos no administrados

Contiene una lista gestionada de forma manual, con los dispositivos de la red que no son gestionados por **Panda Systems Management** pero que el administrador quiere representar en la consola a efectos de inventario.

Haz clic en el icono **+** para introducir la información relevante del equipo no administrado.

Figura 69: campos para indicar las características de un dispositivo no administrado por Panda Systems Management

12.2.3 Nivel Dispositivo

Las auditorias del Nivel Dispositivo son las más precisas, mostrando toda información relevante del dispositivo elegido.

Dependiendo del tipo de dispositivo, el contenido de la pestaña **Auditoría** cambia, mostrando la información indicada en los puntos mostrados a continuación:

Para sistemas Windows, Linux y OS X

Campo	Descripción
Nombre del host	Nombre del dispositivo.
UID	Identificador interno del dispositivo.
Sistema operativo	Sistema operativo instalado en el dispositivo y versión interna.
Placa madre	Marca y modelo de la placa madre.
Nombre de BIOS	Fabricante de la BIOS.
Versión de BIOS	
Fecha de lanzamiento de BIOS	
Procesador	Fabricante y modelo del procesador.
Memoria	Cantidad de memoria instalada.
Adaptador de pantalla	Fabricante y modelo de tarjeta de vídeo.
Almacenamiento	Información relativa a los discos duros y almacenamiento local instalado: **Unidad de disco, Tamaño, Libre** y **Descripción.**
Memoria	Se mostrarán los slots de memoria disponibles y si están usados o disponibles, además de su **Número de pieza**, **Número de serie**, **Capacidad** y **Velocidad.**
Monitores	Fabricante y modelo del monitor conectado.
Adaptadores de red	Fabricante y modelo de la tarjeta de red instalada, dirección Mac y velocidad de la interface.
Dispositivos conectados	Dispositivos externos conectado por USB al equipo

Tabla 22: información de equipos Windows, Linux y macOS en el Nivel Dispositivo

Sistemas Android e iOS

Campo	Descripción
Nombre del host	Nombre del dispositivo.
UID	Identificador interno del dispositivo.
Sistema operativo	
IMEI	Código de identificación del terminal móvil.
Modelo	Modelo del smartphone o tablet.
ICCID	Identificador de la tarjeta SIM.
Operadora	Compañía que suministra el servicio de telefonía.
Número	Fabricante y modelo del procesador.
Adaptadores de red	Identificador lógico de la tarjeta de red instalada, dirección Mac y velocidad de la interface.

Tabla 23: información de dispositivos Android e iOS en el Nivel Dispositivo

Sistemas ESXi

Campo	Descripción
Nombre del host	Nombre del dispositivo.
UID	Identificador interno del dispositivo.
Sistema operativo	
Procesador	Fabricante y modelo del procesador.
Guest info	Información de las máquinas virtuales creadas en el servidor ESXi: **Nombre de host, Nombre del invitado, Sistema operativo, Almacén de datos, CPU, RAM, Imágenes**
Memoria	Información detallada de los bancos de memoria instalados: **Módulo, Tipo, Número de pieza, Número de serie, Capacidad, Velocidad.**
Almacenamiento	Información detallada de los almacenes de datos locales y remotos configurados en el servidor: **Almacén de datos, Almacenamiento, Sistema de archivos, Capacidad, Libre, Suscripción, Estado**
Adaptadores de red	Identificador lógico de la tarjeta de red instalada, dirección Mac y velocidad de la interface.

Tabla 24: información de servidores ESXi en el Nivel Dispositivo

12.3. Auditoría de software

12.3.1 Nivel Cuenta

Muestra toda la información del software instalado en los dispositivos de la red del cliente, agrupado por el nombre del programa y versión.

Haz clic en el nombre del programa para mostrar el listado de dispositivos que lo tienen instalado y ejecutar acciones sobre ellos en conjunto, como por ejemplo actualizar la versión o desinstalar el software mediante la ejecución de scripts.

12.3.2 Nivel Zona

Los programas listados son los instalados en los dispositivos pertenecientes a la zona seleccionada. El tipo de información es la misma que la mostrada en el Nivel Cuenta, descrita en el punto anterior.

12.3.3 Nivel Dispositivo

Los programas listados son los instalados en el dispositivo seleccionado. El tipo de información es la misma que la mostrada en el Nivel Cuenta, descrita en el punto anterior.

12.4. Auditoría de licencias

12.4.1 Nivel Cuenta

El objetivo de la auditoría de licencias es determinar el número de instalaciones producidas de cada programa, para de esta manera calcular las licencias que la empresa tiene en uso y las que necesita adquirir.

Para ello, se permiten definir agrupaciones de uno o más programas, y **Panda Systems Management** comparará estas agrupaciones con el software instalado en los dispositivos.

Paquetes de software

Crear una agrupación o paquete de software tiene sentido cuando los programas que lo forman constituyen una unidad a la hora de su licenciamiento o adquisición. Por ejemplo, el paquete Office esta compuestos por varios programas que a la empresa no le interesa adquirir por separado (Word, Excel, PowerPoint etc). En este caso, la existencia de uno de los programas instalados implica la necesidad de una licencia para todo el paquete.

Para añadir programas independientes a la consola PCSM, será necesario crear un paquete de un solo elemento.

Se recomienda crear paquetes en el Nivel Cuenta si el software utilizado en las diferentes zonas administrados de la empresa es común. De esta manera, la estrategia más productiva para evitar duplicar la definición de paquetes en cada zona de forma individual, es definir todos los paquetes de software posibles en el Nivel Cuenta y activarlos en los niveles de Zona necesarios.

En otras palabras: todos los paquetes creados en el Nivel Cuenta serán accesibles en los niveles inferiores para su uso.

En otras palabras: todos los paquetes creados en el Nivel Cuenta serán accesibles en los niveles inferiores para su uso.

Crear de un paquete de software

Haz clic en el icono  de la barra de iconos para mostrar la ventana donde se indica toda la información relevante del nuevo paquete de software:

- **Nombre**: nombre del paquete de software a crear.
- **Buscar**: buscar un determinado programa entre una lista compuesta por todos los programas instalados en los dispositivos gestionados por la cuenta de **Panda Systems Management**.
- **Todos**: selecciona todos los programas que coincidan con el criterio de selección establecido en el campo **Buscar**.
- **Específica**: permite seleccionar de forma específica el programa de la lista y la versión que formará parte del paquete.

Una vez creado el paquete se mostrará en el listado de paquetes creados, junto con su nombre, el número de programas que componen el paquete y la cantidad de dispositivos en la cuenta que contienen alguno o todos los programas que forman el paquete.

En el Nivel Cuenta únicamente es posible configurar paquetes. Para configurar alertas que avisen al administrador de la falta de licencias es necesario acudir al Nivel Zona.

12.4.2 Nivel Zona

El Nivel Zona también permite crear paquetes como en el Nivel Cuenta si bien de forma limitada al software instalado en los dispositivos que forman parte de la zona.

Además, en el Nivel Zona no solo es posible definir paquetes de software o utilizar los definidos en el Nivel Cuenta, sino que también se ofrece la posibilidad de definir el número máximo de instalaciones permitidas en la zona.

De esta manera, cuando el número de dispositivos que usan un determinado paquete sea superior al número de licencias disponibles configuradas por el administrador en la consola, se disparará una alerta que advertirá al administrador de la necesidad de compra de licencias adicionales.

Crear de un paquete de software

El proceso es el mismo que el mostrado en el Nivel Cuenta.

Incorporar un paquete de software creado en el Nivel Cuenta

Haz clic en la barra de iconos para mostrar todos los paquetes de software creados tanto en el Nivel Cuenta como en el Nivel Zona. Selecciona mediante las casillas los paquetes a incorporar en la zona.

Configurar el número máximo de licencias

Una vez añadidos los paquetes de software necesarios se mostrará una tabla con la siguiente información:

- **Paquete de software:** haciendo clic en su nombre se abrirá una ventana de edición que permitirá modificar la configuración del paquete.
- **Cantidad**: número de veces que el software contenido en el paquete ha sido visto instalado en los dispositivos de la zona gestionada.
- **Alerta**: número máximo de instalaciones permitidas. Si el número de instalaciones encontradas supera al configurado se enviará una alerta al administrador advirtiéndole de la situación.

12.5. Auditoría de servicios

12.5.1 Nivel Dispositivo

Muestra los servicios instalados en el dispositivo junto al estado actual y la configuración de inicio

- **Nombre mostrado al usuario**: nombre del servicio mostrado al usuario.
- **Nombre del servicio**: nombre interno del servicio.
- **Estado en la última auditoría**: estado el servicio (**running**, **stopped**) la última vez que se realizó la auditoria del dispositivo.
- **Tipo de inicio**: configuración de arranque del servicio (**Auto**, **manual**, **disabled**)

12.6. Auditoría de cambios

12.6.1 Nivel Dispositivo

Muestra los cambios a nivel hardware y software que se han efectuado en el dispositivo junto a la fecha en los que se produjeron.

Esta funcionalidad le permite al administrador facilitar el diagnóstico de problemas ante dispositivos con un mal funcionamiento, ya que podrá relacionarlos con los cambios producidos en el equipo.

Los cambios se agrupan en tres bloques de información:

- **Cambios en el sistema**: muestra los cambios en los módulos del sistema operativo del dispositivo.
- **Cambios en el software**: muestra el nuevo software encontrado, actualizado o eliminado en el dispositivo
- **Cambios en el hardware**: muestra el nuevo hardware encontrado o eliminado en el dispositivo.

13. Distribución e instalación centralizada de software

13.1. Objetivo de la instalación centralizada de software

El servidor PCSM puede distribuir ficheros y paquetes de software de forma remota y desatendida en los dispositivos de la red gestionados. De esta manera, el administrador puede garantizar que todos los dispositivos que gestiona tienen instalado el software o los documentos necesarios para que los usuarios puedan realizar sus tareas, y todo ello sin necesidad de desplazarse o conectar por acceso remoto a cada dispositivo de forma individual.

La distribución de software de forma automática también ayudará al administrador a mantener el software libre de vulnerabilidades (Java, Adobe, etc.), reduciendo así de forma considerable el riesgo de infección y la pérdida de información confidencial.

13.2. Requisitos para la instalación centralizada de software

La distribución e instalación de software es un proceso que se ejecuta a través de componentes de tipo aplicación para las plataformas de escritorio Windows, Linux y Mac.

Para la instalación de aplicaciones en smartphones y tablets iOS consulta al final de este mismo capítulo.

Al igual que los componentes de tipo monitor y script explicados en el Capítulo 11: Componentes y la ComStore, los componentes aplicación constan de un pequeño script, que en este caso tiene el objetivo de guiar el proceso de instalación, y de una serie de ficheros y/o programas a instalar.

Para cada grupo de ficheros o programas a instalar en los dispositivos de usuario será necesario crear un componente independiente.

13.3. Procedimiento para distribuir e instalar paquetes.

El procedimiento general consta de 4 pasos:

1 Determinar los dispositivos sobre los cuales se instalará el software.

El procedimiento para encontrar los dispositivos que no tienen los ficheros o programas instalados varía dependiendo de si el Servidor puede determinar si el programa está instalado en el dispositivo o no.

Si el software a instalar aparece en la lista de programas instalados mantenida por el propio sistema operativo, también se mostrará en las auditorias de software de **Panda Systems Management** y,

por tanto, será posible crear un filtro que discrimine los dispositivos que ya tengan instalado el software.

Si el software no tiene instalador y, por tanto, no aparece en la lista de programas instalados o si se trata de documentos sueltos, ficheros de configuración, etc. el servidor no será capaz de filtrar dispositivos que ya tengan estos ficheros instalados y será el propio script de instalación el que tenga que realizar las comprobaciones oportunas de forma manual.

2 Generar un componente de instalación de software

Los pasos involucrados son los mismos que los descritos en el Capítulo 11: Componentes y la ComStore para la creación de componentes de tipo script o monitor.

3 Lanzar una tarea para empujar el componente de instalación a los agentes de los dispositivos afectados.

Se puede lanzar una tarea programado para cierta fecha en la que el usuario no esté trabajando con el dispositivo, con el objetivo de minimizar el impacto en el rendimiento.

4 Recoger el resultado del despliegue para determinar posibles fallos.

Una vez terminado el proceso, es posible recoger un código de error y/o mensaje que muestre en la **consola** el resultado del despliegue.

Se distinguen cuatro estados finales:

- **Con éxito**: la ejecución del despliegue fue completada sin errores. El script devuelve el código de `Errorlevel 0`.
- **Con éxito - Advertencia**: la ejecución del despliegue fue completada con algunos errores no importantes. El script devuelve el código de `Errorlevel 0` y una cadena de caracteres por la salida estándar o error estándar que será interpretada por la consola.
- **Error**: la ejecución del despliegue no se completó. El script devuelve el código de `Errorlevel 1`.
- **Error - Advertencia**: la ejecución del despliegue no se completó. El script devuelve el código de `Errorlevel 1` y una cadena de caracteres por la salida estándar o error estándar que será interpretada por la consola.

13.4. Ejemplos de despliegue

Para ilustrar la distribución de software se proponen cuatro ejemplos:

- Distribución de documentos mediante lenguaje de script.
- Distribución de documentos sin lenguaje de script.
- Distribución de software autoinstalable.
- Distribución de software sin instalador.

Los procedimientos aquí mostrados, así como las herramientas de terceros utilizadas y lenguajes de script son ejemplos y pueden cambiar. Panda Systems Management está pensando para ser flexible y adaptarse a las herramientas con las que el administrador se encuentre más cómodo.

13.4.1 Distribución de documentos mediante lenguajes de script

El objetivo de este ejemplo es distribuir una carpeta en el directorio raíz del dispositivo del usuario con tres documentos de tipo Word. Para ello se siguen los siguientes pasos:

1 Determinar los dispositivos sobre los que se instalará el software

Como en este caso el servidor no tiene visibilidad sobre el estado del disco duro del dispositivo del usuario a nivel de sistema de ficheros, el script de instalación se distribuirá entre todos los dispositivos de la zona y será el propio script (líneas 19-24) el que compruebe si la carpeta con los documentos existe o no.

```
19      Set objFolder = objFSO.Getfolder(CONST_PATH)
20      If Err.Number=0 Then
21          'the folder already exists, the files won't be copied
22          WScript.Echo "Deploy unsuccessful: The folder already exists"
23          WScript.Quit (0)
24      End If
```

Si la carpeta no existe se crea (línea 28), se mueven los documentas a ella (líneas 30-32) y se enviará un mensaje por la salida estándar (línea 37).

```
28      Set objFolder = objFSO.CreateFolder(CONST_PATH)
29      'the documents will be moved to the folder
30      objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
31      objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
32      objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
33      If Err.Number<>0 Then
34          WScript.Echo "Deploy unsuccessful: " & Err.Description
35          WScript.Quit (1)
36      Else
37          WScript.Echo "Deploy successful: All files were copied"
38          WScript.Quit (0)
39      End If
```

2 Generar un componente de instalación de software

En el menú general **Componentes** haz clic en el botón **Añadir componente**. Agrega un componente de tipo **Aplicaciones**, añade los documentos a distribuir y el script que creará la carpeta y moverá los tres documentos en cada uno de los dispositivos.

En la pantalla de **Componentes: Aplicación** es importante indicar:

- El componente es **Favorito** para que aparezca en los listados de componentes (icono de la estrella arriba a la izquierda).
- La categoría (**Aplicaciones**) del componente y su nombre.

- El lenguaje de script utilizado (**Instalar comando**).
- Agregar los documentos a distribuir en la sección **Archivos**.

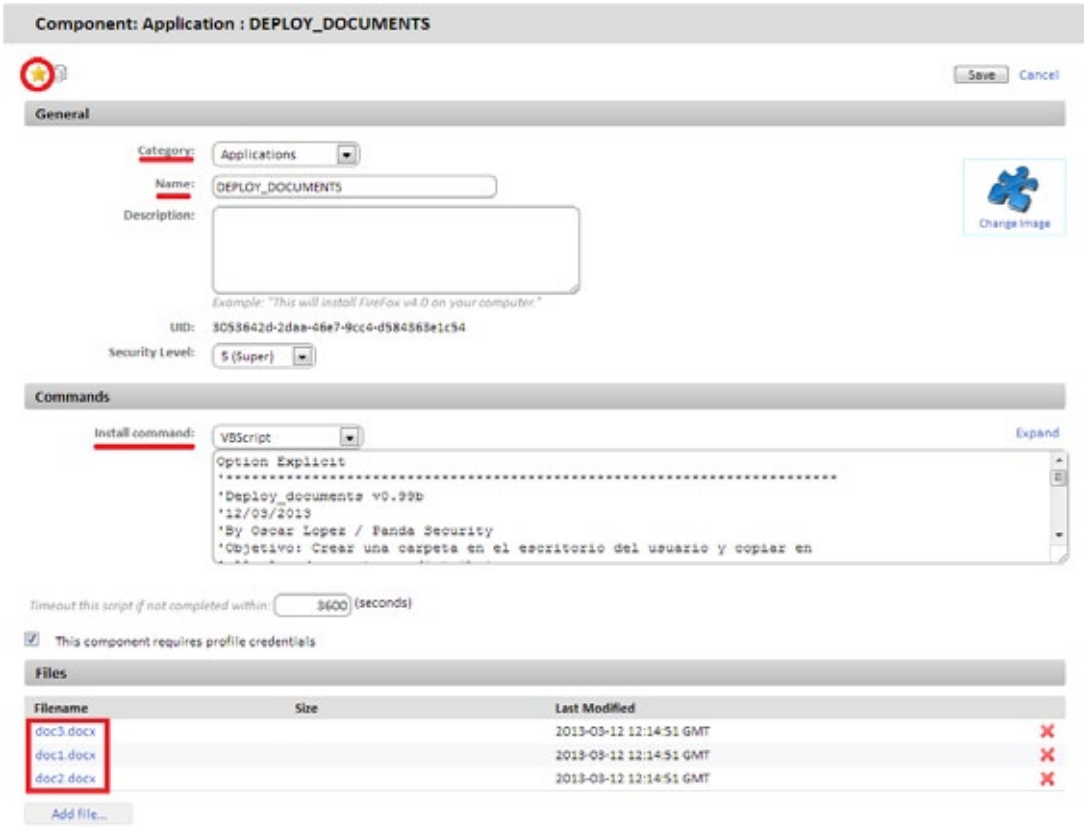


Figura 70: configuración del componente

En la zona de **Condiciones posteriores** se pueden indicar cadenas de texto que serán interpretadas por la **consola** como avisos.

En el ejemplo se indica que si en la salida estándar (**Recurso:stdout**) se encuentra (**Calificador: se encuentra en**) la cadena "**Deploy unsucessfull"**, el resultado de la ejecución del script será considerado como aviso.

3 Lanzar una tarea para empujar el software a los agentes de los dispositivos afectados

Haz clic en T**area rápida** o **Tarea** con los dispositivos de la zona donde quieres desplegar los documentos seleccionados.

> ***En el Nivel Cuenta se permiten seleccionar zonas completas sobre las cuales aplicar la distribución de software.***

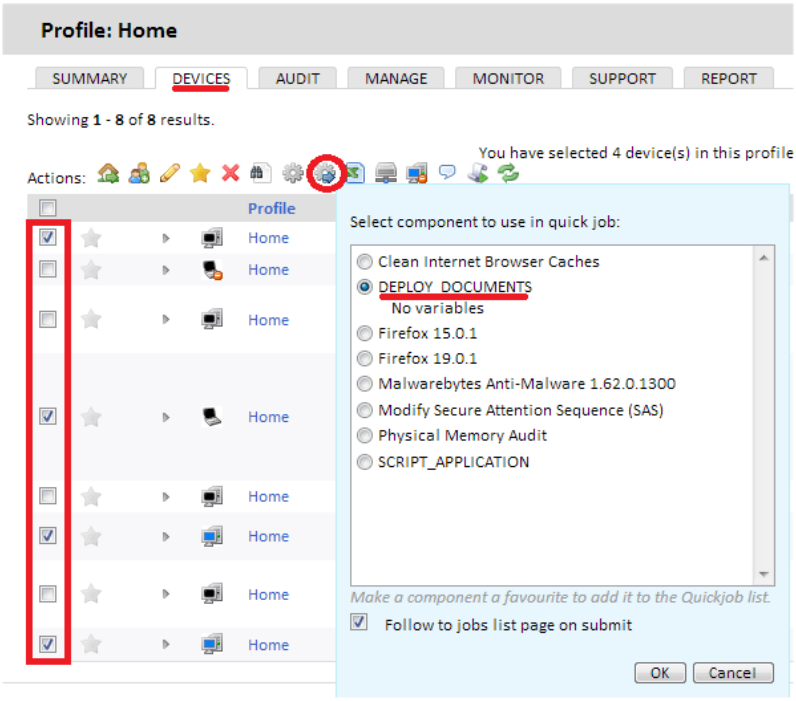


Figura 71: ejecución de un componente de instalación como tarea rápida

4 Recoger el resultado del despliegue para determinar posibles fallos

Las condiciones de salida definidas en el script de ejemplo son 3:

- **Éxito**: los ficheros con copiados sin errores en la carpeta destino (líneas 30-32). Se termina con un `Errorlevel 0` (línea 38).

```
28      Set objFolder = objFSO.CreateFolder(CONST_PATH)
29      'the documents will be moved to the folder
30      objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
31      objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
32      objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
33      If Err.Number<>0 Then
34          WScript.Echo "Deploy unsuccessful: " & Err.Description
35          WScript.Quit (1)
36      Else
37          WScript.Echo "Deploy successful: All files were copied"
38          WScript.Quit (0)
39      End If
```

- **Error**: se produce algún error en la copia de ficheros. Se termina con un `Errorlevel 1` (línea 35).
- **Éxito - Advertencia**: la carpeta ya existe, de forma que los ficheros no se copian. Se termina con un `Errorlevel 0` (línea 23) y se genera la cadena **Deploy unsuccessful**, que el servidor interpretara como Warning tal y como se configuró en la zona **Condiciones posteriores** del paso 3.

```
19      Set objFolder = objFSO.Getfolder(CONST_PATH)
20      If Err.Number=0 Then
21          'the folder already exists, the files won't be copied
22          WScript.Echo "Deploy unsuccessful: The folder already exists"
23          WScript.Quit (0)
24      End If
```

Una vez lanzado la tarea, aparecerá en menú general **Tareas Programadas, Tareas Activas**.

Para ver el resultado del despliegue haz clic en la barra de pestañas **Tareas completadas:** en **Rojo** si terminó con Error, **Naranja** si hubo un Warning o en **Verde** si fue Successful.

Los iconos **Stdout** y **Stderr** muestran una copia de la salida estándar y error estándar generado por el propio script.

Además, en esta pestaña hay una barra de iconos que te permitirá desencadenar varias acciones:

- En la zona **Acciones** se agrupan los iconos que permiten relanzar la tarea, recargar la página para actualizar el estado de la tarea descargar en un fichero la salida y error estándar.
- Con el filtro **Vistas** se pueden filtrar las tareas según su estado.

13.4.2 Distribución de documentos sin utilizar lenguaje de script.

Puede simplificarse el script de instalación enormemente si no son necesarias comprobaciones previas ni generación de advertencias en la consola.

En este ejemplo se distribuyen los 3 documentos del ejemplo anterior, pero en vez de generar la estructura de carpetas desde el script, simplemente se creará un paquete .EXE autoextraíble con los documentos comprimidos y la estructura de carpetas en su interior oportuna. La generación del paquete .EXE puede hacerse con muchas herramientas, en este ejemplo se usa `WinRar`.

Para descargar una versión gratuita de `WinRar` visita la página http://www.winrar.com

En este ejemplo se va a generar un fichero .EXE auto extraíble con las siguientes características:

- Funcionamiento en modo silencioso.
- La carpeta con el contenido será creada de forma automática en `C:\.`
- Si la carpeta existiera previamente se sobrescribirá su contenido sin avisar.

Es imprescindible generar un fichero auto extraíble que funcione en modo silencioso, es decir, que no muestre diálogos ni ventanas ni requiera de la interacción del usuario.

Pasos para generar un fichero autoextraíble de instalación silencioso:

1 Prepara la carpeta con los documentos a distribuir.

Crea la carpeta raíz `ACME Documents` del ejemplo, y en su interior coloca todos los ficheros, carpetas y subcarpetas que se necesiten distribuir.

2 Genera el ejecutable.

Con el programa `WinRar` abierto, arrastra la carpeta recién creada `ACME Documents` y marca las opciones **Crear un archivo autoextraíble** y **Crear un archivo sólido**.

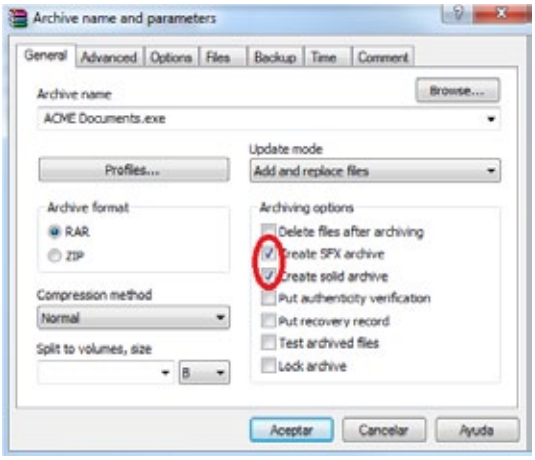


Figura 72: crear archivo autoextraíble

3 Configura el ejecutable como silencioso.

Activa Ocultar Todo en Avanzado, Autoextraíble, Modos, Mostrar.

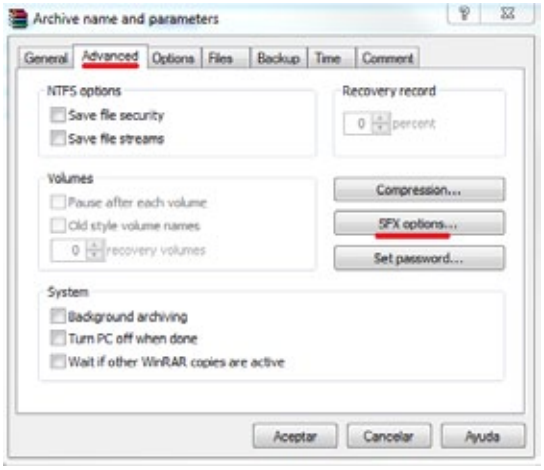


Figura 73: ejecución del archivo en modo silencioso

4 **Indica la ruta de destino donde se creará la carpeta en la pestaña General.**

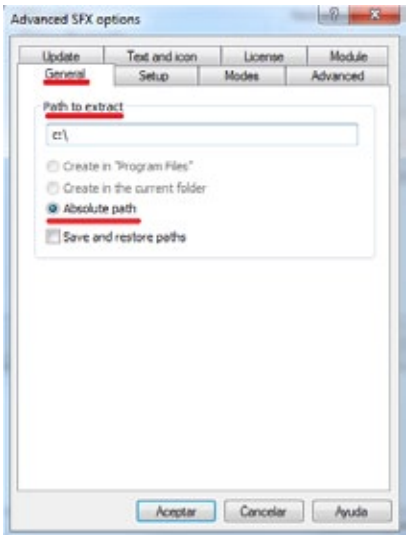


Figura 74: ruta del archivo

5 **Indica que se sobrescribirán los ficheros en caso de existir previamente sin preguntar nada al usuario.**

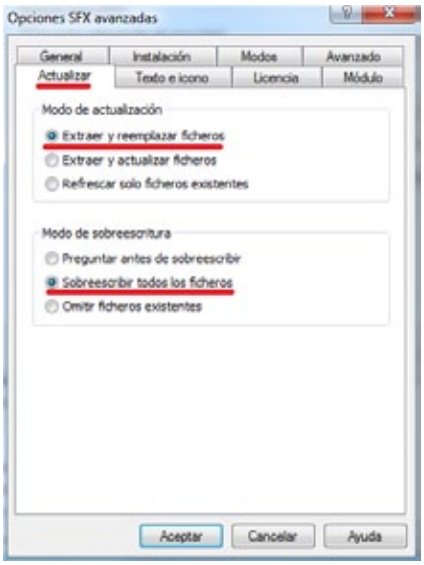


Figura 75: reemplazar archivos descomprimidos sin preguntar

Una vez generado el paquete `ACME Documents.exe` se creará un componente **Aplicación** para su distribución.

En la pantalla de **Componentes: Aplicación** es importante indicar:

- El componente es **Favorito** para que aparezca en los listados de componentes (icono de la estrella arriba a la izquierda).
- La categoría (Aplicaciones) y el nombre del componente.
- El lenguaje de script utilizado (Comando de instalación), en este caso Batch.
- Agregar el paquete a instalar `ACME Documents.exe`

El script ejecutará el paquete auto extraíble que se encargará de crear la carpeta en la unidad `c:\` junto con toda su estructura interna, machacando cualquier contenido anterior.

13.4.3 Distribución de software autoinstalable

En este ejemplo se desplegará el paquete Framework .NET 4.0 `dotNetFx40_Full_x86_x64.exe` de Microsoft en aquellas máquinas que no lo tengan ya instalado.

Para ello, y dado que Microsoft Framework .NET 4.0 es un programa que sí aparece en el listado de programas mantenido por el sistema operativo del dispositivo, se utilizará un filtro para discriminar aquéllos que no lo tengan instalado.

El paquete de instalación es un .EXE auto extraíble que acepta los parámetros `/q /norestart` para ejecutarse en modo silencioso y evitar el reinicio del dispositivo, de forma que no será necesaria ninguna preparación especial adicional.

1 Determinar los dispositivos sobre los cuales se instalará el software.

Para filtrar todos los dispositivos que ya tienen instalado el software, es necesario conocer qué cadena de identificación se corresponde con el paquete ya instalado. Este dato se puede obtener en la barra de pestañas **auditoría**, **Software** de un dispositivo que ya tenga instalado el paquete.

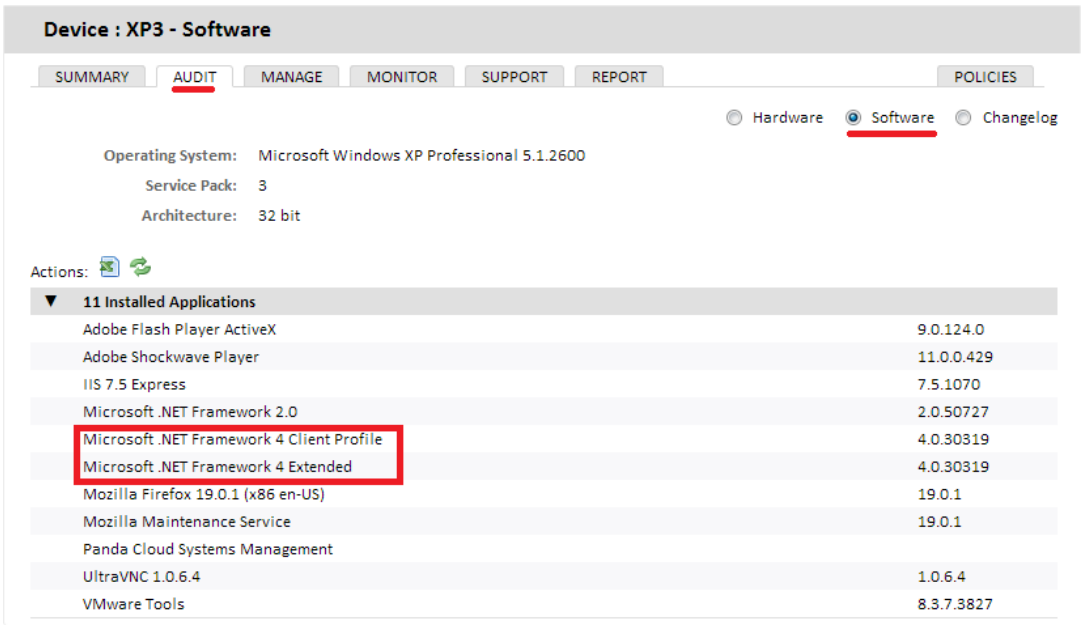


Figura 76: obtención de la cadena de identificación del paquete instalado

Con este dato crea un filtro de zona o un filtro de cuenta con la siguiente configuración:

- **Término**: **Paquete de Software** para inspeccionar el software instalado en el dispositivo.
- **Búsqueda**: aquí se indica la cadena que identifica el software a instalar.
- **Condición**: **No contiene** para seleccionar aquellos dispositivos que no contengan en el campo **Paquete de Software** el contenido especificado en **Búsqueda**.

2 Generar un componente de instalación de software.

La generación del componente de instalación es extremadamente sencilla.

En la pantalla de **Componente: Aplicación** hay que indicar:

- El componente es **Favorito** para que aparezca en los listados de componentes (icono de la estrella arriba a la izquierda).
- La categoría (**Aplicaciones**) y el nombre del componente.
- El lenguaje de script utilizado (**Comando de instalación**), en este caso **Batch**.
- **Comando de instalación** contiene la línea de comando que ejecuta el paquete:

```
@echo off
pushd %~dp0
dotNetFx40_Full_x86_x64.exe /q /norestart
```

- Agregar el paquete a instalar `dotNetFx40_Full_x86_x64.exe`.

El script únicamente tiene una línea relevante, que es la que ejecuta el paquete de instalación con los parámetros necesarios para conseguir una instalación silenciosa.

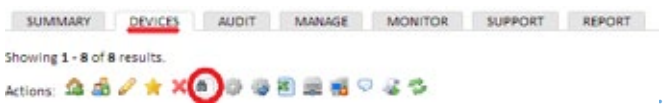
3 Lanzar una tarea para empujar el software a los Agentes de los dispositivos afectados.

Primero se selecciona el filtro previamente preparado y después se ejecutará una tarea con la Aplicación creada.

4 Recoger el resultado para determinar posibles fallos.

Una buena manera de comprobar el resultado de la instalación es revisando el filtro de dispositivos previamente preparado, para ver si el número de dispositivos que no tienen instalado el software desplegado es menor. Todos aquellos dispositivos que sigan apareciendo en el filtro, habrán tenido algún tipo de error.

La información de auditoría de dispositivos con el contenido del hardware y software instalado es enviada por el agente al servidor cada 24 horas, de forma que la lista de software recién instalado no se actualizará hasta pasado ese tiempo. No obstante, se puede forzar una actualización manual con la acción Solicitar auditoría(s) de dispositivos de la Barra de acciones.



13.4.4 Distribución de software sin instalador

Muchos programas están formados por un único ejecutable, sin instalador asociado, que genere la estructura necesaria en el menú Inicio ni los accesos directos en el escritorio ni las entradas pertinentes en Añadir y Quitar programas. Este tipo de programas puede ser distribuido siguiendo el ejemplo de distribución de documentos o de paquete auto extraíble; sin embargo, hacerlo de esta manera impide al servidor generar una auditoria de programas instalados fiable ya que no aparecerán en el listado de programas instalados mantenidos por el sistema operativo del dispositivo.

Por esta razón, frecuentemente se recurre a herramientas de terceros que generan un único paquete MSI con todos los programas a añadir, creando los grupos necesarios en el menú Inicio y los accesos directos en el escritorio del usuario para facilitar su ejecución.

Para realizar esta labor, se utilizará en este caso el programa `Advanced Installer`, que en su versión gratuita nos permite generar instaladores MSI de forma simple.

Para descargar la versión gratuita de Advanced Installer visita la página: http://www.advancedinstaller.com/download.html

Para generar el instalador sigue los siguientes pasos:

- Elige la plantilla **Simple** (gratuita).

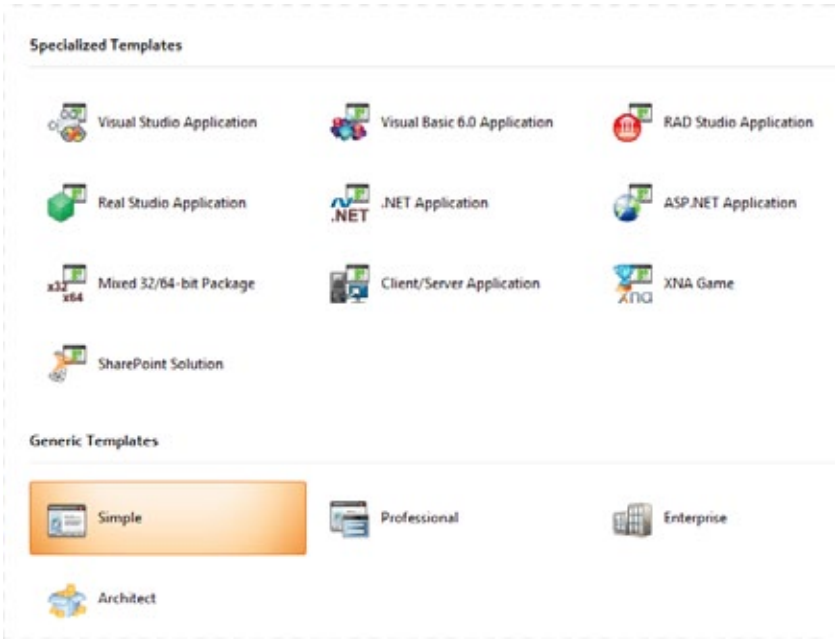


Figura 77: selección de plantilla

- En **Products Details** rellena los datos básicos del instalador: **Product Name**, **Product Version** y **Company Name**.

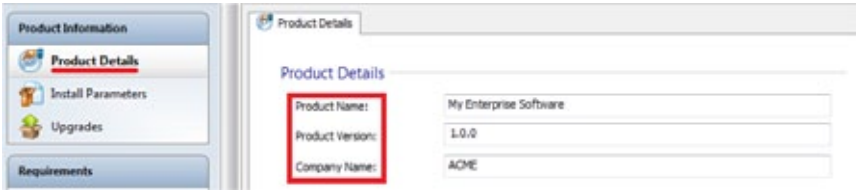


Figura 78: datos del instalador

- Añade los ficheros y programas a instalar, así como los accesos directos a crear. Esto se lleva a cabo en la pestaña **Files and Folders**.

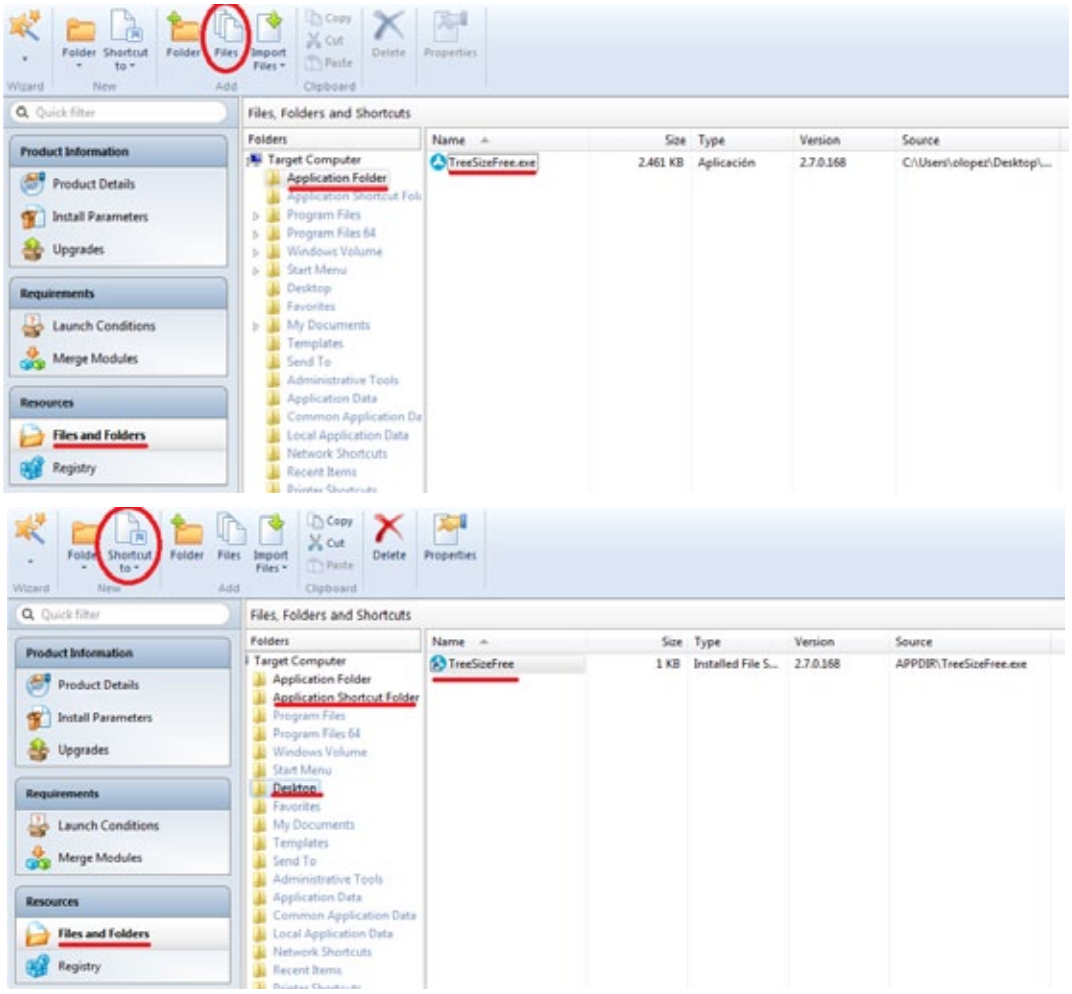


Figura 79: agrega los ficheros a desplegar

- Finalmente ejecuta **Build**, con lo que el paquete MSI quedará generado en la carpeta de nuestra elección.

Una vez generado el paquete de instalación, los pasos para crear un componente de instalación y distribuirlo son equivalentes a ejemplos anteriores, excepto por el script en Batch, que varía ligeramente en el comando para la instalación.

```
@echo off
pushd %~dp0
MSIEXEC /I "my software.msi" /qn
```

El agente PCSM ejecutará la utilidad `MSIEXEC` con el parámetro `/qn` para lanzar una instalación silenciosa.

- El componente es **Favorito** para que aparezca en los listados de componentes (icono de la estrella arriba a la izquierda).
- La categoría (**Aplicaciones**) y el nombre del componente.
- El lenguaje de script utilizado (**Comando de instalación**), en este caso **Batch**.
- Agregar el paquete a instalar `My Software.msi`.

13.5. Ahorro de ancho de banda en el despliegue de software

El agente instalado en cada uno de los dispositivos pregunta cada 60 segundos si hay alguna descarga que realizar desde el Servidor, y en caso de ser así se ejecuta de forma individual para cada agente. De esta forma, para un paquete de instalación de 50 Mbyte y una red de 50 equipos, el resultado aproximado de descarga será 2'4 Gbytes.

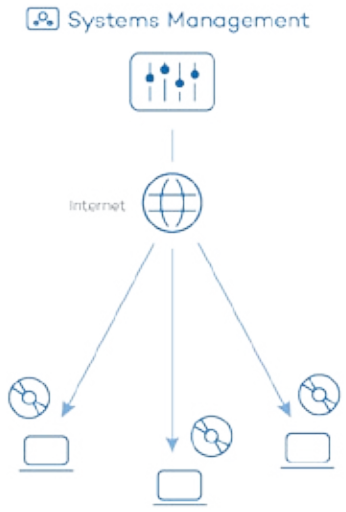


Figura 80: distribución individual de paquetes

Para minimizar el volumen total de la descarga, es posible promocionar uno de los dispositivos de la red al rol de repositorio / caché. De esta forma, sólo este dispositivo realizará la descarga desde el servidor para luego distribuir el paquete entre todos los dispositivos de la red afectados.

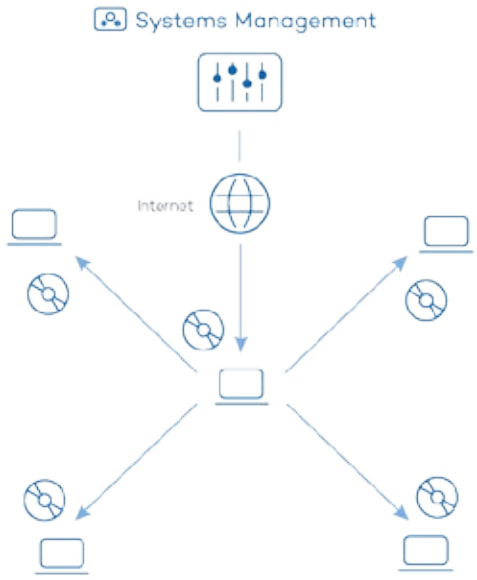


Figura 81: distribución centralizada de paquetes

13.5.1 Promoción de dispositivo a rol de cache

Para promocionar un dispositivo al rol de repositorio / caché, deberás acceder al nivel dispositivo del dispositivo en la consola y hacer clic en el icono **Añadir / eliminar como cache local** de la **Barra de acciones**.

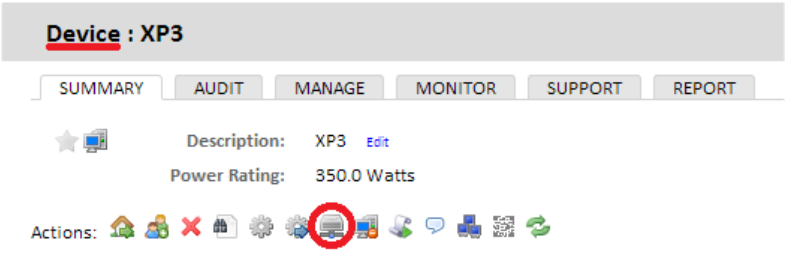


Figura 82: promoción de un dispositivo a rol de cache

Se mostrará una ventana que permite determinar la unidad del dispositivo donde se mantendrán los componentes cacheados.

Además, el dispositivo con el rol de cache también almacenará los parches descargados de Windows Update, tal y como se detalla en el capítulo 15 Gestión de parches

Desde ese momento, el dispositivo designado descargará y distribuirá los componentes y paquetes de instalación entre los dispositivos de la red local, acelerando el despliegue y minimizando el ancho de banda.

13.5.2 Configuración del comportamiento de los dispositivos con rol de cache

Mediante el apartado local caches del menú de pestañas **Configuración** será posible indicar el máximo número de días que los componentes y parches se mantendrán cacheados en cada dispositivo, así como el orden de precedencia de los dispositivos en la red.

13.6. Instalación de software en dispositivos iOS

El procedimiento para la distribución de software en tablets y teléfonos iOS difiere del mostrado anteriormente, ya que estos dispositivos tablets tienen limitado el origen del software a instalar. En el caso de iOS, todas las descargas e instalaciones de software tienen que estar publicados en la Apple Store.

La instalación de aplicaciones en dispositivos Android no está soportada en esta versión de Panda Systems Management.

13.6.1 Requerimientos para la instalación de aplicaciones en dispositivos iOS

Para activar la descarga de aplicaciones en dispositivos iOS:

- Haz clic en el menú general **ComStore.**
- Descarga el componente **Mobile Device Management.**

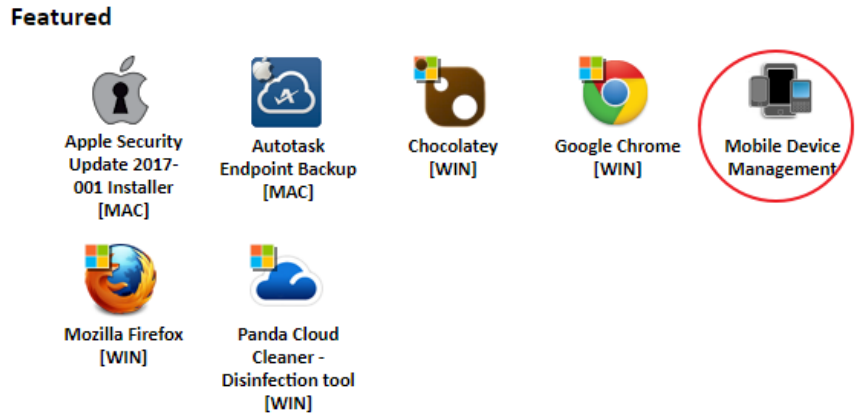


Figura 83: componente Mobile Device Management

- Para añadir a la **Lista de aplicaciones** los programas a distribuir en los dispositivos iOS, haz clic en el botón **Añadir app de iOS** y accede a la ventana de selección de aplicaciones.

Figura 84: acceso a la ventana de aplicaciones iOS

- Establece el país del cliente y utiliza la caja de texto para indicar el nombre de la aplicación.
- Haz clic en el botón **Buscar** para lista la aplicación junto con su información básica y el precio.
- Haz clic en el botón **Add** y la aplicación a desplegar se integrará en la **Lista de aplicaciones.**

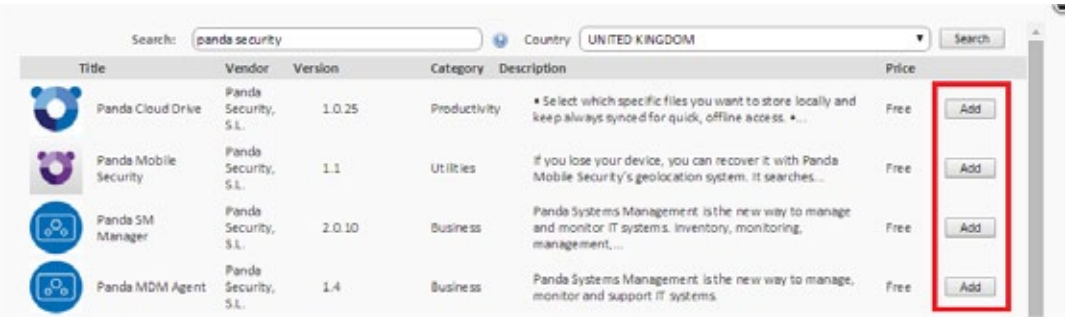


Figura 85: agregar las aplicaciones iOS a distribuir

13.6.2 Instalación de las aplicaciones iOS integradas en la Lista de aplicaciones

Crea una política de gestión de software para desplegar las aplicaciones en los dispositivos iOS de los usuarios:

- Determina si la instalación de software se ejecutará en dispositivos de varias zonas o de una única zona.
  - **Para varias zonas**: haz clic en el menú general **Cuenta** y en la pestaña **Administrar.**
  - **Para una zona**: haz clic en el menú general **Zonas**, selecciona una zona y haz clic en la pestaña **Administrar.**
- Selecciona **Gestión de software** en el botón de selección y haz clic en el botón **Nueva política de cuenta / zona** en la parte inferior izquierda de la pantalla.
- Para seleccionar las aplicaciones a desplegar haz clic en el botón **Añadir una app** y en **Añadir un destino** para añadir los dispositivos donde se desplegarán.
- Una vez seleccionadas las aplicaciones a desplegar, es necesario editar aquéllas que sean de pago para introducir el **Redemption Code.** Para ello, haz clic en el icono .

- Finalmente, haz clic en el botón **Forzar cambios** para enviar de forma instantánea las aplicaciones configuradas a los dispositivos seleccionados en la política y que se encuentren encendidos en ese momento.

Si el dispositivo iOS se encuentra apagado en el momento del envío de la política, se mostrará en la sección non-compliant devices. Para programar la ejecución de la política de forma automática en el momento en que el dispositivo se vuelva accesible, haz clic en el icono .

14. Ticketing

Descripción de un ticket

Creación de un ticket

Gestión de tickets

14.1. Introducción

El incremento de equipos a gestionar y el creciente número de técnicos asignados a la resolución de problemas, obliga más pronto que tarde a la implantación de un sistema que permita la documentación y coordinación de cada caso tratado por el departamento de IT.

Los sistemas de ticketing sirven para registrar cada incidencia desde el momento de su creación hasta su cierre, registrando todos los estados intermedios por el que evolucione.

De esta manera, es posible asignar un caso a un técnico concreto y reasignarlo a otro posteriormente si el técnico original ya no se encuentra disponible o la tarea requiere de conocimientos muy específicos, conservando toda la documentación y avances conseguidos hasta el momento y minimizando así las interrupciones al usuario final con requerimientos repetidos de información sobre el mismo problema.

Por otra parte, el hecho de obligar a documentar las incidencias permite reutilizar el procedimiento en el futuro y refinarlo, minimizando el tiempo de respuesta de los casos abiertos.

Finalmente, con un sistema de ticketing es posible determinar la carga de trabajo del departamento de IT, filtrando los tickets que están abiertos en un determinado momento y asignar más recursos si fuera necesario.

14.2. Descripción de un ticket

Cada ticket contiene una serie de campos que lo describen:

Figura 86: vista general de un ticket

- **Creador:** creador del ticket. Puede ser un dispositivo si el ticket fue creado desde el **agente** por un usuario, o una cuenta del sistema si fue creado por un monitor y asignado a un técnico.
- **Zona:** agrupación de dispositivos a la que pertenece el ticket.
- **Creado en fecha:** fecha de creación del ticket.
- **Estado:** se distinguen cuatro estados:
  - **Nuevo**: ticket recién creado con la descripción del problema y asignado a un técnico. Todavía no se ha realizado ningún trabajo.
  - **En progreso**: la incidencia está siendo gestionada por el técnico del departamento de IT asignado.
  - **En espera**: la resolución de la incidencia se ha determinado por causas externas (falta de información, confirmación de cambios por parte del usuario u otras).
  - **Cerrado**: la incidencia se ha resuelto y se cierra.
- **Gravedad**: severidad del ticket. Si fue generado por un monitor, se copia la severidad asignada a éste.
- **Asignado a**: técnico asignado para la resolución de la incidencia.
- **Resumen**: resumen de la incidencia.
- **Contenido**: descripción de la incidencia.
- **Comentarios:** en este campo, tanto el técnico como el usuario pueden añadir entradas que completen y actualicen la incidencia.

Se recomienda utilizar el campo Comentarios frecuentemente, documentando los cambios de la incidencia y las acciones realizadas, tanto por parte de los técnicos del departamento de IT como del usuario con pruebas realizadas y otros datos de interés. El objetivo de esto es reutilizar esta información para agilizar futuras incidencias similares.

14.3. Creación de tickets

Los tickets son creados de tres maneras:

- Creación manual por el usuario desde el agente instalado en su equipo.
- Creación automática desde un monitor que detecta una condición anómala.
- Creación manual por el departamento de IT desde la consola.

14.3.1 Creación manual de tickets por el usuario desde su propio agente

Indicada para el caso de que el usuario compruebe que su dispositivo funciona mal y quiere dejar constancia de los síntomas por escrito.

Para dar de alta un ticket de forma manual, el usuario del dispositivo tiene que:

- Hacer clic en el agente con el botón derecho en su icono y seleccionar la opción **Abrir.**
- Hacer clic en la pestaña **Tickets, Abrir nuevo Ticket.**

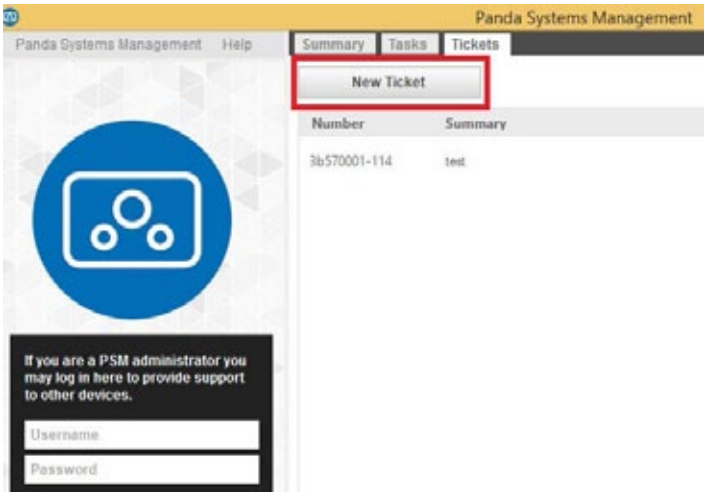


Figura 87: acceso a la herramienta de creación de tickets desde el agente PCSM instalado en el dispositivo del usuario

Una vez creado el ticket es posible añadir nuevos comentarios y cerrarlo.

Figura 88: herramientas de edicion de tickets desde el agente PCSM instalado en el dispositivo del usuario

Los tickets creados desde el agente quedan automáticamente asignados a la cuenta de usuario configurada en el menú general Cuenta, Ajustes, Configuración de cuenta, Usuario asignado de ticket de usuario final, o desde la propia zona en Configuración.

14.3.2 Creación automática de tickets desde un monitor que detecte una condición anómala en el dispositivo

Se configura al definir una política de tipo monitor, en la pestaña **Información del ticket**.

En este caso, se puede elegir el técnico asignado y si se generará un mail de notificación con la creación del ticket.

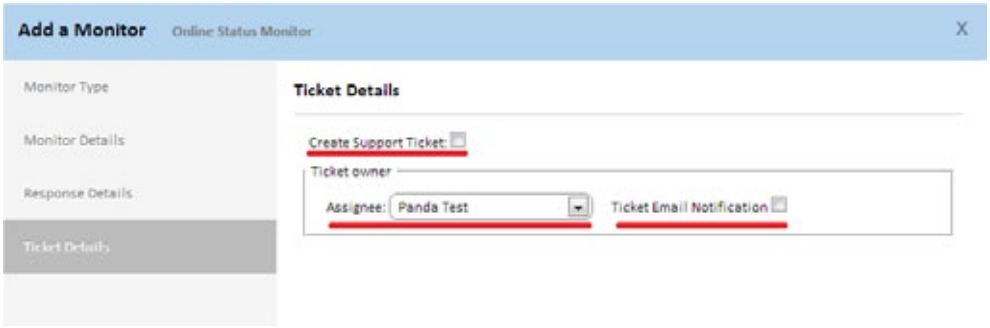


Figura 89: configuración para generar tickets de forma automática

14.3.3 Creación manual de tickets por el departamento de IT desde la Consola

Indicada para generar recordatorios o tareas que entran de manera oficial en la cola del departamento.

Para crear un ticket desde la consola:

- Determina el nivel en el que se creará el ticket
  - Para crear un ticket en el nivel Cuenta haz clic en el menú general **Cuenta** y haz clic en la pestaña **Soporte.**
  - Para crear un ticket en el nivel zona haz clic en el menú general **Zonas**, selecciona una zona y haz clic en la pestaña **Soporte**.
- Haz clic en **Crear ticket de soporte.**

Los tickets creados en el Nivel Cuenta no tienen zona asignada y no se muestran en ninguno de las zonas creadas.

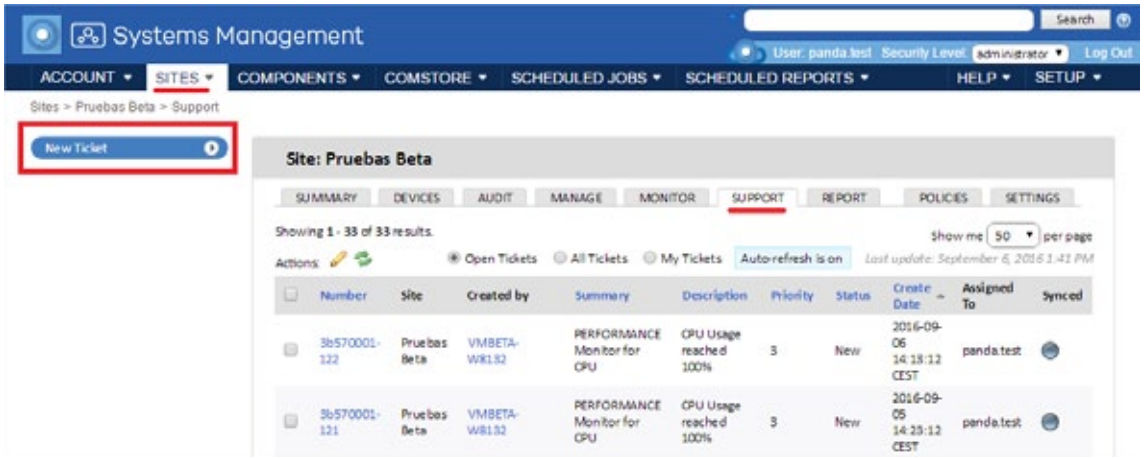


Figura 90: creación de tickets desde el nivel zona

En este caso se pueden especificar la severidad del ticket y su contenido, así como asignarlo a un técnico para su resolución o reasignación posterior.

14.4. Gestión de tickets

La gestión de los tickets ya creados se realiza desde la barra de pestañas **Soporte** en los niveles Zona, Cuenta o Dispositivo.

> *Los tickets creados en los niveles inferiores se mostrarán en niveles superiores. Por ejemplo, si se crean tickets en el Nivel Dispositivo aparecerán en el Nivel Zona al que pertenezca ese dispositivo.*

Filtra el listado de tickets (**Tickets abiertos, Mis tickets, Todos los tickets**) o edita su estado utilizando el icono del bolígrafo de **la Barra de acciones**. Para cambiar la severidad, el estado y a quien está asignado haz clic en el número de ticket.

15. Gestión de parches

¿Qué es la gestión de parches?

¿Qué parches puedo distribuir / aplicar?

Distribución e instalación de parches

Auditorías

15.1. ¿Qué es la gestión de parches?

La gestión de parches es un conjunto de recursos orientados a automatizar la distribución e instalación de parches y actualizaciones de software de forma centralizada.

La gestión de parches no solo facilita la actualización diaria del software de tus dispositivos, sino que permite realizar auditorías, mostrando de forma sencilla y rápida aquellos equipos sin actualizar o con vulnerabilidades conocidas.

Con la gestión de parches el administrador puede reforzar la seguridad de la red y minimizar los fallos de software, garantizando que todos los dispositivos están actualizados con los últimos parches publicados.

La gestión de parches utiliza la API Windows Update existente en todos dispositivos Microsoft Windows compatibles con Panda Systems Management. La gestión de parches es compatible con sistemas Microsoft Windows.

15.2. ¿Qué parches puedo distribuir / aplicar?

Panda Systems Management gestiona de forma centralizada todos los parches y actualizaciones publicadas por Microsoft a través de Windows Update.

Microsoft publica actualizaciones para todos los sistemas operativos Windows que soporta en la actualidad y también para el software que desarrolla:

- Microsoft Office
- Exchange 2003
- SQL Server
- Windows Live
- Windows Defender
- Visual Studio
- Zune Software
- Virtual PC
- Virtual Server
- CAPICOM
- Microsoft Lync
- Silverlight
- Windows Media Player
- Otros…

15.3. Distribución e instalación de parches

Panda Systems Management incorpora dos métodos independientes, aunque complementarios, para la gestión de parches, cada uno de ellos con diferentes funcionalidades que se adaptan a distintas necesidades y/o escenarios posibles:

- Política Windows Updates
- Política Gestión de parches

El método Política Windows Updates y Política Gestión de parches son mutuamente excluyentes. Desactiva Windows Updates cuando utilices políticas de gestión de parches para actualizar los sistemas operativos de los dispositivos Windows. En caso contrario el resultado puede ser impredecible. Consulta en la sección Método I: Política Windows Update más adelante en este capítulo para desactivar la política Windows Update.

Los procedimientos aquí descritos pueden colisionar con otros procedimientos definidos por software de terceros, como, por ejemplo, políticas de Windows Update definidas en una GPO. Se recomienda desactivar políticas de terceros fabricantes que interfieran con las definidas en Panda Systems Management.

15.4. Método I: Política Windows Update

Las políticas de tipo **Windows Update** establecen de forma centralizada la configuración del servicio Windows Update, accesible desde el panel de control de los dispositivos Windows de la red.

De esta forma, el administrador controlará desde un único panel el comportamiento de los dispositivos Windows de la red en lo tocante a la actualización del sistema operativo y otros programas de Microsoft.

Al tratarse de una política, los niveles de agrupación compatibles con este método son Nivel Cuenta y Nivel Zona.

15.4.1 Creación de Políticas Windows Update

Para crear una política de tipo **Windows Update** en el Nivel Zona o Nivel Cuenta haz clic en la pestaña **Políticas** y selecciona el tipo de política **Windows Update**.

Se mostrará una pantalla donde configurar de forma centralizada el comportamiento de Windows Update de todos los dispositivos afectados por la política creada.

La configuración de las políticas **Windows Update** siguen el mismo esquema que el mostrado por el servicio Windows Update accesible desde el panel de control de cada dispositivo Windows individual.

Windows Update cataloga los parches que recibe en tres niveles:

- Importantes
- Recomendados
- Opcionales

Sólo se instalan de forma automática los parches importantes y recomendados. El resto de parches serán instalados de forma manual desde el propio dispositivo del usuario o sino desde **Panda Systems Management** utilizando otros métodos de gestión de parches.

Toda la configuración de esta política es una transposición de las funcionalidades de Windows Update de los dispositivos Windows. Todas las acciones indicadas se refieren por tanto a los propios dispositivos y no al agente o a la consola.

Aunque la configuración de la política es única para todos los dispositivos, el comportamiento de Windows Update en cada dispositivo puede variar ligeramente entre las distintas versiones del sistema operativo.

A continuación, se explican las opciones disponibles en este tipo de política:

- **Añadir un destino**: añade filtros o grupos que delimiten el ámbito de aplicación de la política.
- **Política de parches**: indica el comportamiento general de Windows Update dentro de cada dispositivo con respecto a los parches catalogados como "Importantes" por Microsoft:
  - Descarga e instalación automática.
  - Descarga y selección manual por el usuario.
  - Notificación sin descarga.
  - Desactivar Windows Update.

Para evitar el solapamiento de políticas si ya se está utilizando otro método de actualización de parches dentro de PCSM o con productos de terceros, crea una política de Windows Update con el campo Política de parches en "desactivar Windows Update".

- **Instalar nuevas actualizaciones**: indica en qué momento se instalarán los parches.
- **Actualizaciones recomendadas**: aplica la política elegida en política de parches tanto a los parches **Importantes** como a los **Recomendados**.
- **Quién puede instalar actualizaciones**: permite al usuario la instalación de parches de forma manual.

- **Actualización de Microsoft**: busca parches de tipo **Opcional**, generalmente parches de otros productos de Microsoft.
- **Notificaciones de software**: muestra al usuario notificaciones detalladas cuando se encuentre disponible nuevo software de Microsoft.
- **Comportamiento del reinicio**: si esta activado se advierte al usuario que es necesario un reinicio tras instalar un parche. Si no está activado, el parche se instala y se advierte al usuario que se realizará un reinicio en 5 minutos.
- **Volver a solicitar el reinicio con instalaciones programadas**: establece el tiempo para que Windows Update vuelva a solicitar al usuario el reinicio del dispositivo, en caso de que haya parches instalados que lo requieran.
- **Demorar reinicio para instalaciones programadas**: establece el tiempo que el sistema espera para reiniciar después de instalar los parches. Si no se indica nada, se toma el valor por defecto: 15 minutos.
- **WSUS**: permite utilizar un servidor Windows Server Update Services alternativo local o remoto para minimizar la descarga de parches individuales por cada dispositivo en la red.
    - **No permitir conexiones a Microsoft para la instalación o búsqueda de parches cuando se utilice un servidor WSUS Server**: en el caso de que el administrador cuente con un servidor WSUS instalado en la red, esta opción evita la búsqueda de parches en la red de Microsoft en el caso de que el servidor WSUS este fuera de servicio.
    - **Activar destinos del lado del cliente**: en caso de utilizar un servidor WSUS con **Destinos del lado del cliente** (Client-side targeting) activado, los grupos y los dispositivos que los forman son definidos de forma manual en el servidor WSUS. En este parámetro de la política se permite especificar los grupos separados por punto y coma a los que pertenece el dispositivo sobre el que aplica la política.

Si algún o todos los dispositivos afectados por la política Windows Update no coinciden con los dispositivos definidos en los grupos de WSUS, la política quedará sin efecto en esos dispositivos.

Escenarios de uso del método Windows Update

- Cuando es necesario tener la garantía de que todos los parches importantes son instalados de forma automática, sin posibilidad de que el usuario entorpezca el proceso.
- Cuando es necesario llevar un control centralizado de parches de forma rápida y sin mantenimiento posterior.
- Cuando los equipos de la red son todos muy similares y no se distinguen casos particulares que requieran la exclusión de parches.
- Cuando no se requiere la instalación automática de los parches catalogados como Opcionales.

15.5. Método II: Política Gestión de parches.

Las políticas **Gestión de parches** permiten la instalación de actualizaciones de forma automática, de forma similar a las políticas **Windows Update**.

La principal diferencia viene a la hora de gestionar los parches a instalar: si en el método Windows Update se permitía aplicar parches según su nivel (Importante, Recomendado, Opcional), **Gestión de parches** permite definir condiciones más o menos complejas que permiten seleccionar de forma muy precisa los parches que serán instalados en los dispositivos, así como definir el comportamiento posterior del dispositivo en cuanto a reinicios e interacción con el usuario.

Al tratarse de una política, los niveles de agrupación compatibles con este método son Nivel Cuenta y Nivel Zona.

15.5.1 Flujo de trabajo general y redefinición de políticas Gestión de parches

En redes de tamaño mediano y grande, el número de casos particulares y escenarios incompatibles con la política general de Gestión de parches definida en el nivel Cuenta puede incrementarse de forma importante. Por esta razón el administrador de la red suele necesitar definir tantas políticas de gestión de parches como casos especiales existan en la red, requiriendo un esfuerzo adicional muy importante para su mantenimiento, sobre todo en casos de redes muy heterogéneas, donde se mezclan dispositivos utilizados por usuarios de diferentes perfiles y responsabilidades.

Por esta razón **Panda Systems Management** establece un flujo de trabajo alternativo al seguido en el resto de la consola a la hora de definir las políticas de Gestión de parches. El objetivo de este nuevo flujo de trabajo es acelerar la generación de políticas de Gestión de parches sin perder flexibilidad a la hora de determinar los parches que serán instalados en cada dispositivo de la red.

En la Figura 91 se establece el flujo de trabajo propuesto.

Establecimiento de política Gestión de parches en el Nivel Cuenta

Establece una política de gestión de parches en el nivel más general que abarque a todos los dispositivos del cliente y aplique las configuraciones por defecto y más comunes. Este paso no es necesario si solo existe una Zona en la cuenta.

Consulta el apartado **Creación de Políticas de Gestión de parches** más adelante para configurar una política de Gestión de parches.

Redefinición de políticas en el Nivel Zona

Establece en el Nivel las redefiniciones de políticas necesarias: a diferencia del resto de la consola, las políticas de Gestión de parches definidas en el Nivel Cuenta se pueden modificar **parcialmente.** De esta forma se elimina la necesidad de crear una nueva configuración completa en cada nivel Zona que solape a la ya creada en el nivel superior. La configuración heredada del Nivel Cuenta puede ser parcialmente modificada manteniendo en todo momento los dispositivos marcados como destino.

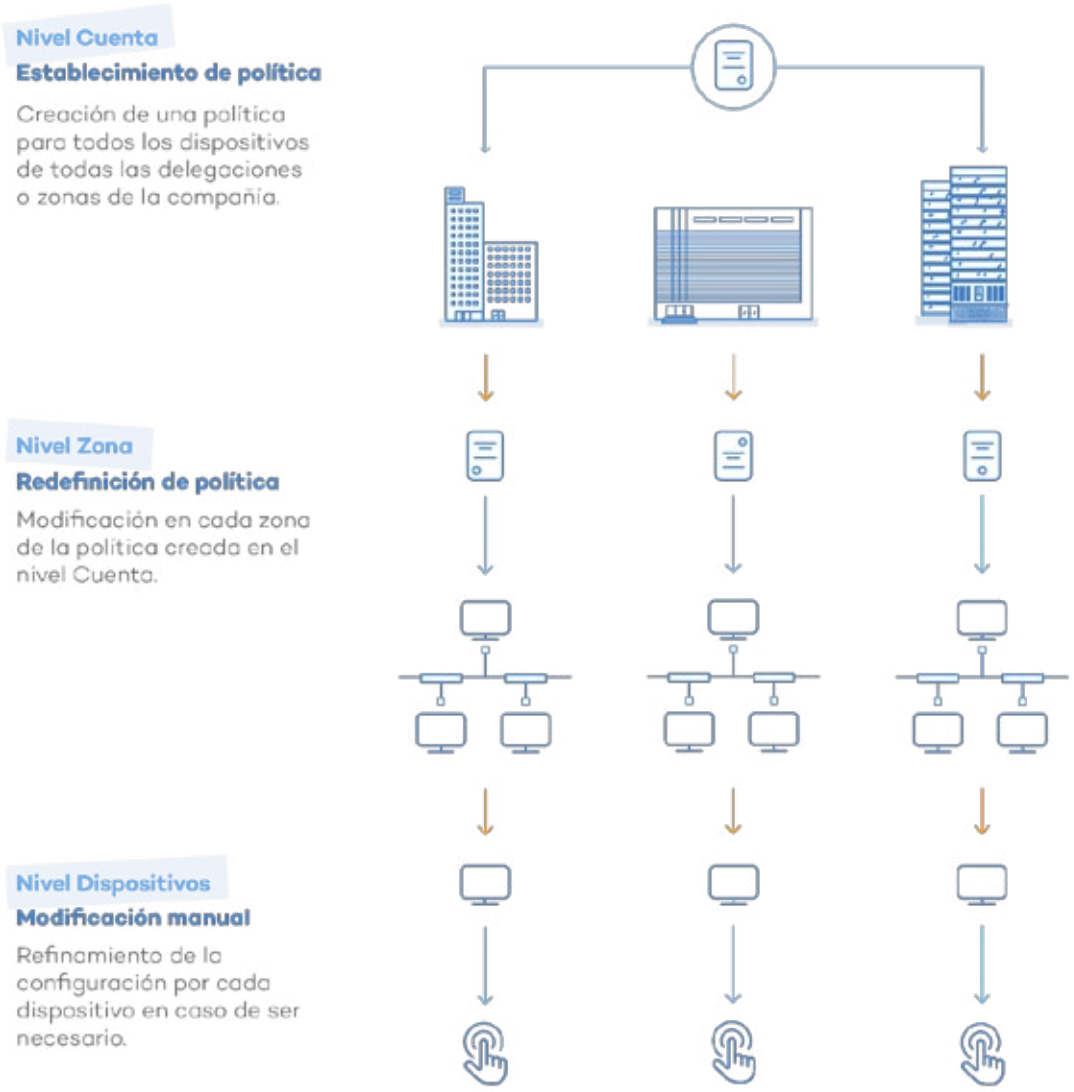


Figura 91: estrategia general para definir las políticas de parches

Modificaciones particulares por dispositivo

Finalmente, si fuera necesario, es posible modificar a nivel de dispositivo las políticas de gestión de parches definidas para aquellos casos en los que se requieran ajustes menores personalizados por dispositivo.

15.5.2 Creación de Políticas de Gestión de parches

Para crear una política de tipo Gestión de parches en el Nivel Zona o Nivel Cuenta haz clic en la pestaña **Políticas** y selecciona el tipo de política **Gestión de parches**.

Se mostrará una pantalla donde se podrá configurar de forma centralizada el comportamiento de la gestión de parches para todos los dispositivos afectados por la política creada.

Aprobación de parches y orden de precedencia

En una política de **Gestión de parches** se pueden establecer filtros y condiciones que permitirán de forma automática instalar o evitar la instalación de parches. Estos filtros recogen los metadatos que acompañan a cada uno de los parches publicados por Microsoft y los evalúan para tomar una decisión sobre su instalación.

La instalación o exclusión de un parche o grupo de parches en un dispositivo o conjunto de dispositivos se lleva cabo mediante el proceso de **aprobación de parches**, que forma parte de la configuración de la política **Gestión de parches**:

- **Aprobación de parches**: al aprobar un parche se marca para su aplicación en la próxima ventana de instalación, definida en la política, y sobre los dispositivos especificados.
- **No Aprobación**: al no aprobar un parche se marca su exclusión de forma indefinida del proceso de actualización de dispositivos.

La aprobación / no aprobación de parches puede efectuarse sobre:

- **Grupos de parches**: definidos por reglas creadas por el administrador para agrupar uno o más parches. Por ejemplo "todos los parches publicados de importancia Crítica". Existen un gran número de atributos de filtrado de parches y operaciones lógicas que permiten concatenarlos para generar criterios complejos y precisos.
- **Parches individuales**: la aprobación / no aprobación aplica a un parche concreto seleccionado por el administrador de forma manual.

De esta manera se disponen de cuatro combinaciones que se recorren en el siguiente orden:

Figura 92: flujo de aprobación y denegación de parches

Cada etapa tiene una mayor precedencia sobre la anterior; de esta forma si una regla de grupo aprueba un parche que posteriormente es rechazado a nivel individual prevalece este último.

Configuración de la política Gestión de parches

A continuación, se detallan las opciones de una política **Gestión de parches**.

- **Destinos:** añade filtros o grupos que limiten el ámbito de aplicación de la política. Dependiendo del nivel de creación de la política (Nivel Zona o Nivel Cuenta) se mostrarán los filtros y grupos de dispositivos apropiados.
- **Opciones de política de gestión de parches**: determina el momento en que se aplicarán las políticas de Gestión de parches y su duración:
  - **Programación**: define la ventana de instalación de parches. Para establecer el intervalo de instalación haz clic en el botón **Haga clic para cambiar.**, Se mostrará un formulario donde establecer el intervalo de tiempo que durará la ventana de instalación y la frecuencia de repetición.

Figura 93: configuración de la programación de parches

Al seleccionar una frecuencia, el recuadro de la derecha mostrará las opciones que permitirán al administrador de la red precisar el inicio de la ventana de instalación de parches.

  - **Duración**: establece la duración de la ventana de instalación de parches. Si el proceso de instalación de parches supera el tiempo establecido, la política se interrumpe con error.
- **Ubicación de los parches**: permite definir el repositorio del cual los agentes PCSM recogerán los parches a instalar.
  - **Descargar parches desde Windows Update**: los dispositivos se conectarán al servidor Windows Update para la descarga de parches.
  - **Utilizar una caché local**: los equipos utilizan el dispositivo local configurado como cache de parches para las descargas.

> *Para más información sobre asignar el rol de cache de parches a uno o varios dispositivos de la red consulta el apartado 13.5.1 del capítulo 13*

  - **Permitir que los dispositivos contacten con Windows Update**: en caso de haber configurado el uso de dispositivos locales para las descargas de parches y no estar ninguno de ellos disponible, los equipos se conectarán al servidor Windows Update para descargar los parches necesarios.
- **Aprobación de parches**: establece filtros que seleccionan los parches a instalar. Los parches disponibles en un momento dado se dividen en dos categorías: parches aprobados y parches no aprobados.

- **Parches aprobados**: establece filtros en base a las características de los parches publicados por Microsoft para su instalación en los dispositivos afectados por la política.
- **Parches no aprobados**: establece filtros en base a las características de los parches publicados por Microsoft para excluirlos de su instalación. Los parches no aprobados tienen precedencia sobre los aprobados.

  Para definir un filtro consulta más adelante en este mismo capítulo.

- **Configurar parches individuales**: aprueba o rechaza parches de forma manual.
  - **Disponibles**: recoge todos los parches publicados en el directorio de Microsoft reportados como disponibles para su instalación.
  - **Aprobar**: parches que se seleccionan para su instalación.
  - **No aprobar**: parches que se rechaza su instalación.

    Los tres bloques implementan un sistema de búsqueda que permite filtrar los parches a mostrar según los criterios indicados a continuación:

    - **Prioridad**: muestra todos los parches de las prioridades seleccionadas: **Critico**, **Importante**, **Moderada**, **Baja**, **No especificada.**
    - **Puede requerir reinicio**: muestra todos los parches que requieran un reinicio para poder completar su instalación.
    - **Puede requerir información del usuario**: muestra todos los parches que requieran interacción con el usuario para poder completar su instalación.
    - **Buscar**: introduce una búsqueda libre sobre los campos que describen los parches.

      Una vez localizados los parches, selecciónalos y haz clic en el icono  para aprobarlos o en el icono  para excluirlos. Para exportar el listado de parches obtenido haz clic en el icono 

- **Opciones de energía**: determina el comportamiento del dispositivo antes y después de la instalación de los parches:
  - **Inicio**: arranca los dispositivos apagados compatibles con Wake-On-Lan 10 minutos antes de la instalación de los parches.

Es necesario que el soporte Wake-On-Lan este activado en la Bios del equipo y que haya un dispositivo en la red local con el rol de Nodo de red asignado

  - **Reinicio**: define el comportamiento del dispositivo después de la instalación de parches:
    - **Apagar**: apaga el equipo después de que expira la ventana de instalación
    - **Reiniciar los dispositivos**: reinicia el equipo si alguno de los parches instalados lo requiere. Si el equipo tiene un USB de almacenamiento conectado se impide el reinicio para prevenir un posible arranque desde el sistema operativo almacenado en el USB. Se puede evitar este comportamiento utilizando la casilla **Permitir el reinicio.**
    - **No reiniciar**: impide el reinicio del dispositivo y muestra al usuario una ventana de advertencia / recordatorio cada intervalo de tiempo especificado, pudiendo establecer un número máximo de posposiciones / rechazos.

15.5.3 Creación de filtros

En la sección **Aprobación de parches** se muestra una serie de recursos que permiten construir filtros avanzados que permiten agrupar parches según el criterio elegido.

Consulta el punto 6.4.2 para obtener una descripción sobre el procedimiento de creación de filtros

Los campos disponibles en la creación de un filtro tanto de aprobación como de no aprobación de parches se detallan a continuación:

- **(Todos)**: selecciona todos los parches publicados.
- **Categoría**: selecciona los parches según la categoría del parche.
- **Descripción**: busca cadenas de texto en el campo descripción de los parches publicados.
- **Tamaño de la descarga.**
- **Número de Kb**: selecciona los parches según la referencia al artículo de la Microsoft Knowledge base asociado.
- **Prioridad**: selecciona los parches según la severidad del parche publicado en los Microsoft Security Bulletins (**Crítica**, **Importante**, **Moderada**, **Baja**, **No especificada**). El contenido de este campo es independiente del publicado en el servicio Windows Update.
- **Reinicio**: selecciona los parches según el comportamiento del parche una vez instalado: **Nunca se reinicia** (0), **Siempre requiere reinicio** (1), **Puede solicitar reinicio** (2).
- **Fecha de lanzamiento.**
- **Solicitar entrada de usuario**: selecciona los parches que pueden requerir interacción por parte del usuario para completar su instalación (**Puede requerir**) o no la requieren nunca (**No la requiere**).
- **Título**: nombre del parche.
- **Tipo**: selecciona el parche si es software o driver.

15.5.4 Redefinición de políticas definidas en el nivel Cuenta

Para agilizar la creación de políticas específicas para zonas que se apartan de la configuración establecida en el Nivel Cuenta, **Panda Systems Management** permite modificar o redefinir partes de la política del Nivel Cuenta sin tener que generar una política completamente nueva. De esta forma el administrador gana en velocidad a la hora de configurar el sistema y ahorra tiempo de mantenimiento posterior, al gestionar un número de políticas inferior.

Para redefinir una política de Nivel Cuenta es necesario acceder al menú **Política** en la zona donde se quiere redefinir la política. En la parte inferior de la ventana se listan las políticas de **Gestión de parches** creadas en el nivel Cuenta. Estas políticas tienen el icono de un circulo verde situado a su izquierda para distinguirlas de las políticas normales, e incorporan el botón **Editar modificación.**

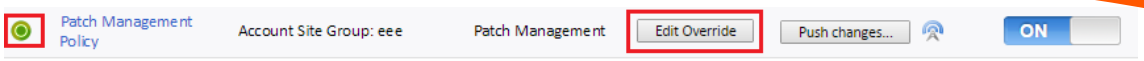


Figura 94: redefinición de políticas Patch Management

Al hacer clic en el botón **Editar modificación** se muestra la pantalla de configuración de la política del Nivel Cuenta, pero con nuevos controles que permiten su modificación selectiva. Al hacer clic en el nombre de la política, se mostrará la pantalla de configuración de la política original.

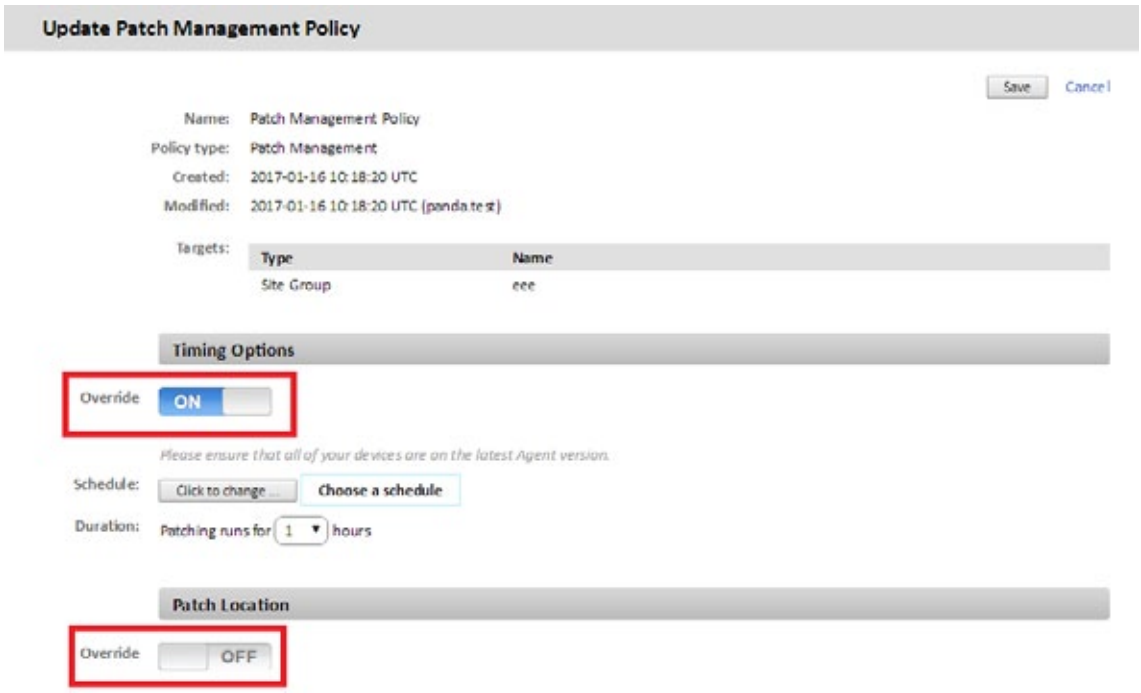


Figura 95: configuración de la aplicación de políticas Patch Management modificadas

Haz clic sobre los botones **Sustituir** para habilitar modificar y sobrescribir los valores configurados originalmente.

15.5.5 Modificaciones particulares para cada dispositivo

En el menú **Administrar** del Nivel Dispositivo que representa a cada equipo de la red, se pueden refinar los parches aprobados y no aprobados en las etapas anteriores del proceso de creación de una política Gestión de parches. Además, esta pantalla muestra cuándo se ejecutó la política Gestión de parches asignada al dispositivo y fuerza su ejecución nuevamente si fuera necesario.

En esta pantalla se divide en dos secciones, una primera de control de las políticas aplicadas sobre el dispositivo y otra que contiene los parches aprobados y no aprobados por reglas establecidas en la policía Gestión de parches asignada al dispositivo.

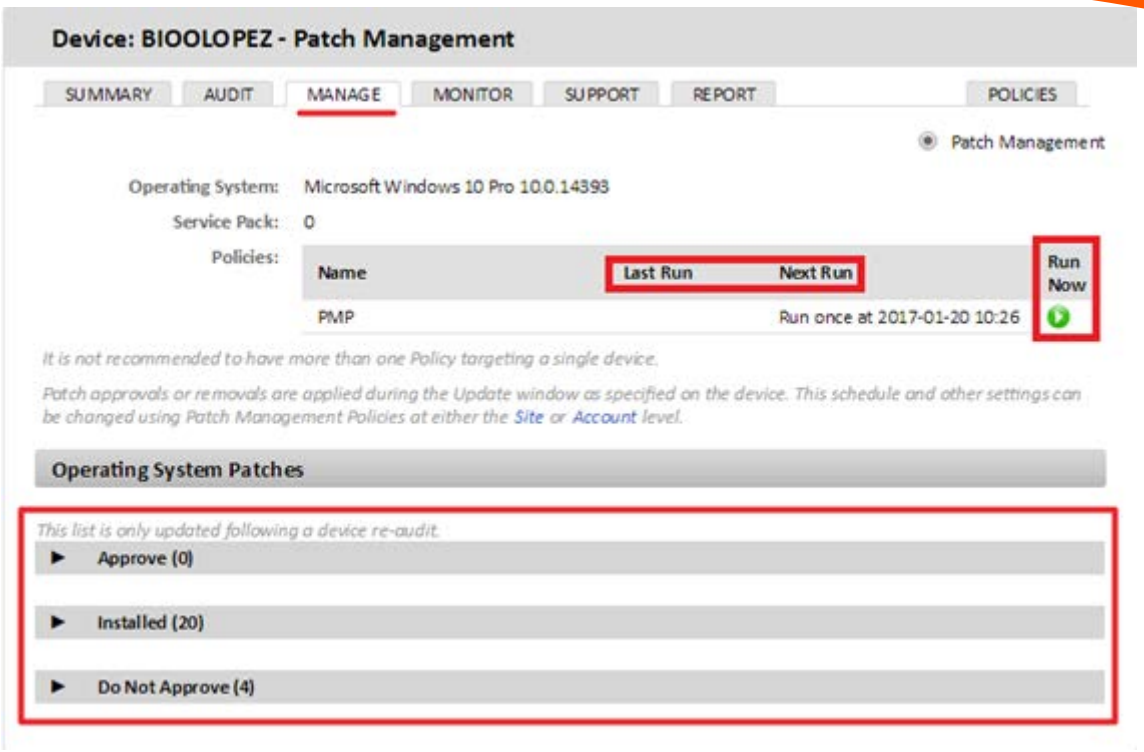


Figura 96: modificación de politicas Patch Management aplicadas a un dispositivo particular

Estado de la política Gestión de parches asignada

En esta primera sección se incluye información sobre el sistema operativo instalado en el dispositivo y su nivel de Service Pack. Además, se incluye información sobre las políticas que se están aplicando al dispositivo:

- **Nombre**: nombre de la política.
- **Última ejecución**: fecha con su última ejecución.
- **Siguiente ejecución**: fecha con la próxima ejecución según la programación configurada en la política.
- **Ejecutar ahora**: fuerza la ejecución de la política independientemente de la programación configurada.

Parches del sistema operativo

El objetivo principal de esta sección es permitir al administrador refinar los parches a instalar en dispositivos concretos.

Los parches a gestionar se organizan en tres bloques mostrados a continuación:

- **Aprobar**: son los parches asignados al dispositivo que todavía están pendientes de instalación. Estos parches se instalarán en la próxima ejecución de la política Gestión de parches asignada.
- **Parches instalados**: son los parches asignados al dispositivo y ya instalados.
- **No aprobar**: son los parches que no han sido aprobados para su instalación en este dispositivo. Si un dispositivo no tiene asignada una política de parches que los apruebe para su instalación, todos los parches publicados por Microsoft aparecerán en este bloque.

Si un parche se desinstala de forma manual en el equipo y no se añade una entrada en este bloque que lo excluya, el parche se volverá a instalar en la próxima ejecución de la política de Gestión de parches.

Para desinstalar remotamente un parche utiliza el componente Uninstall Windows Update by KB Number

En cada uno de los tres bloques se incluye un juego de filtros de búsqueda que permiten localizar de forma rápida parches concretos según sus características.

- **Prioridad**: muestra todos los parches de las prioridades seleccionadas: **Crítico**, **Importante**, **Moderada**, **Baja**, **No especificada.**
- **Puede requerir reinicio**: muestra todos los parches que requieran un reinicio para poder completar su instalación.
- **Puede requerir información del usuario**: muestra todos los parches que requieran interacción con el usuario para poder completar su instalación.
- **Buscar**: introduce una búsqueda libre sobre los campos que describen los parches.

15.5.6 Escenarios de uso del método Gestión de parches

- Cuando necesites una precisión completa a la hora de definir los parches que se instalarán en cada dispositivo.
- Cuando necesites instalar todos los parches sin excepción, de forma automática y centralizada.
- Cuando necesites iniciar y apagar los equipos antes y después de la instalación de parches de forma automática.

15.6. Estado de la actualización de los dispositivos

En la pestaña **Administrar** del Nivel Zona o Nivel Cuenta, seleccionando **Gestión de parches**, se muestra de un solo vistazo el estado del parque informático administrado en lo que a instalación y aplicación de parches se refiere.

La pantalla de administrar se divide en tres zonas claramente diferenciadas:

- **Gráfico de tarta**: indica en porcentajes los dispositivos actualizados y con parches pendientes de instalación.
- **10 dispositivos más vulnerables**: incluye los 10 equipos que demandan atención con mayor prioridad en lo relativo a la actualización e instalación de parches pendientes.

- **Listado de políticas asignadas**: ayuda a localizar las policías de tipo Gestión de parches asignadas a la zona.

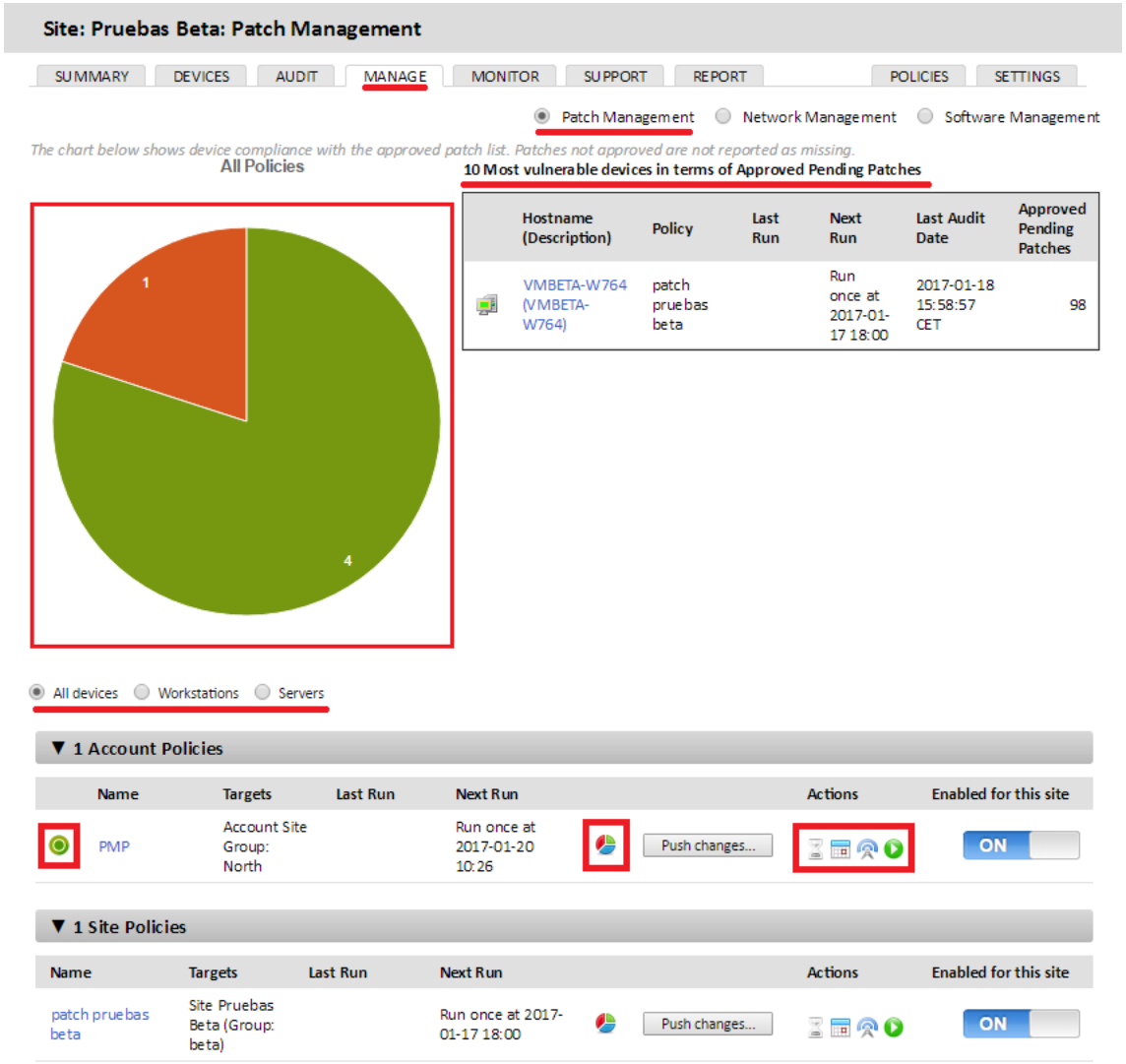


Figura 97: pantalla de estado del parque informático para Patch Management

Gráfico de tarta

El grafico de tarta permite determinar el porcentaje de equipos que están actualizados y los que tienen parches pendientes de instalación.

Un equipo se considera actualizado cuando todos sus parches aprobados están instalados correctamente. De esta manera, en color rojo únicamente se mostrarán aquellos equipos que, teniendo parches aprobados, no han sido instalados todavía, o han producido algún tipo de error que ha impedido su completa actualización.

Inicialmente el grafico representa a todos los dispositivos de la zona / cuenta. Haz clic en el icono  del listado de políticas asignadas para reflejar únicamente los dispositivos asignados a esa política.

Además, en la parte inferior del gráfico se incorpora un selector que permite filtrar los datos mostrados por el tipo de dispositivo (**Todos los dispositivos**, **Estaciones de trabajo**, **Servidores**).

Listado 10 equipos más vulnerables

Es una lista de los equipos más vulnerables en cuento a parches pendientes de instalación. El listado se ordena de mayor a menor número de parches pendientes de instalación sin atender a su importancia. Por cada equipo se presenta la información siguiente:

- **Nombre del host**: nombre del dispositivo. Haciendo clic la consola PCSM presentará la pestaña **Administrar** del Nivel Dispositivo asociado al equipo.
- **Zona**: en el Nivel Cuenta se muestra la zona a la que pertenece el dispositivo.
- **Policy**: nombre de la política Gestión de parches asignada al dispositivo.
- **Ultima ejecución**: última vez que la política Gestión de parches fue ejecutada en el dispositivo.
- **Siguiente ejecución**: próxima ejecución programada según la configuración de la política. Si la política fue definida en el Nivel Cuenta y fue modificada en el Nivel Zona, se mostrará el resultado de la modificación.
- **Fecha de la última auditoría**: fecha con la última auditoría realizada en el dispositivo.
- **Parches aprobados pendientes**: número de parches aprobados por la política asignada pero que todavía no se han instalado en el equipo.

Listado de políticas asignadas

En esta sección se listan todas las políticas de tipo Gestión de parches creadas, separados en dos bloques según el nivel donde fueron creadas (Cuenta o Zona).

Por cada política listada se presenta la información mostrada a continuación:

- **Icono de modificación activa**  . indica si la cuenta fue creada en el Nivel Cuenta y actualmente está modificada en el nivel Zona. Para visualizar las modificaciones en el Nivel Zona, haz clic en la pestaña políticas. Para visualizar la configuración original de la política haz clic en su nombre.
- **Nombre**: nombre de la política.
- **Destinos:** dispositivos afectados por la política según su configuración.
- **Última ejecución:** fecha en la que la política se ejecutó por última vez.
- **Siguiente ejecución**: fecha de la próxima ejecución de la política según la configuración establecida.
-  : filtra el gráfico de tarta y el listado de los equipos más vulnerables presentados anteriormente, para reflejar únicamente los dispositivos afectados por la política.
- **Aplicar cambios**: aplica de forma inmediata los cambios efectuados en la política.
- **Acciones**: controla ciertos aspectos de la política.
  -  : visualiza los resultados de la última ejecución de la política incluyendo: **Descripción del parche**, **Tamaño**, **Dispositivos de destino**, **Instalaciones correctas**, **Errores.**

-  : muestra los parches que se instalarían si la política fuera lanzada en el momento actual. De esta forma es posible validar la política creada comprobando que los parches no aprobados no se incluyen en el listado y que todos los parches a instalar se encuentran en el listado.
-  : muestra un listado de todas las zonas afectadas por la política, indicando además si alguna de las zonas ha redefinido alguna configuración y permitiendo habilitar o deshabilitar la política por zona.
-  : ejecuta la política en el momento actual, sin esperar a la programación configurada.

- **Activado para esta zona**: activa o desactiva la política para la zona.

15.7. Tabla comparativa de métodos de Patch Management.

Método	Nivel de detalle de la selección de parches	Automatización	Tiempo de configuración
Windows Update	Bajo Selección de parches según grupos "Importantes" y "Recomendados".	Alto Se configuran una vez los grupos de parches a instalar.	Bajo Elegir si instalar los parches "importantes" y "opcionales".
Gestión de parches	Medio Selección de parches por múltiples criterios configurables.	Alto Una vez creados los filtros, los parches se instalan automáticamente según Microsoft los libere.	Medio Establecer los filtros para seleccionar los parches a instalar.

Tabla 25: comparativa de politicas de aplicación de parches disponibles en Panda Systems Management

16. Cuentas de usuario y roles

16.1. Cuentas de usuario

Una cuenta de usuario es un recurso formado por información que regula el acceso a la consola PCSM y las acciones que los técnicos pueden realizar sobre los dispositivos de los usuarios.

Las cuentas de usuario son utilizadas únicamente por los administradores de IT que acceden a la consola PCSM o a otros servicios ofrecidos por **Panda Systems Management**.

Generalmente, cada administrador de IT tiene una única cuenta de usuario.

Los usuarios de dispositivos no necesitan ningún tipo de cuenta de usuario, ya que no acceden a la consola PCSM. El agente instalado en sus dispositivos está por defecto configurado en modo monitor de forma que no requiere de ninguna interacción por parte del usuario.

A diferencia del resto del manual donde "usuario" es la persona que utiliza un dispositivo gestionado por el administrador con la ayuda de Panda Systems Management, en este capítulo "usuario" puede referirse a una cuenta de usuario o cuenta de acceso a la consola.

16.2. El usuario principal

El usuario principal es la cuenta de usuario suministrada por Panda Security al cliente en el momento de provisionar el servicio **Panda Systems Management**. Esta cuenta tiene asignado el rol **administrador** explicado más abajo en este mismo capítulo.

Por motivos de seguridad, el cambio de contraseña del usuario principal, el cambio de su configuración o el acceso al servicio haciendo login desde un agente PCSM están bloqueados.; no obstante, con la cuenta de usuario principal se permite el acceso al agente instalado en el equipo del administrador si se hace desde la propia consola PCSM.

16.3. Roles

Un rol es una configuración específica de permisos de acceso a la consola que se aplica a una o más cuentas de usuario. De esta forma, un administrador concreto estará autorizado a ver o modificar determinados recursos de la consola según el rol al que pertenezca la cuenta de usuario con la que acceda a **Panda Systems Management**.

Una o más cuentas de usuario pueden pertenecer a uno o más roles.

Los roles solo afectan al nivel de acceso de los administradores de IT a los recursos de la consola para gestionar los dispositivos de la red. No afectan al resto de usuarios de dispositivos.

16.4. Objetivo de los roles

En un departamento de IT pequeño, todos los técnicos van a acceder a la consola como administradores sin ningún tipo de límite; sin embargo, en departamentos de IT de mediano o gran tamaño o en partners con muchos clientes es posible que sea necesario organizar el acceso a los dispositivos aplicando tres criterios:

- **Según la cantidad de dispositivos a administrar.**

Redes de tamaño medio/grande o redes pertenecientes a delegaciones de una misma empresa o a distintos clientes de un mismo partner pueden requerir de la distribución y asignación de dispositivos a técnicos. De esta forma, los dispositivos de una delegación administrados por un técnico determinado serán invisibles para los técnicos que administren los dispositivos de otras delegaciones.

También pueden existir restricciones de acceso a datos delicados de clientes concretos que requieran un control exacto de los técnicos que van a poder manipular los dispositivos que los contienen.

- **Según el cometido del dispositivo a administrar.**

Según la función que desempeñe, un dispositivo puede asignarse a un técnico experto en ese campo: por ejemplo, los servidores de bases de datos de un cliente o de todos los clientes gestionados por el partner pueden ser asignados a un grupo de técnicos especialistas, y de esa misma forma otros servicios como, por ejemplo, servidores de correo, podrían no ser visibles para este grupo.

- **Según los conocimientos del técnico.**

Según las capacidades del técnico o su función dentro del departamento de IT, puede requerirse únicamente un acceso de monitorización/validación (solo lectura) o, por el contrario, uno más avanzado, como el de modificación de configuraciones de dispositivos.

Los tres criterios se pueden solapar, dando lugar a una matriz de configuraciones muy flexible y fácil de establecer y mantener, que permite delimitar perfectamente las funciones de la consola accesibles a cada técnico, según su perfil y responsabilidades.

16.5. El rol administrador

Una licencia de uso de **Panda Systems Management** viene con un rol de control total predefinido, llamado **administrador**. A este rol pertenece la cuenta de administración creada por defecto y con ella es posible realizar absolutamente todas las acciones disponibles en la consola. **administrador,** además, es el único rol que puede crear nuevos roles y usuarios, así como modificar los ya existentes.

El rol **administrador** no puede borrarse del servidor y cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola.

Todos los procedimientos descritos en este capítulo requieren de una cuenta que pertenezca al rol administrador.

16.6. Acceso a la configuración de cuentas de usuarios y roles

Haz clic en el menú general **Cuenta** para acceder a la gestión de roles y cuentas de usuario:

- **Pestaña Usuarios**: crea nuevas cuentas de usuario y define su pertenencia a uno o varios roles.
- **Pestaña Roles**: crea y modifica una nueva configuración de acceso a los recursos de **Panda Systems Management.**

Las pestañas de Usuarios y roles solo son accesibles si el usuario pertenece al rol especial administrador.

16.7. Creación y configuración de cuentas de usuario

Haz clic en el menú general **Cuenta, Usuarios** para crear y modificar cuentas de usuario.

- **Añadir nueva cuenta de usuario**: haz clic en **Añadir usuario** para añadir un nuevo usuario, establecer su contraseña, indicar el nivel o roles a los que pertenece y establecer su **Nivel componente** asociado (de 1 a 5).

El Nivel componente asociado al usuario permite restringir el acceso a aquellos componentes desarrollados o importados de la ComStore cuyo Nivel componente sea superior.

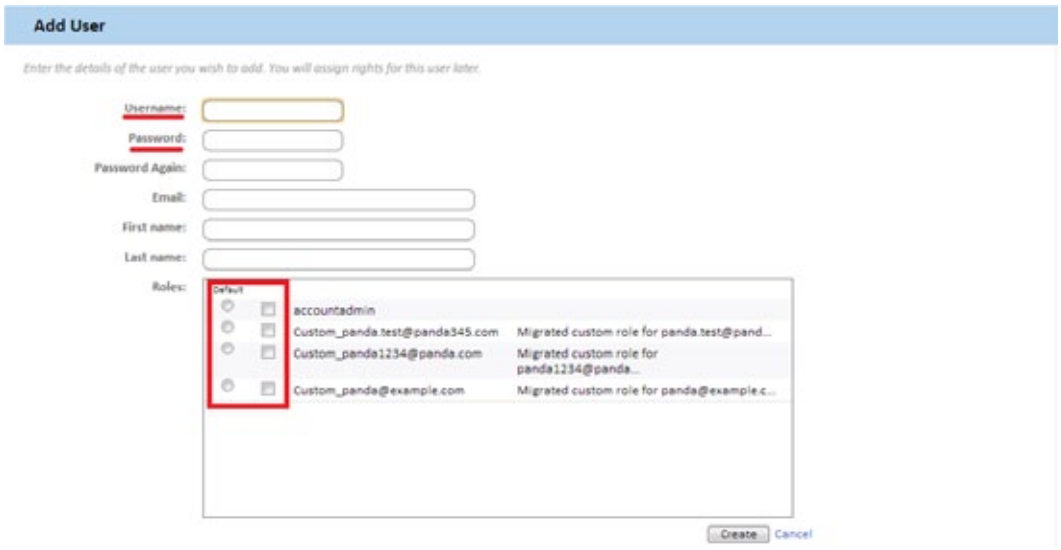


Figura 98: asignación de nombre de usuario, contraseña y rol a una cuenta de acceso

- **Editar una cuenta de usuario**: haz clic en el nombre del usuario para mostrar un formulario con todos los datos de la cuenta.
- **Borrar o desactivar cuentas de usuarios**: selecciona los usuarios con las casillas asociados y haz clic en los iconos de prohibido y aspa de la **Barra de Acciones**.
- **Dar permisos de control total**: haz clic en el botón On/OFF en **Administrador**.

Una cuenta de usuario puede pertenecer a un único rol o a más de uno. En este último caso, en la consola se mostrará un desplegable mediante el cual es posible elegir el rol con el que la cuenta de usuario opera.

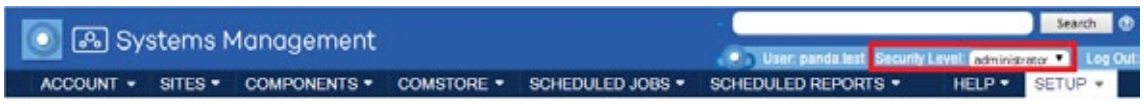


Figura 99: cambio de rol de la cuenta con una sesión ya iniciada

16.8. Creación y configuración de roles

Haz clic en el menú general **Cuenta, roles** para crear y modificar roles.

- **Añadir nuevo rol**: haz clic en **Añadir rol e** introduce el nombre del rol y si quieres tomar como base una configuración/plantilla vacía o el nuevo rol se basa en uno anterior.
- **Editar un rol**: haz clic en el nombre del rol o en el icono del lápiz para mostrar su configuración.
- **Borrar rol**: haz clic en el icono X.

Si al borrar un rol tiene cuentas de usuario asignadas, se nos preguntará qué nuevo rol será asignado a esas cuentas.

16.9. Configuración de roles

La configuración de un rol se divide en cuatro apartados:

- **Visibilidad de los dispositivos**: habilita o restringe el acceso a agrupaciones de dispositivos.
- **Permisos**: habilita o restringe el acceso a funcionalidades de la consola**.**
- **Herramientas del explorador del agente**: habilita o restringe el acceso a funcionalidades en el agente**.**
- **Miembros**: indica las cuentas de usuario que pertenecen al rol configurado.

16.9.1 Visibilidad de los dispositivos.

Este grupo de configuración establece qué dispositivos de la red serán visibles para los usuarios de la consola que pertenezcan a un rol determinado.

El sistema de roles de **Panda Systems Management** permite establecer el acceso a los cuatro tipos de agrupaciones estáticas disponibles:

- Zonas
- Grupos de dispositivos de zona
- Grupos de dispositivos
- Grupos de zonas

> *No es posible establecer el acceso a agrupaciones dinámicas como filtros.*

El sistema de roles permite establecer el acceso a cada elemento individual dentro de cada tipo de agrupación de dispositivos disponible. Para definir el acceso a los elementos dentro de uno de los cuatro tipos de agrupación haz clic en el botón **ON** correspondiente. Se mostrará su panel de configuración asociado.

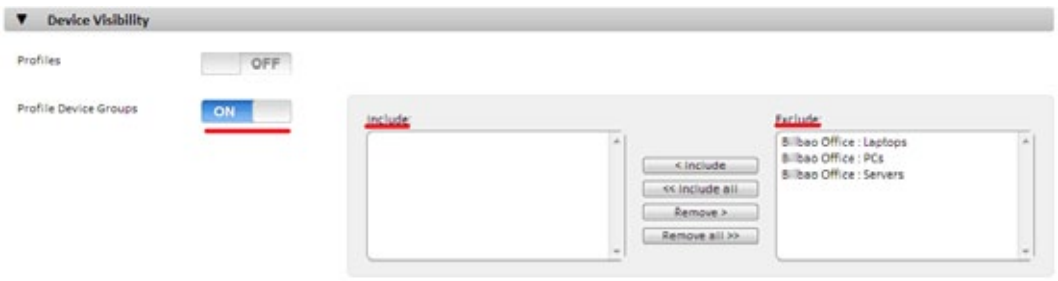


Figura 100: panel de configuración de elementos de agrupación por tipo

Un elemento (grupo) incluido en la caja de texto **Incluir** será visible para todas las cuentas de usuario que pertenezcan a ese rol. De la misma forma, si el elemento (grupo) se muestra en la caja de texto **Excluir,** no será visible en la consola.

16.9.2 Permisos

Permisos establece el acceso a cada uno de los recursos de la consola. Para ello presenta en un primer nivel el listado de áreas disponibles en la consola, que coinciden con las entradas del menú general:

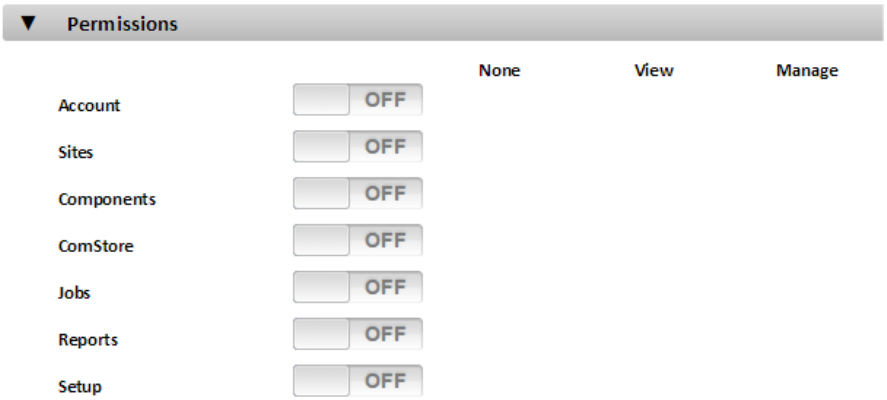


Figura 101: elementos del menú general

Para establecer el nivel de acceso del rol a cada una de las áreas de la consola (pestañas del menú general) haz clic en el botón ON, con lo cual se desplegarán los recursos asociados a cada área. Por ejemplo, al hacer clic en el botón ON de la entrada Cuenta se muestran los recursos de esta área y se permite indicar el nivel de acceso a cada uno de ellos.

Los niveles de acceso son tres:

- **Desactivado**: el recurso no se muestra en la consola.
- **Vista:** el recurso se muestra en la consola, pero no permite la configuración ni modificación de parámetros**.**
- **Administrar:** el recurso se muestra en la consola y se permite el acceso completo.

16.9.3 Herramientas del explorador del agente

Este grupo de configuración especifica el acceso a las diferentes herramientas de administración remota disponibles en el agente.

Cualquier cambio efectuado en Herramientas del explorador del agente debe ir acompañado de un reinicio del agente.

Estas restricciones aplican a la consola local del agente, al iniciar sesión para administración dispositivos remotos (modo administrador).

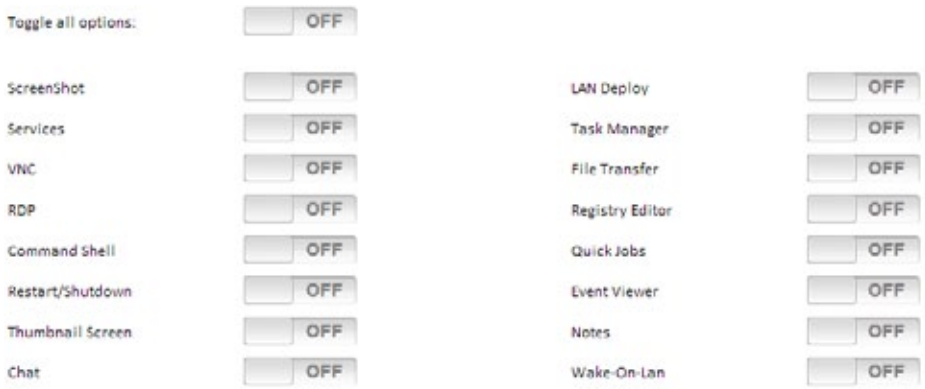


Figura 102: configuración del acceso a las herramientas de administracion del agente PCSM

16.9.4 Miembros

Configura las cuentas de usuario que pertenecen al rol modificado.

16.10. Estrategias para el diseño de roles

Es posible generar tantos roles como se consideren necesarios, teniendo en cuenta que el objetivo final de un rol es el de limitar el acceso de los administradores a dispositivos o a recursos de la consola para aportar así una mayor seguridad y protección contra el fallo humano. Sin embargo, esta mayor seguridad viene de la mano de una menor flexibilidad a la hora de reutilizar el personal técnico entre varios clientes o tareas, de modo que el número exacto de roles en un sistema lo dará la ponderación que se haga de estas dos variables: flexibilidad y seguridad.

16.10.1 Roles de tipo horizontal

Como norma general, una empresa con varias delegaciones y un equipo de IT independiente por cada delegación buscará un rol de control total pero limitado a los dispositivos de cada delegación.

De esta forma, los dispositivos administrados por la delegación A no serán visibles por la delegación B y viceversa.

Por el contrario, en una empresa con varias delegaciones será necesaria la siguiente configuración por cada delegación:

- 1 zona o grupo de dispositivos que agrupe a los dispositivos de la delegación.
- 1 rol que permita el acceso a los dispositivos de la zona y deniegue el resto.
- Una cuenta por cada técnico, asignada al rol que cubra la delegación designada.

El mismo esquema se puede utilizar para el partner que quiera segregar clientes y asignarlos a técnicos concretos.

16.10.2 Roles de tipo vertical

Para dispositivos fuertemente orientados a tareas específicas, como pueden ser servidores de impresión, bases de datos, correo, etc., pueden crearse roles que limiten el acceso a este tipo de dispositivo.

De esta forma, una empresa o partner que tenga múltiples delegaciones o clientes con servidores de correo puede querer agruparlos y asignarlos a un grupo de técnicos para su administración, mientras el resto de técnicos de perfil más generalista se dedican a mantener los dispositivos de usuario.

Será necesaria la siguiente configuración general:

- Un grupo de dispositivos que agrupe a todos los servidores de correo independientemente de la zona /cliente/delegación al que pertenezcan.
- Un rol A que permita el acceso a los dispositivos contenidos en el grupo de dispositivos y deniegue el acceso al resto de dispositivos.
- Un rol B que deniegue el acceso a los dispositivos contenidos en el grupo de dispositivos y permita el acceso al resto de dispositivos.
- Tantas cuentas de usuario de rol A como técnicos lleven el mantenimiento de los servidores de correo de la empresa o partner.
- Tantas cuentas de usuario de rol B como técnicos lleven el mantenimiento de los dispositivos de usuario de la empresa o partner.

16.10.3 Roles de acceso a recursos

Atendiendo al perfil o grado de experiencia de cada técnico, el director del departamento de informática puede dividir el trabajo de los miembros de su departamento. De esta forma, es posible crear grupos de técnicos con responsabilidades complementarias:

- Técnicos de monitorización y generación de Informes: con acceso completo a la barra de pestañas **Informes** y acceso de solo lectura al resto de la consola.
- Técnicos de desarrollo de scripts y despliegue de software: con acceso al menú general **Componentes** y **ComStore**.
- Técnicos de soporte: con acceso a la barra de pestañas **Soporte** y a los recursos del dispositivo del usuario a través del agente**.**

También es posible limitar el acceso a determinados componentes de la **ComStore** o desarrollados por el departamento de IT que realicen operaciones delicadas en los dispositivos del usuario, asignando niveles de componente superior al establecido en la cuenta de usuario.

17. Gestión de dispositivos móviles

Plataformas soportadas

Políticas de administración de dispositivos móviles

Herramientas para la gestión remota de dispositivos móviles

17.1. Introducción

Panda Systems Management incluye herramientas de MDM (Mobile Dispositivo Management) que permite gestionar el parque de dispositivos móviles de la empresa de una forma sencilla y centralizada. Con **Panda Systems Management** podrás hacer frente a la creciente presencia de dispositivos móviles en tu empresa desde la misma consola que ahora utilizas para gestionar el resto de tu parque informático.

17.2. Plataformas soportadas

Panda Systems Management es compatible con tablets y smartphones iOS y Android.

Los terminales iPhone y tablets iPad que soporten iOS 7 o superior son compatibles con **Panda Systems Management**. A continuación, se ofrece un listado orientativo:

Modelo
iPhone 4, 4S
iPhone 5, 5c, 5s, SE
iPhone 6, 6 Plus
iPhone 6s, 6 Plus
IPhone 7, 7 Plus
IPhone 8, 8 plus
IPhone X
Ipod Touch 5º, 6º generación
iPad 2, 3, 4, Air, Air 2, mini, mini 2, mini 3, mini 4, Pro (todos los tamaños)

Tabla 26: listado de dispositivos iOS compatibles con Panda Systems Management

Los terminales Android compatibles son todos aquellos que soporten la versión 2.3.3 (Gingerbread) y superiores, en la actualidad la práctica totalidad de los terminales en circulación.

17.3. Políticas de administración de dispositivos móviles

Para gestionar y controlar el uso de los dispositivos móviles, **Panda Systems Management** ofrece un conjunto de políticas que permiten configurar los teléfonos móviles y tablets basados en plataformas iOS. Así, el usuario dispondrá desde el primer momento de un dispositivo preparado para su uso en entornos corporativos e integrado en la infraestructura de la empresa.

Consulta el Capítulo 9: Políticas para obtener más información.

Solo se permite la activación de una política de administración de dispositivos móviles en un momento dado.

17.3.1 Políticas obligatorias u opcionales

En el momento de la creación de la política, el administrador tiene que determinar la obligatoriedad de la misma. De esta forma, en la pantalla de creación de la política se puede elegir entre **Permitir a los usuarios eliminar esta política** o **Exigir contraseña para eliminar esta política**. En función de lo elegido, los usuarios podrán desactivar manualmente desde el propio dispositivo móvil la política establecida por el administrador o tendrán que introducir una contraseña establecida por el administrador para poder eliminar la política.

17.3.2 Tipos de políticas de administración de dispositivos móviles

Existen cuatro tipos de políticas de administración de dispositivos móviles disponibles. Cada una de ellas afecta a un conjunto de características y configuraciones del dispositivo móvil.

- **Códigos de acceso**: características de las contraseñas introducidas por el usuario en el dispositivo móvil, bloqueo del terminal, etc.
- **Restricciones**: gestión del acceso a los recursos del terminal.
- **VPN**: configuración de VPN.
- **Wi-Fi**: configuración de la conexión Wifi.

Códigos de acceso

Campo	Descripción
Nivel de protección de los códigos de acceso	Define la fortaleza mínima de la contraseña elegida por el usuario.
Longitud mínima de los códigos de acceso	
Número mínimo de caracteres complejos	Establece el número mínimo de caracteres no alfanuméricos necesarios para dar por válida una contraseña nueva.
Antigüedad máxima de los códigos de acceso	Define la duración máxima de una contraseña.
Bloqueo automático	

Campo	Descripción
Historial de códigos de acceso	El dispositivo mantiene un histórico de contraseñas ya utilizadas por el usuario para evitar su repetición al elegir una contraseña nueva.
Número máximo de intentos fallidos	

Tabla 27: configuración de las caracteristicas de la contraseña

Restricciones

Campo	Descripción
Permitir el uso de cámaras	Deshabilita las cámaras y elimina los iconos correspondientes de la pantalla de inicio. Impide que los usuarios puedan sacar fotos, vídeos o utilizar FaceTime.
Permitir la instalación de aplicaciones	Deshabilita App Store y elimina el icono de App Store de la pantalla de inicio. Impide que los usuarios puedan instalar o actualizar ninguna aplicación mediante App Store o iTunes.
Permitir la captura de pantalla	Permite que el usuario haga capturas de pantalla.
Permitir el marcado por voz	Permite que el usuario marque mediante comandos de voz.
Permitir FaceTime	Permite que el usuario haga o reciba video llamadas con FaceTime.
Permitir sincronización automática en itinerancia	Permite al dispositivo sincronizar automáticamente las cuentas incluso cuando el dispositivo se encuentre en itinerancia.
Permitir Siri	Permite el uso de Siri.
Permitir Siri mientras está bloqueado	Permite el uso de Siri cuando el dispositivo está bloqueado.
Permitir notificaciones de Passbook mientras está bloqueado	Permite el uso de Passbook cuando el dispositivo está bloqueado
Permitir compras desde aplicaciones	Permite la compra a través de aplicaciones internas.
Obligar a los usuarios a introducir la contraseña de iTunes Store para todas las compras	Solicita la contraseña de iTunes cada vez que se realiza una descarga.
Permitir el juego multijugador	Permite participar en juegos multijugador.
Permitir añadir amigos de Game Center	Permite añadir amigos a Game Center.
Mostrar Control Center en la pantalla de bloqueo (iOS 7)	Permite acceder a Game Center cuando el dispositivo está bloqueado.
Mostrar Notification Center en la pantalla de bloqueo (iOS 7)	Muestra el Centro de Notificaciones cuando el dispositivo está bloqueado.
Mostrar vista Today en la pantalla de bloqueo (iOS 7)	Muestra la vista "Hoy" del Centro de Notificaciones cuando el dispositivo está bloqueado.
Permitir documentos de aplicaciones administradas en aplicaciones no administradas (iOS 7)	Permite compartir y utilizar datos de una aplicación corporativa en una aplicación personal no distribuida por la empresa.

Campo	Descripción
Permitir documentos de aplicaciones no administradas en aplicaciones administradas (iOS 7)	Permite compartir y utilizar datos de una aplicación personal en una aplicación corporativa distribuida por la empresa.
Permitir el uso de iTunes Store	Permite acceder a iTunes Store.
Permitir el uso de Safari	Permite el uso de Safari.
Activar la opción de autorrellenar en Safari	Permite la opción de auto-completado.
Forzar la advertencia de fraude en Safari	Safari mostrará una advertencia cuando el usuario visite un sitio Web fraudulento o peligroso.
Activar javascript en Safari	Permite JavaScript.
Bloquear ventanas emergentes en Safari	Permite las ventanas emergentes.
Permitir la copia de seguridad en iCloud	Permite hacer copias de seguridad de datos.
Permitir la sincronización de documentos con iCloud	Permite la sincronización de documentos.
Permitir la sincronización con iCloud Keychain (iOS 7)	Permite la sincronización automática con iCloud de los nombres de usuario, contraseñas, números de tarjeta de crédito, etc.
Permitir transmisión de fotos	Permite transmitir fotografías vía streaming
Permitir transmisiones compartidas	Permite compartir secuencias de streaming.
Permitir el envío de datos de diagnóstico a Apple	Permite enviar información de diagnóstico a Apple.
Permitir al usuario que acepte certificados TLS no fiables	Permite el uso de certificados TLS que no sean de confianza.
Forzar copia de seguridad cifrada	Fuerza el cifrado de las copias de seguridad.
Permitir actualizaciones automáticas para certificar la configuración de confianza (iOS 7)	Permite la actualización automática de los certificados de confianza.
Forzar seguimiento limitado de anuncios (iOS 7)	Limita el seguimiento de anuncios en el dispositivo.
Permitir huella dactilar para desbloquear (iOS 7)	Permite desbloquear el dispositivo con la huella dactilar.
Permitir música y podcasts explícitos	Permite música y podcasts explícitos.
Calificar aplicaciones	Permite utilizar aplicaciones según su clasificación.
Calificar películas	Permite ver películas según su clasificación.
Calificar programas de televisión	Permite ver programas de TV según su clasificación.
Mostrar iMessage	Permite el uso de iMessages.
Permitir la eliminación de aplicaciones	Permite la desinstalación de aplicaciones.
Permitir Game Center	Permite el uso de Game Center.
Permitir Bookstore	Permite acceder a la tienda de iBooks.
Permitir contenidos eróticos de Bookstore	Permite la descarga de contenidos etiquetados como eróticos.

Campo	Descripción
Permitir la instalación de perfiles de configuración de interfaz	
Permitir la modificación de la configuración de las cuentas (iOS 7)	Permite al usuario modificar la configuración de sus cuentas: añadir y eliminar cuentas de correo, modificar la configuración de iCloud, iMessages, etc.
Permitir AirDrop (iOS 7)	Permite compartir documentos con AirDrop.
Permitir cambios en el uso de datos móviles para las aplicaciones (iOS 7)	Restringe el consumo de datos móviles para algunas aplicaciones específicas.
Permitir contenido generado por el usuario en Siri	Permite a Siri consultar contenido de la Web (Wikipedia, Bing y Twitter).
Permitir la modificación de la configuración de Find My Friends	Permite modificar la configuración de "Find my Friends".
Permitir el emparejamiento de hosts	Permite emparejar el dispositivo con cualquier otro equipo. Si la opción está deshabilitada, sólo será posible emparejar el dispositivo con un host que disponga de Apple Configurator.

Tabla 28: configuración de las restricciones de uso del dispositivo

VPN

Campo	Descripción
Nombre de la conexión	Nombre de la conexión VPN.
Tipo de conexión	Tipo de VPN (L2TP, PPTP, IPSec).
Servidor	Dirección IP del servidor de VPN.
Secreto compartido	Secreto compartido entre el servidor y el cliente.
Autenticación del usuario	Método de autenticación: contraseña o esquema de clave pública – privada.
Cuenta	Cuenta del usuario para autenticar la conexión.
Tipo de proxy	Configura el proxy a utilizar con la conexión VPN.

Tabla 29: configuración de la VPN

Wifi

Campo	Descripción
SSID	Establece el Service Set IDentifier.
Seguridad	Tipo de seguridad de la red inalámbrica.
Contraseña	Contraseña de la red inalámbrica.

Campo	Descripción
Tipo de proxy	Configura el proxy a utilizar con la conexión Wi-Fi.

Tabla 30: configuracion de la conexión WiFI

17.4. Herramientas para la gestión remota de dispositivos móviles

A continuación, se detallan las herramientas disponibles desde la consola, su modo de funcionamiento y sus beneficios asociados.

Las funcionalidades específicas de la consola se muestran únicamente en el Nivel Dispositivo que se corresponde al dispositivo a administrar.

Al mostrar el dispositivo en la consola, la **Barra de acciones** y la barra de pestañas se adaptan de forma automática, habilitando las nuevas acciones disponibles.

17.4.1 Borrado del dispositivo (Dispositivo Wipe)

Devuelve el dispositivo a su estado original para prevenir el robo de información en caso de pérdida o sustracción, o ante casos de mal funcionamiento del terminal.

Todos los datos personales del terminal, programas instalados por el usuario, configuraciones particulares y modificaciones se perderán de forma irreversible. El estado del terminal se revierte al original entregado de fábrica.

17.4.2 Geolocalización

Representa la posición del dispositivo en un mapa. Las coordenadas del dispositivo para situarlo en un punto del mapa son obtenidas de diferentes formas en función de los recursos disponibles del dispositivo, siendo muy variable su nivel de precisión. A continuación, se listan las tecnologías soportadas, ordenadas de mayor a menor precisión.

- GPS (Global Positioning System)
- WPS (Wifi Position System)
- GeoIP

Los dispositivos posicionados con GeoIP pueden aparecer en localizaciones totalmente diferentes a donde se encuentran realmente.

17.4.3 Bloqueo del dispositivo (Lock Device)

Apaga la pantalla del dispositivo, y si estaba establecido un PIN de seguridad se le solicitara de nuevo al usuario cuando active el móvil. Este bloqueo del dispositivo resulta útil en caso de robo del terminal.

17.4.4 Desbloqueo del dispositivo (Unlock Device)

Resetea el PIN en el caso de que el usuario haya olvidado su contraseña.

17.4.5 Política de contraseña (Password Policy)

Obliga al dueño del terminal a establecer una contraseña (PIN). Una vez establecida, el administrador podrá bloquear el dispositivo si es robado, de forma que al encenderlo de nuevo se pedirá la contraseña establecida por su legítimo dueño.

Esta funcionalidad lanza de forma remota un requerimiento al usuario para establecer el PIN, no permite al administrador establecerlo desde la consola.

17.4.6 Auditorias

Las auditorias funcionan de la misma manera que en dispositivos Windows, quedando totalmente integradas en la consola. De esta manera, por ejemplo, se pueden aplicar filtros a dispositivos móviles en base a los programas instalados.

El agente instalado en el dispositivo móvil recaba toda la información de hardware y software y notifica los cambios al servidor, que los muestra en la consola bajo la pestaña **Auditoría.**

El apartado **Hardware** muestra la información relevante del dispositivo móvil:

- Sistema operativo y versión.
- Modelo.
- ICCID (Integrated Circuit Card ID, identificador internacional de la SIM).
- Operador de la SIM instalada.
- Número de teléfono de la SIM instalada.
- Almacenamiento (memoria interna y SD instaladas).
- Adaptadores de red instalados (generalmente Wifi).

En el apartado **Software** se muestran todos los paquetes instalados en el terminal.

En el apartado **Registro de cambios** se muestran los cambios a nivel hardware y software que se han producido en el dispositivo móvil.

17.4.7 Informes

Los Informes ofrecidos se adaptan al tipo de dispositivo.

El comportamiento de la pestaña **Informes** es idéntico al del resto de dispositivos Windows y Mac.

18. Registro de actividad

Registro de actividad en el Nivel Cuenta

Registro de actividad general

Registro de actividad en el Nivel Dispositivo

18.1. Introducción

Panda Systems Management mantiene un registro de la actividad desarrollada por los administradores del servicio. Con este registro se puede comprobar los cambios que se realizaron en los dispositivos de los usuarios, quien los realizo y en qué momento.

El registro de actividad está distribuido en tres secciones de la consola, dependiendo del nivel de detalle que se quiera conseguir.

18.2. Registro de actividad del Nivel Cuenta

Haz clic en el menú general **Cuenta,** la pestaña **Informes** y después en el selector **Actividad.**

El registro de actividad del nivel Cuenta muestra únicamente los movimientos de los dispositivos entre zonas, indicando la fecha y hora del movimiento.

18.3. Registro de actividad general de usuario

Haz clic en el menú general **Ajustes,** pestaña **Usuarios** y después en el selector **Registro de actividad** para visualizar las acciones más importantes ejecutadas por los administradores de red sobre la consola de administración.

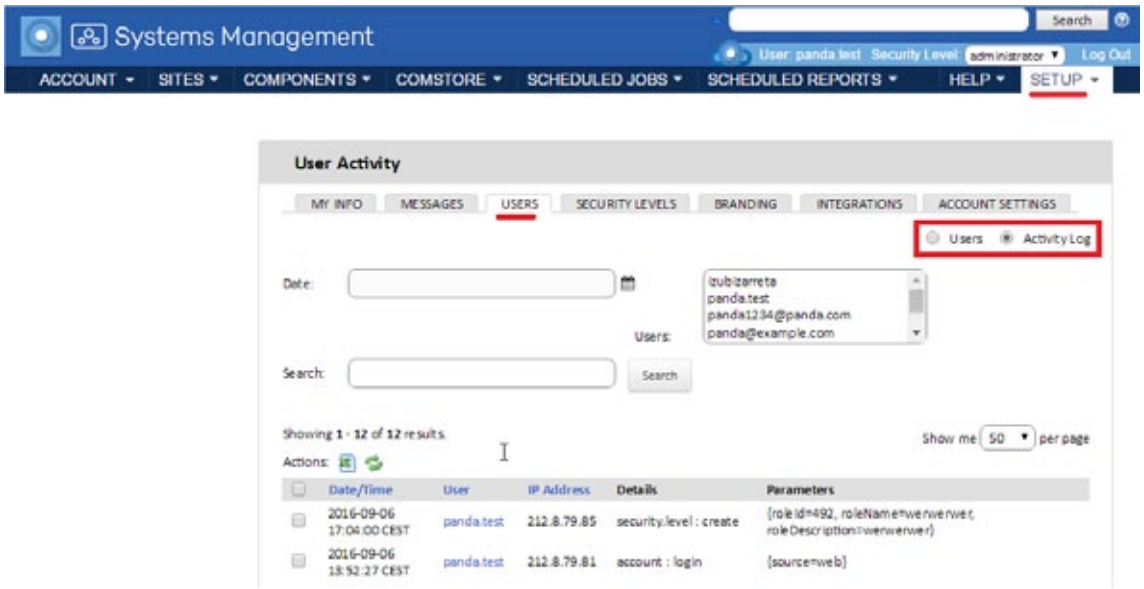


Figura 103: listado de acciones ejecutadas por el administrador

18.3.1 Listado de actividades

Consiste en una tabla - listado de actividad, con la siguiente información por cada acción registrada:

- **Casilla de selección**: selecciona registros de la lista para ejecutar sobre ellas acciones como exportar a Excel los registros seleccionados.
- **Fecha / hora**: muestra la fecha, hora y huso horario del registro de la acción.
- **Usuario**: muestra el usuario de **Panda Systems Management** utilizado por el administrador para realizar la acción.
- **Dirección IP**: muestra dirección IP desde la cual el administrador se conectó a la consola
- **Detalles**: muestra la entidad de **Panda Systems Management** sobre la cual se realizó la acción y el tipo de acción que fue ejecutada.
- **Parámetros**: muestra los campos y los valores que la acción aplicó a la entidad afectada.

18.3.2 Filtrado y búsqueda de actividades

Para facilitar la búsqueda de actividades se implementan las herramientas mostradas a continuación:

Fecha

Selecciona un intervalo de tiempo de varias formas diferentes atendiendo a la precisión y velocidad de configuración del filtro

- **Rápido**: selecciona uno de los intervalos pre configurados por defecto: últimas 24 horas, últimos 2 días, últimas dos semanas, último mes, últimos dos meses, últimos 6 meses.
- **Custom Range**: selecciona de forma libre el inicio y el final del intervalo.

Usuarios

Muestra un desplegable donde se puede elegir un usuario. Al elegir un usuario se mostrará únicamente el registro de su actividad.

Búsqueda

filtra por el contenido de los campos registrados.

18.4. Registro de actividad del Nivel Dispositivo

Visualiza las acciones ejecutadas sobre un dispositivo concreto sin importar el usuario / administrador que las lanzó.

El acceso a este registro se efectúa de dos maneras:

- En el menú general **Zonas** selecciona la zona que contiene el dispositivo el dispositivo indicado y haz clic en pestaña **Resumen** del nivel dispositivo.

- Haz clic en la pestaña **Informes** y en el selector **Registro de actividad.**

En ambos casos se muestra un listado de acciones, una entrada por actividad, con la siguiente información:

- **Tipo**: indica el tipo de actividad realizada sobre el dispositivo mediante un icono.
  - Escritorio remoto por RDP.
  - Captura remota de pantalla.
  - Lanzamiento de tarea.
  - Apertura de Shell remota.
  - Escritorio remoto por VNC.
  - Transferencia de ficheros.
- **Nombre**: nombre de la actividad.
- **Iniciado**: fecha de comienzo de la actividad
- **Finalizado**: fecha de finalización de la actividad.
- **Estado**: estado de la actividad.
  - **Resultados**: muestra el resultado de la intervención del administrador haciendo clic en el icono.
  - **Progreso**: si la actividad es una tarea se añade una barra de progreso indicado su estado.
  - **Stdout**: haz clic en el icono si la tarea configurada muestra datos en la salida estándar como resultado de su ejecución.
  - **Stderr**: haz clic en el icono si la tarea configurada muestra datos en la salida estándar como resultado de su ejecución se muestran.

19. Informes

19.1. Introducción

Panda Systems Management visualiza de múltiples maneras la información recogida del parque informático, una de ellas es a través del sistema de informes.

El sistema de informes permite volcar el estado de los dispositivos en pdfs entregables, con una información de detalle configurable dependiendo de las necesidades y del público al que vaya dirigido. También se puede volcar la información en formato .xls en caso de que se desee gestionar mediante herramientas externas la información de detalle contenida en el informe.

Existen más de 50 informes que cubren todos aspectos gestionados por **Panda Systems Management**. En este capítulo se muestra la manera de seleccionar el informe adecuado para cada público objetivo, así como se describe cada informe de forma general.

19.2. Acceso a la funcionalidad de informes

El sistema de informes se encuentra accesible en los tres niveles de **Panda Systems Management**. El grado de detalle de la información variará dependiendo del nivel elegido, así como el ámbito de los dispositivos que participarán con información en el informe.

No todos los informes están disponibles en todos los niveles; muchos de ellos solo se ajustan a dispositivos particulares (Nivel dispositivo) o tienen más sentido para una zona o para toda la cuenta administrada.

Los tres niveles de informes son accesibles desde la pestaña **Informes** del menú de pestañas. Si el menú de pestañas es accedido desde el menú general **Cuenta** se mostrará una ventana con los informes accesibles para el nivel. De la misma forma seleccionando una zona concreta o un dispositivo, la pestaña **Informes** mostrará los informes accesibles al Nivel Zona y para el nivel Dispositivo respectivamente.

19.3. Generación de informes

La generación de informes puede ser bajo demanda o programada.

19.3.1 Generación de informes bajo demanda

Haz clic en los iconos  del listado de informes en la pestaña **Informes** para lanzar una recopilación de datos en segundo plano. Cuando el proceso se complete, se mostrará un popup de descarga en la esquina superior derecha de la pantalla.

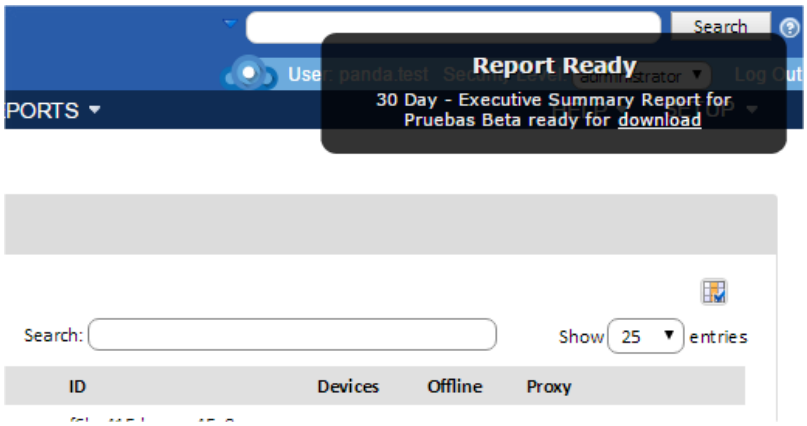


Figura 104: popup de descarga de informes

Se pueden lanzar tantas generaciones de informes como sean necesarias a lo largo del tiempo.

19.3.2 Generación de informes programados

Para programar la generación de informes haz clic en el icono  de la barra de acciones de la pestaña **Informes**.

Se mostrará una nueva ventana con la información necesaria para programar la ejecución de uno o varios informes.

- **General**
  - **Nombre**: nombre de la tarea programada de generación de informes.
  - **Descripción**
  - **Calendario**: determina cuándo se ejecutará la tarea de generación de informes.
  - **Activado**: activa o desactiva las configuraciones de generación de informes con el objetivo de tenerlas preparadas, pero sin que generen ruido innecesario.
- **Informes:** selecciona los informes a generar, en pdf y / o en Excel.
- **Destinatarios de correo electrónico**
  - **Asunto**
  - **Cuerpo**
  - **Destinatarios de informes de cuenta predeterminados**: envía los informes a las cuentas de correo definidas para toda la cuenta de **Panda Systems Management**, configurables en la sección Destinatarios de correo del menú general Ajustes.
  - **Destinatarios predeterminados de los informes de zona**: envía los informes a las cuentas de correo definidas para la zona, configurables en la sección Destinatarios de correo del menú de pestañas Configuración, dentro de la zona seleccionada.
  - **Destinatarios adicionales**: añade cuentas de correo adicionales a las configuradas a nivel de Zona o Cuenta.

19.4. Características de los informes y tipos de información contenida

Los informes están definidos por parámetros y características predefinidas que es necesario conocer para poder generar el informe más adecuado. Los parámetros quedan reflejados en el nombre del informe y en el nivel (Cuenta, Zona o Dispositivo) en el que fueron creados.

A continuación, se indican los parámetros que definen un informe:

- Nivel de creación
- Intervalo
- Tipo de informe

19.4.1 Nivel de creación

El nivel de creación (Cuenta, Zona o Dispositivo) se utiliza para definir el ámbito del informe.

- **Cuenta**: abarca todos los dispositivos de la cuenta.
- **Zona**: abarca los dispositivos de la zona elegida.
- **Dispositivo**: abarca el dispositivo seleccionado.

19.4.2 Intervalo

Determina el rango temporal de los sucesos que abarcará el informe. El intervalo viene definido en el nombre del informe mediante el prefijo "x day".

- **30 day**: contiene información de los últimos 30 días. El informe abarca los datos correspondientes hasta el día anterior a su generación.
- **7 Day**: contiene información de los últimos 7 días. El informe abarca los datos correspondientes hasta el día anterior a su generación.
- **Sin prefijo**: informes que no consolidan información a lo largo del tiempo, sino que muestran el estado de los dispositivos en el momento en que se genera el documento.

En algunos casos el informe abarca semanas o meses vencidos. Estos casos se indican en la descripción del informe y se corresponden con aquellos utilizados por los partners (VAR o MSP) y destinados a clientes finales para justificar las intervenciones del periodo de facturación.

19.4.3 Tipo de informe

El tipo de informe se indica en el nombre y refleja los aspectos del parque informático que cubre. A continuación, se muestran los diferentes tipos de informe y más adelante en este capítulo se agrupan los diferentes informes según su tipo, explicando cada uno de ellos.

Executive

Reúnen en un mismo documento resúmenes consolidados de varios aspectos de la red administrada. Son útiles para determinar el estado de la red de forma rápida, sin entrar en demasiado detalle, y para mostrar tendencias y evoluciones.

Activity

Muestran la actividad de los administradores de red gestionando los dispositivos de la empresa. Dependiendo del informe la actividad se puede desglosar en las siguientes partidas:

- Tareas
- Líneas de comando remotas
- Soporte remoto
- Notas

Alert

Muestran las alertas generadas por monitores y otros componentes, que permiten a su vez determinar el buen funcionamiento del parque informático. También muestran la productividad tanto de los empleados que ven disminuidos los tiempos de parada por fallos de sus dispositivos, como la de los técnicos de IT, medida en el tiempo medio de resolución de incidencias.

Inventariado

Recopilan los activos gestionados por el departamento de IT, tanto hardware como software, y así determinar si hay tecnología en el parque informático ya obsoleta o con alta probabilidad de fallo que deba de ser sustituidos por componentes más modernos.

Health

Reflejan la propensión a problemas de los dispositivos, dependiendo de parámetros como la existencia de antivirus, falta de aplicación de parches críticos etc.

Performance

Indican la evolución del consumo de CPU, disco duro y otros parámetros que dan indicios del buen funcionamiento del equipo.

Patch management

Reflejan el nivel de parcheo de los equipos de la red administrada: que parches faltan, cuáles de ellos son críticos y que rol tienen los dispositivos de la red.

Otros informes

Son los informes que no encajan claramente en ninguna de las anteriores.

19.5. Informes Ejecutivos

19.5.1 30/7 Day Account Executive Summary (Account)

Intervalo: últimos 7 o 30 días.

Ámbito: cuenta.

Información

- Las 5 zonas principales por número de actividades.
- Las 5 zonas principales por número de alertas.
- Por cada zona:
  - Actividades totales.
  - Alertas por categoría.
  - Actividad de cada usuario.

19.5.2 30 Day - Executive Summary Report (Site Level)

Intervalo: últimos 7 o 30 días.

Ámbito: zona.

Información:

- Información general del estado actual de los servidores:
  - Inventario.
  - Uso de disco.
  - Estado de los parches.
  - Parches críticos no instalados.
  - Tiempo activo.
- Información general del estado actual de las estaciones:
  - Recomendaciones de sustituciones.
  - Sistemas operativos en uso.
  - Comprobaciones de inventario.
- Detalles:
  - Inventario de hardware de las estaciones.
  - Uso de disco.
  - Estado de los parches y parches críticos no instalados.
- Listas:
  - Dispositivos de red administrados.
  - Dispositivos móviles administrados.

- Resumen de:
  - Alertas de monitorización (totales por categoría).
  - Actividad en los dispositivos (totales por categoría, tiempo total y número de actividades de los 5 dispositivos principales).

19.5.3 30/7 Day Site Executive Summary (Site)

Intervalo: últimos 7 o 30 días.

Ámbito: zona.

Información:

- Actividades y tiempos totales por categoría.
- Los 5 dispositivos principales por número de actividades.
- Información de cada actividad, por dispositivo.

19.5.4 30 Day - Executive Summary Report - Only Servers and Workstations (Site Level)

- Estado de los servidores:
  - Inventario.
  - Uso de disco.
  - Estado de los parches.
  - Parches críticos no instalados.
  - Tiempo activo.
- Estado de las estaciones:
  - Recomendaciones de sustituciones.
  - Sistemas operativos en uso.
  - Comprobaciones de inventario.
- Detalles de las estaciones:
  - Inventario de hardware.
  - Uso de disco.
  - Estado de los parches.
  - Parches críticos no instalados.

19.6. Informes de Actividad

19.6.1 30/7 Day Site Activity Summary

Intervalo: últimos 7 o 30 días.

Ámbito: zona.

Información:

- Actividades y tiempos totales por categoría.
- Los 5 dispositivos principales por número de actividades.
- Información de cada actividad, por dispositivo.

19.6.2 30 Day/7 Account Activity Summary

Intervalo: últimos 7 o 30 días.

Ámbito: cuenta.

Información:

- Las 5 zonas principales por número de actividades.
- Por cada zona:
  - Lista de actividades por categoría, con totales y cantidades detalladas.

19.6.3 Site Activity

Intervalo: últimos 30 días.

Ámbito: zona.

Información:

- Lista las tareas, notas y sesiones de control remoto.

19.6.4 30/7 Day Account User Summary

Intervalo: últimos 7 o 30 días.

Ámbito: cuenta.

Información:

- Lista de actividades por categoría, con totales y cantidades detalladas.
- Por cada nombre de usuario:
  - Actividad de la zona, hora de comienzo y fin, y tiempo total.

19.6.5 Remote Activity

Intervalo: último mes vencido.

Ámbito: cuenta.

Información:

- Lista todas las sesiones de control remoto:
  - Nombre de usuario, zona y nombre de host, hora de comienzo y fin, tiempo total, duración, y herramienta empleada en el control remoto.

19.6.6 Site Remote Takeover Report

Intervalo: últimos 30 días.

Ámbito: zona.

Información:

- Lista todas las sesiones de control remoto:
  - Nombre de usuario, zona y nombre de host, hora de comienzo y fin, tiempo total, duración, e icono de la herramienta empleada en el control remoto.

19.6.7 30/7 Day Device Activity Summary

Intervalo: últimos 7 o 30 días.

Ámbito: dispositivo.

Información:

- Actividades y tiempos totales por categoría.
- Detalles de cada evento de la actividad:
  - Nombre de usuario.
  - Hora de comienzo y fin.
  - Tiempo total.

19.7. Informes de Alertas

19.7.1 30/7 Day Site Alert Summary

Intervalo: últimos 7 o 30 días.

Ámbito: zona.

Información:

- Número total de alertas y tiempo medio de respuesta por categoría.
- Por cada alerta:
  - Prioridad, hora y fecha de la alerta, hora de finalización y tiempo de respuesta.

19.7.2 30/7 Day Account Alert Summary

Intervalo: últimos 7 o 30 días.

Ámbito: cuenta.

Información:

- 5 zonas principales por número de alertas.
- Por cada zona:
  - Alertas por tipo, con número total y tiempo total.

19.7.3 30/7 Day Device Alert Summary

Intervalo: últimos 7 o 30 días.

Ámbito: dispositivo.

Información:

- Número total de alertas y tiempo medio de respuesta por categoría.
- Por cada alerta:
  - Prioridad, hora y fecha de la alerta, hora de finalización y tiempo de respuesta.

19.7.4 Monitor Alerts Report (Device Level)

Intervalo: actual.

Ámbito: dispositivo.

Información:

- Para cada tipo de alerta:
  - Mensaje de la alerta, prioridad y hora de la alerta.

19.7.5 Monitor Alerts Report (Site Level)

Intervalo: actual.

Ámbito: zona.

Información:

- Indica el nombre del dispositivo, tipo de alerta, mensaje y prioridad, así como fecha/hora de la alerta.

19.7.6 Monitor Alerts Report (Account Level)

Intervalo: actual.

Ámbito: cuenta.

Información:

- Indica el nombre del dispositivo, zona, número total de alertas activas, y número de alertas activas por prioridad.

19.8. Informes de Inventario

19.8.1 Computer Summary

Intervalo: actual.

Ámbito: zona.

Información:

- Por cada equipo:
  - Nombre, sistema operativo y Service Pack.
  - Memoria, procesador, letra.
  - Espacio total de las unidades, cantidad y porcentaje de espacio libre.

19.8.2 Critical 3rd-Party Software Summary Report

Intervalo: actual.

Ámbito: zona.

Información:

- Lista todos los dispositivos Windows y Mac de la zona con un agente PCSM instalado.
  - Por cada dispositivo se incluyen las versiones de los programas más comúnmente utilizados instalados en el equipo.

- Skype
- QuickTime
- Java
- Adobe Acrobat Reader
- Mozilla Firefox
- Adobe Flash
- Adobe Air
- Adobe Shockwave
- Google Chrome
- Silverlight

19.8.3 Site Serial Numbers

Intervalo: actual.

Ámbito: zona.

Información:

- Indica cada dispositivo con su número de serie.

19.8.4 Account Server IP Information

Intervalo: actual.

Ámbito: cuenta.

Información:

- Dirección IP de todos los servidores.

19.8.5 Account Server Storage

Intervalo: actual.

Ámbito: cuenta.

Información:

- Información gráfica de la capacidad de almacenamiento de los servidores:
  - Etiqueta y tamaño de la unidad.
  - Cantidad y porcentaje de espacio.

19.8.6 Site Server Storage

Intervalo: actual.

Ámbito: zona.

Información:

- Por cada servidor:
  - Letra de la unidad.
  - Tamaño.
  - Cantidad y porcentaje de espacio libre.

19.8.7 Site Software

Intervalo: actual.

Ámbito: zona.

Información:

- Para cada software instalado:
  - Número de instalaciones.

19.8.8 Site Software and Hotfixes

Intervalo: actual.

Ámbito: zona.

Información:

- Por cada software instalado:
  - Hotfixes y actualizaciones.
  - Número de instalaciones.

19.8.9 Software Audit Report

Intervalo: actual.

Ámbito: zona.

Información:

- Por cada dispositivo en la zona:
  - Software instalado.
  - Versión del software.

19.8.10 User Software Install

Intervalo: últimos 30 días.

Ámbito: zona.

Información:

- Por cada software instalado:
  - Nombre del software.
  - Versión.
  - Cambios (añadido o eliminado).
  - Fecha de la acción.

19.8.11 Site Storage

Intervalo: actual.

Ámbito: zona.

Información:

- Por cada dispositivo:
  - Nombre
  - Letra
  - Tamaño
  - Cantidad y porcentaje de espacio libre

19.8.12 Site IP Information

Intervalo: actual.

Ámbito: zona.

Información:

- Por cada dispositivo:
  - Nombre del adaptador.
  - Dirección IP.

19.8.13 Detailed Computer Audit

Intervalo: últimos 7 o 30 días.

Ámbito: cuenta.

Información:

- Por cada equipo:
  - Información de hardware: fecha y etiqueta del dispositivo, número de serie, memoria, placa madre, BIOS, procesador, vídeo.
  - Dominio y nombre de usuario.
  - Información del antivirus.
  - Fecha del último contacto.
  - Sistema operativo, Windows Update.
  - Direcciones IP y MAC.
  - Tamaño de la unidad de disco física y espacio libre.

19.8.14 Device Summary

Intervalo: actual.

Ámbito: dispositivo.

Información:

- Por cada dispositivo:
  - Versión y estado del agente.
  - Dominio, último usuario.
  - Fecha de la última auditoría, fecha en que fue visto por última vez.
  - Hardware: fabricante, modelo, ID, placa madre, procesador, memoria, almacenamiento, adaptador de pantalla y red, e información del monitor.
  - Software: sistema operativo, service pack, número de serie, software instalado con su número de versión.

- Seguridad: antivirus, firewall y actualizaciones.

19.8.15 Device Change Log

Intervalo: desde que se instaló el agente.

Ámbito: dispositivo.

Información:

- Cambios en el sistema:
  - Fecha en la que se cambió, añadió o eliminó software.
  - Fecha y dirección IP.

19.8.16 Site Device

Intervalo: actual.

Ámbito: zona.

Información:

- Por cada dispositivo:
  - Dirección IP.
  - Fecha de la última actualización.
  - Modelo, número de serie.
  - Último usuario conectado.

19.8.17 Inventory Age

Intervalo: actual.

Ámbito: zona.

Información:

- Recomendaciones para la sustitución de dispositivos en un plazo de 12 meses a 2 años.
- Sistemas operativos en uso.
- Listado de cada dispositivo por nombre, último usuario, número de serie y fecha de compilación.
- Avisos por baja memoria, bajo espacio libre en disco o por no haber estado online durante el mes actual.

19.8.18 Microsoft License

Intervalo: actual.

Ámbito: zona.

Información:

- Tipo de software, nombre del producto Microsoft, y número de dispositivos con dicho producto instalado.

19.9. Informes de estado

19.9.1 Customer Health Summary

Intervalo: actual.

Ámbito: zona.

Información:

- Resumen de hardware.
- Resumen de seguridad.
- Resumen de software de mantenimiento.
- Reproductores y lectores instalados.
- Número de dispositivos que han superado o suspendido el test.
- Dispositivos con avisos.

19.9.2 Exception Report

Intervalo: Actual.

Ámbito: zona.

Información:

- Resumen de todos los dispositivos MS Windows:
  - Sin antivirus actualizado.
  - Sin actualizaciones de MS.
  - Sin firewall.
  - Dispositivos con bajo espacio libre en disco.
  - Dispositivos que no hayan estado online durante el mes actual.

19.9.3 Site Health

Intervalo: actual.

Ámbito: zona.

Información:

- Número de dispositivos por sistema operativo:
  - Número de compilación.
- Número de dispositivos:
  - Sin antivirus actualizado.
  - Sin actualizaciones de MS o sin firewall.
  - Con bajo espacio libre en disco o memoria.
  - Que no hayan estado online durante el mes actual.
- Por cada dispositivo:
  - Nombre.
  - Último usuario conectado.
  - Estado.

19.9.4 Health Report

Intervalo: últimos 30 días.

Ámbito: zona.

Información:

- Informe por servidores y estaciones, con y sin avisos.
- Alertas, tareas ejecutadas y duración de control remoto (minutos).
- Resumen del tiempo de respuesta a las alertas.
- Listado de cada dispositivo por nombre de host, dirección IP, y último usuario conectado.
- Avisos de equipos con antivirus y anti-spyware desactualizado, sin actualizaciones de MS o sin firewall.
- Avisos de equipos con bajo espacio libre en disco y que no hayan estado online durante el mes actual.

19.10. Informes de Gestión de Parches

19.10.1 Patch Management Activity Report

Intervalo: últimos 30 días.

Ámbito: zona.

Información:

- Por cada dispositivo:
  - Número de parches publicados, instalados y pendientes de instalación.
  - Porcentaje de parches pendientes de instalación y número de alertas.
- Dispositivos a los que les faltan parches.
- Resumen y análisis de los dispositivos completamente parcheados y a los que les faltan parches por instalar.
- Lista detallada de parches por dispositivo:
  - Nombre.
  - Severidad.
  - Estado de instalación.

19.10.2 Patch Management Detailed Report

Intervalo: actual.

Ámbito: zona.

Información:

- Por cada dispositivo:
  - Número de parches disponibles, instalados y no instalados.
  - Porcentaje de parches no instalados y número de alertas.
- Dispositivos a los que les faltan parches.
- Resumen y análisis de los dispositivos a los que les faltan parches por número de parches necesarios.
- Lista detallada de parches por dispositivo:
  - Nombre.
  - Severidad.
  - Estado de instalación.

19.10.3 Patch Management Summary Report

Intervalo: actual.

Ámbito: zona.

Información:

- Porcentaje de dispositivos con todos los parches instalados, o a los que les falten un número específico de parches.
- Dispositivos a los que les faltan parches y número de parches no instalados.
- Por cada dispositivo:
  - Número de parches disponibles, instalados y no instalados.

19.11. Otros informes

19.11.1 Site User-Defined Fields

Intervalo: actual.

Ámbito: zona.

Información:

- Informe sobre los campos personalizados de la zona.

19.11.2 Server Performance Report (Site Level)

Intervalo: últimos 30 días.

Ámbito: zona.

Información:

- Muestra el rendimiento de cada servidor en relación a los siguientes aspectos:
  - CPU.
  - Memoria.
  - Disco.
  - Uso medio de CPU y memoria.
  - Diferencial del espacio disponible en disco.

19.11.3 Server Performance Report (Account Level)

Intervalo: actual.

Ámbito: cuenta.

Información:

- Muestra el rendimiento de cada servidor en relación a los siguientes aspectos:
  - CPU.
  - Memoria.
  - Disco.
  - Uso medio de CPU y memoria.
  - Diferencial del espacio disponible en disco.

20. Seguridad y control de acceso al servicio

Autenticación en dos fases

Política de contraseñas

Restricción por IP del acceso a la Consola

Restricción por IP del Agente al Servidor

20.1. Introducción

Para mejorar la seguridad del acceso al servicio el administrador dispone de varias herramientas, entre las que se encuentran:

- Activación del sistema autenticación en dos fases.
- Establecimiento de una política de contraseñas.
- Restricción por IP del acceso a la consola.
- Restricción por IP del agente al servidor.

20.2. Autenticación en dos fases

Autenticación en dos fases obliga al uso de un segundo dispositivo para validar las credenciales del administrador introducidas en la pantalla de login de la consola. De esta forma, además de introducir sus credenciales, el administrador deberá proveer un código personal que se genera cada minuto de forma automática en su dispositivo móvil.

La autenticación en dos fases únicamente afecta al acceso a la consola y, por tanto, está destinado al administrador de la red. Ni los usuarios ni los administradores de red que acceden a otros dispositivos a través del agente se ven afectados por las configuraciones aquí descritas.

20.2.1 Requisitos para su funcionamiento

- Dispositivo móvil compatible con una aplicación para la generación de tokens.
- Aplicación gratuita `Google Authenticator` o compatible instalada en el dispositivo móvil.

20.2.2 Configuración

Para activar la autenticación en dos fases en la cuenta del administrador que ha hecho login en la consola:

- En el menú general **Ajustes**, **Información personal** haz clic en el botón **Habilitar autenticación en dos fases,** situado en la sección **Configuración de la seguridad**.
- Aparecerá un código QR en pantalla y un espacio para introducir el token. Este token será generado por la aplicación `Google Authenticator`. En caso de no disponer de una aplicación de autenticación capaz de leer un código QR, puedes activar la casilla para que el sistema envíe un código QR a la dirección de correo del administrador, especificada en esa misma ficha.
- Instala la aplicación `Google Authenticator` desde la Google Play en el dispositivo móvil propiedad del administrador que accede a la consola (ver Instalación `de Google Authenticator,` más adelante en este capítulo).

- Toca en **Iniciar configuración** y en **escanear el código de barras mostrado por la consola**. Si no tienes instalada ninguna aplicación de escaneo de códigos de barras, la aplicación sugerirá instalar el programa gratuito `ZXing Barcode Scanner`.

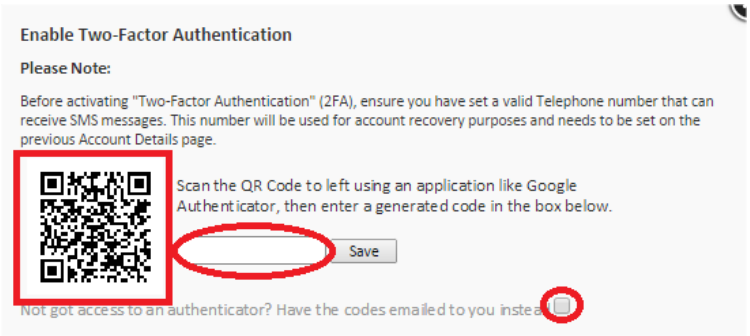


Figura 105: generación y envío por correo del token

- Una vez escaneado el código QR, la aplicación comienza a generar tokens cada 30 segundos. A continuación, es necesario introducir un token en el espacio indicado en el formulario de login de la consola. Una vez hecho esto, se activará completamente la autenticación en dos fases.
- A partir de este momento el administrador únicamente podrá acceder a su cuenta si introduce sus credenciales correctamente y un token válido.

20.2.3 Instalación de Google Autheticator

Para la instalación de `Google Autheticator` en un dispositivo móvil compatible con Android sigue los pasos mostrados a continuación:

- Descarga de la aplicación de Google Play.
- Una vez iniciada la aplicación pulsar **Begin Setup.**

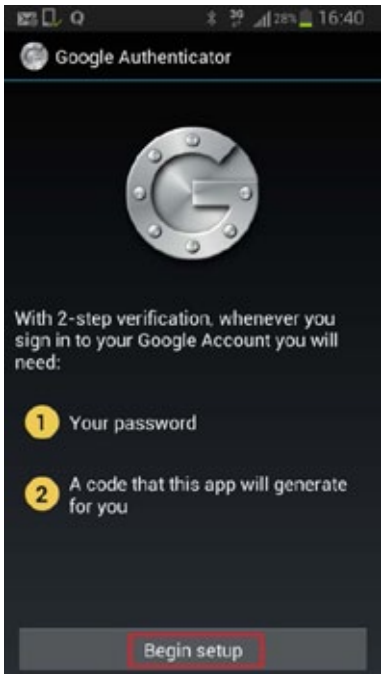


Figura 106: pantalla de configuración de la aplicación Google Authenticator

- Pulsa en **Scan a barcode** para escanear el código QR mostrado en la consola.

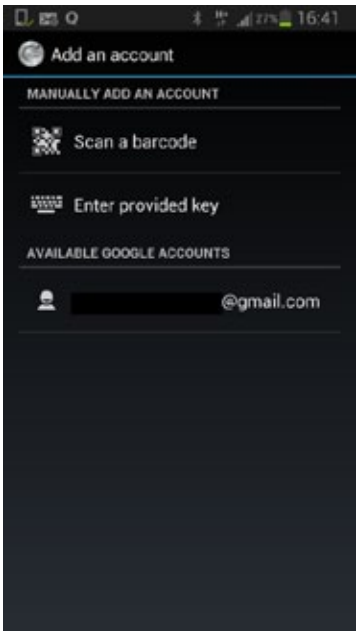


Figura 107: escaneo del código QR

- La aplicación comenzará a generar token de forma automática. Cada token tiene un periodo de validez de 30 segundos.

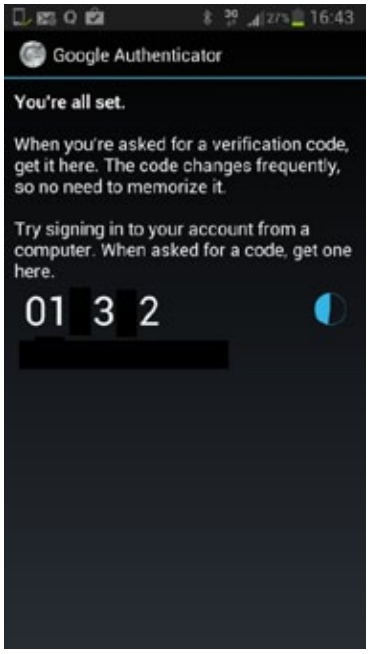


Figura 108: pantalla de generación de tokens

20.2.4 Habilitar Autenticación en dos fases para todas las cuentas

Una vez habilitada la autenticación en dos fases para la propia cuenta de acceso del administrador, puedes forzar su uso al resto de cuentas de administración creadas en la consola. Para ello, haz clic en el menú general **Ajustes**, **Configuración de cuenta**, **Requerir autenticación en dos fases** en la sección **Control de acceso.**

Para forzar el uso de la autenticación en dos fases al resto de cuentas de acceso, es necesario que la cuenta desde la que se realiza la configuración tenga ya habilitado el uso de la autenticación en dos fases.

Cada vez que un usuario sin la autenticación en dos fases configurado acceda a la consola, se le mostrará un mensaje de advertencia, impidiendo la navegación.

20.2.5 Desactivar la autenticación en dos fases desde la pantalla de login

Desde la pantalla de login, es posible desactivar el servicio de autenticación en dos fases. Para ello, es necesario ingresar el usuario y contraseña correctamente, momento en que se mostrará la pantalla de petición de token. En la parte inferior se mostrará el link **Disable TOTP**. Al hacer clic en el link, el servidor enviará un SMS con un código válido solo durante 10 minutos al número de teléfono configurado en el sistema. Al introducir el código, el servicio de autenticación en dos fases quedará desactivado.

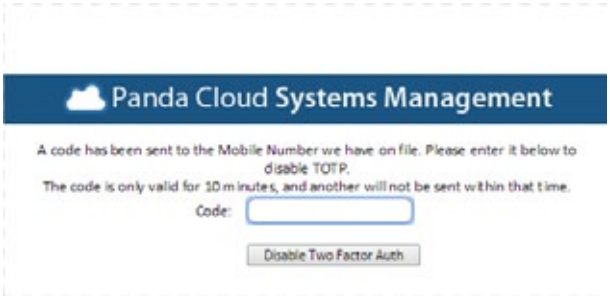


Figura 109: ventana para desactivar la autenticación en dos fases

20.3. Política de contraseñas

Para reforzar la seguridad del acceso a la consola puedes establecer una política de contraseñas que obligue a que todas las contraseñas elegidas cumplan una serie de requisitos.

Para configurar una política de contraseñas accede al menú general **Cuentas, Configuración** y allí establece valores para los campos:

- **Vencimiento de contraseña**: establece el tiempo máximo de duración de la contraseña elegida (30, 60, 90 días o nunca expira).
- **Contraseñas únicas**: el sistema guarda un listado de contraseñas por cada cuenta, de forma que le impide al administrador reutilizarlas al requerir un cambio de contraseña. El listado/histórico de contraseñas guardado tendrá la longitud elegida desde 0 (nunca) hasta 6 entradas.

20.4. Restricción por IP del acceso a la consola

Para limitar el acceso a la consola a un conjunto de IPs conocidas, en el menú general **Cuenta, Ajustes** activa la funcionalidad **PCSM Console Restricción de dirección IP** indicando además en **Lista de IP restringidas** un listado de IPs desde donde será posible acceder a la consola.

20.5. Restricción por IP del Agente al Servidor

Para limitar el acceso de los agentes al servicio, en el menú general **Cuenta, Ajustes** activa la funcionalidad **Agente Restricción de dirección IP** indicando además en **Lista de IP restringidas** un listado de IPs desde donde los agentes podrán acceder al servidor.

21. Apéndice A: código fuente

Capítulo 10

Capítulo 11

21.1. Capítulo 10

```
Option Explicit
'*********************************************************************
'Quarantine_Monitor v0.99b
'06/03/2013
'By Oscar Lopez / Panda Security
'Target: It monitors changes on PCOP quarantine folder
'Input: PCOP_PATH environment variable
'Output: stdout "Result=n new items detected in PCOP quarantine",
'n is the added file number in the monitored folder
'*********************************************************************

dim WshShell,WshSysEnv
dim objFSO,objFolder,colFiles
dim iCountPast,iCountNow
dim bHit
Dim n

Set WshShell = WScript.CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSistemaObject")

'access to environment variable and quarantine path
On error resume Next
    Set WshSysEnv = WshShell.Environment("PROCESS")
    Set objFolder = objFSO.GetFolder(WshSysEnv("PCOP_PATH"))
    if err.number <> 0 then
        'SM didn't send the environment variable
        err.clear
        WScript.Echo "<-Start Result->"
        WScript.Echo "Result=PCOP_PATH variable not defined on SM console or
path not found"
        WScript.Echo "<-End Result->"
        Set WshShell = nothing
        Set WshSysEnv = nothing
        Set objFolder = nothing
        WScript.Quit(1)
    end if
On error goto 0

'it gets the collection that contains the folter files
set colFiles = objFolder.files

On error resume Next
    'access to the registry. 10 incremental entries will be created, one per
minute.
    n=0
    While Err.Number=0 And n < 10
        iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda
Security\Monitor" & n))
        If err.number<>0 then
            WshShell.RegWrite "HKLM\Software\Panda Security\Monitor" & n,
colFiles.count, "REG_SZ"
        Else
            n=n+1
        End If
    Wend
    Err.Clear
```

```
    If n=9 Then
        iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda
Security\Monitor0"))
        iCountNow= cint(WshShell.RegRead("HKLM\Software\Panda
Security\Monitor9"))
        if iCountPast < iCountNow then
            'there are more items in the folder, it updates the registry and
sends an alert
            WScript.Echo "<-Start Result->"
            WScript.Echo "Result=" & iCountNow - iCountPast & " new items in
PCOP quarantine"
            WScript.Echo "<-End Result->"
            bHit=true
        end if
        For n=0 To 9
            WshShell.RegDelete("HKLM\Software\Panda Security\Monitor" & n)
        Next
        WshShell.RegWrite "HKLM\Software\Panda Security\Monitor0",
colFiles.count, "REG_SZ"

    end if
On error goto 0

'finale
Set colFiles = nothing
set objFolder = nothing
set WshShell = nothing
set WshSysEnv = nothing
set objFSO = nothing

if bHit then
    WScript.Quit (1)
else
    WScript.Quit (0)
end if
```

21.2. Capítulo 11

```
Option Explicit
'**********************************************************************
'Deploy_documents v0.99b
'12/03/2013
'By Oscar Lopez / Panda Security
'Target: It creates a folder int the user's desktop and copy on it the
'documents to deploy
'Entrada: files to copy
'Salida: error code or OK
'**********************************************************************

Dim CONST_PATH
Dim objFSO,objFolder,colFiles

'Maybe you want to use a global variable for this constant?
CONST_PATH="C:\ACME Documents"
On Error Resume Next
    Set objFSO=CreateObject("Scripting.FileSistemaObject")
    Set objFolder = objFSO.Getfolder(CONST_PATH)
    If Err.Number=0 Then
        'the folder already exists, the files won't be copied
        WScript.Echo "Deploy unsuccessful: The folder already exists"
        WScript.Quit (0)
    End If

    'the folder will be created in the user's desktop
    Err.Clear
    Set objFolder = objFSO.CreateFolder(CONST_PATH)
    'the documents will be moved to the folder
    objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
    objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
    objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
    If Err.Number<>0 Then
        WScript.Echo "Deploy unsuccessful: " & Err.Description
        WScript.Quit (1)
    Else
        WScript.Echo "Deploy successful: All files were copied"
        WScript.Quit (0)
    End If
On Error Goto 0
WScript.Quit (0)
```

22. Apéndice B: plataformas soportadas

Plataformas soportadas

Requisitos Windows detallados

Requisitos de administración VMWARE ESXi

22.1. Plataformas soportadas

Para Windows

- Windows XP SP3 (ediciones Home, Profesional, Profesional x64)
- Windows Vista 32/64-bit (ediciones Starter, Home Basic & Premium, Business, Enterprise, Ultimate)
- Windows Server 2003 & R2 SP2 32/64-bit (ediciones Web, Standard, Enterprise, Datacenter, Small Business, Home Server)
- Windows 7 (32/64-bit)
- Windows 8/8.1 (32/64-bit)
- Windows 10 (32/64-bit)
- Windows 2008 & R2 32/64-bit (ediciones Standard, Enterprise, Datacenter, Web, Small Business)
- Windows Server 2012 (64-bit) & Windows Server 2012 R2
- Windows Server 2016 (64-bit)

Para Apple Macintosh (1)

- macOS 10.12
- macOS 10.13

Para Linux

- Fedora 19, 20, 21, 22, 23
- CentOS 7
- Debian 7, 8 **(2)**
- Ubuntu LTS
- Red Hat Enterprise Linux 7 y versions posteriors **(3)**

Para teléfonos móviles y tablets

- iOS 7 y superiores
- Android 2.3.3

Exploradores compatibles: (4)

La consola PCSM está probada con las dos últimas versiones de los navegadores listados a continuación:

- Internet Explorer
- Google Chrome
- Mozilla FireFox
- Safari

(1) El agente PCSM es compatible con las versiones macOS 10.7.x y posteriores, aunque Panda Security solo ofrece soporte en las versiones indicadas.

(2) El agente PCSM es compatible con cualquier distribución basada en Debian, aunque Panda Security solo ofrece soporte en las versiones indicadas.

(3) En nuevas instalaciones del agente PCSM es necesario instalar previamente las librerías Mono.

(4) La consola PCSM puede funcionar con versiones de navegadores anteriores u otros proveedores, aunque Panda Security solo ofrece soporte en las versiones indicadas.

22.2. Requisitos de equipos Windows detallados

El agente **Systems Management** requiere de ciertos componentes para completar el despliegue en dispositivos Windows. En caso de no encontrarse instalados, el proceso de instalación descargara e instalara de forma silenciosa todas las dependencias necesarias.

El proceso de descarga e instalación de dependencias solo se produce de forma automática en la instalación de nuevos agentes. Los procesos de actualización de versión no incluyen este proceso. Un dispositivo con una versión del agente PCSM instalada que no cumple con los requisitos no se actualizará.

Las dependencias necesarias son:

- **Framework.NET Full 4.0** (requisito para framework.NET 4.0.3 (https://www.microsoft.com/en-us/download/details.aspx?id=17718)
- **Framework .NET Full 4.0.3** (https://www.microsoft.com/en-us/download/details.aspx?id=29053)

Se requiere la versión full, no la versión Client del framework. NET 4.0.3

Los sistemas operativos Windows 7 y posteriores cumplen con estos requisitos de forma automática.

- **Windows Imaging Component** (https://www.microsoft.com/en-us/download/details.aspx?id=32)

22.3. Requisitos de administración VMWare ESXi

Los servidores VMWare se gestionan a través de dispositivos Windows con el rol Nodo de red activado. No es necesario que el nodo de red y el servidor ESXi residan en la misma subred.

Panda Systems Management es compatible con las versiones ESXi 4.1, 5.0, 5.1, 5.5, 6.0 y 6.5.

Para la versión VMWare ESXi 6.5 es necesario conectarse por ssh para activar el acceso por CIM.

- Activa el servicio SSH en el servidor ESXi
- Abre una línea de comandos con el servidor ESXi por ssh. Utiliza Putty o un programa compatible.
- Ejecuta los comandos siguientes:

```
esxcli system wbem set --enable true
/etc/init.d/sfcbd-watchdog start
```

euskaltel

Panda Systems Management